Einführung von IPv6 in Unternehmensnetzen – ein Leitfaden –

Wilhelm Boeddinghaus, Christoph Meinel, Harald Sack

Technische Berichte Nr. 52

des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam

Technische Berichte des Hasso-Plattner-Instituts für
Softwaresystemtechnik an der Universität Potsdam

Technische Berichte des Hasso-Plattner-Instituts für
Softwaresystemtechnik an der Universität Potsdam | 52

Wilhelm Boeddinghaus | Christoph Meinel | Harald Sack

Einführung von IPv6 in Unternehmensnetzen

Ein Leitfaden

Universitätsverlag Potsdam

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.de/ abrufbar.

STRATO AG
Dipl.-Inf. (FH) Wilhelm Boeddinghaus
Head of Network

Pascalstraße 10, 10587 Berlin
Tel. +49 (30) 39802-0 / Fax: -222
www.strato.de

Prof. Dr. Christoph Meinel
Dr. Harald Sack
Hasso-Plattner-Institut für Softwaresystemtechnik GmbH
Campus Griebnitzsee

Prof.-Dr.-Helmert-Straße 2-3, 14482 Potsdam
Tel. +49 (331) 5509-0 / Fax: -129
www.hpi-web.de

Universitätsverlag Potsdam 2011
http://info.ub.uni-potsdam.de/verlag.htm

Die Schriftenreihe **Technische Berichte des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam** wird herausgegeben von den Professoren des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam.

ISSN (print) 1613-5652
ISSN (online) 2191-1665

Online veröffentlicht auf dem Publikationsserver der Universität Potsdam
URL http://pub.ub.uni-potsdam.de/volltexte/2011/5458/
URN urn:nbn:de:kobv:517-opus-54582
http://nbn-resolving.de/urn:nbn:de:kobv:517-opus-54582

Zugleich gedruckt erschienen im Universitätsverlag Potsdam:
ISBN 978-3-86956-156-1

Inhaltsverzeichnis

1. Geschichte von IPv6

1990 startete die Internet Engineering Task Force (IETF) ein Projekt zur Entwicklung eines Nachfolgers für das Internetprotokoll IPv4, da bereits damals klar wurde, dass die IPv4 Adressen knapp werden mussten. Das Wachstum des Internet war hoch, und die Weltbevölkerung schon damals größer als 4,3 Mrd. Menschen. Es lag auf der Hand, dass nicht jedem Bewohner der Erde eine IP-Adresse zugeteilt werden konnte, geschweige denn mehr als eine.

Die Entwicklung von IPv6 wurde begonnen und 1998 wurde der erste Standard festgelegt. Wenn also heute über das „neue“ IP-Protokoll gesprochen wird, muss man sich klarmachen, dass die Entwicklung schon vor ca. 20 Jahren angestoßen worden ist.

Geplant war, dass die Unternehmen rechtzeitig und langsam IPv6 einführen und IPv4 aus den Netzwerken herausgenommen wird, bevor die Adressen knapp werden. Aber so ist es nicht gekommen. Mit Hilfe der Network Address Translation Technologie (NAT) wurde das Leben von IPv4 nur künstlich verlängert und an diesem Punkt ist das Internet heute.

Doch IPv6 wurde von den Kunden nicht verlangt und so sah die Industrie zunächst wenig Grund, IPv6 anzubieten. Wer zaghaft nachfragte, fand halbfertig entwickelte Produkte vor und musste sein IPv6-Projekt schnell wieder begraben. Das hat sich geändert; die Industrie ist nun in der Lage, IPv6-fähige Geräte in entsprechend guter Qualität zu liefern.

Inzwischen sind auch alle Routing-Protokolle für IPv6 verfügbar, so dass einem Einsatz nichts mehr im Wege steht. Zurzeit werden viele neue Technologien geschaffen, die den Übergang von IPv4 zu IPv6 erleichtern sollen.

Da viele Techniker IPv6 schon lange anpreisen, aber die Unternehmen die Notwendigkeit für eine Umstellung nicht gesehen haben, verhallten die Rufe. Und jetzt, da die IPv4-Adressen wirklich zur Neige gehen, will die Rufe kaum jemand mehr hören.

Obwohl IPv6 heute flächendeckend implementiert werden kann, fehlt es dem Protokoll bislang noch an großmaßstäblicher Einsatzerfahrung. Die Reife kommt auch erst mit der Zeit. Auch IPv4 ist ständig weiterentwickelt worden, sicherer und schneller geworden. Dies wird mit IPv6 auch geschehen, aber nur, wenn es tatsächlich auch benutzt wird. Da viele Unternehmen sich der frühzeitigen Erfahrung mit IPv6 verschlossen haben, muss das Versäumte jetzt nachgeholt werden.

2. IPv4 Adressmangel

Es gibt ca. 4,3 Milliarden IP-Adressen nach dem heutigen Standard IPv4. Das reicht zugegebenermaßen nicht für alle Menschen aus, aber einen Mangel sollte es demnach noch nicht geben. Wäre da nicht die sehr großzügige Vergabepraxis im vergangenen Jahrhundert, die sich zum Teil aus historischer Sicht erklären lässt.

Als das Protokoll am 1. Januar 1983 zeitgleich für das ganze Internet eingeführt wurde, war der Erfolg des Internets in seiner heutigen Form nicht abzusehen. Und so wurden vor allem in den USA Unternehmen und Universitäten, aber auch staatlichen Stellen wie dem Verteidigungsministerium, Adressebereiche zugewiesen, die aus heutiger Sicht viel zu groß waren. Diese Unternehmen und Organisationen nutzen nur einen Teil der Adressen, es gibt aber keine Handhabe, die ungenutzten Adressbereiche zurückzufordern. Und eine freiwillige Rückgabe ist selten, kommt aber vor.

IPv4-Adressen werden zentral von der Internet Assigned Numbers Authority (IANA, www.iana.org) verwaltet. Die IANA vergibt Netze, oder Blöcke von Adressen, an fünf Regional Internet Registries (RIR). Dies sind:

- ARIN American Registry for Internet Numbers
- RIPE Réseaux IP Européens
- APNIC Asia Pacific NIC
- LACNIC Latin American and Caribbean Internet Address registry
- AFRINIC Africa NIC

Die Blöcke besitzen einen Umfang von je 16.777.216 Adressen und es gibt 256 Stück davon. Die letzten fünf Blöcke wurden Anfang Februar 2011 an die RIRs vergeben, so dass der globale Pool der IANA nun leer ist. Die RIRs werden die letzen Adressen aus ihren Pools im Laufe des Jahres 2012 vergeben. Das ist eine Prognose, die für alle Regionen außerhalb Asiens gilt, da der Pool der freien Adressen in Asien seit April 2011 leer ist. Schon jetzt ist ein Ansturm auf die letzen freien IPv4-Adressen in den anderen Regionen der Welt abzusehen.

Was also tun? Die Lösung war und ist, dass nur neue Adressen in einem neuen Format Abhilfe schaffen können. Diese Erkenntnis hatte sich schon in den 1990er Jahren durchgesetzt, und so wurde IPv6 geschaffen. Die Entwicklung dauerte lange, aber jetzt ist IPv6 verfügbar. Und es gibt endlich genug Adressen für alle Menschen auf diesem Planeten. Wenn also heute behauptet wird, die Knappheit der IPv4-Adressen sei nicht bekannt oder sichtbar gewesen, so ist das nicht richtig. Und auch die Zeit zur Einführung von IPv6 war da, und ist immer noch vorhanden, aber die Unternehmen sollten bald beginnen.

Die Vergabe der IPv6-Adressen folgt den gleichen Wegen und ähnlichen Richtlinien wie die Vergabe von IPv4-Adressraum. Auch für IPv6 ist hier in Europa das RIPE mit Sitz in Amsterdam zuständig. Jedes Unternehmen bekommt über seinen Provider (Internet Service Provider, ISP) ausreichend Adressen. Im Gegensatz zu IPv4 besteht für IPv6 kein Mangel, sodass die Prüfung auf Bedarf relativ großzügig gehandhabt wird.

Rückgabe von Adressen

In der Theorie können IPv4-Adressen von den RIRs zurückgefordert werden. Dies geschieht regelmäßig, wenn Serviceprovider das ISP-Geschäft aufgeben oder Unternehmen in die Insolvenz gehen. Aber auch die zurückgeholten Adressen reichen nicht für lange Zeit und verschieben das Ende von IPv4 nur um wenige Monate.

Die Rückforderung von Adressen von großen Unternehmen ist noch komplizierter, da die Unternehmen die Adressen ja regulär zugewiesen bekommen haben, auch wenn sich die Regeln der Vergabe verändert haben. Die Unternehmen nutzen die Adressen auf vielfältige Weise und müssten die internen Netze umstellen, was mit einem hohen Aufwand verbunden wäre. Diese Quelle ist also verschlossen.

Es hat auch freiwillige Rückgaben gegeben, die den Unternehmen viel Lob und Zustimmung eingebracht haben. Aber seit Microsoft 11,25 US-Dollar je IPv4-Adresse gezahlt hat[1], haben alle Unternehmen den Wert ihrer Adressblöcke erkannt und würden wohl eher einen Verkauf denn die freiwillige Rückgabe anstreben.

Auswirkungen des IPv4-Adressmangels

Es gibt viele Auswirkungen des IPv4-Adressmangels. Einige sind offensichtlich, andere eher versteckt. Aber gerade die versteckten Auswirkungen können ein Unternehmen umso stärker und unerwarteter treffen. Nicht jedes Unternehmen ist von allen Auswirkungen gleichstark betroffen, aber die Sorgfalt gebietet es, dass alle möglichen Probleme beleuchtet und bewertet werden. Diesen Prozess in Gang zu setzen, ist Aufgabe der Geschäftsleitung und macht aus der vermeintlich rein technischen IPv6-Einführung eine strategische Fragestellung für das Unternehmen.

Carrier Grade NAT

Carrier Grade Network Address Translation (CGN) nennt man die mehrfache Umschreibung einer IPv4 Adresse in einem Datenpaket.

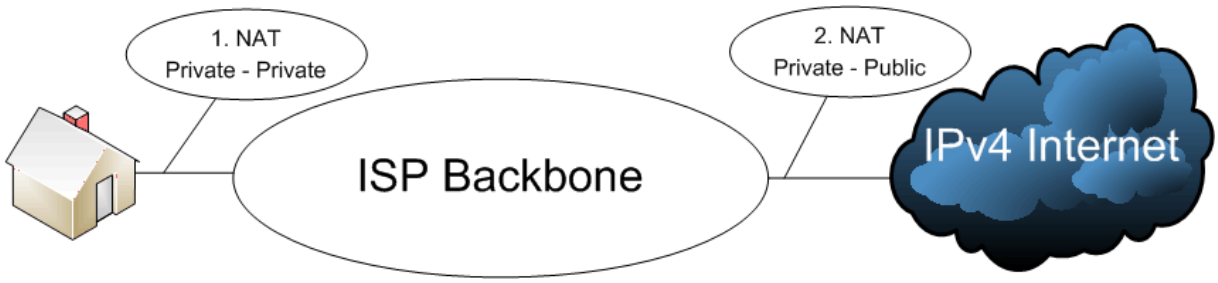

Abbildung 1:Carrier Grade NAT

In fast allen Netzwerken, seien es Heimnetzwerke oder Unternehmensnetzwerke, wird an dem Router, an den die Internetverbindung angeschlossen ist, von privaten IPv4-Adressen auf eine öffentliche IPv4-Adresse „umgeschrieben“. Somit teilen sich alle Rechner im Netzwerk eine öffentliche Adresse. Bei einem Unternehmen wird NAT oft nicht nur auf einer Adresse gemacht, sondern auf einem kleinen Block von Adressen. Damit müssen sich nicht alle Mitarbeiter eine Adresse teilen. Auch besteht

[1] Nortel verkauft eigene IPv4-Adressen an Microsoft, heise news ticker, 24.03.2011, http://www.heise.de/newsticker/meldung/Nortel-verkauft-eigene-IPv4-Adressen-an-Microsoft-1214670.html

so die Möglichkeit, dass Dienste von außen zugänglich gemacht werden. Dabei wird die Umschreibung der IPv4-Adresse in die andere Richtung vorgenommen.

Carrier Grade NAT betrifft vor allem die Kunden, die nur eine öffentlich IPv4-Adresse zugewiesen bekommen. Wenn im Provider-Netzwerk ein weiteres Mal NAT konfiguriert ist, teilen sich mehrere Kunden eine öffentlich IPV4-Adresse. Das spart dem Provider viele Adressen, bringt aber Probleme, vor allem für den Endkunden, mit sich.

Kosten

Die Provider können Carrier Grade NAT nur mit Hilfe spezieller und teurer Hardware realisieren. Dafür werden in Einschübe von großen Routern Karten eingesetzt, die NAT in Hardware abbilden und genug Speicher haben, um für viele tausend Kunden über alle Verbindungen Protokoll zu führen. Denn nur wenn die Karte alle NAT Status vorhält, kann ein Antwortpaket wieder umgeschrieben werden[2].

Diese spezielle Hardware ist sehr teuer, je Router müssen schnell einige hunderttausend Euro investiert werden. Wer trägt die Kosten? Schon heute ist das Geschäft mit DSL-Anschlüssen für Endkunden eher margenschwach, so dass die Kosten für die Extra-Hardware nicht finanziert werden können. Die Provider werden versuchen, über Preiserhöhungen das Geld wieder zu verdienen oder werden anbieten, dass gegen Aufpreis die Datenpakete nicht durch die NAT Gateways geschleust werden. Dann würde in Zukunft für eine selbstverständliche Leistung, die im heute Preis enthalten ist, ein Aufpreis fällig. Wie die Kunden reagieren werden, ist absehbar.

Diejenigen Provider, welchedie teure NAT-Hardware anschaffen, wollen und werden die Hardware mindestens über den Abschreibungszeitraum von ca. 5 Jahren nutzen wollen. Das könnte die schnelle Einführung von IPv6 zusätzlich behindern.

Geo IP

Bei IPv4 sind alle weltweit genutzten Adressen in Datenbanken verzeichnet und einer Region oder Stadt zugeordnet. So können die Betreiber von Websites genau feststellen, woher der Besucher kommt und können entweder regionale Inhalte oder regionale Werbung platzieren.

Wenn CGN zum Einsatz kommt, wird erst durch ein zweites NAT im Backbone des ISPs die Adresse des Kunden in eine öffentliche IPv4-Adresse umgeschrieben. Wenn das die Zuordnung der IPv4-Adresse zu einer Stadt oder Region verändert, können keine regionalen Inhalte mehr gezielt ausgeliefert werden. Regionale Werbung funktioniert ebenfalls nicht mehr. Die Werbeplatzanbieter sowie die Inserenten und Agenturen, die Werbung vermitteln und erstellen, werden Umsatzeinbußen hinnehmen müssen.

Zugriff auf das Heimnetzwerk

Viele Internetnutzer greifen heute wie selbstverständlich aus aller Welt auf das Heimnetzwerk zu. Die öffentliche Adresse, die der Provider dem Heimrouter zur Verfügung stellt, wird zwar täglich gewechselt, aber es gibt Dienstleister wie z.B. DynDNS, die bei jedem Wechsel der Adresse einen Datenbankeintrag pflegen, welcher der wechselnden IPv4-Adresse einen festen Namen zuordnet.

[2] Die gleiche Funktion wird vom Heimrouter wahrgenommen, auch hier müssen die Verbindungen in Tabellen vorgehalten werden. Da der Heimrouter aber nur wenige Nutzer bedienen muss, kann die Umschreibung in Software geschehen und ist daher preiswert zu realisieren.

Wenn nun aufgrund von Carrier Grade NAT sich viele Kunden eine öffentliche IPv4 Adresse teilen, schlägt die Zuordnung fehl. Der Zugriff auf das Heimnetzwerk ist nicht mehr möglich. Zusätzlich wüsste der ISP auch nicht, welchem der vielen Kunden, die sich diese eine Adresse teilen, er einen Zugriff von außen zuteilen müsste.

Ohne Zugriff aufs Heimnetzwerk ist die Musiksammlung oder aber die Haussteuerung nicht mehr zugänglich. Viele Kunden haben sich an den Komfort eines solchen Zugriffes gewöhnt und werden den Verlust nicht ohne Protest hinnehmen.

Weitere gute Gründe für den Zugriff auf das Heimnetzwerk sind Heimautomatisierung, also die Steuerung der Infrastruktur des Hauses, und Hilfestellung von außen bei Computerproblemen.

