Frank-Michael Krupp krupp@epost.de www.vuni.de

IPv6 – Das neue Internet-Protokoll

Gründe für IPv6

Das aktuelle Internet-Protokoll Version 4 (IPv4) kann den neuen Anforderungen von Multimedia und den ständig steigenden, exponenziell wachsenden Teilnehmerzahlen (zurzeit schätzungsweise 60 Millionen Menschen) im Internet auf Dauer nicht gerecht werden. Abhilfe verspricht das "Internet Protocol next generation" (IPv6 oder IPng), mit dessen Einführung zugleich zahlreiche Neuerungen einhergehen.

Bei IPv4, das Ende der Siebzigerjahre entwickelt wurde, ist die Länge der Adressen auf 32 Bit festgelegt. Dies war ausreichend, um ein paar Tausend Rechner des amerikanischen Verteidigungsministeriums und später ein paar Millionen Rechner von wissenschaftlichen Einrichtungen miteinander zu verbinden. Seit aber zunehmend Privatleute hauptsächlich mit den Diensten E-Mail und World Wide Web das Internet in Anspruch nehmen und kommerzielle Unternehmen große Gewinne wittern, wird der Adressraum eng. Dazu kommt die Umstellung vieler Unternehmensnetze auf die TCP/IP-Technik („Intranet``) und deren teilweiser Verbindung mit dem globalen Internet. Auch neue Anwendungsgebiete wie mobile Komponenten vergrößern den Adressbedarf.

Erweiterte Adressierungsmöglichkeiten

Der Hauptgrund für die Umstellung ist also der zu Neige gehende Vorrat an IP- Adressen. Diese stellen die Anwahlnummern der Server dar, so entspricht www.mathematik.uni-karlsruhe.de der IP- Adresse 129.13.115.114. Derzeit kennt man demnach die Adressen als vier, durch einen Punkt getrennte Zahlen zwischen 0 und 255. Rechnerisch sind 2^{32}, also 4.294.967.296 Adressen verfügbar. Das sieht zwar auf den ersten Blick recht gewaltig aus, aber es kann in Wirklichkeit nur ein kleiner Teil davon verwendet werden. Anfangs teilte man die Adressen in Klassen A, B und C ein. Ein Klasse A- Netz umfasst etwa 16 Millionen Rechner (z.B. 172.xxx.xxx.xxx), weil kaum ein Unternehmen so viele Adressen braucht, wurde das C- Netz (z.B. 172.20.249.xxx) eingeführt, die möglichen 255 Adressen sind wiederum vielen Firmen nicht ausreichend, und so erfreuen sich die B- Netze (z.B. 172.20.xxx.xxx) mit 65000 Rechnern besonderer Beliebtheit. An den großen Sprüngen erkennt man, dass das Ganze alles andere als ideal ist und wertvoller Adressraum ungenutzt bleibt.

In den letzten Jahren haben sich brauchbare Konzepte entwickelt, die höhere Effizienz versprechen. Zu nennen ist hier zum einen die dynamische Vergabe von IP- Adressen, wie das beispielsweise bei Internetprovidern geschieht. Zum anderen sind „Network Address Translator“ (NAT) bei Firmen sehr beliebt. Hierbei wird ein Gateway (u.U. mit Firewall-Abschottung) verwendet, um ein komplettes privates Netz nach außen hin hinter einigen

wenigen offiziellen Adressen zu verbergen, wobei der NAT- Rechner schnell zum bremsenden Flaschenhals wird und die Verwaltbarkeit nicht besonders einfach verläuft. Doch für NAT & Co. ist es im Grunde zu spät. Sie können den Kollaps nur hinauszögern, verhindern können sie ihn nicht.

