Technische Universität Ilmenau
Fakultät für Informatik und Automatisierung
Institut für Praktische Informatik und Medieninformatik
Fachgebiet Telematik

Hauptseminar Telematik

IPv6

Bearbeiter: Martin Heise
Ingenieurinformatik

Betreuer: Dipl.-Inf. Thorsten Strufe
Dipl.-Inf. Ralf Döring

Gliederung

IPv6 – das Internet-Protokoll der „nächsten Generation"

Vor ca. einem Jahrzehnt gab es bereits die ersten Ansätze.
Trotzdem ist heute immer noch IPv4 der Standard.
Oder doch nicht? Was ist eigentlich mit „*IPv6*"?

1. Einführung und Motivation

IPv6 ist die Abkürzung für „Internet Protocol Version 6". Bisher basiert der grösste Teil des Internets sowie seiner angeschlossenen Netze auf IPv4. Was ist *IPv6*, was ist neu daran? Und wozu eigentlich? Diesen Fragen soll hier nachgegangen werden, wobei der Fokus auf den (notwendigen?) neuen Features sowie Möglichkeiten zum „sanften" Übergang (Migration) der bisherigen IPv4-Struktur auf *IPv6* liegen soll. Diese Arbeit soll das Bewusstsein für *IPv6* stärken (awareness) und dem Leser vor Augen führen, welche Vorteile die Nutzung von *IPv6* für aktuelle oder zukünftige Projkete hat und warum trotz offensichtlicher Vorteile und teilweise sogar Notwendigkeiten *IPv6* noch nicht zum permanenten Standard geworden ist.
Bezüglich genauerer Details im Aufbau des Protokolls an sich, seiner Optionen/Erweiterungen und Headerformate wird auf die im Angang aufgeführten Quellen verwiesen; insbesondere die Requests for Comments (RFC), welche wohl die eindeutigste Quelle für die direkte Arbeit am und mit dem Protokoll darstellen.

IPv4 ist schon mehrere Jahrzehnte im Einsatz und hat sich dort auch bewährt. Dennoch wurden einige Verbesserungswünsche laut, Schwächen bekannt, und natürlich der Wunsch nach neuen Merkmalen wie Quality of Service (QoS) und Sicherheit. Nicht zuletzt stellt sich die Frage, ob IPv4 weiterhin mit dem Wachstum der Netzwerke standhalten kann. Gerade im letzten Jahrzehnt des vergangenen Jahrhunderts entstand eine Zahl von Erweiterungen zu IPv4, die – parallel mit den ersten Diskussionen um *IPv6* – einige der Schwächen von IPv4 bereits vor Einführung von *IPv6* beheben sollten (stellvertretend seien hier z.B. Classless Internet Domain Routing (CIDR) und Network Address Translation (NAT)/Masquerading genannt). Bedeuten diese Erweiterungen nun, dass *IPv6* ein akademisches Produkt bleibt, weil man bereits alles hat, was man braucht? Auch dies soll hier diskutiert werden. Nicht alle gewünschten Erweiterungen lassen sich aber einfach so einführen. Als Beispiele seien hier Erweiterungen des IPv4-Headers oder der Paketfragmetierungsstrategie erwähnt. Daraus wird bereits ersichtlich, dass *IPv6* weit mehr ist als nur der grössere Adressraum, welcher wohl dennoch das populärste Merkmal von *IPv6* ist.
Die immer weiterführende Expansion der vorhandenen Netzwerke und deren globaler Zusammenschluss führen zur Notwendigkeit, diese

logisch wieder in kleinere, leicht administrierbare Teile zu zerlegen. IPv4 mit seiner flachen Adressstruktur macht dies nur bedingt möglich; hierbei war der Übergang von der alten, klassenbasierten Stuktur zur mittlerweile als Standard geltenden Adressierung frei definierbarer Subnetze schon ein grosser Schritt. *IPv6* geht jedoch auch hier noch weiter und unterstützt somit insbesondere auch Administratoren und Netzwerkplaner bei ihrer Arbeit.

2. Volkes Stimme

IPv6 ist zwar an sich neu, aber mittlerweile auch schon eine ganze Weile im Gespräch. Nur in wie weit haben sich auch schon die Administratoren damit beschäftigt und was halten sie davon? Hier daher – recht locker – ein paar Kommentare von für IT-Infrastrukturen zuständigen Administratoren oder Leuten, die in Forschung und Lehre damit zu tun haben:

- neues Nummernschema
- mehr Sicherheit
- Umstellungsarbeiten ... somit sicherlich Ausfälle
- Auf Grund genug vorhandener v4-Adressen (NAT/Masq) kein Bedarf an v6
- Schlechter oder fehlender Support bei einigen Betriebssystemen
- An sich wird sicher kein Weg mehr daran vorbeiführen in den nächsten Jahren. Eine ernsthaft praktische Anwendung hab ich dafür aber auch noch nicht.
- *IPv6* ist gerade echt hip - wer „in" ist, der redet drüber
- Prinzipiell sehr sehr schön, nur manchen Details sind noch etwas praxisfern (meistens bei Default-Werten).
- Keine Ahnung. Ich mache es aus Zeitmangel nicht.

3. Gründe für eine neue Version

Warum eine neue Version wünschenswert ist, wurde bereits eingangs erwähnt. Das wohl primäre Motiv für einen Nachfolger des Internet-Protokoll-Standards IPv4 war der Adressraum. Weitere Bereiche, in denen Neuerungen oder Verbesserungen Teil von *IPv6* sind, seien hier noch mal aufgezählt:

- Sicherheit
- QoS
- mobile IP
- Autokonfiguration
- verbessertes Multicast
- AnyCast (z.B. für den Domain Name Service (DNS)), dafür kein Broadcast mehr
- Routing(tabellen), Scopes und Aggregation
- Verbesserung der Problematik mit der Paketfragmentierung
- erweiterbare Paketheader
- real-time flows
- veränderte Paketfragmentierungsstrategie
- ...

Warum aber nur gerade IP v6?

