CHAOS IM QUADRAT
WWW.CCC-MANNHEIM.DE

IPv6
Neu sind nicht nur
128-bit
…aber eigentlich bleibt doch alles beim Alten…

fzahn

Chaos Computer Club Mannheim e.V.

2017-03-03

Was ist IPv6

- Layer 3 Protokoll zur Übertragung von Daten in paketvermittelten Netzen
- Layer3 ist die Netzwerkschicht
  - Wegewahl
- Adressraum 128 bit

IPv4 vs IPv6

- 32-bit Adressraum vs 128-bit Adressraum
- Subnetting im IPv4-> Adressknappheit
- IPv4 bietet in der Praxis of keine Ende-zu-Ende-Adressierung (NAT-Router)
- im Internet am 1.3.2017: mehr als 626000 IPv4 Präfixe und 29700 IPv6 Präfixe

Vorteile

- deutlich größerer Adressraum
  - zukunftssicher
  - erlaubt die Vergabe ganzer Netze anstelle von einzelnen IPs an Kunden
- NAT nicht erforderlich

Vorteile

- Ende-2-Ende Konnektivität
- Multihoming
- Vereinfachte Umnummerierung

Nachteile von IPv6

- Adressen sind für $Mensch deutlich schwerer lesbar und merkbar
- Subnetting-Rumgerechne is komplizierter
- DNS is a must

Mythen

- IPv6 ist nix neues (Standard von 1998)
- IPv6 ist nicht wirklich der Nachfolger von IPv4, es ist auch da
- es gibt (mMn) wohl keine Umstellung von IPv4 zu IPv6

IPv6 Adressen

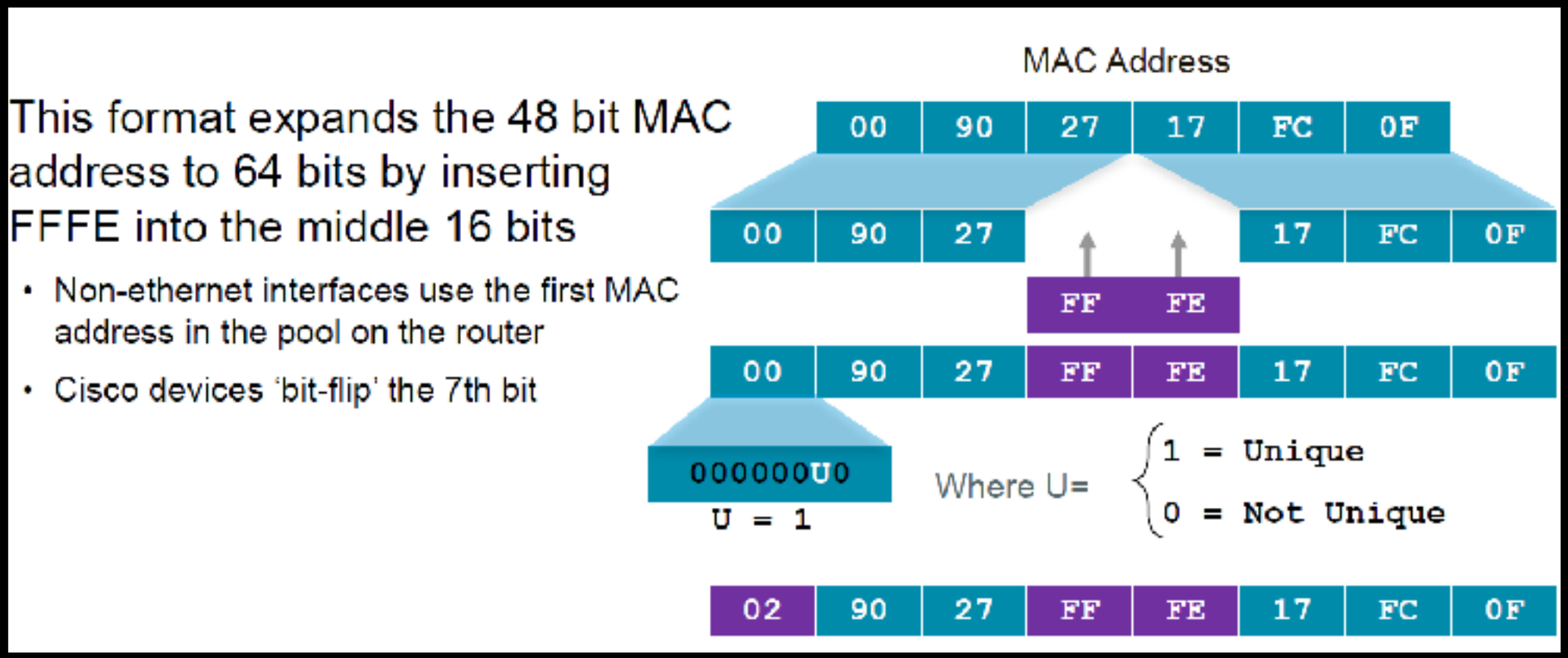
- 2001:db8:20:2000:0001::3/56
- Genereller Aufbau
  - 128 Bit Länge, bestehend aus Präfix (Netzanteil)und Interface-Identifier (Hostanteil)
  - Darstellung: 8 durch Doppelpunkt getrennte hexadezimale Blöcke zu 16-bit
  - Führende Nullen können weggelassen werden
    (Achtung! 20 ist nicht 2000, sondern 020)
  - eine oder mehrere Blöcke aus Nullen dürfen durch :: ersetzt werden, aber nur einmal pro Adresse !
  - Netze werden in CIDR-Notation geschrieben