1992 wurde von der Internet Engineering Task Force (IETF) eine Arbeitsgruppe gebildet. Es entstand das "Internet Protocol next generation", das das derzeitige Protokoll IPv4 ablösen soll. Der neue 128 Bit umfassende Adressraum sollte mit $3*10^{38}$ möglichen Adressen auch bei sehr ineffizienter Vergabe auf weite Sicht ausreichen. Die neuen Adressen werden zur besseren Lesbarkeit in 8 Gruppen von je 16 Bit zusammengestellt, durch Doppelpunkte getrennt, z.B. FA30:2165:0000:0000:000D:37A1:E2BC:90E1. Es ist erlaubt, innerhalb der Gruppen auf führende Nullen zu verzichten. Außerdem kann man einmal (nicht zweimal, da dann nicht mehr eindeutig) innerhalb der Adresse mehrere aufeinander folgende Gruppen von Nullen durch zwei Doppelpunkte ersetzen. Damit kann obige Adresse dargestellt werden als FA30:2165:0:0:D:37A1:E2BC:90E1 oder noch kürzer FA30:2165::D:37A1:E2BC:90E1.

Da die Provider immer stärker die Struktur des Internet prägen, stellt man Provider - basierte Unicast - Adressen bereit, die streng hierarchisch vergeben werden. Jeder dieser Adressen beginnt mit einer besonderen 3 Bit umfassenden Kennung, gefolgt von der Kennnummer für die Top-Level-Aggregation (Superprovider oder zentrale Austauschpunkte). Die Next-Level-Aggregation kann ein Provider sein, die folgende Site-Level-Aggregation eine Firma, die dann mit den restlichen 64bit die angeschlossenen Endsysteme identifiziert.

3 bit	13 bit	32 bit	16 bit	64 bit
001	TLA	NLA	SLA	Zwischen-/Endsystem - ID

In den ersten Implementierungen tauchte der Entwurf einer Unicast- Adresse mit flexiblen Felder auf, erste Erfahrungen mit dem 6bone - Testnetz zeigten, dass dies jedoch auf Dauer zu einem zu starken Anwachsen der Routing - Tabellen führen würde.

Es sind ferner lokale Adressen vorgesehen, die nur innerhalb eines Unternehmens Gültigkeit besitzen. So kann ein Betrieb, der noch keinen Internet-Anschluss realisieren möchte, bereits ein Netz mit Internet-Adressen konfigurieren und später bei Bedarf die firmeninternen Adressen in weltweit gültige umwandeln.

10 bit	N bit	118-N bit
1111111010	000000000000000...	Interface-ID

Neue Anwendungsfelder erschließen Multicast- und Anycast- Adressen. Multicast bezeichnet nicht nur einen einzigen Rechner, sondern mehrere Internet-Teilnehmer, die sich zu einer permanenten oder transienten Gruppe zusammengeschlossen haben, etwa für Videokonferenzen.

8 bit	4 bit	4 bit	112 bit
11111111	000T Schalter (flags)	Reichweite (scope)	Gruppen-ID

Die Anycast- Adressen stellen einen Kompromiss zwischen den Unicast- und Multicast- Adressen dar. Mit einer Anycast- Adresse lässt sich ebenfalls eine Gruppe von Computern ansprechen. Daten, die man an eine Anycast-Adresse schickt, erreichen im Normalfall aber nur einen Rechner dieser Gruppe, und zwar den, der zuerst antwortet. Das auf den ersten Blick exotisch anmutende Verfahren erhält in der Praxis durchaus Sinn: Fasst beispielsweise ein Provider alle Rechner wie Name- und Zeitserver oder Router in einer Gruppe zusammen, können Kunden sie mit einer einheitlichen Adresse erreichen. Kommt ein neuer Server hinzu, bedarf es keiner neuen Konfiguration seitens der Anwender. Eine weitere Anwendung ist das Weiterleiten von Datenpakete über ein bestimmtes Teilnetz eines Netzanbieters, wobei die Adressen im Anycast- Format in die Routing - Anweisungen eingetragen werden. Das Anycast- Verfahren gibt es nicht bei IPv4, somit werden weitere Anwendungen erst von einer Arbeitsgruppe der IETF erforscht.

