Datenschutz-konformes IPv6 auf xDSL

Lutz Donnerhacke
IKS Service GmbH
http://lutz.donnerhacke.de/Blog/
http://www.iks-service.de/

IKS service

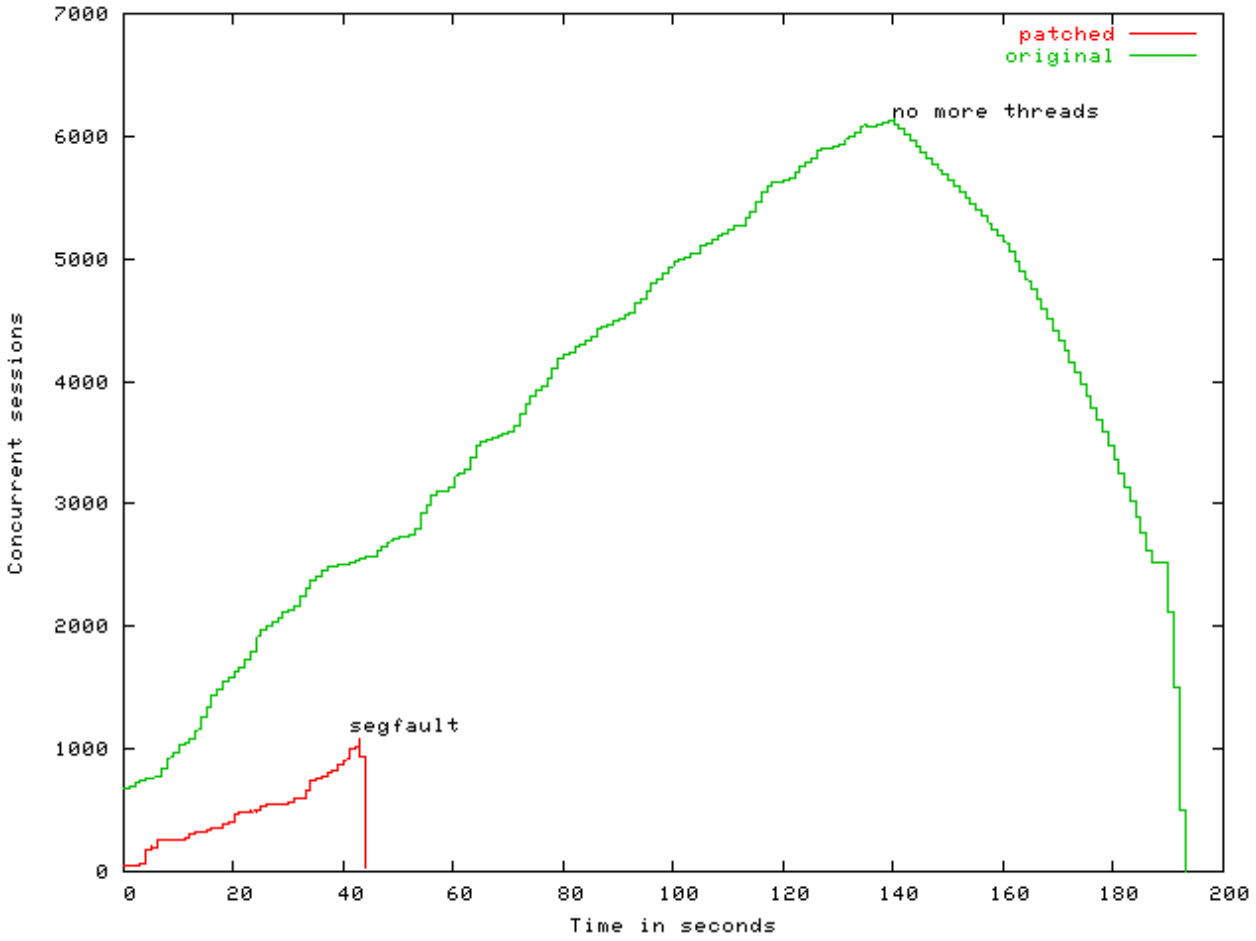
Ausgangslage

- IKS Service GmbH
  - Regionaler ISP, Hosting, Consulting, etc.
  - Seit 1995 kommerziell aktiv
  - Zu klein für große Lösungen
  - Seit 2009 xDSL im ländlichen Thüringen
- Aufgabenstellung
  - Ablösung von Redback durch **irgendwas**
  - Billig, skalierbar, zukunftssicher