Protokolle

Einige anwendungsbezogene Protokolle nutzen mehr als eine einzelne Verbindung für die Übertragung von Daten im Internet. Diese Protokolle können eventuell mit CGN nicht arbeiten und fallen daher aus. Besonders betroffen sind Voice-over-IP Protokolle, die für die Telefonie oder Videoübertragung benötigt werden.

Adresshandel

Wenn keine IPv4-Adressen mehr aus den herkömmlichen Quellen zu beziehen sind, wie es in Asien schon der Fall ist, kann der Kauf von IPv4-Adressen eine Option sein. Aber halt - wem gehören die Adressen eigentlich? Ganz geklärt ist die Eigentumsfrage nicht, und so ist es nicht klar, ob ein Käufer Eigentum an IPv4-Adressen erlangen kann. Und es ist genauso unklar, ob der Verkäufer überhaupt verkaufen kann.

Die RIRs erlauben die Übertragung von Adressen, mindestens innerhalb der jeweiligen RIR-Region. Der Käufer muss den Bedarf an Adressen nachweisen. Dabei gelten die gleichen Regeln wie bei der regulären Vergabe aus den RIR-Pools. Für die RIRs wichtig ist die Dokumentation der IPv4-Adressen in den RIR-Datenbanken, da aus diesen Datenbanken Filterlisten in Routern erzeugt werden. Wenn die Netze nicht korrekt in den Datenbanken stehen, ist eine Kommunikation mit diesen Adressen im Internet nahezu unmöglich, da die Provider nur Netzwerke transportieren, die in den Datenbanken der RIRs dokumentiert sind.

Quellen

Wenn die Preise hoch genug sind, werden Unternehmen bereit sein, IPv4-Adressen abzugeben. Dabei ist zu beachten, dass nur solche Adressen verkauft werden können, die unabhängig vom Provider sind (PI, Provider Independent). IPv4-Nummern, die vom Provider an ein Unternehmen zur Nutzung überlassen wurden, sind dem Provider zugeordnet und bleiben das auch.

Ob es zu Unternehmensübernahmen wegen IPv4-Adressen kommt, bleibt abzuwarten. Es ist sicher ein Zeichen von Verzweiflung, wenn ein Unternehmen nur wegen der IPv4-Adressen gekauft wird. Aber bei Insolvenzen von Providern könnte es wie im Fall von Nortel durchaus zu solchen Käufen kommen. Die Insolvenzverwalter werden aber schnell merken, dass die IPv4-Adressen ein teuer verkaufbares Gut sind.

Kosten

Die Kosten für die IPv4-Adressen sind schwer zu ermitteln. Microsoft hat aus der Insolvenz von Nortel IPv4-Adressen zum Stückpreis von 11,25 US-Dollar erworben. Dieser Preis kann als Richtwert dienen.

Wenn alle RIRs die Pools an IPv4-Adressen vollständig ausgeschöpft haben werden, könnte der Preis noch steigen. Tabelle 1 rechnet mit 11,25 US-Dollar pro IPv4 Adresse.

Tabelle 1: Erlöse aus dem Verkauf von IPv4 Adressen

Adressen	US-Dollar
256	2.880,00
512	5.760,00
1024	11.520,00
4096	46.080,00
8192	92.160,00

Unternehmen, die dann von den Providern noch neue IPv4-Adressen erbitten, werden ganz sicher dafür zahlen müssen, denn die Provider wollen das investierte Geld wieder zurückverdienen.

Kunden und Provider haben die Kosten für IPv4-Adressen heute nicht in den Kalkulationen ihrer Produkte eingerechnet. Entweder werden also die Margen sinken oder die Preise zwangsläufig steigen müssen.

Der Käufer von Adressen muss berücksichtigen, dass gekaufte Adressen eventuell als Anlagegut zu betrachten sind. Da dies bisher nicht vorgekommen ist, muss die Reaktion der Finanzbehörden auf den Vorgang abgewartet werden.

Da es im Falle von IPv6 ausreichend viele Adressen gibt, können diese Adressen auf absehbare Zeit kein knappes Gut werden und somit Kosten verursachen. Die Provider zahlen nichts für die IPv6-Adressen, daher sollte es auch keine Weiterberechnung geben.

Kommunikation des Unternehmens

Die Kommunikation des Unternehmens nach innen und außen hat heute strategische Bedeutung. Daher sollte jede Geschäftsleitung genau analysieren, wann, wo und mit wem über welche Kanäle Daten und Nachrichten ausgetauscht werden. Dieser Aspekt macht aus dem vorgeblich technischen Thema IPv6 ein strategisches, das nicht von der IT-Abteilung alleine gelöst werden kann. Wenn die Außenwelt Probleme hat, das Unternehmen zu erreichen, drohen Verluste an Umsatz und Marktanteil.

Mitarbeiter

Der erste betroffene Mitarbeiter, der ohne IPv6 Probleme bekommt, könnte ausgerechnet der Geschäftsführer sein. Auf einer Asienreise möchte er vom Hotel aus auf das heimische Netzwerk zugreifen, das Hotel kann aber keine IPv4-Adressen mehr zur Verfügung stellen. Somit ist ein Zugriff nicht möglich. Aber genauso könnte die Kommunikation zwischen Niederlassungen gestört oder unmöglich werden.

Eine mehrfache Adressenumsetzung stört zudem die Internettelefonie nach dem VoIP-Protokoll. Ein Mitarbeiter im Homeoffice könnte also von der Telefonie abgeschnitten sein (siehe oben).

Kunden

Was passiert, wenn ein Kunde eine E-Mail senden möchte oder ein Produkt im Onlineshop erwerben möchte, aber nur IPv6 als Protokoll hat? Wahrscheinlich scheitert seine Bestellung oder seine Anfra-

ge. Vielleicht hat ein Provider auf dem Weg zwischen Kunde und dem Webshop ein Gateway, einen Protokollübersetzer, aufgestellt und kann zwischen IPv6 und IPv4 übersetzen. Wenn nicht, ist die Kommunikation mit dem Kunden gestört und der Kunde wird sich dem Mitbewerber zuwenden.

Selbst wenn es ein Gateway gibt, gehen Informationen verloren, da die Protokolle IPv4 und IPv6 nicht vollständig gleich aufgebaut sind.

Lieferanten

Auch die Kommunikation mit den Lieferanten sollte beide Protokolle beherrschen. Niemand will erst im Notfall die Kommunikation mit IPv6 aufbauen, wenn dringend Hilfe des Lieferanten erforderlich ist. Und eine Bestellung auslösen zu können, um nicht selber in Lieferschwierigkeiten zu kommen, kann ebenfalls sehr wichtig sein. Da in Asien keine neuen IPv4-Adressen mehr vergeben werden können, sind besonders Kunden von asiatischen Lieferanten auf IPv6 angewiesen, um die Bestellkette nicht zu gefährden.

Neue Geschäftsfelder

Wer hätte vor 20 Jahren Google, Twitter oder Facebook für möglich gehalten? Wohl kaum jemand. Und trotzdem sind diese Unternehmen heute Milliarden schwer und mächtig. Bisher hat noch jede neue Technologie neue Ideen und Unternehmen hervorgebracht. Und mit den neuen Unternehmen sind auch immer neue Vermögen geschaffen worden.

Jedes der neuen Unternehmen erzeugt ein Umfeld, in dem andere Unternehmen gedeihen. Bei Google kann jedermann mit Anzeigen Geld verdienen, und die Firma Zynga betreibt Onlinespiele bei Facebook mit großem Erfolg.

So ist zu erwarten, dass sich auch aus der fast unendlichen Fülle von IPv6-Adressen neue Ideen und Geschäftsmodelle ergeben. Welche? Wenn ich das wüsste. Aber Unternehmen und Unternehmer, die sich dem Trend zu IPv6 verschließen, werden weder diese Ideen selber entwickeln noch im Umfeld solcher Ideen gedeihen können. Eine frühzeitige Beschäftigung mit dem Thema IPv6 eröffnet Chancen, die anderen Unternehmen verschlossen bleiben.

3. Vorteile von IPv6

Welche Vorteile hat ein Unternehmen von der Einführung von IPv6? Die Frage steht natürlich am Anfang aller Betrachtungen und die Antwort entscheidet, ob ein Unternehmen in IPv6 investiert oder nicht. Um es vorweg zu nehmen: Die „Killerapplikation“, die eine Einführung von IPv6 zwingend notwendig macht, gibt es nicht. Man hat zwar lange danach gesucht und auch skurrile Vorschläge diskutiert, aber am Ende hat man die „Killerapplikation“ nicht finden können. Aber natürlich hat die Einführung von IPv6 Vorteile, die ein Unternehmen sich zu Nutze machen kann.

Mehr Adressen

Der wichtigste Vorteil von IPv6 gegenüber IPv4 ist die große Menge an IP-Adressen, die das Protokoll bereitstellt. Somit ist der Adressknappheit für die nächsten Jahrzehnte vorgebeugt.

Reichen die IPv6-Adressen jetzt auch für alle Zeiten aus? Die Antwort lautet: vielleicht.

Auch der Adressraum von IPv6 ist endlich, aber so groß, dass wir uns heute nicht vorstellen können, dass er vollständig aufgebraucht wird. Aber es konnte sich in den 1970er Jahren auch kein Mensch vorstellen, dass ca. 4.300.000.000 Adressen einmal zu einer knappen Ressource werden könnten. Es ist also Vorsicht geboten, wenn der Adressraum von IPv6 als nahezu unendlich groß beschrieben wird.

Für die heutigen Anwendungen des Internets ist der Adressraum von IPv6 ausreichend groß, und alle Unternehmen, die IPv6 einsetzen wollen, erhalten für die heutigen Netze und die drauf laufenden Applikationen mehr als ausreichend viele Adressen.

Da die Provider relativ leicht neue IPv6-Adressen bekommen, können die sie ihren Kunden auch leicht viele Adressen zuteilen. Es sollte also kein Mangel herrschen, und wenn doch, dann ist der Mangel zum jetzigen Zeitpunkt künstlich erzeugt. Da IPv6 keine knappe Ressource ist, darf den Gesetzen des Marktes folgend auch der Preis für IPv6-Adressen nicht hoch sein. Die RIRs zumindest vergeben IPv6 zu einem sehr kleinen Preis, wenn nicht sogar kostenfrei.

Direkte Kommunikation

Wenn zwei Menschen, Rechner oder Applikationen kommunizieren wollen, aber beide Partner keine öffentlichen IP-Adressen haben, ist es nicht möglich, eine direkte Kommunikation aufzubauen. Man nennt diese Situation „Bruch des Ende-zu-Ende-Modells“. Es wird ein vermittelnder Rechner irgendwo im Netzwerk benötigt, der die Verbindung herstellt und aufrecht erhält. Wo dieser Rechner steht, wer ihn betreut und wie verlässlich der Service ist, unterliegt nicht der Kontrolle des Anwenders.

Eine typische Anwendung ist ein Telefonat oder eine Videokonferenz, die über einen frei verfügbaren Dienst geführt werden soll. Niemand garantiert die Vertraulich der Daten. Selbst wenn die jeweilige Verbindung zwischen Anwender und zentralem Server verschlüsselt ist, ist noch keine Ende-zu-Ende-Verschlüsselung garantiert. Auf dem zentralen Server lassen sich die Daten leicht mitschneiden und abhören.

Bei IPv6 ist der Mangel an Adressen aufgehoben. Alle Teilnehmer können ohne Network Address Translation (NAT) mit öffentlichen Adressen arbeiten. Und mit einer guten Firewall ist das auch kein Sicherheitsproblem.

Die direkte Kommunikation macht eine Verschlüsselung der Daten unter der vollen Kontrolle des Anwenders erst möglich. Und wenn der sonst notwendige vermittelnde Server im Ausland steht, bringt eine direkte Verbindung oft zusätzlich noch einen Geschwindigkeitsvorteil, da die Paketlaufzeiten geringer sind.

Internet der Dinge

Das Internet der Benutzer wird künftig in wachsendem Maße zum Internet der Dinge werden. Immer mehr Geräte werden an das Internet angeschlossen, um Informationen auszutauschen. Ob der Mensch dabei Teil dieser Kommunikation ist, kann bezweifelt werden. Aber sie sollte immer zum Nutzen des Menschen sein.

Verkehr

Autos, die mit der Umwelt kommunizieren, sind schon heute Realität. Meist allerdings ist das Auto reiner Empfänger von Informationen. So werden über das Radio und das Navigationsgerät Staus und Unfälle gemeldet, die der Fahrer dann umfahren kann. Aber auch das Auto selber könnte Informationen über die aktuelle Verkehrssituation liefern. Das Auto im Stau kann seine durchschnittliche Geschwindigkeit melden und damit die Vorhersage über Staulänge und Staudauer verbessern.

Ob die Kommunikation mit anderen Autos hergestellt wird, oder mit Sensoren am Straßenrand, wird sicher von Anwendung zu Anwendung verschieden sein. So oder so wird das Auto Informationen geben und nehmen. Auch eine Kommunikation mit der Werkstatt ist denkbar, damit Defekte frühzeitig gemeldet werden können und dem Fahrer der Werkstattbesuch empfohlen werden kann.

Am Straßenrand stehen Laternen, die über Kabelkanäle miteinander verbunden sind, an das Stromnetz angeschlossen sind und Netzwerkkomponenten aufnehmen können. Somit sind die Masten ideal für einen Netzausbau geeignet. Allerdings könnte, da der Abstand der Masten zueinander bekannt ist, auch die Einhaltung der Höchstgeschwindigkeit überwacht werden.

Neben den reinen Informationen können natürlich auch Filme oder interaktive Inhalte ins Auto übertragen werden, wenn die Passagiere es wünschen. Und wer kennt nicht die langen Fahrten mit Kindern?

Werbung

Laternenmasten als Standorte für Netzwerkgeräte können nicht nur für Fahrzeuge, sondern auch für Fußgänger mit Smartphones genutzt werden. Die relativ preiswerte WLAN-Technologie (im Gegensatz zu Mobilfunk) würde eine flächendeckende Installation ermöglichen. Das Smartphone könnte dann mit lokalen Informationen versorgt werden und es werden neue Werbemärkte entstehen. Alle diese Anwendungen benötigen viele Adressen und direkte Kommunikation. Beides ist mir IPv6 machbar.

Maschinenüberwachung

Wenn Maschinen, im besonderen Verkehrsmittel, mit IPv6 ausgestattet werden können, sind Werte immer und schnell abrufbar. So könnte jedes Rad, jedes Ventil und jede Tür im Zug abgefragt werden. Ähnliches gilt auch für Flugzeuge. Es gäbe einen einfachen und standardisierten Weg, Daten zu bekommen, der weltweit leicht gegangen werden kann. Internet ist fast überall verfügbar.

Heimvernetzung

Sind Fenster und Türen geschlossen? Ist der Herd ausgeschaltet, das Bügeleisen auf Null gestellt? Wie warm ist das Wasser im Wasserspeicher? Welche Leistung bringen die Solarkollektoren aktuell? Wie hoch ist die Raumtemperatur?

Nur wenn das Haus mit Sensoren ausgestattet ist, können Fragen dieser Art beantwortet werden. Und nur, wenn die Sensoren und Steuerungen von überall erreichbar sind, kann das Haus aus dem Urlaub, also von jedem Punkt der Welt, gesteuert und kontrolliert werden. Das gilt natürlich auch für den Videorecorder, der programmiert werden soll oder die Warmwasserbereitung, die auf dem Weg nach Hause angeschaltet werden muss, damit das Bad am Abend nicht kalt ist.

In Zukunft wird vielleicht das Haus die Verkehrsmeldungen abrufen, damit der Wecker früher als geplant schellt, weil auf dem Weg zur Arbeit ein langer Stau gemeldet wird. Und natürlich wird auch die Kaffeemaschine frühzeitig angeschaltet. Oder man wird später geweckt, weil sich ein Meeting verschoben hat.

Ohne IPv6 und direkte Kommunikation können solche Szenarien nicht Wirklichkeit werden. Theoretisch ist das auch mit IPv4 möglich, aber niemand hat ausreichend viele Adressen dafür. Und Techniken wie Carrier Grade NAT machen den Zugriff auf das Heimnetzwerk unmöglich.

Smart Metering

Moderne Energienetze sind auf ständigen Datenfluss angewiesen. In der Zukunft sollen alle Stromzähler von außen abgefragt werden können. Das dient nicht nur der Abrechnung, sondern auch der Prognose über den Stromverbrauch. So können Kraftwerkskapazitäten besser geplant werden und es kann Energie gespart werden.

