KOMPAKT
IPv6-LEITFADEN

Ein Sonderheft des Magazins für professionelle Informationstechnik, www.ix.de 4/2013

Die Internet-Umgestaltung

Grundlagen:

Basiswissen zum neuen Internet-Protokoll

Der Traum von der Netzneutralität

Sicherheit:

Monitoring im fast unendlichen Raum

Angriffspunkt lokales Netz

Firewalls testen

Planen:

IPv6-Einführung im Unternehmen

Adressmanagement

Praxis:

Server umstellen

FRITZBox konfigurieren

Recht und Datenschutz:

Logfiles ohne Bußgeldgefahr

Privacy Extensions nutzen

Managed Hosting

IT-Sicherheit zertifiziert nach ISO 27001

Hosting made in Germany

Professionelles Hosting am Standort Deutschland mit persönlichem und kompetentem Support.
Individuelle Hostinglösungen vom Server bis zum Cluster-Cloudsystem, inklusive Beratung, Planung und Service 24/7

Wir bieten über 10 Jahre Erfahrung in Hosting und Systemadministration.
Für mehr Performance, Sicherheit und Verfügbarkeit.

hostserver.de/hosting

IPv6 ready

HOSTSERVER
Berlin ▪ Marburg ▪ Frankfurt am Main

Beratung unter:
0 30 / 47 37 55 50

Hosting made in Germany

Einfach machen

Der Durchbruch des heutigen Internets lässt sich genau datieren. Am 1. Januar 1983 begann die bis heute andauernde Erfolgsgeschichte mit einem gemeinsamen, mutigen Schritt aller damaligen Arpanet-Betreiber. Sie hatten sich darauf geeinigt, den Kommunikationsstandard Transmission Control Protocol/Internet Protocol in ihrem Forschungsnetz-Verbund einzuführen. Von einem Tag auf den anderen ersetzte TCP/IP alle bis dahin verwendeten Datenübertragungsverfahren.

Offensichtlich hat das Experiment funktioniert. So gut, dass viele in ihm den eigentlichen Beginn der Internet-Geschichte sehen. Obwohl es damals nur um die überschaubare Infrastruktur der Forschungseinrichtungen ging, bildet TCP/IP heute die Grundlage eines damals unvorstellbaren globalen, kommerziellen Kommunikationsnetzes.

30 Jahre haben daher tiefe Spuren hinterlassen, doch die Netzbetreiber und ihre Kunden kommen – dank damit einhergehender Geschäftsmodelle einerseits und der langen Gewöhnungszeit andererseits – recht gut mit unzähligen Flicken und haarsträubenden Provisorien zurecht. So gut, dass die weitaus meisten Teilnehmer die notwendige, frühzeitig anberaumte Teilrenovierung bis heute ignorieren. Seit 15 Jahren steht IPv6 bereit. Allerdings ließ sich der Vorgänger IPv4 damals im enorm gewachsenen Internet nicht mehr weltweit wie auf Knopfdruck beiseite fegen.

Jedes noch so ausgeprägte Improvisationstalent stößt jetzt jedoch an die Grenze der Adressierbarkeit. Alle IPv4-Adressen sind reserviert oder vergeben. Zusätzliche global gültige Adressen lassen sich nicht improvisieren, sondern nur noch mittels IPv6 einrichten. Und ohne Adresse kann kein Gerät zu einem Teil des Internets werden. Das hat endlich den Handlungsdruck herbeigeführt, ohne den IPv6 wohl ein unbeachtetes goldenes Jubiläum hätte begehen können.

Dass IPv6 nicht nur mehr und längere Adressen mit sich bringt, sondern auch viele weitere Vorteile, können diejenigen bestätigen, die es bereits eingeführt haben – zum Beispiel die Autoren der folgenden Seiten. Wer es bereits benutzt, kann aber auch bestätigen, dass es eben keine Umstellung wie vor 30 Jahren bedeutet, sondern erst einmal ein zusätzliches Protokoll und mehr Komplexität. Doch je schneller IPv6 Anhänger gewinnt, desto eher kann sich IPv4 endlich auf seinen Ehrenplatz in den Geschichtsübersichten vergangener Technologien zurückziehen.

BERT UNGERER

Foto: Martin Klauss

Ein neues Kapitel im Internet-Zeitalter

Nach einem zähen Start kommt das bereits vor 15 Jahren offiziell verabschiedete neue Internet-Protokoll allmählich bei Zugangs-Providern, Inhaltsanbietern und Anwendern in Schwung. Was die Beteiligten über IPv6 wissen sollten – und wie sie mit einer gut geplanten Einführung Risiken minimieren und Stolperfallen umgehen können.

Ab Seite 7

Grundlagen

Alle Links: www.ix.de/ix1316SSS Artikel mit Verweisen ins Web enthalten am Ende einen Hinweis darauf, dass diese Webadressen auf dem Server der *iX* abrufbar sind. Dazu gibt man den *iX*-Link in der URL-Zeile des Browsers ein. Dann kann man auch die längsten Links bequem mit einem Klick ansteuern. Alternativ steht oben rechts auf der *iX*-Homepage ein Eingabefeld zur Verfügung.

Planen und organisieren

Netzsicherheit

Planen und organisieren

Die Einführung von IPv6 in Unternehmen und anderen Organisationen bedeutet einen gewissen Umstellungsaufwand für alle Beteiligten – aber auch die Chance, eine bisher wild gewachsene eigene Infrastruktur gründlich aufzuräumen.

Ab Seite 35

Recht und Datenschutz

Schon wer ein Logfile anlegt und Informationen über die Zugriffe seiner Webseiten-Besucher speichert, kann sich strafbar machen, es sei denn, er anonymisiert die Daten. Umgekehrt bietet IPv6 seinen Anwendern die Möglichkeit, Rückschlüsse aus den IP-Adressen gar nicht erst zuzulassen.

