9 Jahre IPv6 im Abteilungsnetz . . . und zu Hause

oder

IPv6 mit kleinem Budget

Erfahrungsbericht, mit etwas Geschichte

Ignatios Souvatzis

Institut für Informatik, Abt. V
Universität Bonn
<ignatios@cs.uni-bonn.de>
. . .
The NetBSD Project
<is@netbsd.org>

BGNW 2009

universitätbonn

- *Konfigurationstipps werde ich im Erfahrungsbericht mündlich eintreuen und im letzten Abschnitt detailliert erläutern.*
- *Sicherheitsfragen detailliert in einem Vortrag später am Tag.*

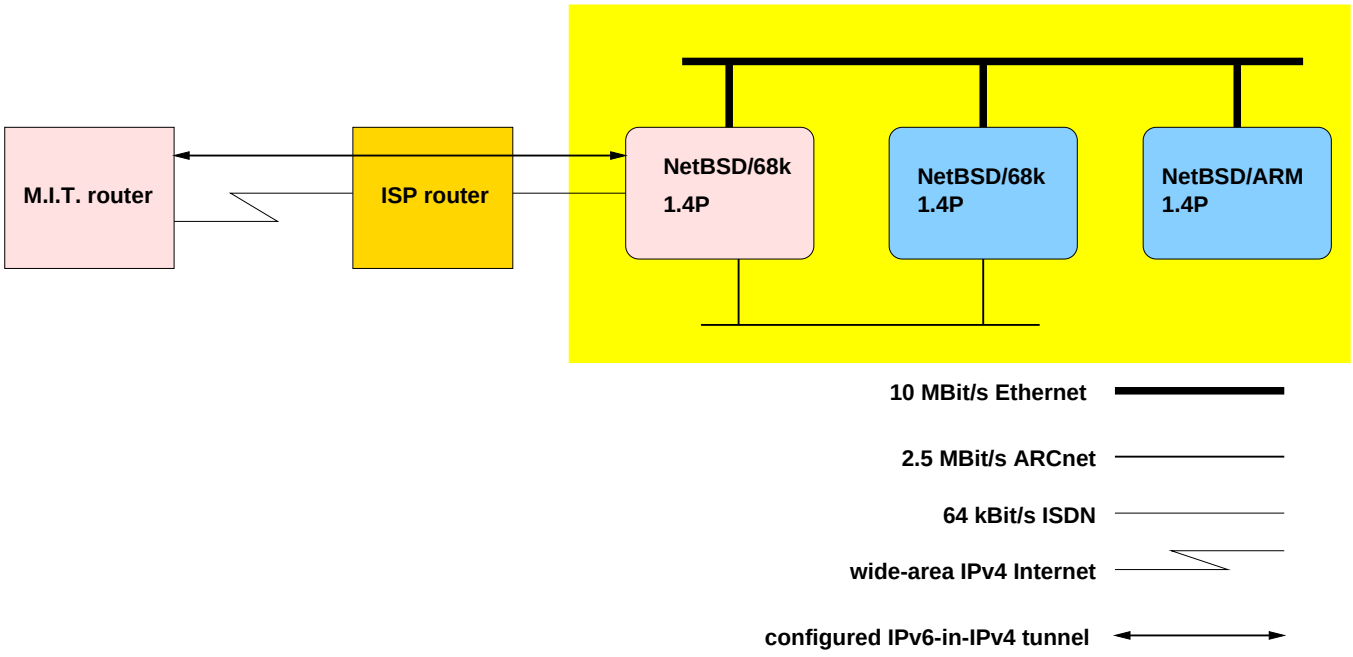
Was ist IPv6?

- Protokoll auf ISO Layer 3
- kann parallel zu IPv4 benutzt werden
- kann anstatt zu IPv4 benutzt werden (wenn die Gegenstelle es spricht)
  - ... mit moderner Hard- und Software
  - ... ~~nur mit teuerer Hard- und Software?~~
    Nicht unbedingt.

Inhaltsverzeichnis

konfigurierter Tunnel, 1999/2000

- wurde damals benötigt, um den ARCnet-Treiber zu testen (Routing, PMTUd)
- 6BONE-Verbindung zum M.I.T.
- funktionierte, aber nur für Verbindungsversuche zu gebrauchen
- hohe Latenzzeit, hohe Paketverlustrate

