

Warum IPv6 alle etwas angeht

von Michel Chappuis, Adrian Schmidlin und Urs Haug

Geschichtliches

Bereits anfangs der 90-iger Jahre hat die Internet Engineering Task Force (IETF) erkannt, dass der Adressraum, den die Version 4 des Internet Protokolls (IPv4) zur Verfügung stellt, niemals ausreichen wird, um in Zukunft alle über IP ansprechbaren Netzknoten und Endgeräte zu adressieren. Deshalb wurde sehr bald mit der Entwicklung einer neuen Version des IP-Protokolls begonnen. Nach zähem Ringen um die Ausprägung des neuen Protokolls innerhalb der Gremien wurde 1998 das erste Standardpapier (RFC 2460) ratifiziert, welches das neue Protokoll unter dem Namen IP Version 6 (IPv6) definierte. Dies war allerdings erst der Grundstein. Viele weitere Standards für unterstützende Funktionen und Implementationsrichtlinien (DNS, DHCP, Adress-Architektur usw.) folgten erst nach und nach.

Mit IPv6 wurde der Adressraum von 4 Milliarden Adressen auf 34×10^{37} Adressen erweitert. Theoretisch könnten damit pro Quadratmillimeter Erdoberfläche (inkl. Meeresoberfläche) 667 Billionen Knoten adressiert werden. Im Wissen, dass nicht alle Adressen eines Adressraumes nutzbar sind, und auch angesichts der kühnsten Wachstumsprognosen, sollte dies für die vorhersehbare Zukunft genügen.

In Anbetracht der drohenden IPv4 Adressknappheit sowie der eher schleppenden Entwicklung und Umsetzung von IPv6 wurden innerhalb von IPv4 andere Ansätze wie Network Address Translation (NAT) und der Mehrfachgebrauch von IPv4 Adressen (private Adressen, RFC 1918) entwickelt und eingesetzt. Durch diesen Mehrfachgebrauch von definierten Adressbereichen, konnte die drohende Adressknappheit wenigstens vorübergehend entschärft werden. Ebenso wurde IPv4 mit Neuerungen aus IPv6 ergänzt (IPsec) und laufend verbessert.

Die Situation heute

Getrieben durch den global anhaltenden Trend zur Vernetzung von immer mehr Geräten (PCs, Laptops, Mobiltelefone, Smartphones, Navigationsgeräte, Sensoren, Prozesssteuerungen, Haustechnik, usw.) im privaten wie auch im geschäftlichen Umfeld, steigt der Bedarf an neuen IP Adressen ununterbrochen. Es liegt deshalb auf der Hand, dass es nur eine Frage der Zeit ist, bis definitiv die letzten öffentlichen IPv4 Adressen vergeben sein werden. Experten schätzen, dass dies etwa 2011 bis 2012 der Fall sein wird (siehe z.B. <http://ipv4.potaroo.net>). Das heisst, dass wir

heute wieder am gleichen Punkt stehen, wie vor etwas mehr als zehn Jahren: Um die globalen Netzwerke weiter ausbauen und skalieren zu können, benötigen wir viel mehr Adressraum. Es zeigt sich auch, dass der weit verbreitete Einsatz von NAT zwar manch einem Sicherheitsverantwortlichen ans Herz gewachsen ist, diese aber der Skalierbarkeit und dem Einsatz von neuen peer-to-peer Applikationen, wie z.B. Unified Communications, nicht nur förderlich ist. Dies ist der Grund, weshalb IPv6 auch ausserhalb der Gilde der IPv6 Propheten wieder zum einem aktuellen Thema geworden ist.

Die Entwicklung von IPv6 ist in den vergangenen zehn Jahren nicht stehen geblieben. Viele Pilotprojekte wurden durchgeführt und erste Erfahrungen gesammelt. Die Standards und Implementationen wurden entsprechend angepasst und erweitert. Eine wichtige Rolle spielte sicher auch der Entscheid des amerikanischen Department of Defense (DOD) aus dem Jahre 2003, wonach alle vom DOD beschafften Geräte IPv6 tauglich sein müssen. Dies hat die Hersteller einem riesigen Druck ausgesetzt, IPv6 in ihre Produkte einzubauen. Nicht zuletzt deswegen unterstützen heute die meisten Netzwerkkomponenten aller namhaften Hersteller das IPv6 Protokoll. Ebenso unterstützen auch die Betriebssysteme der Rechnerplattformen (Unix, Linux, Solaris, MS Windows Server 2003, MS Windows XP, usw.) IPv6 schon seit einiger Zeit oder können mittels Service-Packs einfach dazu gebracht werden. In den letzten zwei Jahren hat Microsoft einen weiteren grossen Schritt Richtung globaler Einführung von IPv6 gemacht, indem IPv6 bei einer Standardinstallation von Windows Vista und Windows Server 2008 ein integraler Bestandteil der Konfiguration ist und auch automatisch aktiviert wird. Dies kann heute zu der unerwünschten Situation führen, dass Endgeräte innerhalb einer Broadcast Domain (LAN Segment resp. VLAN) untereinander via IPv6 kommunizieren (können), ohne dass Netzwerkverantwortliche etwas davon sehen respektive überhaupt davon wissen.

