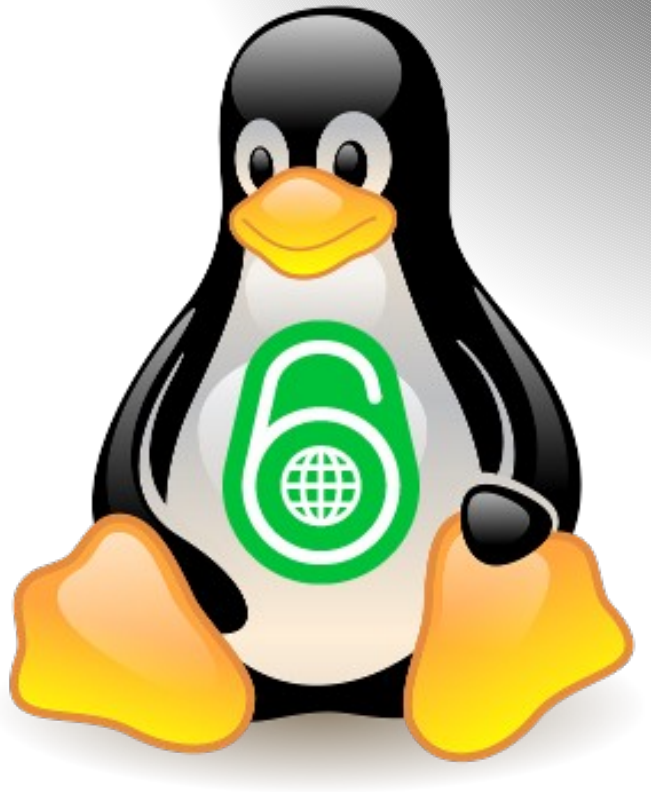
Mit Linux ins IPv6 Internet

DI Stefan Kienzl, BSc



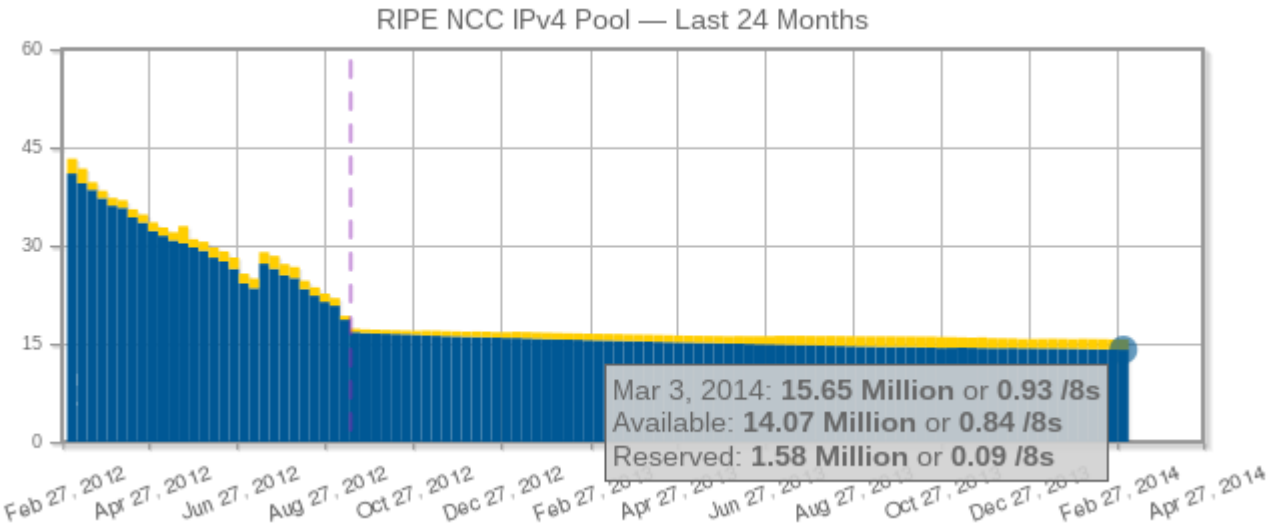
Grazer Linuxtage 2014

Entwicklung von IPv6

- 1992 wurde Problem der Adressknappheit erkannt
- 1998 wurde IPNG definiert
- IPv5 wurde 1979 definiert und findet sich heute in MPLS wieder
- Umbenennung von IPNG in IPv6
- IPv6 wurde durch CIDR und NAT/PAT verzögert
- Wird wahrscheinlich mit IPv4 lange koexistieren
- Es ist unklar, wann IPv6 eine bedeutende Rolle im Internet spielen wird