Ab Seite 77

MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

iX Kompakt 4/2013 – IPv6-Leitfaden

Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover

Redaktion: Telefon: 05 11/53 52-387, Fax: 05 11/53 52-361, E-Mail: post@ix.de

Chefredakteur: Jürgen Seeger (js) -386

Konzeption und redaktionelle Leitung: Bert Ungerer (un) -368, E-Mail: un@ix.de

Ständige Mitarbeiterin: Barbara Lange

Autoren dieser Ausgabe: Werner Anrath, Stefan Behrens, Peter Bieringer, Wilhelm Boeddinghaus, Andreas Brück, Dennis Burkhardt, Lutz Donnerhacke, Egon Grünter, Safuat Hamdy, Joerg Heidrich, Peer Heinlein, Marc Heuse, Martina Kannen, Reiko Kaps, Klaus Keppler, Martin Leischner, Stefan Marksteiner, Christoph Meyer, Frank Meyer, Dominique Petersen, Norbert Pohlmann, Tahar Schaa, Christian Schneider, Benedikt Stockebrand, Bert Ungerer, Christoph Wegener, Sabine Werner

Abbildungen © Can Stock Photo Inc.: tobkatrina (Titel), frente (S. 4, 7), defun (S. 8, 44, 100, 106), petrsalinger (S. 10), rustyphil (S. 24), photobee (S. 30, 118), Penywise (S. 5, 35), podius (S. 36), yellowj (S. 41), ALong (S. 50, 66), Feverpitched (S. 53), paulrommer (S. 54), jianghaistudio (S. 62), lunamarina (S. 70, 136), sasel77 (S. 74), Kartouchken (S. 5, 77), chas53 (S. 78), ingpablogodoy (S. 84), njaj (S. 88), Orson (S. 93), leah613 (S. 94), sadakko (S. 114), kamchatka (S. 121), Antrey (S. 122), Subbotina (S. 128), epantha (S. 132), dashark (S. 135)

Redaktionsassistenz: Carmen Lehmann (cle) -387, Michael Mentzel (mm) -153

Korrektorat: Wiebke Preuß, Hinstorff Verlag, Rostock; Anja Fischer, Heise Zeitschriften Verlag

Layout und Satz: Enrico Eisert, Matthias Timm, Hinstorff Verlag, Rostock; Jürgen Gonnermann, Heise Zeitschriften Verlag

Titelidee: *iX*, Bert Ungerer

Verlag: Heise Zeitschriften Verlag GmbH & Co. KG, Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover; Telefon: 05 11/53 52-0, Telefax: 05 11/53 52-129

Geschäftsführer: Ansgar Heise, Dr. Alfons Schräder

Mitglied der Geschäftsleitung: Beate Gerold

Verlagsleiter: Dr. Alfons Schräder

Anzeigenleitung: Michael Hanke (-167), E-Mail: michael.hanke@heise.de

Teamleitung Herstellung: Bianca Nagel (-456)

Druck: Dierichs Druck + Media GmbH, Kassel

Verantwortlich: Textteil: Jürgen Seeger; Anzeigenteil: Michael Hanke

***iX* Kompakt 4/2013 – IPv6-Leitfaden:** Einzelpreis € 9,90, Österreich € 10,90, Schweiz sfr 17,50, BeNeLux: € 10,90, Italien: € 10,90

Die Inserenten

Die hier abgedruckten Seitenzahlen sind nicht verbindlich. Redaktionelle Gründe können Änderungen erforderlich machen.

Nachschlagewerk

Im Dezember 2013 feiert das „neue“ Internet-Protokoll mit der Versionsnummer 6 sein 15. Jubiläum. Im Jahr 1998 protestierten französische Internet-Anwender gegen die Einwahltarife ihrer Telefonanschlüsse, und ein Newcomer namens Google startete mit einem Suchindex von ein paar Millionen Webseiten.
Wer damals einen neuen, auf viele Jahrzehnte hinaus nutzbaren Kommunikationsstandard ersinnen wollte, musste über wahrlich seherische Fähigkeiten verfügen, und nicht jedes Detail saß von Beginn an. Doch nun ist IPv6 da – und die Netzwerk-Welt um viele Fachbegriffe und Fragestellungen reicher.

Ein Mythos
geht in Produktion

Im Aufwind

Wilhelm Boeddinghaus

IPv6 ist kein Mythos mehr. Im 15. Jahr des Übergangs von IPv4 kommt das „neue“ Protokoll endlich in nennenswertem Umfang in produktiven Netzwerken zum Einsatz. Die Einführung lief und läuft offenbar nicht so glatt und schon gar nicht so rasch wie von den Standardisierungsgremien erhofft. Eine Situationsbeschreibung.

Im Jahr 1998 tauchte IPv6 erstmals in einem RFC auf. Trotzdem kam die Einführung bisher kaum voran. Das liegt auch an Mythen, die sich um IPv6 ranken, und an falschen Vorstellungen, die sich hartnäckig halten. Von „erhöht die Sicherheit“ bis „hebelt den Datenschutz aus“ ist alles dabei.

Befürworter preisen IPv6 als Wunderwaffe gegen alle Internet-Probleme, Gegner verdammen es als Teufelszeug. Dabei ist es eigentlich nur ein Protokoll, das ein drängendes Problem angeht: Den Adressmangel bei IPv4. Zur Kommunikation benötigen zwei Computer eindeutige Adressen. Und der Adressraum von IPv4 bietet keinen Platz mehr. Bei Hausnummern behilft man sich mit Buchstaben, auf „30“ folgt notfalls „30a“. Da Adressen in der IT immer feste Längen haben müssen, hilft dieser Trick hier nicht weiter. Also musste ein neuer Adresstyp her.

Die Versionsnummer 5 war bereits vergeben (kam aber nie zum Einsatz), sodass das neue Protokoll die Nummer 6 erhielt. Zur Ehrenrettung der IPv4-Designer sei ihnen zugute gehalten, dass das Wachstum des heutigen Internet nicht absehbar war. Nun also IPv6. Neben dem praktisch unerschöpflichen Adressvorrat versprechen sich manche von dem Protokoll mehr Sicherheit, mehr Flexibilität und mehr Tempo. Ob diese Ziele realistisch sind, soll das Folgende beantworten.

Ist IPv6 sicherer als IPv4?

Leider nein. IPsec, also die verschlüsselte Übertragung von Daten, wurde gleichzeitig mit IPv6 entwickelt und für IPv4 parallel implementiert. Somit gibt es hinsichtlich der geschützten Datenübertragung einen Gleichstand zwischen den Protokollen. Bei IPv6 mangelt es allerdings allen Beteiligten an Erfahrung. Administratoren machen Fehler, aus denen sie hoffentlich lernen, und neue Software enthält ohnehin stets Fehler. Selbst einige Protokoll-Spezifikationen sind anzupassen, um Sicherheitslücken zu schließen.

