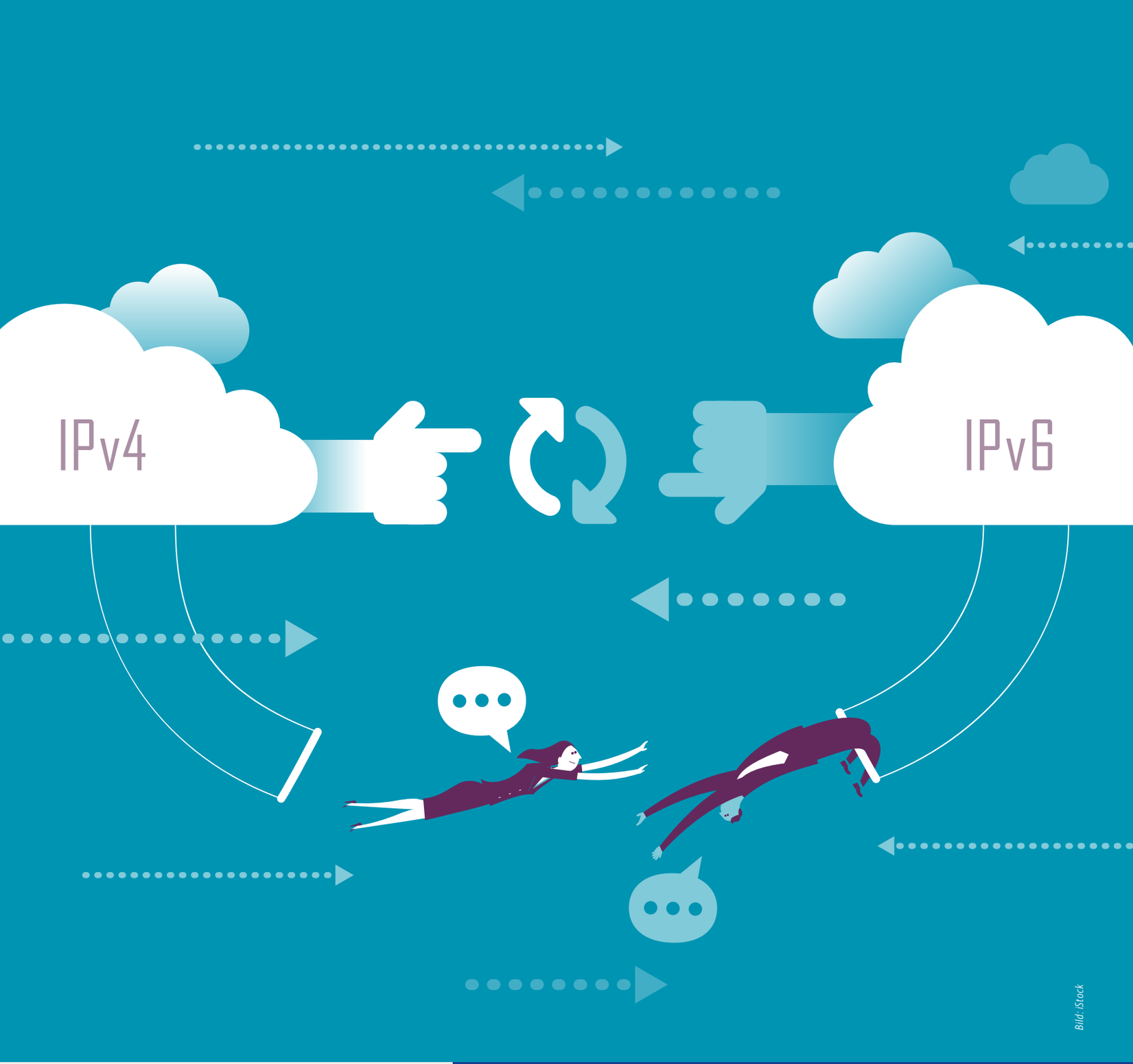


Bild: iStock

Dossier
IPv6

In Kooperation mit Boll Engineering

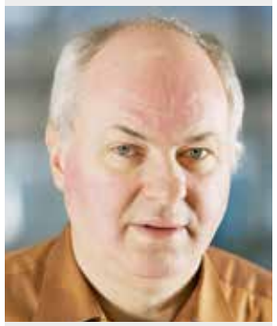
Auf dem Weg zu IPv6

cgr. Die Umstellung von IPv4 auf IPv6 ist in der Schweiz ins Stocken geraten. Nachdem die Schweiz viele Jahre weltweit den ersten Platz im Ranking von Akamai belegte, stagniert der Wert nun bei rund 20 Prozent. Inzwischen hält Belgien mit rund 40 Prozent den ersten Platz. Auch Griechenland und die USA sind inzwischen an der Schweiz vorbeigezogen. Die IPv4-Adressen werden aber immer knapper. Durch das Internet der Dinge werden immer mehr Geräte an das Netz angeschlossen, die eine eigene IP benötigen. Laut Gartner sollen es in drei Jahren schon 20 Milliarden IoT-Geräte sein. IPv6 wurde schon Ende der 1990er-Jahre als Lösung eingeführt. Der Standard vervielfacht die Zahl der Adressen auf 340 Sextillionen, dies entspricht einer 1 mit 21 Nullen. Die Umstellung ist jedoch nicht so einfach. Denn es braucht IPv6-fähige Hardware. Das ist eine Investition, vor der viele Unternehmen zurückschrecken. Walter Benz, Product Manager für A10 Networks bei Boll, empfiehlt daher eine gestaffelte Einführung. In der Zwischenzeit muss die Kommunikation zwischen den beiden Standards durch die Netzwerkinfrastruktur sichergestellt werden. Neue Projekte sollten von Beginn an auf IPv6 umgesetzt werden.

IPv4 und IPv6 – die grosse Herausforderung

Die Transition zwischen IPv4 und IPv6 stellt Unternehmen und Serviceprovider vor enorme Aufgaben. Eine integrierte Plattform mit vielfältigen Übersetzungs- und Tunneling-Technologien stellt die Koexistenz zwischen den beiden Welten sicher und ermöglicht einen reibungslosen Übergang.

