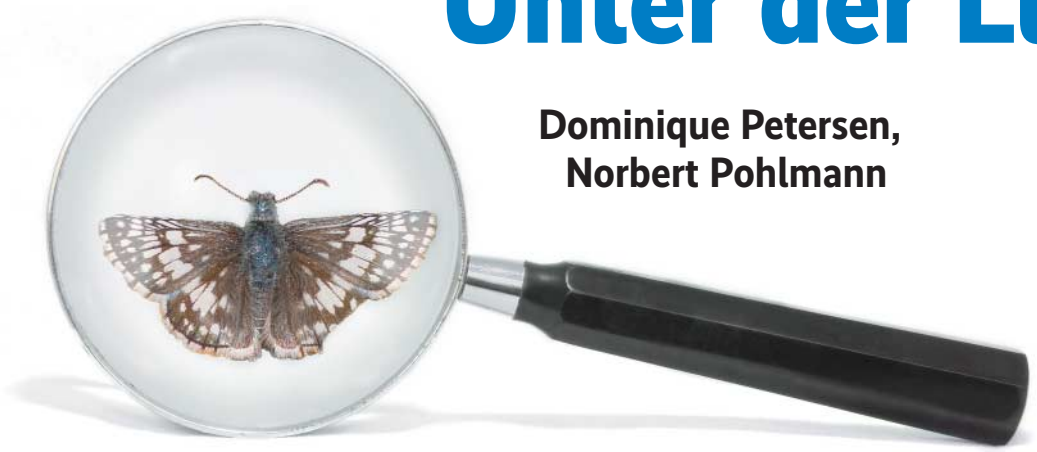
Langsam, aber sicher kommt IPv6 in Gang

Unter der Lupe

Dominique Petersen,
Norbert Pohlmann



Die weitaus meisten ans Internet angeschlossenen Geräte kommunizieren gemäß der altbewährten Version 4 des Internet Protocol (IP) miteinander. Sie erfreut sich noch immer der weitaus größten Verbreitung, denn der Übergang zur Nachfolgeversion IPv6 findet deutlich langsamer statt als ursprünglich gedacht. Doch nun kommt Bewegung hinein.

In absehbarer Zeit wird IPv6 seinen Vorgänger ablösen – vor allem aufgrund der Knappheit freier IPv4-Adressen, da immer mehr Geräte an der Internet-Kommunikation teilnehmen sollen, etwa im „Smart Home“. Andere Gründe sind jedoch auch die bequeme Realisierung von Quality of Service und die Unterteilung des Netzwerkverkehrs in unterschiedliche Verkehrsklassen mit verschiedenen Prioritäten.

Viele Komponenten der Netzinfrastruktur (Router, Firewalls etc.) können noch nicht korrekt mit dem Nachfolger IPv6 umgehen. Damit nicht jeder alle veralteten Geräte auf einmal aktualisieren oder durch IPv6-fähige ersetzen muss, sind eine Reihe von Verfahren im Einsatz, IPv6-Pakete über die bestehende IPv4-Infrastruktur zu übertragen (siehe Abb. 1).

Als möglichen Zwischenschritt gibt es eine Reihe von Verfahren zum Transportieren von IPv6-Paketen über ein IPv4-Netzwerk (das aktuelle „Internet“) und vice versa. Dieser Artikel gibt einen Überblick über die am häufigsten benutzten Tunnelprotokolle, deren Funktion, einige Sicherheitsbetrachtungen sowie die detaillierte Verbreitungsanalyse der Zugangstechnologien von IPv6.

Tunnelbau als Zwischenschritt

Derzeit kommen im Wesentlichen drei Varianten der IPv6-Übertragung zum Einsatz – natives IPv6, 6in4/6over4/6to4 und Teredo –, die die Sensorik des Internet-Analyse-Systems (IAS) vom Institut für Internet-Sicherheit if(is) unterscheidet. Das IAS beobachtet passiv und paketorientiert den Netzwerkverkehr und zählt dabei nur anonymisierte, vorher definierte Protokoll-Header-Informationen („Deskriptoren“) für seine Statistiken. Es identifiziert ausschließlich datenschutzrechtlich nicht relevante und eindeutige Kommunikationsparameter der OSI-Schichten 2 (Sicherungsschicht) bis 7 (Anwendungsschicht), wie ein gesetztes TCP-Syn-Flag beim Verbindungsaufbau, die verwendete TLS/SSL-Verschlüsselung oder einen speziellen Browser-Typ, aber keine personenbeziehbaren Informationen wie IP-Adressen oder die Nutzdaten (Payload) eines HTTP-Pakets. Derzeit unterscheidet es über 3 Millionen Kommunikationsparameter im Datenstrom voneinander und speichert sie in einer Datenbank für spätere, detaillierte Analysen oder Prognosen. Dass dabei der Datenschutz eingehalten wird, hat der Bundesdatenschutzbeauftragte Peter Schaar bereits 2005 bestätigt.

