

IPv6-Tunnelbroker leicht gemacht: OpenVPN

40. DFN-Betriebstagung in Berlin

9.3.-10.3.2004

Copyright © 2004 by Christian Strauf



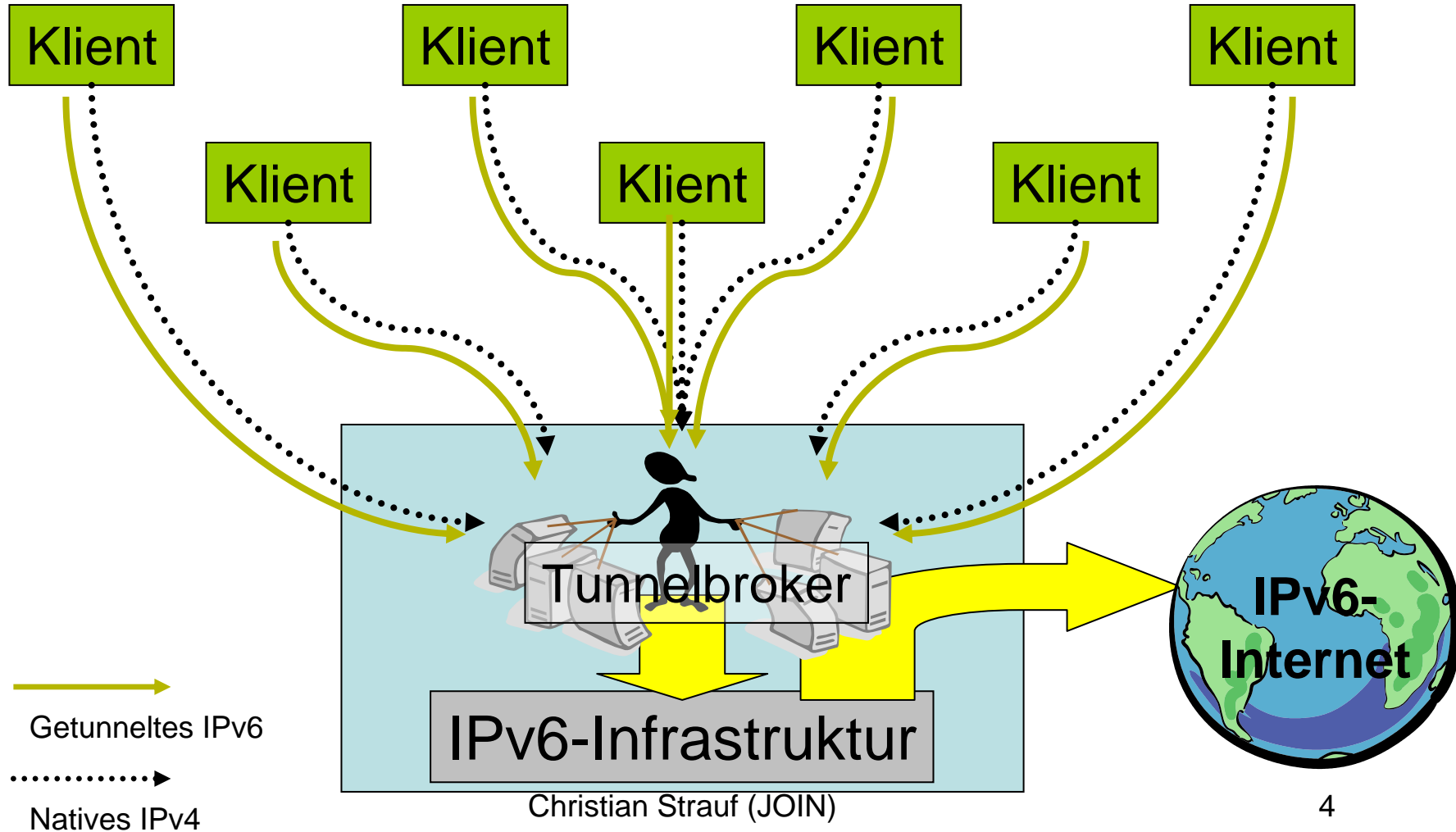
Agenda

- Was ist ein Tunnelbroker?
- Szenarien für Tunnelbroker
- Warum nicht IPsec für Tunnelbroker?
- Was ist OpenVPN?
- Tunnelbroker: Bestandteile
- Exemplarisch: Anbindung eines Kunden
- Tunnelbroker aufbauen
- Tunnelbroker an der WWU Münster

Was ist ein Tunnelbroker?

