Zeitschrift: Bulletin Electrosuisse
Herausgeber: Electrosuisse, Verband für Elektro-, Energie- und Informationstechnik
Band: 96 (2005)
Heft: 19

Artikel: IPv6 : das zukünftige Internetprotokoll?
Autor: Farkas, Károly
DOI: https://doi.org/10.5169/seals-857848

IPv6 – das zukünftige Internetprotokoll?

Der Wechsel von IPv4 auf IPv6

Das Internetprotokoll (IP) ist das Garn, welches das Internet zusammenhält. Das Protokoll auf Netzwerkebene wurde von Anfang an für Anwendungen in grossen Netzwerken – wie es das Internet heute ist – entwickelt. Es soll Datenpakete[1] so gut wie möglich (best effort) vom Sender zum Empfänger transportieren. Die aktuelle Version 4 des Internetprotokolls (IPv4) datiert aus dem Jahr 1981 und ist weltweit verbreitet. Es scheint jedoch, dass diese Version nicht mit der wachsenden Zahl der Geräte mithalten kann, auch wenn dessen Funktionen kontinuierlich erweitert werden. Dazu kommt, dass das Routing[2] komplexer wird. Die Frage ist also, was passiert mit dem Internet, wenn IPv4 überfordert ist, seine Aufgabe nicht mehr erfüllen kann? Die Internet Engineering Task Force (IETF) schlägt eine leistungsfähigere Version des Internet-Protokolls vor: IPv6. Diese soll IPv4 ersetzen. Noch ist aber offen, wann dies sein wird, oder ob es überhaupt so kommen wird.

Károly Farkas

Das Internet verbindet tausende Computer und Netzwerke weltweit. Es wuchs aus dem Arpanet-Netzwerk des amerikanischen Militärdepartementes, das 1960 in Betrieb genommen wurde. Die Anzahl Computer, Netzwerke und Benutzer, die mit dem Arpanet verbunden sind, steigerte sich rapide, nachdem am 1. Januar 1983 TCP/IP[3] als offizielles Protokoll definiert wurde. Dieses Datum gilt als Geburtstag des heutigen Internets. Der Erfolg des Internets basiert auf Anwendungen wie E-Mail, dem Datentransport (FTP) oder den Homepages des World Wide Web. Multimedia-Präsentationen berieseln den Surfer per Mausklick. Auch Online-Spiele wären ohne das Internet nicht möglich. Entscheidend war für die rasante Entwicklung des Internets, dass das IP-Protokoll die darunterliegende physikalische Verbindung nicht vorschreibt.

Bis Mitte der 90er-Jahre verband das Internet nur Universitäten, öffentliche Ämter und die Hightech-Industrie. Danach explodierte das Interesse am Internet förmlich. Die breite Masse, beginnend bei den Teenagern, die Industrie und das Gewerbe machen die zahlreichen Benutzer aus, die heute das Internet nutzen. Elektronische Marktplätze wie E-Bay oder Multimedia-Unterhaltung treiben heute das Wachstum des Internets an. Das exponentielle Wachstum des letzten Jahrzehntes wird auch in den nächsten Jahren so bleiben – die Anzahl der an das Internet angeschlossenen Geräte verdoppelt sich jedes Jahr.

Das Wachstum bringt aber auch Probleme: Wie lange kann IPv4 dieses Wachstum mittragen, wann ist es überfordert? Denn jedes Netzerwerkinterface eines jeden Gerätes im Internet wird über eine eindeutige IP-Adresse identifiziert. So können sich die verschiedenen Geräte, also die Computer oder Router, unterscheiden und eine logische Verbindung zwischen zwei Endgeräten aufbauen. Nutzdaten werden zwischen diesen als kleine Pakete versendet. Jedes Paket erhält einen Paket-Header, in dem die IP-Adressen des Senders und die des Empfängers vermerkt werden. Diese Adressen erlauben das so genannte Hop-by-Hop-Routing des Internets, bei dem Router die Pakete entsprechend ihrer eigenen Routing-Tabelle weiterleiten. Dies bedeutet, dass ein Router mit mehreren Netzwerkinterfaces die Empfängeradresse in der Routing-Tabelle sucht und das Paket gemäss der gefundenen Zuordnung an das entsprechende Netzwerkinterface sendet.