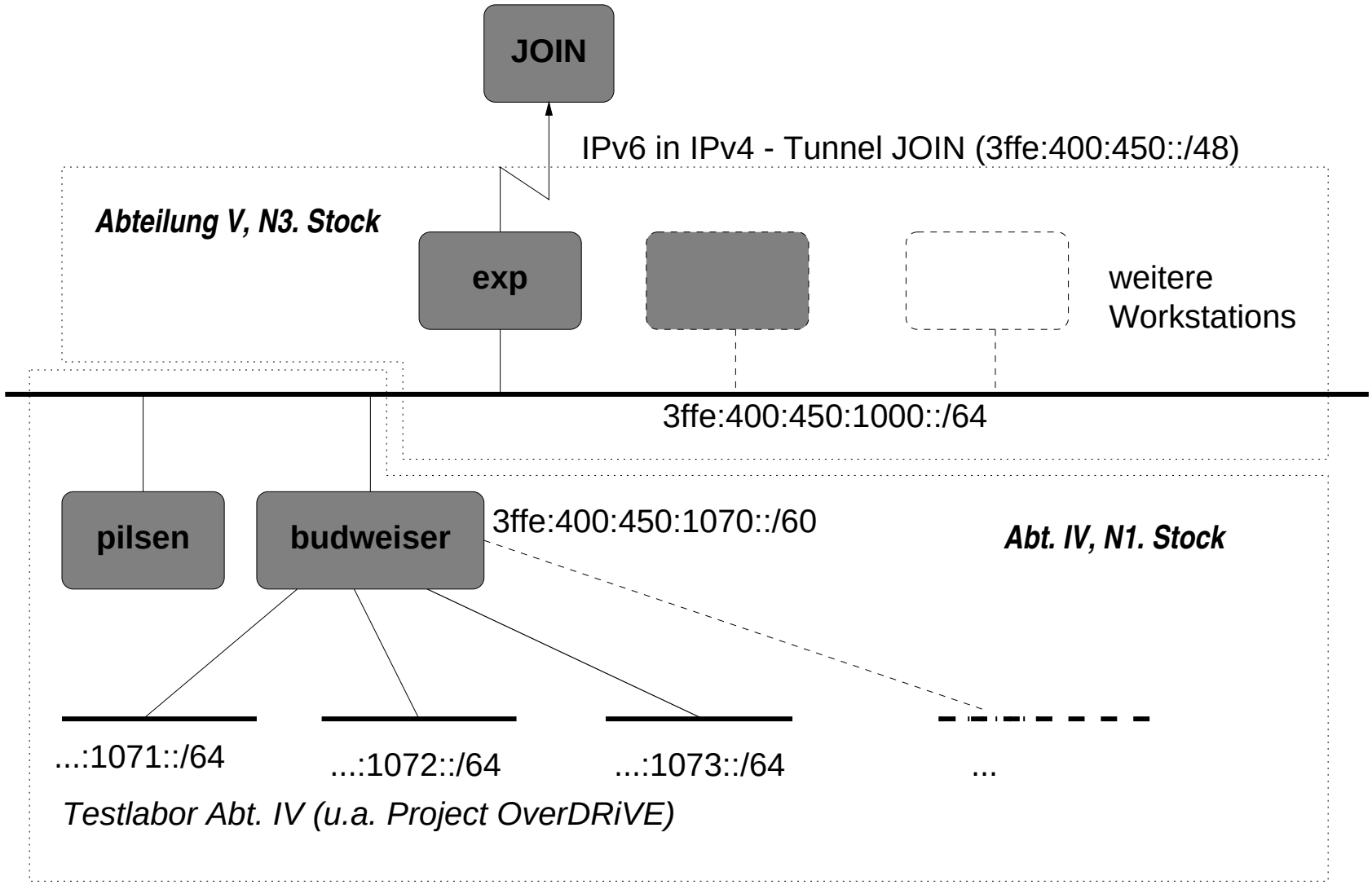


Inhaltsverzeichnis

Netz an der Universität Bonn, 2000

- Tunnel-Router: i486/66 MHz, Fast Ethernet, NetBSD-1.4P
- IPv6 in IPv4 nach Münster (JOIN)
- IPv6 direkt auf dem LAN
- erste Produktionsanwendung: Das Netzlabor der Abteilung IV brauchte mehrere geroutete drahtlose und verdrahtete Netze für den Test von Netzübergabealgorithmen.

Universität Bonn 2000-2002



IPv6 im DFN bis Juni 2005

- Overlay-Netz, Topologie-unabhängig
- zentraler IPv6-in-IPv4-Router an der Universität Münster (DFN-Project JOIN)
- Experimentalbetrieb
- verbundem mit dem globalen Experimentalnetz 6BONE
- abgeschaltet 20050607

http://www.join.uni-muenster.de

Bonn - Norwegen 2000

cosinus# traceroute6 www2.no.netbsd.org
traceroute to server.pasta.cs.uit.no (3ffe:2a00:100:3001::2), 30 hops max, 12 byte packets
1 6bone.ipv6.uni-muenster.de 28.443 ms * 22.275 ms
2 3ffe:600:8000::d 55.623 ms * 59.225 ms
3 6bone-gw.sics.se 274.208 ms * 220.015 ms
4 3ffe:200:1:b::2 218.731 ms * *
5 3ffe:2a00:100:7003::2 249.568 ms * 280.394 ms
6 tromso-ipv6.uninett.no 285.326 ms * 246.398 ms
7 3ffe:2a00:100:7011:280:1cff:fe5d:3038 238.394 ms * 156.65 ms
8 server.pasta.cs.uit.no 186.663 ms 282.858 ms 287.064 ms

- nur wenige offensichtlicht Zwischenschritte
  . . . aber jeder davon repräsentiert eine ganze Reihe IPv4-Zwischenscrhitte!
- ... das führt zu hoher Latenz und relativ hoher Verlustrate!