Als Alternativen hätte man ja auch ein Nachfolgerprotokoll von z.B. der IPX/SPX-Suite entwickeln können. Primäres Argument für IP war aber sicherlich der hohe Verbreitungsgrad der TCP/IP-Protokollsuite. Im WAN-Bereich trifft man es auf über 2/3 der Systeme an und selbst im LAN-Bereich - wo z.B. auf Grund älterer Novell-Installationen und der etwas einfacheren Konfiguration oft noch IPX/SPX eingesetzt wird – laufen bereits über die Hälfte der Netze mit TCP/IP.
Dazu kommt noch, dass in den 90er Jahren des letzten Jahrhunderts die Branchenriesen Microsoft und Novell TCP/IP standardmässig in ihre hauptsächlichen Produkte (Microsoft Windows bzw. Novell NetWare) integrierten und somit ein recht grosser Teil der ab da installierten Systeme bereits IPv4-fähig waren. Unix und dessen Derivate verstehen sowieso TCP/IP, und selbst proprietäre Betriebssysteme wie AmigaOS oder MacOS besitzen Implementierungen für einen TCP/IP-Stack.

4. Geschichte

Da die Geschichte des Internet an sich in fast jedem Buch über TCP/IP zumindestens in einem kurzen Abriss zu finden ist (vgl. Literaturliste im Anhang), soll sie hier nur kurz umschrieben werden.

Das Ende der 60er Jahre gilt als Geburtsstunde des Internets – damals unter dem Projekt (D)ARPANET, obwohl erst Anfang der 80er Jahre IPv4 eingeführt und das Netz aufgespalten wurde in das MILNET und das klassische ARPANET (Forschung). Mitte der 80er Jahre waren damit dann auch "nicht-Forscher" am Netz, also Personen, die das Netz einfach nur nutzen und nicht direkt an dessen Weiterentwicklung beteiligt sind.
In den 90er Jahren wurde der Zugang für Privatpersonen durch die Entwicklung von HTML (und dem damit aufgepannten www) sowie durch Einführung des bekannten opensource-Betriebssystems Linux und der im vorigen Kapitel erwähnten Unterstützung durch Firmen wie Microsoft und Novell immer einfacher und damit stieg natürlich auch die Anzahl der Netznutzer.

1995 schliesslich wurden mit RFC 1752 "IPng Requirements" (RFC 1883 proposed standard) die ersten Grundsteine für *IPv6* gelegt, welches zu der Zeit noch unter dem Namen "IPng" (IP next generation) firmierte. Erste Ansätze beruhten auf dem Connection-Less Network Protocol (CLNP), was sich zu TUBA (TCP/UDP over Bigger Addresses) weiterentwickelte. Als weiteren Ansatz gab es die sog. Network Service Access Point-Adresse (NSAP): 20 Oktets; jedoch waren auch hier die gewünschten weiteren Features wie QoS und Multicast nicht integriert. Auch übergreifende Versuche, ein IP-, CLNP- und IPX- kompatibles Paketformat zu erschaffen erschaffen, gab es. Und schliesslich noch Simple IP Plus (SIPP), welches den Adressraum von 32 Bit auf 64 Bit erweiterte und ein paar verbesserte Eigenschaften (z.B. bessere Routing-Strategien) aufwies. Diese 64 Bit wurden dann noch mal auf 128 Bit erweitert und daraus dann *IPv6* (die Bezeichnung IPv5 wurde bereits für ein anderes Protokoll benutzt).

5. *IPv6* heute

Die Grundidee hinter *IPv6* war also, IP prinzipiell gleich lassen, aber die mit v4 gewonnenen Erfahrungen zu nutzen, einen grösseren Adressraum zur Verfügung zu stellen und verschiedene neue Features einzubauen.

Da bereits von Anfang an klar war, dass eine schlagartige Migration auf *IPv6* nicht möglich sein würde, wurden auch weiterhin Lösungen gesucht, die man mit IPv4 einsetzen konnte ohne dies gleich komplett austauschen zu müssen. Und so entwickelte man im Laufe der Zeit einige Erweiterungen für IPv4, die Abhilfe versprachen und auch heute noch erfolgreich im Einsatz sind und weiterentwickelt werden. Dies natürlich nur teilweise und mit der Konsequenz, dass in verschiedenen Bereichen die Einführung von *IPv6* immer weiter nach hinten verschoben wird. So gibt es Multicast, Traffic Flows, IPsec und automatische Konfiguration (mittels BOOTP oder DHCP) mittlerweile auch für IPv4. Dem Problem der Adressknappheit auf Grund ungünstiger Vergabe der vorhandenen Ressourcen versucht man mit Variable-Length Subnet Mask (VLSM) und Classless Inter-Domain Routing (CIDR) zu begegnen.
Damit wurde das starre, flache Konzept der Klassen ablöst, neue IP-Adressen sollten und werden topologisch vergeben auf Grund der Möglichkeit der besseren Subnetzbildung, welche den Aufbau komplexer strukturierter Netze erlaubt. Private IP-Adressen erlauben es, Netzwerke auch ausserhalb des Internets aufzubauen und mit Lösungen wie NAT/Masquerading ist es möglich, diesen Intranets mit einer geringeren Anzahl öffentlicher IP-Adressen wieder eine Verbindung mit dem Internet zu gewährleisten. Wobei gerade im Fall von NAT/Masquerading erwähnt werden muss, dass dies seit je her einen erhöhten Administrationsaufwand bedeutet. Schwierigkeiten bereiten insbesondere Protokolle, die die IP-Adresse von Sender und/oder Empfänger nochmals im Payload eines Datenpakets enthalten – als Beispiel sei hier das File Transfer Protocol (FTP) erwähnt. Dennoch ist es heutzutage eine gängige und sehr häufig anzutreffende Praxis, Intranets auf diese Weise aufzubauen, mittels Paketfiltern in der Funktionalität wieder absichtlich einzuschränken und z.B. Verbindungen für bestimmte Protokolle nur mittels Proxies in andere Netze zuzulassen.

