

FAQ IPv6

Antworten auf die häufigsten Fragen

VON HOLGER ZULEGER UND
CARSTEN STROTMANN

IPv4 zu Gunsten von IPv6 abschalten

? Kann ich mein lokales Netz komplett von IPv4 auf IPv6 umstellen?

! Technisch gesehen geht das, aber solange es IPv4-Geräte und -Server auf der Welt in nennenswerter Zahl gibt, sollten Ihre Geräte am besten beide Protokolle sprechen, also IPv4 und IPv6 parallel. Das gewährleisten Provider und Router beispielsweise mit der Dualstack-Technik. Falls Sie testweise IPv4 abschalten wollen, kann man die Kommunikation von IPv6 zu IPv4 mit Übersetzungsinstanzen gewährleisten (NAT64-Gateway, RFC 6146). NAT64-Gateways gibt es für Linux als Open-Source-Pakete (siehe c't-Link am Artikelende), aber auch als Option in Routern für Unternehmensnetze, etwa von Cisco oder Juniper.

Daneben braucht man einen Domain Name Server mit DNS64 (RFC 6147), der Anfragen nach Hostnamen, die nur per IPv4 erreichbar sind, mit konstruierten IPv6-Zieladressen beantwortet, die die IPv4-Zieldressen enthalten. Das beherrschen die meisten verbreiteten Name-server bereits: BIND ab Version 9, PowerDNS Recursor ab 3.4 und Unbound ab 1.5.

Viele IPv6-Adressen

? Warum sind auf meinem Netzwerk-Interface so viele IPv6-Adressen zu sehen?

! Alle modernen Betriebssysteme sind für IPv6 ausgelegt und nutzen das Protokoll automatisch. Die mit fe80:: beginnende Adresse ist die konstante Link-Local-Adresse. Sie dient zur Kommunikation im LAN. Pakete, die diese Absenderadresse verwenden, darf der Router per Definition nicht ins Internet schicken. Die zweite Hälfte einer solchen Adresse (Suffix) ist bei Linux und OS X aus der MAC-Adresse abgeleitet. Windows erwürfelt sie

bei der Systemeinrichtung. Falls der Router per IPv6 mit dem Internet kommunizieren kann, dann annouciert er üblicherweise ein Präfix im LAN (erste Adresshälfte) – beispielsweise 2001:db8:1803:101:: und dann hat ein PC mindestens eine weitere konstante IPv6-Adresse, nämlich die global gültige für die Kommunikation mit dem Internet. Der Suffix ist bei der link-lokalen und der globalen Adresse derselbe.

Zusätzlich erwürfeln viele IPv6-fähige Geräte noch temporäre globale Adressen. Diese sind aus Datenschutzgründen nur für den vorübergehenden Gebrauch ausgelegt (IPv6 Privacy Extensions). Weil deren Gültigkeit unter anderem wegen eventuell lange anhaltender TCP-Verbindungen immer größer ist als das Neubildungsintervall, sammeln sich zu jeder Schnittstelle im Laufe der Zeit einige solcher Adressen an. Bei Hosts, die lange laufen, sind daher insgesamt neun IPv6-Adressen üblich, weil standardmäßig täglich eine neue temporäre Adresse gebildet wird, die sieben Tage gilt.

IPv6-Problemdiagnose

? Wie erkenne ich, ob IPv6 Verbindungsprobleme verursacht?

! Klären Sie zunächst, ob die Anwendung mit IPv4 funktioniert. Schalten Sie dazu IPv6 vorübergehend ab. Falls es mit IPv4 geht, isolieren Sie mit folgenden Prüfschritten die Fehlerquelle: Testen Sie, ob die IPv6-Verbindung ins Internet funktioniert, beispielsweise per Ping auf einen bekannt IPv6-fähigen Host. Unter Windows geht das am schnellsten auf der Kommandozeile mit `ping -6 ct.de`. Das „-6“ erzwingt einen IPv6-Ping, denn sonst würde Windows unter Umständen auf IPv4 zurückfallen, was man nur an der Antwort erkennt. Kommt die Antwort von einer Adresse wie `2a02:2e0:3fe:1001:302::`, funktioniert nicht nur IPv6, sondern auch die Namensauflösung für IPv6-Anfragen (AAAA-Records).

