Kommunikation ohne Tricks

IPv6 – das Internet-Protokoll der nächsten Generation (Teil 1)

Torsten Braun

Aufgrund der steigenden Popularität des Internet und seiner angebotenen Dienste wächst die Zahl der Internet-Knoten seit Jahren stark an. Die Zahl der Benutzer verdoppelt sich zur Zeit ca. alle eineinhalb Jahre. Speziell im privaten Bereich wird erwartet, daß neuartige Endgeräte mit Internet-Adresse in Autos und im Haushalt zunehmend Verbreitung finden. Experten gehen davon aus, daß im Jahre 2020 rund 10 Milliarden Menschen jeweils ca. 100 IP-Adressen benötigen, so daß dann der derzeit verfügbare IPv4-Adreßraum nicht mehr ausreichen würde. Eine Lösung des Problems besteht darin, einen größeren Adreßraum mit mehreren Adressierungshierarchien zu schaffen, was die Entwicklung eines neuen IP-Protokolls bedeutet.

Prof. Dr. Torsten Braun ist Leiter der Forschungsgruppe Rechnernetze und Verteilte Systeme am Institut für Informatik und Angewandte Mathematik der Universität Bern

Anfang des Jahres 1992 entschied die IETF (Internet Engineering Task Force), eine neue Version des Internet-Protokolls (IP) zu entwickeln, was zu einem kompletten Neuentwurf des Protokolls genutzt wurde.

Die Standardisierung des IPv6-Protokolls ist inzwischen sehr weit fortgeschritten, die wichtigsten Dokumente wurden als RFC (Request For Comment) veröffentlicht. Schon seit mehreren Jahren gibt es IPv6-Implementierungen als Produkte in verschiedenen Routern und Endsystemen. Allerdings ist entgegen den Erwartungen der IETF die Verbreitung und Benutzung des Protokolls nicht so stark wie erhofft. Dies liegt im wesentlichen daran, daß der Bedarf an global eindeutigen IP-Adressen trotz des Internet-Booms der letzten Jahre nicht so schnell zunimmt wie ursprünglich erwartet. Durch den verstärkten Einsatz von NATs (Network Address Translator) wächst die Zahl der benutzten IP-Adressen um lediglich 6 % über eineinhalb Jahre hinweg an. Der Grund: Die meisten Firmen, die sich in der jüngeren Vergangenheit ans Internet angeschlossen haben, setzen Firewalls oder NAT-Systeme ein. Beide Konzepte benötigen nur eine oder wenige global eindeutige IP-Adressen. Die hinter Firewall oder NAT liegenden Endsysteme im Firmennetz benutzen nach außen hin nicht sichtbare private IP-Adressen.

Diese Entwicklung reduzierte das allgemeine Interesse an IPv6, weil der wichtigste Grund für dessen Einführung – die ausgehenden IP-Adressen – nicht mehr so dringend erscheint.

Allerdings besitzt IPv6 über den vergrößerten Adreßbereich hinaus weitere verbesserte Eigenschaften und Funktionen. Diese waren zunächst nur für das IPv6-Protokoll vorgesehen. Einige dieser Funktionen wurden aber mittlerweile auch für die aktuelle IP-Version 4 entwickelt. Es gibt aber dennoch einige Funktionalitäten, die sich in IPv4 nicht integrieren lassen. Daher erscheint die Strategie, IPv4 mit NATs einzusetzen, technologisch gesehen als eine Art Flickwerk mit signifikanten Einschränkungen was zukünftige Internet-Anwendungen und Einsatzbereiche betrifft.

IPv6-Adressierung

Als wichtigste Neuerung wurden in IPv6 die Adressen auf 128 Bits gegenüber 32 Bits bei IPv4 erweitert. Grundsätzlich werden Unicast-, Anycast- und Multicast-Adressen unterschieden. Der Typ einer IPv6-Adresse wird durch ein Format-Präfix festgelegt, das aus den führenden Bits einer IPv6-Adresse besteht.