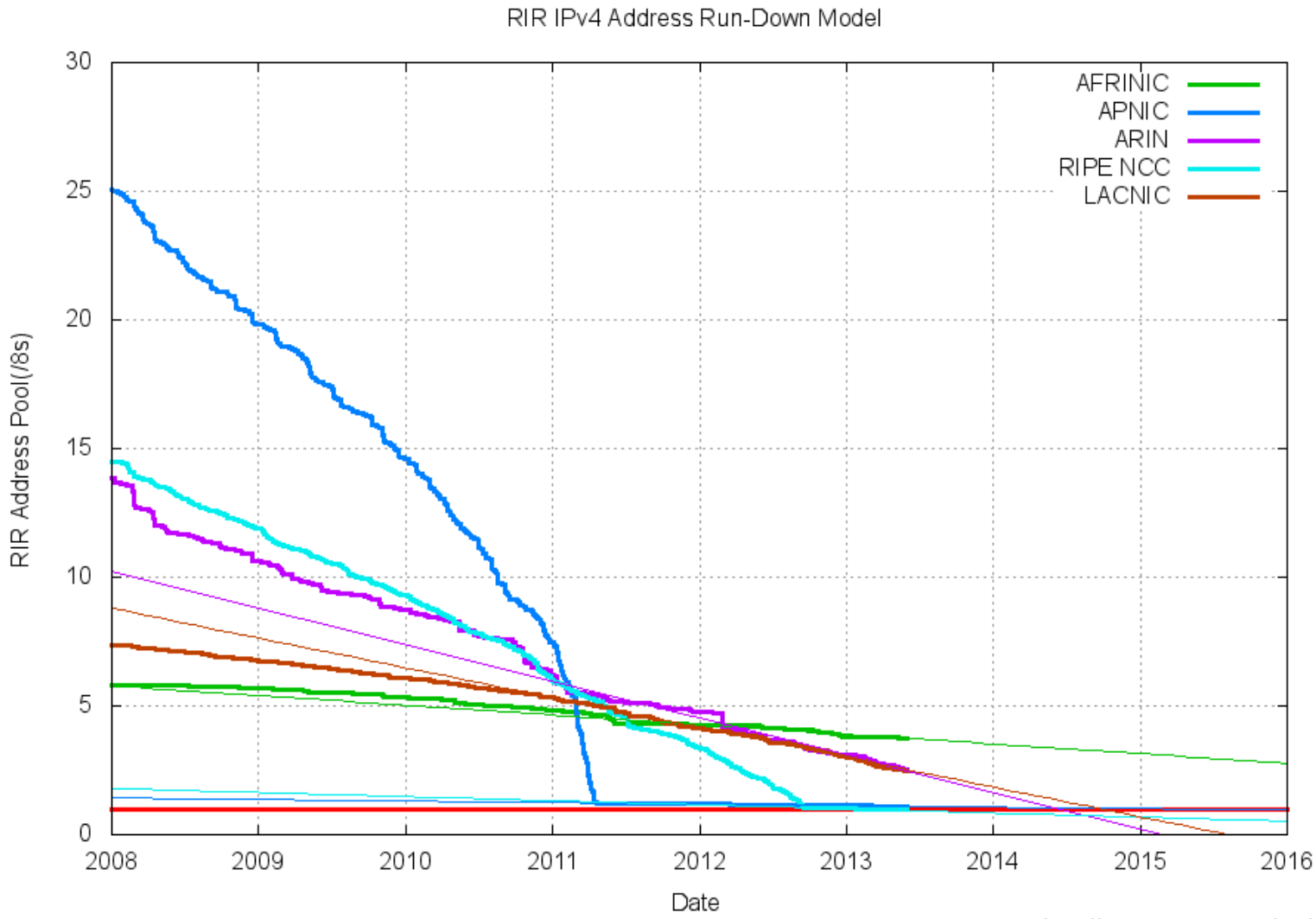
Warum gerade jetzt IPv6?

- Am 3. Februar 2011 wurden die letzten /8s von der IANA an die RIRs ausgegeben
- Am 15. April 2011 trat bei der APNIC die „last /8 Policy“ in Kraft
- Am 14. September 2012 trat beim RIPE NCC die „last /8 Policy“ in Kraft
- Mit jedem Tag wird die Einführung von IPv6 teurer