Unter Linux und OS X lautet das Kommando `ping6 ct.de`. Wenn der Befehl

Paketlaufzeiten liefert, ist alles gut. Meldet er jedoch „Unknown host“ oder „...nodename ... not known“, hat das Ziel keinen IPv6-DNS-Eintrag. Das ist zurzeit etwa bei `twitter.com` der Fall. Windows antwortet in solchen Fällen, dass es den Host nicht finden kann. Der DNS-Eintrag lässt sich mit Bordmitteln unter Windows per `nslookup twitter.com` auf der Kommandozeile prüfen. Bei Linux und OS X nimmt man `host twitter.com`. Wenn dann zwei Adresstypen erscheinen, sollte der Host per Ping6 erreichbar sein.

Im Anschluss an die grundsätzlichen Tests prüfen Sie mit `ping -6` beziehungsweise `ping6`, ob sich die gewünschte Gegenstelle Ihrer Anwendung per IPv6 erreichen lässt. Antwortet sie auf die Pings, liegt das Problem mit hoher Wahrscheinlichkeit nicht an IPv6, sondern an der Anwendung.

IPv6-Adressverkürzung

? Was kann ich bei Angabe von IPv6-Adressen weglassen, um mir Tipparbeit zu sparen?

! Führende Nullen in den 4er-Blöcken können entfallen. Außerdem darf man genau einmal eine Nullenserie durch :: ersetzen; das können auch mehrere 4er-Blöcke hintereinander sein. Aus `2001:0db8:0006:0000:0000:0030:0000:0001` wird so `2001:db8:6::30:0:1`. Falls Sie einen DNS im LAN betreiben, empfiehlt es sich, die IPv6-fähigen Hosts ins DNS aufzunehmen – so können Sie jeden anhand seines sprechenden Namens verwalten. Mehr dazu finden Sie im Beitrag ab Seite 144.

Zertifikate

? Gibt es etwas IPv6-Spezifisches bei Zertifikaten zu beachten?

! x509-Zertifikate sollten auf Hostnamen ausgestellt sein, nicht auf IP-Adressen. Daher gibt es bei den Zertifikaten weiter nichts zu beachten.

IPv6 auf Tablets & Co

? Sind Smartphones, Tablets und IP-TVs auch für IPv6 geeignet?

! Das hängt sehr vom Hersteller ab, ob solche Geräte für IPv6 ausgelegt sind. Aktuell hängt IP-TV hinterher, Smartphones und Tablets sollten im Allgemeinen kein Problem mit IPv6 haben. Aber es gibt weiterhin Applikationen, die nur für IPv4 ausgelegt sind, zum Beispiel die Twitter-App.

Einfache Gerätesuche

? Wie finde ich IPv6-Geräte in meinem LAN?

! Es gibt verschiedene Methoden dafür. Ein IPv6-Werkzeug bietet sich mit Node Information Querys an (RFC 4620). Damit lassen sich Netzwerkkonfigurationen von entfernten Rechnern per ICMPv6 abfragen – beispielsweise Hostnamen. Eine Node Information Query lässt sich per ping6-Befehl an die Multicast-Adresse ff02::1 absetzen (all-nodes). In diesem Beispiel wird der Befehl über die Schnittstelle en0 abgesetzt:

```
ping6 -c 2 -I en0 -w ff02::1
```

In der Ausgabe sind alle aktiven IPv6-Rechner des lokalen Netzwerksegments zu sehen, die auf ICMP-Echo-Request antworten. Ein Beispiel:

```
PING6 fe80::03e0%en0 --> ff02::1
59 bytes from fe80::03e0%en0:
MacBook-Pro.local
56 bytes from fe80::bda%en0:
Mac-mini.local
59 bytes from fe80::03e0%en0:
MacBook-Pro.local
```