Qual der Wahl

- Kommerziell oder Open Source
  - Einmalinvestitionen: Preis vs. Zeit
  - Skalierungskosten: Lizenzen und Hardware
  - Featuritis nach Angebot vs. Gutdünken
  - Wartung und Fingerpointing vs. DTAC?
- Empfehlungen
  - MPD auf FreeBSD: Russland >1 Mio Subscriber
  - OpenL2TP auf Linux: Bekannte Umgebung

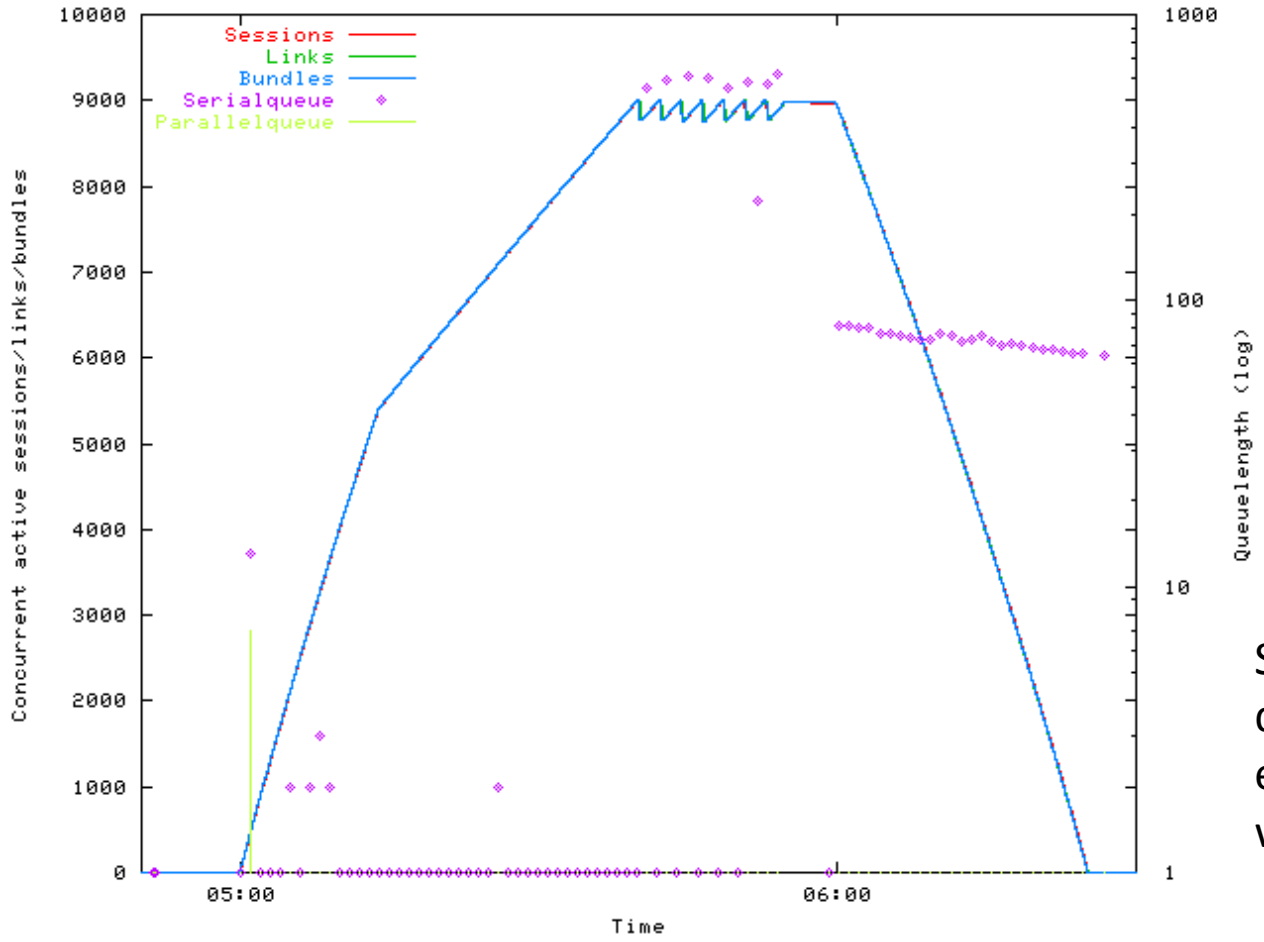
Erste Ernüchterung



Pimp my MPD

- Eventhandling kaputt
