GCCSI

Ihr Dienstleister in:

Gürbüz Computer Consulting & Service International 1984-2007 l Önder Gürbüz l Aar Strasse 70 l 65232 Taunusstein
info@gccsi.com l +49 (6128) 757583 l +49 (6128) 757584 l +49 (171) 4213566

IPv6 kommt 2011: So wird man fit für das neue Protokoll

Die Deutsche Telekom wird nächstes Jahr IPv6 für alle DSL-Anschlüsse anbieten. Andere große ISPs werden nachziehen. ZDNet zeigt, was das neue Protokoll bietet und was man wissen muss, um es ohne Probleme optimal zu nutzen.

Die Deutsche Telekom hat letzte Woche angekündigt, alle DSL-Anschlüsse bis Ende 2011 auf IPv6 aufzurüsten. Für Privatkunden gibt es einen Pilotversuch ab Mitte 2011. Im Geschäftskundenbereich wird der Regelbetrieb für die Dienste Peering und Transit bereits im ersten Quartal nächsten Jahres starten.

Wenn der Ex-Monopolist vorangeht, dürften auch die anderen großen Anbieter von Breitbandinternetanschlüssen via DSL und Kabel nicht mehr lange auf sich warten lassen und in nicht allzu ferner Zukunft IPv6-Dienste anbieten. Das ist allein schon deswegen notwendig, weil die IPv4-Adressen langsam knapp werden.

Daher bekommen in vielen asiatischen Ländern private Internetnutzer schon heute keine öffentliche IPv4-Adresse mehr. In Deutschland vergeben Mobilfunkanbieter zunehmend nur noch private IP-Adressen. O2 vergibt grundsätzlich keine öffentliche Adressen. Bei Vodafone gibt es öffentliche IP-Adressen nicht in den günstigen Websessions-Tarifen.

Die Einführung von IPv6 stellt sicher, dass jeder Privatkunde genügend öffentliche IP-Adressen erhält. IPv4 und IPv6 werden bei allen Anbietern parallel betrieben, das heißt, man kann sowohl mit IPv4 als auch mit IPv6 im Internet kommunizieren. Das wird von allen Betriebssystemen unterstützt.

Diese Dual-Stack-Implementierung ist notwendig: Fast alle öffentlichen Server im Internet verfügen heute ausschließlich über eine IPv4-Adresse. Sie sind per IPv6 gar nicht erreichbar. Man kann also über IPv6 nur mit Rechnern kommunizieren, die ebenfalls über IPv6 verfügen.

In der Anfangsphase ergeben sich daher vor allem Vorteile in der Kommunikation zwischen Endbenutzern. So wird beispielsweise das P2P-Filesharing deutlich vereinfacht, da kein NAT mehr erforderlich ist. Beim Filesharing muss ein IPv4-NAT-Router häufig Verbindungstabellen zu mehreren hundert Peers verwalten. Das zwingt einen Consumer-Router schnell in die Knie. Der Durchsatz beträgt dann nur ein Bruchteil dessen, was die Leitung erlauben würde.

Ein anderer Einsatz sind Netzwerkspiele. Serverlose Spiele, die man heute nur im LAN spielen kann, lassen sich mit IPv6 auch über das Internet aufsetzen. Allerdings ist zu beachten, dass viele existierende Spiele anders als die meisten P2P-Filesharingprogramme kein IPv6 unterstützen.

Bei Spielen, die einen Server erfordern und IPv6 unterstützen, muss der Server nicht mehr notwendigerweise bei einem Hoster aufgestellt werden. Dazu lässt sich auch ein Rechner zuhause verwenden. Voraussetzung ist natürlich, dass man über eine ausreichend schnelle Internetverbindung verfügt.

Einfacher wird es auch für Nutzer, die von unterwegs auf Rechner oder andere Endgeräte wie digitale Videorecorder zugreifen möchten. Mit IPv6 ist es kein Problem, Rechner per Remote Desktop oder VNC fernzusteuern beziehungsweise Dateien zu kopieren.

Wer IPv6 schon nutzen oder testen möchte, bevor es der eigene Internetprovider anbietet, hat die Möglichkeit, kostenlos verschiedene Tunnelmechanismen zu nutzen. Für jeden Internetanschluss lässt sich 6to4 einrichten, wenn der NAT-Router das unterstützt. Eine andere Möglichkeit besteht darin, sich bei einem Tunnelbroker wie SixXS eine IPv6-Anbindung zu holen. Das hat aber den Vorteil, dass man feste IPv6-Adressen bekommt und die Anbindung auch von einem Rechner mit privater IPv4-Adresse aus realisieren kann.