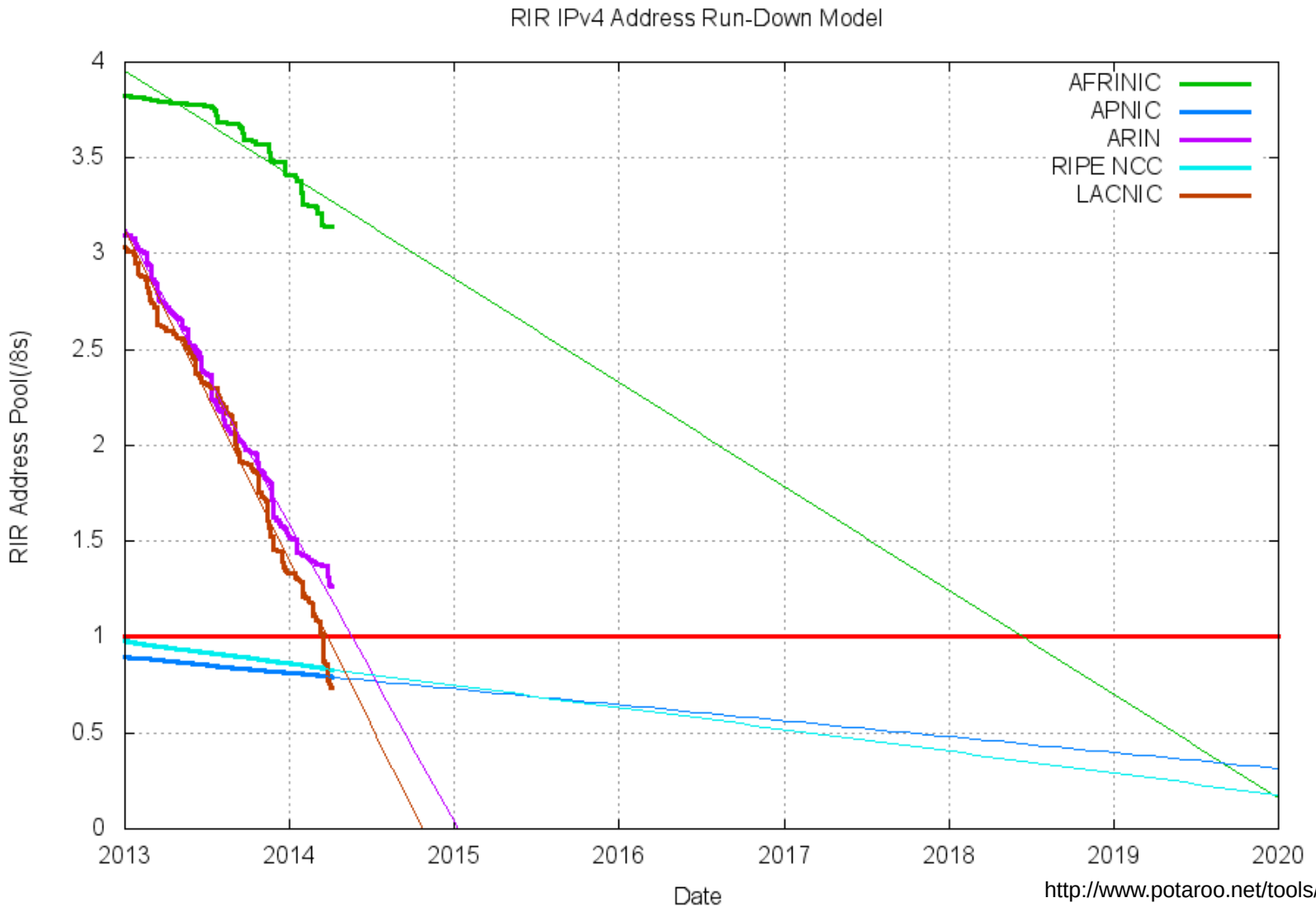
http://www.ripe.net/internet-coordination/ipv4-exhaustion/ipv4-available-pool-graph