Datenformat

Der Datenkopf wurde mit den Erfahrungen, die mit IPv4 gesammelt wurden, optimiert. Es wurde dabei vor allem auf eine einfache und schnelle Verarbeitung für die Router geachtet. Wie man an der Gegenüberstellung der beiden Header sehen kann, wurde der Aufbau vereinfacht, Felder entfernt und, wenn man einmal von den beiden 128 Bit Adressen absieht, die Größe verringert, die nun konstant 40 Byte beträgt.

Version	Header-Länge	Precedence	Diensttyp	Gesamtlänge	
Identifikation				Schalter	Fragment offset
Time to live		Protokoll		Header Prüfsumme	
Absenderadresse					
Zieladresse					

IPv4-Kopf

0	4	8	16	24	
Version	Priorität	Flussmarken (flow lable)			10 * 32 bits 40 byte
Daten-Länge			Next header	Hoplimit	
Absenderadresse					
Zieladresse					

IPv6-Kopf

Ein entferntes Feld beinhaltet eine Prüfsumme, die bei IPv6 nicht mehr zu finden ist. Begründet wird das damit, dass die umgebenden Protokollschichten größtenteils mit Prüfsummen ausgestattet sind und somit eine weitere Prüfung nicht notwendig ist. Aber vor allem ist der damit zu erwartende Geschwindigkeitsgewinn ausschlaggebend (in der Praxis nehmen sich Router schon seit längerem nicht mehr die Zeit, die Prüfsumme zu überprüfen).

Es gibt hier viele kleine Detailänderungen, wovon noch eine genannt werden soll: Das Time-to-Live-Feld wurde in Hop-Limit umbenannt. Mit Time-to-Live sollte die „Lebenszeit" eines IPv4-Pakets beschrieben werden, jeder Router sollte anhand der Warte- und Verarbeitungszeit für dieses Paket diesen Wert entsprechend zurücksetzen. In der Praxis ist eine Zeitschätzung nicht durchführbar und auch nicht notwendig, da die Transportprotokolle (z.B. TCP) mit Zeitstempel selbst in der Lage sind, alte Pakete zu erkennen. IPv6 erlaubt nun maximal 255 Sprünge (hops), danach wird das Paket, um ein unendliches Umherirren von fehlgeleiteten Daten zu verhindern, einfach gelöscht und eine ICMP (Internet Control Message Protocol) an den Sender gegeben.

Header-Erweiterungen

Ein völlig neuer Weg wurde auf dem Gebiet der Optionen beschritten. Optionen, die beim IPv4-Kopf noch im Hauptkopf vorhanden waren, wurden auf Erweiterungs- Header verlagert. Dies geschah aus der Erfahrung, dass der bisherige Datenverkehr weitgehend ohne Optionen ablief, woraufhin die Router vor allem auf diese Standardpakete optimiert wurden. Datenpakete mit Optionen waren massiv benachteiligt, sodass die Verwendung von Optionen immer restriktiver gehandhabt wurde. Es drohte der Verlust dieser Optionenvergabe. IPv6 behebt dieses Problem mit einer Kopf- Erweiterungskette. Das Ganze ist flexibler, entlastet Router und vereinfacht Neueinführungen. Das next-header-Feld gibt immer den Typ der folgenden Kopf- Erweiterung an.

Next header= hop-by-hop Optionen	Next header= Zieloptione n	Next header= Routing Optionen	Next header= fragment optionen	Next header= Authentifizierung s-optionen	Next header= Verschlüsselungsoptio nen	Next header= Zieloptionen	Next heade r= TCP	
IPv6 Header	Hop-by-hop Header	Ziel- Header	Routing Header	Fragment Header	Authentifizierungs-Header	Verschlüsse-lungs-Header	Ziel-Heade r	TCP-Heade r + Daten

Der Routing- Header wird nur bearbeitet, wenn die Zieladresse im Basiskopf erreicht ist, dann wird die neue anzusteuernde Adresse aus dem Feld Adresse(1) genommen, in den Haupt- Kopf eingetragen und die Liste entsprechend aktualisiert. Dieses Verfahren ermöglicht es für den Absender, den Weg seiner Nachricht beim Transport zu bestimmen.