Wer heute schon seinen DSL-Anschluss für IPv6 fit machen möchte, braucht vor allen Dingen einen IPv6-fähigen DSL-Router. Viele Router unterstützen heute bereits IPv6, beispielsweise alle neueren Fritzbox-Modelle wie die 7390 oder 7270.

Wie es bei den Kabelanbietern aussieht, lässt sich derzeit noch nicht abschätzen. Anders als die DSL-Anbieter vergeben sie die IP-Adressen nicht über PPP, sondern über DHCP. Das erlaubt den Anschluss beliebig vieler Rechner an das Kabelmodem über einen einfachen Ethernet-Switch, ohne dass ein Router erforderlich ist. Welche technische Lösung die Kabelprovider für IPv6 anbieten werden, kann man aber noch nicht sagen.

Für DSL-Anschlüsse ist bei der Nutzung von nativem IPv6 keine spezielle Unterstützung für Tunnelungsmechanismen erforderlich. Jeder IPv6-fähige Router unterstützt natives IPv6 via PPP. Sobald der Provider IPv6 anbietet, kann es losgehen.

Bei den Betriebssystemen braucht man sich keine Gedanken machen. Alle aktuellen OS unterstützen IPv6. "Produktionsqualität" haben Windows ab XP SP1, Mac OS X ab 10.3 und alle Linux-Varianten ab Kernel 2.6. Auch andere Betriebssysteme wie FreeBSD oder Solaris bieten in neueren Versionen volle Unterstützung für IPv6.

Grundsätzlich funktioniert IPv6 nur mit Programmen, die das Protokoll explizit unterstützen. Da das Anpassen einer bestehenden Anwendung auf IPv6 in der Regel trivial ist, kommt aktuelle Software meist mit IPv6 zurecht. Dazu zählen etwa alle gängigen Browser und P2P-Filesharingprogramme. Allerdings muss man immer im Einzelfall prüfen, ob eine Programm IPv6-fähig ist.

IPv6-Adressen sind 128 Bit lang. Sie werden hexadezimal notiert und nach jeweils 16 Bit wird ein Doppelpunkt geschrieben. Eine gültige IPv6-Adresse ist beispielsweise *2001:0db8:1234:5678:0000:0000:0000:0001*. Führende Nullen dürfen weggelassen werden. Die genannte IPv6-Adresse könnte also auch als *2001:db8:1234:5678:0:0:0:1* notiert werden.

Bestehen ein oder mehrere komplette 16-Bit-Blöcke zwischen zwei Doppelpunkten nur aus Nullen, darf man das einmal durch zwei Doppelpunkte abkürzen, so dass sich bei der Beispieladresse *2001:db8:1234:5678::1* ergibt. In einer IPv6-Adresse darf die Abkürzung durch zwei Doppelpunkte nur ein einziges Mal verwendet werden.

Bei IPv4 gibt man IP-Adresse und Port häufig in der Form <Adresse>:<Port>, beispielsweise *192.168.0.5:8080* an. Da der Doppelpunkt Bestandteil von IPv6-Adressen ist, muss eine IPv6-Adresse in eckige Klammern gesetzt werden, wenn sie mit einem Port zusammen benutzt wird. Im Browser ist etwa *http://[2001:db8:1234:5678::1]:8080* eine korrekte IPv6-URL.

Bei IPv4 sind alle Adressen, für die keine Ausnahme definiert ist, öffentliche IP-Adressen. Eine solche Ausnahme sind beispielsweise die privaten Adressräume *192.168.0.0/*16 und *10.0.0.0/8*. Unter IPv6 zählen nur die Adressen 2000::/3 (Adressen, die mit einer zwei oder einer drei beginnen) zum öffentlichen Adressraum.

Eine besondere Adresse ist die ::1. Sie bezeichnet den eigenen Rechner (localhost) und entspricht der Adresse 127.0.0.1 in IPv4. Allerdings gibt es nur eine einzige localhost-Adresse. In IPv4 ist jede Adresse aus dem Bereich 127.0.0.0/8 eine lokale IP-Adresse. Alle IPv6-Adressen aus dem Bereich ff00::/8 (alle Adressen, die mit *ff* beginnen) sind Multicast-Adressen.

Obwohl man den IPv6-Adressraum wie bei klassenlosen IPv4-Adressen nach Belieben bitweise aufteilen kann, gilt für LANs faktisch immer, dass die ersten 64 Bit das Netz und letzten 64 Bit den Host bezeichnen. Wer in einem LAN, etwa seinem Heimnetz, das Prefix 2001:db8:1:2::/64 vom Internetprovider zugeteilt bekommt, kann die Adressen *2001:db8:1:2::0* bis *2001:db8:1:2:ffff:ffff:ffff:ffff* nutzen. Das sind 18.446.744.073.709.551.616 öffentliche IPv6-Adressen.