IPv4 Exhaustion



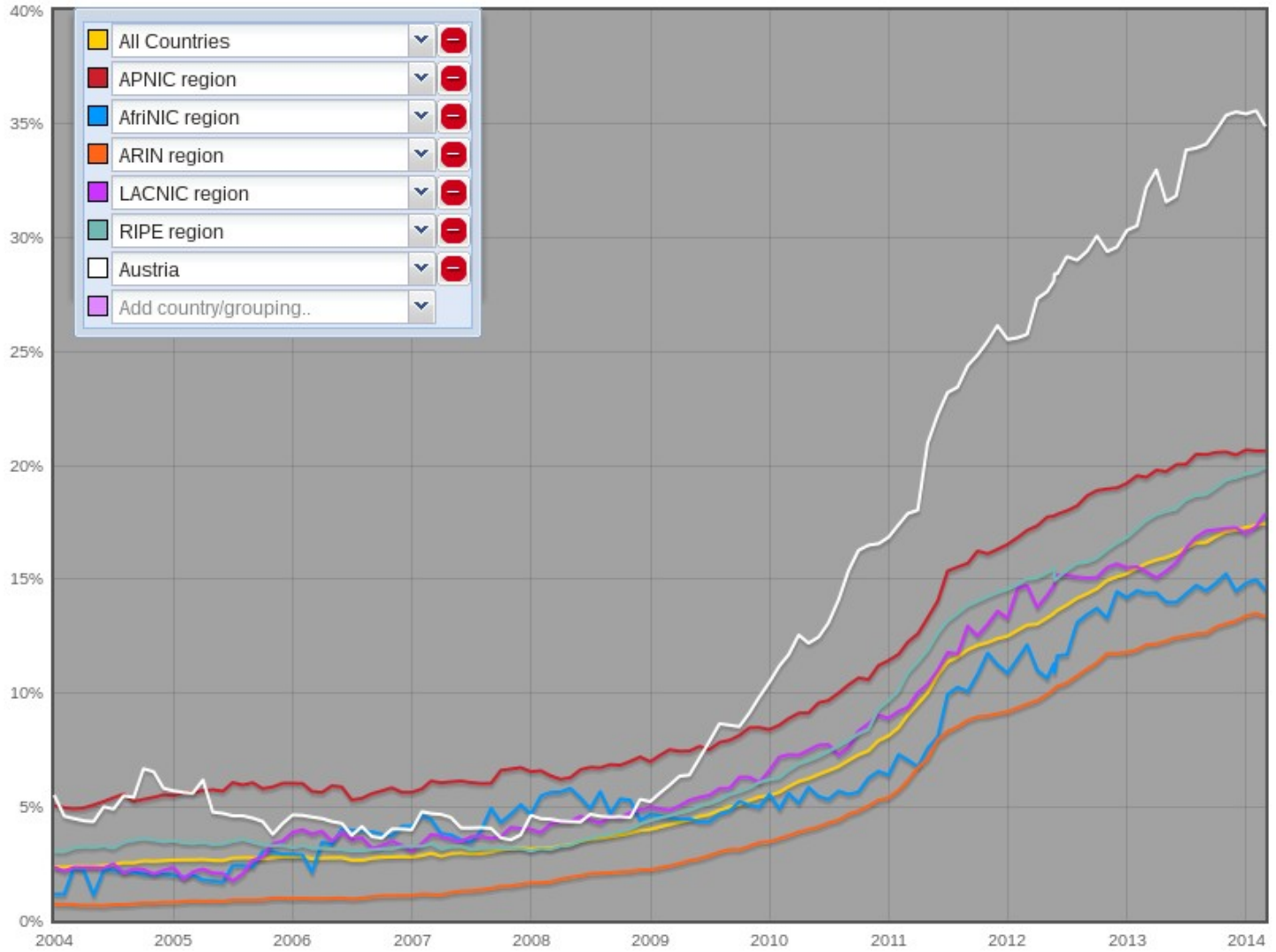
http://www.potaroo.net/tools/ipv4/

IPv4 Exhaustion



http://www.potaroo.net/tools/ipv4/

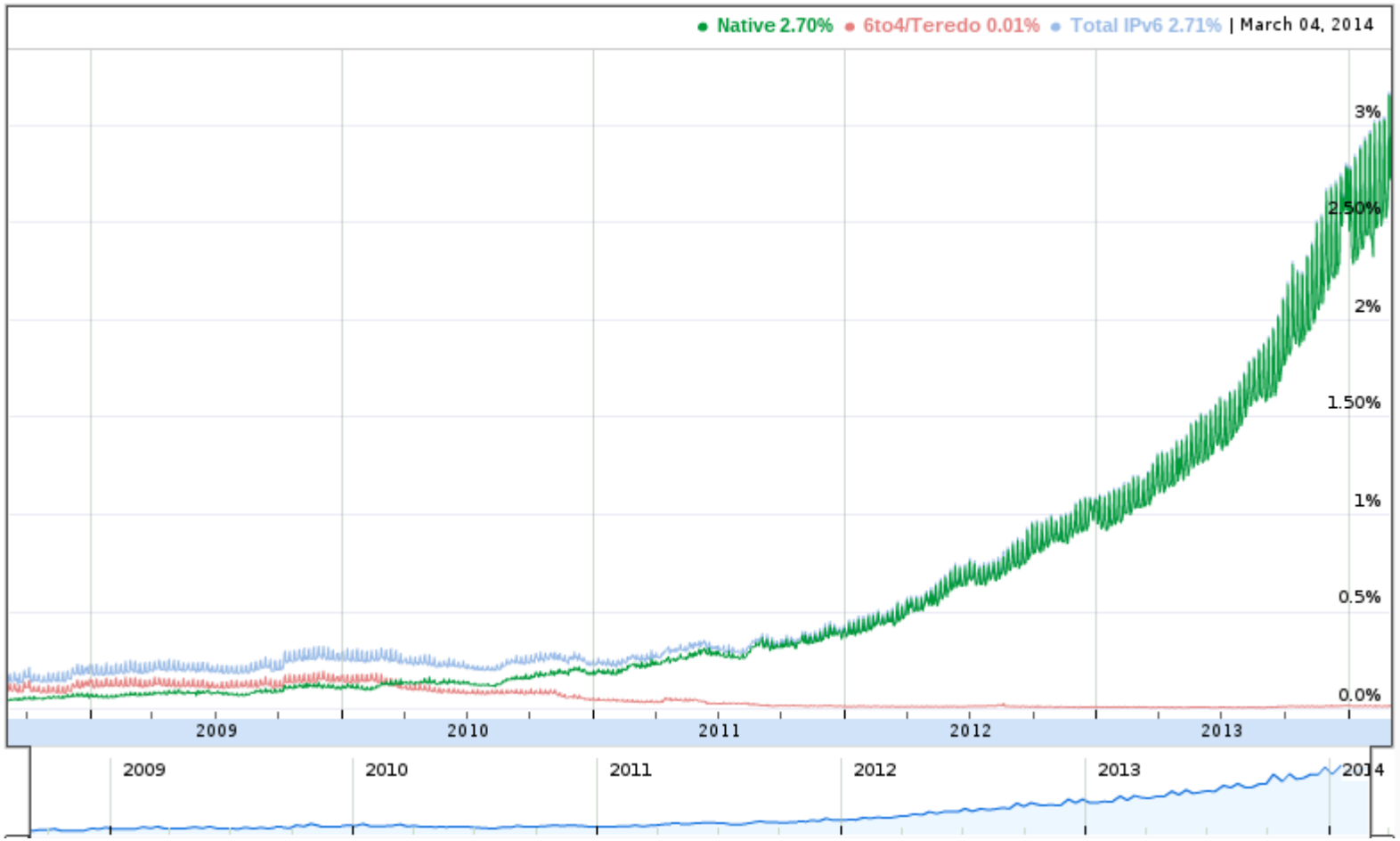
IPv6 im Internet



percentage of networks (ASes) that announce an IPv6 prefix

http://www.ipv6actnow.org/info/statistics/

IPv6 im Internet



Anteil der Nutzer, die über IPv6 auf Google zugreifen.