Inhaltsverzeichnis

Universität Bonn 2005–2007

- Informatik V:
  - Tunnelrouter:
    i586 MHz, fast ethernet, NetBSD-1.6
  - IPv6 in IPv4 nach Münster (JOIN), außer Betrieb
  - IPv6 in IPv4 zum Rechenzentrum
  - IPv6 in IPv4 zum Netzlabor der Abt. IV
  - native IPv6 im lokalen Netz
- Informatik, Abteilung IV:
  - Tunnelrouter: eine Linux-Workstation
  - mehrere Ethernet- und WLAN-Anschlüsse für das Labor

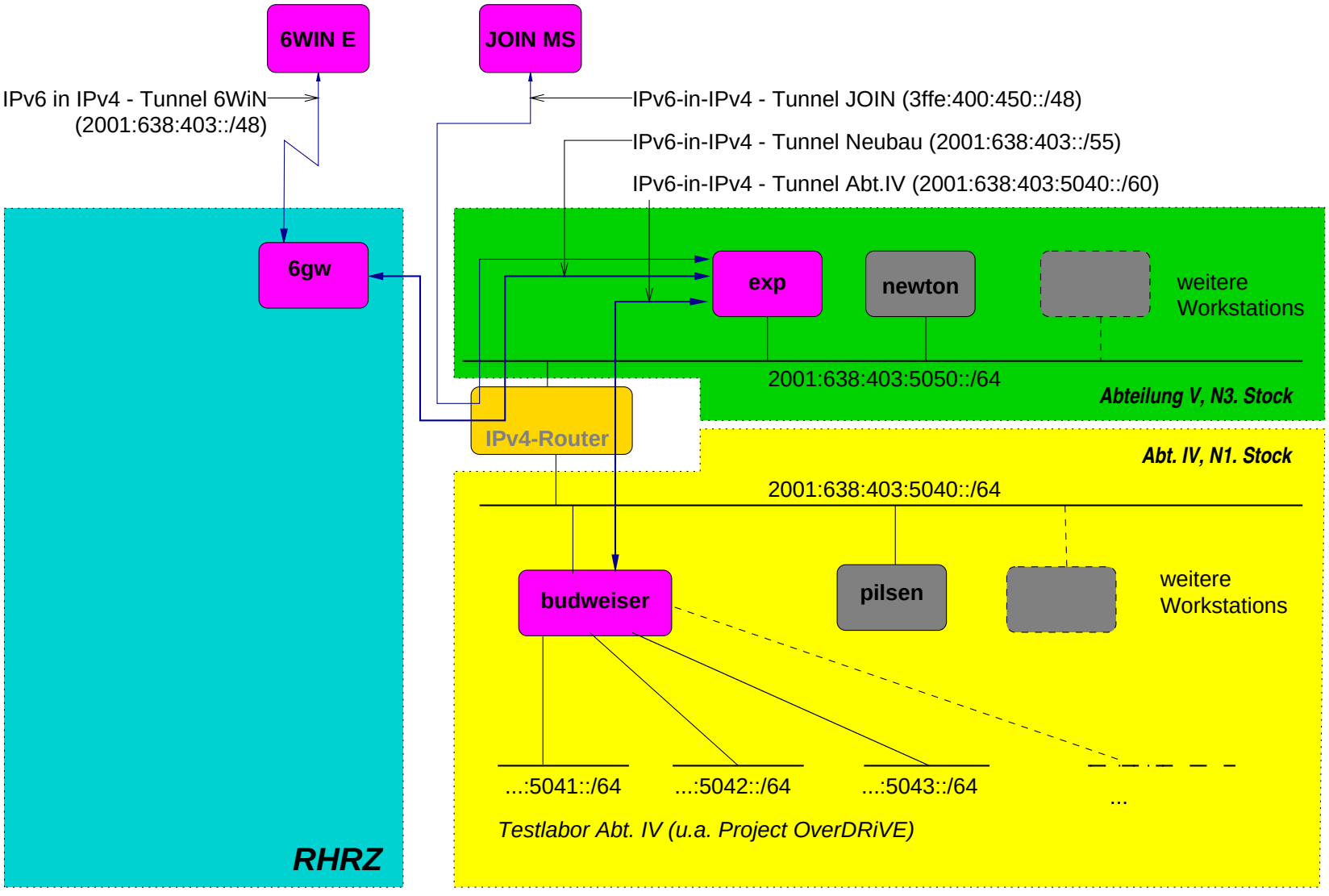
Universität Bonn 2005–2009

Rechenzentrum:

- eigener (für die IPv6-Anbindung) Hardware-Router
- Tunnel zur Informatik V
- Experimentelle Tunnel zur Kernphysik und den Wirtschaftswissenschaften (2006-. . .)

