IPv6

Migration, Betrieb und Deployment

Markus Schade

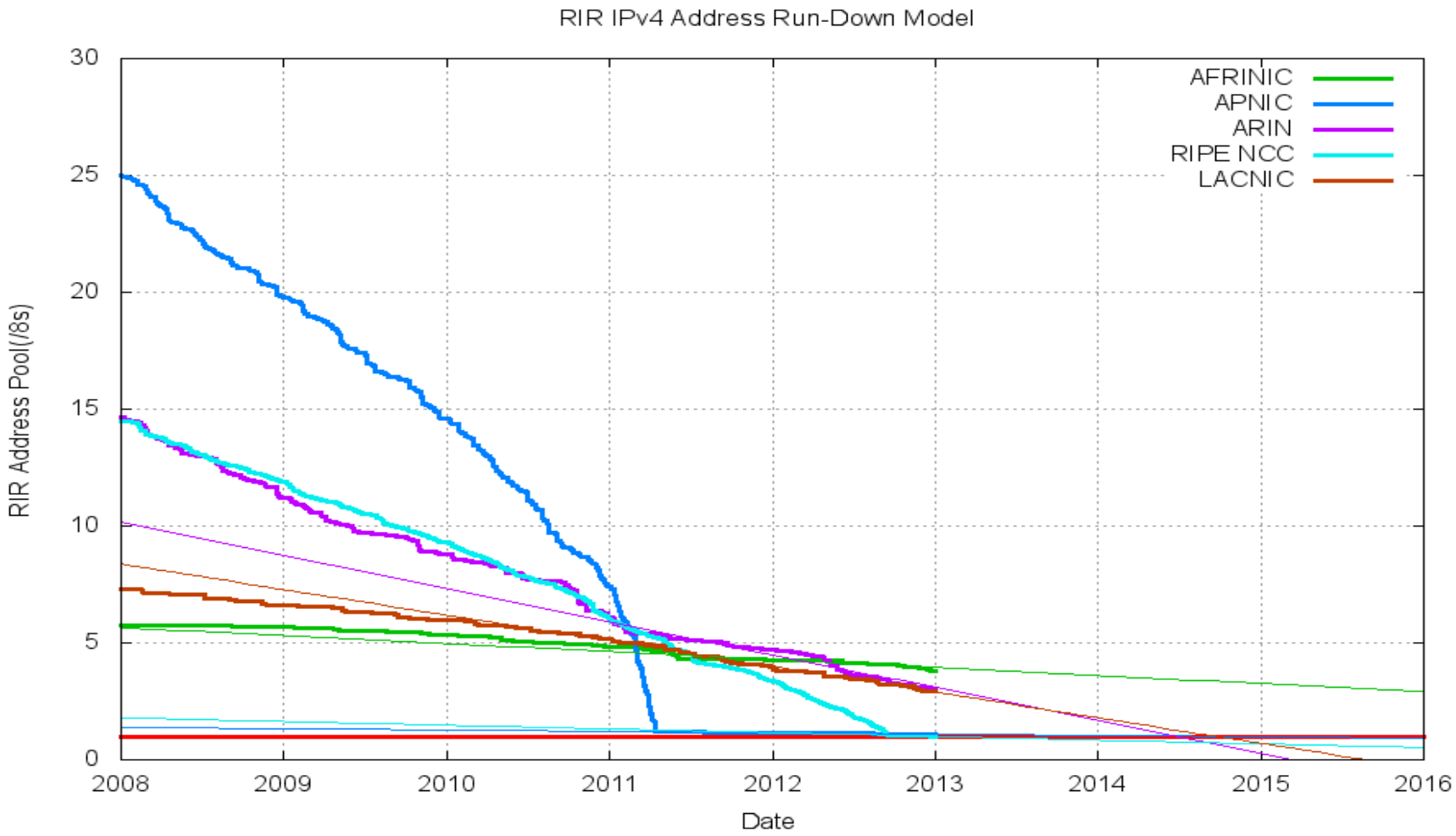
Wer hat schon mal?

- Etwas von IPv6 gehört?
- mit IPv6 gespielt?
- IPv6 zu Hause/auf Arbeit/an der Uni?
- IPv6 im Produktivbetrieb?