http://www.google.de/ipv6/statistics.html#tab=ipv6-adoption

IPv6 Unterstützung

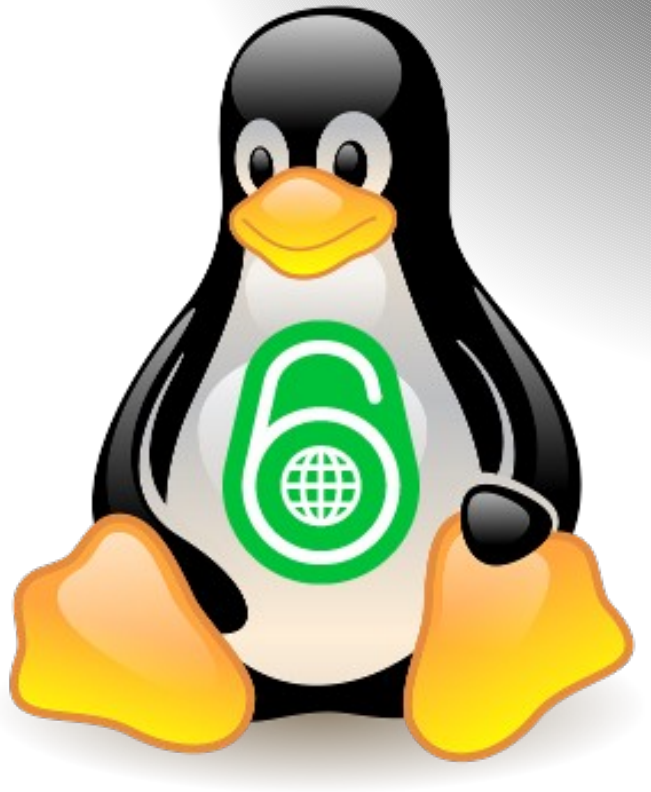
- Viele Hersteller behaupten IPv6 zu unterstützen
- Keiner weiß was das im Detail heißt
- Hinterfragen Sie die Angaben der Hersteller

- RIPE-554 als Orientierungshilfe
  http://www.ripe.net/ripe/docs/ripe-554
- Es besteht Raum für Verbesserungen...

IPv6 und Sicherheit

- IPv6 wird teilweise als unsicherer als IPv4 beschrieben
- Es hat sich im Vergleich zu IPv4 wenig geändert
- Attacken unter IPv4 sind in ähnlicher Form unter IPv6 immer noch möglich
- Security Komponenten beherrschen IPv6 aber nicht in gleichem Ausmaß wie IPv4
- Attacken mit IPv6 funktionieren mangels implementierter Gegenmaßnahmen gut – sind jedoch noch sehr selten

IPv6 Tunnel



Grazer Linuxtage 2014

Tunnelnutzung

PRO

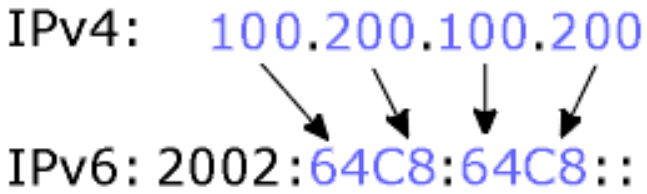
- IPv6 ist nicht bei jedem ISP verfügbar
- Testen der eigenen Infrastruktur „von Außen“
- F&E
- Privatnutzung

KONTRA

- Keine native IPv6 Verbindung
- Adressierung unklar
- Schlechte Verfügbarkeit
- Unklare Verbindungswege
- Nicht für produktive Firmennutzung
- Sicherheitsrisiko

Arten von Tunneln

- 6to4
  - *Spezieller Präfix + Kodierung der v4 Adresse in die v6 Adresse*
  - *Tunnelendpunkt benötigt öffentliche IPv4 Adresse*
  - *Lokal ein /48 zur weiteren Verwendung verfügbar*



- Tunnel Broker
  - *Tunneltransport über IPv4*
  - *Login bei einem Tunnel Provider – stellt Verbindung ins IPv6 Netz und einen Prefix zur Verfügung*
  - *http://tunnelbroker.net/ (Hurricane Electric)*
  - *http://www.sixxs.net/*
- ISATAP
- Teredo

6to4 mit Linux

- Steht am WAN Interface eine öffentliche IP zur Verfügung, kann daraus sehr einfach eine 6to4 Adresse abgeleitet und ein entsprechendes Interface erstellt werden
- Anschließend können im LAN weitere Interfaces mit dem zugehörigen Prefix versorgt werden
- Bei Änderung der IPv4 Adresse ist auch IPv6 neu zu konfigurieren
- Konfiguration:

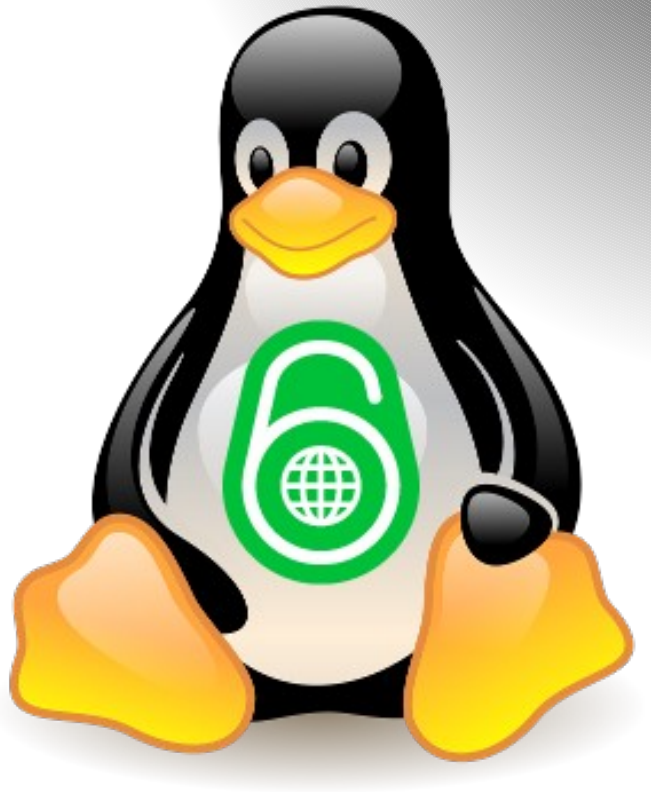
```
ipv4="x.x.x.x"; printf "2002:%02x%02x:%02x%02x::1 \n" `echo $ipv4 | tr "." " "`
ip tunnel add tun6to4 mode sit remote any local [lokale v4 Adresse] ttl 64
ip link set dev tun6to4 up
ip -6 addr add [6to4 Prefix]/16 dev tun6to4
ip -6 route add 2000::/3 via ::192.88.99.1 dev tun6to4 metric 1
```

SixXS unter Linux

- SixXS bietet mit einem Client eine einfache Möglichkeit sich über verschiedene Tunnel-Modi mit seinem POP zu verbinden
- AICCU - Automatic IPv6 Connectivity Client Utility
- Nach der Installation müssen nur noch Username und Passwort eingetragen werden [*aiccu.conf*]
- Verfügbar für Linux, BSD, Windows, Mac, Solaris, AIX und Android
- Starten des Clients als root

```
# aiccu start
```

Linux als IPv6 Router und Firewall



Grazer Linuxtage 2014

Grundlegendes

- Wie bei IPv4 kann Linux sehr einfach auch als Router für IPv6 Verbindungen genutzt werden
- Die dafür notwendigen Schritte sind im Wesentlichen gleich

1) Herstellen der WAN Verbindung
   (nativ oder mittels Tunnel)
2) Verbindung mit einer Firewall (ip6tables) absichern
3) Am LAN Interface eine IPv6 Adresse konfigurieren
   und IP Forwarding aktivieren
4) Verteilen von IP Informationen im LAN
   (radvd bzw. dhcpv6)

Interfaces und IP Forwarding

- Hinzufügen einer LAN IP am lokalen Interface

```
ip -6 addr add 2001:db8::1/64 dev eth0
```

- IPv6 Forwarding aktivieren

```
echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
```

RADVD

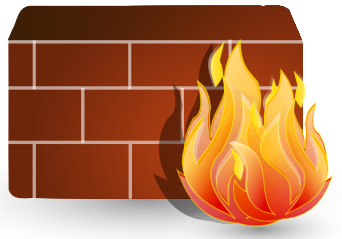
- IPv6 benutzt Router Advertisements um IPv6 Prefix und Default-Gateway zu verteilen
- Eventuell weitere Infos per DHCPv6
- SLAAC mit RDNSS für Clients prinzipiell ausreichend, jedoch nur von wenigen Betriebssystemen unterstützt
- Linux kann das natürlich :)
- Nutzung statischer oder IPv4 DNS Server als Alternative

Beispiel radvd.conf

```
interface eth0 {
        AdvSendAdvert on;

        prefix 2001:db8:1::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
        };

        RDNSS 2001:db8::cafe
        {
        };
    };
```

IP6TABLES

- Clients werden mit öffentlichen IPv6 Adressen versorgt, sind damit aus dem Internet direkt erreichbar und eine Firewall daher umso wichtiger



- Grundprinzip für die Firewallkonfiguration
  „So wenig wie möglich, so viel wie nötig erlauben“
- ICMPv6 spielt eine sehr wichtige Rolle - die gängige Praxis, ICMP generell zu verbieten kann unter IPv6 nicht mehr angewendet werden. [RFC 4890]
- IPv6 Extension Header sind sicherheitskritisch