  - Begrenzte Queuegröße (Absturz)
  - Unkontrollierte Fork-Orgie
  - **Kompletter Rewrite**
- Eigentlich eine CPE-Implementierung
  - Debugging statt Logging
  - Ein kleiner Fehler = Daemon beendet sich
  - Konfig nicht abspeicherbar
  - Radius-Accounting fehlerhaft und unvollständig
- Obskure Endgeräte (Speedports)
  - Selbstjustierendes LCP anhand von Caller-ID

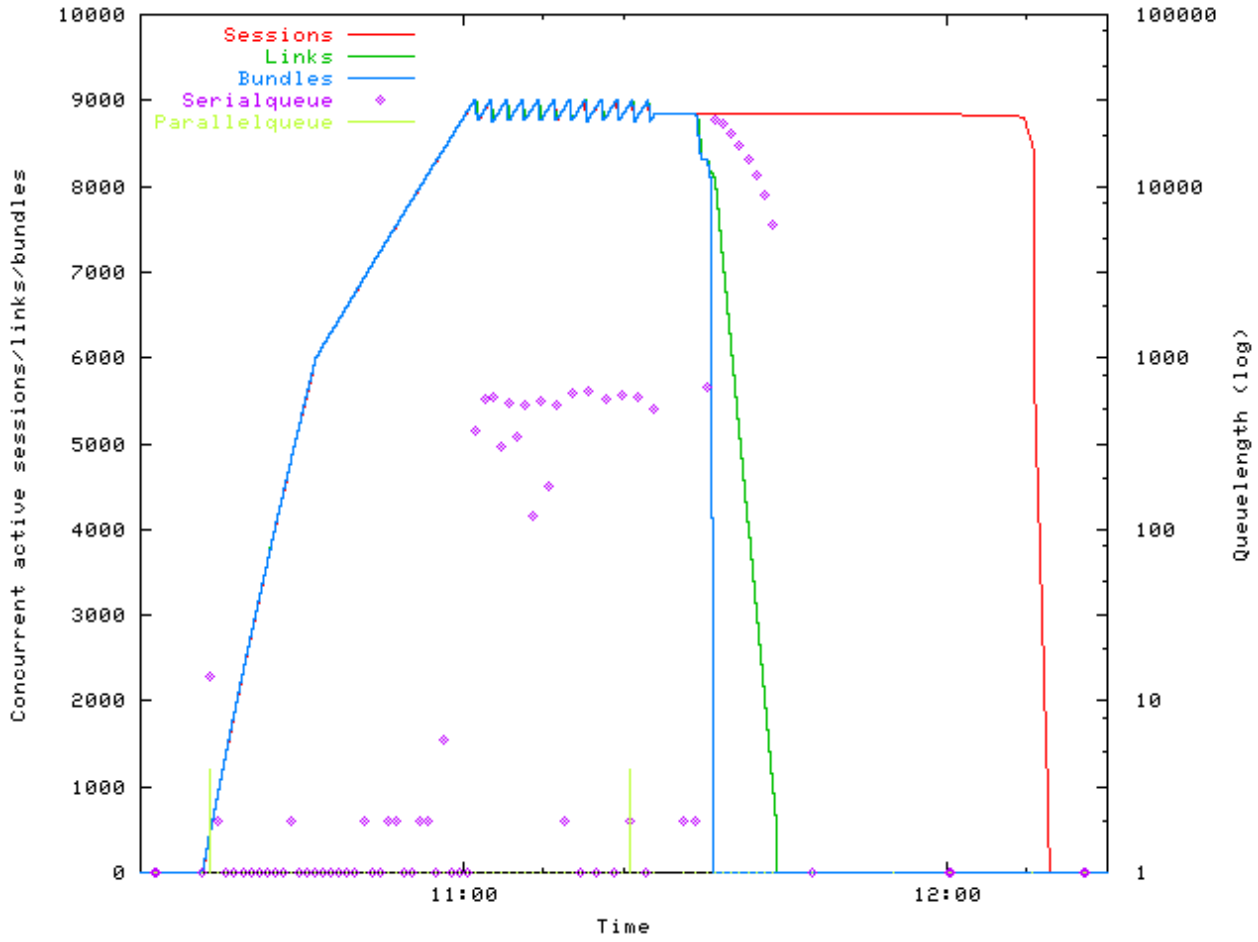
Lasttest (normal)