Die Deutsche Telekom hat angekündigt, sogar /56-Prefixe zu vergeben. Damit haben auch Privatkunden die Möglichkeit, 256 /64-Netze (LANs) mit einem einzigen DSL-Anschluss zu versorgen. Allerdings ist dieses Features eher für Geschäftskunden interessant, die etwa besonders sicherheitsempfindliche Bereiche haben und in einem eigenen Netz besonders absichern möchten. Einige andere DSL-Provider, die heute schon IPv6 anbieten, etwa tal.de oder portunity.de bieten zum Teil auch /48-Netze an.

Private Adressebereiche in IPv6

Obwohl man unter IPv6 eigentlich keine privaten Adressen benötigt, ist ein Bereich dafür reserviert worden. Private IPv6-Adressen heißen "Unique Local Addresses" (ULA). Sie stammen aus dem Bereich fc00::/7 (alle Adressen, die mit *fc* oder *fd* beginnen). Für die Adressen, die mit *fc* beginnen, ist vorgesehen, dass man sie wie öffentliche Adressen registrieren kann. Eine solche Registrierungsstelle existiert jedoch noch nicht. Die ULAs, die *fd* beginnen, werden wie private IPv4-Adressen ohne Registrierung benutzt.

Wer private IPv6-Adressen benutzen möchte, sollte möglichst nicht Adressen wie *fd00::1* oder *fd00::2* verwenden. Wer stattdessen beispielsweise fd12:7e6f:8ab1:84b7::1 nutzt, kann nahezu ausschließen, dass es einen Konflikt mit anderen privaten Adressen gibt. Das ist vor allem bei Firmenfusionen wichtig. Unter IPv4 kommt es bei Fusionen häufig zu Problemen, wenn beide Unternehmen bisher den Adressraum 192.168.0.0/24 genutzt haben.

Heimanwender können ULAs bei der Fehlerdiagnose einsetzen: Einige Router, etwa die Fritzbox, vergeben an ihre Clients ULAs mit *fd* am Anfang, wenn die Fritzbox keine korrekte IPv6-Verbindung bekommen hat. Dabei ist zu beachten, dass ein Beheben des Fehlers am Router nicht ausreicht. Die Clients behalten ihre ULA nämlich eine Weile und können nicht mit dem Internet kommunizieren. Das einfachste ist es, das Netzwerkinterface zu deaktivieren und danach wieder zu aktivieren. Dann erhält die LAN- oder WLAN-Karte eine öffentliche IPv6-Adresse.

Neben den privaten Adressen gibt es linklokale Adressen. Dafür ist der Bereich *fe80::/10* reserviert. Dem Bereich *fe80::/64* (Adressen, die mit *fe80:0:0:0:* beginnen) kommt dabei eine besondere Bedeutung zu. Jedes Netzwerkinterface benötigt eine solche Adresse zusätzlich zu ihrer eigentlichen IPv6-Adresse. Damit kann es im LAN kommunizieren und unter anderem autokonfiguriert werden. Linklokale Adressen werden überhaupt nicht geroutet, auch nicht innerhalb der eigenen Organisation.

Beim Hochfahren eines Netzwerkinterfaces wird der Hostteil der linklokalen Adresse durch die MAC-Adresse bestimmt. Eine Netzwerkkarte mit der MAC-Adresse *00:1e:37:d9:68:19* erhält die linklokale Adresse *fe80::21e:37ff:fed9:6819*. Mit dieser Adresse kann die Netzwerkkarte unter anderem die Autokonfiguration einleiten oder einen DHCPv6-Server finden.

In kleineren Netzwerken verwendet man anders als bei IPv4 normalerweise kein DHCP, sondern die Autokonfiguration. Dazu sendet ein Client mit seiner linklokalen Adresse eine Anforderung an die Multicast-Adresse *ff02::2*. Jeder Router muss auf diese Adresse hören. Anschließend schickt der Router ein Paket zurück, dass den Netzwerkteil der IPv6-Adresse enthält und die Destinationen, die man über ihn erreichen kann, etwa *2000::/3* für das Internet.

Der Hostteil der Adresse ist identisch mit dem Hostteil aus der linklokalen Adresse. Ein Rechner mit der linklokalen Adresse *fe80::21e:37ff:fed9:6819*, der vom DSL-Router das Netzwerkprefix *2001:db8:1234:5678::/64* bekommen hat, erhält also die öffentliche IPv6-Adresse *2001:db8:1234:5678:21e:37ff:fed9:6819*.