Spezielle Adresstypen

- ::/128 —> unspecified (vgl. 0.0.0.0)
- ::1/128 —> Loopback (eigener Standort)
- fe80::/64 —> Link Local
    - Bildung siehe nächster Slide
- ff00::/8 (ff…) Multicast-Adressen

Auflistung nicht abschliessend!

Link Local Adressen



- FE80:0:0:0:0:0: + modifizierte EUI-64
  - erste 24bit der MAC, dann FFFE dann letzte 24bit der MAC
  - 7. Bit invertieren

Global Unicast

- alle nicht speziellen Adressen sind Global Unicast („normale“ IPv6 Adresse)
  - 2001:db8::/32 speziell für Dokumentation
- bisher sind nur Adressen aus folgendem Block vergeben:
  - 2000::/3 (2000… - 3fff….)
  - genau unter: https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml

Autoconfiguration

- Stateless Autoconfiguration macht DHCP (fast) überflüssig
  - Client sendet NDP-Paket (Router Solicitation) an Multicast ff02::2
    „Mami Mami, Gibts hier funktionierende Router?? Ich will Netz“
    ICMP Typ 133
  - Router antwortet mit NDP-Paket (Router Advertisement) und verkündet seine Präfixe (min /64), aus denen sich ein Client Adressen holen kann. Das schreit ein Router ggfs. auch ungefragt raus.
    ICMP Typ 134
  - Client bildet eine Adresse aus Präfix und seiner modifizierten EUI-64
- Angaben zu Gültigkeit
- kein DNS (Shit!), NTP, oder andere DHCP-Options
  - —> Stateless DHCP

Privacy Extensions

- Das Verfahren mit der EUI-64 in der Link Local-Adresse und bei Autoconfiguration is ja cool, aber:
- ich bin jetzt trackbar. An meiner IP eindeutig identifizierbar
- —> IPv6 Privacy Extensions
  - Randomisierung des Host-Identifiers
  - Node must perform DAD Duplicate Address Detection
    —> Neighbor Discovery

NDP Neighbour Discovery Protocol

- basiert auf ICMPv6
- Präfixermittlung
  - Router Solicitation (Typ 133)
  - Router Advertisement (Typ 134)
- Nachbarschaftsbeziehung („ARP-Ersatz“ - naja, nicht wirklich)
  - Neighbor Solicitiation (Typ 135)
  - Neighbor Advertisement (Typ 136)
- Redirect (Typ 137)

DO NOT BLOCK ICMPv6 ! You need it!

DNS-Einträge

- A-Einträge für IPv4
- AAAA-Einträge für IPv6

```
;; ADDITIONAL SECTION:
ns.florianzahn.de. 17280 IN   A  138.68.70.191
ns.florianzahn.de. 86400 IN   AAAA 2a03:b0c0:3:d0::2398:1
server42.florianzahn.de. 86400   IN A  78.47.92.225
server42.florianzahn.de. 86400   IN AAAA 2a01:4f8:c17:2776::2
```