IPv4 nutzt einen 32-Bit-Raum für die Adressierung der Netzwerkknoten, womit 2^{32}, also etwa 4,3 Milliarden Knoten adressiert werden können[4]. Heute sind 70% dieses Adressraumes besetzt oder reserviert – es bleiben 1,3 Milliarden Adressen. Dies scheint eine grosse Zahl, aber alleine China könnte diese Adressen innerhalb eines Jahres verbrauchen. Man spricht von der Dezimierung des IPv4-Adressraumes (engl. Address Depletion). Doch nicht nur der Adressraum ist limitiert, auch der Protokoll-Header ist zu komplex: Erweiterungen und Optionen können nur schwer eingeführt werden, die Anzahl verschiedener Dienste bleibt limitiert, die Routing-Tabellen werden immer grösser und komplexer und nicht zuletzt ist die Sicherheit und Privatsphäre mit IPv4 nicht gewährleistet.

Da heute nicht mehr nur Universitäten und Ämter das Internet nutzen, musste sich das Netzwerkprotokoll weiterentwickeln, flexibler werden [1]. So begann die Internet Engineering Task Force (IETF)[5] 1990 die Entwicklung einer neuen Version des Internet-Protokolls, der Version 6 (IPv6) [2]. Der Kern des Protokolls ist bereits als Standard definiert, IPv6 muss aber erst noch den Weg in die Praxis finden. Ob es diesen findet, ist noch ungewiss. Deshalb werden in diesem Artikel kurz die wesentlichen Eigenschaften von IPv6 beleuchtet und diese dann mit den entsprechenden Ansätzen von IPv4 verglichen.

Ein neues Protokoll entsteht

Die IETF wollte nicht nur das Problem der Adressknappheit mit dem neuen Internet-Protokoll lösen, sondern auch andere Schwachstellen von IPv4 ausbes-

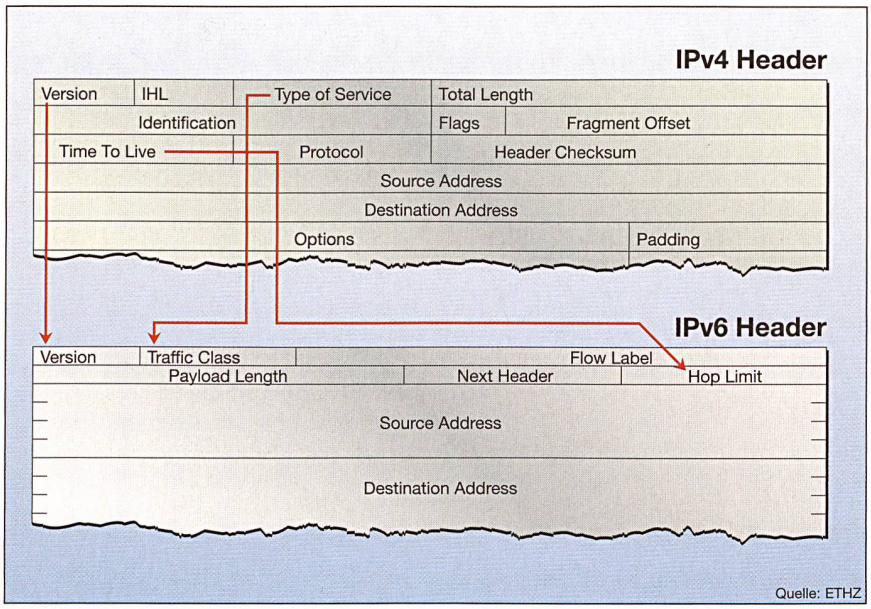

Bild 1 Die Header von IPv4 und IPv6 im Vergleich

sern. So wurden folgende Ziele für IPv6 definiert:

- Unlimitierter Adressraum: Milliarden von Geräten sollen an das Internet angeschlossen werden können;
- Grösse der Routing-Tabellen: Kleinere Routing-Tabellen sind nötig;
- Protokoll-Vereinfachung: Router sollen IP-Pakete schneller verarbeiten können;
- Sicherheit: Bessere Sicherheit als in IPv4 (Authentisierung, Privatsphäre);
- Mobilität: Geräte können den Ort wechseln, ohne die Adresse wechseln zu müssen;
- Erweiterbarkeit: Zukünftige Änderungen am Protokoll müssen möglich sein;
- Koexistenz: Alte und neue Version des Protokolls müssen über Jahre nebeneinander existieren können.