Damit ist die IPv6-Verbindung ins Internet hergestellt. Allerdings hat der Client auf diese Weise keinen DNS-Server bekommen. Der DNS-Server gehört zwar streng genommen nicht zu den für die IP-Connectivity notwendigen Parametern, dennoch hat man die IPv6-Autokonfiguration später um RFC 5006 erweitert.

So kann der Router seinen Clients auch einen oder mehrere DNS-Server mitteilen, ohne dass dafür extra ein DHCPv6-Server aufgesetzt werden muss. Wer jedoch weitere Parameter an seine Clients übergeben will, etwa NTP-Server zur Zeitsynchronisation, muss DHCPv6 aufsetzen.

Consumer Router verwenden üblicherweise die Autokonfiguration ohne DHCPv6. Dazu muss weder am DSL-Router noch an den meisten Clients etwas konfiguriert werden.

Bei Linux ist zu beachten, dass die Autokonfiguration komplett im Kernel-Code enthalten ist, allerdings mit Ausnahme der Erweiterung nach RFC 5006. Das heißt, es wird kein DNS-Server in die Datei */etc/resolv.conf* eingetragen. Um das zu erreichen, muss ein RDNSS-Client-Daemon wie *rdnssd* installiert werden. Unter Debian oder Ubuntu geht das mit dem Befehl *sudo apt-get install rdnssd*.

Unter Windows gibt es auf den ersten Blick keine Probleme. Jedoch wird man feststellen, dass der Rechner bei jedem Booten eine andere IPv6-Adresse bekommt. Das ist allerdings kein Bug, sondern ein Feature: Windows aktiviert nämlich standardmäßig die Privacy Extensions nach RFC 4941.

Mit einer ständigen wechselnden IP-Adresse soll die Identität eines Nutzers besser geschützt werden. Das ist aber insofern wenig sinnvoll, da in einem Heimnetz der Anschlussinhaber alleine anhand des Netzprefixes identifiziert werden kann.

Wer einen Windows-Rechner über IPv6 auch von unterwegs erreichen möchte, sollte ihm eine feste IPv6-Adresse geben. Das erreicht man am einfachsten von einer Kommandokonsole mit Administratorrechten, indem man die Befehle *netsh interface ipv6 set privacy state=disabled store=persistent* und *netsh interface ipv6 set global randomizeidentifiers=disabled store=persistent* eingibt.

Das IPv6-Protokoll wird kommen. Für die DSL-Kunden der Deutschen Telekom ist es spätestens Ende nächsten Jahres so weit. IPv6 wird noch viele Jahre zusammen mit IPv4 angeboten werden. Wer jedoch neue Möglichkeiten nutzen möchte, kommt an IPv6 nicht vorbei.

Das betrifft vor allem die direkte Kommunikation zwischen Endbenutzern. Auch Anwendungen, die nur sehr umständlich oder langsam über NAT genutzt werden können, dürften in Zukunft ausschließlich über IPv6 funktionieren. Niemand wird sich mehr die Mühe machen, IPv4-NAT-Kompatibilitätscode zu entwickeln.

Man sollte sich daher langsam mit dem neuen Protokoll vertraut machen. Grundsätzlich ist eine automatische Konfiguration noch einfacher als mit IPv4, da nicht einmal ein DHCP-Server benötigt wird. DHCPv6 kommt nur bei komplexen Konfigurationen zum Einsatz. Wer einen IPv6-fähigen DSL- oder Kabelrouter anschafft, muss nicht viel einstellen.

Trotzdem gibt es einige Besonderheiten, die man wissen sollte: So hat Windows die Privacy Extensions nach RFC 4941 standardmäßig eingeschaltet, was weniger zu "Privacy", aber dafür zu umso mehr Problemen führt. Unter Linux ist es in der Regel erforderlich, einen RDNSS-Client-Daemon zu installieren, wenn man seinen DNS-Server automatisch zugewiesen haben möchte.

Außerdem sollte man sich den neuen Adressen vertraut machen. Es ist wichtig zu wissen, wie eine IPv6-Adresse aufgebaut ist, und was der Unterschied zwischen öffentlichen, privaten und linklokalen IP-Adressen ist.

Nur wer über das ausreichende Basiswissen verfügt, kann bei Problemen schnell reagieren, etwa wenn der Windows-Befehl *ipconfig* die private IPv6-Adresse fd29:439a:9391:98ec:201:10ff:fe93:45c anstelle einer öffentlichen anzeigt.

Artikel aus ZDNet

http://www.zdnet.de/magazin/41539006/ipv6-kommt-2011-so-wird-man-fit-fuer-das-neue-protokoll.htm