- Funktionsweise:
 - verwaltet Tunnel-Infrastruktur (Layer2 oder Layer3)
 - regelt ggf. Authentifizierung der Klienten
 - regelt Routing von IPv6 durch Tunnel
- Beispiele für verwendete Tunnel (Auszug):
 - 6in4
 - IPsec
 - OpenVPN

Was ist ein Tunnelbroker? (2)



Szenarien für Tunnelbroker

- Wo verwenden:
 - Anbindung von Professoren, Studenten, Wohnheimen oder WGs über externe Einwahl
 - IPv6-Anbindung von Mitarbeitern an externen Aufenthaltsorten
 - Anbindung nicht nativ erreichbarer Einzelplatzsysteme (nur in Ausnahmen)

Szenarien für Tunnelbroker 2

- Wo nicht verwenden:
 - permanente Anbindung von Instituten oder Arbeitsplätzen über Tunnel (besser: 6in4, falls statische IPv4-Adressen vorhanden)
 - generell: Tunnel zwischen Systemen mit statischen IPv4-Adressen, wo Authentifizierung unnötig ist
- Statische Tunnel != Tunnelbroker

Warum nicht IPsec für Tunnelbroker?

- IPsec läuft nicht im Userspace des OS
- Tiefe Eingriffe auf IP-Stack-Ebene nötig
- Schwierig zu konfigurieren (Client, aber auch VPN-Server)
- Verfügbarkeit über un stabile Verbindungen (WLAN, Modem, ISDN, DSL) schlecht (Verbindungsabbrüche!)

Was ist OpenVPN?

- OpenVPN ist ein OpenSource (GPL) Tunnelmechanismus
- Benutzt freie OpenSSL-Library für:
 - TLS-Key-Exchange
 - Verschlüsselung und Multiplexing in UDP-Streams
 - Bereitstellung von Ciphers und Digest-Funktionen
- Verwendet tun/tap-Treiber des Betriebssystems

Was ist OpenVPN? (2)

- Vorteile:
 - Unterstützt Vielzahl von Betriebssystemen (Windows, Linux, Solaris, BSD, MacOS X)
 - Sichere Authentifizierungsmechanismen
 - Hohe Verfügbarkeit auf instabiler Leitung
 - Läuft im Userspace des OS => keine Beeinflussung anderer Programme im Userspace
 - NAT-Traversierung (!)
 - Leichte Installation und Konfiguration (Client & Server)