Die ersten Ideen zu IPv6 sind schließlich mehr als 20 Jahre alt, und die Erfinder konnten sich damals das heutige Internet kaum vorstellen. Eine frühzeitige Einführung von IPv6 hätte geholfen, Erfahrungen zu sammeln und Bugs zu finden, aber wegen dieser vergebenen Chance zu lamentieren, hilft niemandem weiter. Wir alle, die Administratoren der Netzwerke und Server, die Programmierer, die Hersteller und die Systemintegratoren, müssen den Tagesbetrieb mit IPv6 lernen. Niemand sollte darauf warten, dass andere die Fehler gefunden und beseitigt haben. Jeder sollte mithelfen, den Druck auf die Hersteller hoch zu halten – und nicht zuletzt daraus zu lernen: zum Beispiel, das nächste wichtige Protokoll schneller einzuführen und IPv6 im Alltag zu beherrschen.

Sind Datenschutz und IPv6 miteinander vereinbar?

Diskussionen mit Datenschützern und über den Datenschutz sind nicht erst seit dem Bekanntwerden der weltweiten, ausufernden Überwachung ernst zu nehmen. Die Privatsphäre im Internet ist mindestens bedroht, wenn nicht gänzlich verloren. Die Anwender machen sich zu Recht Gedanken, ob jemand jeden ihrer Schritte im Internet protokolliert. Bei IPv6 erregen zwei Faktoren Besorgnis: Mithilfe von IPv6 kann jeder Arbeitsplatz eine öffentliche, nicht mehr mittels Network Address Translation (NAT) verschleierte IPv6-Adresse erhalten. Und über seine IPv6-Adresse lässt sich ein Gerät eindeutig identifizieren.

Beides stimmt, aber beides kann man so konfigurieren, dass es eben nicht die Privatsphäre beeinträchtigt. RFC 4941 beschreibt die „Privacy Extensions for Stateless Address Autoconfiguration in IPv6“ (siehe S. 78 „Maskiert im Netz“ und S. 84

„Datenschatten“). Die IP-Adresse des Rechners, Telefons oder Tablets ergibt sich per Zufall. Dabei geht es um den Host-Anteil der Adresse. Der vordere, einer Organisation zugeordnete Teil bleibt unverändert. Da die IPv6-Adresse nun nicht mehr nachvollziehbar ist, entfällt die Notwendigkeit des Verschleierns mithilfe von NAT, und auch das Gerät ist nicht mehr eindeutig identifizierbar. Wie gesagt: Es geht immer nur um das Gerät, der Mensch dahinter ist nicht so leicht zu identifizieren.

Auf den ersten Blick könnten Sicherheitsbeauftragte in Unternehmen laufend wechselnden IPv6-Adressen mit Argwohn begegnen, denn feste Adressen ließen sich auf bequeme Weise für Zugriffskontrollen etwa auf Datenbanken oder die Buchhaltung nutzen. Aber diese Anwendungen müssen ohnehin Menschen, nicht Computer, sicher identifizieren. Dafür sind Zertifikate, Benutzernamen und Passwörter erforderlich und nicht feste oder zufällige Adressen von Geräten. In Diskussionen des Deutschen IPv6-Rates mit Peter Schaar, dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), haben beide Seiten betont, dass IPv6 dem Datenschutz nicht entgegensteht (siehe „Alle Links“).

Ist bei der Einführung von IPv6 etwas schiefgegangen?

Ja, so ziemlich alles. Geplant war, dass die Internet-Provider und Unternehmen IPv6 zügig parallel zu IPv4 einführen, bevor die IPv4-Adressen zur Neige gehen. Aber das haben die Beteiligten aus Kostengründen immer wieder aufgeschoben. Mit IPv6 war kein Geld zu verdienen, und die Kunden haben erstaunlicherweise nicht danach gefragt. Statt IPv6 einzuführen, setzten die Verantwortlichen auf lebensverlängernde Maßnahmen für IPv4, etwa Network Address Translation, und ignorierten IPv6, solange es eben ging. Aber jetzt ist die Not umso größer. Das Wachstum des Internet kann ohne IPv6 nicht gelingen, das Internet der Dinge ist ohne IPv6 vollkommen undenkbar (siehe S. 50 „Bedingt lauffähig“).

Was ist jetzt zu unternehmen?

Schnell beginnen. Das ist das einzige, was wirklich hilft. Administratoren in den Unternehmen und Universitäten müssen Zeit und Material bekommen, damit sie Erfahrungen sammeln können. Gleichzeitig sollte die Geschäftsleitung eine Strategie erarbeiten, wie man mit IPv6 umgehen will. Der Einkauf bekommt die Anweisung, nur noch IPv6-fähige Hard- und Software zu beschaffen. Die Technik muss den Einkauf dabei unterstützen, denn die Hersteller und Anbieter von Waren und Dienstleistungen nennen IPv6 nur zu gerne in einem Nebensatz. Sie sagen einem Kunden IPv6 zu, ohne dass er auch nur ansatzweise erfährt, was er genau bekommt. In Ausschreibungen finden sich zum Teil viele Seiten zu IPv4 und gerade einmal eine Zeile wie „IPv6-Fähigkeit wird verlangt“. So ein Ungleichgewicht darf es nicht geben, IPv6 muss gleichberechtigt neben IPv4 stehen.

Kann man nach der Migration IPv4 weiterhin nutzen?

Das Wort „Migration“ beschreibt eine unumkehrbare Verlagerung von Punkt A nach Punkt B. Und genau das gilt für den Weg zu IPv6. Ziel kann und darf es nicht sein, den Parallelbetrieb von IPv4 und IPv6 lange aufrecht zu erhalten. Heute geht es leider nicht ohne. Der Parallelbetrieb wird einige Jahre andauern. Das bedeutet doppelte Arbeit bei der Netzwerkplanung und alle Sicherheitseinstellungen sind zweimal erforderlich. Das birgt Gefahren, denn der hektische Tagesbetrieb einer IT-Abteilung könnte die Administratoren der dafür notwendigen Zeit berauben. Heute neu angelegte Netzbereiche sollten direkt mit IPv6, ohne IPv4, geplant werden. Das vermeidet doppelte Arbeit – und es gibt wieder ein Migrationsprojekt weniger.