Natives IPv6 ohne Tricks und Tunnel

Derzeit unterstützen längst nicht alle Netzwerkgeräte vom Absender bis zum Empfänger komplett natives IPv6. In den Unternehmen sind bei Weitem noch nicht alle Herausforderungen gelöst, vor allem aufgrund der notwendigen Anschaffung, Installation und Konfiguration für IPv6 geeigneter Hardware. Für Serversysteme (etwa Webserver) ist der Dual-Stack-Betrieb recht verbreitet. Die Server sind bei dieser Variante sowohl per IPv4 als auch IPv6 erreichbar und können die Antwortpakete über beide Interfaces versenden.

Dies funktioniert jedoch nur, wenn auch die Namensauflösung (DNS) IPv6-fähig ist (also AAAA-Records liefert) – eben-

falls vielerorts noch nicht der Fall. Zurzeit stellen Betreiber großer Rechenzentren und Serverfarmen ihre Infrastruktur nach und nach auf IPv6 um. Allerdings könnten vor allem kleine und mittlere Hoster deutlich aggressiver vorgehen als momentan. Es mangelt einfach an Motivation, komplett IPv6 zu sprechen, solange der Hauptteil der Anwender oder Kunden davon kaum profitiert.

Viele Anwender könnten dank aktueller Betriebssysteme zwar natives IPv6 nutzen, müssen jedoch nach wie vor darauf warten, dass sowohl ihr eigener Router als auch diejenigen ihres Providers damit zurechtkommen. Bis dahin gibt es mit nativem IPv6 keinen Datenaustausch. Durch dieses Henne-Ei-Problem zwischen Dienstanbietern und ISPs einerseits und Anwendern andererseits schreitet der Einsatz von IPv6 nur mühsam voran, da sich viele Institutionen scheuen, für eine aus ihrer Sicht bislang unnötige komplette IPv6-Unterstützung viel Geld auszugeben.

Ineinander verschachtelte Protokolle

Die IPv4-Infrastruktur lässt sich als virtuelle Vermittlungsschicht zum Übertragen von IPv6-Paketen nutzen, als Payload neu generierter IPv4-Pakete. Das „Protocol"-Feld des IPv4-Headers enthält dann den Wert 41 für die „Verkapselung von IPv6- in IPv4-Paketen". 6in4, 6to4 und 6over4 sind drei verschiedene Übertragungsverfahren, die einander so sehr ähneln, dass sie sich zusammenfassen lassen – im Folgenden als „6*4".

Bei der Variante 6in4 müssen die IPv6-Adressen zuvor bekannt sein, etwa über IPv6-fähige DNS-Server. Zudem sind zwei Systeme im Dual-Stack-Betrieb erforderlich, die zwischen der IPv4- und IPv6-Welt vermitteln können. Der erste Dual-Stack-Router generiert ein neues IPv4-Paket, in dessen Payload sich das komplette IPv6-Paket befindet. Es gelangt über die IPv4-Infrastruktur bis zu einem Dual-Stack-Router, der das IPv6-Paket extrahiert und an den IPv6-fähigen Server weiterreicht.

Die Varianten 6over4 und 6to4 funktionieren ähnlich, allerdings legen beide die IPv6-Adressen fest. 6over4 berechnet eine neue virtuelle IPv6-Adresse nach dem Muster *FE80::<IPv4 in hexadezimaler Darstellung>* und versendet die Link-lokalen IPv6-Pakete eingebettet in IPv4 über ein Multicast-IPv4-Netzwerk. Diese Funktion findet allerdings selten Unterstützung, da sie zu Durchsatz- und Sicherheitsproblemen führen kann.

6to4 berechnet Adressen, die in den Header passen, in der Form *2002:<IPv4 in hexadezimaler_Darstellung::>*. Es handelt sich nicht um Link-lokale, sondern um global gültige IPv6-Adressen. Der gesamte IPv6-Adressraum 2002::/16 ist für das Tunnelverfahren 6to4 reserviert. Von der Variante 6to4 gibt es einen Ableger namens „6rd" (IPv6 Rapid Deployment). Er eignet sich nur für Privatanwender und deren Provider, da die IPv6-Adressen zentral vergeben werden. Allerdings erhöht 6rd gegenüber dem normalen 6to4 das Übertragungstempo und die Sicherheit, da der ISP bestimmte Angriffsvektoren blockieren kann.

Da das Internet-Analyse-System aus Datenschutzgründen keine IP-Adressen betrachtet, kann es nicht zwischen den drei Mechanismen unterscheiden. Die einfacheren und praktikableren 6in4 und 6to4 sind jedenfalls viel stärker verbreitet als 6over4.