Für die Kommunikation im globalen Internet ist die aggregierbare, globale *Unicast-Adresse* vorgesehen. Diese setzt sich aus einem globalen/öffentlichen Teil, einem Lokations-spezifischen Teil und dem Endsystem-Identifikator zusammen *(Bild 1)*. Der globale Teile bestehend aus Präfix, Top Level Aggregator (TLA) und Next Level Aggregator (NLA), beschreibt eine Lokation (Site)

Das Thema in Kürze

Der zweiteilige Beitrag gibt anhand eines Vergleichs mit der Version 4 einen Überblick über Funktionen, die für IP Version 6 entwickelt wurden.In *Teil 1* steht – als wichtigste Neuerung – zunächst die Adressierung im Mittelpunkt. Weitere Themen sind Änderungen beim Datenformat, die Angabe von Dienstgüten und die einfachere Konfigurierbarkeit von IP-Knoten. *Teil 2* befaßt sich vor allem mit Übergangsstrategien von IPv4 auf IPv6. Darüber hinaus werden Vor- und Nachteile des NAT-Konzeptes diskutiert.

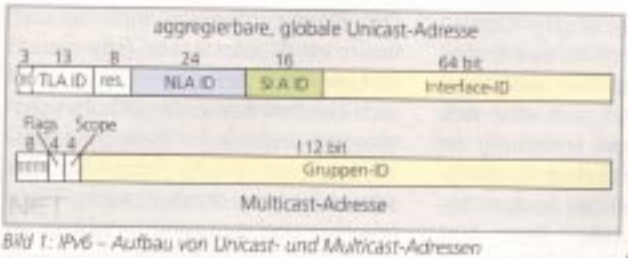

Bild 1: IPv6 – Aufbau von Unicast- und Multicast-Adressen

im globalen Internet. Diese Information wird benutzt, um Pakete über das globale Internet zur Ziellokation weiterzuleiten. TLA-Identifikatoren werden nur an Service-Provider vergeben, die einen öffentlichen Transit-Internet-Dienst anbieten. NLA-Identifikatoren werden an untergeordnete Service-Provider oder an Firmen vergeben, die direkt an einen TLA-Service-Provider angeschlossen sind. Die NLA-Ebene kann wiederum in mehrere verschiedene Hierarchiestufen eingeteilt werden. Der Lokations-spezifische Teil (Site Level Aggregator, SLA) beschreibt die Subnetz-Struktur innerhalb einer Lokation, und die Interface ID beschreibt das Interface des IP-Systems. Die 64 Bit lange Interface-ID kann lokale oder globale Eindeutigkeit besitzen. Typischerweise werden die niederwertigsten 48 Bits der Interface-ID durch die IEEE-802-MAC-Adresse belegt. Die Interface-Kennungen können auch lokal, z.B. durch einfaches Numerieren, konfiguriert werden. Insgesamt zeichnet sich dieses Adressierungskonzept im Vergleich zur IPv4-Adressierung durch eine klare Struktur und mehr Hierarchieebenen aus.

Daneben sind die sogenannten Link-lokalen Unicast-Adressen zu erwähnen, die neben dem Präfix lediglich eine Interface-Kennung in den niederwertigsten Bits enthalten. Link-lokale Unicast-Adressen werden während der automatischen Konfiguration oder in Netzen ohne Router verwendet. Standort-lokale Adressen werden benutzt, falls ein Standort bzw. eine Organisation noch nicht an das Internet angeschlossen ist. In diesem Fall müssen solche Organisationen nicht eine von einem anderen Internet-Knoten belegte Adresse verwenden, sondern können eine speziell für diesen Zweck vorgesehene Adresse benutzen. Bei einem späteren Internet-Anschluß muß dann lediglich das fest definierte Standort-lokale Präfix durch ein Provider-basiertes Präfix ersetzt werden. Subnetz- und Interface-Kennung bleiben unverändert. Weitere Adreßtypen (IPv4-kompatible oder IPv4-mapped Adressen) werden in der Übergangsphase von IPv4 nach IPv6 benötigt.