Und wenn ich trotz alledem noch etwas warte?

Das Internet ist an eine Wachstumsgrenze geraten, die es ohne den großen Adressraum von IPv6 nicht überwinden kann. Wer in der Welt des zukünftigen Internet kommunizieren oder Umsätze erzielen will, muss IPv6 beherrschen. Wer heute startet, gehört schon nicht mehr zu den ersten, die IPv6 einsetzen, aber auch nicht zu den letzten. Jedes Unternehmen muss sich fragen, ob die eigene Zukunft ohne IPv6 möglich ist. Das gilt für alle Branchen, nicht nur die IT.

In wenigen Jahren wird das Internet weitgehend auf IPv6 basieren. Es dürfte immer irgendwo auf der Welt noch IPv4 bleiben. Gerade in Unternehmensnetzen wird es viele Bereiche geben, die nicht in absehbarer Zeit umstellen können oder wollen. Wem nur IPv4 zur Verfügung steht, der muss in naher Zukunft mithilfe eines Gateways seine Daten von IPv4 auf IPv6 wandeln lassen (siehe S. 128 „Doppeldecker“). Die Provider werden sich das teuer bezahlen lassen, und so eine Lösung bleibt ein Provisorium. Ein Unternehmen sollte sich das sehr gut überlegen. Ignorieren geht nicht, IPv6 wird gebraucht, und je später man damit beginnt, desto hektischer und teurer gerät die Einführung des neuen Protokolls.

Hat IPv6 überhaupt Vorteile?

Natürlich hat IPv6 Vorteile. Der große Adressraum ermöglicht eine viel bessere Aufteilung von Netzwerken. Wo heute vielleicht 100 Rechner in einem Subnetz laufen, können die Verantwortlichen mit IPv6 eine feinere Unterteilung vornehmen (siehe S. 44 „Geordnete Vielfalt“). Sie können die Rechner der Mitarbeiter besser voneinander trennen. Und es wird möglich, eigenen Adressraum zu bekommen. So kann man selbst zwei Uplinks betreiben und ist nicht mehr darauf angewiesen, dass der Provider Adressen zur Verfügung stellt. Das Internet, und besonders das Internet der Dinge, wird unser Leben noch stärker als bisher durchdringen. Hier Kontrolle über seine Verbindung ins Internet zu bekommen und Abhängigkeiten zu reduzieren, ist in Zukunft unabdingbar.

Also, ran an IPv6! (un)

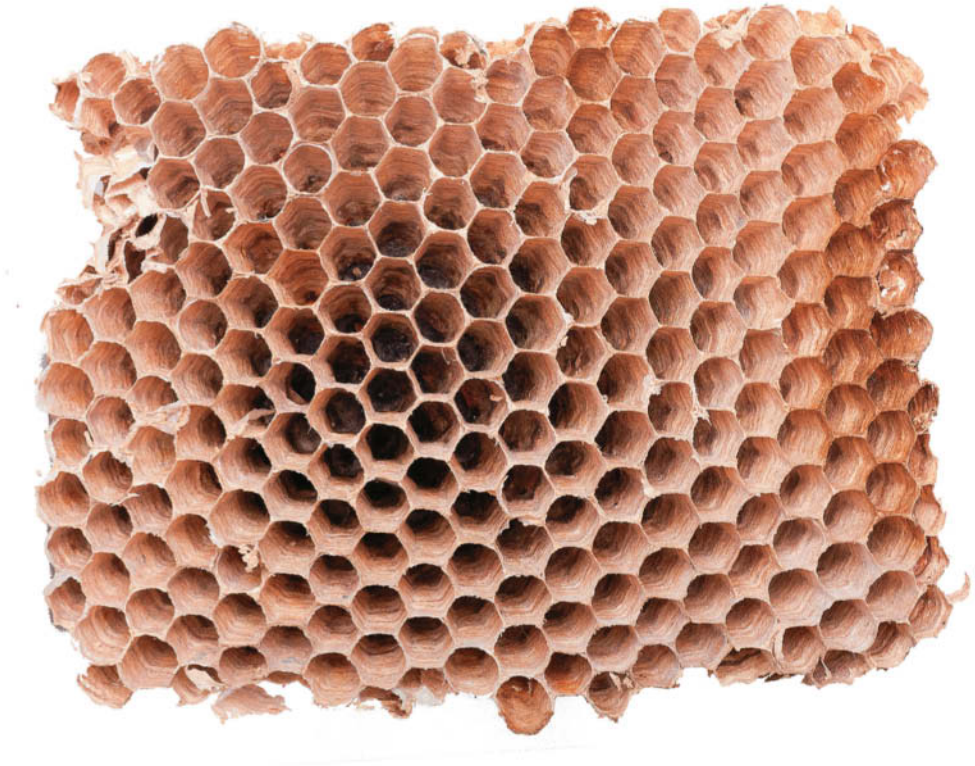
Wilhelm Boeddinghaus
hat als Leiter Netzwerk IPv6 bei der Strato AG eingeführt und dadurch viele Jahre praktische Erfahrung mit dem neuen Internet-Protokoll gesammelt. Er ist heute als selbstständiger Trainer und Berater für IPv6 und Netzwerke tätig.

Alle Links: www.ix.de/ix1316008

Basiswissen zum neuen Internet-Protokoll

Grundstruktur

Safuat Hamdy



Allmählich kommt IPv6 in Gang. Der Markt an Geräten und Angeboten wächst. Einige Provider bieten es bereits für Privatkunden an. Es hängt nun von der Professionalität und der Vorstellungskraft des jeweiligen IT-Managements ab, ob sich die Einführung als Meilenstein einer betrieblichen Entwicklung oder als Stolperstein am Abgrund erweist.

Ob IPv6 oder der Vorgänger IPv4: Die Aufgabe des Internet-Protokolls besteht im Wesentlichen darin, Datenpakete von einem System über verschiedene Netzwerke hinweg zu einem Zielsystem zu vermitteln. Ohne eine gültige IP-Adresse kann kein System Teil des Internet sein.