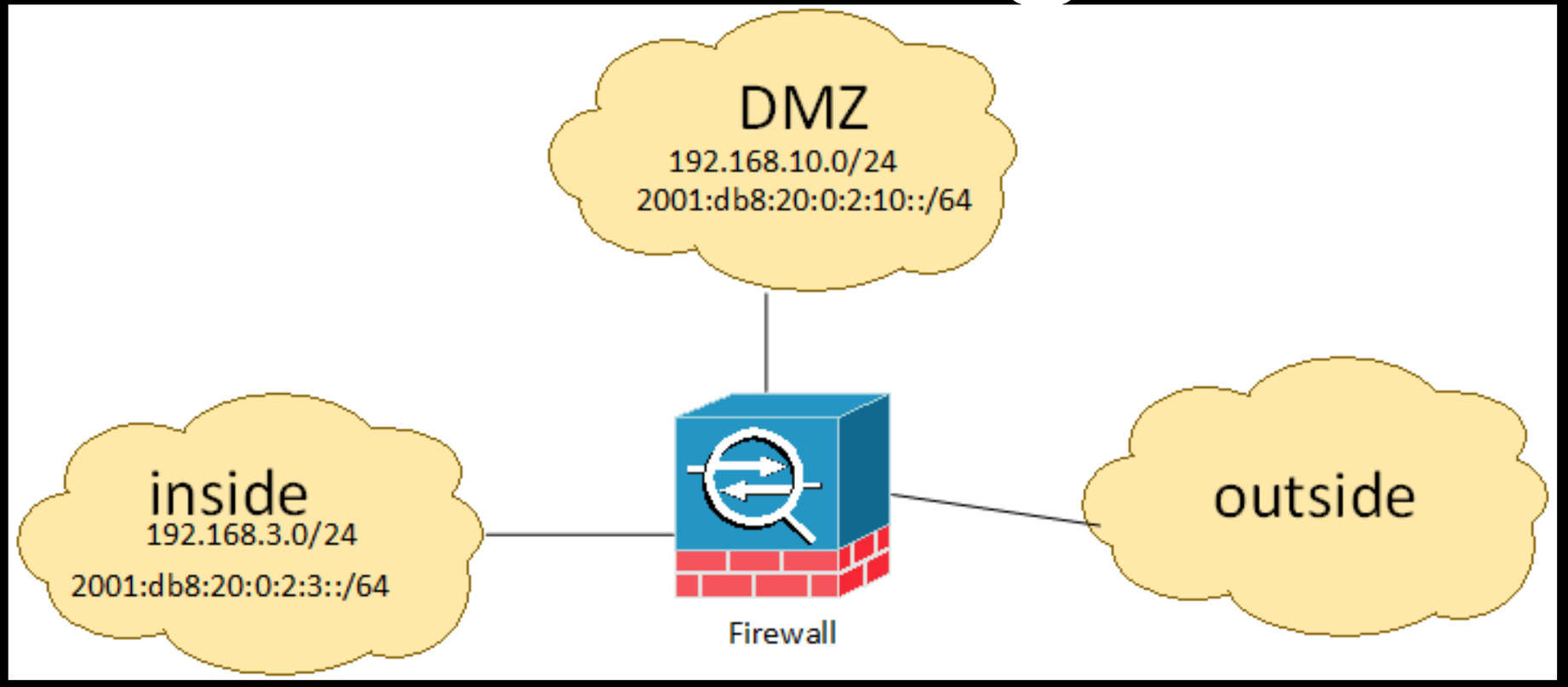
Dual Stack

- Parallelbetrieb zwischen IPv4 und IPv6
- Interface hat beide Adresstypen gleichzeitig
- IPv4-Adresse kann durchaus eine RFC-1918-Adresse sein Standard bei privaten Internet-Anschlüssen
- Handy-Internet ist inzwischen auch meist Dual Stack
- Vorteil: echte routbare IP-Adressen, DynDNS nutzbar
- Nachteile: Der Provider benötigt für jeden Kunden eine IPv4-Adresse

Dual Stack Lite

- „richtiges“ IPv6
- „kastriertes“ IPv4 mit Carrier-grade NAT
  Kundenrouter (CPE-Router) kapselt IPv4-Pakete und transportiert diese zu seinem Carrier-grade-NAT Router. NAT passiert also nicht mehr auf dem eigenen Router, sondern für alle Kunden auf den Systemen des Providers
- Vorteil: Provider kann eine Public-IP für mehrere Kunden nutzen
- Nachteil: kein VPN, kein Portforwarding (z.B. mit DynDNS)

Firewall-Konfiguration



access-list acl-dmz deny ipv4 any 192.168.0.0 255.255.0.0
access-list acl-dmz deny ipv4 any 172.16.0.0 255.240.0.0
access-list acl-dmz deny ipv4 any 10.0.0.0 255.0.0.0
access-list acl-dmz permit tcp 192.168.10.0 255.255.255.0 any4 eq 80
-> Zugriff nach drinnen verboten druch Blocken der RFC1918-Adressen (private Adressen)
aber in IPv6 gibts das nicht, implizites Blocken nach drinnen erforderlich, da Ziel any6 sonst auch für intern gilt
access-list acl-dmz deny ipv6 any6 2001:db8:20:0:2:3::/64
access-list acl-dmz permit tcp 2001:db8:20:0:2:10::/64 any6 eq 80

chaotisches wiresharken

- wollen wir mal schaun, was unser Client im Netz so tut?
- Wireshark ist unser Freund.

CHAOS IM QUADRAT
WWW.CCC-MANNHEIM.DE

Ende

…ferdisch