RUB

RUHR-UNIVERSITÄT BOCHUM

EINSATZ VON IPV6-MOSTLY IM CAMPUS-NETZ DER RUHR-UNIVERSITÄT BOCHUM

Nötige Schritte und Erfahrungswerte aus eher technischer Sicht

Einführung

- Robin Därmann
- Seit 2003 an der RUB, seit 2011 im NOC
- Sachgebietsleiter NOC im Dezernat 5 an der Ruhr-Universität Bochum
- Network-Operation-Center-Team mit sieben, bald acht Personen
- Campus-Netzwerk umfasst ~3.000 aktive Komponenten, ~140.000 Ethernet-Access-Ports, ~2.600 Wireless-APs (>1.000 weitere in Planung)
- Jede Menge Automation in Eigenentwicklung (Perl)

Motivation

- IPv6 seit 2011, seitdem bringen wir IPv6 voran wo es geht
- Traditionell mit Dual-Stack-Ansatz
- Seit 2022 auch etwas NAT44 wegen IPv4-Adressmangel

- NAT44 parallel mit IPv6 funktioniert, aber das geht besser, denn...

BIS JETZT WURDE NICHT EINE EINZIGE IPv4-ADRESSE EINGESPART!

Das möchten wir ändern.

Der lange Weg...

- Wir können nicht hart umschalten (wer kann das schon?), also müssen wir irgendwie migrieren
- „Besserer“ Ansatz als Dual-Stack: Endgeräte zwingen, IPv6 wenn möglich zu nutzen und NAT44 zu vermeiden
- „Happy Eyeballs“ versteckt Probleme mit IPv6 (oder IPv4!)

- NAT64 mit DNS64 (RFC 6146 + 6147) kam uns in den Sinn, aber das ist problematisch...

Der lange Weg...

- Wi… …rieren
- „Be… NA…
- „H…
- NA…

Exkurs: NAT64 und DNS64

- Client fragt DNS64-fähigen Resolver nach IPv6-Adresse
- Resolver antwortet mit IPv6-Adresse, zur Not erzeugt er sie mit Hilfe des NAT64-Präfixes
- Client baut Verbindung mit IPv6-Adresse auf. Wenn sie das NAT64-Präfix enthält, geht der Traffic zum NAT64-Translator
- NAT64-Translator übersetzt nach IPv4 und auf dem Rückweg zurück nach IPv6

Client: `ping6 x.com` → DNS64 → `64:ff9b::68f4:2a01` → NAT64 → `104.244.42.1`

Der lange Weg...

- Wir können nicht hart umschalten (wer kann das schon?), also müssen wir irgendwie migrieren
- „Besserer“ Ansatz als Dual-Stack: Endgeräte zwingen, IPv6 wenn möglich zu nutzen und NAT44 zu vermeiden
- „Happy Eyeballs“ versteckt Probleme mit IPv6 (oder IPv4!)

- NAT64 mit DNS64 (RFC 6146 + 6147) kam uns in den Sinn, aber das ist problematisch:
  - Wie bei NAT44 benötigen einige Protokolle spezielle Behandlung (z.B. IPsec)
  - Kommunikation mit numerischen IPv4-Adressen (z.B. `ping 104.244.42.1`) funktioniert nicht. DNS64-aktivierter Resolver muss befragt werden.
  - Veraltete Software möchte gerne IPv4-only-Sockets benutzen

...über 464XLAT...

- Besserer Ansatz: 464XLAT (RFC 6877)
  - Nutzt NAT64 auf Provider-Seite (PLAT) und einen „Stateless IP/ICMP Translator“ (SIIT) auf dem Endgerät (CLAT)
  - IPv4-Übersetzung nach IPv6 direkt auf dem Endgerät und zurück nach IPv4 beim Provider
  - Kein DNS64 nötig, daher Kommunikation direkt mit IPv4-Adressen möglich!

- Aber auch 464XLAT ist nicht perfekt:
  - Ursprünglich erdacht für Mobile-ISPs, die große IPv6-Only-Netze betreiben
  - Einige populäre Betriebssysteme unterstützen 464XLAT nicht auf WiFi- und LAN-Schnittstellen

...zu IPv6-Mostly

- Spart IPv4-Adressen weil Endgeräte entscheiden können, nur IPv6 zu benutzen (und sie tun das auch!)

- Kombination aus 464XLAT, einer DHCPv4-Option und einer IPv6-RA-Option
  - **RFC 8925:** „*IPv6-Only Preferred Option for DHCPv4*“
  - **RFC 8781:** „*Discovering PREF64 in Router Advertisements*“

- Endgeräte ohne IPv6-Mostly-Support laufen einfach Dual-Stack
  - Mit DNS64-aktivierten Resolvern ist der meiste Traffic jedoch IPv6

- Konfigurationsaufwand praktisch nur an DHCP-Server und Router, nicht am Client

Wie funktioniert‘s?