Die Aufzehrung des IPv4-Adressraumes im Jahr 2012, in dem die Internet Assigned Numbers Authority (IANA) den letzten /8-Block vergeben hat, gilt als wichtige Motivation, IPv6 einzuführen. Zwar verfügen die regionalen Internet-Registrierungsstellen noch über freie Adressblöcke, die jedoch in absehbarer Zeit vergeben sein werden. Es folgten eine Test- sowie eine Konsolidierungsphase, die ihren vorläufigen Abschluss etwa im Jahr 2011 hatte. Regelrechte Meilensteine sind die RFCs 6204 (IPv6 CE Router Requirements) sowie 6434 (IPv6 Node Requirements), außerdem RIPE-501 und dessen derzeit gültiger Nachfolger RIPE-554 (Requirements for IPv6 in ICT Equipment, [1]).

Davor galt IPv6 im Wesentlichen als Konstruktion aus dem Elfenbeinturm und Überlegungen zu einer Einführung als rein akademische Betrachtungen. Doch auch danach kam IPv6 nicht in Gang. Hersteller und Provider verwiesen einander auf fehlende Unterstützung in Produkten und fehlende Angebote von IPv6-Diensten.

Gleichzeitig wurde die Adressknappheit bei IPv4 jedoch immer offensichtlicher. Einige Provider und Hersteller haben bereits erkannt, dass die Auseinandersetzung mit IPv6 nicht nur unvermeidlich ist, sondern ihnen eine günstige Ausgangsposition auf einem neu entstehenden Markt verschafft. In der Folge nahm das Angebot an IPv6-fähigen Netzwerkgeräten, an IPv6-Anbindungen sowie an über IPv6 angebotenen Inhalten zu. Interessengruppen wie die Internet Society haben darüber hinaus 2011 den World IPv6 Day und 2012 den World IPv6 Launch Day veranstaltet. Der IPv6 Day war im Wesentlichen ein Awareness-Event, bei dem es um den Nachweis ging, dass IPv6 auf globaler Ebene einsatzbereit ist; hierzu haben die teilnehmenden Organisationen einen Tag lang ihre Dienste auch über IPv6 angeboten. Beim IPv6 Launch Day ging es darum, diese Angebote dauerhaft über IPv6 verfügbar zu machen.

Nun wächst der Markt an Geräten und Angeboten rund um IPv6 so schnell wie nie zuvor. In Fachkreisen herrscht Konsens darüber, dass eine unternehmensweite Umstellung auf IPv6 bezüglich des zu erwartenden Aufwands etwa mit der Euro-Einführung oder der Vorbereitung auf das Jahr-2000-Problem vergleichbar ist; ein Vergleich mit der Umstellung von Windows XP auf beispielsweise Windows 7 ist ebenfalls angemessen.

Datenpakete von IPv4 und IPv6 sind inkompatibel

Da der Aufbau der Datenpakete bei IPv6 vollkommen inkompatibel zu IPv4 ist und IPv6 einige neue Konzepte mitbringt, ist es in jedem Fall notwendig, vor einer Einführung ausreichend Fachkenntnis zu erwerben und Erfahrungen zu sammeln. Mit anderen Worten, die Hoffnung, IPv6 mit minimalem Aufwand etwa im Rahmen einer Wochenendaktion einzuführen, wird sehr wahrscheinlich an der Komplexität der Aufgabe zerschellen. Zur Erleichterung des Übergangs stehen zwar einige Mechanismen zur Verfügung, beispielsweise Dual-Stack-Betrieb, Tunnelung oder Protokollübersetzung, die in den folgenden Artikeln ausführlich beschrieben sind. Gerade wegen der damit einhergehenden Komplexität erfordert der Übergang ein Mindestmaß an Vorbereitung und Planung, was seinerseits eine gewisse Kenntnis und Erfahrung voraussetzt.

Gegenstand dieses Artikels sind die Grundfunktionen von IPv6. Es bringt reichlich neue Terminologie mit sich, zum Teil selbst für gestandene IPv4-Administratoren. Ein Glossar (siehe S. 135) erklärt alle relevanten Begriffe und Akronyme in Kurzform.

Neues Protokoll – neue Terminologie

Internet4 bezeichnet den Teil des Internet, der über IPv4 erreichbar ist; entsprechend umfasst **Internet6** alle per IPv6 angebundenen Geräte und Dienste. Gegenstand dieses Artikels ist IPv6, auf dessen Grundlage Netzwerk-Knoten (Nodes) Datenpakete miteinander austauschen. Die wichtigsten Begriffe finden sich im Folgenden – ein ausführliches Glossar ergänzt den vorliegenden Artikel im Anschluss.

Ein IP-Datenpaket besteht aus einem **Header** mit Steuerinformationen und – üblicherweise – einer **Nutzlast (Payload)**. Die Nutzlast wird vom Format des sogenannten **Upper Layer Protocol (ULP)** bestimmt, typischerweise handelt es sich dabei um ICMP oder ein Transportschicht-Protokoll wie TCP, UDP oder SCTP; im Fall von Tunnelung kann es sich um ein Netzwerkprotokoll wie IPv6 selbst oder IPv4 handeln.

Node: Gerät, das über ein oder mehrere Interfaces an ein oder mehrere Netzwerke angeschlossen ist.

Router Node, der Pakete weiterleitet, die nicht an ihn selbst gerichtet sind.

Host Node ohne Router-Eigenschaft

Über ein **Interface** findet ein Node Anschluss an ein Netzwerk (in IPv6-Terminologie auch als **Link** bezeichnet). Aus der Sicht eines spezifischen Node, der an einen Link angeschlossen ist, heißen alle weiteren Nodes, die an denselben Link angeschlossen sind, **on-link**; diese Nodes heißen auch **Nachbarn (Neighbors)**. Nodes, die nicht on-link und nur indirekt über wenigstens einen Router erreichbar sind, heißen **off-link**.

Netze und die daran angeschlossenen Nodes bilden eine **Site**, wenn sie einer gemeinsamen und zusammenhängenden Verwaltung unterstellt sind.

Grundlegende Eigenschaften von IPv6

Dieser Abschnitt stellt die Konzepte von IPv6 in Kurzform vor. Detaillierte Beschreibungen finden sich in den einschlägigen RFCs. Eine relativ aktuelle und breite Darstellung der IPv6-Konzepte findet sich bei Silvia Hagen [2] sowie beim NIST [3]; für Praktiker ist das Buch von Benedikt Stockebrand [4] von Nutzen.

IPv6 soll insbesondere diverse Komplikationen und Schwächen des Vorgängerprotokolls beseitigen.