DER AUTOR



Walter Benz
Product Manager für A10 Networks, Boll Engineering

Im Internet herrscht Adressknappheit, jedenfalls was die herkömmlichen IPv4-Adressen anbelangt. Zwar bietet der IPv4-Adressraum Platz für mehrere Milliarden Teilnehmer, und bisher hat es immer irgendwie gereicht. Jetzt aber wird die Problematik wirklich akut: Internet-Service-Provider erhalten von den offiziellen Vergabestellen keine neuen IPv4-Adressen mehr, und auf dem Graumarkt werden die wenigen verbleibenden Adressblöcke zu exorbitanten Preisen gehandelt. Gerade die unzähligen kleineren Provider können sich das nicht leisten.

In Zukunft wird sich die Adressknappheit weiter zuspitzen. Die Population der Mobilgeräte wächst ungebremst und verlangt für Dienste wie Streaming nach jederzeit verfügbaren, gleichmässig stabilen Verbindungen. Geradezu explosionsartig verbreitet sich das Internet der Dinge – die von Gartner für 2020 prognostizierten 20 Milliarden IoT-Geräte sind fast schon sprichwörtlich. Und jedes einzelne Device braucht seine eigene IP-Adresse.

Mit IPv6 steht in der Theorie bereits seit 1998 eine neue Version des Internetprotokolls bereit, die mit 340 Sextillionen möglichen Adressen vermutlich für alle Zeiten genügend Kapazität für neue Geräte bietet. In der Praxis ist die IPv6-Einführung jedoch aufwendig und kostspielig. Sie setzt Investitionen in neue, IPv6-fähige Hardware und mühsame Konfigurationsanpassungen voraus. Nicht zuletzt aus diesem Grund empfiehlt sich im Allgemeinen eine gestaffelte Einführung. Bestehende Systeme können zum Beispiel auf IPv4 belassen werden, während man neue Projekte von Anfang an auf IPv6-Basis umsetzt.

Die Adressknappheit wird sich weiter zuspitzen.