Falls zumindest kundenseitig ein IPv6-fähiger Router vorhanden ist, können Client-Systeme über dessen Tunnelfunktion per IPv6 kommunizieren, unabhängig davon, wann der eigene Provider das neue Protokoll in Betrieb nimmt. Der Router übernimmt dann die Abwicklung der IPv6-Pakete über einen Tunnelprovider wie SixXS oder Hurricane Electric und versendet den Verkehr mittels 6in4/6to4/6over4 über die IPv4-Verbindung. Auch Client-Systeme können eigene Tunnelverbindungen aufbauen, jedoch führt dies an vielen Endkundenanschlüssen noch zu Problemen, da an diesen Stellen oft NAT („Network Address Translation") beziehungsweise PAT („Port- and Adress-Translation") oder restriktive Firewall-Systeme im Einsatz sind, die kein Tunnelprotokoll beherrschen.

Teredo – der Windows-Standard

Bei Teredo und Miredo handelt es sich um ein Tunneling-Protokoll, das IPv6-Pakete im Payload von IPv4-UDP-Datagrammen einkapselt. Auf diese Weise lassen sich Firewalls durchtunneln, die auf der OSI-Schicht 4 (Transportebene) nur TCP, UDP und ICMP erlauben. Die Verfahren 6in4/6to4/6over4 würden in diesem Fall geblockt. Als UDP-Port dient 3544.

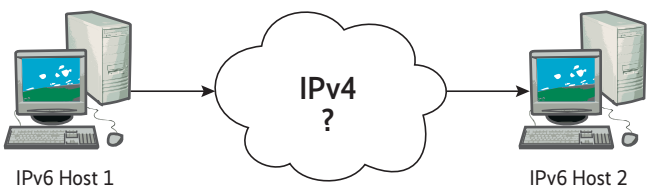
Teredo nutzt UDP statt TCP, da bei UDP der Verbindungsaufbau entfällt und sich UDP-Pakete aufgrund ihrer kleineren Header schneller übertragen lassen. Zudem ergibt es wie bei VPNs keinen Sinn, eingekapselten IPv6-TCP-Verkehr über einen IPv4-TCP-Strom zu leiten, da sich TCP-Optimierungen wie „Slow Start" und „Congestion Window" aufeinander negativ auswirken. Außerdem könnte man bei Verwendung eines TCP-Tunnels für Anwendungen wie VoIP (Voice over IP) keine echtzeitorientierten Protokolle nutzen, die für die kontinuierliche und ungesicherte Datenübertragung auf UDP angewiesen sind.

Bei neueren Windows-Betriebssystemen kommt Teredo als Standardverfahren für eine IPv6-Nutzung über eine IPv4-Infrastruktur zum Einsatz. In Gestalt von Miredo existiert ein Pendant für Unix-Systeme. Teredo benötigt auf der Gegenseite ebenfalls einen Dual-Stack-Teredo-Router, der die Pakete auf natives IPv6 umschreibt. Daher initiieren üblicherweise nur Clients Teredo. Es macht im Privatbereich den Großteil des IPv6-Verkehrs aus. Den Tunnelverkehr für sämtliche Windows-Systeme bewerkstelligen Microsofts Teredo-Server.

Routing von IPv4 über IPv6

Selbstverständlich gibt es auch den umgekehrten Weg, nämlich IPv4-Pakete über ein IPv6-Netz zu routen, zum Beispiel über das Tunnelprotokoll „4in6". Die IPv6-Infrastruktur transportiert das verpackte IPv4-Paket, bis ein Dual-Stack-Gateway es wieder extrahiert und zum gewünschten IPv4-Server weiterleitet.

Ein anderes Verfahren, von einem IPv6-Client auf einen IPv4-Server zuzugreifen, besteht in NAT64 und DNS64. Der IPv6-Client fragt den DNS64-Server nach der IPv6-Adresse des IPv4-Servers. Der DNS64-Server konvertiert die IPv4- in eine IPv6-Adresse (ähnlich wie bei 6over4/6to4) und teilt sie dem Client mit, der seine Pakete zum passenden NAT64-Gateway schickt. Das muss sich im IPv4/IPv6-Dual-Stack-Betrieb befinden und erkennt, dass mit der IPv6-Adresse eigentlich ein IPv4-Server gemeint war, woraufhin er den Payload der Vermittlungs-



Tunnelverfahren ermöglichen zunächst vor allem eine IPv6-Kommunikation über die IPv4-Infrastruktur. Später wird der Bedarf am umgekehrten Weg zunehmen (Abb. 1).

schicht in ein neu generiertes IPv4-Paket verpackt und weiterleitet. Die Antwortpakete nehmen dann den gleichen Weg zurück. Der Vorteil ist hier, dass der IPv6-Host nicht wissen muss, dass er praktisch eine Kommunikation mit einem IPv4-Server verwendet.