Die Zusammenschaltung von lokalen Blockheizkraftwerken, die in Wohnanlagen betrieben werden, zu einem virtuellen großen Kraftwerk ist heute schon Realität, wird aber noch über Mobilfunk gesteuert. Mit IPv6 könnte auch hier die preiswerte Internettechnik genutzt werden. So wird es möglich, auf Lastspitzen im Stromnetz schnell zu reagieren, weil die vielen kleinen Kraftwerke viel spontaner hoch- und wieder heruntergefahren werden können, als es mit Großkraftwerken überhaupt möglich ist.

Für eine flächendeckende Vernetzung der Stromnetze mit IPv4 fehlen heute die IP-Adressen, hier kann nur IPv6 zum Einsatz kommen.

Sensornetze

Die Wissenschaft betreibt zum Teil großflächige Sensornetzwerke, die mit IPv6 adressiert werden können. Die Sensoren werden genutzt, um Vulkane zu überwachen oder am Meeresgrund Temperatur und Strömung zu messen. Gerade bei der Überwachung von Vulkanen kommt es auf viele Messwerte an, die ständig von zentralen Forschungseinrichtungen abgefragt werden müssen. Eine konsequente Adressierung mit IPv6 macht die Abfrage von weltweit verteilten Stellen aus möglich. So können Ergebnisse an vielen Orten errechnet werden und die Vorhersage von Erdbeben oder Vulkanausbrüchen kann hoffentlich zum Wohle der Menschen verbessert werden.

Dabei ist jeder Sensor ein kleiner Server, der weltweit erreichbar ist. Es ist sicher notwendig, den Zugriff zu schützen, so dass nur Forschungseinrichtungen Zugriff haben, aber es muss keine zentrale Datenbank vorgehalten werden, welche die Werte der Sensoren aufnimmt, denn alle Interessenten

können die Rohdaten abfragen und dann selber verarbeiten. IPv6 als standardisiertes Protokoll macht den Zugriff auf die Sensordaten leicht und preiswert.

Landwirtschaft

Landwirten ermöglichen die vielen Adressen eine auf IPv6 basierende Überwachung von Viehherden. Jedes Tier „meldet“ eigenständig Daten über Bewegung, Standort und Gesundheitszustand. So kann der Landwirt leichter auf Notfälle reagieren und hat Daten für Statistiken und den Tierarzt.

Zukunft

Das Internet der Zukunft kann nur weiter wachsen, wenn genug Adressen zur Verfügung stehen. Welche neuen Anwendungen entstehen werden, ist im Moment nur schwerlich abzusehen. Aber bisher ist noch jede neue Technik von findigen Unternehmern genutzt worden. Es ist daher nicht klug, sich von diesen Entwicklungen abzuschneiden, nur weil das Unternehmen sich neuen Techniken verschließt.

Schon die oben skizzierten Anwendungsszenarien bieten viele gute Entwicklungsmöglichkeiten für Unternehmen. Aber wie immer werden noch mehr Ideen gesucht und sicher auch gefunden werden.

4. Woher bekommt mein Unternehmen die IP-Adressen?

IP-Adressen müssen eindeutig sein, um eine direkte Kommunikation zwischen zwei Computern oder Endgeräten zu ermöglichen. Ähnlich einer Telefonnummer (Landeskennzahl + Ortskennzahl + Teilnehmeranschluss) würde es bei doppelt genutzten Nummern zu Verwechslungen kommen. Das kommt bei IPv4 sehr häufig vor, wenn private Adressen genutzt werden, die vom Router mit Hilfe von NAT in öffentliche Adressen übersetzt werden müssen.

Private Adressen

Im Protokoll IPv4 hat man im RFC 1918 drei Adressbereiche festgelegt, die jedes Netzwerk, jede Organisation und jedes Unternehmen intern nutzen kann (vgl. Tabelle 2). Diese Netzbereiche werden im Internet nicht weitervermittelt. Sollte doch ein Datenpaket mit einer IP-Adresse aus diesem Adressbereich im globalen Internet auftauchen, verwerfen die meisten Provider dieses Paket. Wenn ein Netzwerk diese Adressen nutzt, was oft geschieht, muss an der Netzwerkgrenze eine Umsetzung der privaten Adressen in eine oder mehrere nicht private Adressen erfolgen. Diesen Vorgang nennt man NAT (Network Address Translation). Dabei werden die privaten Adressen hinter der öffentlichen Adresse versteckt, was von vielen Netzbetreibern als notwendige Sicherheitsmaßnahme gesehen wird. Die Sicherheit ist trügerisch, aber dazu mehr in einem späteren Kapitel.

Tabelle 2: Private IPv4-Adressbereiche nach RFC 1918

RFC 1918 Adressen
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

IPv6 sieht keinen Bereich für private Adressen mehr vor, das Konzept wurde als überholt wieder verworfen. Heute sollen die Rechner, auch in den Büros, mit öffentlichen Adressen ausgestattet werden, um Ende zu Ende ohne Umschreibung von Adressen kommunizieren zu können.

Organisationen

IP-Adressen, sowohl nach dem Protokoll IPv4 als auch nach IPv6, werden zentral von der IANA (Internet Assigned Numbers Authority) weltweit vergeben. Damit nicht jeder Provider zentral anfragen muss, vergibt die IANA die Adressen an fünf RIRs (Regional Internet Registries). Die RIRs sind der Ansprechpartner für die Provider, die wiederum die Adressen an die Kunden ausgeben.

Netztypen

Bei Internetadressen, nicht nur bei IPv6, sondern auch bei IPv4, unterscheidet man zwischen PA- (Provider Aggregateable) und PI- (Provider Independent)Netzen.

Provider Aggregateable Netze (PA-Netze)

Unternehmen bekommen IPv6-Adressen ähnlich wie heute vom Internet Service Provider (ISP). Jeder ISP hat auf Anforderung vom RIPE einen ausreichend großen IPv6 Adressblock erhalten, aus dem die eigene Infrastruktur des Providers und die Netze der Kunden bedient werden können. Der Provider stellt seinem Kunden die Netze für die Dauer des Vertrages zur Verfügung. Sollte der Vertrag zwischen Kunde und ISP gelöst werden, fallen die IPv6-Adressen an den Provider zurück. Das ist nicht tragisch, da der neue Provider (und ohne ISP geht es heute nicht mehr) einen neuen Bereich von IPv6-Adressen zur Verfügung stellt.

Der Provider sorgt für das Routing des Netzes, das er dem Kunden zur Verfügung stellt, d.h. er gewährleistet die Weiterleitung und korrekte Zustellung der transportierten Datenpakete. Daher muss sich der Kunde nicht mit den zu befolgenden Routingregeln oder den Aspekten der Routingsicherheit befassen. Oft hat der Kunde nur eine Leitung, den Uplink, ins Netz eines Providers und muss selbst daher kein dynamisches Routing implementieren.

Vorteil dieser Lösung ist die einfache Implementierung und der einfache Betrieb. Eventuell übernimmt der ISP selber das Management des Routers, so dass der Kunde keine Mühe damit hat und auch kein ausgebildetes Personal für die Betreuung des Routers haben muss. Da der Provider nur sehr wenig Routinginformationen an den Kundenrouter geben muss, reicht auf Seite des Kunden eine relativ kleine Hardware für den Internetanschluss. Somit muss keine große Investition getätigt werden.

Der Nachteil dieser Lösung besteht darin, dass der Provider über ein hohes Maß an Kontrolle verfügt. Ein technisches Problem beim ISP kann leicht die Internetanbindung des Kunden beeinträchtigen, ohne dass der Kunde eine Möglichkeit hat, die Störung zu umgehen. Ob es die Sicherheit erlaubt, im eigenen Netzwerk einen vom Provider kontrollierten Router zu betreiben, muss jedes Unternehmen für sich selbst beantworten. Mit einer gut platzierten Firewall ist das aber für gewöhnlich kein Problem.

Provider Independent Netze (PI-Netze)

Für mehr Flexibilität und Kontrolle kann jedes Unternehmen einen eigenen IPv6-Addressblock vom RIPE erhalten. Das RIPE sieht dafür zwei Wege vor.

Sponsoring LIR

Ein RIPE-Mitglied wird als Local Internet Registry (LIR) bezeichnet. Ein Sponsoring LIR vermittelt einem Unternehmen einen eigenen IPv6-Adressblock und verwaltet den Block in der RIPE-Datenbank. Somit muss das Unternehmen keine eigene Mitgliedschaft eingehen und bekommt trotzdem eigene Adressen, die weltweit weitervermittelt werden können.

RIPE-Mitgliedschalft

Jedem Unternehmen steht es frei, selber Mitglied beim RIPE zu werden und somit in die Vorzüge der direkten Kommunikation mit dem RIPE zu kommen. Ein Sponsoring LIR als Zwischeninstanz wird nicht gebraucht. Die Mitgliedschaft kostet einen Jahresbeitrag ab 1.300,- Euro. Jedes Unternehmen muss für sich entscheiden, welches der richtige Weg ist.

Internetanschluss mit eigenen Adressen

Der Anschluss mit eigenen Adressen an das Internet kann mit einem oder mehreren ISPs realisiert werden. Ob ein ISP bereit ist, Netze zu routen, die nicht in seinem eigenen Adressbereich liegen, muss geklärt werden. Nicht jeder ISP wird auf jeder Leitung den Transport fremder Adressen zulassen oder zulassen wollen. Der ISP erfährt einen Kontrollverlust und der Kunde gewinnt Unabhängigkeit, was nicht jeder ISP wollen wird. Den Mehraufwand, den der ISP hat, wird der ISP sicher in Rechnung stellen wollen.

Wenn der Kunde nur einen Uplink, also nur eine Verbindung ins Internet hat, kann der Anschluss ähnlich erfolgen wie bei PA-Netzen. Der ISP sorgt für die weltweite Verbreitung der Adressen und führt dem Kundennetzwerk den Datentransfer zu, der für das Netzwerk bestimmt ist.

Mit zwei Uplinks sieht es etwas anders aus. Um volle Redundanz zu gewährleisten, muss der Kunde dann über zwei ISPs selber aktiv am weltweiten Routing teilnehmen. Dabei gibt jeder ISP und somit auch ein Unternehmen mit PI-Netzen, seinen Uplinks bekannt, über welche IPv6-Adressen es verfügt. Diese Bekanntmachung trägt der ISP weiter zu seinen Uplinks und Partnern, so dass sich die Information weltweit verbreitet. Im Gegenzug bekommt der Kunde vom ISP alle Informationen, die der ISP aus anderen Quellen hat.

Damit ist sichergestellt, dass der Endkunde alle Netzwerke, die ans Internet angeschlossen sind, kennt und Daten dorthin versenden kann. Dieser Versand ist die zweite Dienstleistung des ISPs.

Der Kunde lernt so über beide ISPs, wie ein Netzwerk zu erreichen ist, und sucht sich den jeweils besseren Weg aus. Sollte der Weg über einen Provider gestört sein, wird automatisch auf den Weg des anderen Providers umgeschaltet. Das geschieht schnell und automatisch und erfordert keinen manuellen Eingriff des Kunden.

Der Preis für diese Ausfallsicherheit und Flexibilität ist erhöhter Aufwand und es sind Investitionen zu tätigen, sowohl in Hardware als auch in die Ausbildung der Mitarbeiter.

Jeder ISP erhält vom RIPE eine AS-Nummer (ASN) für sein Autonomes System (AS). Als AS wird ein Netzwerk bezeichnet, das geschlossen unter einer administrativen Hoheit steht. Das ist bei Unternehmensnetzwerken gegeben. Diese AS-Nummer erhält ein Mitglied des RIPE, aber auch ein Sponsoring LIR kann eine AS-Nummer vermitteln.

Mit Hilfe der AS-Nummer kann auf einem Router die Verbindung zu einem oder mehreren ISPs aufgenommen werden. Das Routing Protokoll, das alle die Informationen über die weltweit verfügbaren Netze transportiert, nennt sich Border Gateway Protocol Version 4 (BGP4).

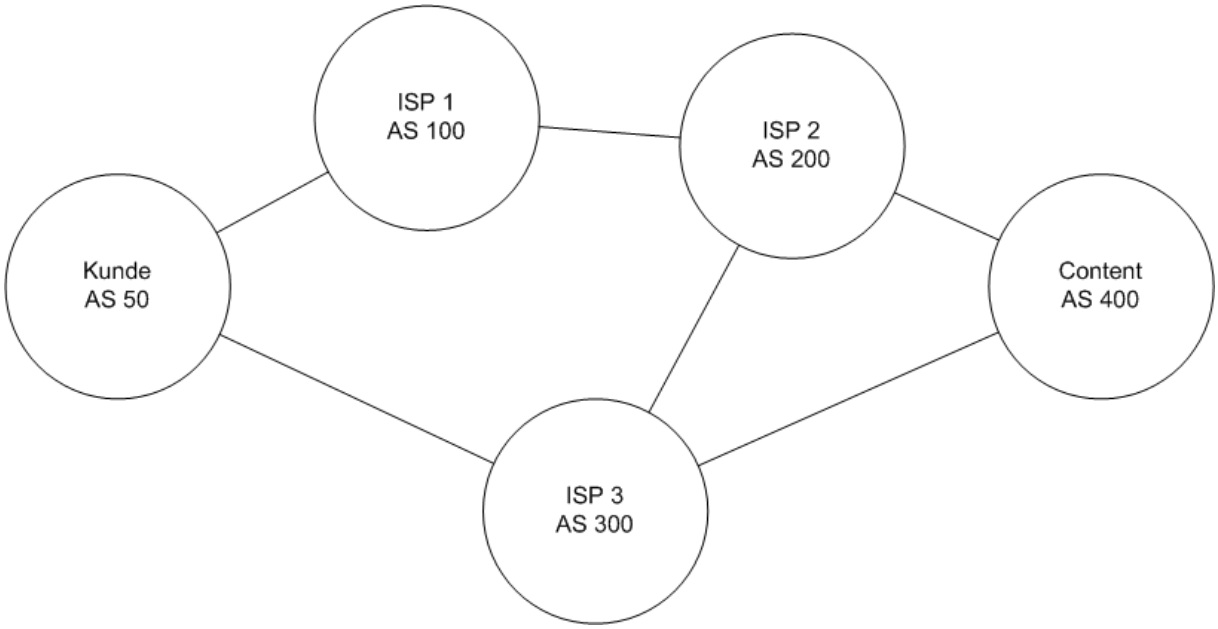

Abbildung 2: AS Nummer

Der Kunde erfährt über mehrere Wege, wie das AS 400 erreicht werden kann (vgl. Abbildung 2). Sollte eine Verbindung ausfallen, steht immer eine andere Verbindung bereit, die Daten zu transportie-

ren. Diese Ausfallsicherheit erkauft sich ein Unternehmen mit dem erhöhten Aufwand, sich auf diesem Wege ans Internet anzuschließen.

5. Wie viel kostet der Umstieg auf IPv6?

Das ist die Frage der Fragen. Aber leider ist die Antwort wie so oft: Kommt drauf an. In jedem Unternehmen sind die Kosten anders, aber es ist sicher sinnvoll, diejenigen Bereiche zu beleuchten, die betroffen sind. Dann kann jedes Unternehmen zu einer Abschätzung des Aufwands kommen und die Kosten in die Planung mit hinzunehmen. Grundsätzlich gilt: Je früher mit der Einführung von IPv6 begonnen wird, umso preiswerter wird es. Das kann mit einer Einkaufsrichtlinie beginnen, damit die Liste der nicht IPv6-fähigen Geräte schon jetzt verkürzt wird.

Inventur

Bei einer Inventur für IPv6 werden alle Bereiche des Unternehmens auf die Einführung von IPv6 hin geprüft. Am Ende ergibt sich eine Liste mit Komponenten, die für eine Einführung von IPv6 neu angeschafft werden müssen.

Hardware

Die PC- und Server-Hardware alleine, ohne Betriebssystem, ist nicht gemeint. In die Kategorie Hardware fallen vor allem Appliances, z.B. Router, Switches, Firewalls und Intrusion Prevention Systeme. Diese Netzwerkgeräte sind als Erstes zu untersuchen, da ohne Router und Switches das Netzwerk nicht funktioniert.

Nicht zu vergessen: Drucker, Plotter und Scanner, die bei einer Einführung von IPv6 im Büronetzwerk ebenfalls IPv6 beherrschen müssen. Randbereiche wie z.B. IP-Kameras dürfen nicht vergessen werden.