Nach langen Diskussionen entschied sich die IETF für einen von mehreren Vorschlägen und gab ihm den Namen IPv6. Die Version 5 war bereits reserviert und in verschiedenen Experimenten in Betrieb. IPv6 erfüllt die Anforderungen gut: behält die Vorteile des Internet-Protokolls, merzt die Nachteile aus und erweitert das Protokoll mit neuen Funktionen, wo diese nötig sind. IPv6 ist aber nicht kompatibel mit IPv4.

IPv6 vergrössert den Adressraum

Die Adresse des IPv6 ist 128 Bit lang und deckt damit einen wesentlich grösseren Adressraum ab als IPv4 mit 32 Bit. Die Anzahl der IPv6-Adressen ist praktisch unlimitiert, wie eine kurze Rechnung zeigt: 2^{128} Adressen können $3 \cdot 10^{38}$ Geräten zugeordnet werden; das sind $7 \cdot 10^{23}$ Adressen pro Quadratmeter Erdoberfläche, die Wasseroberfläche mit eingerechnet. Die lange Adresse bringt aber praktische Probleme mit sich: Wie soll ein Administrator sie eingeben, wie wird sie dargestellt? IPv4-Adressen werden mit durch Punkte getrennte Dezimalzahlen geschrieben. Für IPv6 beschloss die IETF, dass eine Adresse in 8 Gruppen zu 4 hexadezimalen Zahlen geschrieben wird, getrennt mit Doppelpunkten zwischen den Zahlengruppen: 0000:0000:0000:0000:1234:5678:9ABC:DEFF. Da die meisten Adressen viele Nullen enthalten, sind folgende Vereinfachungen erlaubt: Vorangehende Nullen dürfen in jeder Zahlengruppe weggelassen werden, aus 0345 wird 345. Ganze Gruppen von 16 (binären) Nullen werden mit einem Doppelpunkt ersetzt, so wird die obige Adresse ::1234:5678:9ABC:DEFF geschrieben. IPv4-Adressen werden weiterhin mit Dezimalzahlen geschrieben, mit vorangehenden Doppelpunkten: ::129.132.66.157.

Eine weitere, wesentliche Verbesserung in IPv6 ist der vereinfachte Protokoll-Header. IPv6 hat nur 8 Felder im Header, verglichen mit 14 in IPv4. Damit können Router das Paket schneller weiterleiten, was den Durchsatz erhöht. Bild 1 zeigt die Header von IPv4 und IPv6 sowie die Felder, die von IPv6 übernommen wurden, wenn zum Teil auch an anderer Stelle im Header. Interessant ist das Feld «Next Header» bei IPv6. Dieses erlaubt erst, den Header zu vereinfachen. Sind neben den Feldern des Basis-Headers weitere, optionale Felder nötig, werden diese in einem zusätzlichen Header angehängt, als sogenannter Extension-Header. Das Feld «Next Header» zeigt an, welcher der bisher 6 definierten Extension-Headers folgt. Bild 2 zeigt, wie das Prinzip funktioniert. Wichtig ist, dass der letzte Extension-Header immer angibt, welches Transport-Protokoll folgt, zum Beispiel das Transmisson Control Protocol (TCP).

IPv6 verschlüsselt die Daten

IPv6 führt wesentliche Sicherheitsmassnahmen ein. Sicherheit (Security) ist nun ein optionaler Bestandteil des Internet-Protokolls, während sie bei IPv4 immer ein Zusatz war. Die Pakete werden bei IPv6 sowohl verschlüsselt als auch authentisiert. Die Verschlüsselung garantiert, dass die Daten nur vom richtigen Empfänger gelesen werden können. Die Authentisierung stellt sicher, dass die Daten vom Absender kommen, der angegeben ist, und dass die Daten unterwegs nicht verändert wurden. IPv6 regelt aber nicht den Zugang zu den Ressourcen im Netzwerk (Autorisierung). Wenn ein Benutzer identifiziert ist, wird es der Applikationsschicht des Netzwerkes überlassen, dessen Zugang zu reglementieren. Um die Sicherheitsfunktionen von IPv6 in die Praxis umzusetzen, wurde ein Schlüsselsystem eingeführt: Sender und Empfänger machen vor der Übertragung einen Schlüssel aus, um die Datenpakete zu verschlüsseln und zu authentisieren. Weiter definieren sie, mit welchen Algorithmen die Pakete verschlüsselt und authentisiert werden und wie lange der Schlüssel gültig ist. Diese Zusammenarbeit wird in sogenannten Security Associations geregelt. Eine Security Association gilt nur immer für eine bestimmte Zeit zwischen diesen beiden Teilnehmern. Der Empfänger wird ein Paket nur dann bearbeiten, wenn dieses einer gültigen Security Association zugehört.