Aufgrund der noch recht geringen Verbreitung von IPv6 (höchstens große Unternehmen betreiben intern eine IPv6-Instrastruktur) kommt das Routing von IPv4 über IPv6 kaum zum Einsatz und spielt daher in den folgenden Auswertungen keine Rolle.

Sicherheitsaspekte von IPv6 und den Übergangsverfahren

IPv6 steht bereits seit 1998 als Norm fest und erfuhr seitdem eine Reihe von Verbesserungen. Aufgrund seiner schleppenden Verbreitung und des entsprechend dürftigen Erfahrungsschatzes im Vergleich zum Vorgänger IPv4 weist es nach wie vor einige Kinderkrankheiten auf, die Paketfilter erkennen und aussortieren müssen. Das Hauptsicherheitsproblem bei der Verwendung von nativem IPv6 besteht darin, dass die bisherigen Security-Produkte fast nur IPv4 beherrschen und Implementierungen von IPv6-Komponenten noch in den Kinderschuhen stecken.

Die Lage bei den Soft- und Hardwareherstellern ähnelt derjenigen bei ISPs und Serverbetreibern: Sie stecken nicht viel Geld in die Entwicklung IPv6-fähiger Komponenten, da es noch keinen großen Markt dafür gibt. Zudem fehlen einschlägige negative Erfahrungen wie mit IPv4. Für Heimanwender ist die Anzahl IPv6-fähiger Geräter überschaubar, und leider sind die IPv6-Implementierungen oft unsicher und lassen etwa dubiosen Netzwerkverkehr passieren, den sie eigentlich abfangen müssten. Diverse Angriffsszenarien sind denkbar, etwa unter Stichworten wie „Duplicate Address Detection DoS“, „Neighbor Discovery MITM“ (altes „ARP-Spoofing“ unter IPv4, siehe S. 62) oder den anderen MITM-Varianten (Man In The Middle) via „ICMPv6 Redirect“ und „Router Advertisement“.

Gleichzeitig sind Tunnelprotokolle eine Herausforderung für jede Firewall. Bisherige Systeme halten sich beim Analysieren der Pakete an den vorgegebenen OSI-Stack und setzen voraus, dass es jede OSI-Schicht nur einmal gibt. Die gängigen Tunnelprotokolle enthalten mindestens die Schicht 3 doppelt, und eine Firewall analysiert dann nur die erste (IPv4). Pakete in der zweiten Schicht 3 (IPv6) samt Payload bleiben üblicherweise unbehelligt. Die Tunnelprotokolle 6in4/6to4/6over4 lassen sich ganz einfach blockieren, indem die Router als Transportschicht nur die Protokolle TCP und UDP erlauben. Die meisten Router sind standardmäßig genau so konfiguriert.

Komplizierter steht es um Teredo, das eine IPv4-Firewall regelrecht durchlöchern kann. Da ein Client Teredo per UDP-Port 3544 initiiert, dürfen Antworten vom Teredo-Server die Firewall passieren. Der Windows-Client würde das IPv4-UDP-Paket auspacken und das eingekapselte IPv6-Paket benutzen oder möglicherweise im lokalen Netz weiterleiten, falls ein Täter das Paket entsprechend manipuliert hat. So könnten Angreifer ein internes Heimnetzwerk von innen scannen oder sogar angreifen, ohne dass der Paketfilter des Routers oder der Benutzer es merken. Zurzeit gebräuchliche Firewall- und Personal-Firewall-Systeme analysieren die eingebetteten IPv6-Pakete nicht.

Zudem nutzen Windows-Systeme standardmäßig Teredo-Server von Microsoft. Will jemand aus Deutschland mit einem IPv6-fähigen Server in Deutschland kommunizieren, läuft sämtlicher Verkehr über Microsoft-Server, die möglicherweise in den USA stehen. Gerade die Enthüllungen der Überwachung diverser Geheimdienste mittels PRISM und TEMPORA gebieten hier besondere Vorsicht, da die Daten im Klartext übers Netz gehen. Der einzig wirkungsvolle Schutz besteht derzeit darin, Teredo mittels *netsh interface ipv6 set teredo disable* auszuschalten oder IPv6 global zu deaktivieren.

Messungen von IPv4 und IPv6

Die Sensoren des Internet-Analyse-Systems sind auf viele Institutionen international verteilt, damit sich unterschiedliche Standorte und auch Länder miteinander vergleichen lassen. Die folgende Analyse bezieht sich auf einige repräsentative Messpunkte.