Software

Die Inventur der Software ist bei Standardsoftware relativ leicht, da die heutigen Betriebssysteme durchgängig IPv6 beherrschen. Kompliziert wird es bei angepasster oder selbst entwickelter Software. Eventuell müssen viele tausend Zeilen Programmcode geprüft werden. Die Abschätzung dieses Punktes ist schwierig und sehr individuell für jedes Unternehmen.

Unter Software fallen auch alle Programme, die für die Überwachung der IT notwendig sind und den Administratoren über den Zustand der Systeme Auskunft geben. Wenn die IP Address Management-Software nur IPv4 beherrscht, muss hier ebenfalls angesetzt werden.

Mitarbeiter

Inventur bei Mitarbeitern? Das hört sich erst einmal menschenfeindlich an, aber es geht um den Wissensstand der Mitarbeiter in Bezug auf IPv6. Zuvorderst sind die Mitarbeiter der hausinternen IT zu nennen, die auf IPv6 geschult werden müssen. Aber auch die Produktion, die Produktentwicklung und sogar der Vertrieb können betroffen sein. Wahrscheinlich steht aber auf der Liste die Geschäftsleitung selber, ohne deren Unterstützung die Einführung von IPv6 nicht gelingen kann.

Training und Schulung

Training und Schulung sind der vielleicht aufwändigste Teil der Einführung von IPv6. Mitarbeiter benötigen Zeit, sich mit dem neuen Protokoll vertraut zu machen.

Die IT-Abteilung des Unternehmens benötigt Zeit und Testmöglichkeiten, um Routine mit IPv6 zu erlangen. Oft sind aber gerade die IT-Abteilungen unter hohem Druck und haben kaum Freiraum für IPv6. Diesen Freiraum muss die Geschäftsführung gewähren und ein Budget für Testhardware zur Verfügung stellen. Nur so können die Mitarbeiter IPv6 anfassen und testen. Eine direkte, ungetestete

Einführung im Produktionsnetz wäre zu gefährlich. Das Testlabor muss alle relevanten Komponenten des Produktionsnetzwerkes enthalten, da andernfalls die Tests kein reales Bild ergeben werden.

Trainings bei Schulungsanbietern sind ebenfalls eine gute Möglichkeit, die Mitarbeiter auf das neue Thema vorzubereiten. Aber alle Theorie nutzt nur, wenn sie in die Praxis umgesetzt werden kann. Bei der Auswahl der Schulung ist zu beachten, dass die Praxis den Hauptanteil des Lehrgangs ausmacht.

Bewährt haben sich Inhouse-Schulungen, die von den Mitarbeitern gehalten werden, die sich schon mit IPv6 befasst haben. Solche Schulungen können kurz sein, damit sie in den Tagesablauf passen, und werden von Kollegen für Kollegen gehalten. Daher ist der Inhalt voll auf das Publikum zugeschnitten und es muss wenig Rücksicht auf Firmengeheimnisse genommen werden. Die Mitarbeiter, die eine Schulungen vorbereiten und halten, sind danach voll in dieses Thema eingearbeitet und bringen die Einführung von IPv6 schnell und kompetent voran.

Ein Budget für Bücher ist wie immer empfehlenswert. Auch wenn die eigentliche Routine mit dem Protokoll IPv6 aus der praktischen Anwendung kommt, ist die Erarbeitung der Theorie aus Büchern unverzichtbar.

Neuanschaffungen

Bei den Neuanschaffungen ist die Inventur die Grundlage. Eine Einkaufsrichtlinie ist in einem späteren Kapitel beschrieben. Wenn die Entscheidung für IPv6 in einem Netzwerkbereich gefallen ist, kann eine genaue Komponentenliste erstellt werden, anhand der die Beschaffung erfolgt. Da die meisten Netzwerkgeräte seit einiger Zeit IPv6 beherrschen, ist meistens nicht sehr viel anzuschaffen.

Lieferanten

Viele Unternehmen haben Vertragspartner für Netzwerkdienstleistungen und IT. Wenn das Unternehmen eine Begleitung dieser Partner für die Einführung von IPv6 wünscht, sollte frühzeitig mit dem Partner gesprochen werden. Viele kleinere IT Systemhäuser sind unerfahren mit IPv6 und müssen erst selber lernen.

Wenn der Partner mit IPv6 nicht weiterhelfen kann, muss eventuell der Betreuungspartner für die IT gewechselt werden. Die daraus resultierenden Kosten sind meistens sehr hoch, da der neue Partner sich ja nicht nur mit IPv6 befassen soll, sondern auch die vorhandene IT pflegen muss. Dies kann ein Unternehmen in große Probleme bringen, die dann wieder hohe Folgekosten nach sich ziehen.

Outsourcing

Sollte die IT komplett an einen Partner ausgelagert worden sein, muss der Auftraggeber bald über IPv6 sprechen. Falls IPV6 nicht Bestandteil des ursprünglichen Vertrages ist, muss nachverhandelt werden. Die Kosten sind an dieser Stelle nicht abschätzbar. Wenn der Partner IPv6 nicht unterstützt, oder noch nicht unterstützt, bleibt dem Kunden wahrscheinlich nichts, als abzuwarten und zu hoffen, dass der Schaden gering ist. Auch hier gilt: Frühzeitig das Gespräch mit dem Partner suchen.

6. Widerstände im Unternehmen

Jede neue Technik bringt auch Widerstände im Unternehmen hervor. Zweifler gibt es immer. Die Zweifler zu überzeugen, ist nicht einfach, aber die Geschäftsleitung wird sich dieser Aufgabe nicht verschließen können.

„Noch viele IPv4-Adressen vorhanden“

Es sind nach heutigem Stand noch IPv4-Adressen vorhanden. Aber bei einer Verbrauchsrate von ca. 16 Millionen IPv4-Adressen pro Monat ist ein Ende doch abzusehen. Auch wenn es den RIRs gelingt, ungenutzte Adressen wieder einzusammeln, wird der Zeitpunkt, an dem die letzte IPV4-Adresse vergeben ist, maximal einige Monate nach hinten geschoben.

Hat Ihr Unternehmen noch IPv4-Adressen übrig? Vielleicht wollen Sie ja Adressen zurückgeben, damit andere Unternehmen aus einer Zwangslage befreit werden? Es gehört schon viel Altruismus zu solch einem Schritt. Nur sehr wenige Organisationen werden diesen Schritt gehen. Bei staatlich kontrollierten (beeinflussten) Organisationen wie Universitäten in Europa könnte solch ein Schritt denkbar sein, aber kaum bei privaten Unternehmen. Die meisten Organisationen und Unternehmen werden die IPv4-Adressen hüten wie einen Schatz, unabhängig davon, ob die Adressen noch gebraucht werden oder nicht.

Ein Schatz, der so wertvoll ist, soll auch genutzt werden, oder? Lösen Sie sich von den alten Adressen und verstehen Sie IPv4 eher als Ballast, aber nicht als wertvolle Ressource.

„Wir haben noch viel Zeit“

In fast allen Regionen der Welt gibt es noch IPv4-Adressen, daher ist eine Einführung von IPv6 noch nicht nötig. Das kann geschehen, wenn wirklich keine IPv4-Adressen mehr zur Verfügung stehen.

So weit so gut. Aber wenn die Adressen wirklich zu Ende gehen, ist es für eine kontrollierte und sorgfältige Einführung von IPv6 zu spät. Die Einführung von IPv6 benötigt Zeit und erzeugt Aufwand, ist aber letztendlich nicht zu verhindern. Die Zeit, die zur Einführung von IPv6 benötigt wird, muss zumindest grob geschätzt werden, damit der Zeitpunkt des Projektstarts nicht verpasst wird. Es ist also jetzt an der Zeit, das Projekt zu starten. Vielleicht stellt sich dann heraus, dass noch etwas Zeit bleibt, aber mindestens eine Einkaufsrichtlinie sollte verabschiedet werden, damit der Aufwand bei der Einführung von IPv6 nicht zusätzlich erhöht wird.

„Die anderen stellen auch nicht um“

Wirklich nicht? Wer sind denn die anderen? Sind in der globalisierten Welt die Unternehmen im lokalen Gewerbepark der Maßstab, oder vielleicht doch der Mitbewerber aus Asien? Wenn Sie Ihr Umfeld betrachten, dann schauen Sie auf Kunden und Lieferanten und Mitbewerber. Wenn Ihr Unternehmen nicht auf IPv6 umstellt, werden Sie irgendwann der letzte sein und unter Zeitdruck umstellen müssen. Ihr Mitbewerber hat sein Projekt ohne Druck und mit Sorgfalt umgesetzt, und Ihnen steht nun eine Schnelleinführung ins Haus…

Unternehmen, die IPv6 einführen, könnten einfach darüber schweigen. Nur Service Provider müssen die Unterstützung von IPv6 öffentlich bewerben, nicht aber andere Unternehmen. IPv6 wird stillschweigend an vielen Stellen eingeführt und getestet, ohne dass es an die Öffentlichkeit gerät.

Schnell und überhasstet ausgeführte Projekte neigen zum Scheitern. Oder die Kosten sind viel höher als nötig. Das kann vermieden werden - aber nur durch eine rechtzeitige Beschäftigung mit dem Thema IPv6.

„Meine Kunden fragen IPv6 nach“

Jedes Unternehmen ist Lieferant und Kunde zugleich. Fragen Ihre Kunden nach IPv6 oder nach funktionstüchtigen Produkten? Liefern Sie nach Asien? Dann ist es jetzt Zeit, die eigene Produktpalette auf IPv6 zu untersuchen und IPv6 in den nächsten Entwicklungszyklus aufzunehmen. Die Bedenken von Controllern wegen der Kosten und der Ingenieure wegen der zusätzlichen Zeit zur Entwicklung müssen behandelt werden. Aber der Verlust eines Marktes wiegt schwerer.

„Nicht nötig“

Es gibt ja noch IPv4-Adressen, und selbst wenn die knapp werden, sorgt der Provider dafür, dass mein Unternehmen kommunizieren kann. Das ist teilweise richtig. Viele Provider versuchen das Leben von IPv4 zu verlängern, weil die Einführung von IPv6 zu spät angegangen wurde. Das eigene Versäumnis wird nun mit Notfallmaßnamen „repariert“. Das kann und wird nicht lange funktionieren. Die Provider müssen viel Geld ausgeben, um das Leben von IPv4 zu verlängern. Die Kosten dafür werden auf die Kunden umgelegt - auf wen sonst…? Die Unternehmen erhalten somit einen verschlechterten Service zu höheren Kosten. Eine baldige Einführung von IPv6 hingegen verbessert den Service und hält die Kosten gering, da die Provider nicht so viel Geld für die Erhaltung von IPv4 ausgeben müssen. Und wenn Sie IPv6 haben, fehlt dem Provider das Argument für höhere Preise.

„Mein Provider macht das für mich“

Aber tut er es wirklich? Im Sommer 2011 hatte noch nicht einmal ein Drittel der Provider im europäischen Raum ein IPv6-Netzwerk beantragt. Es kann also keine Rede davon sein, dass die Provider hier besonders schnell sind, im Gegenteil. Die Führungsrolle haben die Provider nicht inne.

Jedes Unternehmen muss also die IPv6-Projekte des Providers beleuchten und für sich festlegen, ob es reicht, was der Provider bisher umgesetzt hat. Die Provider beklagen, dass die Kunden IPv6 nicht nachfragen. Aber die Kunden haben auch nie IPv4 nachgefragt, sondern einen funktionstüchtigen Internetzugang, der die Kommunikation mit allen Geschäftspartnern weltweit sicherstellt. Unternehmen sollten hier keine Kompromisse machen und wenn nötig den Provider wechseln. Es geht um die Unternehmenskommunikation, nicht um ein technisches Protokoll.

„Nicht vor meiner Rente / Angst vor Neuem“

Auch IT-Mitarbeiter werden älter und verlieren die Bereitschaft der Jugend, sich mit Begeisterung in neue Themen einzuarbeiten. Diese Mitarbeiter müssen gefordert und gefördert werden, damit keine Widerstände gegen die Einführung von IPv6 bestehen bleiben. Wie das einzelne Unternehmen das angeht, ist sicher sehr individuell.

Dass der Mensch von neuen Entwicklungen Angst haben kann, ist bekannt. Auch hier muss die Geschäftsleitung fördernd eingreifen. Durch Training und Schulung die Ängste abzubauen, ist eine gute Möglichkeit. Es muss ein Plan entwickelt werden, wie die Mitarbeiter an IPv6 und die damit verbundenen Herausforderungen herangeführt werden können.

7. Einkaufspolitik

Kurzversion

Eigentlich ist es ganz einfach. Wer heute noch IT-Produkte einkauft, die nicht mit IPv6 arbeiten können, riskiert, dass die Investitionen vor Ende der Abschreibungszeit aus dem Netzwerk genommen werden müssen und nicht mehr brauchbar sind.

Langversion

Der Einkauf von Hardware und Software, die IPv6 unterstützt, ist leider immer noch kompliziert. Viele Hersteller behaupten von sich, dass die eigenen Produkte IPv6 unterstützen, aber diese Behauptung muss nicht heißen, dass alle notwendigen Features unterstützt werden. Der Käufer muss also jeweils Stück für Stück eigenhändig prüfen, ob die eigenen Anforderungen erfüllt werden.

Anforderungen

Eigene Anforderungen

Die eigenen Anforderungen zu definieren, ist keine leichte Aufgabe, sollte aber sorgfältig gemacht werden. Anderenfalls drohen teure Fehlkäufe, die jeder gerne vermeiden möchte. Wie geht man also vor? Startpunkt ist eine Liste der IPv4-Features, die heute genutzt werden. Sofern diese IPv4-Features noch alle gebraucht werden, kommen diese Punkte auf die Liste der Anforderungen. Vielleicht führt diese Liste ja auch zu einem Überdenken der IPv4-Netzstruktur, so dass die Einführung von IPV6 zu einem neuen und moderneren Netzwerk führt.

Als zweites muss eine Liste mit Unterschieden zwischen IPv4 und IPv6 erstellt werden. Die Unterschiede können marginal sein oder das Netzwerkdesign massiv beeinflussen. Aus der Liste ergeben sich Anforderungen an das Netzwerk, die Applikationen und die Netzwerküberwachung.

Die Sicherheit darf nicht vergessen werden. Einige Sicherheitsfeatures sind bei IPv6 anders implementiert als in IPv4. Es muss geprüft werden, ob hier eine Deckung beider Protokolle erreicht werden kann, oder ob es neue Features geben muss. Bei dieser Betrachtung fällt automatisch eine Liste aller Punkte im Netzwerk ab, an der Sicherheitseinstellungen vorgenommen wurden. Da in der Zukunft diese Sicherheit für zwei Protokolle gewährleistet werden muss, kann diese Liste schon eine Arbeitsgrundlage für die Einführung von IPv6 sein. Außerdem ist es sicher gut, wenn die Sicherheitseinstellungen im Netzwerk auf diese Weise durchgesehen werden. Bei diesen Listen dürfen die Applikationen nicht fehlen, denn auch Datenbanken und andere Server können Accesslisten haben, die den Zugriff nur von festgelegten IP-Bereichen zulassen. Das muss für IPv6 angepasst werden.

Externe Anforderungen

Gibt es externe Einflüsse, die meine Kaufentscheidung beeinflussen? Je nach Branche könnte der Einkauf von Hardware und Software strengen Richtlinien unterliegen. Die IT in Flugzeugen z.B. sollte sicher besonders gut getestet sein. Lieferanten für militärische Ausrüstung oder für Atomkraftwerke könnten ebenfalls externen Zertifizierungen unterliegen. Es muss also geklärt werden, ob die einzukaufenden Geräte solchen Anforderungen genügen.

Was sagen Banken und Versicherungen zu der Struktur meiner IT? Müssen ein neues Netzdesign und neue Protokolle mit diesen externen Partnern abgesprochen sein?

Verlangen meine Kunden, dass mein Unternehmen in bestimmten Bereichen zertifiziert ist? Dann muss der Einkauf von Hardware und Software den Anforderungen dieser Zertifikate genügen. Anderenfalls drohen Ärger und Verlust von Kunden. Eventuell haben aber auch die Kunden IPv6 noch nicht eingeführt und machen sich selber nicht klar, dass IPv6 Einfluss auf diese Anforderungen nimmt. Dann helfen nur Gespräche, die Zeit in Anspruch nehmen.