Im Beispiel sind zwei aktive Macs zu sehen, ein MacBook Pro, von dem die Anfrage ausgeht und ein Mac Mini – der in diesem Fall als IPv6-Router arbeitet. Mit „-w“ fragen Sie nach den Hostnamen der Maschinen; mit „-c 2“ senden Sie zwei ICMPv6-Anfragen. Das ist erforderlich, weil die erste Anfrage immer von der eigenen Maschine beantwortet wird; erst

auf die zweite hin melden sich die anderen. Ping6 mit dem Parameter „-a agl“ liefert Information über alle konfigurierten IPv6-Adressen der lauschenden Geräte. Im Beispiel ist die Ausgabe gekürzt:

```
ping6 -c 2 -I en0 -a agl ff02::1
PING6() fe80::03e0%en0 --> ff02::1
136 bytes from fe80::03e0%en0:
 fe80::1(TTL=infty)
 fe80::03e0(TTL=infty)
 2001:db8::03e0(TTL=86029)
```

In der Antwort sind alle Rechner aufgeführt, die im gleichen IPv6-Subnetz stecken. Es lassen sich aber weitaus mehr Informationen erfragen. Ein bequemes Werkzeug dafür ist das Shell-Script `ipv6finder.sh` für Linux und Mac OS X (siehe c't-Link).

Netzwerk-Tools

? Sind die üblichen Linux-Netzwerk-Tools wie ping, route, traceroute, netcat oder netstat für IPv6 geeignet?

! Für Linux-Nutzer gibt es auf www.deeptime.net eine Übersicht über Netzwerk-Tools, die für IPv6 ausgelegt sind.

IPv6 ohne Nameserver

? Ich habe keinen Nameserver, der über IPv6 erreichbar ist. Kann ich IPv6 trotzdem nutzen?

! Ja, wenn der Nameserver in Ihrer Dual-Stack-Umgebung auf IPv4 antwortet. Welches Transportprotokoll für die DNS-Anfragen und -Antworten verwendet wird, spielt keine Rolle. Der Nameserver muss aber Anfragen nach IPv6-Adressen beantworten können (Typ AAAA). In einer IPv6-only-Umgebung muss zumindest der Resolver ein Dual-Stack-System sein. Sonst braucht er einen Dual-Stack-Nameserver zur Unterstützung. Denn es gibt noch zahlreiche Domains, deren Nameserver nur über IPv4 erreichbar sind.

Default-Route setzen

? Wie wird die Default-Route bei Endgeräten gesetzt?

! In der Regel erfahren Hosts die Default-Route automatisch über die Router Advertisements. Man kann sie zwar auch manuell konfigurieren, aber damit beraubt man sich der automatisierten Konfiguration sowie redundanter Next Hops. Bei IPv6 dürfen nämlich mehrere Router ein LAN mit Internetzugängen versorgen (einfaches Load Balancing).

Eingehende IPv6-Verbindungen

? Was bedeuten auf Linux bei `netstat -nat` die Zeilen, die mit `tcp6` anfangen? Und wie finde ich heraus, welche Dienste auf eingehende IPv6-Verbindungen mit IPv6 warten?

! Der Befehl `netstat -nat` führt Dienste auf, die auf TCP-Ports auf IPv6-Connects warten oder bereits geöffnet haben. Der Befehl

```
lsof -i6 | grep -v "ESTABLISHED"
```

führt auf, welche Dienste auf eingehende IPv6-Verbindungen warten.

Firewall-Einmaleins

? Wie stelle ich sicher, dass niemand durch einen IPv6-Tunnel in mein LAN hinter die Firewall hineinreitet?

! Dafür genügen dieselben Vorsichtsmaßnahmen, die man auch bei IPv4 anwendet: Im Router und in den PCs sollten Teredo- und sonstige IPv6-Tunnel abgeschaltet sein. Auf Router und Hosts sollten die IPv6-Firewalls sämtlichen unverlangt eingehenden Verkehr verwerfen. Viele Router sind schon ab Werk so eingestellt. (dz@ct.de)

Shell-Skript: ct.de/yfq