Bei vielen Unternehmen und kleinen Providern liegt der IPv6-Anteil nach wie vor extrem niedrig, manchmal kommt nur ein IPv6-Paket auf -zig Millionen IPv4-Pakete. Gerade Technologieunternehmen, deren Know-how das eigentliche Firmenkapital darstellt, haben IPv6 konsequent und mit aktuellen Sicherheitskomponenten unterbunden, sodass weder natives IPv6 noch die Tunnelverfahren 6*4 und Teredo den Grenzübertritt zwischen Intra- und Internet schaffen. Eine führende Universität in den USA, die Stanford University, kommt dagegen sogar bereits auf 2,2 % IPv6-Anteil, fast komplett nativ. Für repräsentative Zahlen aus Deutschland kamen Rohdaten vom zentralen Internet-Austauschknotenpunkt DE-CIX zur Auswertung.

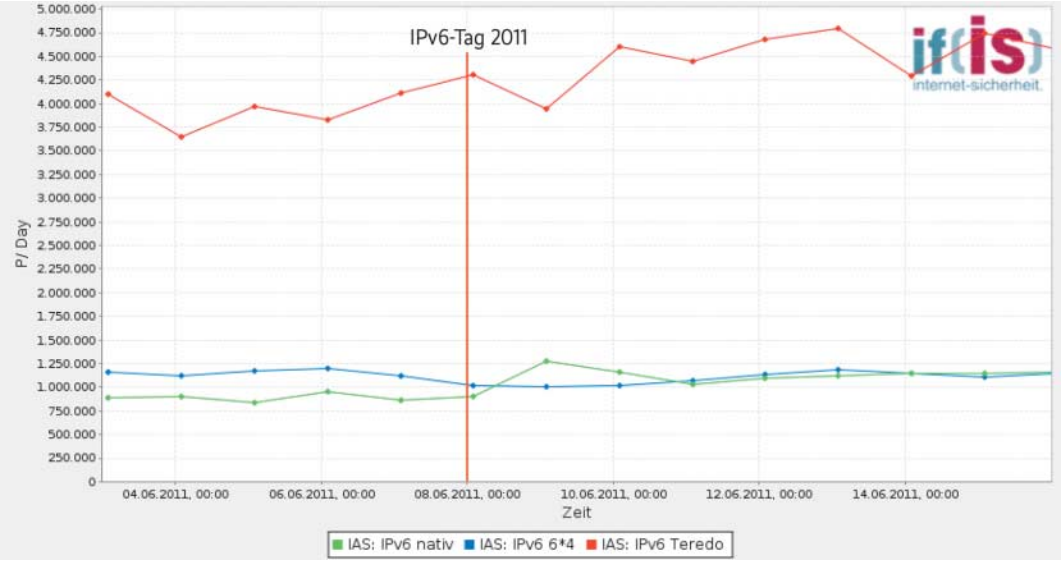
Im April 2011 kam IPv6 hierbei lediglich auf einen Anteil von 0,72 %. Im Vergleich zu anderen Sondenstandorten lag er damit sogar relativ hoch. Bei IPv6 sind alle möglichen Kommunikationsformen berücksichtigt, die die Sonde des IAS messen kann. Vom gesamten IPv6-Verkehr geht etwa ein Viertel auf das Konto des essenziellen Protokolls ICMPv6, das wie der Vorgänger Steuerungs- und Fehlermeldungen transportiert, aber auch der Neighbor Discovery und damit als ARP-Nachfolger dient. Der Anteil von nativem IPv6 betrug nur etwa 12,75 %, der Rest lief über Tunnel, mit einem 6*4-Anteil von 21,56 %. Der Löwenanteil ging mit 65,69 % an Teredo – ein wichtiger Maßstab, da er meist auf das Konto von Client-Systemen geht.

Zum Voranbringen von IPv6 riefen die Internet Society (ISOC) sowie zahlreiche Provider und Inhalteanbieter den internationalen IPv6-Tag ins Leben. Er sollte Unternehmen den Anstoß geben, ihre Infrastruktur umzustellen und zu testen. Viele große ISPs und Webserverbetreiber aktivierten für einen Tag den Dual-Stack-Modus, um in der neuen Hardware Fehler aufzudecken und IPv6 allgemein auszuloten.

Am 8. Juni 2011 war es erstmals so weit. Die DNS-Konfiguration etlicher Internet-Größen wie Facebook, Google und Yahoo, aber auch des Heise-Verlags, erhielt zusätzliche AAAA-Records. Somit ergab die Abfrage eines Hostnamens (beispielsweise im Browser) auch eine IPv6-Adresse, falls das Client-System damit etwas anfangen konnte.

IPv6-Anteil am DE-CIX

Zeitpunkt	IPv6 total	natives IPv6	6to4/ 6over4	Teredo
Mai 2011	0,72 %	0,09 %	0,16 %	0,48 %
IPv6-Tag 2011	0,86 %	0,17 %	0,14 %	0,55 %
Mai 2012	0,97 %	0,22 %	0,22 %	0,53 %
IPv6-Tag 2012	0,96 %	0,25 %	0,18 %	0,52 %
August 2012	0,94 %	0,31 %	0,15 %	0,49 %
Dezember 2012	1,07 %	0,41 %	0,14 %	0,52 %
März 2013	1,24 %	0,51 %	0,13 %	0,60 %
Juni 2013	3,91 %	3,15 %	0,12 %	0,64 %
August 2013	1,20 %	0,56 %	0,12 %	0,52 %



Seit dem IPv6-Tag am 8. Juni 2011 liegt der „echte" IPv6-Verkehr vor den unter „6*4" zusammengefassten Tunnelverfahren (Abb. 2).