- Tunnel nach Essen (bis Mitte 2007)
- Tunnel nach Birlinghoven (jetzt)

Universität Bonn 2005/2006



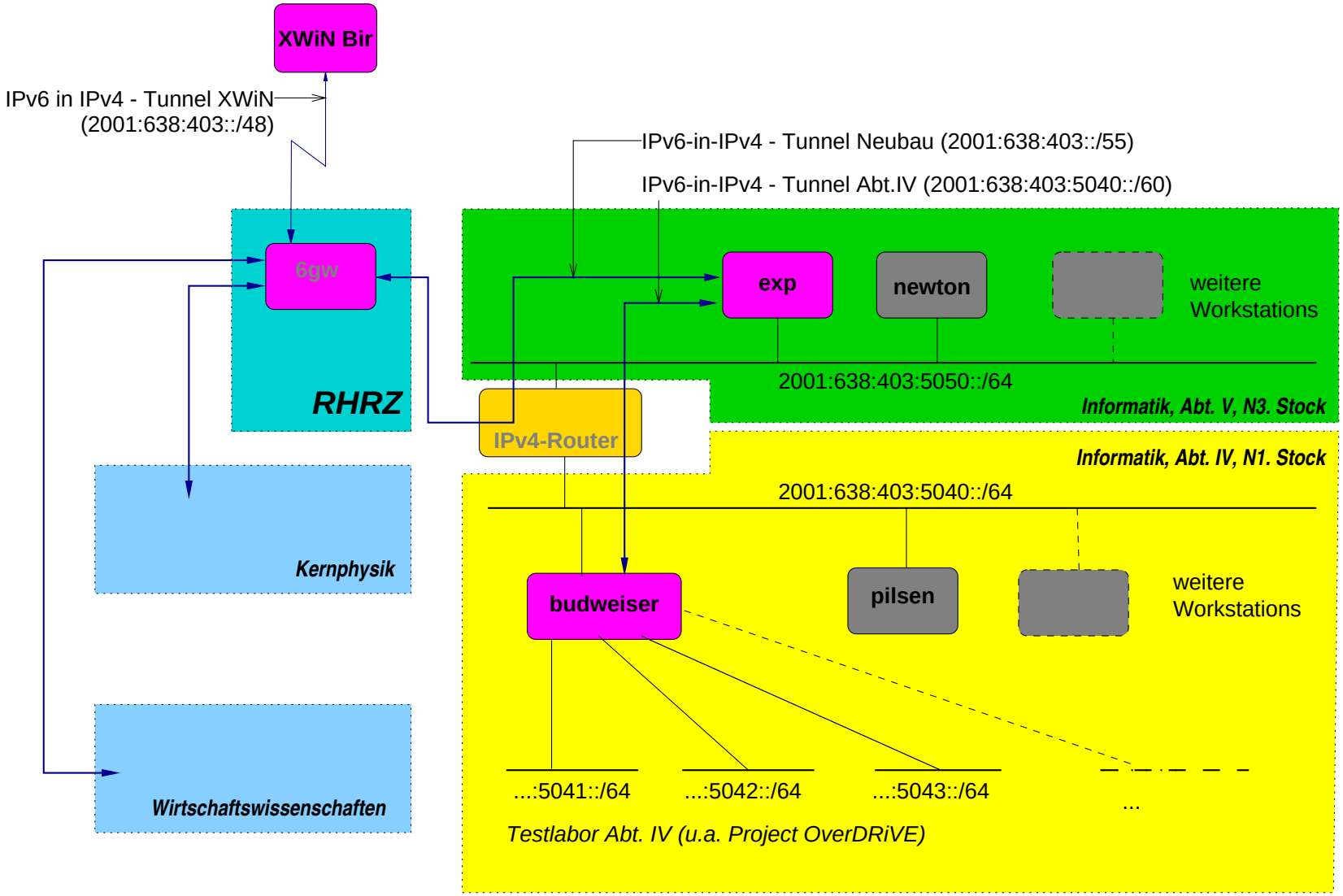
IPv6-Netz Uni Bonn/Informatik

2005-Mar-11 I. Souvatzis

IPv6-in-IPv4-Tunnel (WAN) IPv6-in-IPv4-Tunnel (LAN/MAN) Echtes IPv6 (LAN/MAN)

universitätbonn

Universität Bonn 2007–



IPv6-Netz Uni Bonn/Informatik

2005-Mar-11 I. Souvatzis

IPv6-in-IPv4-Tunnel (WAN) IPv6-in-IPv4-Tunnel (LAN/MAN) Echtes IPv6 (LAN/MAN)

