Sei Dein eigener ISPv6

Matthias Bauer
bauerm@pestilenz.org

27. Dezember 2022

Disclaimer

- Bin absolut kein Experte für Large-Scale Routing
- Kein richtiges HOWTO, weils keinen kanonischen Weg gibt AFAICS.
- DNS- und IPv4/6-Basics werden vorausgesetzt

Warum?

- Ich zahle einem Provider Geld, um eine Internet-Verbindung nach Hause zu haben
- Also sollte ich da auch Server dran betreiben können

ISPs und Adressen I

1. In den 90ern/frühen 2000ern haben ISPs auf den Dialup/ISDN/DSL Anschlüssen echte IPv4 Adressen vergeben
2. Die wurden alle 24 Stundenoderso gewechselt, damit man da keine Server dran betreiben kann
3. Würgaround von damals:
   `dyndns.org`: man hat einen DNS Namen für den Server, und ändert alle naslang die zugeordnete Adresse auf die nächste

ISPs und Adressen II

1. Seit spätestens 2019 sind IPv4 Adressen solche Mangelware, dass ISPs alle Kunden auf einen ganz kleinen Pool von IPv4 Adressen NATten.
2. Die Adresse auf dem Uplink daheim ist dann eine `100.64.0.0/16` oder ähnlich "interne" Adresse
3. Da drauf kann man keine Server laufen lassen, ua. weil man schon gar nicht weiss, welche Adresse man nach aussen hätte.

IPv6 to the rescue

- Aber es gibt ja IPv6
- Das hat so viele Adressen, dass es keine Knappheit geben kann. Anschlüsse haben immer komplette /64 Netze
- Deswegen haben die ISPs den Rollout zu Kundinnen verzögert
- AFAIK bekommt man in Dtland von std-ISPs keine dauerhaften Prefixe, damit man da keine Server dran betreiben kann

ISPs und Adressen III

- Anbindungen gehen jetzt über *NAT464* oder *DS-Lite*
- In beiden Fällen läufts drauf raus, dass eine IPv6 Verbindung mit einer Middlebox (weisse Plastikdose vom Provider) aufgebaut wird
- Die Middlebox macht im Kundinnennetz ein privates IPv4 Netz, verschickt Traffic aber über IPv6 zum Provider
- Dort wird IPv4 Traffic auf eine Adresse aus einem kleinen Pool geNATet. Rückwärts das gleiche.

IPv6 to the rescue, cont.

- Damit das mit dem IPv6 Rollout schneller geht, gabs *Tunnel-provider*, die IPv6-Netze über IPv4 an Interessierte vergeben und geroutet haben
- Früher mal z.b. `sixxs.net`
- Da konnte man dann Server über Tunnel betreiben, und hatte beinahe “eigene” Netze
- Aber die haben 2017 zugemacht

Hier fängt die Geschichte an

- Damit war 2017 auch mein Servernetz weg.
- Rumgesucht, `tunnelbroker.net` von Hurricane Electric gefunden
- Aber das war kein eigenes Netz
- Und hing an dem einen Provider (wann macht der dann zu...)

Wie “hat” man ein Netz?

```
> dig +short www.ccc.de
195.54.164.39
> whois 195.54.164.39
...
CIDR:           195.0.0.0/8
NetType:        Allocated to RIPE NCC
...
inetnum:        195.54.164.0 - 195.54.165.255
...
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-END-MNT
mnt-by:         CHAOS-MNT
...
```

Wie “hat” man ein Netz? cont.

- In der `whois` Database steht `status: Assigned PI` (“Provider Independent”) und nach `mnt-by` der eigene Name (in der DB)
- (Es gibt auch “Provider Assigned” (PA), da gehört das Netz einem ISP, der es weiterreicht.)

Was tun, um ein eigenes Netz zu kriegen?