Die Ansichten über diese Vorgehensweise sind sehr unterschiedlich, und es liegt auch am konkreten Einsatzfall, ob sich so eine befriedigende Lösung für eine Netzanbindung aufbauen lässt. Tatsache ist jedoch, dass durch NAT/Masquerading und durch die Möglichkeit der flexibleren Subnetzbildung das Problem der Adressknappheit weiter aufgeschoben werden konnte. Die Internet Engineering Task Force (IETF) geht derzeit davon aus, dass bis ins Jahr 2010 genügend IP-Adressen zur Verfügung stehen. Als weiteren Effekt konnte durch die stärker hierarchische

Struktur der IP-Adressen auch die Grösse der Routingtabellen in den Backbone-Routern von 90k auf 60k reduziert werden.

Das klingt alles recht optimistisch, verschiebt das Problem aber nur in die Zukunft. Diese zeichnet sich bereits heute vielerorts ab:

- IP überall: Data, Voice, Audio, Video, Multimedia!
- Mobiltelephone (UMTS ... 3G, 4G & beyond)
- Personal Digital Assistents (PDA) und Laptops/Notebooks tummeln sich in den bereits vorhandenen und immer mehr entstehenden (public) Wireless LANs (WLAN)
- schätzungsweise eine Milliarde Autos im Jahr 2010 mit Global Positioning System (GPS)
- Gebiete, die in Zukunft auch noch mit IP versorgt werden wollen:China, Indien, Korea, Russland, ...
- Internet in jeder Schule
- öffentliche Netzzugänge (Bahnhöfe, in der Stadt, in Museen usw.)
- Kühlschrank und Kaffeemaschine mit IP (z.B. mit JINI)
- Kabelmodem, xDSL, Wireless: bald wird es nicht nur eine IP-Adresse pro Haushalt geben, sondern eher ein ganzes Lokales Netzwerk (LAN) pro Familie, pro Gruppe, pro Verein

... und alle brauchen IP-Adressen!

Woran liegt es also, dass *IPv6* immer noch nicht flächendeckend eingeführt wird?
Bei einer solch gross angelegten Sache wie einem neuen Internetprotokoll gibt es eine grosse Anzahl von Einflussgruppen, z.B.. Endbenutzer, Telekommunikationsunternehmen, KabelTV-Netzbetreiber, Internet Service Provider (ISP), Telephonie-Equipmenthersteller, Mobilfunknetzbetreiber, Router- und Backboneequipmenthersteller, IP-Backbone-Betreiber, Administratoren, ... Und alle haben eine Meinung, sehen in *IPv6* Vor- oder Nachteile, sehen die Neuerung als dringend notwendig oder scheuen noch den Aufwand der Umstellung bzw. zweifeln an der Sinnhaftigkeit oder Rentabilität für den jeweiligen Bereich.

Pro ...

Zur Zeit sind es hauptsächlich noch Visionäre, Hacker, ein paar Experten oder Power-Enduser, die die sofortige Einführung von *IPv6* begrüssen würden. Entscheidungsträger oder Marketing nutzen gerne die Vorteile von *IPv6* in ihren Argumentationen; allerdings nur, wenn sie sich dessen auch bewusst sind (awareness). Anwender mobiler Geräte freuen sich schon auf *IPv6* (auch hier wiederum natürlich nur insofern ihnen das etwas sagt), hoffen sie doch auf öffentliche und statische IP-

Adressen beim Einsatz ihrer Geräte an verschiedenen Netzzugangspunkten.

… zögernd …

Erstaunlicherweise scheint *IPv6* an Universitäten und anderen Forschungseinrichtungen, die sich nicht explizit *IPv6* verschrieben haben, eher eine untergeordnete Rolle zu spielen. Am Beispiel der TU Ilmenau sei erwähnt, dass es in der praktischen Informatik einen *IPv6*-Tunnel und bei der uninahen Forschungsgemeinschaft elektronische Medien e.V. (FeM) ein Projekt zum Thema gibt – beides jedoch führt eher ein Schattendasein. Im Fachgebiet Nachrichtentechnik dagegen spielt *IPv6* noch keine Rolle – was aber durchaus auch daran liegen kann, dass das dortige Augenmerk momentan auf Mobilität und drahtlosen Netzen liegt.
Die Scheu vor den Umstellungsarbeiten mit den damit verbundenen Planungen und ggf. den Ausfällen sind genau so Gründe, die Umstellung auf *IPv6* so weit wie möglich zu vermeiden, als auch der derzeit aus Sicht vieler Administratoren noch mangelnde Support bzw. das Selbstverständnis des Einsatzes von v6 bei einigen Betriebssystem und anderer Software. Oft fehlt auch einfach die Zeit, sich mit den Neuerungen zu beschäftigen, weil man mit Routineaufgaben bereits ausgelastet ist.

… und contra

Direkte Gegenstimmen bekommt man derzeit eher aus dem Lager der Software-Entwickler und auch der ISPs, die sich teilweise schon mit der Komplexität von IPv4 in ihren Projekten überfordert sehen.
Die Hersteller von Routern, Firewall-Elementen und anderen Infrastrukturkomponenten sehen das Problem am Markt: *IPv6* verkauft sich noch nicht so gut, daher ist die Entwicklung hier noch eher gering. Als Beispiel sei hier Cisco erwähnt, die für einen grossteil der Produkte bisher nur softwarebasierte *IPv6*-Lösungen für ihre Geräte anbieten. Anbieter virtueller privater Netzwerke (VPN) wiederum machen sich Sorgen, wer denn noch ihre Produkte kauft, wenn Sicherheit doch bereits in *IPv6* integriert ist – auch wenn hier noch unklar ist, ob im Endzustand hier eine wirkliche Konkurrenzsituation herrscht.
Ähnlich verhält es sich bei den Telekommunikationsanbietern; ist doch auch hier noch nicht entschieden, ob weiterhin ein separates Netz betrieben werden soll oder ob man auch auf eine Infrastruktur wie *IPv6* umsteigt. Den Vorteilen der einheitlichen Technologie steht wohl als mit wichtigster Faktor entgegen, dass die Trennung von „Internet" und „Telekommunikation" (i.S.v. Sprachkommunikation) derzeit eine gewisse Redundanz bereitstellt, falls eines der beiden Netze einmal ausfällt.