Die Vorteile von IPv6

Die wichtigste Verbesserung von IPv6 gegenüber der Version 4 ist, wie oben geschildert, der signifikant grössere Adressraum. In unzähligen Fachartikeln und technischen Publikationen ist immer wieder über die weiteren Vorteile von IPv6 geschrieben worden. Die Liste

at rete

der wichtigsten Erweiterungen und Verbesserungen umfasst:

- Vereinfachung des Header-Formates
- Größere Flexibilität für Protokollerweiterungen und Optionen
- Traffic Flow Label (Quality of Service)
- Integrierte Sicherheitsmechanismen als Komponente des Transport-Layers (IPSec)
- Autokonfiguration der Endgeräte
- und viele mehr

Bei einer genaueren Analyse stellt man allerdings rasch fest, dass die meisten dieser Funktionen in der Zwischenzeit als Erweiterungen von IPv4 implementiert worden oder mittels Zusatzlösungen auch für IPv4 einsetzbar sind.

Der Vorteil von IPv6 ist, dass alle diese Funktionalitäten direkt vom Protokoll unterstützt werden, was den Betrieb und die Kompatibilität der verschiedenen Produkte untereinander sicherlich verbessern kann. Dem gegenüber stehen aber die langjährige Erfahrung und das gewachsene Vertrauen in die heutigen Lösungen. Zum Beispiel wurde IPv6 so konzipiert, dass Endgeräte automatisch zu ihren IP-Adressen kommen können (Autokonfiguration). In der Praxis zeigt sich jetzt aber, dass heute dem Endgerät mittels DHCP weit mehr als nur seine IP-Adresse zugeteilt wird. Zum Beispiel können mit DHCP Informationen übermittelt werden, welche es Endgeräten erlauben, bei Systemstart spezifische Konfigurationsfiles herunterzuladen. Solche Hilfs-Funktionen und die Tatsache, dass mit DHCP alle aktiven Netzgeräte mit ihrer eindeutig zugeordneten IP-Adresse zentral erfasst sind, halten viele Netzwerkmanager davon ab auf DHCP zu verzichten und die IPv6 Autokonfigurations-Funktion zu nutzen.

Ein weiteres, oft angeführtes Argument für die Einführung von IPv6 ist die Tatsache, dass mit der Einführung von NAT in IPv4 die End-zu-end Erreichbarkeit verhindert wird, was dem ureigensten Ziel des IP-Protokolls widerspricht. Dies führt auch bei einigen Applikationen zu erheblichen Problemen. Auf der anderen Seite schläft wahrscheinlich doch manch ein Sicherheitsverantwortlicher besser bei dem Gedanken, dass die Endgeräte in seiner Firma a priori vom Internet aus nicht adressierbar und demzufolge auch nicht erreichbar sind.

Insgesamt wird offensichtlich, dass all diese Zusatzfunktionen von IPv6 wohl kaum als Treiber für eine rasche Ausbreitung des Protokolls wirken. Vielmehr öffnet sich hier ein Spannungsfeld von theoretischen Vorteilen und Nachteilen, welches erst durch konkrete Erfahrungen mit IPv6 im produktiven Einsatz beigelegt werden kann.

Schlussfolgerung

Leider ist es so, dass die in IPv6 enthaltenen Neuerungen allein zu wenig bieten, als dass eine Einführung von IPv6 aufgrund der erweiterten Funktionalitäten und anderer Verbesserungen ökonomisch zu rechtfertigen wäre. Aber trotzdem führt aus heutiger Sicht kein Weg an IPv6 vorbei. Früher oder später wird IPv6 eingesetzt werden müssen. Der Tag wird kommen an dem der letzte IPv4 Adressbereich vergeben sein wird und an dem Applikationen auf dem Markt erscheinen, welche IPv6 voraussetzen. Natürlich ist es so, dass IPv4 nicht über Nacht abgelöst werden wird. Unsere Business-Applikationen werden noch lange auf IPv4 laufen. Ebenso klar ist aber auch so, dass IPv6 nicht einfach über Nacht eingeschaltet werden kann, wenn dies plötzlich Business-relevant wird. Es wird eine lange Phase mit einer schleifenden Ablösung werden. Während dieser Zeit werden beide IP Versionen nebeneinander koexistieren. Eine Vielzahl von Techniken, welche diesen Parallelbetrieb ermöglichen, steht heute zur Verfügung.