Aufzehrung des Adressraums: Der offensichtlichste Mangel von IPv4 besteht in der Knappheit an global routbaren Unicast-Adressen, landläufig als öffentliche IP-Adressen bekannt. Diese Knappheit ist teilweise dem anfänglich kaum vorhersehbaren Wachstum des Internet und teilweise der unbedachten Vergabepraxis in den Anfangsjahren geschuldet, in denen großzügig Class-A- und -B-Netze vergeben wurden (in der heutigen Schreibweise /8 und /16, entsprechend der Zahl der Netzwerk-Bits). Viele dieser Zuweisungen haben sich im Nachhinein als nicht gerechtfertigt gezeigt. Die Architektur von IPv4 lässt keine einfachen Auswege aus dieser Situation zu: Eine Rückgabe ungenutzter Netzbereiche führt zu einer starken Fragmentierung des Adressraums (siehe unten). Ein Austausch großer gegen kleinere Netzblöcke führt zu signifikanten Ausfallzeiten, da die betroffenen Systeme neu adressiert (das heißt umnummeriert) werden müssen.

Dem steht eine zunehmende Zahl von Endgeräten gegenüber, die vernetzt werden sollen, angefangen von zahlreichen mobilen Geräten (Smartphones, Tablets und so weiter), einer wachsenden Nutzerbasis bis hin zum sprichwörtlichen Kühlschrank mit IP-Adresse und anderen integrierten Steuersystemen. Als Folge dessen sollte NAT den verbleibenden und immer knapper werdenden Adressraum besser auf ein stark wachsendes Internet verteilen:

Network Address Translation (NAT) ist ein Netzwerkmechanismus, der gemäß RFC 3489 IP-Adressen oder ganze Netzwerke – typischerweise private Netzwerke nach RFC 1918 – auf eine einzelne (global routbare) IP-Adresse abbildet. Meist sind Firewalls „nebenbei“ für NAT zuständig, was zu der (falschen) Annahme verleiten kann, dass es der Sicherheit dient.

Aus Sicht der Sicherheit hat NAT die interessante Eigenschaft, dass ein Angreifer den internen Zustand der NAT-Engine nicht kennt und daher nicht weiß, welche Ports zu welchen internen Systemen führen. Die Entscheidung darüber, eine Anfrage weiterzuleiten oder zu verwerfen, trifft jedoch streng genommen die Firewall und nicht die NAT-Engine. Das NAT-Gateway schreibt die Adressen in den IP-Headern um, bei der hier rele-

vanten Form in ausgehenden Paketen die Absender- auf die eigene IP-Adresse.

Bei eingehenden Paketen schreibt sie die Zieladresse auf eine Adresse im internen Netz um, entweder gemäß einer statisch konfigurierten oder einer dynamisch im Rahmen einer ausgehenden Verbindung eingerichteten Weiterleitung. Im letzteren Fall muss das NAT-Gateway Buchhaltung über die aktiven Verbindungen führen, wodurch das NAT-Gateway zum Flaschenhals oder gar zum Single Point of Failure werden kann.

Die Vor- und Nachteile von NAT diskutiert beispielsweise RFC 2993. Die sichtbarste Nebenwirkung von NAT ist das Aufgeben des Ende-zu-Ende-Prinzips. Eine weitere Nebenwirkung, die im praktischen Betrieb zu Schwierigkeiten führen kann, ist die Tatsache, dass die Adressen im IP-Header umgeschrieben werden. Dadurch scheitern Mechanismen wie IPsec, sobald die Integrität des IP-Headers überprüft wird. Auch Internet-Telefonie (VoIP) mit einer Signalisierung auf Grundlage von SIP oder H.323 schlägt an dieser Stelle zunächst fehl. Damit beispielsweise SIP unter diesen Bedingungen noch funktioniert, müssen zusätzliche Gateways die SIP-Pakete in geeigneter Weise modifizieren. Jede Hilfskonstruktion steigert jedoch die Komplexität und die Fehleranfälligkeit davon abhängiger Systeme und Anwendungen.

Andererseits sind die Systeme im per NAT abgebildeten Netzwerk von außen nicht mehr anhand der IP-Adresse voneinander zu unterscheiden, was einen gewissen Grad an Privatsphäre einbringt.

Aufgeblähte Routing-Tabellen als Flaschenhälse

Ein weiteres Problem, das den Anwendern meist verborgen bleibt, ist die starke Fragmentierung des IPv4-Adressraums. Auch dies ist der unbedachten Vergabe von IP-Adressblöcken in der Anfangszeit des Internet geschuldet und hat zur Folge, dass die Routing-Tabellen in der sogenannten Default-free Zone auf etwa 500 000 Einträge gewachsen sind. Für jedes einzelne Datenpaket und jedes Provider-Netz auf dem Weg vom Absender zum Empfänger muss der entsprechende Eintrag in der Routing-Tabelle wenigstens einmal ermittelt werden. Dieser Flaschenhals droht die Expansion des Internet mit einer rasant ansteigenden Zahl von angebundenen Geräten zu bremsen.

Daneben haben sich im Zuge der intensiven Nutzung von IPv4 weitere Schwächen und Verbesserungsmöglichkeiten herauskristallisiert, die sich nicht ohne Weiteres beheben oder umsetzen lassen. So hat sich Broadcast-Übertragung im Wesentlichen für Angreifer als interessant und nützlich erwiesen, während legitime Nutzungsmöglichkeiten selten sind. Multicast dagegen ist genau wie Dienstgüte (Quality of Service, QoS) in den Ansätzen stecken geblieben, und Mobile IP wurde für IPv4 zwar spezifiziert, doch die IPv4-Adressarchitektur verhindert einen praktikablen Einsatz.

Unterschiede zwischen IPv6 und IPv4

Bei IPv6 handelt es sich entsprechend den vielfältigen Vorgaben um weit mehr als nur IPv4 mit längeren Adressen; es bringt in vielen Punkten eine andere Architektur mit. Wer IPv6 sicher betreiben will, muss als Administrator auch in den Kategorien von IPv6 denken – viele Rezepte aus der IPv4-Welt taugen unter IPv6 nicht mehr. Das Folgende führt die wichtigsten Neuerungen von IPv6 auf.

Größerer Adressraum: Der wohl am deutlichsten sichtbare Unterschied zu IPv4 ist die Größe des IPv6-Adressraums. Mit 128 Bit erlaubt IPv6 die Adressierung von deutlich mehr Nodes und Sites, als dies bei IPv4 mit 32 Bit der Fall war.