Clients, die sowohl IPv4 als auch IPv6 verstehen, entscheiden sich nach gängigen Implementierungen für IPv6. Bei falscher oder unzureichender Endgerätekonfiguration kann es passieren, dass zwar das Heimnetzwerk IPv6 beherrscht, aber nur über IPv4 nach außen kommunizieren kann. Infolge dessen erhalten Clients zwar IPv6-Adressen für die abgefragten Hosts, die eigentliche Verbindung über IPv6 hingegen scheitert (siehe auch S. 132). Somit konnten einige Browser keinen Inhalt laden, der eigentlich per IPv4 erreichbar gewesen wäre. Zugunsten verwertbarer Ergebnisse und der Verbreitung von IPv6 als Vorreiter waren die Teilnehmer des IPv6-Tages allerdings bereit, dieses Risiko für einen Tag einzugehen.

Startschuss zum IPv6-Tag 2011

Als Resultat stieg der Anteil von IPv6 um mehr als ein Zehntel auf 0,86 % an (siehe Tabelle). Offenbar hatten tatsächlich einige Unternehmen den IPv6-Tag als Anlass genommen, ihre Infrastruktur zu testen. Gleichzeitig sank der Verkehr von IPv4 um rund 6,5 %. Der Anteil von ICMPv6 betrug nur noch 23,7% statt 25% wie noch im April 2011.

Wie die Tabelle ebenfalls zeigt, betraf der IPv6-Zuwachs größtenteils natives IPv6 mit 20,16 % und Teredo mit 63,68 %. 6*4 fiel hingegen auf 16,16 %. Die Unternehmen nutzten also mindestens den Dual-Stack-Modus. Heimanwender griffen auf diese IPv6-Server vornehmlich über Teredo zu. Die 6*4-Tunnelverfahren kamen erwartungsgemäß nicht mehr so häufig zum Einsatz, da „echtes" IPv6 möglich war.

Die Auswertungen der Teilnehmer führten zu weitgehend positiven Ergebnissen. Der Heise-Verlag nahm dies als Anlass, dauerhaft auf den Dual-Stack-Betrieb umzusteigen. Facebook stellte als einer der größeren Teilnehmer seine Entwicklerseiten ebenfalls dauerhaft auf Dual-Stack um. Im Nachhinein zeigte sich, dass der IPv6-Tag 2011 die Verbreitung von IPv6 positiv beeinflusst hat (Abb. 2).

Ein knappes Jahr darauf, im Mai 2012, dominierte – wenig überraschend – weiterhin IPv4. Der IPv6-Verkehr kam auf „nur" 0,97 % (siehe Tabelle). Immerhin: Er hatte sich annähernd verdoppelt (+86,65 %) und war damit stärker gewachsen als der IP-Verkehr insgesamt. Vom gesamten IPv6-Verkehr gehen rund 22 % auf ICMPv6. Im April 2011 waren es noch 25 %. Der Anteil von nativem IPv6 beträgt nun gut 23 % (im April 2011 knapp 13 %), den Rest tragen Tunnelmechanismen bei. Der Anteil von 6*4 bleibt etwa konstant bei gut 22 % (im April 2011 21,56%). Den Löwenanteil hat mit 54,49 % weiterhin Teredo inne, gab aber gegenüber den anderen Verfahren nach: Im April 2011 waren es noch fast 66 %. Es zeigt sich deutlich, dass natives IPv6 gegenüber den anderen Tunnelmechanismen stark zugenommen hat. Es existieren also mehr funktionierende IPv6-Infrastrukturen. Den Anteil, den natives IPv6 gewinnen konnte, musste Teredo abgeben – ein Zeichen dafür, dass sich nun immer mehr Ende-zu-Ende-Verbindungen durchgängig mit IPv6 realisieren lassen.