0	8	16	24
Next header	Header-Länge	Routing Typ	Segments left
(reserviert)			
Adresse(1)			
Adresse(2)			
...			
Adresse(n)			

Der Fragment- Header ermöglicht größere Pakete zu senden, als es der Netzwerktyp, der eine spezifische MTU (Maximum Transmission Unit) hat, erlaubt. Das Paket wird in mehrere Teilpakete zerlegt. Das ist noch nichts Neues, auch IPv4 war natürlich in der Lage, große Pakete zu verschicken. Der Unterschied ist der Ort der Segmentierung und Reassemblierung. Bei IPv4 wurden die großen Pakete an die Router gegeben, die dann selbst schauen sollten, wie sie die Pakete aufteilen, mit Erkennungsnummern versehen und alles wieder zusammenbauen können. In Zeiten der Router-Überlastung ist eine Verlagerung dieser Verfahren auf Quelle und Ziel angebracht. Der IPv6-Knoten schickt ein Paket mit zulässiger Größe an den ersten Router. Im unten angegebenen Beispiel gibt es mit diesem Paket keine Probleme, es wird weitergeleitet. Tritt dann ein Übergang in ein anderes Netz ein, für das dieses Paket nicht geeignet ist, wird es gelöscht und der Sender erhält die zulässige MTU-Größe mitgeteilt. Er teilt die Nachricht entsprechend auf und versucht sein Glück von Neuem. Das Verfahren mag auf den ersten Blick etwas umständlich erscheinen. In der Praxis hat sich nichtsdestoweniger gezeigt, dass wegen einer garantierten Mindest- MTU für IPv6-Verbindungen, dieses Verfahren schnell konvergiert und sich der positiven Seiteneffekt einstellen könnte, dass bei einem verlorenem Teilstück nur dieses und nicht das ganze Paket nachgeliefert werden muss; inwiefern dies implementierbar ist, wird sich noch zeigen.

	MTU=4352 byte	MTU=4352 byte	MTU=1500 byte	
4352	→	→	⇓	
	←	←	ICMP: message too big (MTU=1500)	
1500	→	→	→	
Endsystem	FDDI	FDDI	Ethernet	Endsystem

Die Jumbo-Payload-Option, die in dem Hop-by-Hop-Erweiterungs-Header zu finden ist, erlaubt es, Pakete von bis zu 2 Gbyte zu senden. Dies wurde von Betreiber der Supercomputer gefordert. Normalerweise ist nämlich die Größe einer Nachricht auf 64kByte beschränkt. Damit will man eine Blockierung der Router durch zu lange Pakete verhindern. Wenn man nun 128kByte senden will, ist der zusätzliche 40byte-Header für ein weiteres Paket sekundär.

Die Ziel-Optionen ermöglichen, wie der Name schon sagt, Optionen für das Zielsystem. Sie werden erst dort betrachtet. Bisher gibt es noch fast keine Anwendungen hierfür.

Sicherheitsaspekte

Zwei Mechanismen von IPv6 sollen die Lücke im Sicherheitsbereich schließen. Zum einen steht eine Authentifizierungsoption zur Verfügung, die eine digitale Unterschrift (aus der Nachricht wird eine Prüfsumme berechnet, die dann mit dem geheimen Schlüssel des Verfassers verschlüsselt wird, der dazu passende öffentliche Schlüssel kann die Prüfsumme entschlüsseln und erkennt somit sowohl Veränderungen als auch vorgetäuschte Identitäten) für die übermittelten Nachrichten enthält.
Zum anderen sollen manche Nachrichten nicht im Klartext übertragen werden. Die Verschlüsselung auf IP-Ebene verwendet den Tunnelmodus, bei dem das gesamte verschlüsselte Datenpaket in ein neues Datenpaket eingekapselt wird. Beide Verfahren gab es zweifelsohne auch bei IPv4, sollen aber durch die bessere Integration eine breitere Verwendung finden.