IP6TABLES - Basiskonfiguration

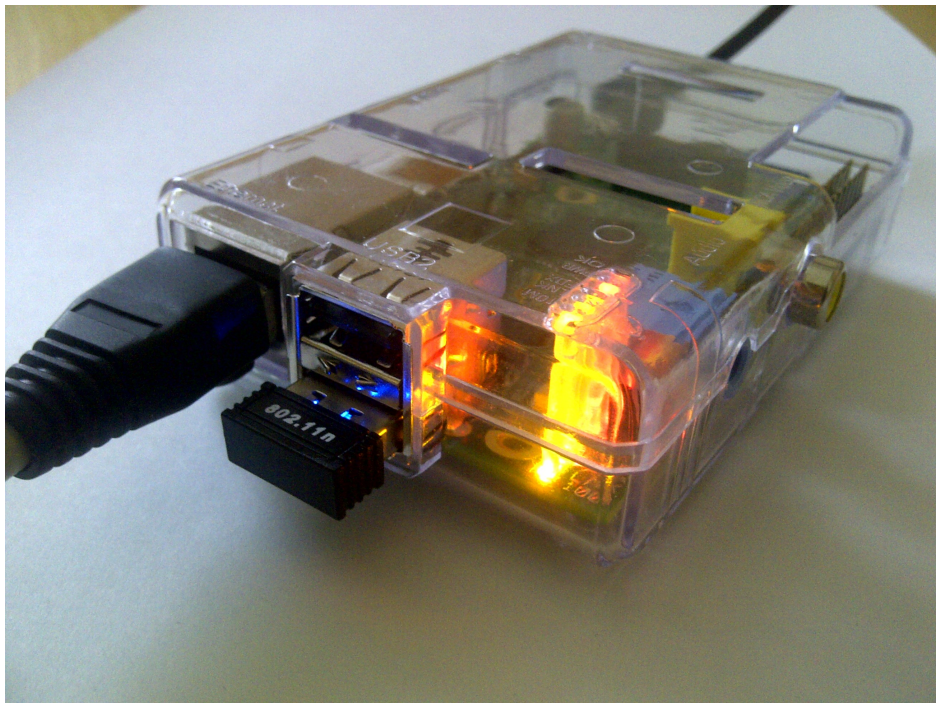
```
# Grundsätzlich alle Pakete verwerfen
$IP6TABLES -P INPUT DROP
$IP6TABLES -P OUTPUT DROP
$IP6TABLES -P FORWARD DROP

# Lokalnet erlauben
$IP6TABLES -A INPUT  -i lo -j ACCEPT
$IP6TABLES -A OUTPUT -o lo -j ACCEPT

# Verbindungen vom Router aus erlauben
$IP6TABLES -A OUTPUT -o $WAN_IF -j ACCEPT
$IP6TABLES -A INPUT  -i $WAN_IF -m state --state ESTABLISHED,RELATED -j ACCEPT

# Zugriff des LANs erlauben (je nach Anforderung weiter einschränken)
$IP6TABLES -A INPUT    -i $LAN_IF  -j ACCEPT
$IP6TABLES -A OUTPUT   -o $LAN_IF  -j ACCEPT

# Ausgehendes IPv6 Forwarding erlauben (je nach Anforderung weiter einschränken)
$IP6TABLES -A FORWARD -m state --state NEW -i $LAN_IF -o $WAN_IF -s $SUBNETPREFIX -j ACCEPT
$IP6TABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

IP6TABLES - spezifische Konfiguration

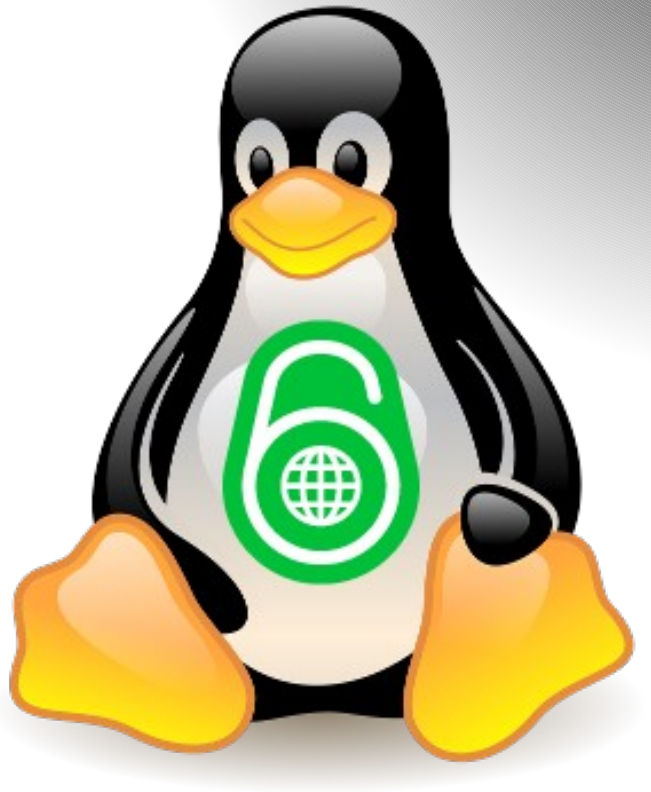
```
# Pakete mit RH0 Header filtern:
$IP6TABLES -A INPUT -m rt --rt-type 0 -j DROP
$IP6TABLES -A FORWARD -m rt --rt-type 0 -j DROP
$IP6TABLES -A OUTPUT -m rt --rt-type 0 -j DROP