MPD	OpenL2TP
Load: 3	Load: 20
280MB	2GB

Schnell auf 9000 Nutzer, dann Schwankungen erzeugen und ruhig wieder auflegen.

Lasttest (L2TP-Cut)



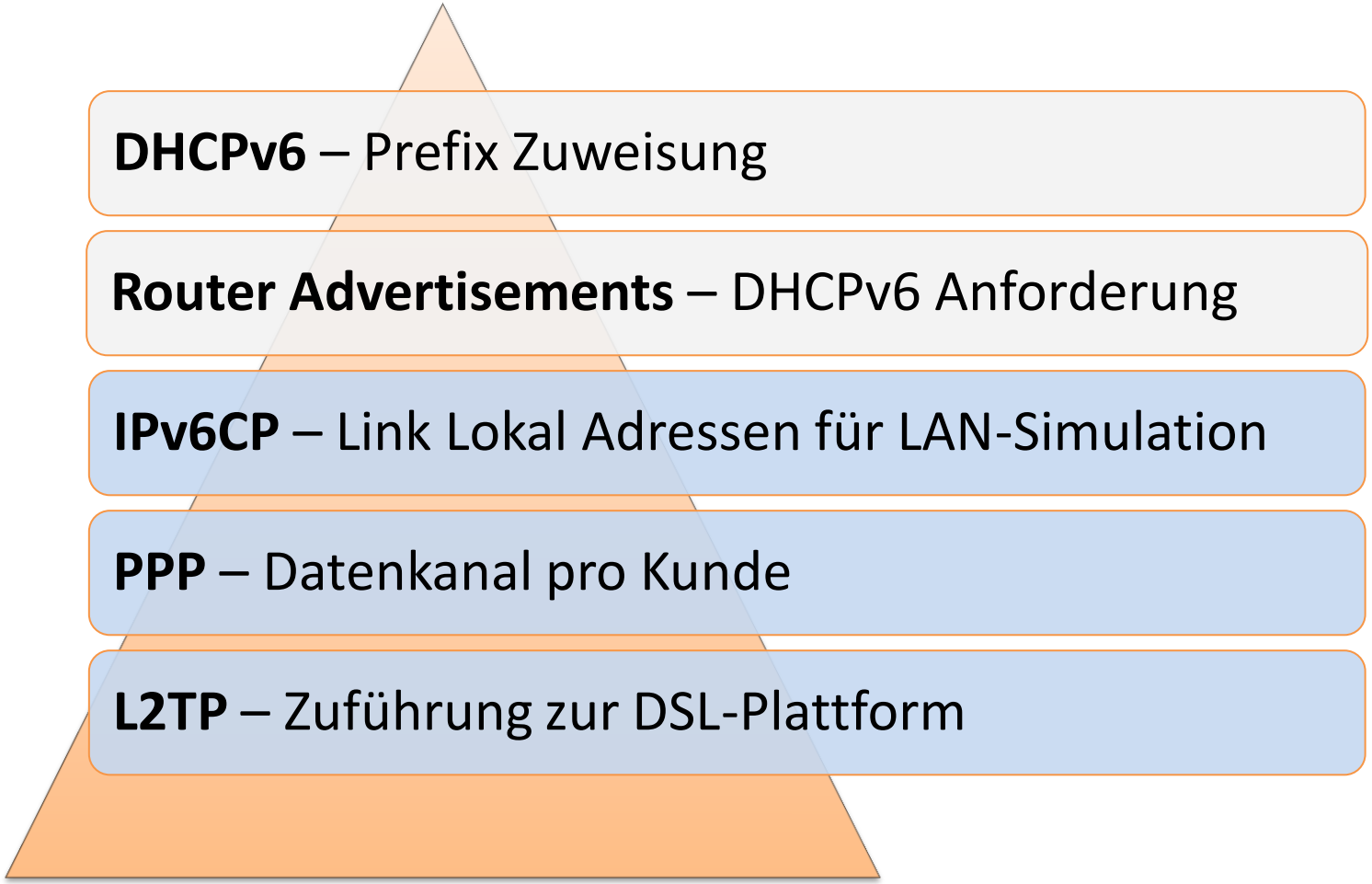
MPD	OpenL2TP
Load: 6	Load: 700
280MB	>4GB

