Public IPv6 in Freifunk Netzen - Betrachtung für Freifunk Kiel

Nis Börge Wechselberg

November 2016

Der erste Teil dieses Dokumentes soll den aktuellen Stand des Netzes und die Änderungen für die Einführung von IPv6 im Freifunk Netz Kiel dokumentieren. Im zweiten Teil werden häufige Fragen und Probleme gesammelt und beantwortet.

1 Aktueller Stand

Das Freifunk Netz in Kiel verwendet sowohl IPv4 als auch IPv6 Adressen. Allerdings sind beide Adresstypen nicht global, also im gesamten Internet, sondern nur innerhalb des Freifunk Netzes gültig.

Für IPv4 wird das Netz 10.116.0.0/16 gemäß RFC1918[1] verwendet. Dieses Netz wird (fast) nicht innerhalb der Knoten verwendet, sondern mittels DHCP an die Clients verteilt. Für den Zugang zum Internet wird mittels *Network Address Translation (NAT)* in den Gateways eine Verbindung hergestellt. Im Internet treten somit erstmal nur die Gateways in Erscheinung.

Für IPv6 wird das Netz fda1:384a:74de::/48 gemäß RFC4193[2] verwendet. Auch diese IP Adressen sind speziell für die interne Verwendung vorgesehen. Dieses Netz wird an Knoten sowie an Clients verteilt. Da auch diese Adressen nicht globale Gültigkeit besitzen können sie nicht im Internet verwendet werden.

2 Vorgeschlagene Änderungen

Mit der Einführung von "echtem" IPv6 würden den Knoten und den Clients Adressen aus einem global gültigen Adressbereich zugewiesen werden (bzw. sich aussuchen). Sowohl Endgeräte als auch Knoten könnten direkt Verbindungen mit dem gesamten Internet aufbauen. Eine Übersetzung der internen Adressen wäre nicht mehr nötig.

[1] Siehe `https://tools.ietf.org/html/rfc1918`
[2] Siehe `https://tools.ietf.org/html/rfc4193`

Die bisherigen "lokalen" IPv6 Adressen wären weiterhin für die interne Kommunikation im Freifunk Netz nutzbar.

3 Fragen und Antworten

Warum ist IPv6 überhaupt nötig?

Der Vorrat von IPv4 Adressen ist verbraucht. In Zukunft werden nicht mehr alle Dienste mittels IPv4 erreichbar sein. Für ein zukunftsfähiges Netz ist früher oder später die Einführung von IPv6 unumgänglich. Zusätzlich wurden mit IPv6 einige "Fehler", die in IPv4 existieren, behoben. Dies betrifft besonders strengere Regeln, wie sich Geräte im Netzwerk verhalten sollen. Eine Perspektive ist, dass mit IPv6 die Netze besser und einfacher funktionieren sollen.

Was ändert sich, wenn ich IPv6 habe?

Für den Endbenutzer sollte sich (in einer idealen Welt) nichts ändern. Allerdings ist nicht auszuschliessen, dass während der weltweiten Umstellung von IPv4 auf IPv6 ab und zu Störungen auftreten können.

Ich habe gehört, IPv6 ist unsicherer als IPv4. Stimmt das?

Diese Fragen hat viele Antworten. Grundsätzlich gilt erstmal "nein".

Bei IPv4 kann mich wegen NAT niemand direkt erreichen. Das ist sicherer!

Nein. NAT hat nur wenig mit Sicherheit zu tun. Mit geschickt gebauten Datenpaketen kann auch ein NAT durchbrochen werden. Ausserdem ist es im Freifunk Netz nicht schwer auf die "innere" Seite des NAT zu gelangen, da das Netz eh frei zugänglich ist.

Aber warum kommt dann niemand zu meinem IPv4 Gerät durch?

Üblicherweise verfügen Heimrouter neben dem NAT auch über eine Firewall. Diese wird in den Geräten gerne mit dem IPv4-NAT kombiniert, so dass sie nicht so auffällig ist. Diese Firewall lässt nur eingehende Daten zu, wenn zuvor eine ausgehende Verbindung aufgebaut wurde. So eine Firewall ist aber auch in praktisch allen Betriebssystemen mitgeliefert oder verfügbar.

Kann ich auch eine Firewall mit IPv6 verwenden?

Das kommt darauf an. Am Endgerät kann (und sollte) so eine Firewall problemlos weiterhin eingesetzt werden. Auf den Gateways kann das nicht mehr so einfach gemacht werden, da bei IPv6 durchaus die ausgehenden Verbindungen über einen anderen Gateway erfolgen, als die eingehenden Verbindungen. Somit ist eine Firewall in den Gateways nicht mehr so einfach möglich. (Und im Allgemeinen auch nicht gewollt.)

Wenn jemand meine IPv6 bekommen hat, dann kann er einen Port Scan machen und rausfinden, was noch so auf meinem Gerät läuft. Das geht bisher mit NAT nicht!

Das liegt nicht an NAT, sondern wieder an der Firewall. Diese Sicherheit muss aber auf den Endgeräten umgesetzt werden und ist keine Aufgabe eines offenen Netzes.

Zusätzlich ist es auch zur Zeit schon möglich den selben Portscan innerhalb des Freifunk Netzes durchzuführen. Wir betreiben ein offenes Netz für jeden.

Durch NAT tauche ich aber nicht direkt im Netz auf. So kann ich nicht identifiziert werden.

Das ist korrekt. Bei IPv6 wird (üblicherweise) ein Teil der Adresse aus der MAC-Adresse des Endgeräts gebildet. Diese MAC ist einzigartig im Netz und ändert sich auch nicht. Somit wäre eine Verfolgung des Endgeräts durch das Netz möglich. *Aber:* Bei IPv6 hat ein Gerät nicht nur eine Adresse sondern kann diverse verschiedene Adressen haben. Um die Identität der Nutzer besser zu schützen wurden die IPv6 Privacy Extensions[3] entwickelt.

Was bringen die IPv6 Privacy Extensions?

Wenn Privacy Extensions (PEX) aktiviert sind, generiert das Endgerät sich regelmäßig neue IPv6 Adressen. Die generierten Adressen sollten zufällig und nicht zu einer MAC-Adresse rückverfolgbar sein. Wenn das Endgerät nun eine Verbindung aufbaut, wird diese zufällige Adresse genutzt.

Diese Erweiterungen sind in praktisch allen Systemen heutzutage standardmäßig aktiviert[4]. Microsoft Windows unterstützt PEX seit Windows Vista, Android seit Version 4.0[5] und iOS seit Version 4.3[6].

[3] `https://tools.ietf.org/html/rfc4941`
[4] Siehe auch den Heise Artikel von 2011 unter `http://heise.de/-1204783`
[5] Aktueller Marktanteil für Geräte mit Android < 4.0 ca. 2 %
[6] Aktueller Marktanteil für Geräte mit iOS < 4.3 weniger als 1 %