In IPv6 wird die Authentisierung in einem der Extension Headers übertragen, dem Authentication Header. Die Daten zur Authentisierung werden aus der Sender-Adresse und einigen weiteren Feldern des IP-Headers berechnet. Der eingesetzte Algorithmus MD5[6] lässt sich nur extrem schwer brechen und stellt sicher, dass die Senderadresse im empfangenen Paket mit dem wirklichen Sender übereinstimmt. Der Authentication Header verschlüsselt aber nicht die übertragenen Nutzdaten – diese können von jedem Knoten im Netzwerk gelesen werden. Um die Daten im IP-Paket zu verschlüsseln, wird ein weiterer Extension Header eingesetzt, der Encrypted Security Payload Header. Dieser kommt an erster Stelle nach dem Default IPv6 Header, da er sowohl die Nutzdaten als auch die Au-

thentifikation verschlüsselt. Normalerweise wird der Data Encryption Standard (DES) eingesetzt.

IPv6 regelt die Übertragungsqualität

Die Version 6 des Internet-Protokolls kümmert sich auch besser um die Übertragungsqualität als IPv4, man spricht von Quality of Service (QoS). Im Feld Traffic Class des IP-Headers wird definiert, mit welcher Priorität das Paket behandelt werden soll (siehe Bild 1). So kann der Router feststellen, ob er den Datenfluss eines Senders bremsen darf oder nicht. Bei Paketen mit einem Wert zwischen 0 und 7 im Traffic-Class-Feld kann er den Datenfluss kontrollieren, sollte eine Leitung überlastet sein – zum Beispiel, wenn ein Web-Server zu viele Anfragen bekommt. Werte zwischen 8 und 15 sind für den Echtzeitverkehr vorgesehen, dessen Datenrate konstant sein muss, auch wenn einige Pakete verloren gehen. Audio und Video fallen in diese Kategorie. Das Feld Traffic Class erlaubt einem Router also, den Datenverkehr zu regulieren und Prioritäten zu setzen.

Ein weiteres Feld mit dem Namen Flow Label ist noch experimentell. Das Flow Label gestattet einem Router die effizientere Bearbeitung von Paketen, die zu einem bereits bekannten Datenstrom gehören. Empfängt ein Router ein Paket mit einem Wert im Feld Flow Label, kann er in einer internen Tabelle nachschauen, wie er das Paket behandeln soll. Dabei können zwei Netzwerkknoten mehrere solche logischen Verbindungen aufbauen.

Mobile Geräte melden sich an

IPv6 unterstützt mobile Geräte. Diese sind Netzwerkknoten, die sich im Internet bewegen – zum Beispiel in einem drahtlosen Netzwerk – und ständig mit anderen Teilnehmern verbunden sind. Bei einem Wechsel in eine andere Zelle dürfen die Verbindungen nicht unterbrochen werden. Diese Anforderung bedingt, dass sich das Gerät automatisch mit einer neuen IP-Adresse in der nächsten Zelle anmeldet. IPv6 unterstützt zwei verschiedene Arten von Autokonfiguration: stateless und statefull, d.h. mit oder ohne Status. Autokonfiguration mit Status läuft über einen DHCP-Server[7], der wie in IPv4 die Adressen vergibt. In der statuslosen Autokonfiguration ist ein solcher Dienst nicht nötig. Das Gerät teilt sich die Adresse selbst zu, indem es dem Subnet-Prefix seine weltweit eindeutige MAC-Adresse[8] anhängt. Damit werden Adresskonflikte ausgeschlossen. Das Subnet-Prefix ist der vordere Teil der IP-Adresse, der das Netzwerksegment identifiziert. Das Gerät erfährt das Subnet-Prefix, indem es die Router im Segment mit einem speziellen Code anfragt.