Eine *Anycast-Adresse* kennzeichnet eine Menge von Interfaces, die typischerweise zu verschiedenen Zwischensystemen gehören. Ein an eine Anycast-Adresse gesendetes Paket wird dabei genau an ein Interface dieser Menge ausgeliefert, in der Regel dem nächstgelegenen Interface gemäß der Routing-Metrik. Anycast-Adressen werden aus dem Unicast-Adreßbereich allokiert und können daher syntaktisch nicht von einer Unicast-Adresse unterschieden werden. Anycast-Adressen sind auch in IPv4 möglich. Mögliche Einsatzzwecke von Anycast-Adressen sind Provider-Auswahl oder Lastverteilung auf mehrere Server.

Im Gegensatz zu IPv4 ist Multicast in IPv6 nicht optional, sondern integraler Bestandteil. Daher wurde bei der Gestaltung der *Multicast-Adresse* Rücksicht auf die Bedürfnisse der Multicast-Kommunikation genommen. Eine Multicast-Adresse besitzt daher ein Flag-Feld, ein Scope-Feld und die Gruppenkennung. Das Flag-Feld zeigt an, ob es sich bei der Gruppe um eine transiente oder um eine permanente Gruppe handelt. Bei IPv4 wurden ganze Adreßbereiche als permanent oder transient definiert. Permanente Gruppen sind wohl bekannte Gruppen mit einer durch die Internet Assigned Numbering Authority (IANA) registrierten Adresse. Im Gegensatz dazu sind transiente Adressen nicht permanent eingerichtete Adressen und werden bei Bedarf für die Multicast-Kommunikation verwendet. Das Scope-Feld kodiert die Reichweite, d.h. den Gültigkeitsbereich, der Multicast-Gruppe. Dieser kann explizit auf den Knoten, den Link, den Standort oder die Organisation beschränkt sein oder eine globale Gültigkeit besitzen. Beispielsweise haben zwei in unterschiedlichen Organisationen eingerichtete, transiente Gruppen mit Gültigkeitsbereich Organisation keine Beziehung zueinander. Bei IPv4-Multicast-Kommunikation konnte die Reichweite eines Pakets nur mit Hilfe des Time-to-Live-Felds begrenzt werden. Beispiele vordefinierter, permanenter Multicast-Adressen sind die Gruppe aller IPv6-Knoten (all nodes), die Gruppe aller IPv6-Router (all routers), die Gruppe aller DHCP-Server (Dynamic Host Configuration Protocol) und Relay-Agenten oder die sogenannte Solicited-Nodes-Multicast-Adresse. Die Link-lokale Solicited-Nodes-Multicast-Adresse besteht aus einem 96 Bit langen Präfix und den unteren 32 Bits der Unicast- bzw. Anycast-Adresse. Jeder Knoten ist automatisch Mitglied in der mit der Solicited-Nodes-Multicast-Adresse verbundenen Gruppe.