- DHCPv4-Option 108 („*IPv6-Only Preferred*“, RFC 8925):
  - In DHCPDISCOVER und DHCPREQUEST von fähigen DHCPv4-Clients angefragt
  - Vom DHCPv4-Server in DHCPOFFER zurück gesendet, mit positivem Wert

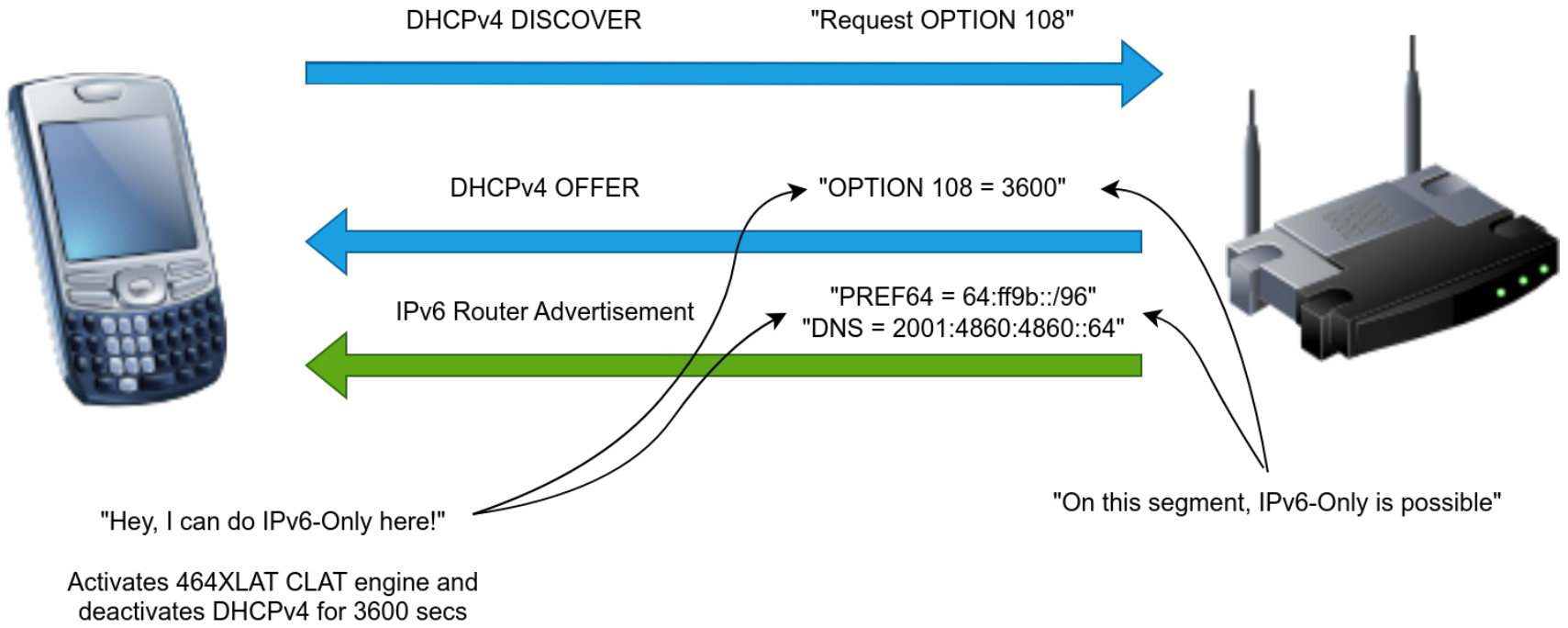
  → Client darf IPv4-Stack für die vorgegebene Zeit deaktivieren

  Es wird dann üblicherweise IPv4 lokal nach IPv6 übersetzt (464XLAT CLAT)