Linux benötigte
killall -9 pppd

Die NAT-Hölle

- CGN schon länger im Einsatz
  - Adressmangel wird akzeptiert
  - Dynamische öffentliche IP auf Zuruf
- Memory Corruption
  - Häufige Reboots durch *panic* (in *libalias*)
  - Viele Fehlerursachen (NAT Konfig, Raceconditions)
  - Einstellbarer Delay zwischen Events
  - Wegwerfen von NAT-Tabellen statt *panic*
  - Todo: Trennung von *malloc* Pools
  - Todo: Verzögerung von *free*

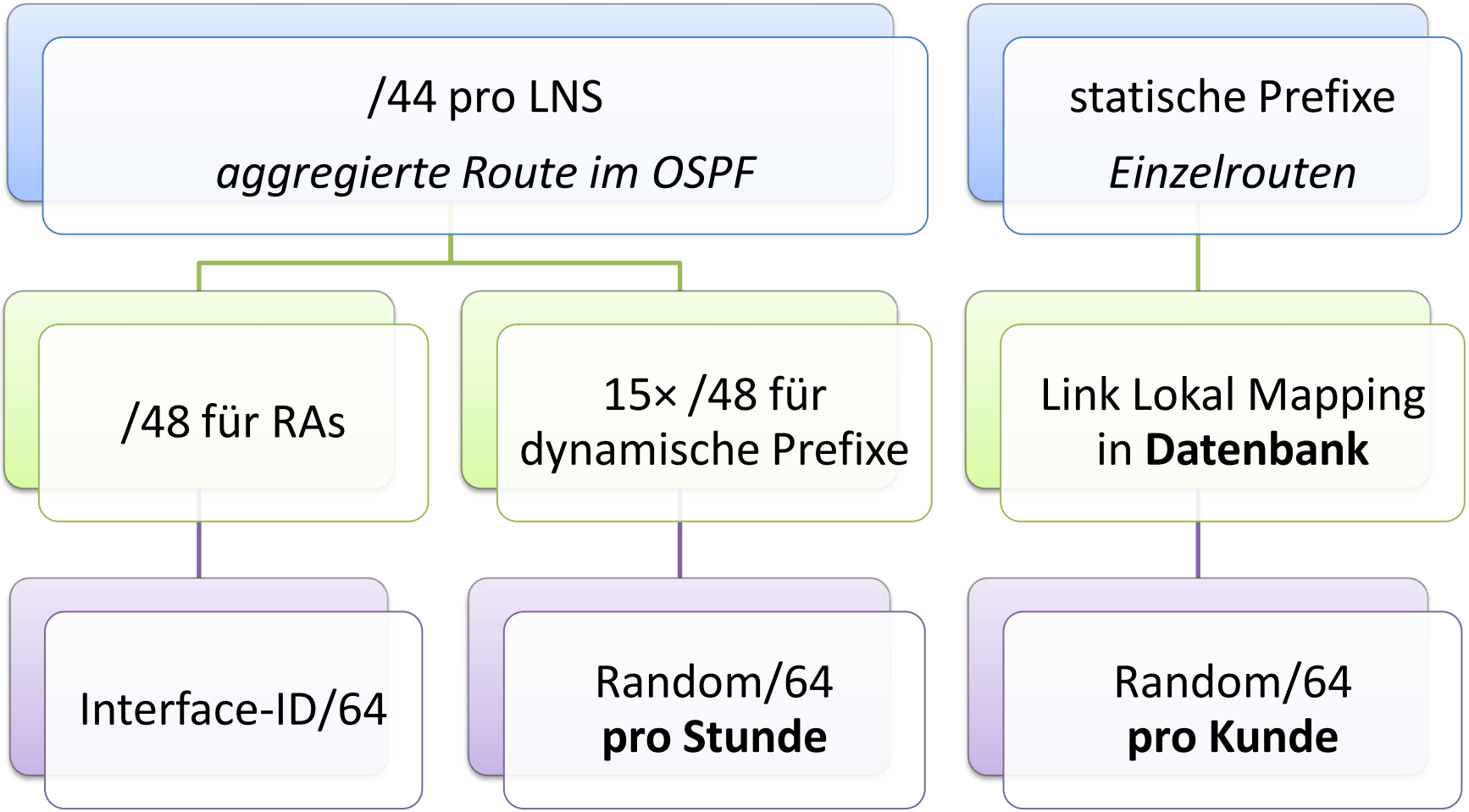
IPv6


DHCPv6 – Prefix Zuweisung
Router Advertisements – DHCPv6 Anforderung
IPv6CP – Link Lokal Adressen für LAN-Simulation
PPP – Datenkanal pro Kunde
L2TP – Zuführung zur DSL-Plattform

IPv6 – Aufgabenverteilung

- PPP-Profil auf ADSL
  - L2TP, PPP und IPv6CP
  - MPD erzeugt ein virtuelles LAN zum Kundenrouter
- DHCP-Profil auf VDSL
  - IPv6 durchlassen, aber RA-Guard aktiv
- ➢ **Harmonisierte IPv6-Zuführung der CPE**
- RA von Quagga mit O=1
- DHCPv6 für Prefix Delegation

Adressplanung



Quagga

Statische Konfig für alle Interfaces

```
interface ng1234
  ipv6 address 2001:db8:70:4d2::1/64
  no ipv6 nd suppress-ra
  ipv6 nd other-config-flag
  ipv6 nd prefix 2001:db8:70:4d2::/64 7200 3600