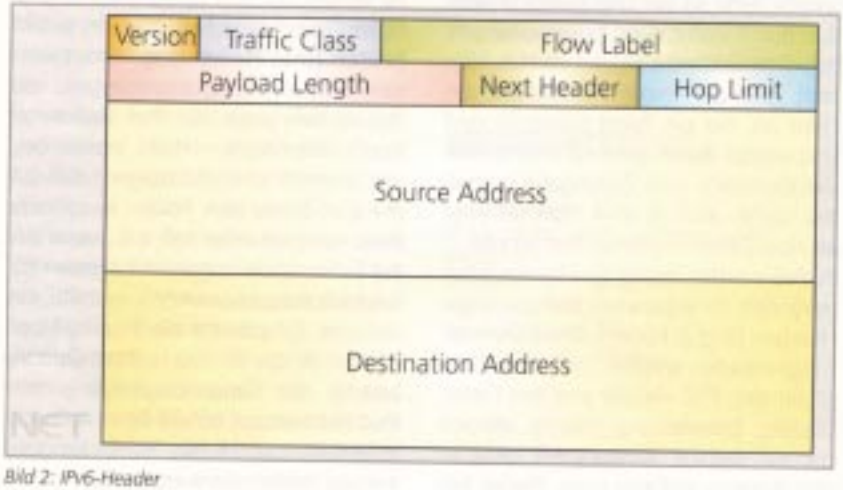

Bild 2: IPv6-Header

Bild 3: IPv6-Erweiterungs-Header

Datenformate

Im Vergleich zu IPv4 wurden bei IPv6 einige gravierende Änderungen beim Paketformat vorgenommen. Insgesamt fällt auf, daß das minimale IPv6-Paketformat *(Bild 2)* weniger Felder enthält als das minimale IPv4-Paketformat. Verschiedene Felder wurden eliminiert, andere IPv4-Felder und Optionen wanderten in verschiedene Erweiterungs-Header. Durch die Änderungen sollen die Verarbeitungskosten für die IP-Dateneinheiten ohne optionale Informationen, die in der Regel den Normalfall darstellen, minimiert und die für den minimalen Header erforderliche Bandbreite gering gehalten werden. Die Minimierung der Felder ist besonders für zukünftige Router-Generationen in Hochgeschwindigkeitsumgebungen von Vorteil.

Die IPv4-Felder precedence, total length, time to live und protocol werden durch traffic class, payload length, hop limit und next header ersetzt. Hop limit gibt die maximale Anzahl von Hops an, die ein Paket passieren darf und ersetzt damit das Feld time to live, das eigentlich eine Zeitangabe enthalten sollte, aber in IPv4 üblicherweise als Hop-Zähler implementiert wurde.

In IPv6 werden optionale Header-Informationen in separaten Erweiterungs-Headern *(Bild 3)* kodiert. Diese Erweiterungs-Header werden zwischen dem minimalen IPv6-Header und den Daten plaziert. Erweiterungs-Header werden bis auf wenige Ausnahmen nicht in den Routern entlang eines Pfades bearbeitet, sondern nur in den Endsystemen ausgewertet, was eine weitere Entlastung der Paketverarbeitung in den Routern bewirkt. Eine Ausnahme bildet die Hop-by-Hop-Option, die in den Routern ausgewertet werden muß. Des weiteren wird der Routing-Header und der erste Destination-Options-Header von den im Routing-Header angegebenen Routern verarbeitet. Die Erweiterungs-Header enthalten jeweils einen Verweis auf den Typ der nachfolgenden Erweiterungs-Header (next header).

Ein wichtiger Erweiterungs-Header ist der Routing-Header, der von einer IPv6-Quelle dazu verwendet wird, einen oder mehrere Router bzw. einen Topologiebereich auszuwählen, die auf dem Weg eines Pakets zum endgültigen Zielknoten passiert werden sollen. Damit kann der Weg eines Pakets zu seinem Ziel beeinflußt werden, um geringere Kosten oder eine bessere Dienstqualität zu erreichen. Pakete können über ein Subnetz eines bestimmten Netzanbieters geleitet werden, indem im Routing-Header eine Anycast-Adresse, die einen oder mehrere Knoten eines bestimmten Netzanbieters beschreibt, angegeben wird.

Die Hop-by-Hop-Optionen werden dazu verwendet, um optionale Informationen auszutauschen, die in jedem Knoten eines Pfades ausgewertet werden müssen. Beispielsweise wird die (inzwischen auch für IPv4 definierte) Router-Alert-Option dazu verwendet, um einem Router anzuzeigen, daß das IP-Paket durch den Router besondere Beachtung erfahren soll, z.B. wenn das Paket Signalisierungsinformationen für Ressourcenreservierungen enthält. Ein weiteres Beispiel für die Hop-by-Hop-Option ist die Jumbo-Payload-Option, welche die Längenbegrenzung von IPv4-Paketen auf 65535 Bytes aufhebt, indem 64 statt 16 Bits für die Längenangabe verwendet werden.