Betriebsrat

Der Datenschutz ist ein Thema, das insbesondere auch für IPv6 intensiv diskutiert wird, da Ängste bestehen, dass global vergebene IPv6-Adressen ein Ende jeglicher Anonymität im Netz bedeuten. Eventuell muss die Einführung von IPv6 mit den Mitarbeitern besprochen werden oder mit dem Betriebsrat. Eine einvernehmliche Festlegung von Standards innerhalb des Unternehmens kann auf die Einkaufspolitik Einfluss nehmen, ist aber wahrscheinlich preiswerter als der Streit, oder andernfalls entstehen kann.

Dokumente als Leitfaden

Es gibt einige Dokumente im Internet, die bei der Auswahl von IPv6-fähigen Produkten helfen sollen.

- Eines der besten und komplettesten ist das Dokument RIPE 501[3], das ab November 2011 in einer überarbeiteten Version zur Verfügung steht, allerdings unter einer neuen Dokumentennummer im Pool der RIPE Dokumente. Eine deutsche Version des Dokumentes ist verfügbar.

- Die US-Regierung hat ein Dokument verfasst, dass sich mit der Einführung von IPv6 befasst (USGv6: A Technical Infrastructure to Assist IPv6 Adoption[4]). Auch wenn das Dokument natürlich auf den US Markt ausgelegt ist, finden sich viele nützliche Hinweise.

- Ebenfalls von der US-Regierung kommt das Dokument „Guidelines for the Secure Deployment of IPv6“[5], das als Grundlage für die Einführung von IPv6 genutzt werden kann.

- Lawrence E. Hughes hat ein Buch über IPv6 geschrieben, dass frei verfügbar ist: „The Second Internet, Reinventing Computer Networking with IPv6”[6].

Zertifikate und Logos

Das IPv6-Forum[7] bietet zu vielen Aspekten von IPv6 Zertifizierungen an. Nach erfolgreicher Zertifizierung darf der Hersteller von Hardware oder Software ein Logo führen, dass die Zertifizierung anzeigt (vgl. Abbildung 3).

[3] http://www.ripe.net/ripe/docs/ripe-501
[4] http://w3.antd.nist.gov/usgv6/
[5] http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf
[6] http://www.ipv6forum.com/dl/books/the_second_internet.pdf
[7] http://www.ipv6forum.com/

Abbildung 3: IPv6 Ready-Logo des IPv6-Forums

Welchen Wert ein Logoprogramm wirklich hat, muss jedes Unternehmen selber bewerten. Wie immer gibt es mehr oder weniger wichtige Programme. Die jeweiligen Zertifizierungsstellen nennen die Kriterien zur Zertifizierung öffentlich, so dass auch diese Listen als Hilfestellung herangezogen werden können.

Gespräch mit Lieferanten und Partnern

Alle Dokumente, die sich mit der Einführung von IPv6 befassen, müssen auf die individuelle Situation des Unternehmens angepasst werden. Nicht immer sind alle Anforderungen aus einem Bereich sinnvoll und müssen eingefordert werden. Aber die Dokumente geben einen Rahmen vor, in dem die Gespräche mit den Partnern ablaufen können.

Wenn aber zusammen mit den Partnern und Lieferanten ein Katalog an Anforderungen erstellt ist, sollte dieser Katalog Vertragsbestandteil sein, damit sich später niemand herausreden kann und der Kunde auf unbrauchbarem Material sitzen bleibt.

Besonders schwierig sind die Anforderungen bei Software, die individuell erstellt oder angepasst wurde. Die IPv6-Fähigkeit muss in Verträgen und Pflichtenheften verbindlich geregelt sein.

Internet Provider

Der ISP muss ebenfalls IPv6 unterstützen. Leider ist das selbst heute noch schwierig. Viele große Provider unterstützen IPv6 auf Nachfrage, manchmal gegen Aufpreis. Da IPv6 aber nur ein weiteres Protokoll ist, sollte ein Aufpreis nicht akzeptiert werden, denn der Provider muss sowieso IPv6 einführen und unterstützen, um nicht vom Markt verdrängt zu werden. Und nur, wenn die Kunden IPv6 nachfragen, entsteht bei den ISPs der notwendige Druck für eine zügige Einführung von IPv6.

Die DSL-Provider sind etwas langsamer, was aber auch daran liegt, dass die Standards lange nicht fertig waren und es daher keine entsprechenden Implementierungen in den kleinen Heimroutern gab. Das wird anders werden. Wenn der Internetanschluss über DSL läuft, muss eventuell ein Tunnel, der IPv6 über IPv4 transportiert, aushelfen, bis der DSL-Provider IPv6 auf der Leitung bereitstellen kann.

Es gibt auch Unternehmen, die getrennte Provider für IPv4 und IPv6 beauftragen.

Partnerwechsel

Wenn ein Partner, Hersteller oder Lieferant nicht in der Lage ist, die Anforderungen an IPv6 zu erfüllen, muss ernsthaft über einen Wechsel des Partners nachgedacht werden. Das kann beliebig kompliziert sein, denn oft binden langfristige Verträge Kunde und Partner. Hier kommt der Faktor Zeit wieder ins Spiel, denn wenn nicht absehbar ist, dass der Partner IPv6 unterstützt, bleibt jetzt noch Zeit für lange Kündigungsfristen.

Wenn der Partner IPv6 nicht unterstützt, könnte bei bestimmten Produkten, die gekauft werden sollen, über einen zweiten Partner nachgedacht werden. Konkurrenz belebt das Geschäft, und vielleicht bewegt sich der langjährige Partner ja, wenn der Mitbewerber ins Haus kommt.

Grundsätzlich gilt natürlich, dass die Unterstützung von IPv6 in alle Verträge hineingehört, die heute geschlossen werden.

Stuhlwechsel

Es darf nie vergessen werden, dass Ihr Unternehmen der Partner, Lieferant, ISP oder das IT-Systemhaus sein könnte, das sich mit den Kundenforderungen nach IPv6-Compliance auseinandersetzen muss. Sind Sie auf alle Punkte vorbereitet, wenn Ihr Kunde mit den Anforderungen aus RIPE 501[8] kommt?

[8] Requirements for IPv6 in ICT Equipement, http://www.ripe.net/ripe/docs/ripe-501

8. Einführung von IPv6

Wie viele Adressen stehen zur Verfügung?

Grundsätzlich gilt, dass ein Unternehmen vom Provider oder dem RIPE ein „/48“-Netzwerk erhält. Das sind genug Adressen für ca. 65.500 eigene Netzwerke bzw. Netzwerksegmente. Nur wenige Unternehmen dürften diese große Menge an Adressen je benötigen.

Da so viele Adressen und Netzwerke genutzt werden können, sollte eine kluge Aufteilung der Adressen für Zukunftssicherheit sorgen. Eine hierarchische Vergabe schützt obendrein vor Überlastungen der Router und anderer Netzwerkhardware.

Hierarchisches Netzwerkdesign

Ein guter Adressplan orientiert sich an den Gegebenheiten der Firma. So könnte ein Gebäude einen großen Adressblock erhalten, der dann innerhalb des Gebäudes feiner aufgeteilt wird. Dieses Vorgehen vereinfacht das Routing zwischen den Gebäuden, da für ein ganzes Gebäude immer nur eine Route in den Routern existieren muss, um alle Netze zu erreichen. Für die Sicherheit ist es ebenfalls von Vorteil, nur eine Regel in der Firewall zu pflegen, und die Netzwerkdokumentation wird erleichtert.

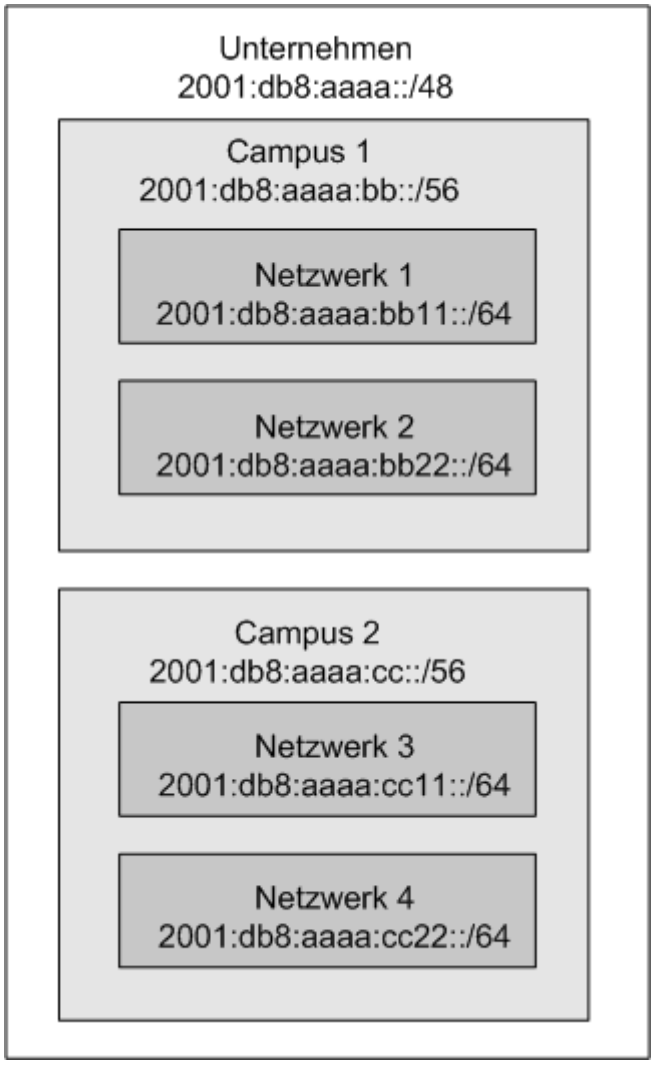

Abbildung 4: Hierachischer Adressplan

Wichtig ist, dass zwischen den vergebenen Netzwerken noch Platz gelassen wird für zukünftige Netzwerke. Bei dem in Abbildung 4 gezeigten Adressenplan gehören zu Campus 1 die Netze 2001:db8:aaaa:bb00/64 bis 2001:db8:aaaa:bbff/64, also 256 Netze, von denen hier im Beispiel nur zwei Netze vergeben sind. Wenn der Standort wächst, muss das Design des Gesamtnetzwerks nicht geändert werden.

Die Aufteilung des Netzwerkes, wie oben gezeigt, macht 256 Standorte mit je 256 Netzwerken möglich. Je vier „Standortnetze“ sollten für die Router und das eigene Rechenzentrum vorgesehen werden. So entsteht auch hier niemals Knappheit an Adressen. Der verschwenderische Umgang mit IP-Adressen muss neu gelernt werden, bringt aber Vorteile. Eine Neuverteilung der IPv6-Adressen im Netz wird nie wieder notwendig sein.

Wenn die Standorte zu weit auseinander liegen oder nicht durch ein eigenes Netzwerk miteinander verbunden sind, kann für jeden Standort ein Adressblock der Größe „/48“ beantragt werden. Somit wird das Design abermals erleichtert.

Wo starten?

Wo im Netzwerk sollte mit der Einführung von IPv6 begonnen werden? Diese Frage ist nicht leicht zu beantworten, aber es gibt einige Strategien, die sich bewährt haben. Jedes Unternehmen muss allerdings selber entscheiden, welchen Weg es gehen will. Eine allgemeingültige Strategie gibt es nicht.

In Richtung Kunden

Die Kommunikation mit Kunden ist der wichtigste Grund, IPv6 einzuführen. Denn wenn ein Kunde oder Interessent nur IPv6 zur Verfügung hat, das Unternehmen aber nicht, wird die Kommunikation scheitern. Es wird sicher in den Netzen der Provider Gateways geben, die eine Umsetzung von IPv4 auf IPv6 und umgekehrt möglich machen. Aber davon unabhängig zu sein, ist auf jeden Fall besser. Diese Gateways sind wieder ein zusätzliches Netzwerkelement zwischen dem Kunden und dem Unternehmen. Die Gateways sind teuer und die Provider müssen versuchen, die Kosten einzuspielen. Zudem greifen sie in die Kommunikation direkt ein.

Webserver

Das Angebot eines Unternehmens im Internet sollte spätestens 2012 per IPv6 im World Wide Web (WWW) erreichbar sein. So ist sichergestellt, dass die Kunden und Interessenten immer auf alle Informationen des Unternehmens zugreifen können. Es darf nicht sein, dass auch nur ein Kunde verloren geht.

Sollte der Webserver nicht im Haus betrieben werden, sondern im Netz eines ISP stehen, muss dieser IPv6 anbieten. Tut er dies nicht, muss ernsthaft über eine Verlagerung der Dienste zu einem anderen Anbieter nachgedacht werden.

E-Mail-Server

Wichtiger noch als die Internetseiten ist die Kommunikation des Unternehmens per E-Mail. Das gilt nicht nur für die Kommunikation mit Kunden und Lieferanten, sondern auch für den internen Informationsaustausch. Wenn heute die Mitarbeiter längere Zeit vom E-Mail-Dienst abgeschnitten sind, geraten zahlreiche Prozesse im Unternehmen ins Stocken. Daher muss der E-Mail-Service schnell mit IPv6 ausgestattet werden. Wenn der E-Mail-Server im Haus steht, wird sich die interne IT darum

kümmern müssen. Bei einem Dienstleister sollte IPv6 verlangt werden oder der Dienstleister muss ausgetauscht werden.

Gerade bei E-Mail will man keine Gateways des Providers zwischen sich und dem Kunden haben, denn genau an dieser Stelle könnte leicht eine unberechtigte Kopie der E-Mail gemacht werden.

Fernwartung

Viele Unternehmen bieten ihren Kunden einen Remote-Zugriff für die Fernwartung an. So kann der Hersteller von Hardware, Software oder Maschinen aus der Ferne helfen. Wenn der Kunde seine Hardware oder Software in einer reinen IPv6-Umgebung betreibt, muss auch der Hersteller aus Deutschland IPv6 beherrschen.

Solche Szenarien kann es schnell geben. Die deutsche Industrie exportiert in alle Welt komplizierte und technisch hochwertige Maschinen, gerade und besonders nach Asien. Dort sind die IPv4-Adressen besonders knapp, so dass die Fernwartung über IPv6 als realistisches Szenario angesehen werden kann.

Unternehmen sollten es sich nicht leisten, wegen eines Netzwerkprotokolls Probleme mit Kunden in aller Welt zu haben.

Produktentwicklung

Viele Hersteller von Maschinensteuerungen und Embedded Systems statten ihre Produkte mit Netzwerkschnittstellen aus, die eine direkte Verbindung zum Internet möglich machen. So kann der Kunde des Systems seine Maschine in sein lokales Netzwerk bringen und für eine Fernwartung, Neuprogrammierung oder Überwachung freischalten.

Da viele Produkte in asiatische Länder exportiert werden, in denen heute ein IPv4-Adressmangel herrscht, sollten die netzwerkfähigen Maschinen sowohl IPv6 als auch IPv4 anbieten, um dem Kunden die Wahl zu lassen, in welchem Netzwerk die Maschine eingesetzt wird. Es ist zu erwarten, dass asiatische Einkäufer sehr bald IPv6-Fähigkeiten verlangen werden.

Um einen Nachteil im Markt zu vermeiden, müssen die Entwickler heute IPv6 einplanen, wenn ein Produkt entworfen wird. Dazu kann die Geschäftsleitung eine Anweisung geben, die IPv6 für alle Produkte vorschreibt. Auch hier gilt, dass frühzeitig mit Vorlieferanten das Gespräch gesucht werden muss.

VPN Remote-Zugriff

Wenn es für Vertriebsmitarbeiter aus aller Welt wichtig ist, mit dem Stammhaus zu kommunizieren, muss der VPN-Zugang IPv6-fähig gemacht werden. Mitarbeiter aus Asien könnten sonst bald von der Kommunikation mit dem Stammhaus ausgeschlossen sein. Auch in diesem Fall gilt, dass die Gateways der Provider als Übergangslösung genutzt werden können, aber eine ideale Lösung ist das nicht. Und bei verschlüsselten VPNs via IPSec muss es eine direkte Kommunikation geben, da das Protokoll keine Gateways erlaubt. Die Provider werden hierfür eine Rechnung stellen wollen, und es kann nicht im Interesse von Unternehmen liegen, die Kommunikation durch fremde Gateways laufen zu lassen.