```

Routing

```
ipv6 prefix-list statics6 deny 2001:db8:70::/44 ge 45
ipv6 prefix-list statics6 permit 2001:db8::/32 le 64
route-map redistribute6 permit 1
  match ipv6 address prefix-list statics6
router ospf6
  redistribute kernel route-map redistribute6
  redistribute static route-map redistribute6
```

DHCPv6 für Prefix Delegation

- Standard Software braucht
  - Interfaceliste
  - Reload oder Patch für Prefixrotation
- Quagga kann kein dhcpv6-relay
- Eigenentwicklung
  - Entwurfsprinzipen: NIH, WFM, DIB
  - Datenausleitung per *divert*

    divert 1 udp from fe80::/64 to ff02::1:2 dst-port 547 recv ng* in
    - Patch des Kernels notwendig: *divert* kann nur IPv4
  - Nur Relay oder Daemon?

DHCPD-PD

- Eigenentwicklung eines DHCPv6 Daemon
  - **Verteilt** DNS, NTP, … Server
  - Holt **Prefixe** pro *Link-Local%Interface* per Script
    - NDBM für dynamische Prefixe
    - Routen setzen und alte Routen löschen
    - Datenbankzugriff für statische Prefixe
  - Holt **Adressen** pro *Link-Local%Interface* per Script
    - Pseudorandom, fixed im Bereich des RA-Prefix
    - Benötigt für halbtransparente CPEs
  - **Verlängert** alte Prefixe auf Wunsch