Es war einmal

- 1970er: 32 Bit für das Experiment Internet v4
  - Vint Cerf ist Schuld ;-)
- 1980er: Das Experiment entkommt
- 1990er: kommerzielle Verbreitung
- 2000er: Adressraum geht (jetzt wirklich) zur Neige

Aktueller Stand IPv4



Quelle und mehr: http://www.potaroo.net/ispcol/2013-01/2012.html

IPv6

- 128 Bit
- 3,4 * 10^38 Adressen
- 7,9 * 10^28 mal so groß wie das IPv4 Internet
- Jetzt neu mit Buchstaben!
  - 2a01:4f8:d0a:2001::2
  - 2a01:04f8:0d0a:2001:0000:0000:0000:0002

IPv6 Features

- Automatische IP-Konfiguration
  - Seit 2010 auch mit Reverse DNS Server (RFC6106)
    - außer Windows oder Android
- kein Broadcast
- zwingend Multicast
- (Server-)systeme erhalten Subnetze statt Einzel-IPs (/64)
- (vorläufig) ausreichend großer Adressraum
  - selbst bei /64 pro System = 2^32 * IPv4 Internet

Stand IPv6

- März 2013: weniger als 1% des Traffics IPv6
  - DE-CIX: 13 Gbit vs 2500 Gbit
- http://www.google.com/ipv6/statistics.html
  - 1,19% der Zugriffe
- Deutschland hängt hinterher (1,69%)
  - Frankfreich: free.fr – seit 2007 (gesamt >5%)
  - Rumänien: RCD&RDS – seit 2012 (>10%)

Warum?

- Verfügbarkeit (oft abhängig von wenigen Anbietern)
- genügend(?) große IPv4-Adressreserven
- NAT, Carrier Grade NAT, NAT444
- Komplexität, Gleichgültigkeit, Desinteresse
- never touch a running system
- Fehlende und fehlerhafte Software
- Sicherheitsprobleme in/durch IPv6 (*hust*)

Wieviele IPv6-Adressen bekommt man so?

- Anfangs /48 (=65536 /64) pro Site angedacht (RFC3177)
- auf /56 (=256 /64) pro Site reduziert (RFC6177)
  - /60 pro Kunde (US DSL Anbieter) = 16 /64
  - /56 pro Kunde (DTAG) = 256 /64
- zwischen /64 und /56 für dedizierte Server
- /48 minimale PI (Provider Independent) Allokation
- RIPE-Minimum /32 an LIR (auf Wunsch /29)
  - DTAG 2003::/19 = 137.438.953.472 /56
  - US DoD: 2608::/13 = 64 * DTAG

Netzplanung

- Umdenken von IPv4 nötig
- in Subnetzen (/64) denken!
  - keine Clientsysteme mehr zählen
- Addressraum ist groß genug
  - Allokation sollte für die nächsten 10+ Jahre reichen
- echte Hierarchie von Anfang an planen
  - keine Netzfragmentierung
- Best current pratice
  - Subnetting an Nibble (4 Bit) = Hex-Stelle der Adresse
  - Aber: bis zu 16x zu viele Adressen

Netzplanung (cont.)

- Beispiel: /64 pro Server oder Client-Subnet
  - 24/48-Port: /56 statt /59 bzw /58
  - Uplink 12-Port Router: /52 statt /55 bzw. /54

- Beispiel: /48 als Site-Allokation oder PI
  - 10 (Firmen-)standorte: Minimum 4 Bits ($2^4 = 16$)
  - = /52 pro Standort = 4096 /64 Subnetze
  - oder /53 pro Standort = 2048 /64

Netzplanung (cont.)

- Prefixe kleiner als /64 möglich
  - aber ohne „Bling“ wie SLAAC, DAD
  - z.B. für VMs oder NAT64 (/96)

- http://www.ripe.net/lir-services/training/material/IPv6-for-LIRs-Training-Course/IPv6_addr_plan4.pdf

Anschnallen nicht vergessen!

- IPv6 ist fast überall per default aktiviert und wird bevorzugt
- Neighbor Discovery (ND) anfällig gegen Spoofing wie ARP
  - Secure ND schwierig (erfordert PKI)
- SLAAC nur für vertrauenswürdige Netze !!!11elf
  - IPv6 wird gegenüber v4 bevorzugt (MITM)
  - Fake RA / RA Flooding
  - Fake DAD

Gegenmaßnahmen

- Kundennetze auf Link-Local-IP routen
  - statisches ND (aka static ARP für v4)
  - verhindert Flooding mit vielen NDP Einträgen

- Server in öffentlichen Netzen sollten v6-Magie abschalten
  - autoconf
  - accept_ra*
  - accept_dad