Der Druck der mangelnden Adressen trifft die Service Provider am stärksten. Sie müssen die stetig wachsende Anzahl individueller Kommunikationsgeräte als auch Unternehmensnetze von tausenden von Kunden laufend mit neuen Adressen versorgen. Einige Service Provider sind heute bereits daran ihre eigenen Infrastrukturen auf IPv6 umzustellen, um so IPv4 Adressen zu sparen und um auf die neuen zukünftigen Anforderungen vorbereitet zu sein. Mittels Tunneling von IPv4 Verkehr durch IPv6 basierte Infrastrukturen werden sie in der Lage sein, ihren Kunden sowohl IPv4 als IPv6 Services anzubieten. Orange Business Services zum Beispiel bietet seit Mai 2009 erstmals global IPv6 Services für Unternehmen an. Es ist davon auszugehen, dass die Provider mit der Zeit für ihre Kunden Anreize schaffen werden, damit diese auf IPv6 migrieren. Einerseits um damit ihre Investitionen auszuschöpfen und die Betriebskosten gering zu halten aber andererseits auch weil mit der Zeit IPv4 Adressen Seltenheitswert bekommen werden.

Unternehmensnetze spüren den Druck der Adressknappheit viel weniger. Sie haben ihre Netze mittels NAT und privaten Adressen soweit gut im Griff. Nichtsdestotrotz sollten Netzwerkverantwortliche in Unternehmen sich bewusst sein, dass sie mit ihrem Schiff auf eine Stromschnelle zufahren. Jetzt ist noch Zeit da, um sich auf die unruhigeren Zeiten vorzubereiten. Wer das Wasser um sich aufmerksam beobachtet, wird feststellen, dass es nicht mehr so ruhig dahinfließt, sondern schon begonnen hat sich zu kräuseln. Wer nämlich keine strenge Weisung betreffend der

Ausbreitung von IPv6 im Netzwerk herausgegeben hat, wird feststellen, dass es in seinem Netzwerk schon eine stattliche Anzahl Endgeräte hat, welche IPv6 Pakete versenden. Solche Geräte können zum Beispiel die internen DNS-Server substantiell mit Anfragen für IPv6 Adressen (AAAA Records) beschäftigen, obwohl eigentlich gar keine Geräte mit IPv6 Adressen existieren. Auch wird sicher der Zeitpunkt kommen, wo bestimmte Hosts im Internet nicht mehr direkt via IPv4 erreichbar sein werden. Handlungsbedarf entsteht als sowohl innerhalb als auch ausserhalb des Unternehmens.

Netzwerkverantwortliche in Unternehmen sollten jetzt unbedingt das Ruder in die Hand nehmen und sich mit dem Thema IPv6 aktiv auseinandersetzen, ganz im Sinne eines Technologie Life-Cycle Management. Folgenden Fragen müssen sie sich in diesem Zusammenhang stellen:

- Wie gehe ich mit der Tatsache um, das immer mehr Endgeräte schon mit aktiviertem IPv6 Stack im Netz stehen? Was bedeutet dies für das Monitoring, Troubleshooting usw.? Wie sieht es mit dem Sicherheitskonzept aus?
- Wie gehe ich vor, wenn gewisse Sites im Internet nur noch über IPv6 erreicht werden können? Welche Tunneling Mechanismen stelle ich meine Benutzern dafür zur Verfügung?
- Genügt mein IP Adressierungskonzept den zukünftigen Anforderungen an Wachstum und Flexibilität? Die Wahrscheinlichkeit, noch zusätzliche öffentliche IPv4 Adressen zu erhalten ist verschwindend klein.

- Inwiefern ist die aktuelle Netzwerkinfrastruktur IPv6 fähig? Wo müsste noch ein Technologie Life-Cycle vollzogen werden? Wo fehlen noch IPv6 Funktionalitäten?
- Wie soll ein neues IPv6 Adressierungskonzept aussehen? Will man weiterhin auf private Adressen setzen? (ja, auch das gibt es in IPv6)
- Hat das Unternehmen schon IPv6 Adressraum beschafft/reserviert? Wo und wie würde der beschafft (Provider dependent vs. Provider independent)
- In welchen Teilbereichen des Netzes werden als erstes Forderungen nach IPv6 Konnektivität auftreten (Internet Access, Datacenter, Access Layer)? Welche Teilbereiche eignen sich am besten für Pilotprojekte?
- Welchen Einfluss hat IPv6 auf die Sourcing Strategie? Sind meine Provider in der Lage IPv6 Services zu liefern? Soll das verlangt werden?

Netzwerkverantwortliche müssen sich so vorbereiten, dass sie in der Lage sind die richtigen Entscheidungen zu treffen und das Unternehmen so zu positionieren, dass es nicht von fremdgesteuerten Ereignissen überrascht und überrollt wird. Den Kopf in den Sand stecken und warten bis der Sturm vorbei ist, ist wie so oft die schlechteste aller möglichen Strategien. Deshalb geht IPv6 alle etwas an – schon heute.

Michel Chappuis, Adrian Schmidlin und Urs Haug sind Partner von atrete und beraten schwerpunktmässig Kunden im Bereich Networking.

> to network
businesses and people