Neue Netzwerksegmente

Neue Segmente im Netzwerk bieten die Chance der „grünen Wiese“. Die Planung kann mit einem leeren Blatt Papier begonnen werden, eine seltene aber doch sehr schöne Situation. Bei solch einem

neuen Netzwerk IPv6 nicht zu berücksichtigen wäre sträflich, denn später wird das Design sicher schwieriger werden.

In einem neuen Netzwerksegment sollte IPv6 direkt eingeplant werden. Dafür ist es aber notwendig, das hierarchische Netzwerkdesign zu erstellen, das oben vorgestellt wurde. Auch wenn die endgültige Aufteilung der Netze noch nicht feststeht, muss doch ein grober Plan vorliegen. Andernfalls muss später das Netzwerk noch einmal verändert werden, was wieder Zeit braucht und Kosten verursacht.

Private Cloud

Das Thema Cloud, also die Virtualisierung der IT-Dienste mit Hilfe eines zentralen Rechnerpools, wäre auch ein guter Einstieg in IPv6. Eine neugeplante Cloud bietet ebenfalls eine „grüne Wiese“. IPv6 einzuplanen, ist notwendig und klug. Da die Cloud die Arbeitsweise der Unternehmen verändern wird, muss ohnehin viel neu gelernt werden und sie ist somit ein idealer Einstieg in IPv6.

Wer bekommt welche Adresse wie zugeteilt?

In einem IPv6-Netzwerk können Adressen dynamisch von den Hosts oder anderen Geräten gebildet werden. Das nennt man Autokonfiguration. Der Vorteil ist, dass der Administrator nichts tun muss, um alle Geräte mit IPv6 auszurüsten. Nachteilig ist, dass die Sicherheitsabteilung nicht anhand der IPv6-Adresse direkt auf einen Rechner schließen kann und somit das Regelwerk in einer Firewall nicht fein genug eingestellt werden kann. Grundsätzlich gelten die gleichen Regeln wie bei IPv4. Server, Router, Firewalls und Drucker bekommen statische Adressen, Hosts können mit dynamisch vergebenen IP-Adressen ausgestattet werden.

Router

Router müssen feste IPv6-Adressen auf allen Schnittstellen zugewiesen bekommen, da die Routing-Protokolle nicht mit wechselnden Adressen umgehen können. Der Netzwerkadministrator will wissen, wo welche Adresse vergeben ist, um den Überblick zu behalten. Es ist kontraproduktiv, wenn eine Route heute in Gebäude A gehört, morgen aber in Gebäude B.

Damit Hosts die IPv6-Adresse selbst erzeugen können, muss der Router das Netzwerk bekannt machen, aus dem die Adresse stammen soll. Der Router gibt zusätzlich bekannt, dass er als Gateway zur Welt genutzt werden kann. Diese Informationen müssen im Tagesbetrieb statisch sein und dürfen sich nur aufgrund eines Re-Designs des Netzwerkes ändern.

Hosts

Hosts, dazu gehören auch Tablet-PCs und Smartphones, können ihre Adresse aus dem vom Router genannten Netzwerkteil selbstständig ermitteln. Dabei gibt es grundsätzlich zwei Mechanismen für diese sogenannte Stateless Address Autoconfiguration (SLACC). Die Adresse kann aus der Hardwarekennung Media Access Control (MAC) gebildet werden, oder per Zufall, den so genannten Privacy Extensions. Da die MAC-Adresse der Netzwerkkarte sich nicht ändert, ist die einmal erzeugte Adresse des Hosts immer gleich. Das bringt Bedenken beim Datenschutz mit sich, die in einem späteren Kapitel beleuchtet werden.

Die Privacy Extensions bilden die Adresse per Zufall, wobei die Gültigkeit der Adresse von wenigen Stunden bis zu einigen Tagen gewählt werden kann. Diese zufällig gewählte Adresse lässt sich schwerer nachverfolgen, sowohl im Internet als auch für die hausinterne Sicherheit.

Server

Server müssen statische Adressen bekommen, damit immer klar ist, wo der Server erreichbar ist. Die Adresse wird im Domain Name System (DNS) eingetragen und sollte ich nicht ändern. Das gilt für alle Arten von Servern, seien es Fileserver, Domänenserver oder E-Mail-Server.

Es gelten die gleichen Regeln wie bei IPv4 für die Vergabe von Adressen.

Drucker

Drucker, Kopierer und Scanner sind in einer gewissen Weise ebenfalls Server, die eine statische Adresse im Netzwerk erhalten müssen. Auch hier gelten die gleichen Regeln wie bei IPv4. Betrachtungen zum Parallelbetrieb von IPv4 und IPv6 finden sich in einem späteren Kapitel.

Testlabor

IPv6 muss erfahren werden. Das Studium von guten Büchern kann die Erfahrung des Umganges mit IPv6 nicht ersetzen, auch wenn Bücher die Grundlagen legen können. Ein Unternehmen, das ernsthaft über die Einführung von IPV6 nachdenkt, wird ein Testlabor einrichten müssen. Das Testlabor muss alle Bereiche der IT umfassen, nicht nur das Netzwerk, sondern auch die Applikationen, die Betriebssysteme und die Security.

Das Netzwerk ist heute an vielen Stellen die Basis aller Arbeit im Unternehmen. Ein Eingriff wie die Einführung von IPv6 muss sorgfältig vorbereitet sein. Daher müssen die IT-Mitarbeiter alle Komponenten des Netzwerkes testen können, ohne Schaden im produktiven Netzwerk anzurichten. Die Unternehmensleitung muss dazu die notwendigen Materialien (Server, Router, Switches, Software) bereitstellen und den Mitarbeitern die Zeit einräumen, die für die Tests genutzt werden kann.

Eine Einkaufsrichtlinie, die nur Hardware und Software mit IPv6-Fähigkeiten ins Haus lässt, muss ebenfalls im Testlabor durchgesetzt werden. Die Versprechungen der Hersteller sollten im Testlabor geprüft werden. Aber dazu muss das Labor aufgebaut sein und die Mitarbeiter müssen mit IPv6 so vertraut sein, dass die Tests der neuen Hardware oder Software sinnvoll durchgeführt werden können.

Training

Die Schulung von Mitarbeitern für IPv6 ist notwendig, wenn nicht die Zeit vorhanden ist, sich alles selbst beizubringen. Zum Training können auch Bücher und das Testlabor gerechnet werden. Es gibt Menschen, die fürchten sich unbewusst vor Neuerungen. „IPv6, ganz wichtig, aber nicht mehr vor meiner Rente“. Wenn solch eine Aussage im Raum steht, muss dem Mitarbeiter mit Training und Förderung die Angst vor IPv6 genommen werden. Das geht sicher nicht von heute auf morgen.

Die Trainingsunternehmen bieten bereits Kurse zum Thema IPv6 an. Eine generelle Empfehlung für einen Anbieter kann nicht ausgesprochen werden.

Aber Training muss nicht immer extern eingekauft werden. Wenn ein oder zwei Mitarbeiter aus der IT tief in das Thema IPv6 eingearbeitet sind, können hausinterne Schulungen eine gute Alternative zu externen Schulungen sein. 90 Minuten Vortrag im Haus lassen sich oft leichter einrichten als externes Training, das Zeit braucht, Geld kostet und Reisekosten verursachen kann. Zudem kann ein hausinternes Training viel besser auf die individuellen Bedürfnisse der Kollegen zugeschnitten werden, als es ein externes Training jemals sein könnte.

Security

Die Sicherheit eines Unternehmensnetzwerkes muss immer einen sehr hohen Stellenwert haben. IPv6 ist allerdings nicht unbedingt „von Natur aus“ sicher, auch wenn der Eindruck manchmal erweckt wird. Da von sieben Schichten des kompletten Kommunikationsnetzwerks nur eine, nämlich die dritte ausgetauscht wird, wenn IPv4 durch IPv6 ersetzt wird, bleiben die Sicherheitsaspekte der anderen sechs Netzwerkschichten unverändert. Somit wird an dieser Stelle die Sicherheit weder besser noch schlechter. Für den Virus, der in ein Computernetzwerk eindringen möchte, ist es egal, ob die E-Mail per IPv6 oder IPv4 transportiert wird, die Wirkung bleibt die gleiche. Aber für den Virenscanner kann es jedoch einen großen Unterschied machen, wenn die IP-Adresse als ein Merkmal zur Erkennung von Viren oder SPAM herangezogen wird.

Firewall

Bei Firewalls gibt es einige Unterschiede zu beachten. Durch Funktionsunterschiede zwischen IPv4 und IPv6 müssen ein Teil der verwendeten Regeln unterschiedlich sein. Hier gilt es, im Testlabor Erfahrung zu sammeln, um herauszufinden, welche Regeln tatsächlich wichtig sind für das jeweils spezielle Netzwerk. Sicher ist nur, dass bei einer Fehlkonfiguration das ganze Netzwerk betroffen sein wird.

Die Firewallregeln müssen für die Übergangszeit für beide Protokolle in gleichem Maße gepflegt werden, was doppelten Aufwand mit sich bringt und natürlich auch zu Fehlern führen kann. Die Hersteller sollten dem Kunden einen Satz von Regeln vorschlagen, der den schlimmsten Fehlern durch Unwissenheit vorbeugt.

Intrusion Prevention System

Intrusion Prevention Systeme (IPS) müssen IPv6-Pakete verarbeiten können, um den Inhalt der Pakete auf schadenstiftenden Code zu prüfen. Diese Prüfung unterscheidet sich nicht von der Prüfung von IPv4-Paketen.

Für die Erkennung von IPv6-Angriffen wichtig ist die Analyse der Header von IPv6-Datenpaketen. Da IPv6 mit einer Kette von Datenpaketheadern arbeitet, können hier Angriffe verborgen sein. Eine ungewöhnliche oder verbotene Reihenfolge von Headern muss erkannt werden und eventuell muss Alarm ausgelöst werden. Da sich bei IPv6 noch Einiges im Fluss befindet, müssen die Hersteller schnell mit neuen Signaturen bereitstehen, wenn sich etwas verändert.

Routing-Protokolle

Routing-Protokolle kennen auch eine Authentifizierung der Router untereinander. Wenn die Security Policy des Unternehmens eine solche Authentifizierung verlangt, muss sichergestellt werden, dass die Router diese Funktion beherrschen. Eventuell muss die Security Policy verändert werden, da die Mechanismen in einigen Routing-Protokollen verändert worden sind. Besonders betroffen ist hier das weit verbreitete OSPF-Routingprotokoll.

Zugriffslisten

Zugriffslisten, oder Accesslisten, werden an vielen Stellen im Netzwerk und in den Applikationen eingesetzt. So ist es nicht unüblich, den Zugriff auf das Intranet oder eine Datenbank nur von vorher festgelegten IP-Bereichen aus zu gestatten. Wenn nun IPv6 ins Netzwerk kommt, müssen diese Listen erweitert werden, damit die Zugriffe wie gewohnt funktionieren. Um die doppelte Pflege der Listen kommt man während der Übergangszeit nicht umhin.

Da es gut möglich ist, dass die IPv6-Adresse eines Rechners sich täglich ändert, muss überlegt werden, ob die Beschränkung des Zugrifffs mittels Accessliste auf IP-Adressen oder IP-Netzwerke überhaupt noch zeitgemäß ist. Eine Identifikation des Mitarbeiters anhand von Schlüsseln und Zertifikaten könnte sinnvoller sein als die Identifikation eines Netzwerkgerätes über dessen IP-Adresse, sei es IPv4 oder IPv6.

NAT

Network Address Translation (NAT) dient der Umschreibung von IP-Adressen. Heute wird NAT vornehmlich am Internetanschluss der Unternehmen und Heimnetzwerke eingesetzt, um intern mit privaten Adressen zu arbeiten. Dabei werden öffentliche IPv4-Adressen in private umgeschrieben.

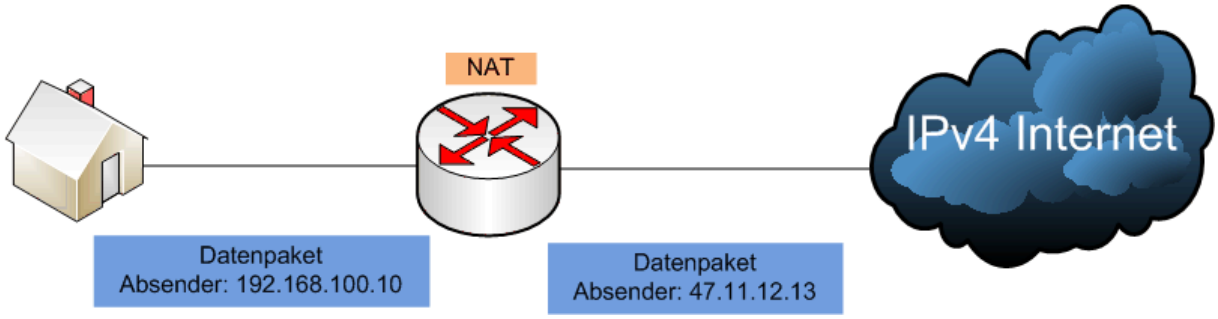

Abbildung 5: Network Address Translation zur Übersetzung privater IPv4-Adressen in öffentliche IPv4-Adressen

Security mit NAT?

Damit NAT funktioniert, muss der NAT-Router eine Tabelle mit Verbindungen bereitstellen und vorhalten, die auf dem Rückweg die Umschreibung der IP-Adresse wieder ermöglicht. Andernfalls würde die Zuordnung nicht funktionieren und eine Datenverbindung käme nicht zustande. Diese Tabelle ist so eingerichtet, dass nur Verbindungen von innen heraus eröffnet werden können. Ein Angreifer von außen kann keine Pakete ins Netzwerk des Unternehmens senden. NAT wird daher als Bestandteil der Security gesehen.

NAT untersucht aber nicht die Inhalte der Datenpakete. Wenn eine Verbindung erst einmal offen ist, können über die Paketinhalte Angriffe vorgenommen werden. Und das ist auch der häufigste Weg, Netzwerke anzugreifen. In E-Mails werden Viren und Trojaner transportiert, und Webseiten schleusen Javascript-Programmcode ein, der die Arbeitsplätze der Mitarbeiter ausspäht.

Da jede Firewall über Verbindungstabellen verfügt, kann die NAT-Funktionalität der Verbindungstabellen der Firewall überantwortet werden. Die Prüfung der Paketinhalte muss durch eine Firewall in Verbindung mit einem Intrusion Prevention System erfolgen. Der letzte Grund, NAT einzusetzen, besteht also in der Adressknappheit von IPv4, die mit IPv6 aufgehoben wird.

Netzwerk ohne NAT?

Die Antwort ist: ja! Ohne NAT bekommen alle Arbeitsplätze und Server im Unternehmen öffentliche IPv6-Adressen zugewiesen. Die Firewall schützt das Netzwerk auch mit öffentlichen Adressen. Aber ohne NAT können zwei Rechner direkten Kontakt miteinander aufnehmen, ohne dass dabei ein Mittler notwendig ist. So wären z.B. Dienste wie Videotelefonie, heute gerne über Skype gemacht, ohne zentralen Server eines Anbieters möglich.

Es gibt immer wieder Diskussionen, dass Staaten an zentralen Servern die Kommunikation überwachen und mitverfolgen wollen. Oft wird eine Verschlüsselung zwischen jedem der beiden Kommuni-

kationspartner und dem zentralen Server hergestellt, aber nicht von Ende zu Ende direkt zwischen den beiden Kommunikationspartnern. Daher ergibt sich am zentralen Server ein ganz natürlicher Punkt, an dem die ausgetauschten Nachrichten unverschlüsselt mitgelesen werden können. Die Diskussion um die Blackberry-Server, die einige arabische Staaten lokal im eigenen Land betreiben wollen[9], hat genau diese Gefahr des Servers in der Mitte gezeigt.

Wenn die beiden Rechner, die miteinander kommunizieren wollen, durch IPv6-Adressen eindeutig zu erkennen sind, lässt sich mit Hilfe von Firewallregeln die Kommunikation sogar besser absichern als es heute möglich ist. Öffentliche IP-Adressen, richtig eingesetzt, erhöhen die Sicherheit sogar.

Techniken für den Übergang

Solange IPv6 nicht flächendeckend zur Verfügung steht, wird es Bedarf an Übergangstechniken geben, die IPv6-Inseln miteinander verbinden. Ähnliche Techniken werden in einigen Jahren die verbleibenden IPv4-Inseln untereinander erreichbar machen.