Dieses Auskundschaften der Nachbarschaft wurde in IPv6 verbessert. Alle diese Dienste, die zwischen den Endgeräten, den so genannten Hosts, und den Routern in einem Netzwerksegment ablaufen, sind in das Neighbor Discovery Protocol (ND) integriert. Dieses ersetzt das bisherige Address Resolution Protocol (ARP) von IPv4 sowie die Funktion Router Discovery und die Umadressierung des Internet Control Message Protocols (ICMP). Zusätzlich zur Autokonfiguration (ND) ist der Standard Mobile IP definiert, der die Übergabe des Gerätes von einem Netzwerksegment in das andere regelt.

Ist IPv6 die Lösung?

IPv6 scheint die Probleme von IPv4 zu lösen. Die Frage bleibt, weshalb es sich nicht bereits weltweit durchgesetzt hat? Die wesentlichen Teile von IPv6 sind längst standardisiert und das IPv6-Forum[9] vermarktet das neue Internet-Protokoll seit Jahren [3]. Ein Aspekt, weshalb sich IPv4 hartnäckig hält, ist, dass einige Verbesserungen von IPv6 durch Zusätze an IPv4 bereits seit langem gelöst sind [4, 5]. Der praktisch unlimitierte Adressraum von IPv6 ist ein Schritt vorwärts, aber ist dies in naher Zukunft wirklich unerlässlich? Es scheint nicht, denn Zusatzfunktionen wie das Network Address Translation (NAT) sparen in IPv4 Adressen. Wenn die Adressen sorgfältig vergeben werden, wird IPv4 noch für Jahre ausreichen.

NAT wird an der Grenze zwischen einem privaten und öffentlichen Netzwerk eingesetzt (Bild 3). Im privaten Netzwerk werden beliebig viele private Adressen vergeben. Gegen aussen nutzt der NAT-Router nur wenige öffentliche Adressen, oft sogar nur eine Adresse. Er tauscht bei jedem Paket, das das Netzwerk verlässt, die private IP-Adresse des Senders gegen eine öffentliche Adresse. Kommt eine Antwort aus dem Internet zurück, vertauscht der NAT-Router die öffentliche IP-Adresse wieder in die private Adresse des Empfängers im Netzwerk. Da die privaten Adressen gegen aussen nicht sichtbar sind, können sie in verschiedenen Netzwerken mehrmals vergeben werden.

NAT hat aber auch Nachteile: Die Verbindung muss von innen aufgebaut werden, also von einem Gerät im privaten Netzwerk. Geräte von aussen, vom Internet, können den NAT-Router nicht überwinden, da sie die privaten Netzwerkknoten schlicht nicht adressieren können. Von aussen sieht das Gerät nur den NAT-Router, keine weiteren Netzwerkknoten. Zudem kann keine kohärente End-zu-End-Übertragung oder End-zu-End-Sicherheit aufgebaut werden, weil die Endpunkte nicht direkt miteinander kommunizieren.

NAT bremst aber effektiv die Dezimierung der verfügbaren IPv4-Adressen: Vor 1994 wurde 36% des Adressraumes alloziert. Seitdem wurden weitere 20% vergeben, den Internet-Boom Ende 90er-Jahre mit eingeschlossen [4]. Werden die aktuellen Praktiken beibehalten, reicht der IPv4-Adressraum also noch für viele weitere Jahre.

Auch IPv4 lässt sich sicher betreiben

Es ist offensichtlich, dass eine sichere Kommunikation heute wichtiger ist als zu den Anfängen des Internets. Die Sicher-