Überholt dagegen dürfte mittlerweile die ablehnende Haltung der Entscheidungsträger in der Industrie sein. Postulierte doch Felix von Leitner anno 2000 noch: "Windows hat es nicht, also brauchen wir es nicht", so hat mittlerweile *IPv6* auch den Einzug in (nicht nur) dieses mainstream-Betriebssystem gefunden.

6. Technik

Wie bereits eingangs erwähnt, soll im Rahmen dieser Arbeit nur kurz auf konkrete technische Details eingegangen werden.

6.1. Header

Das Hauptaugenmerk bei der Neugestaltung des IP-Headers lag hierbei auf dessen Modularität. So ist jetzt ein gegenüber IPv4 kleinerer minimaler Header möglich. Erweiterungen lassen sich durch die Verkettung von Headern einfach einführen. Ein Router muss nicht alle diese Header bearbeiten; zusammen mit der Verkleinerung des minimalen Headers ergibt dies einen Geschwindigkeitsgewinn im aktiven Equipment des Backbone.

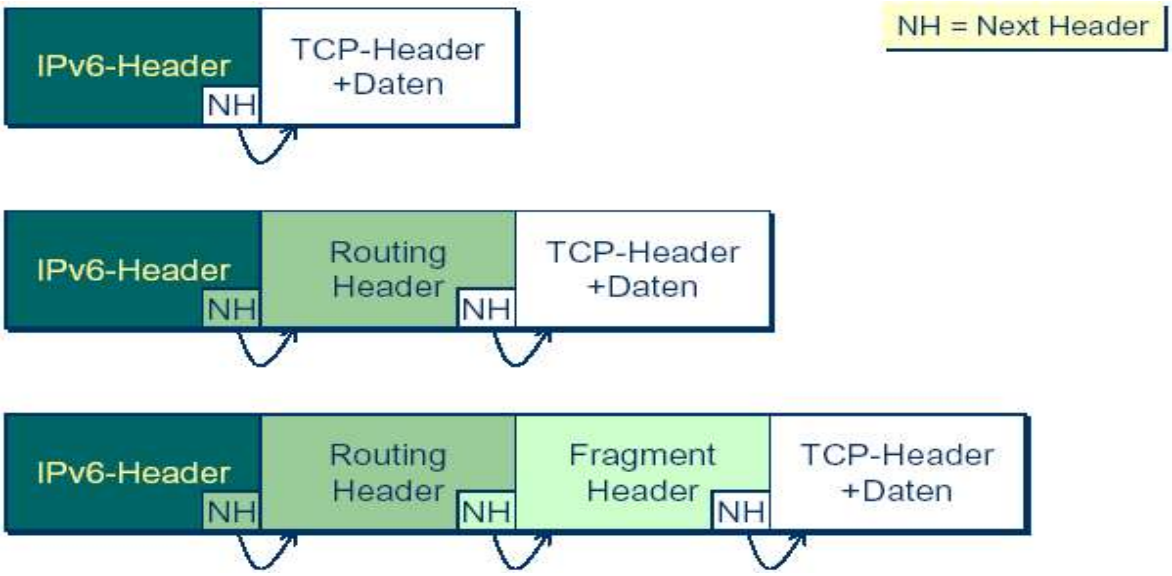

Abb. 1: Header-Verkettung

Mögliche Aufgaben der Zusatzheader sind Sicherheitsüberprüfungen, Segmentierung, Source Routing oder auch Netzmanagement.

6.2. Adressraum

Nach wie vor auch im minimalen Header verblieben sind natürlich die Adressinformationen. Statt wie bisher 32 Bit umfassen die Adressen bei *IPv6* jetzt 128 Bit, so dass theoretisch 3,4 * 10^{38} Adressen möglich sind. Der gesamte Adressraum wird allerdings – ähnlich wie bisher mit den verschiedenen Klassen und den eingeschobenen privaten Adressbereichen – auch bei *IPv6* wieder in mehrere Teile geteilt.

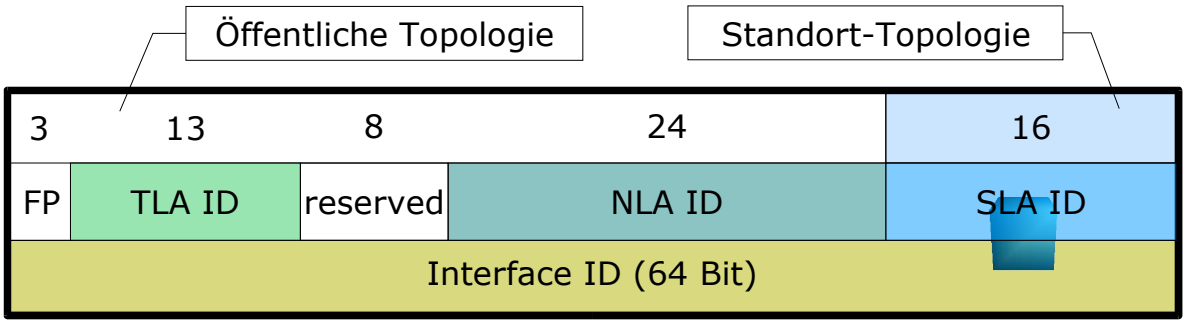

Abb. 2: Aufbau einer IPv6-Adresse

Dabei bedeuten:

- FP: Format Prefix (001 = global routingfähige Unicast-Adresse)
- TLA: Top-Level Aggregation
  grosse ISPs mit Transitnetzen, an denen andere ISPs angeschlossen sind
- NLA: Next-Level Aggregation
  Organisationen auf einer niedrigeren Stufe; es sind mehrere NLA-Ebenen möglich
- SLA: Site-Level Aggregation
  individuelle Adressierungshierarchie einzelner Organisationen

Diese Aufteilung in Topologien erleichtert u.a. das Routing im Backbone, da somit die Routingtabellen kleiner gehalten werden können.