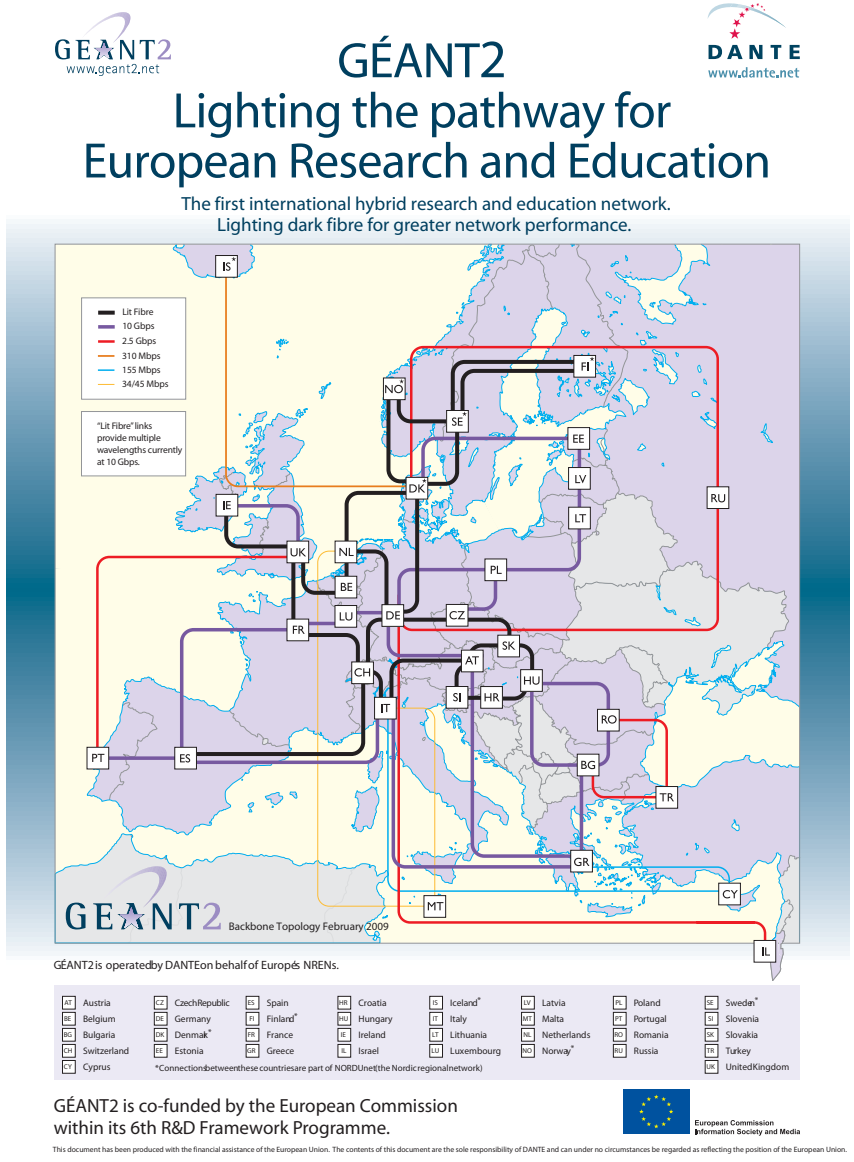
universitätbonn

DFN 2002-2006-...

- Ab etwa 2002 begann JOIN mit dem Aufbau eines Präproduktionsnetzes für das DFN
  http://web.archive.org/web/*/http://www.6win.de/
  (nur noch in historischen Archiven)
- Backbone: Ring mit 5 Knoten und einer zusätzlichen Querverbindung
  - getrennt von den IPv4-Routern
- Teilnehmende Institutionen waren nativ (an den Backboneknoten) oder über topologisch kurze Tunnel angebunden.
- Im Jahr 2005 lief das Projekt JOIN aus, und das DFN-NOC übernahm den Betrieb des 6WiN
- ... inzwischen wurde IPv6 in die normale Infrastruktur integriert und das 6WiN abgeschaltet

European education & research network

- http://www.geant2.net/
- Backbone 2.5 bis N*10 GB/s
- internes Routingprotokoll wurde Anfang 2005 von OSPF auf IS-IS umgestellt
- IPv4 und IPv6 werden parallel gleichartig transportiert



Bonn - Norwegen 2006

1 exp.cs.uni-bonn.de 0.489 ms 0.355 ms 0.347 ms
2 2001:638:403:f01::1 2.074 ms 1.932 ms 2.023 ms
3 2001:638:f:500::403:1 8.709 ms 8.644 ms 8.659 ms
4 2001:638:0:9::2 32.253 ms 32.108 ms 32.007 ms
5 dfn.rt1.fra.de.geant2.net 32.524 ms 32.533 ms 32.531 ms
6 so-1-3-0.rt1.lux.lu.geant2.net 46.637 ms 46.667 ms 46.547 ms
7 nordunet-gw.rt1.cop.dk.geant2.net 46.462 ms 46.504 ms 46.593 ms
8 dk-gw.nordu.net 47.242 ms 46.97 ms dk-gw.nordu.net 47.075 ms
9 no-gw2.nordu.net 54.922 ms 55.019 ms 54.859 ms
10 no-gw.nordu.net 55.022 ms 54.84 ms 54.952 ms
11 oslo-gw1.uninett.no 55.316 ms 55.093 ms 55.212 ms
12 trd-gw.uninett.no 63.106 ms 62.954 ms 62.934 ms
13 tromso-gw.uninett.no 76.801 ms 76.422 ms 76.849 ms
14 tromso-ipv6-gw.uninett.no 77.269 ms 77.124 ms 77.319 ms
15 cisco.pasta.cs.uit.no 77.93 ms 77.526 ms 78.088 ms
16 server.pasta.cs.uit.no 77.94 ms 77.937 ms 77.836 ms