NAT64

Bei NAT64 wird ein IPv6-Datenpaket in ein IPv4-Datenpaket übersetzt. Dabei geht der IPv6-Datenpaketheader verloren. Und da die Struktur des IPv6-Headers sich vom IPv4-Header unterscheidet, muss bei dieser Umschreibung zwangsläufig Information verloren gehen. Im Gegensatz zum Tunnel wird das IPv6-Datenpaket am Ende der Reise auch nicht wieder in ein IPv6-Datenpacket zurückverwandelt.

Mit Hilfe von NAT64 können Benutzer aus der reinen IPv6-Welt IPv4-Webseiten aufrufen. Besser ist natürlich die Bereitstellung von originären IPv6-Diensten, so dass die Datenpakete des Besuchers nicht durch ein Gateway laufen müssen.

Tunnel mit GRE und MPLS

Als Tunnel bezeichnet man die Verpackung (Kapselung) von IP-Datenpaketen in andere IP-Datenpakete. Auf diese Weise kann IPv6 als Nutzdatenanteil in einem IPv4-Paket „mitreisen“. Verbreitete Technologien zum Aufbau von Tunneln über Virtual Private Networks (VPNs) sind heute das von der Firma Cisco entwickelte Generic Routing Encapsulation Protokoll (GRE) oder das Multilabel Protocol Switching (MLPS). Problematisch wird dabei generell die gestiegene Paketgröße (der IPv4-Header kommt hinzu), die eine Fragmentierung der ursprünglichen Datenpakete wahrscheinlich macht. Das mindert Geschwindigkeit und Durchsatz der Verbindung. Aber es ist eine gute und schnelle Art, IPv6 ohne größere Verluste zu tunneln.

So wie IPv4-MPLS-VPNs im Internet heute normal sind, kann natürlich auch IPv6 mit Hilfe von MPLS über IPv4 transportiert werden. Dabei wird einem IPV6 Paket ein 20 Bytes großes Label vorangestellt, dass die Transportinformation über das Netzwerk enthält. Daher muss ein IPv4-Router nur das Label auswerten und muss nicht die IPv6-Adresse lesen.

[9] http://tra.ae/news_TRA_Announces_the_Suspension_of_Blackberry_Messenger,_Blackberry_E_mail_and_-180-1.php, 11. Oktober 2010

6to4-Tunnel

6to4-Tunnel werden automatisch aufgebaut, da eine IPv4-Adresse in eine IPv6-Adresse hineinkodiert wird. Der 6to4-Router nimmt die IPv4-Adresse, an der das nächste 6to4-Gateway zu finden ist, aus der IPv6-Adresse und schickt die Daten zum richtigen Ziel.

Teredo

Teredo wurde von Microsoft erfunden und in RFC 4380 als Standard festgelegt. Teredo ist der lateinische Name eines Schiffsbohrwurms, der Löcher (Tunnel) in Firewalls „bohrt“. In eine IPv6-Adresse wird die Adresse eines Relay-Gateways geschrieben, der bei der Weiterleitung des Paketes hilft. Teredo verbindet wie 6to4 automatisch IPv6-Inseln über IPv4.

9. Parallelbetrieb IPv6 und IPv4

Der Parallelbetrieb ist nicht problemfrei und auch nicht kostenfrei. Viele Dinge müssen doppelt erledigt werden, doppelt dokumentiert und doppelt gelernt werden.

Netzwerkhardware

Alle Router und Switches müssen beide Protokolle IPv4 und IPv6 in Hardware unterstützen. Eine reine Softwareunterstützung reicht nicht aus, da bei steigendem IPv6-Datenverkehr Probleme mit der Geschwindigkeit zu erwarten sind.

Die Hersteller dieser Geräte müssen die Hardware für beide Protokolle auslegen. Das kostet schon beim Entwurf viel Geld, und auch die Herstellung ist teuer, denn es muss z.B. mehr Hauptspeicher eingebaut werden, um die Routen beider Protokolle im Hauptspeicher halten zu können. Diese Kosten werden auf die Kunden umgelegt werden.

Die Software, die auf den Netzgeräten läuft, muss ebenfalls für beide Protokolle ausgelegt sein. Nicht alle Features können 1:1 von IPv4 nach IPv6 umgesetzt werden, da sich die beiden Protokolle unterscheiden. Aber im Grundsatz sollten alle Funktionen in beiden Protokollen unterstützt werden.

Sicherheit

Jede Firewallregel, jeder Zugriff auf Datenbanken, der IP-gesteuert erfolgt, und jede weitere Sicherheitseinstellung muss für beide Protokolle, IPv4 und IPv6, angelegt und gepflegt werden. Dabei werden Fehler gemacht, oder ein Protokoll wird vergessen. Auch Administratoren sind Menschen, die in der Arbeit unterbrochen werden und dann Fehler machen. Dabei ist zu beachten, dass die Firewallregeln für IPv4 und IPv6 ähnlich sind, aber nicht gleich, da beide Protokolle an einigen Stellen sehr unterschiedlich sind. Auch das ist eine Quelle für Fehler.

Wenn das Unternehmen eine „Security Policy“ erarbeitet hat, muss diese um IPv6 ergänzt werden. Auch dabei sind die Unterschiede der beiden Protokolle zu beachten, da eine zu allgemeine Vorschrift den Einsatz eines der beiden Protokolle ungewollt verbieten könnte.

Training

Die Netzwerkadministratoren und Softwareentwickler in einem Unternehmen müssen sowohl IPv4 als auch IPv6 beherrschen. Heute gibt es noch einen Mangel an in IPv6 geschultem Personal, aber das wird sich ändern, wenn IPv6 häufiger eingesetzt wird und auch die Universitäten und Fachschulen IPv6 verstärkt lehren. Und es wird der Zeitpunkt kommen, wo IPv4 aus den allgemeinen Vorlesungen und Lehrplänen verschwinden wird. Dann werden die Unternehmen, die noch IPv4 nutzen, die Mitarbeiter auf das alte Protokoll schulen müssen.

Aber heute gilt es erst einmal, den Netzwerkadministratoren Zeit und Schulung zu gewähren, um sich mit IPv6 und den Unterschieden zu IPv4 vertraut zu machen. Es gilt, die Sicherheitseinstellungen für beide Protokolle zu implementieren, das interne Routing für beide Protokolle einzurichten, die Dokumentation für beide Protokolle zu erstellen etc.

Support

Mitarbeiterin: „Ich kann nicht drucken.“

Support: „Drucken Sie über IPv4 oder IPv6?“

Mitarbeiterin: „IPv was?“

So oder ähnlich könnte ein Gespräch in Zukunft laufen. Bevor den Mitarbeitern geholfen werden kann, muss der Support feststellen, welches der beiden IP-Protokolle der Anwender nutzt. Und gerade in einer Migrationsphase ist das nicht immer klar. Somit wird der Support für die Kunden oder Kollegen aufwändiger und teurer.

Netzwerküberwachung

Ohne eine gute Überwachung des Netzwerkes sind die Administratoren blind, wenn Fehler gesucht werden müssen. Die Netzwerküberwachung muss also zukünftig nicht nur die Datenmengen ermitteln, die durch ein Interface laufen, sondern auch eine Aufteilung der Datenmenge nach IPv4 und IPv6 vornehmen. Wenn die Hardware keine getrennten Zähler anbietet, wird das schwierig. Aber es gibt noch andere Möglichkeiten, z.B. Netflow, um die Daten zu erheben. Angriffe können nur sinnvoll bekämpft werden, wenn bekannt ist, über welches der beiden Protokolle, oder beide Protokolle zugleich, der Angriff vorgetragen wird.

Eine genaue Analyse der Netzüberwachung ist nötig. Gerade die Neujustierung von Schwellenwerten, ab denen ein Alarm ausgelöst wird, benötigt Zeit. Und wenn in den nächsten Jahren der IPv6 Verkehr zunimmt und IPv4 verdrängt, müssen die Schwellenwerte eventuell laufend neu ermittelt werden.

Partner

Genau wie das Unternehmen müssen auch die Partner beide Protokolle beherrschen. Das gilt in erster Linie für die IT-Unternehmen, die als Lieferanten und Berater Dienste anbieten. Wenn der langjährige Partner IPv6 nicht beherrscht, muss ein Unternehmen, das IPv6 benötigt, vielleicht den Partner wechseln, was bei langfristigen Verträgen oftmals nicht einfach ist.

Aber auch der Rechtsanwalt des Unternehmens muss über Probleme beim Datenschutz bei beiden Protokolle IPv4 und IPv6 Auskunft geben können. Das könnte problematisch werden oder Zeit brauchen.

10. Betrachtungen zum Datenschutz

Das Thema Datenschutz ist in letzter Zeit viel in der Presse diskutiert worden. Es gibt die Befürchtung, dass der Nutzer anhand seiner IPv6-Adresse dauerhaft und weltweit identifiziert werden kann. Wenn es kein Verstecken mehr hinter einem NAT-Gateway gibt, ist der Nutzer tatsächlich mit der öffentlichen Adresse im Internet sichtbar.

Da das Thema Datenschutz wichtig ist, sollten die Unternehmen es mit dem Betriebsrat besprechen und eventuell die Rechtsabteilung und den Datenschutzbeauftragten des Unternehmens hinzuziehen.

Adressaufbau

Um die Diskussion auf ihren Kern zu führen, muss der Aufbau einer Adresse verstanden werden. Technische Feinheiten sollen hier außen vor bleiben.

Die 128 Bits der IPv6-Adresse werden gedanklich in zwei Teile aufgeteilt. Die ersten 64 Bits bilden den Netzanteil, die hinteren 64 Bits den Hostanteil der Adresse.

Abbildung 6: Netzanteil und Hostanteil der 128 Bits langen IPv6-Adresse

Der Netzanteil ist für alle User im Netzwerksegment gleich. So werden einem Unternehmen vom Provider ca. 65.500 zusammenhängende "Netzwerkanteile" zugewiesen, ein Netz für 65.500 Teilnetze. In jedem Netzwerksegment wird dem Host mitgeteilt, welches Netzwerk genutzt werden kann. Den Hostanteil der Adresse baut der Client selber zusammen, sofern keine statische Konfiguration vorgenommen wird.

Jede Netzwerkkarte, mit der ein netzwerkfähiges Gerät an das Netzwerk angeschlossen wird, hat eine weltweit einmalige (Hardware-)Kennung eingebrannt (MAC Adresse), die für die Kommunikation im lokalen Netzwerk benötigt wird. Normalerweise verlässt diese Information das lokale Netzwerk nicht, ist also für den Datenschutz kein Problem.

Aber in IPv6 wird diese 48 Bits lange Hardwarekennung in den 64 Bit-Hostanteil der Adresse hineinkodiert (vgl. ‚Abbildung 7, “fffe“ kommt dabei in die Mitte der MAC-Adresse, um von 48 Bits auf 64 Bits zu kommen. Ein Schritt wurde weggelassen, es geht nur um das Schema)

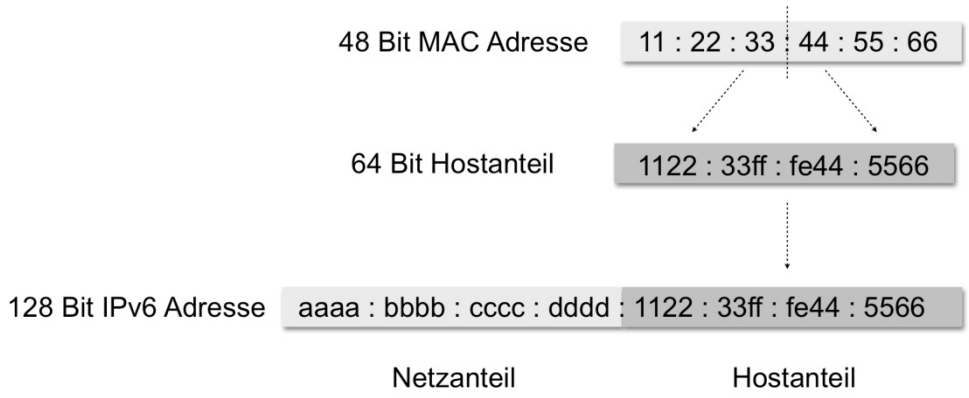

Abbildung 7: Automatische IPv6-Adressgenerierung aus Hardwareadressen

Diese Adresse ist in der Tat immer erkennbar und identifiziert das Gerät, an dem der Nutzer arbeitet, sehr gut. Da sich die eingebrannte MAC-Adresse in der Netzwerkkarte nicht ändert, wird bei jedem Neustart des Gerätes die gleiche IPv6-Adresse errechnet und dann genutzt.

Privacy Extensions

Um die Erkennbarkeit von IPv6-Adressen zu erschweren- wurden die IPv6 Privacy Extensions erfunden. Hierbei wird der Hostanteil der Adresse zufällig gebildet. Da es theoretisch zu einer doppelten Vergabe der Adresse kommen könnte, auch wenn die Wahrscheinlichkeit gering ist, wird eine Prüfung auf doppelte Adressen vorgenommen.

Die Adresse ist so weder weltweit noch hausintern wiederzuerkennen. Der Vorteil im globalen Netz wird mit der Anonymität im Unternehmensnetz erkauft, die aus Sicherheitsgründen eventuell nicht gewünscht ist.

Anforderungen an die Sicherheit

Die IP-Adresse, egal ob IPv6 oder IPv4, wird oft für die Gewährung oder die Verweigerung eines Zugriffes auf eine Ressource im Netzwerk genutzt. Wenn die Adresse eines Rechners sich täglich, eventuell noch öfter, ändert, ist dieser Mechanismus nicht mehr brauchbar. Aus Sicht der Netzwerksicherheit sind feste Adressen wünschenswert.

Dem steht das berechtigte Bedürfnis der Mitarbeiter nach Datenschutz gegenüber. Wie der Konflikt gelöst wird, muss jedes Unternehmen selbst bestimmen, aber es gibt Wege, die hier beschrieben werden sollen.

Zertifikate

Wenn der Zugriff auf Ressourcen nicht von der IP-Adresse abhängt, wäre die Nutzung wechselnder IPv6-Adressen unproblematisch. Es ist so oder so besser, den Benutzer anhand von Zertifikaten oder Passworten zu erkennen, als einen Computer anhand seiner IP-Adresse zu authentifizieren. Denn selbst wenn die IP-Adresse die richtige ist, kann der Benutzer vor dem Bildschirm der falsche Benutzer sein. Sollte der Rechner von einem Virus infiziert sein, bringt die IP-Adresse als Identifikationselement keine Sicherheit, sondern öffnet sogar dem Missbrauch Tür und Tor.

Mehrere Adressen

Das IPv6-Protokoll kennt das Konzept mehrerer IPv6-Adressen für jedes Interface, auch aus verschiedenen Netzwerken. Wenn die Adressen für die interne Kommunikation statisch vergeben oder aus

der MAC-Adresse gebildet werden können, wäre der internen Sicherheit genüge getan. Für den Zugriff auf das Internet könnte dann eine wechselnde IPv6-Adresse konfiguriert werden, welche die Erkennbarkeit im Internet schwerer macht.

11. Abschaltung von IPv4

Ziel der Einführung von IPv6 ist die Abschaltung von IPv4. Es wird oft von der Umstellung auf IPv6 gesprochen. Das ist allerdings das Ende des Prozesses. Heute wird der Parallelbetrieb gestartet, der auch eine ganze Weile anhalten wird. Aber je schneller IPv6 von den Unternehmen eingeführt wird, umso schneller kann IPv6 reifen und auch die letzen IPv4-Inseln können verschwinden.

Für die Abschaltung von IPv4 sprechen einige gewichtige Gründe. Aber zunächst müssen viele Voraussetzungen erfüllt sein, bevor überhaupt über die Abschaltung von IPv4 nachgedacht werden kann. Bis dahin müssen sich die Unternehmen und Administratoren mit dem aufwändigen Parallelbetrieb anfreunden.

Voraussetzungen für IPv4-Abschaltung

Der Tag, an dem kein IPv4-Datenpaket mehr durch die Weiten des Internet fließt, könnte der Tag der IPv4-Abschaltung sein. Aber das wird dauern. Es gibt viele Voraussetzungen für die Abschaltung von IPv4, die erst einmal erfüllt sein wollen.

Alle Netzwerke laufen auf IPv6 oder im Parallelbetrieb

Das wird sicher nie passieren, denn es gibt immer irgendwo Netze, die nicht angefasst werden. Und es wird immer Provider geben, die noch IPv4 unterstützen, denn die Kunden, die es noch lange benötigen, werden viel Geld dafür ausgeben, dass ihnen IPv4 nicht genommen wird. Die Provider werden über Tunnel und NAT diesen Kunden weiterhin IPv4 Dienste anbieten.