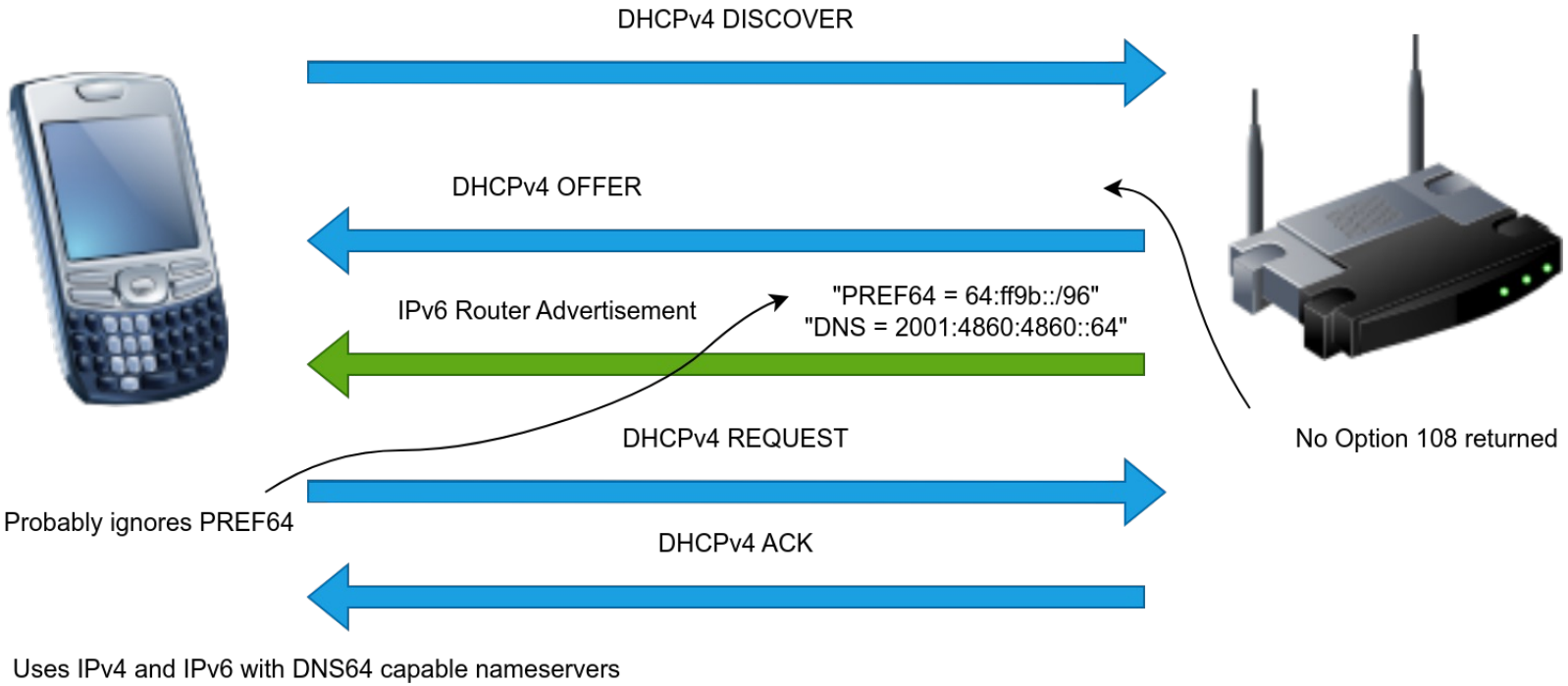
- Router Advertisement Option Type 38 („*PREF64*“, RFC 8781):
  - Gesendet in Router Advertisements (RA), enthält ein benutzbares NAT64-Präfix

  → NAT64-Präfix wird für lokale DNS64- and CLAT-Konfiguration benutzt

Onboarding mit IPv6-Mostly-Unterstützung



Onboarding ohne IPv6-Mostly-Unterstützung



Erster Test und Statistik

- Campusweites Wireless-Segment mit Authentifizierung via Captive Portal
- DHCPDISCOVER-Mitschnitt zwischen 31.08.2023 und 01.11.2023 (9 Wochen)
- 10,794 verschiedene MACs / Geräte insgesamt
  - 7,772 Geräte haben Option 108 im DHCPDISCOVER angefragt (72%)
  - 3,022 Geräte haben Option 108 nicht angefragt (28%)

Statistik – wer will nicht mit spielen?

- 3,022 Geräte haben Option 108 **nicht** angefragt (28%)
- Schnelle Analyse mit Fingerbank API zeigt:
  - 1,932: „Operating System/Windows OS/Microsoft Windows Kernel 10.0“
  - 243: „Operating System/Apple OS“
  - 191: „Operating System/Google OS/Android OS“
  - 128: „Phone, Tablet or Wearable/Generic Android/Samsung Android“
  - 117: „Phone, Tablet or Wearable/Generic Android/Huawei Android“
  - 102: „Operating System/Linux OS“
  - ...
  - 4: „Internet of Things (IoT)/Appliance/iRobot/iRobot Roomba“

Statistik – wer will nicht mit spielen?