- scheinbar mehr Hops — weniger Verzögerung, keine Paketverluste

Produktionsanwendungen

- Netzinstallation von NetBSD von ftp.fr.netbsd.org: 1 MB/s, in wenigen Minuten beendet.
- . . . zu schnell, um einen lokalen Spiegel in Betracht zu ziehen
- war früher schneller als IPv4 (durch das getrennte IPv6-Netz), aber, ach, die guten Zeiten (6WiN (.de) + 6NET (.eu) sind vorbei
- andererseits ist das neue integrierte Netz schneller als das alte IPv6-Netz

Inhaltsverzeichnis

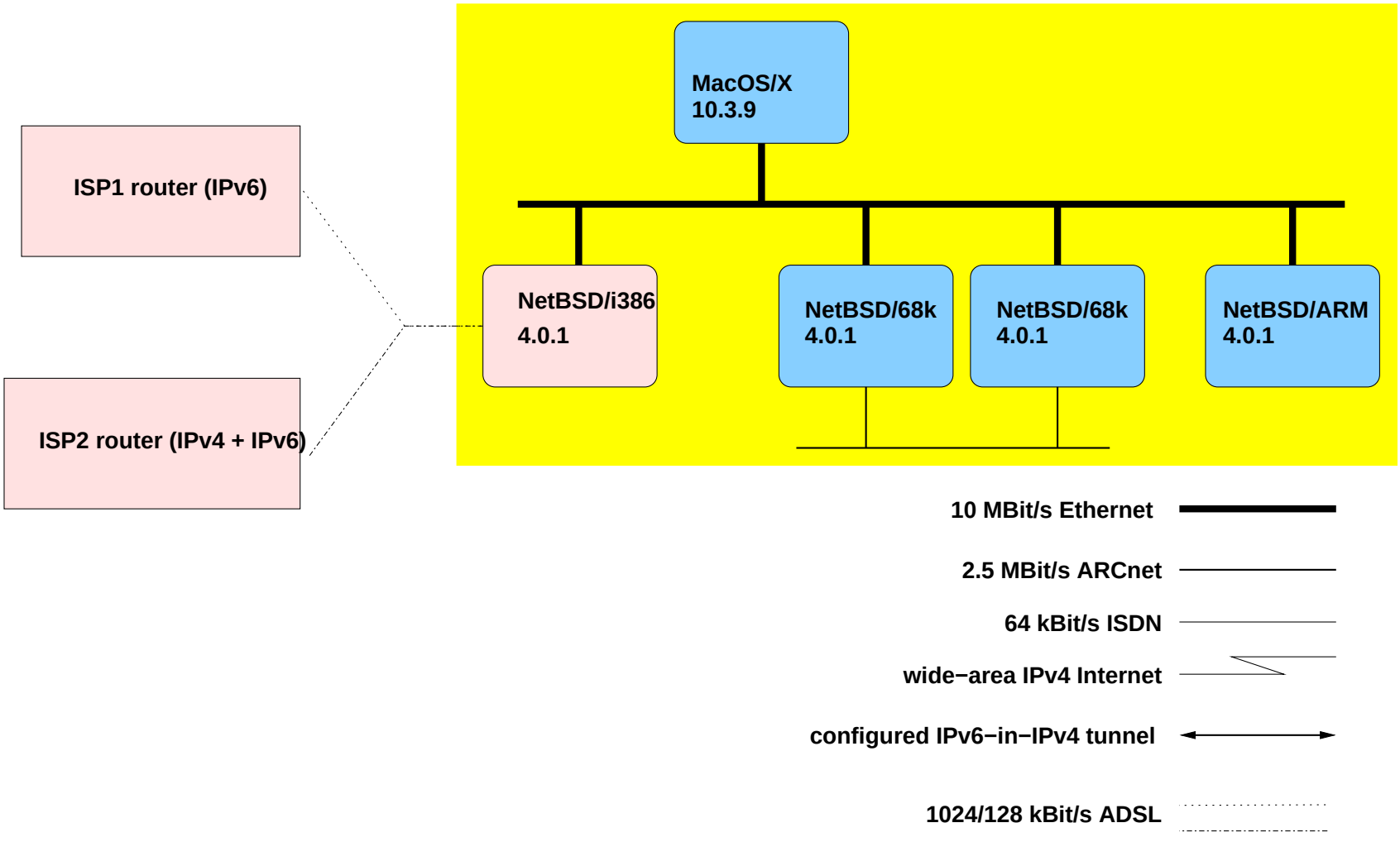
Heimnetz/kleines Büronetz: Tunnelverbindungen