Die Voraussetzung wird also nie vollständig umzusetzen sein, aber wenn eine hinreichende IPv6-Abdeckung vorhanden ist, kann die Voraussetzung als erfüllt gelten.

Alle Anwendungen unterstützen IPv6

Auch diese Bedingung wird sich nicht vollständig erfüllen lassen, denn viele Unternehmen haben sehr alte Anwendungen, die niemals mit IPv6 laufen werden. Unternehmen, die diese Anwendungen nutzen, werden wohl oder übel IPv4 weiterhin einsetzen müssen und, sofern die Anwendungen aus dem Internet heraus erreichbar sein sollen, von IPv6 auf IPv4 umsetzen. Das kostet Geld und bringt Fehlerquellen ins Netz, ist aber vielleicht ohne Alternative.

Auch diese Voraussetzung wird also nie vollständig umzusetzen sein, aber (siehe oben): Wenn eine hinreichende IPv6-Abdeckung vorhanden ist, kann die Voraussetzung als erfüllt gelten.

IPv6 ist so sicher wie IPv4

IPv6 muss sich im harten Tagesbetrieb noch bewähren, bevor es so sicher ist wie IPv4. Aber auch IPv4 hat Schwachstellen. An den Sicherheitslücken in Applikationen ändert sich mit IPv6 nichts, da IPv6 nur den Transport neu regelt, nicht aber die Inhalte der Pakete verändert.

Die Reife im Tagesbetrieb gibt es nur im Tagesbetrieb, und jedes Unternehmen muss für sich und sein Netzwerk selber feststellen und festlegen, wie IPv6 eingeführt wird. Es nutzt nichts, erst einmal alle anderen vorangehen zu lassen und abzuwarten. Lernen wird das Unternehmen nur durch „Selbermachen“.

Zeitrahmen

Das ist eine schwierige Frage, die zu beantworten heute nicht möglich ist.

Der Parallelbetrieb wird sicher zehn Jahre anhalten. Dann sollte IPv4 soweit zurückgedrängt sein, dass Unternehmen IPv4 abschalten und vollständig auf IPv6 setzen. Manche Prognosen liegen aber bei 20 bis 25 Jahren, ehe IPv4 abgeschaltet werden kann. Die Entscheidung treffen die Kaufleute im Unternehmen, denen der Parallelbetrieb irgendwann zu teuer werden wird.

12. Glossar

Autokonfiguration:
Bezeichnung für die in IPv6 durchgeführte automatische Ermittlung der IP-Adresse für ein netzwerkfähiges Gerät. Mit Hilfe der Stateless Address Autoconfiguration (SLAAC, zustandslose Adressenautokonfiguration) kann ein netzwerkfähiges Gerät automatisch eine funktionsfähige Netzwerkverbindung auf der Internetschicht aufbauen. Dazu kommuniziert das Gerät mit den Routern, die für das betreffende Netzwerksegment zuständig sind, um die zur Konfiguration notwendigen Parameter zu ermitteln.

Autonomes System:
Bezeichnung für eine Menge von Teilnetzen und Rechensystemen, die unter der Kontrolle eines einzelnen Betreibers stehen und ein gemeinsames Routing-Verfahren benutzen. Das Routing-Verfahren innerhalb eines autonomen Systems wird als Interior Gateway Protocol (IGP) bezeichnet. Das Routing-Verfahren zwischen verschiedenen autonomen Systemen dagegen als Exterior Gateway Protocol (EGP).

AS-Nummer (ASN):
Jedem autonomen System wird eine eindeutige, 32-Bits lange AS-Nummer (Autonomous System Number, ASN) zugewiesen. Die Verwaltung der ASN übernimmt die Internet Assigned Numbers Authority (IANA), welche die Zuteilung weiter an die Regional Internet Registries (RIR) delegiert. Um eine ASN zu erhalten, muss ein ISP mit mindestens zwei anderen autonomen Systemen ein dynamisches Routingprotokoll (BGP) verwenden.

Backbone:
Als Backbone wird der Zusammenschluss von Netzwerken bezeichnet, die gemeinsam über eine besonders hohe Übertragungskapazität und Bandbreite verfügen. Ein Backbone dient als Ausgangspunkt für den Anschluss eigener Netze an das Internet. Diese verfügen in der Regel über eine geringere Kapazität und teilen sich die Ressourcen des Backbones mit anderen daran angeschlossenen Netzen.

Border Gateway Protocol (BGP4):
Das Border Gateway Protocol (BGP) implementiert ein Provider übergreifendes Routingprotokoll, das einzelne ISP-Netzwerke (Autonome Systeme) miteinander verbindet. Es zählt zu den Exterior Gateway Protokollen (EGP) und beschreibt, wie Router untereinander die Verfügbarkeit von Verbindungswegen zwischen den autonomen Systemen weitergeben.

Firewall:
Als Firewall bezeichnet man eine Netzwerkkomponente in einem Unternehmensnetz, über das dieses an das globale Internet angekoppelt ist und das spezielle Schutz- und Filterungsmaßnahmen ausführt, um die Sicherheitsinteressen des Unternehmensnetzwerks zu gewährleisten. Dabei soll ein möglichst ungestörter Zugriff der unternehmensinternen Nutzer auf das globale Internet möglich sein, während das Unternehmensnetzwerk selbst vor Übergriffen unberechtigter Dritter aus dem Internet geschützt wird.

Gateway:
Zwischensystem im Netzwerk, das in der Lage ist, einzelne Netzwerke zu einem neuen System zu verbinden. Gateways ermöglichen die Kommunikation zwischen Anwendungsprogrammen auf unterschiedlichen Endsystemen und sind in der Anwendungsschicht des Kommunikationsprotokollmodells angesiedelt. Daher sind sie in der Lage, unterschiedliche Anwendungsprotokolle ineinander zu übersetzen.

Internet Protocol (IP, genauer IPv4 oder IPv6):
Protokoll auf der Netzwerkschicht des TCP/IP-Referenzmodells. Als einer der Grundpfeiler des Internets sorgt IP dafür, dass ein aus vielen heterogenen Einzelnetzwerken bestehendes Internet als einheitliches, homogenes Netzwerk erscheint. Ein einheitliches Adressierungsschema (IP-Adressen) sorgt für eine von der jeweiligen Netzwerktechnologie unabhängige, eindeutige Rechneridentifikation. IP stellt einen verbindungslosen, paketvermittelten Datagrammdienst bereit, der keine Dienstgüte-Garantien erfüllen kann, sondern stets nach dem Best-Effort-Prinzip arbeitet. Zur Kommunikation von Steuerungsinformation und Fehlermeldungen dient das ICMP-Protokoll (ICMPv4 bzw. ICMPv6) als integraler Bestandteil von IP.

Internet Service Provider (ISP):
ISPs sind Anbieter von Diensten, Inhalten oder technischen Leistungen, die für die Nutzung oder den Betrieb von Inhalten und Diensten im Internet erforderlich sind. Zu diesen Leistungen zählen unter anderem die Bereitstellung der Internet-Konnektivität, d.h. der Transfer von IP-Datenpaketen und das Hosting (Zurverfügungstellen) verschiedener Dienste und Anwendungen, wie z.B. die Namens- und Adressübersetzung (DNS), E-Mail oder Webhosting-Dienste.

IP-Security (IPsec):
Als IP-Security (IPsec) wird eine Familie von Protokollstandards bezeichnet, die von der IP Security Working Group der IETF entwickelt wurde und eine umfassende Sicherheitsarchitektur für IP-basierte Netzwerke bietet. Die darin zusammengefassten Technologien beschreiben Verfahren zur Verschlüsselung und Authentifizierung von IP-Datenpaketen.

Network Address Translation (NAT):
Die NAT-Technologie ermöglicht es, über eine kleine Zahl öffentlicher IPv4-Adressen unter Nutzung eines privaten IPv4-Adressraums eine wesentlich größere Zahl von Rechnern in einem gemeinsamen Netzwerk dynamisch mit dem Internet zu verbinden. Dabei bleiben die in einem NAT-Netzwerk betriebenen Geräte öffentlich über das Internet erreichbar, obwohl diese nicht über eine eigene öffentliche IP-Adresse verfügen und nur über ein entsprechendes NAT-Gateway erreicht werden können.

Provider Independent Address Space (PI Netz):
Als PI-Adressraum werden Blöcke von Internet-Protokoll-Adressen bezeichnet, die von einer Regional Internet Registry (RIR) direkt an einen Endnutzer vergeben werden, ohne noch von einem Internetdienstanbieter für die Adressvergabe abhängig zu sein. Dies bietet dem Inhaber eines PI-Netzes die Möglichkeit, den Provider zu wechseln, ohne die zugewiesenen IP-Adressen ändern zu müssen, oder sogar mehrere Provider gleichzeitig nutzen zu können.

Provider Aggretable Address Space (PA Netz):
Als PA-Adressraum werden Internet-Protokoll-Adressen bezeichnet, die von einer Regional Internet Registry (RIR) an eine Local Internet Registry (LIR) vergeben werden, die diese weiter in kleinere Netze aufteilt und an ihre Kunden weitergibt. Z.B. erwirbt ein kleinerer Internet Service Provider eine Anbindung (upstream) zu weiteren Teilnehmernetzwerken bei einem LIR und erhält von diesem in begründeten Fällen auch PA-IP-Adressen, wenn er nicht selbst über eigene PI-Adressen verfügt. Dies kann zu Schwierigkeiten führen, wenn mehrere Internetanbindungen genutzt werden sollen oder der Upstreamanbieter gewechselt werden soll, da die PA-IP-Adressen beim LIR verbleiben und zurückgegeben werden müssen.

RIPE:
Das 1992 als Non-Profit Organisation gegründete Réseaux IP Européens Network Coordination Centre (RIPE NCC) mit Sitz in Amsterdam ist eine Regional Internet Registry (RIR), zuständig für die Vergabe von IP-Adressbereichen und AS-Nummern in Europa, dem Nahen Osten und Zentralasien.

Router:
Vermittlungsrechner, der in der Lage ist, zwei oder mehrere Teilnetze miteinander zu verbinden. Router arbeiten in der Transportschicht (IP-Layer) des Netzwerks und sind in der Lage, ankommende Datenpakete gemäß ihrer Zieladresse auf der kürzesten Route durch das Netzwerk weiterzuleiten.

Routing:
In einem Internet liegen entlang des Weges zwischen Sender und Empfänger oft mehrere Zwischensysteme (Router), die sich um die Weiterleitung der versendeten Daten an den jeweils nächsten Router auf dem Weg zum jeweiligen Empfänger kümmern. Die Ermittlung der Wegstrecke vom Sender zum Empfänger wird dabei als Routing bezeichnet. Die Router empfangen ein versendetes Datenpaket, werten dessen Adressinformation aus und leiten es entsprechend zum nächsten Router bzw. schließlich zum Empfänger weiter.

Uplink:
Als Uplink wird im Rahmen dieses Dokuments der (gerichtete) Anschluss des eigenen, lokalen Netzwerks bzw. eines Endgeräts an das weltweite Internet bezeichnet.

Virtual Private Network (VPN):
Ein Virtual Private Network ermöglicht es, über eine verschlüsselte Verbindung einzelne Rechner oder Netzwerke so mit einem vom Internet aus nicht direkt "sichtbaren" Intranet zu verbinden, dass die Benutzer des VPNs den Eindruck haben, der jeweilige Rechner bzw. das entfernte Netzwerk befände sich innerhalb des privaten Netzwerks. Heimarbeitsplätze können auf diese Weise ins Unternehmensnetzwerk integriert werden, so dass es für den Mitarbeiter in Hinsicht auf die Netzwerkfunktionen keinen Unterschied mehr macht, ob er sich im Unternehmen oder an einem anderen Ort aufhält.

13. Literatur

Deutscher IPv6 Rat: *Nationaler IPv6 Aktionsplan für Deutschland*, Potsdam, 15.9.2009, verfügbar unter http://www.ipv6council.de/fileadmin/summit09/Aktionsplan.pdf

Ch. Meinel, H. Sack*: Internetworking – Technische Grundlagen und Anwendungen*, Springer, Heidelberg, Berlin, New York, 2011.

Ch. Meinel, H. Sack: *Digitale Kommunikation – Vernetzen, Multimedia, Sicherheit*, Springer, Heidelberg, Berlin, New York, 2009.

Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear: *Address Allocation for Private Internets, RFC 1918*, Internet Engineering Task Force, 1996.

C. Huitema: *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)*. RFC 4380, Internet Engineering Task Force, 2006.

L. E. Hughes: *The Second Internet, Reinventing Computer Networking with IPv6*, 2010, verfügbar unter http://www.ipv6forum.com/dl/books/the_second_internet.pdf

S. Frankel, R. Graveman, J. Pearce, M. Rooks: *Guidelines for the Secure Deployment of IPv6*, Recommendations of the National Institute of Standards and Technology, Special Publication 800-119, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2010,
verfügbar unter http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

J. Zorz, S. Steffann; *Requirements for IPv6 in ICT Equipement*, RIPE Best Current Practice Document RIPE-501, 2010, verfügbar unter http://www.ripe.net/ripe/docs/ripe-501

14. Webseiten

Deutscher IPv6 Rat: http://www.ipv6council.de/

Aktuelle Technische Berichte des Hasso-Plattner-Instituts

Band	ISBN	Titel	Autoren / Redaktion
51	978-3-86956-148-6	**Advancing the Discovery of Unique Column Combinations**	Ziawasch Abedjan, Felix Naumann
50	978-3-86956-144-8	**Data in Business Processes**	Andreas Meyer, Sergey Smirnov, Mathias Weske
49	978-3-86956-143-1	**Adaptive Windows for Duplicate Detection**	Uwe Draisbach, Felix Naumann, Sascha Szott, Oliver Wonneberg
48	978-3-86956-134-9	**CSOM/PL: A Virtual Machine Product Line**	Michael Haupt, Stefan Marr, Robert Hirschfeld
47	978-3-86956-130-1	**State Propagation in Abstracted Business Processes**	Sergey Smirnov, Armin Zamani Farahani, Mathias Weske
46	978-3-86956-129-5	**Proceedings of the 5th Ph.D. Retreat of the HPI Research School on Service-oriented Systems Engineering**	Hrsg. von den Professoren des HPI
45	978-3-86956-128-8	**Survey on Healthcare IT systems: Standards, Regulations and Security**	Christian Neuhaus, Andreas Polze, Mohammad M. R. Chowdhuryy
44	978-3-86956-113-4	**Virtualisierung und Cloud Computing: Konzepte, Technologiestudie, Marktübersicht**	Christoph Meinel, Christian Willems, Sebastian Roschke, Maxim Schnjakin
43	978-3-86956-110-3	**SOA-Security 2010 : Symposium für Sicherheit in Service-orientierten Architekturen ; 28. / 29. Oktober 2010 am Hasso-Plattner-Institut**	Christoph Meinel, Ivonne Thomas, Robert Warschofsky et al.
42	978-3-86956-114-1	**Proceedings of the Fall 2010 Future SOC Lab Day**	Hrsg. von Christoph Meinel, Andreas Polze, Alexander Zeier et al.
41	978-3-86956-108-0	**The effect of tangible media on individuals in business process modeling: A controlled experiment**	Alexander Lübbe
40	978-3-86956-106-6	**Selected Papers of the International Workshop on Smalltalk Technologies (IWST'10)**	Hrsg. von Michael Haupt, Robert Hirschfeld
39	978-3-86956-092-2	**Dritter Deutscher IPv6 Gipfel 2010**	Hrsg. von Christoph Meinel und Harald Sack
38	978-3-86956-081-6	**Extracting Structured Information from Wikipedia Articles to Populate Infoboxes**	Dustin Lange, Christoph Böhm, Felix Naumann
37	978-3-86956-078-6	**Toward Bridging the Gap Between Formal Semantics and Implementation of Triple Graph Grammars**	Holger Giese, Stephan Hildebrandt, Leen Lambers
36	978-3-86956-065-6	**Pattern Matching for an Object-oriented and Dynamically Typed Programming Language**	Felix Geller, Robert Hirschfeld, Gilad Bracha
35	978-3-86956-054-0	**Business Process Model Abstraction : Theory and Practice**	Sergey Smirnov, Hajo A. Reijers, Thijs Nugteren, Mathias Weske

ISBN 978-3-86956-156-1
ISSN 1613-5652