- Variante 1: einen non-std Provider finden, der ein Netz unter-vermietet ("Provider Assigned") und durch einen Tunnel anschliessen. Der ist dann die Default-Route raus und rein
- Variante 2: Local-Internet-Registrar ("Sponsor") finden, der/die beim RIPE ein Netz stellvertretend beantragt.
- Und selber um das Routing kümmern

Routing: BGP ASN OMG

- Man kann mehrere Tunnels zu verschiedenen "Transit-Providern" aufmachen $\rightarrow$ "Multihoming"
- Manche bieten das bezahlbar zum Experimentieren an
- OK, jetzt hab ich ein Netz, aber niemand in der Weiten Welt weiss, wie man Datagramme zu diesem Netz schickt
- Um in der Routingwelt mitreden zu können, braucht man einen Identifier, eine "Autonomous System Number" (AS)
- Hat mein Sponsor für mich beantragt (einmalige Gebühr)
- Damit hatte ich auch einen Zugang zur RIPE-Database, um meine Objekte dort managen zu können
- Damit wiederum konnte ich eintragen, welcher DNS Server für die Reverse-Lookups nach meinem Netz zuständig ist

Routing: BGP ASN OMG cont.

- Nachdem ich Transit-Providern
  1. Geld gegeben
  2. einen “Letter of Authorization” geschickt

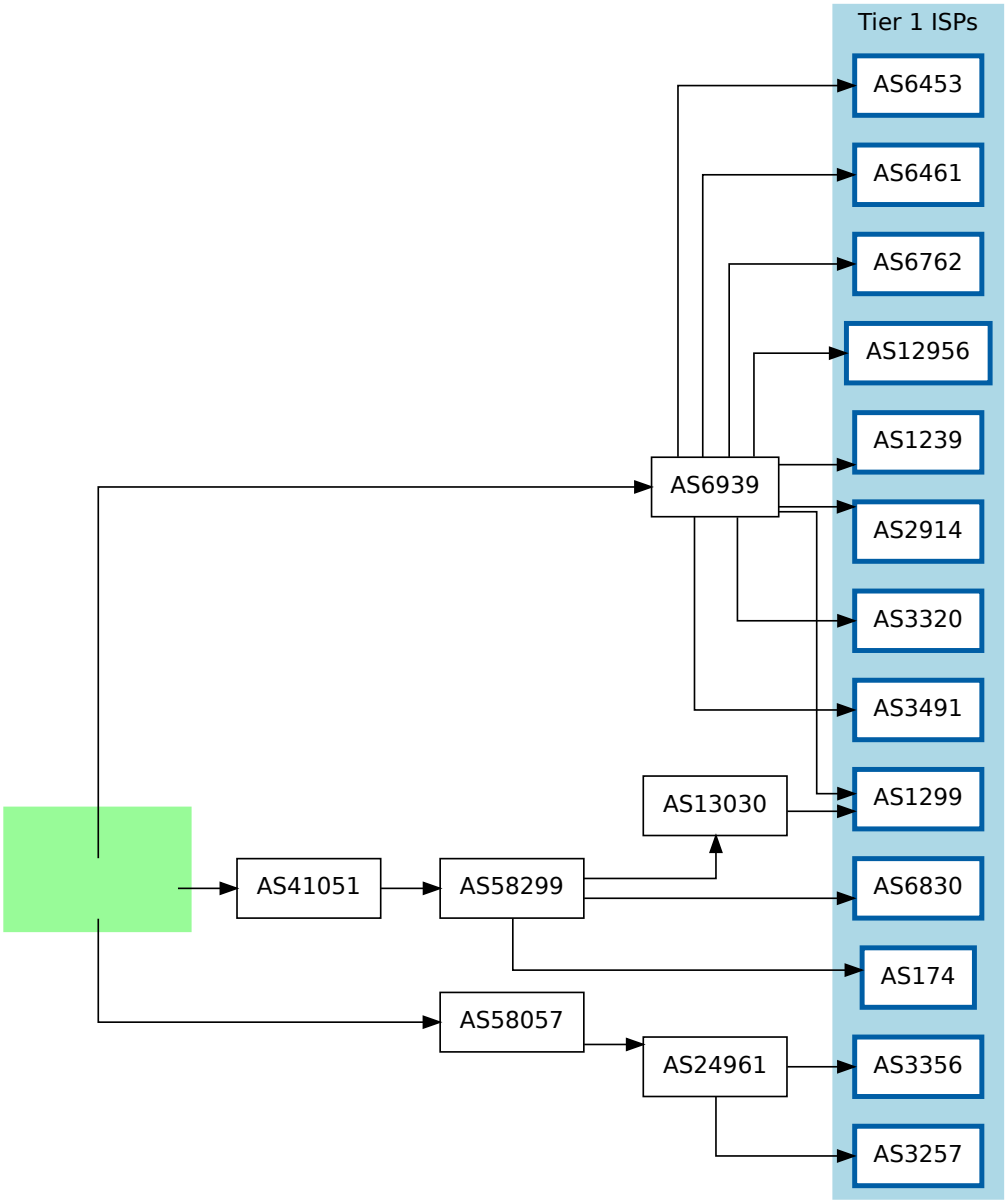
  hab, verkünden die über das “Border Gateway Protocol”, dass sie Daten für die Netze in meinem AS entgegennehmen.
- Dazu musste ich Tunnel aufbaun und einen BGP Daemon konfigurieren, mein Netz über die Provider anzukündigen
- Umgekehrt liefern die Provider mir Info, welche Netze jeweils wie erreichbar sind