Der Fragment-Header wird benutzt, wenn ein Nutzlastpaket fragmentiert werden muß. Im Gegensatz zu IPv4 wird bei IPv6 nur in Quellknoten segmentiert und nur im Zielknoten reassembliert, d.h. Router führen (aus Geschwindigkeitsgründen) keine Segmentier- und Reassemblierfunktionen durch, so daß IPv6-Endsysteme eine Pfad-MTU-Erkennung (path MTU discovery) durchführen müssen. Pakete müssen dann von der Anwendung, d.h. dem darüberliegenden Protokoll, kleiner als die Pfad-MTU gewählt werden. Bei der Pfad-MTU-Erkennung leitet der Sender das erste Paket an eine gegebene Zieladresse mit der Größe der Link-MTU des ersten Links. Falls das Paket auf dem Weg zum Ziel die Link-MTU-Größe eines Netzes übertrifft, so daß es nicht weitergeleitet werden kann, sendet der betreffende Router die ICMP-Nachricht „message too big" mit Angabe der Link-MTU an den Sender zurück. Dieser wählt die Größe der folgenden Pakete so, daß die Link-MTU nicht überschritten wird. Falls keine Pfad-MTU-Erkennung durchgeführt werden kann, werden lediglich Pakete mit einer minimalen MTU-Größe gesendet, um die Benutzung von Segmentier- und Reassemblierfunktionen sowie von Fragment-Headern zu vermeiden.

Dienstgüten angeben

Dienstgüten können durch die Angabe einer Art Priorität (traffic class) im IP-Header oder durch die spezielle Kennzeichnung einzelner Datenströme durch Flußmarken unterstützt werden. Die gekennzeichneten IP-Pakete können dann eine Sonderbehandlung bei der Verarbeitung in den IP-Routern erfahren. Das Feld traffic class besteht aus acht Bits, wird bei der Realisierung von Differentiated Services eingesetzt und wird dabei auch als Differentiated Services Byte bezeichnet.

Die Flußmarken (flow labels) werden von einem Quellknoten dazu verwendet, Pakete zu kennzeichnen, die eine besondere Behandlung durch IPv6-Router benötigen. Beispielsweise können damit Pakete gekennzeichnet werden, die Realzeitdaten enthalten oder zu Verbindungen höherer Protokolle

mit bestimmten Dienstgüteanforderungen gehören. Unter einem Fluß (flow) wird in der Internet-Welt eine Folge von Paketen von einer speziellen Quelle zu einem speziellen (Unicast- oder Multicast-) Ziel verstanden. Ein IPv6-Fluß kann durch eine eindeutige Kombination von Quelladresse und einer von 0 verschiedenen Flußmarke gekennzeichnet werden. Flußmarken erlauben die gleichzeitige Existenz mehrerer Flüsse zwischen einem Quell- und einem Zielknoten.

Die Art der speziellen Behandlung für Pakete eines Flusses kann den Routern explizit mit Hilfe eines Kontrollprotokolls, z.B. mit dem Resource Reservation Setup Protocol (RSVP), mitgeteilt werden. RSVP basiert ebenfalls auf dem Flußkonzept und erlaubt Empfängern das Reservieren von Ressourcen für einen bestimmten Fluß. In Abhängigkeit von den Reservierungsnachrichten werden in den zwischen Empfänger und Sender-Endsystem liegenden Routern Systemressourcen, wie CPU-Zeiten oder Pufferspeicher, und Netzwerkressourcen, wie die Bandbreite der angeschlossenen Netze, reserviert.

Während bei der Integration von RSVP und IPv4 die Analyse der TCP/UDP-Port-Nummern zur Identifikation von RSVP-Flüssen unbedingt notwendig ist, machen IPv6-Flußmarken die Analyse von Port-Nummern überflüssig. Dies ist insbesondere dann wichtig, wenn die IP-Nutzlast und damit die Port-Nummern verschlüsselt werden. In diesem Fall ist die Identifikation von Flüssen nur bei IPv6 aber nicht bei IPv4 möglich.

Internet Control Message Protocol (ICMP)

Während beim Internet Control Message Protocol Version 4 (ICMPv4) im wesentlichen Fehler- und Echo-Nachrichten ausgetauscht wurden, wird ICMPv6 auch für die Gruppenverwaltung eingesetzt, die bislang vom IGMP (Internet Group Management Protocol) unterstützt wurde. IGMP-Pakete werden in einer IPv6-Umgebung durch entsprechende ICMPv6-Pakete ersetzt. Die ICMP-Nachrichten lassen sich in verschiedene Klassen einteilen: Fehlernachrichten, Informationsnachrichten, Echo-Nachrichten, Nachrichten zur Gruppenverwaltung (group membership query, report, termination), Neighbor Discovery, Router-Solicitation/-Advertisement, Neighbor Solicitation/-Advertisement, Redirect.