In RFC 1715 findet man eine Abschätzung der nach dieser Aufteilung noch verbleibenden IP-Adressen. Dort gibt es eine optimistische Abschätzung, die von 700 * 10^{21} Adressen pro m² ausgeht. Und selbst die pessimistische Schätzung geht noch von 1.700 Adressen pro m² Erdoberfläche aus.

Ein derartig grosser Adressraum erfordert allerdings auch eine neue Notation der Adressen an sich. *IPv6*-Adressen sind mittels acht durch Doppelpunkte getrennte vierstellige Hexadezimalzahlen darstellbar. Da dies immer noch schwer „human readable" - also vom Menschen schnell les- und erfassbar – ist, kann man ganze Reihen von Nullen weglassen. Als Beispiel sei hier die „localhost"-Adresse – bei IPv4 „127.0.0.1" –

aufgeführt, die sich bei *IPv6* mit der Vereinfachung „::1" schreibt. Gleiches gilt auch für die unspezifierte Adresse („0.0.0.0" bei v4), welche bei *IPv6* schlicht und einfach „::" lautet und damit die kürzeste geschrieben *IPv6*-Adresse ist.

6.3.Multicast

Neu an *IPv6* ist hierbei, dass alle Router und Endsysteme von Haus aus Multicast unterstützen sollen. Es gibt vordefinierte Multicast-Gruppen für Kontrollfunktionen; das Internet Group Management Protocol (IGMP), welches bei IPv4 für die Verwaltung von Multicast-Gruppen benutzt wurde, ist in das Internet Control Message Protocol der Version 6 (ICMPv6) integriert.

Abb. 3: Aufbau einer IPv6-Multicast-Adresse

Eine solche *IPv6*-Multicastadresse enthält zusätzlich noch Flags (zur Zeit definiert ist eine Unterscheidung, ob die Multicast-Gruppe permanent oder nur temporär ist) sowie den Scope (also den Wirkungsgrad bzw. die Reichweite).

6.4.Automatische Konfiguration

"Plug & Play" ist in grossen Teilen der IT-Branche zu einem Schlagwort geworden. So hat man sich natürlich auch bei *IPv6* zum Ziel gesetzt, dieses Konzept mit einzubauen. So sieht *IPv6* Automatismen für folgende Parameter vor:

- Beschaffung der eigenen IP-Adresse
- Entdeckung doppelter IP-Adressen
- Auffinden von Routern
- Adressauflösung, Neighbour Discovery (vgl. Adress Resolution Protocol (ARP) bei IPv4)
- Bestimmung von ortsabhängigen Parametern (Subnetz-ID, Maximum-Transfer-Unit (MTU), DNS)-Server usw.)
- Unterstützung mobiler Endgeräte

und es gibt spezielle ICMP-Nachrichten für Router Solicitation / ~ Advertisement und Neighbour Solicitation / ~ Advertisement.

6.5. Unterstützung mobiler Knoten

Im Hinblick auf die wachsende Zahl mobiler Endgeräte (Laptops / Notebooks, PDAs / cellular phones bzw. deren zusammengefasste Nachfolger und vieler mehr) wurde bereits beim Design des Internetprotokolls der nächsten Generation natürlich auch diesem in den letzten Jahren besonders gewachsenen Markt Beachtung geschenkt.
Dabei ist nicht nur die bereits erwähnte Autokonfiguration (Beziehen einer gültigen IP-Adresse) involviert, sondern es wird direkt eine Infrastruktur für das Weiterleiten von IP-Adressen angestrebt (ähnlich IPIP-Tunneln im aktuellen Netz), so dass die eigene IP-Adresse beim Umzug in ein Fremdnetz weiterhin gültig bleibt.

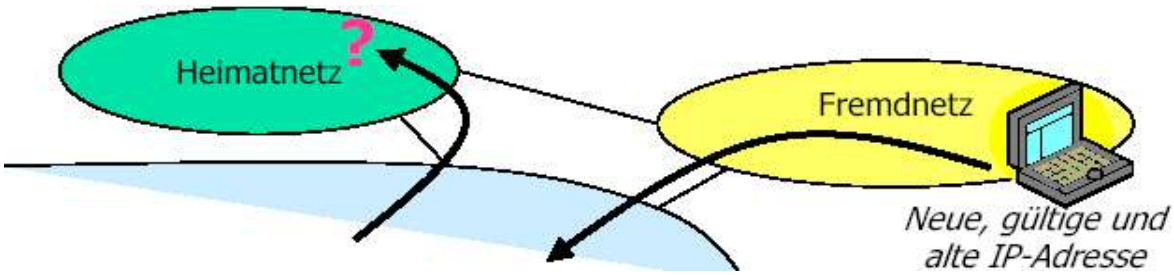

Abb. 4: mobiles IPv6-Endgerät

6.6 Sicherheit

In den letzten Jahren ist das Thema Sicherheit in der IT mehr und mehr in den Vordergrund gerückt, so dass Mechanismen wie IPsec natürlich auch bei *IPv6* zur Pflicht gehören. Sicherheit auch auf IP-Ebene, Verschlüsselung und Authentifizierung, werden bei *IPv6* durch Header-Erweiterungen realisiert. Bereits von IPsec her bekannt sind Authentication Header und Security Encapsulation Header. Für weitere Informationen sei hier z.B. auf die Veranstaltung auf "IT-Sicherheit und Datenschutz" verwiesen (http://www.zeropage.de/itsec).

6.7. Multimedia

IPv6 ist für Multimedia vorbereitet. Bereits heute wird bei IPv4 Multicast (vgl. Kapitel 6.3) genutzt, um identische Multimedia-Ströme (primär natürlich Audio und Video) nur ein Mal für jedes angeschlossene Subnetz übertragen zu müssen.