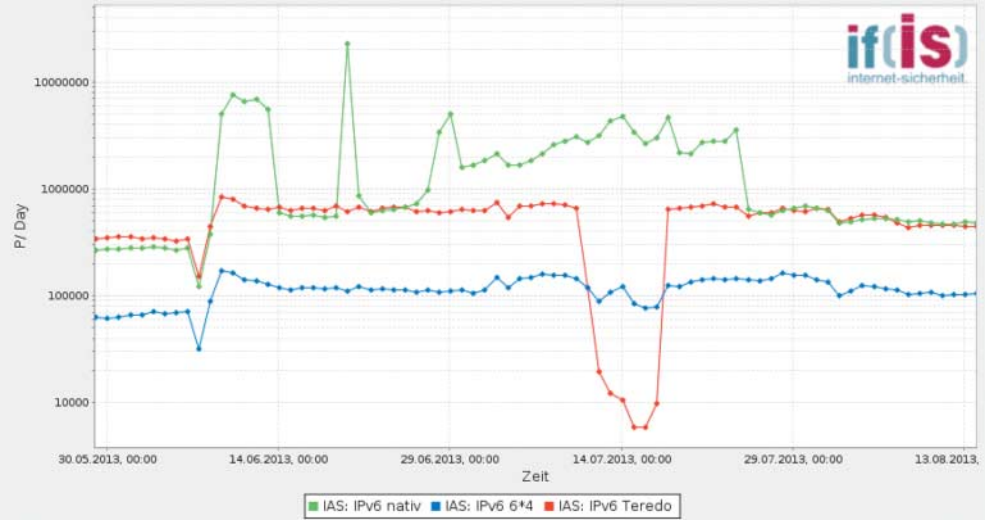
Da der generelle IPv6-Anteil auch zugenommen hat und keines der Protokolle absolute Anteile verloren hat, handelt es sich um echtes Wachstum des IPv6-Verkehrs mit klarem Aufwärtstrend für natives IPv6. Sollte er anhalten, würde der native IPv6-Anteil das bisher führende Teredo spätestens Anfang 2015 überholen. Als Hauptursachen kommen infrage, dass die ersten Internet-Provider langsam auf IPv6 umstellen und dass neue Kommunikationskanäle zwischen autonomen Systemen bevorzugt per IPv6 entstehen.

IPv6-Tag 2012 bestätigte den Aufwärtstrend

Der IPv6-Tag 2012 galt im Vorfeld bei vielen Teilnehmern als mögliche Initialzündung. Nach dem erfolgreichen Testlauf im Vorjahr planten etliche, den IPv6- respektive Dual-Stack-Dauerbetrieb aufzunehmen. Die Beteiligten rechneten mit einem signifikanten und nachhaltigen Anstieg des IPv6-Anteils. Das Interesse deutscher Provider hielt sich allerdings wie 2011 in Grenzen. Eine Ausnahme bildete Kabel Deutschland, das in Feldversuchen bereits einzelne Endkundenanschlüsse für IPv6 eingerichtet hatte.

Der 6. Juni 2012 startete jedoch mit einem enttäuschenden IPv6-Anteil von etwa 0,96 % – das war im Vergleich zum Vormonat praktisch unverändert (genau genommen gab es sogar einen Rückgang um fast 1,3 %). Doch seit April 2011 war der IPv6-Anteil um gut 84 % gestiegen. Offenbar hatten die Beteiligten bereits vor dem offiziellen Termin sehr viel mehr IPv6 „gesprochen" und nicht eigens auf den 6. Juni gewartet. Der Anteil von ICMPv6 betrug nur noch 21,7 % statt 23,7 % wie im Mai 2011, es gab also mehr natives IPv6 (ca. 26,6 %). 6*4 kam auf knapp 19 % und Teredo auf etwa 54,5 % (Tabelle). Gegenüber April 2011 entsprach dies bei den beiden Tunnelmechanismen einer Steigerung um gut 61 % und fast 53 %. Natives IPv6 hingegen wuchs sogar um über 284 %, gegenüber dem IPv6-Tag 2011 war das immerhin mehr als eine Verdoppelung (+119 %).

Den Zuwachs trug größtenteils natives IPv6 bei, von den Unternehmen meistens im Dual-Stack-Modus freigeschaltet. Heimanwender hingegen griffen auf die IPv6-Server über Teredo, teilweise auch über natives IPv6 zu; 6*4-Tunnel waren wie erwartet auf dem Rückzug.



Pünktlich zum IPv6-Kongress Anfang Juni 2013 stieg vor allem der native IPv6-Verkehr deutlich. Im Juli war das fast ausschließlich von Windows-Systemen genutzte Teredo gestört (Abb. 3).

Gerade der repräsentative DE-CIX-Knoten verzeichnete zwischen Mai 2011 und Mai 2012 bei nativem IPv6-Verkehr nahezu eine Verzehnfachung. Kein Wunder also, dass es am offiziellen IPv6-Tag keinen weiteren Anstieg gab. Einige Unternehmen nutzten die Gelegenheit jedoch, ihre Zukunftspläne noch einmal darzustellen. Die Deutsche Telekom etwa verkündete, bis Ende 2012 alle privaten Hausanschlüsse auf natives IPv6 umzustellen.