Routing: BGP ASN OMG cont.

- Damit der Rest der Welt glaubt, dass meine Router was zu diesem Netz sagen dürfen, musste ich
  - ein `route` Objekt in der RIPE DB angelegt
  - an meinem `aut-num` Objekt drangeschrieben, welche anderen ASen die ankündigen dürfen, und was ich von anderen akzeptiere
  - die Route ins "hosted RPKI" eintragen lassen (signiert Eigenschaften, aber ich hab den Secret Key nicht)

Soweit

- Eignes Multihomed IPv6 /48 Netz
- Wird über drei Tunnels über zwei DSL Uplinks geroutet
- Zwei BGP Router, die rauswärts-Routen untereinander abgleichen
- Internes Routing zu einem weiteren Standort und meinem Laptop
- Tor-Bridge, Mail/Web/DNS-server per IPv6 erreichbar


Tier 1 ISPs
AS6453
AS6461
AS6762
AS12956
AS1239
AS6939
AS2914
AS3320
AS3491
AS13030
AS1299
AS41051
AS58299
AS6830
AS174
AS58057
AS24961
AS3356
AS3257

Gelernt und Cool

- Routing auf der “defaultless” Ebene ist eine eigene Welt
- OpenBGP ist einigermassen einfach zu konfigurieren
- Aus Versehen mal per `ssh` das Interface mit der Default Route auf einem Router runtergenommen $\rightarrow$ Macht nix, multihomed.
- Mancher Traffic geht über den einen Router raus nach Düsseldorf und die Antworten kommen über den anderen aus Zürich rein.
- Wenn das interne Routing klappt, hat mein Laptop überall die gleiche IPv6 Adresse, und Verbindungen laufen nach Suspend/Resume einfach weiter

Gelernt und Nicht Cool

- Tunnel machen alles langsam
- Verwaltungsaufwand und die Anzahl der Beteiligten ist erstaunlich
  (LIR, RIPE, DNS Registrar, DNS secondary, drei Tunnelprovider)
- In meinem Setup brauch ich fixe IPv**4** Adressen für die Tunnelendpunkte und den DNS server
- Das IPv6-for-Amateurs Netz ist wackelig
- Das IPv6-Netz hat Routinglöcher

Nicht Gelernt

- Peering: Man routet anderer AS Traffic durchs eigene Netz und umgekehrt
- Ist in meinem Setup wegen dem lausigen Durchsatz nicht möglich

Weiterführend

- https://dn42.eu Offenes, alternatives Internet, in dem jede/r ein AS ist.
- RIPE: How to Request an IPv6 PI Assignment
- BGP For All Playlist Playlist mit Erklärvideos
- https://chown.me/blog/getting-my-own-asn Von jemandem, der das noch viel weiter getrieben hat als ich