Routingtabelle

O>* 2001:db8:0:**ed98**::/64 [110/1] via fe80::204:23ff:fee9:9b3a, vlan115
O>* 2001:db8:0:**ede4**::/64 [110/1] via fe80::204:23ff:fee9:9b17, vlan115
K>* 2001:db8:0:**f423**::/64 via fe80::c225:6ff:fe44:8a5, ng3156
K>* 2001:db8:0:**f7a7**::/64 via fe80::c225:6ff:fe7e:2329, ng3140
K>* 2001:db8:0:**fad7**::/64 via fe80::be05:43ff:fe6d:d1de, ng2359
K>* 2001:db8:0:**fc3a**::/64 via fe80::be05:43ff:fee0:1ae9, ng3240
K>* 2001:db8:0:**fcb1**::/64 via fe80::be05:43ff:fe34:10d7, ng2892
…
S>* 2001:db8:60::/44 [1/0] via ::1, lo0
C>* 2001:db8:60::/64 is directly connected, ng0
C>* 2001:db8:60:**1**::/64 is directly connected, ng**1**
C>* 2001:db8:60:**2**::/64 is directly connected, ng**2**
…

Routingtabelle

K>* 2001:db8:61:e1f0::/64 via fe80::c225:6ff:fe44:1514, ng3325
K>* 2001:db8:61:ed6a::/64 via fe80::224:feff:fe69:777e, ng1657
K>* 2001:db8:61:f7cf::/64 via fe80::be05:43ff:fec5:65bb, ng2487
K>* 2001:db8:6**1**:fa39::/64 via fe80::c225:6ff:fec6:13b1, ng95
K>* 2001:db8:6**2**:4c5::/64 via fe80::be05:43ff:fea2:9391, ng561
K>* 2001:db8:62:16ed::/64 via fe80::c225:6ff:fe7e:2329, ng3140
K>* 2001:db8:62:29c0::/64 via fe80::224:feff:fec2:b538, ng455
K>* 2001:db8:62:2ee6::/64 via fe80::c225:6ff:fe85:92b0, ng2108
…
K>* 2001:db8:6**4**:72ab::/64 via fe80::224:feff:fec2:b538, ng455
K>* 2001:db8:6**6**:2b2::/64 via fe80::be05:43ff:fefb:98a4, ng1900
K>* 2001:db8:6**d**:2ec::/64 via fe80::9ec7:a6ff:fe48:ab04, ng555
K>* 2001:db8:6**e**:ec4e::/64 via fe80::9ec7:a6ff:fe48:ab04, ng555
…

Ergebnisse

- Ohne Kundeninformation bzgl. IPv6 sind
  - 2% der Kunden mit IPv6 versorgt
  - 20% von deren Traffic geht über IPv6
    - DNS, Facebook, kleinanzeigen.ebay, Google, Mail, …
- Reaktionen von Kunden

  „Wie ändert sich der Ping? Gehen 10ms?“

  „Warum hat der IPv6 und ich nicht?“

  „Kann man auch ein statisches /48 bekommen?“

  „Weniger Ausfälle wären mir lieber.“

Voller Erfolg?

Re: IPv6 Prefix

Für Dich hat IPv6 keine Vorteile oder Nachteile, das ist eigentlich nur ein Problem der "DSL Anbieter". Da weltweit die IP-Adressen ausgehen, wird irgend wann auf IPv6 umgestellt. Weil sich da durch wieder viele neue IP-Adressen ergeben.

IPv4 vier Nummernblöcke z.B. 192.168.178.100
IPv6 sechs Nummernblöcke z.B. 192.168.178.188.198.100

Für uns als Endanwender eigentlich uninteresant.

Voller Erfolg!

Re: IPv6 Prefix

Für Dich hat IPv6 keine Vorteile oder Nachteile, das ist eigentlich nur ein Problem der "DSL Anbieter". Da weltweit die IP-Adressen ausgehen, wird irgend wann auf IPv6 umgestellt. Weil sich da durch wieder viele neue IP-Adressen ergeben.

IPv4 vier Nummernblöcke z.B. 192.168.178.100
IPv6 sechs Nummernblöcke z.B. 192.168.178.188.198.100

Für uns als Endanwender eigentlich uninteresant.

- Er hat völlig Recht!
- Technik hat im Hintergrund zu funktionieren.
- Verständnis beim Kunden ist optional.

Fragen?

Die MPD Lösung mit Support gibt‘s von uns.

Sie wollen Geräte testen?
L2TP Tunnel oder Gerät direkt zu uns.

IKS service