Aber mit Multicast an sich ist die Unterstützung von *IPv6* für Multimedia noch nicht beendet. So wurde u.a. ein sogenanntes "Flow Label" eingeführt. Pakete mit gleichem Ziel bekommen identisches Label und können so gleichbehandelt werden. War es bisher bei IPv4 noch

notwendig, dass die Router zum Erkennen des Paketflusses (Flow) die Absender-IP-Adresse, Empfänger-IP-Adresse, das IP-Protokoll und das Layer-4-Protokoll auswerten mussten, reicht bei *IPv6* das Flow Label dazu aus. Dies erinnert an den Ansatz des bereits erfolgreich im Einsatz befindlichen Multiprotocol Label Switching (MPLS). Auch wurden Prioritäten eingeführt, die eine Einstufung der Pakete nach Dringlichkeit ermöglichen. Zur Zeit gibt es nur eine grobe Unterscheidung in "Non realtime" und "Realtime". Jedoch muss auch dafür bereits eine Unterstützung durch die Router vorhanden sein; müssen diese Info doch auch ausgewertet und umgesetzt werden.

Ganz klar in diesen Kontext fällt auch Quality of Service (QoS), welches bei dem ein oder anderen sicherlich sofort Assoziationen zum Asynchron Transfer Mode (ATM) erweckt. Hinter QoS verbergen sich Dienstgütemerkmale wie garantierte "Bandbreite" (Kapazität) und Latenz, möglichst geringer Jitter (Änderungen der Latenz) und auch statistische Angaben über den Paketverlust (package loss).

Als Konzepte stehen hier die sogenannten "Integrated Services" (Int-Serv) und "Differentiated Services" (Diff-Serv) zur Verfügung.

Differentiated Services (RFC 2475) definieren Traffic-Klassen. Ein Router muss dazu keinen "State" führen; das Ganze läuft auf "Traffic Shaping" hinaus. "Traffic Shaping" an sich ist bereits bekannt; ein Umsetzen auf *IPv6* gut machbar.

Integrated Services (RFC 1633) dagegen garantieren Ende-zu-Ende QoS für einzelne Verbindungen. Dafür ist es notwendig, dass die beteiligten Router einen entsprechenden "State" führen. Zur Signalisierung wird hier das Ressource Reservation Protocol (RSVP, RFC 2205) eingesetzt. Es ist notwendig, eine passende Route zu finden, die Netzwerkdaten zu sammeln und dann die benötigten Ressourcen zu reservieren. Hierbei sind natürlich wieder alle Router auf dem Weg involviert und müssen dies unterstützen.

7. Migration von IPv4 zu *IPv6*

Wie bereits festgestellt wurde, ist das primäre Protokoll im Internet heutzutage IPv4. Nun stellt sich also die Frage: Wie migriert man Millionen von Systemen?

Eine schlagartige Umstellung ist nicht möglich. Um dennoch die Einführung von *IPv6* zu beschleunigen bzw. überhaupt erst zu ermöglichen, wurden Methoden für eine "sanfte" Migration, eine zeitweise Koexistenz geschaffen. Als Möglichkeiten existieren hier das Tunneling, der Dual Stack und die Protokolltranslation (z.B. Network Address Translation mit Protocol Translation (NAT-PT)).

Das Tunneling funktioniert ähnlich den bereits existierenden IPv4-Tunneln. Es werden einfach zwischen zwei Netzwerken, die mittels einer anderen Technologie als *IPv6* verbunden sind, die *IPv6*-Pakete ausgetauscht, in dem sie in das andere Paketformat eingepackt und am Zielsystem wieder ausgepackt werden. Dadurch gehen jedoch einige Eigenschaften von *IPv6* verloren, wenn die darunterliegende Infrastruktur diese nicht unterstützt – z.B. QoS.
Mit Dual Stack ist gemeint, dass ein System zwei Protokollstacks führt. Einen für das bisherige Protokoll – z.B. IPv4 – und parallel dazu einen TCP/IP-Stack für *IPv6*. Das System ist somit in der Lage, selbständig "alte" und "neue" Pakete sowohl zu empfangen als auch zu versenden.
Bei der Protkolltranslation schliesslich wird versucht, bestmöglich das *IPv6*-Protokoll in das bereits vorhandene zu übersetzen und umgedreht. Auch hierbei gehen Eigenschaften von *IPv6* verloren, da bei der Übersetzung nur solche berücksichtigt werden können, die dem kleinsten gemeinsamen Nenner entsprechen.

Es gilt also, sowohl für entsprechende Migrationsprojekte als auch neu anzulegende Netzwerke abzuwägen, ob der Einsatz von *IPv6* sinnvoll ist. Bei dem Aufbau eines neuen Netzwerkes gestaltet sich dies meist einfacher, als wenn man vor der Aufgabe der Migration steht – die meistens auch noch ohne Ausfall des laufenden Systems gefordert wird. Folgender loser Fragenkatalog kann einen ersten Anhaltspunkt für eine Abschätzung des Migrationsaufwandes liefern:

- Wie lange haben wir gebraucht, bis das heutige IPv4-Netz einigermassen problemlos in den Betriebsablauf integriert war?
- Wie lange haben die Netzwerker Zeit gehabt, alle neuen Funktionen kennenzulernen?
- Gab es bei der Realisierung des ersten TCP/IP-Netzes nicht eine Reihe von unvorhergesehenen Problemen?
- Welche Fehler haben wir im Laufe der Jahre gemacht?
- Was hat die Mannschaft bzw. was haben die einzelnen Netzspezialisten bis heute alles gelernt?
- Wie viele Nächte des Debuggens waren dazu notwendig?

- Steht ein Budget für eine Migration zur Verfügung?
- Welche realen Kosten entstehen bei der endgültigen Migration?
- Welche der bestehenden Netzkomponenten müssen migriert werden?
- Welche der bestehenden Netzkomponenten müssen nicht migriert werden?
- Welche der bestehenden Netzkomponenten können nicht migriert und müssen ggf. ausgetauscht werden? (Komponente zu alt, zu wenig Memory bzw. CPU-Leistung, Hersteller nicht mehr im Markt etc.)?
- Welche neuen Hardware- und Software-Komponenten müssen beschafft werden?
- Soll ein gemischter Betrieb von IPv4 und *IPv6* realisiert werden?
- Welche personellen Ressourcen werden für die Migration benötigt?
- Bis wann soll die Testphase bzw. die Migrationsphase abgeschlossen sein?
- Wie kann die spätere Migration bzw. der spätere Betrieb von IPv4 bzw. *IPv6* realisiert werden?
- Wie sehen die neuen Adresskonzepte im Netz aus?
- Kann bis zum Zeitpunkt X eine offizielle IP-Netzadresse besorgt werden?
- Wie können alle Mitarbeiter der IT-Truppe auf das neue Protokoll umgeschult werden?
- Welche zusätzlichen Funktionen (z.B. QoS) sollen gleichzeitig mit eingeführt werden?
- Welcher Zeitraum muss für eine Umstellung bzw. Migration geplant werden?
- Wie kann das neue Protokollkonzept (Adressen, Funktionen, Konfigurationen) dokumentiert werden?