Einfachere Adressstruktur: Unicast-Subnetze sind bei IPv6 grundsätzlich einheitlich groß, nämlich 64 Bit (/64); eine weitere Segmentierung dieser Subnetze sieht die Architektur von IPv6 nicht vor. Aufgrund der einfachen Adressstruktur brauchen Netzbetreiber und -Anwender keine Gedanken mehr an Netzmasken zu verschwenden.

Einfache Adresskonfiguration: IPv6 bietet neben einer manuellen Konfiguration oder einer Konfiguration über DHCPv6 mit der Stateless Address Autoconfiguration (SLAAC) einen weiteren Mechanismus zur Vergabe von IPv6-Adressen an. Er beruht darauf, dass die MAC-Adressen der an einem Link angeschlossenen Systeme eindeutig sein müssen. Darauf basiert die automatisch generierte IPv6-Adresse, die zumindest an dem betreffenden Link ebenfalls eindeutig ist. Der Vorteil besteht darin, dass der Node ohne großen Aufwand auf IP-Ebene kommunizieren kann, ohne dass Dienste wie DHCP zur Verfügung stehen müssen.

DHCPv6: Die altbewährte Adresszuweisung per Dynamic Host Configuration Protocol funktioniert weiterhin, sei es, um IPv6-Adressen wie bei IPv4 zu vergeben, sei es, um zusätzliche Konfigurationsinformationen zu verteilen, etwa die IP-Adresse eines DNS- oder NTP-Servers.

DNS: Das Domain Name System bildet IPv6-Adressen mit AAAA-Einträgen (Quad-A) ab; die „Rückwärtsauflösung" von IPv6-Adressen zu Namen erfolgt gemäß RFC 3596 mithilfe der Pseudo-Domain .IPv6.arpa.

Mehrere IPv6-Adressen pro Interface: Konzeptionsbedingt sieht IPv4 nur eine IP-Adresse pro Netzwerkanschluss vor. Diese Beschränkung lässt sich zwar in der Praxis über virtuelle Interfaces umgehen. IPv6 hebt die Beschränkung nicht nur auf, hier ist es sogar üblich, dass ein Interface mehrere IPv6-Adressen hat, nämlich wenigstens eine Link-Local-Adresse sowie eine oder mehrere andere Unicast-Adressen.

Einfachere Umnummerierung: Die Möglichkeit, einem einzelnen Interface mehrere IPv6-Adressen zuzuweisen und die vereinfachte Adressstruktur ermöglichen es, Netze bei Bedarf im laufenden Betrieb relativ einfach und ohne direkten Eingriff an den betroffenen Systemen umzunummerieren. Die entsprechende Funktion ist in ICMPv6 integriert.

Routenaggregation und effizientere Routing-Tabellen: Die Vergabestrategie für IPv6-Adressen stellt sicher, dass sich topologisch benachbarte Adressbereiche Routing-technisch zusammenfassen lassen. Das soll die Routing-Tabellen in der Default-free Zone trotz des enormen Adressraums übersichtlicher gestalten als bei IPv4. Dazu trägt bei, dass sich Netze im Vergleich zu IPv4 mit relativ wenig Aufwand umnummerieren lassen und dass die Vergabe sogenannter Provider-unabhängiger Adressen strikteren Regeln unterliegt als bei IPv4.

Schlankere Routing-Tabellen ermöglichen unter anderem ein schnelleres Routing, was beispielsweise auch die Dienstgüte begünstigt. Darüber hinaus sind Filterregeln viel einfacher zu gestalten. So erfordern länderspezifische Filterregeln mit IPv6 nur wenige Einträge im Vergleich zu IPv4, wo dies praktisch nur mithilfe nicht immer treffsicherer Geolocation-Dienste möglich ist (siehe zum Beispiel ipinfodb.com).

Einheitliches Steuerprotokoll ICMPv6: Im Rahmen von IPv6 erhielt der Nachfolger des Internet Control Message Protocol wesentliche Erweiterungen. Die Steuerfunktionen von ARP und RARP sowie von IGMP in Form von Neighbor Discovery und Inverse Neighbor Discovery sowie Multicast Listener Discovery

snom
VoIP phones

snom:startet:jetzt:IPv6

Individuelle & Professionelle
VoIP-Telefonie mit snom Endgeräten.

eindeutige:IP-:Adresse

NAT:nicht:mehr:notwendig

echte:Plug:and:Play:Umgebung

schnelles:Routing

jetzt:für:alle:snom:7xx:Telefone

Jetzt die neueste Beta-Firmware testen
unter: **www.snom.com/ipv6**

snom.com

sind in ICMPv6 integriert. Die entsprechenden Funktionen erhielten darüber hinaus Erweiterungen; neue Steuerfunktionen wie Router Discovery und Router Renumbering kamen hinzu.

Einfacheres Header-Format: Der IPv6-Header hat sich im Vergleich zum IPv4-Header vereinfacht. Am auffälligsten ist die feste Länge von 40 Byte. Informationen wie zur Fragmentierung, die Prüfsumme oder Optionen (das heißt Felder für optionale Informationen) sind keine Header-Bestandteile mehr. Auch das soll eine effizientere Verarbeitung in Routern ermöglichen und wiederum beispielsweise die Dienstgüte verbessern.

Extension Header: Optionen sind nicht länger direkt im Header, sondern in sogenannten Extension Headers untergebracht. Das beseitigt die von IPv4 her bekannten Größenbeschränkungen für Optionen: Solange das Datenpaket dafür Platz lässt, können Optionen im Prinzip deutlich länger und in beliebiger Zahl vorhanden sein. Darüber hinaus ermöglicht es die neue Architektur, auf einfache Weise neue Optionen einzuführen, ohne das Protokoll selbst zu verändern. Router werten Optionen nur noch selektiv aus, was einer effizienteren Verarbeitung zugute kommt.

Verbessertes Multicast und Abschaffung von Broadcast: Die Multicast-Funktionen sind in IPv6 stark ausgebaut und erweitert. Im Zuge dessen entfiel Broadcasting ganz; Broadcast-Übertragungen sind nun durch geeignetes Multicasting zu erbringen.