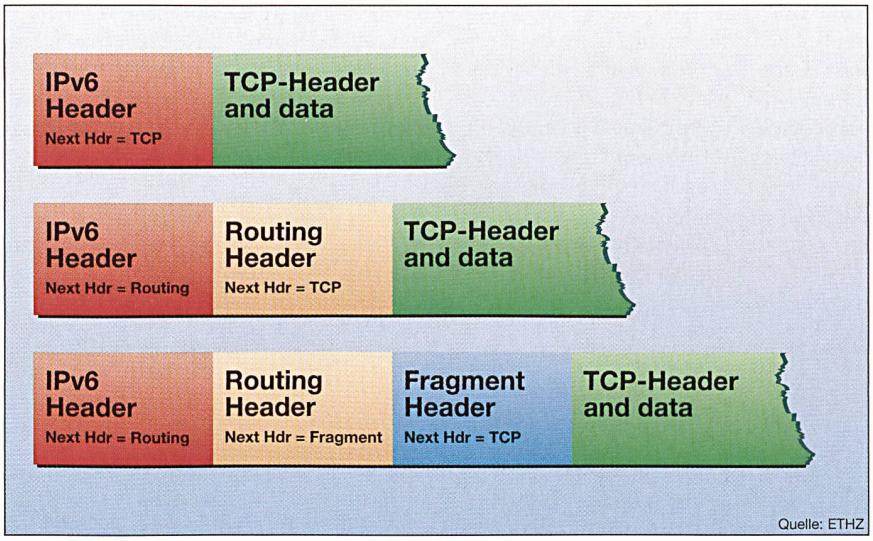

Bild 2 Verkettete Extension Headers

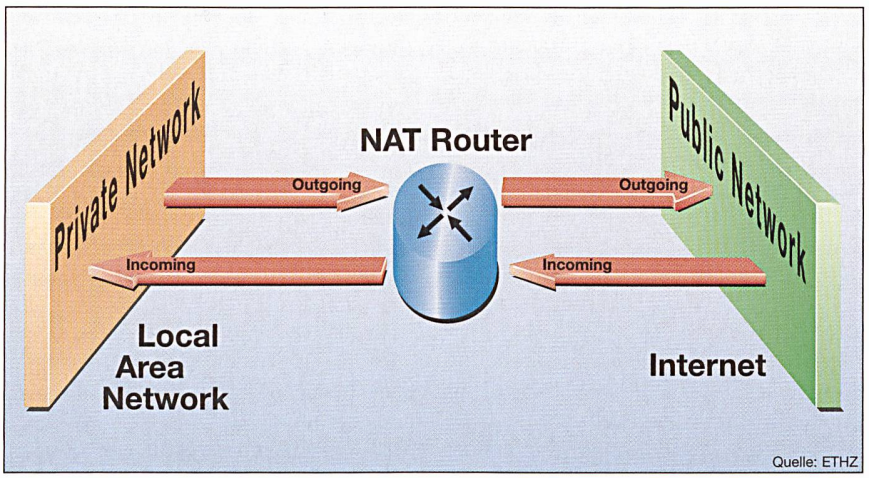

Bild 3 Network Address Translation

heit, also die Verschlüsselung und Authentisierung von Daten, ist als optionaler Bestandteil in IPv6 fest integriert, während sie bei IPv4 ein Zusatz ist (z.B. IPSec). Wie wichtig ist es nun, dass die Sicherheit in die Netzwerkschicht integriert wird? Eine Applikation, die Daten sicher übertragen soll, wird sich nicht auf eine angeblich sichere Netzwerkschicht abstützen, sondern die Daten selber verschlüsseln – zumindest heute. Eine in das Internetprotokoll integrierte Sicherheit scheint also überflüssig.

Auch bezüglich der Übertragungsqualität, der Quality of Service (QoS), ist IPv6 nicht zwingend, denn die günstigste Lösung bleibt die Überdimensionierung des Netzwerkes. Anstatt komplizierte QoS-Regeln und -Techniken einzuführen ist es einfacher, das Netzwerk an der Schwachstelle mit einem zusätzlichen Kabel oder Lichtwellenleiter zu erweitern.

Die verbesserte Mobilität in IPv6 scheint ein Punkt zu sein, wo das neue Protokoll echte Verbesserungen bringt, denn die Anzahl mobiler Geräte, die an das Internet angebunden werden, steigt täglich. Die Autokonfiguration und die verbesserten Dienste zur Erkundung der Nachbarschaft verbessern die Mobilität der Geräte wesentlich. IPv6 per se löst die Probleme mobiler Geräte aber nicht, es braucht ein zusätzliches Protokoll wie Mobile IP. Dieses ist kompatibel zu IPv4 – wiederum also kein zwingender Grund, auf IPv6 zu wechseln.

Kommt IPv6?