- konfigurierte Tunnel werden angeboten von: Freenet6 (oder wie sie dieses Jahr heißen), XS26(?), SixXS, ...
  - oft eine hohe Verlustrate oder Latenzzeit
- 6to4: /48 pro IPv4-Adresse
  - woher eine Defaultroute nehmen? (Anycast, evtl. manuell)
  - asymmetrischer Pfad
  - keine Kontrolle
  - oft hohe Verlustrate oder Latenz (aber nach Ende von 6BONE besser geworden
  - moderne AirPorts sprechen 6to4!
- Teredo (IPv6 über UDP/IPv4 mit NAT-piercing)
  - Komplexität in jedem einzelnen Endgerät, statt im Router
  - kein asymmetrisches Routing!

IPv6 im Heim- und Büronetz, 2009

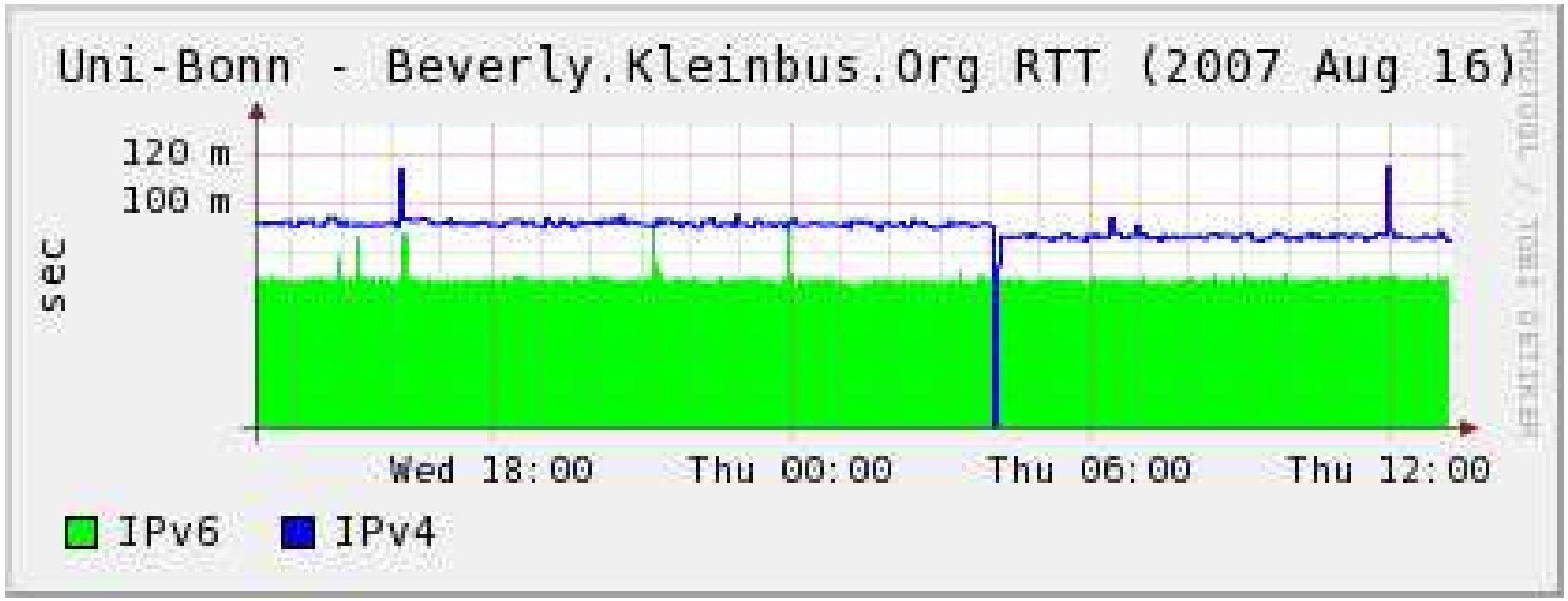
- T-DSL-Zugangsnetz:
  - eine Reihe von Jahren nur ein Provider mit IPv6
  - inzwischen mindestens sieben
  - benutzbar, wenn Sie ein BSD / MacOS-X / oder Linux oder Solaris ... hinter einem simplen ,,ADSL-Modem“ benutzen
  - nicht nutzbar, wenn Sie ein im Router integriertes DSL-Modem haben
  - ... das kann sich aber im Zeitalter der Linux-Firmware schnell ändern