Fragmentierung nur an der Quelle: Anders als bei IPv4 zerlegen Router zu große Pakete nun nicht mehr. Stattdessen informieren sie den Absender des Pakets grundsätzlich per ICMPv6-Fehlermeldung, falls sich sein Paket in der gewünschten Größe nicht weiterleiten lässt. Auch dies dient einer effizienteren Verarbeitung an Routern.

Größere minimale MTU und Path MTU: Die minimal garantierte Maximum Transmission Unit stieg für IPv6 von 576 auf 1280 Byte. Das beschleunigt die Übertragung großer Datenmengen, da es den Protokoll-Overhead verringert. Da die Fragmentierung mit IPv6 nunmehr nur an der Quelle stattfindet, gewinnt die Feststellung der größten zulässigen MTU entlang der Route vom eigenen Node zum Ziel-Node (Path MTU) an Bedeutung.

Abschaffung von NAT: Der Hauptgrund für die Einrichtung von NAT bei IPv4 war die Knappheit an global routbaren Adressen. Der deutlich größere Adressraum von IPv6, die einfachere Adressstruktur sowie die strikteren Vergaberegeln für IPv6-Adressblöcke sollen sicherstellen, dass der ursprüngliche Grund für die Einführung des Provisoriums NAT entfällt. Dementsprechend war es für IPv6 zunächst überhaupt nicht vorgesehen, obwohl eine Adressumsetzung natürlich genau wie bei IPv4 machbar wäre. Die Diskussion über den Sinn von NAT ist noch nicht beendet. Der überwiegende Teil der IPv6-Community steht NAT jedenfalls skeptisch gegenüber. Darüber hinaus wirkt NAT – wenn auch marginal – zum Nachteil der Dienstgüte; die Abschaffung von NAT trägt also zur QoS-Verbesserung bei.

Mobile IPv6 (MIPv6): IPv6 bildet die Grundlage für das Roaming mobiler Geräte. Das Ziel ist es, zwischen verschiedenen Netzen umherwandern zu können, ohne dabei die Konnektivität auf IP-Ebene zu verlieren – selbst für bestehende Verbindungen, beispielsweise per TCP über IPv6. Aus Sicherheitssicht ist MIPv6 aufgrund des Risikos unautorisierter Umleitungen ausgesprochen heikel, und da es sich bei MIPv6 um ein relativ junges Arbeitsfeld handelt, kann es noch nicht als stabil gelten.

Quality of Service: Das bisher Erörterte wies bereits auf mehrere Verbesserungen in Bezug auf die Dienstgüte hin. Neben den genannten Architekturmerkmalen von IPv6, die nebenbei auch der QoS nützen, gibt es ein weiteres Merkmal, das gezielt deren Verbesserung anspricht, nämlich das sogenannte Flow Label. Dieses neue Feld im IPv6-Header kennzeichnet einen Datenfluss. Alle Pakete eines Flusses erfahren dieselbe Behandlung. Mit dem Flow Label entfällt die Angabe von (wiederholten) Optionen in den Paketen des Flusses, die die Router jeweils auswerten und verarbeiten müssten. Das Flow Label vereinfacht und beschleunigt somit im Prinzip Routing-Entscheidungen.

Ungewohnte Schreibweise von IPv6-Adressen

Die auffälligste sichtbare Neuerung von IPv6 gegenüber IPv4 ist die Länge und die Darstellung von IPv6-Adressen. Die Komplexität von IPv6-Adressen wirkt sich nicht zuletzt auf einige Sicherheitsaspekte aus. Mit 128 Bit sind sie viermal länger als IPv4-Adressen. Eine an die IPv4-Notation angelehnte Schreibweise von IPv6-Adressen würde demnach aus sechzehn durch Punkte getrennten Dezimalzahlen zwischen 0 und 255 bestehen. Sie wäre zu unhandlich. Eine IPv6-Adresse besteht stattdessen aus acht durch Doppelpunkte getrennten Gruppen zu je vier hexadezimalen Ziffern (RFC 4291). Ein Beispiel:

```
2001:0db8:0000:0000:0000:cafe:0000:0000
```

Führende Nullen in einer Vierergruppe darf man auslassen, Gruppen aus vier Nullen werden zu jeweils einer einzelnen Null zusammengefasst:

```
2001:db8:0:0:0:cafe:0:0
```

Zwei oder mehr aufeinanderfolgende Blöcke aus Nullen lassen sich als „:“ zusammenfassen. Damit die Zahl der ursprünglichen Nullen eindeutig bleibt, darf diese Notation jedoch höchstens einmal zum Einsatz kommen, im vorstehenden Beispiel also entweder so:

```
2001:db8::cafe:0:0
```

oder so:

```
2001:db8:0:0:cafe::
```

wobei die erste Darstellung mehr Platz spart als die zweite. Nicht erlaubt ist hingegen 2001:db8::cafe::, weil beispielsweise auch 2001:db8:0:0:cafe:0:0:0, also eine andere IP-Adresse, dieselbe Kurzdarstellung hätte.

Eine Besonderheit ergibt sich bei IPv6-Adressen mit eingebetteten IPv4-Adressen, deren letzte 32 Bit in der herkömmlichen „Dotted-Quad-Schreibweise“ von IPv4 angegeben werden dürfen. Die „IPv4-mapped-Adressen“ haben die Form :::ffff:192.0.2.1.

Die sogenannten IPv4-kompatiblen Adressen der Form :::192.0.2.1 sind seit RFC 4291 obsolet und sollten nicht verwendet werden. Sie tauchen bei veralteten Implementierungen aber gelegentlich noch auf.

Adresstypen für vielerlei Einsatzzwecke

Bei IPv6-Adressen unterscheidet man zwischen den Adresstypen Unicast-, Anycast- und Multicast-Adresse. Broadcast-Adressen, wie von IPv4 her bekannt, existieren bei IPv6 nicht. Dafür wurde Multicast besser ausgebaut. So wird die herkömmliche Funktion der Broadcast-Adresse von der Link-Local-All-Nodes-Multicast-Adresse ff02::1 übernommen. Grundsätzlich kann man diese Adresstypen folgendermaßen charakterisieren:

Unicast dient der Kommunikation zwischen zwei Interfaces. Jede Unicast-Adresse gehört zu genau einem Interface; eine Nachricht an eine Unicast-Adresse gelangt nur zum entsprechenden Interface. Global-Unicast-Adressen stammen derzeit