Hetzner IPv6 Status für Kunden

- /64 kostenlos verfügbar für Kunden seit Mitte 2010
  - optional /56
- default in allen Linux-Standardinstallation
  - und bald in Windows Server 2012
- Reverse DNS Einträge
- Monitoring
- DNS Resolver
- Authoritative Nameserver
  - okay, nur teils, aber bald vollständig

IPv6 Migration

- Testphase mit v6-only und Dual-Stack-Subdomain
- DNS Resolver, Backupserver, Mirror, NTP
- nach IPv6 Launch-Day (Juni 2012)
  - sukzessive Umstellung auf echtes Dual-Stack
- Umstellung auf geroutete Kundennetze
  - fe80::1 als Default-GW
  - war erst nach Update der Router-Firmware durch Hersteller möglich

Lessons learned IPv6

- nur noch wenig (Server)software mit IPv6-Problemen
  - z.B. Debian 6.0.x RPC/NFS-Server
- Inzwischen RIPE Vorgaben zur Vergabe / Netzdesign
  - erlauben „schöneres“ Subnetting – an den Nibbles ;-)
  - Policy für Beantragung von neuen Netzen
- v6-only ist keine Option
  - außer man braucht nur Google, Facebook und Youtube
  - fehlender v6-Support in Client-Software:
    - z.B. Skype, Google Hangouts, u.v.a. (Android) Apps
    - https://sites.google.com/site/tmoipv6/464xlat

Deployment

ABLAUF OS DEPLOYMENT

- Start des Servers via Wake on LAN
- PXE Boot des Installers
- Installation via Kickstart / FAI / etc.
- Post-Install

Legacy (BIOS) PXE kann kein IPv6 und wird es auch nie können

„Intel is not investing any time or resources on improvements to legacy PXE implementations for client systems. All our present and future energies are focused on UEFI Spec network boot implementation (which covers both IPv4 and IPv6).“

Und nun?

- Egal.
- Deployment via Legacy PXE
  - v4 bootstrap
  - v6 Konfiguration während/nach der Installation
- Problem für ISPs / Hoster
  - jedes System braucht auf mind. 1 öffentliche IPv4
  - Alternativ Nutzung von RFC1918/RFC6598 Adressen
- Aber
  - Windows-Installation auf HDDs > 2TiB
  - Nur im UEFI Modus möglich

UEFI?

- Unified Extensible Firmware Interface
  - wird BIOS ablösen
  - Bootloader in eigener Partition (EFI System Partition)
  - GUID Partition Table
- erste UEFI Boards seit 2011
  - ohne UEFI PXE
- Im Legacy BIOS Modus kein Zugriff auf UEFI Variablen
- Ab Mitte 2012 auch Mainboards UEFI PXE
  - Aber pxelinux.0 ist kein EFI-Binary

Dual BIOS/UEFI INFRASTRUKTUR

- DHCP Server muß unterscheiden können
  - BIOS PXE Client
  - UEFI Netboot Client
- Bootfile / Bootmenü
  - BIOS: PXELINUX
  - UEFI: z.Z. nur durch Redhat EFI-GRUB1

- Nachteil:
  - Pflege von mehreren Systemen
  - Windowsinstallation mit Linux-Boardmitteln nur mit Tricks möglich

- Wenn man IPv6 bekommen kann, anfangen!
- Testen, Ausprobieren, Lernen
  - z.B. mit dem Mailserver ;-)
- Deployment vorerst über IPv4
- UEFI ist die nächste Großbaustelle

Fragen? Fragen!

Vielen Dank und

viel Spaß noch!

HETZNER ONLINE

Wir suchen Mitarbeiter!

- IT-Servicetechniker (m/w)
- Linux-Administrator (m/w)
- Softwareentwickler (m/w)
- System Engineer (m/w)
- Abschlußarbeiten / Praktika / Ferienarbeit

mehr unter *https://jobs.hetzner.de*

WE LOVE BITS. DO YOU?

DAS UNTERNEHMEN

Hetzner Online ist ein professioneller Webhosting-Dienstleister und erfahrener Rechenzentrenbetreiber. Wir bieten Lösungen an, die durch Qualität, Stand der Technik und Sicherheit überzeugen. Dabei reicht das Angebot für Homepage-Einsteiger bis zum professionellem Webentwickler:

- Root, Managed und vServer
- Colocation
- Shared Hosting
- Internet Domains
- SSL-Zertifikate