# Link-Local erlauben
$IP6TABLES -A INPUT -s fe80::/10 -j ACCEPT
$IP6TABLES -A OUTPUT -s fe80::/10 -j ACCEPT

# Multicast erlauben
$IP6TABLES -A INPUT -d ff00::/8 -j ACCEPT
$IP6TABLES -A OUTPUT -d ff00::/8 -j ACCEPT

#ICMPv6 Pakete vom Typ [1,2,3,4,128,129] erlauben
$IP6TABLES -A FORWARD -p icmpv6 --icmpv6-type 1 -j ACCEPT
```

v6-RPi

- Raspberry Pi als IPv6-only AP mit den beschriebenen Configs
- Die wenigsten Endgeräte können sich mit einem v6-only Netzwerk verbinden bzw. dieses nutzen
- Verbindung wird meist erst als OK eingestuft, wenn IPv4 funktioniert
- Deaktivieren von „Connection requires IPv4“ oder vergeben einer statischen v4 IP



IPv6 Toolkits



Grazer Linuxtage 2014

THC-IPV6-ATTACK-TOOLKIT

- *A complete tool set to attack the inherent protocol weaknesses of IPV6 and ICMP6*
- Sammlung von kleinen Programmen, die sich sehr gut für Sicherheitstests der eigenen Infrastruktur eignet
- Fokus auf Attacken bzw. Implementierungsfehler
- Bsp.: Testen ob Firewall Pakete mit speziellen Optionen/Flags durchlässt

```
# ./firewall6 eth0 2001:db8::1 22
```

SI6 Networks' IPv6 Toolkit

- *The main goal of this toolkit is to provide security analysis and trouble-shooting functionality for the IPv6 protocol suite*
- „Dieses Toolkit verfolgt einen eher akademischen Ansatz“ Gont@IPv6 Kongress, Frankfurt 2013
- Ermöglicht umfangreiche Einstellungen beim Erstellen der Pakete
- Bsp.: Testen des Paket Too Big Verhalten:

```
# ./tcp6 -d 2001:db8::1 -P 1400
```

No.	Time	Source	Destination	Protoc	Lengt	Info
3	0.0105630	2001:	2001:4810::110	TCP	1474	42257 > 10974 [ACK] Seq=1 Ack=1
4	0.0539700	2001: :1	2001:	ICMPv6	1294	Packet Too Big
23	252.82043	2001:	2001:4810::120	TCP	1484	iconp > 60732 [ACK] Seq=1 Ack=1
24	252.87609	2001: :1	2001:	ICMPv6	1294	Packet Too Big

Sicherheitshinweise

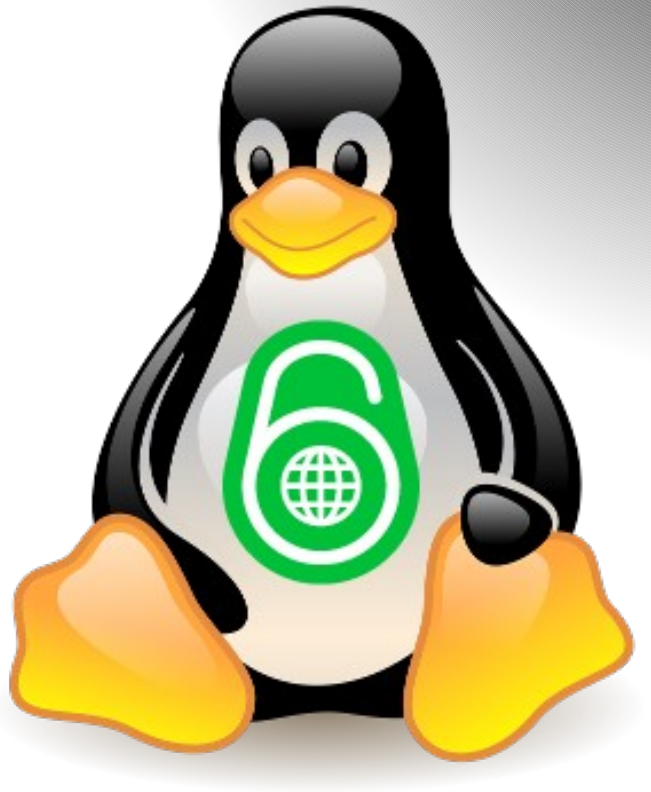
- IPv6 ist in einem modernen Unternehmensnetzwerk bereits aktiv
- Muss in der Sicherheitsstrategie berücksichtigt werden
- Testen der eigenen Infrastruktur
  - *Ungewollt aktive Konfigurationen*
  - *Verhalten bestehender Konfigurationen*
- Beschäftigen Sie sich jetzt damit, bevor es richtig ernst wird :)

Links

- https://www.ietf.org/rfc/rfc4890.txt
- https://www.ietf.org/rfc/rfc7123.txt
- https://www.sixxs.net/wiki/IPv6_Firewalling
- https://www.thc.org/thc-ipv6/
- http://www.si6networks.com/tools/ipv6toolkit/
- http://www.ipv6actnow.org
- http://www.ipv6hackers.org

Mit Linux ins IPv6 Internet

DI Stefan Kienzl, BSc



Grazer Linuxtage 2014