Die Hauptmotivation für IPv6 scheint also die Vision zu bleiben, dass jeder Kühlschrank und all unsere mobilen Geräte, vom Auto bis zum Mobiltelefon, über das Internet kommunizieren. Wenn jedes dieser Geräte eine eigene IP-Adresse erhält, braucht es IPv6 mit dem grösseren Adressraum. Nun ist es schwierig, vorauszusagen, wann diese Vision eintreten wird. Sicher wird dies nicht von einem Tag auf den anderen geschehen, denn ein Wechsel auf ein neues Protokoll kostet viel Zeit und Geld – abgesehen vom fehlenden Know-how und den Risiken jedes neuen technischen Systems.

Trotz allem gibt es weltweit einige Pilotprojekte und sogar kommerzielle Netzwerke mit IPv6. Asien, speziell Japan und Südkorea, führt hier das Feld an. Europa folgt mit einem massiven Forschungsbudget für IPv6. Die Regierung der USA zieht ernsthaft in Erwägung, seine Netzwerke auf IPv6 umzustellen. Das Verteidigungsdepartement entschied 2003, seine Netzwerke bis 2008 auf das neue Protokoll umzustellen [8].

In der Schweiz betreibt Swisscom Innovations, die zentrale Forschungsstelle von Swisscom, seit einiger Zeit ein IPv6-Testnetzwerk und überträgt die Daten im Swisscom-Intranet über ein IPv6-Netzwerk [7]. Switch, das Schweizer Schul- und Forschungsnetzwerk [6], bietet seit November 1996 IPv6-Verbindungen an. Seit Juni 2004 überträgt das Lambda-Backbone-Netzwerk von Switch die beiden Protokolle IPv4 und IPv6 parallel – auf denselben Verbindungen und auf denselben Routern. Das Lambda-Netzwerk ist der fiberoptische Backbone von Switch. Betrachtet man diese Aktivitäten, könnte sich IPv6 um die Jahre 2008 bis 2010 durchsetzen – wir werden sehen.

Referenzen

[1] A. S. Tanenbaum: Computer Networks, Prentice-Hall Inc., ISBN: 0-13-394248-1, 1996
[2] IETF Homepage, http://www.ietf.org
[3] IPv6 Forum Homepage, http://www.ipv6forum.com
[4] G. Huston: Waiting for IP version 6, in the ISP Column, January 2003, http://ispcolumn.isoc.org/2003-01/Waiting.html
[5] L. Ladid, J. Bound: Response by IPv6 Forum to ISP Column article entitled 'Waiting for IP version 6', http://www.isoc.org/pubs/isp/ipv6response.shtml
[6] Switch IPv6 Pilot, http://www.switch.ch/network/ipv6/
[7] Swisscom Innovations – IPv6 Labs and Services, http://www.swisscom.com/Innovations/content/Labs/IPv6/
[8] DoD IPv6 General Information, http://ipv6.disa.mil/

Angaben zum Autor

Károly Farkas arbeitet am Institut für Technische Informatik und Kommunikationsnetze (TIK) der ETH Zürich. Sein Forschungsschwerpunkt liegt bei selbständig organisierten mobilen Netzwerken (Projekt SIRAMON). Wertvolle Ideen und Kommentare zu diesem Artikel hat Lukas Ruf beigetragen.
TIK, ETH Zürich, 8092 Zürich (farkas@@tik.ee.ethz.ch)

[1] engl. Datagrams: Daten aufgeteilt in Pakete, die vom Netzwerk individuell übertragen werden.
[2] Routing: das Steuern der Daten, wo sie im Netzwerk durchgehen sollen
[3] TCP/IP: Transmission Control Protocol/Internet Protocol
[4] In der Praxis liegt die Limite sogar darunter, denn nicht jede Zahl im Adressraum ist eine gültige Knotennummer. Einige Adressen sind reserviert, zum Beispiel als Broadcast-Adresse.
[5] Die IETF ist eine internationale Organisation, die für die Standardisierung des Internets zuständig ist.
[6] Keyed MD5 – Message Digest 5
[7] Dynamic Host Configuration Protocol
[8] MAC steht für Media Access Control. Eine MAC-Adresse identifiziert ein Netzwerkinterface weltweit eindeutig.
[9] Das IPv6-Forum ist ein weltweites Konsortium von Forschungs/Schulungs-Netzwerken und führenden Verkäufern von Netzwerkkomponenten mit dem klaren Fokus, IPv6 zu vermarkten (non-profit).