- 3,022 Geräte haben Option 108 **nicht** angefragt (28%)
- Schnelle Analyse mit Fingerbank API zeigt:
  - 1,932: „Operating System/Windows OS/Microsoft Windows Kernel 10.0“
  - 243: „Operating System/Apple OS“
  - 191: „Operating System/Google OS/Android OS“
  - 128: „Phone, Tablet or Wearable/Generic Android/Samsung Android“
  - 117: „Phone, Tablet or Wearable/Generic Android/Huawei Android“
  - 102: „Operating System/Linux OS“
  - ...
  - 4: „Internet of Things (IoT)/Appliance/iRobot/iRobot Roomba“

Kabelgebundenes Netz

- Wireless ist die Unterstützung von IPv6-Mostly bereits weit verbreitet
- Kabelgebunden haben wir aber viel Windows... (Feature Request bei MS existiert übrigens)
- Testweise Umstellung unseres (heterogenen) Arbeitsgruppennetzes auf IPv6-Mostly

- Zugriff auf IPv4-Adressen von Netzwerkkomponenten sowie Management-Interfaces von Servern etc. nicht mehr möglich
  - Abhilfe schafft VPN-Tunnel mit erlaubtem IPv4-Bereich
  - Mittelfristig Aktivierung von IPv6 auf der gesamten Management-Infrastruktur

- NAT64 mit unseren Border-Routern (Cisco ASR1002-HX) hatte einige kleinere Probleme, das haben wir auf zwei FreeBSD-VMs umgezogen
  - Firefox-Updater, Paypal, irgendwas mit Captchas, ...

Fallstricke

- Keine fremden DNS-Server eintragen!
- IPv6 nicht am Endgerät komplett deaktivieren!
- Nicht mehrere IPv6-Präfixe auf dem Link benutzen!
  - macOS wird für CLAT ein zufälliges auswählen, ohne zu berücksichtigen ob es deprecated oder ULA ist
- SLAAC muss aktiviert sein!
- Man sollte freie Adressen im DHCPv4 pool haben!
  - DHCPv4-Server senden kein DHCPOFFER wenn es keine freien Adressen gibt
- Cisco Catalyst erzeugt einen (unnützen) ARP-Eintrag beim Weiterleiten von DHCPOFFER
- Man sollte **NICHT** das well-known NAT64-Präfix (`64:ff9b::/96`) verwenden, denn:
  - RFC 6052 („*IPv6 Addressing of IPv4/IPv6 Translators*“), Section 3.1:
    „*The Well-Known Prefix MUST NOT be used to represent non-global IPv4 addresses,*“...

DHCPv4 Server-Konfiguration

- ISC Kea:

```
"subnet4": { "option-data": [ "name": "v6-only-preferred", "data": "3600" ] }
```

- ISC DHCP Server (der ältere, der schon **seit 2022 End-of-Maintenance(!)** ist):

```
option option-108 "3600";
```

- Jeder andere:
  - Muss nur fähig sein, eine benutzerdefinierte Option mit Code 108 und einem unsigned integer als Wert zu senden

Router-Konfiguration

- Cisco IOS-XE >= 17.11.1:

```
interface Vlan888
 ip address 10.10.10.1 255.255.255.0
 ip helper-address 10.1.1.1
 ipv6 address 2001:db8:1::1/64
 ipv6 nd ra nat64-prefix 64:FF9B::/96
 ipv6 nd ra dns-search-list domain your-domain.tld
 ipv6 nd ra dns server 2001:4860:4860::64
 ipv6 nd ra dns server 2001:4860:4860::6464
```

- Arista EOS >= 4.31.0F:

```
ipv6 nd ra pref64 64:ff9b::/96
```

Fazit / Ausblick

- Betriebssystemhersteller müssen die nötigen Komponenten bereitstellen bzw. unterstützen (464XLAT, CLAT, Option 108, PREF64)
- Zahlen werden besser (>70% der Geräte fragen bereits Option 108 im WLAN bzw. LAN an)
- Versuch einer Aktivierung im eduroam
  - Wie spielen unsere Firewalls mit?
- Ausweitung auf weitere kabelgebundene Netze
- Unser Netzwerk-Management muss vollständig IPv6-fähig werden (Router, Switche, WLAN-Infrastruktur, sonstige Komponenten)
- Reduktion der IPv4-Adressen auf umgestellten Netzen, dadurch dann:

Echte Einsparung von IPv4-Adressen!

Weitere Informationen

- RFC 8683:
  Additional Deployment Guidelines for NAT64/464XLAT in Operator and Enterprise Networks
  - Diskussion und Vergleich aller möglichen Kombinationen von NAT64, DNS64, 464XLAT

- draft-link-v6ops-6mops:
  IPv6-Mostly Networks: Deployment and Operations Considerations
  - Ganz aktuelles Internet Draft (vom 04.03.2024)

- v6.de

- Und noch was: Bitte an der IPv6 Transition Technology Survey von Microsoft teilnehmen!

Das war‘s.

- Fragen?
- Kontakt: robin.daermann@rub.de