Zwei Welten

Doch die IPv6-basierte Infrastruktur versteht sich nicht von Haus aus auf die Kommunikation mit der bestehenden IPv4-Umgebung: IPv4 und IPv6 sind von Grund auf unterschiedliche Welten. Eine Koexistenz beider Protokolle ist nur möglich, wenn ein Gateway existiert, das den IPv6-Verkehr nahtlos und in Echtzeit in die IPv4-Welt übersetzt.

In besonderem Mass ist dies für Serviceprovider relevant: Während die interne Serverinfrastruktur relativ problemlos auf IPv6 umgestellt werden kann und die Backbone-Anbindung IPv6 bereits unterstützt, sind die Geräte der Kunden oft nicht IPv6-fähig oder sie sind nicht für IPv6 konfiguriert – und viele Kunden sind kaum in der Lage, die nötigen

Anpassungen selbst vorzunehmen. Privatkunden und kleinere Unternehmen verfügen ja nicht über eine eigene IT-Abteilung.

Aber auch grössere Organisationen mit eigener Netzwerkinfrastruktur sind auf eine Lösung angewiesen, die IPv4 und IPv6 in Einklang bringt. Ein guter Teil der aktuellen IoT-Geräte – vom einfachen Sensor bis zum kompletten Home-Automation-System – sind zudem überhaupt nicht IPv6-tauglich – dies ist besonders kritisch angesichts der langen Einsatzdauer solcher Devices.

Technologien für die Transition

Für den Aufbau konvergenter IP-Infrastrukturen, in denen IPv4 und IPv6 nahtlos koexistieren, stehen verschiedene Technologien zur Verfügung:

- Server Load Balancing with Protocol Translation (SLB-PT) macht die eigenen Server, egal ob IPv4- oder IPv6-basiert, für alle externen Clients zugänglich, und zwar unabhängig davon, ob die Clients selbst aus der IPv4- oder IPv6-Welt kommen. Die Übersetzung zwischen den Protokollen ist transparent, die Clients und ihre Nutzer merken nichts davon.
- NAT64/DNS64 ermöglicht IPv6-Clients den Zugang auf IPv4-Serverinfrastrukturen und deren Inhalte.
- Tunneling erlaubt es, IPv4-Verkehr über eine IPv6-Verbindung zu leiten – oder umgekehrt. Die Pakete des einen Protokolls werden dabei jeweils in Pakete des anderen Protokolls verpackt. So kann der IPv6-Verkehr zum Beispiel über einen Router – der selbst keine IPv6-Weiterleitung beherrscht – ins IPv6-Internet gelangen.

- DS-Lite ist eine Tunneling-Variante, die zunehmendes Interesse geniesst. Geräte, die nur IPv4-fähig sind, können mit DS-Lite in einem reinen IPv6-Netzwerk via «Softwires» ins Internet gelangen. Vergleichbare Möglichkeiten bieten die Verfahren LW4o6 und 6rd.
- Mit Carrier-Grade NAT (CGN) können Serviceprovider der IPv4-Adressknappheit ein Schnippchen schlagen: Die Kunden erhalten keine öffentliche IPv4-Adresse, sondern eine private, die ihnen vom CGN-Mechanismus zugeteilt wird. So lässt sich eine einzige öffentliche Adresse beim Provider auf bis zu 100 und mehr Kunden aufteilen – der IPv4-Adressvorrat hält länger. Wichtig ist dabei, dass die Kunden trotzdem eindeutig identifizierbar bleiben, wie es das Gesetz verlangt.
- Application-Layer-Gateways gewährleisten, dass Protokolle wie FTP, H.323 oder DNS funktionsfähig bleiben. Manche herkömmlichen NAT-Implementationen stellen dies nicht sicher.

INFO

Server Load Balancer (SLB) und ADCs (Lösungen für das Application Delivery und Application Networking) kommen dann zum Tragen, wenn es gilt, Anwendungen schneller, besser und sicherer bereitzustellen. Dazu unterstützen innovative Systeme erweiterte Security- und Networking-Funktionen wie etwa:

- Web Application Firewall (WAF)
- DNS Application Firewall (Schutz von DNS-Infrastrukturen)
- DDoS-Abwehr (Schutz vor mehrschichtigen Distributed-Denial-of-Service-Attacken)
- Application Access Management (integrierte Authentifizierungsfunktionen stellen sicher, dass die Backend-Server keinen unerwünschten oder nicht authentifizierten Datenverkehr erhalten)
- Reduktion des Datenverkehrs (z. B. Komprimierung des HTTP-Protokolls und Traffic Caching)
- SSL-Offloading (Terminierung verschlüsselter Client-Verbindungen)
- SSL-Bridging (Überprüfung verschlüsselter Daten auf fehlerhaften Code)
- Software-defined Networking (SDN)

Integrierte Lösung bringt Vorteile

Die besten Voraussetzungen für eine problemlose Transition zu IPv6 bietet eine integrierte Plattform, die alle gängigen Übersetzungs- und Tunneling-Verfahren beherrscht und zudem ermöglicht, verschiedene Methoden parallel einzusetzen. Auf dieser Basis lässt sich der Übergang in die IPv6-Ära schrittweise im gewünschten Tempo abwickeln, ohne dass einzelne Clients oder Server dabei auf der Strecke bleiben.

Verfahren wie CGN sind rechenintensiv und stellen hohe Anforderungen an die Performance der zugrundeliegenden Systeme. Es empfiehlt sich, dafür dedizierte Hardware einzusetzen, am besten eine speziell für die IPv4/IPv6-Transition konzipierte Appliance.

Der Kosten- und Integrationsvorteil kommt noch stärker zum Tragen, wenn die Plattform zusätzliche Funktionen wie hardwaregestütztes SSL-Offloading (Terminierung verschlüsselter Client-Verbindungen) und SSL-Bridging (Überprüfung verschlüsselter Daten auf fehlerhaften Code) sowie Sicherheitsfunktionen wie Abwehr von DDoS-Attacken und DNS- und Web-Application-Firewall anbietet. Dies gilt namentlich dann, wenn sich diese Funktionen zusammen mit genereller Application-Delivery-Controller-Funktionalität gleichzeitig in verschiedenen Partitionen auf der gleichen Hardware betreiben lassen. Dann entfällt die Investition in mehrere unterschiedliche Produkte, die dann doch nicht reibungslos zusammenarbeiten und insgesamt deutlich mehr kosten. Ein weiterer Vorteil einer integrierten Lösung ist ihr einheitliches Management.

Leistung ist gefragt

Grundbedingung für eine so umfassend integrierte Lösung ist eine hoch leistungsfähige Hardwareplattform, die den parallelen Betrieb aller Funktionen auch wirklich zulässt. Nicht alle Hersteller erfüllen diese Voraussetzung – die Leistungsdichte pro Rackeinheit fällt je nach Produkt markant unterschiedlich aus. Für moderne, dynamische Netzwerkinfrastrukturen nach dem Modell Software-defined Networking beziehungsweise Network Function Virtualization kommt auch eine virtuelle Appliance infrage – ideal ist es, wenn der Anbieter beide Varianten zur Wahl stellt.

Mit Carrier-Grade NAT (CGN) können Serviceprovider der IPv4-Adressknappheit ein Schnippchen schlagen: Die Kunden erhalten keine öffentliche IPv4-Adresse, sondern eine private, die ihnen vom CGN-Mechanismus zugeteilt wird.

Gnadenfrist für knappe IPv4-Adressen

Freie IPv4-Adressen werden rar. Was können Firmen unternehmen, bevor es zu spät wird? Christoph Tobler, Leiter IT der Leucom-Gruppe, schildert im Interview, wie der Ostschweizer Internetprovider das Problem mit Carrier-Grade Network Address Translation (CGN) gelöst hat. Interview: George Sarpong

Vor welcher Herausforderung standen Sie?
Christoph Tobler: Wir stehen vor dem gleichen Problem, das eigentlich alle Internetprovider haben: Die IPv4-Adressen werden knapp. Unser Vorrat geht langsam, aber sicher zu Ende. Auf dem Markt Adressen zu kaufen oder gar eine Firma zu übernehmen, die noch freie Adressen besitzt, wäre uns ziemlich teuer zu stehen gekommen. Wir mussten also eine andere Lösung finden.

Welche Alternativen haben Sie ins Auge gefasst?
Naheliegend wäre natürlich eine Migration auf IPv6. Damit hätte man auf einen Schlag eine astronomische Zahl von Adressen zur Verfügung. Die Umstellung wäre aber relativ schwierig – und wir könnten noch nicht alles umsetzen, was wir brauchen. Wir haben also lange überlegt und uns für Carrier-Grade NAT entschieden.