Es stellt sich die Frage, ob man zuerst die alte Funktionalität wieder herstellen und dann neue Features hinzufügen sollte. Prinzipiell scheint das der Übersichtlichkeit zuträglich zu sein, birgt aber den Nachteil, dass eine zu grosse Mehrarbeit notwendig ist, wenn die Änderungen dann an grundlegenden Sachen stattfinden (einfachstes Beispiel: IP-Adressen und deren hierarchische Struktur bei v4 vs v6). Ergo sollte man von Grund auf ein v6-Netzwerk planen.
Je nach Grösse und Komplexität der eigenen Installation sollte man die eigenen Zuliefererfirmen (z.B. Hersteller von Backbonekomponenten) nach Referenzinstallationen fragen und ggf. mit diesen Kunden oder anderen Kooperationspartnern (z.B. verwandten Rechenzentren) Kontakt aufnehmen. Auch kann die Installation eines Testnetz durchaus sinnvoll sein.

Man sollte auch Ressourcen für das Management der Konfigurationen auftretender Fehler, der Performance und nicht zuletzt der Sicherheit sowie einer Dokumentation mit einplanen.

8. Resümee

Wo gibt es denn nun *IPv6*?
Komplexe Infrastrukturen scheinen bisher nur lokal vorhanden zu sein; z.B. als Einsatz in Forschungsnetzen. Verbunden werden diese ganzen kleinen Intranets in guter Tradition durch das Internet, z.B. den "6bone" als *IPv6*-Backbone. Dabei läuft der grösste Teil der Verbindungen der *IPv6*-Hauptknoten über konfigurierte IPv4-Tunnel (vgl. Kapitel 7).

Projekte, die sich mit *IPv6* beschäftigen, gibt es erfreulicherweise viele. Neben den reinen Foren und Gremien sei hier stellvertretend das "Internet2" als praktische Instanz genannt – ein Zusammenschluss von Universitäten, die mit Industrie und Regierung zusammenarbeiten. Dort existieren verschiedene Arbeitsgruppen (Working Groups); unter anderem zu den Themen Engineering (*IPv6*, Multicast, QoS, Routing, Sicherheit, ...), Middleware (Public Key Infrastructure (PKI), ...) also auch Anwendungen (auch Voice-over-IP (VoIP)).

Wenn man selber an *IPv6* teilnehmen möchte, stellt sich natürlich auch die Frage, wo man denn die Adressen herbekommt. Zur Zeit werden hauptsächlich Adressen nach RFC 2471 vergeben; einem Verfahren, bei dem Adressen kostenlos an jeden vergeben werden, der welche haben möchte. Bei diesen Adressen handelt es sich jedoch – wie im gesamten 6bone – nur um eine testweise Vergabe, d.h. wer sich jetzt Adressen reserviert, wird diese vermutlich später noch einmal umstellen müssen. Freie Adressbereiche und ganze /48'er Subnetze inkl. der notwendigen Tunnelsoftware kann man z.B. über freenet6 beziehen.

Daraus wird aber bereits ersichtlich, dass man einige der Features, die *IPv6* unterstützt, vorerst maximal lokal ausprobieren kann (z.B. QoS), da zuerst einmal global die passenden Infrastrukturen gebildet werden müssen. Ethernet z.B. ist kein echtzeitfähiges Medium, auch hier muss also eine schrittweise Migration erfolgen.
Vorreiter dafür könnten durchaus wieder die Universitäten sein; teilweise existieren hier ja bereits entsprechende Projekte; so z.B. an der TU Ilmenau der Tunnel in der Praktischen Informatik und das Projekt der FeM.
Das universitätsnahe Betriebssystem Unix liefert hier mit seinem freien Derivat Linux eine gute Basis; ist doch die *IPv6*-Implementierung für Linux nicht nur eine der am weitesten fortgeschrittenen und die Anzahl der vorhandenen Tools bereits sehr beachtlich, sondern erhält hier der Student gleichzeitig auch die Möglichkeit, am Quellcode der Implementationen selbst den Aufbau und die Funktionsweise nachvollziehen zu können.
Vertiefen liesse sich dieses, in dem man für die Studenten entsprechende Praktika anbietet, in denen ihnen der Umgang mit *IPv6* sowie das Protokoll selber näher gebracht wird. Dies ist insbesondere deswegen nötig, damit die zukünftigen Forschungs- und Lehrkräfte

abschätzen können, in wie weit es Sinn macht, in ihrer zukünftigen Tätigkeit noch Energien in IPv4 und andere bisherige Protokolle zu stecken bzw. ihrerseits den nachfolgenden Studentengenerationen auch *IPv6* propagieren.

Ausserdem sollen sich ja auch die Studenten mit den teilweise noch existierenden Problemen und Fragen zu *IPv6* auseinandersetzen. Damit ist nicht nur die generelle Suche nach Alternativen und die kritische Bewertung von IP an sich gemeint. So gibt es z.B. negative Stimmen bzgl. des Themas QoS; besteht doch die Gefahr, dass Bandbreite irgendwann käuflich und die bisherige "best-effort"-Auslieferung durch eine kapitalgesteuerte Verfügbarkeit des IT-Backbones verdrängt wird ("Microsoft kauft die ganze Bandbreite"). Ausserdem muss hier reguliert werden, dass auch andere Einflussgruppen (z.B. Terroristen oder die verrufenen "Scriptkiddies") nicht in der Lage sind, einzig zum Zwecke einer Denial-of-Service (DoS)-Attacke Bandbreite zu allokieren.