Automatische Systemkonfiguration

Ein großer Fortschritt wurde bei IPv6 hinsichtlich der einfacheren Konfigurierbarkeit von IP-Knoten erzielt. Mit Hilfe der automatischen Systemkonfigurationsfunktionen können IP-Knoten Parameter, die bisher manuell konfiguriert werden mußten, automatisch lernen. Die automatische Systemkonfiguration kann entweder zustandslos (über das Neighbor Discovery Protocol) oder zustandsbehaftet (über das Dynamic Host Configuration Protocol, DHCP) erfolgen, wobei in IPv4 nur die zustandsbehaftete Version, welche die Existenz eines DHCP-Servers voraussetzt, definiert ist. In IPv6 wird die zustandslose automatische Systemkonfiguration unterstützt, sobald ein Router in einem Netz aktiv ist.

Das Neighbor-Discovery-Protokoll (ND) ist eine Sammlung von Protokollmechanismen wie z.B. automatische Adreßkonfiguration, Adreßauflösung und Erkennung von Adreßduplikaten. ND-Nachrichten werden als ICMPv6-Pakete transportiert. ND-Protokollmechanismen basieren grundsätzlich wie andere IPv6-Kontrollmechanismen auf IP-Multicast-Kommunikation, d.h., die darunterliegenden Netze müssen Multicast unterstützen.

ND unterstützt die an einem Link angeschlossenen Knoten bei der Erkennung der angeschlossenen Router. Aktive Router werden durch deren Router-Advertisement-Pakete identifiziert. Router-Advertisement-Pakete werden periodisch an die All-Hosts-Multicast-Adresse gesendet oder können auch von einem Endsystem durch ein Router-Solicitation-Paket an die All-Routers-Multicast-Adresse explizit angefordert werden. Ein Router-Advertisement-Paket kann neben den IP- und Link-Adressen des Routers auch Präfix-, Link- und Internet-spezifische Informationen enthalten. Flags geben an, auf welche Art ein Endsystem seine Adresse (zustandslos oder zustandsbehaftet) zu konfigurieren hat. Dieser Mechanismus erleichtert sehr stark die Konfiguration von IP-Knoten. Während zum Installieren von IPv4-Knoten bislang umfangreiche Mengen von Parametern vor dem Anschluß des Knotens an das Netz (meist manuell) zu konfigurieren waren, können diese in einer IPv6-Umgebung automatisch konfiguriert bzw. erlernt werden. Insbesondere ist dieser Mechanismus die Grundlage für die zustandslose automatische Adreßkonfiguration. Nachdem ein Knoten das Link-spezifische Präfix vom Router gelernt hat, kombiniert er dieses mit seiner Interface-ID (MAC-Adresse oder Nummer) zur endgültigen IPv6-Adresse.

ND optimiert auch die Adreßauflösung. Die Adreßauflösung dient zum Bestimmen einer Link-Adresse eines am gleichen Link angeschlossenen Knotens, falls lediglich dessen IP-Adresse bekannt ist. Beim in IPv4-Umgebungen verwendeten Address Resolution Protocol (ARP) werden Adreßanfragen per Broadcast übertragen, was besonders in lokalen Netzen, die auf Switching-Basis realisiert wurden, sehr störend ist. In IPv6 wird der Broadcast-Mechanismus durch Multicast ersetzt. Dazu wird ein Neighbor-Solicitation-Paket an die Solicited-Nodes-Multicast-Adresse gesendet, wodurch nur Knoten angesprochen werden, deren 32 niederwertigste Adreßbits der Unicast-Adresse mit der Solicited-Nodes-Multicast-Adresse identisch sind. Die Antwort in Form eines Neighbor-Advertisement-Pakets enthält die Link-Adresse des gesuchten Knotens.

(wird fortgesetzt)

Universität Bern
Institut für Informatik und angewandte Mathematik
Tel.: (00 41) 3 16 31-49 94
Fax: (00 41) 3 16 31-39 65
braun@iam.unibe.ch
www.iam.unibe.ch/~braun