IPv6 (SOHO)auf dem Draht: 2005-~~2007~~2009



universitätbonn

IPv6 (SOHO)auf dem Draht: 2005-~~2007~~2009



universitätbonn

6to4 Heimnetz–Norwegen, 2007

traceroute6 to 2001:700:400:600::3 from 2002:d5f0:b48b::1
1 2001:a60::89:1:1:3 90.999 ms
2 2001:a60:9002:1::1 90.025 ms
3 2001:a60:0:1ff::1 90.856 ms
4 2001:a60:0:1ff::2 104.457 ms
5 2001:440:eeee:ffc8::2 258.152 ms
6 2001:440:eeee:ffc8::2 258.672 ms
7 2001:440:eeee:ffc8::1 250.807 ms
8 2001:440:1239:1001::2 257.039 ms
9 2001:440:1239:100d::2 286.282 ms
10 2001:7f8:d:fb::24 290.306 ms
11 2001:948:0:f049::2 288.639 ms
12 2001:948:0:f041::2 293.004 ms
13 2001:700:0:123::2 293.732 ms
14 2001:700:0:10::2 301.856 ms
15 2001:700:0:6::2 315.531 ms
16 2001:700:0:702::3 316.225 ms
17 2001:700:0:fff7::2 317.303 ms
18 2001:700:400:600::3 318.217 ms

Native Heimnetz–Norwegen, 2007

traceroute6 to 2001:700:400:600::3 from 2001:1a50:5031:77::1
1 2001:1a50:ffff:ffff::7 71.301 ms
2 2001:1a50:ffff:fffe::b1 64.428 ms
3 2001:7f8::4f9:0:1 67.268 ms
4 2001:5000:0:24::2 67.414 ms
5 2001:5000:0:13::3 64.97 ms
6 2001:5001:200:6::2 99.748 ms
7 2001:2000:3010::2 102.023 ms
8 2001:798:28:10dd::5 101.617 ms
9 2001:798:cc:2201:2801::1 123.657 ms
10 2001:798:cc:1501:2201::1 123.879 ms
11 2001:798:15:10aa::2 127.434 ms
12 2001:948:0:f055::2 123.79 ms
13 2001:948:0:f049::2 135.449 ms
14 2001:948:0:f041::2 145.738 ms
15 2001:700:0:123::2 145.42 ms
16 2001:700:0:10::2 153.449 ms
17 2001:700:0:6::2 171.44 ms
18 2001:700:0:702::3 167.228 ms
19 2001:700:0:fff7::2 167.179 ms
20 2001:700:400:600::3 168.591 ms

Konfigurationstipps

Wenn Sie Ihre externe Verbindung aufsetzen

- Setzen Sie auf Ihrem Router eine Reject- (oder notfalls Blackhole)-Route auf Ihr /48
- Spezifischere Routen existierender Subnetze haben Vorrang

(sonst haben Sie 256-Hop-Pingpongs für jedes fehladressierte Paket!)

Mehr Konfigurationstipps

Bevor Sie AAAA-Einträge für eine Maschine publizieren:

- stellen Sie sicher, dass ICMP6 nach außen funktioniert, oder
- stellen Sie sicher, dass das IPv6-Routing funktioniert, und dass die Services der Maschine über IPv6 ansprechbar sind
- vorzugsweise beides!

(sonst werden Ihre Klienten eine Verzögerung von einer halben bis zu einer ganzen Minute sehen, bis die Applikation die nächste (z.B. IPv4-) Adresse anspricht.)

Noch mehr Konfigurationstipps

Bevor Sie AAAA-Einträge für eine Maschine publizieren, die langfristig Service anbieten soll:

- siehe eben, zusätzlich
- geben Sie der Maschine (zusätzlich zu, oder statt) der auto-konfigurierten Adresse eine statische Adresse im kleinen Bereich
  (der ungeplante Austausch der Maschine oder der Netzwerkkarte passiert früher, als Sie planen, und DNS propagiert *langsam*, jedenfalls langsamer als Neighbour Discovery
- evtl. eine Adresse pro Service für mehr Flexibilität? Sie haben genug. Wirklich.

Konfigurationstipps für Klienten (bzw. deren Router)

Niemals sollte ein Router einen Prefix anpreisen, der nicht (fast immer) eine tatsächliche Verbindung bereitstellt und sonst ein "net unreachable" schickt, denn

- Der Standard schreibt vor, dass IPv6-Adressen bevorzugt werden.
- Ihre Klienten sehen bei jedem Verbindungsversuch einen NN-Sekunden- Timeout, bis die nächste Addresse aus dem DNS benutzt wird.

Weitere Konfigurationstipps für Klienten

- Ihre Klientenmaschinen sollten evtl. IPv6 Autoconfiguration Privacy Extensions benutzen – erschwert das Erstellen von Bewegungsprofilen (wenn Sie alle Cookies abstellen, alle Webservices mit speziellen Sitzungsadresse/Suchparameter etc. vermeiden, usw.)
- Im Gegenzug sollten Sie als Netzverantwortlicher außer Arpwatch (für IPv4) auch NDPmon (für IPv6) laufen lassen, um unbefugte Eindringlinge – aber auch Fehlkonfigurationen – zu bemerken.

Fragen?