Magische Prozentmarke Ende 2012 überschritten

Im Dezember 2012 erreichte IPv6 mit 1,07% erstmals einen Anteil von über einem Prozent des Gesamtverkehrs. Erneut wuchs der IPv6-Anteil stärker als das IPv4-Pendant. Natives IPv6 überstieg im März 2013 erstmals knapp die 0,5 %. Teredo konnte sogar vom Dezember 2012 (0,52 %) deutlich auf 0,6 % im März 2013 zulegen. Andere Tunnel waren offensichtlich immer weniger gefragt: Im März 2013 machte 6*4 nur noch 0,13 % aus.

Im Jahr 2013 gab es zwar keinen IPv6-Tag mehr, aber am 6. und 7. Juni lief der fünfte IPv6-Kongress in Frankfurt/Main, organisiert vom DE-CIX, heise Netze und *iX*. Unmittelbar danach gab es ein überraschend deutliches Wachstum des IPv6-Anteils auf fast vier Prozent. Vor allem natives IPv6 ragte heraus, das zeitweise 80 % zum IPv6-Verkehr beitrug (3,15 % vom Gesamtverkehr). Gegen Ende Juli 2013 ging der Anteil wieder zurück, pendelte sich aber immer noch 50 % höher als Anfang Juni ein. Im Juni und Juli 2013 haben vor allem ISPs ihre IPv6-Konnektivität getestet, aber noch nicht für private Heimanwender aktiviert. Die Tunnelverfahren 6*4 und Teredo hingegen verharrten etwa auf dem Niveau der Vormonate (0,12 % und 0,64 %, siehe Abb. 3).

Mitte Juli 2013 verzeichnete das IAS einen tagelangen, heftigen Einbruch von Teredo (s. Abb. 3), wobei im gleichen Zeitraum natives IPv6 und 6*4 nahezu unverändert blieben. Einen Grund nannte Microsoft kurze Zeit später: Angeblich hatte das Unternehmen absichtlich seine Teredo-Server vom Netz genommen, um prüfen zu können, wie viele Benutzer den Dienst überhaupt nutzen. Am 16. Juli liefen die Server wieder und der Teredo-Anteil erholte sich. Teredo kommt praktisch ausschließlich unter Windows zum Einsatz, das den IPv6-Verkehr über Microsofts Server leitet. Drittanbieter von Teredo respektive Miredo spielen zumindest in Deutschland keine nennenswerte Rolle.

Aktuelle Messwerte bestätigen die im Frühjahr 2013 festgestellten Verhältnisse. IPv6 kommt demnach auf solide 1,2 %. Die native Variante wächst langsam, aber stetig, und liegt nun bei 0,56 %. Die Tunnel gemäß 6*4 gehen kontinuierlich zurück, auf derzeit 0,12 %. Teredo bleibt bis auf den Ausfall im Juli relativ stabil auf 0,52 %. Große Veränderungen sind hier zunächst nicht zu erwarten, da viele Windows-Anwender vermutlich so lange Teredo benutzen, bis Microsoft den Dienst einstellt. Aktuelle Messwerte und Kennzahlen hält das IKS-Portal unter iks.internet-sicherheit.de bereit.

Fazit

Bis zur flächendeckenden Nutzung von IPv6 werden nach aktuellen Prognosen noch einige Jahre ins Land gehen. Deutschlandweit bestehen derzeit rund 1,2 % des Internet-Verkehrs aus IPv6, wovon jeweils knapp die Hälfte auf natives IPv6 und Teredo fällt. Nur 6*4-Tunnel gehen kontinuierlich zurück, mit einem derzeitigem Tiefststand von 0,12 %. Vor allem natives IPv6 dürfte wachsen, da in Zukunft weiterhin immer mehr ISPs und Unternehmen auf echtes IPv6 umstellen. Die Übergangsverfahren dürften zwar nicht verschwinden, aber der Tunnelbedarf wird auch nicht mehr steigen. International bewegt sich Deutschland damit im Mittelfeld, verglichen mit Stanford kommt es nur nur auf knapp die Hälfte.

Jede Marktsondierung IPv6-fähiger Komponenten zeigt, dass die Hersteller noch sehr viel zu tun haben. Vor allem die Sicherheitskomponenten fallen mangels Schutz vor IPv6-Angriffen beim Einsatz der Übergangsverfahren negativ auf. Je schneller die Internet-Provider ihre Netze auf natives IPv6 – für maximale Kompatibilität möglichst auf Dual-Stack – umstellen, desto besser. Sie dürfen dabei allerdings nicht vergessen, ihre Kunden zu unterstützen. (un)

Dominique Petersen
ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit der Westfälischen Hochschule Gelsenkirchen und seit Januar 2007 Projektleiter für den Bereich Internet-Frühwarnsysteme.

Prof. Norbert Pohlmann
ist geschäftsführender Direktor des Instituts für Internet-Sicherheit und Professor an der Westfälischen Hochschule Gelsenkirchen und Leiter des Master-Studiengangs Internet-Sicherheit.