Prioritäten

IPv6 führt eine Sonderbehandlung für Multimediadaten durch, um die nötige Übertragungsqualität zu erreichen. Die Prioritäten sind dabei relativ nur in ihrer Verkehrsart, d.h. 8 hat keine höhere Wichtigkeit als 7.

Wert	Verkehrsart	Wert	Verkehrsart
0	Nicht näher charakterisierter Verkehr	8	z.B. hochwertige Videos (Verlust einiger Pakete nicht zu erkennen)
1	Füllverkehr(z.B. News)	9	
2	Datenverkehr ohne spezielle Behandlung (läuft im Hintergrund, z.B. E-Mail)	10	
3	Reserviert	11	
4	Datenverkehr mit spezieller Behandlung (z.B. Ftp)	12	
5	Reserviert	13	
6	Interaktiver Verkehr (benutzerfreundlich, schnelle Antwortzeiten erforderlich, z.B. Telnet)	14	
7	Kontrollverkehr (z.B. Routing-Protokolle, ICMP)	15	z.B. Ton/Telefon (Verlust von wenigen Paketen störende)
Prioritäten für Verkehrsarten mit Staukontrolle Eine Verzögerung ist akzeptabel, auch die Ankunft der einzelnen Pakete in unterschiedliche Reihenfolge		Prioritäten für Verkehrsarten ohne Staukontrolle Echtzeit Video/Audio Verlorene Pakete müssen nicht nochmals geschickt werden	

Automatische Systemkonfiguration

Das Neighbor Discovery Protokoll ist eine Sammlung von verschiedenen Protokollmechanismen. Neue Knoten sollen durch Kontrollnachrichtenaustausch zwischen IP-Instanzen einfacher in IPv6-Netze eingefügt werden können. Statt aufwändiger Eintragen der Parameter von

Hand soll dies automatisch durch Anforderung der linkspezifischen Parameter (IP- und Link-Adresse, Präfix-, Link- und Internet-spezifische Informationen) von der Umgebung eingerichtet werden.

Migration

Die Entwurfs- und Testphase ist schon einige Zeit abgeschlossen. Einer massenweisen Einführung steht nichts mehr im Weg. Eine Umstellung auf IPv6 kann dabei schrittweise erfolgen. Zuerst werden die Rechner der Provider mit dem neuen Protokoll ausgestattet. Je nach Zugriff können beide Protokolle nebeneinander existieren. So lassen sich die großen Netze schrittweise umrüsten. Dieses Nebeneinander macht gleichwohl schwierige Übersetzungsmechanismen notwendig. Name-Server müssen beide Adress-Typen beherrschen. Vor allem die Änderungen an vielen Anwendungen sind ein Hindernis für IPv6. Und solange der Adressraum noch ausreicht (Schätzungen nennen das Jahr 2002) wird keine Notwendigkeit herrschen für das neue Internet-Protokoll IPv6.

Quellen und weiterführende Literatur

Braun, T.: „Die Internet-Protokollfamilie der nächsten Generation“, Praxis der Informationsverarbeitung und Kommunikation (PIK), 2/96
Stallings, W.: „Ipv6: The New Internet Protocol“, IEEE Communications Magazine, Vol. 34, No. 7
Huitema, C.: „Ipv6- The new Internet Protocol“, 2nd Edition, Prentice Hall, 1997
Dittler, H.: „Ipv6 Das neue Internet-Protokoll“, 1.Auflage, dpunkt-Verlag, 1998
Feit, S.: „TCP/IP“, McGraw-Hill, 1998
RFC der IETF: ftp://ftp. ietf.org/internet-drafts/
www.ipv6.org