Weiterhin noch nicht ganz ausgeräumt ist der Kritikpunkt, ob ein "Scope = Internet" illusorisch sei – insbesondere beim Thema Multicast. Diese Frage ist durch den einfachen Aufbau kleiner Testnetze jedoch auch nicht so einfach beantwortbar sondern muss eher durch geschickte Planung und Protokolldesign verwirklicht werden; und zwar so, das es auch noch mit realem Equipment beherrschbar bleibt.

Offen bleibt vorerst, ob *IPv6* mächtig genug ist, um auch im Bereich des Internet-Backbone das Protokoll an sich zu werden, oder ob es weiterhin Netzwerke geben wird (z.B. ATM), die besser geeignet sind, diesen Kernbereich zu handhaben und ihrerseits nur *IPv6* als eines von mehreren Protokollen transportieren. Dann könnte es gleichsam auch passieren, dass IPv4 gar nicht wie vorgesehen abgelöst wird, sondern die bereits existierenden Erweiterungen dieses Protokolls bereits ausreichend sind und IPv4 weiter mit den vielen anderen Protokollen koexistieren wird. In diesem Fall bleibt nur zu hoffen, dass die immer weiter gehende Entwicklung der IT-Branche nicht irgenwann vor einem zweiten "Y2k"-Problem steht – denn schon die reine Adressproblematik bei IP lässt da doch gewisse Gemeinsamkeiten erkennen.

Es ist also noch einiges zu tun, bis *IPv6* zu dem wird, was das Internet in weiten Teilen schon ist – allgegenwärtig. Die Schaffung geeigneter Infrastrukturen ist dabei zur Zeit noch genau so wichtig wie die Schaffung eines entsprechenden Bewusstseins (awareness), damit neue Projekte gleich von den Vorteilen von *IPv6* profitieren können und auch notwendige Forschungen und Analysen über die Zweckmässigkeit des Einsatzes und/oder der Umstellung betrieben werden.

Anhang - Quellen und Referenzen:

- Requests for Comments (RFC)
- Usenet
- Mailinglisten
- WorldWideWeb (www)
- Bücher
- Vorlesung im Fachgebiet Telematik an der TUI
- VL im Fachgebiet Nachrichtentechnik an der TUI
- Publikationen von Felix von Leitner
- Publikationen von Lutz Donnerhacke

Bücher:

Alle hier aufgeführten Bücher sind über die Universitätsbibliothek der TU Ilmenau erhältlich.

- "Technik der IP-Netze"
  Hanser 2001, ISBN 3-446-21501-8
- Hein, Mathias: "TCP/IP"
  mitp 2002, Mathias Hein, ISBN 3-8266-4094-2
- Dr. Weiss, Manfred: "TCP/IP-Handbuch"
  Franzis' 2002, ISBN 3-7723-5026-7
- Rao/Sletta: "Next Generation Networks"
  Springer 2000, ISBN 3-540-41140-2
- Wegener/Rockell: "IP Addressing & Subnetting"
  mitp 2000, ISBN 3-8266-4077-2
- Wiese, Herbert: "Das neue Internetprotokoll IPv6"
  Hanser 2002, ISBN 3-446-21685-5

RFCs:

RFCs bilden eine der wichtigsten Arbeitsgrundlagen, wenn man sich mit dem Design oder dem Einsatz von IT und deren Protokollen beschäftigt.

0791: IP

1550: IP: Next Generation (IPng) White Paper Solicitation

1597: (superseeded by 1918)

1627: Beschwerde (vgl. mitp klein S. 102)

1752: IPng requirements

1883ff: Spec fuer IPv6 (superseeded bei 2460ff)

1917: Februar 1996: "Appell an die Internet-Gemeinschaft zur Rückgabe nicht genutzter IP-Netzwerke an die IANA"

1918: Private Netzwerkadressen

1933: The transition mechanism (vgl. RFC 2893)

2185: Aspects of IPv6 Transition

2205: Resource ReSerVation Protocol (RSVP)

2460ff: IPv6-Diskussionen & Spec; 1998 zum Draft Standard erhoben

2893: Transition Mechanisms for IPv6 Hosts and Routers

3041: IPv6 privacy extensions

Usenet:

In den hier genannten Diskussionsforen wird über *IPv6* diskutiert, Neuerungen bekanntgegeben oder Details bestimmter *IPv6*-Implementierungen besprochen.

alt.internet

comp.doc.*

comp.networks

comp.os.linux.networking

comp.unix.*

de.org.ccc

de.comm.internet.*

de.comm.protocols.tcp-ip

fa.openbsd.ipv6

info.big-internet

info.ietf

linux.debian.maint.ipv6

linux.kernel

microsoft.public.platformsdk.networking.ipv6

URLs:

http://www.ipv6.org

http://playground.sun.com/pub/ipng/html/ipng-main.html

Internationales Forum führender Hersteller und Entwickler:
http://www.ipv6forum.com

Lancaster University Computing Department IPv6 Ressource Centre:
http://www.cs-ipv6.lancs.ac.uk/ipv6

REN: IPv6 Research and Education Networks:
http://www.6ren.net

Das JOIN-Projekt des DFN:
http://www.join.uni-muenster.de

Das von JOIN betriebene deutschlandweite IPv6-only Backbone:
http://www.6win.de

freenet6 – freie /48'er Subnetze nebst Tunnelsoftware:
http://www.freenet6.net

6bone – ein IPv6-Testbed-Backbone:
http://www.6bone.net

Internet Engineering Task Force (IETF):
http://www.ietf.org

Internet Assigned Numbers Authority (IANA):
http://www.iana.org

Linux+IPv6-HOWTO:
http://www.bieringer.de/linux/IPv6

Microsoft Research 'IPv6':
http://research.microsoft.com/msripv6

Homepage von Felix von Leitner:
http://www.fefe.de

Homepage von Lutz Donnerhacke:
http://www.iks-jena.de/mitarb/lutz