Wie funktioniert das?
Bei Carrier-Grade NAT teilt der Provider dem Kunden keine öffentliche, sondern eine private IPv4-Adresse zu. Der CGN-Gateway übersetzt dann für den Zugriff aufs Internet die private in eine öffentliche Adresse – wobei sich mehrere Kunden eine der rar gewordenen öffentlichen Adressen teilen. Somit reicht der Vorrat an IPv4-Adressen länger.

Wie weit sind Sie mit der Einführung?
Unsere CGN-Lösung ist nun seit bald einem halben Jahr in Betrieb und läuft absolut stabil. Als Erstes haben wir die Kunden mit den preisgünstigsten Abos, die wir Ende 2016 neu lancierten, auf CGN umgestellt. Dann folgten die mittelpreisigen Abos – wir gingen dabei vorsichtig vor und haben in Tranchen von 100, später 500 Kunden umgestellt. So konnten wir Feedbacks sammeln und wenn nötig Anpassungen vornehmen. Bis heute haben wir rund 3000 Kunden migriert – und zwar in der sportlichen Zeit von zwei Monaten!

« Wir haben rund 3000 Kunden migriert – und zwar in der sportlichen Zeit von zwei Monaten! »

Christoph Tobler, Leiter IT, Leucom

Sind die Kunden zufrieden?
Es ist eines unserer grössten Anliegen, dass die Kunden von CGN möglichst gar nichts davon merken sollen. Ein Kunde sollte bei sich nichts umstellen müssen, nur weil wir mit CGN arbeiten. Das hat in der Praxis bestens geklappt: Reklamationen gab es nur bei einem Prozent der migrierten Kunden. Meist waren dann Geräte wie Webcams oder NAS-Server vom Internet aus nicht mehr zugänglich. Für solche Fälle offerieren wir die Möglichkeit, doch eine öffentliche IP-Adresse zuzuschalten.

Christoph Tobler, Leiter IT der Leucom-Gruppe.

Zur gewählten Lösung: Wie sind Sie darauf gekommen?
Einer unserer Partner betreibt CGN seit einem Jahr erfolgreich auf Basis seiner Cisco-Infrastruktur. Ich habe aber weiter recherchiert und bin auf A10 Networks gestossen. Das Produkt Thunder CGN hat mich überzeugt: Es ist explizit auf CGN ausgelegt und ist darüber hinaus zukunftssicher, denn es bietet auch Funktionen für den Übergang zu IPv6. Und ganz besonders hat mich der Support des Herstellers und des Distributors Boll Engineering überzeugt. Wir hatten von Anfang an ausser dem Verkäufer auch einen Techniker zur Verfügung. Es gab offene Gespräche, und die Chemie hat gestimmt.

Wie ist Ihre CGN-Infrastruktur konfiguriert?
Heute betreiben wir zwei Thunder-CGN-Geräte, zwischen denen wir im Fehlerfall umschalten können. Das zweite Gerät übernimmt dann automatisch das Routing für die ausgefallene Einheit. Beide stehen aktuell in Zürich, wo die Backbone-Anbindung erfolgt. In Zukunft ist je nach Bedarf noch ein drittes Gerät in Frauenfeld geplant. Was die Leistung angeht, müssten wir noch lange nicht ausbauen: Die CPU-Last liegt aktuell bei 5 Prozent. Da ist also noch viel Luft für zusätzliche Kunden.

ÜBER LEUCOM

Gegründet als Radio-/TV-Geschäft vor über 50 Jahren ist Leucom heute eine breit abgestützte Multimedia-Firmengruppe mit mehr als 80 Mitarbeitenden (Hauptsitz in Frauenfeld, Filialen in Schlieren und St. Gallen). Leucom baut und betreibt als Triple-Player (TV, Telefonie und Internet) eigene Kabelnetze und treibt den Ausbau zu Glasfaser zügig voran. Rund 25 000 Haushalte vom Aargau bis ins Appenzellerland beziehen TV-Dienste und rund 18 000 ihren Internetanschluss von Leucom.