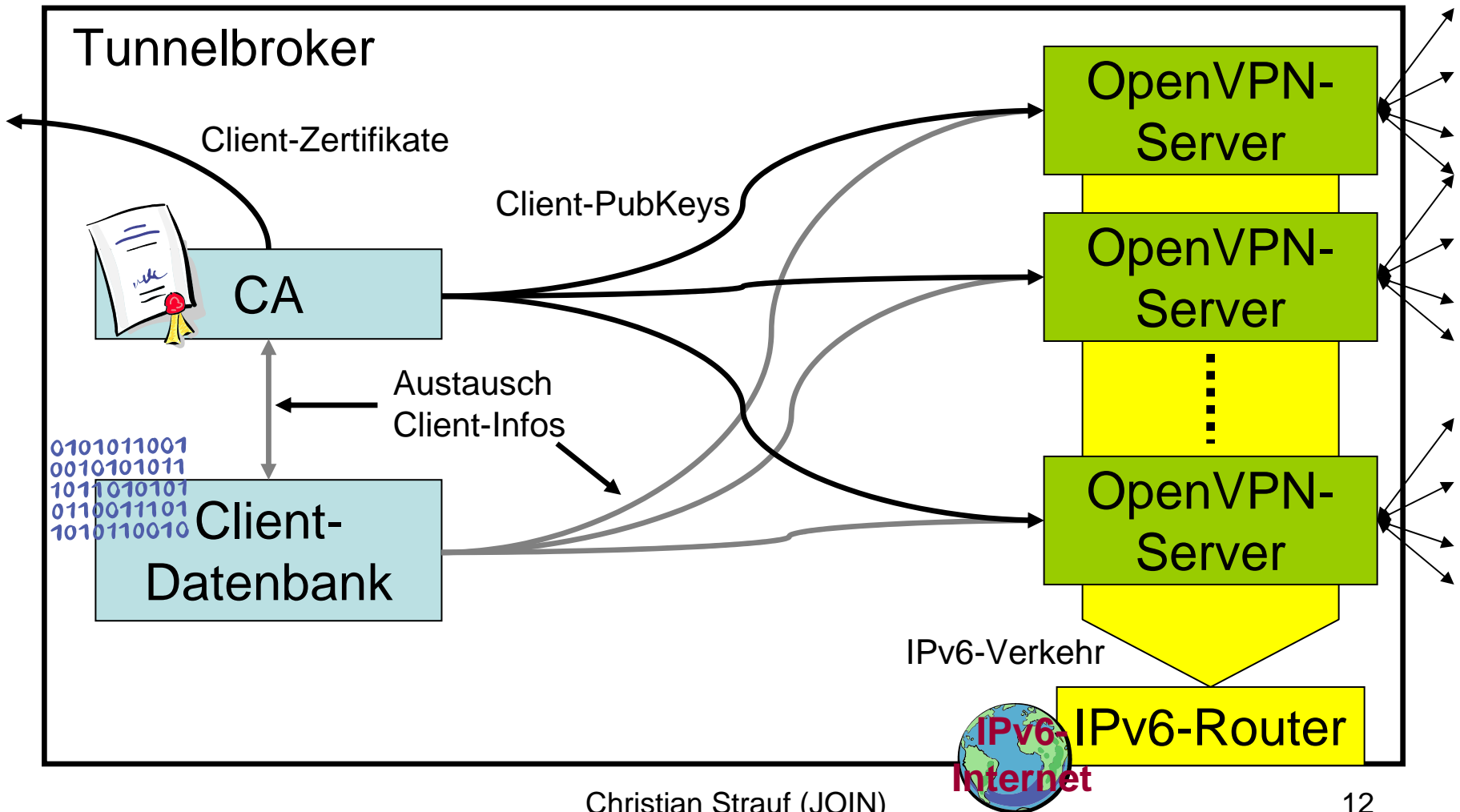
Was ist OpenVPN? (3)

- Vorteile (Forts.):
 - Arbeitet mit OpenSSL PKI zusammen
 - Gute Performanz (Latenz und Bandbreite)
 - IPv6-Unterstützung!
- Nachteile:
 - Standard wird (noch) nicht in Hardware unterstützt
 - Server verbraucht einen UDP-Port pro Client

Tunnelbroker: Bestandteile

- SSL Certification Authority (CA) (erstellt und unterzeichnet Client-Zertifikate)
- OpenVPN-Tunnelbroker-Server (ggf. mehrere)
- Zentrale Verwaltung von Clients (Datenbank)
- Router für Tunnelbroker-Server

Tunnelbroker: Bestandteile (2)

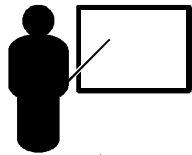


Exemplarisch: Anbindung eines Kunden

- Kunde beantragt Zugang
- Ausstellung eines signierten SSL-Zertifikates für Client nach Überprüfung der Kundenidentität, sowie Client-Konfigurationserstellung
- Automatische Konfigurierung des OpenVPN-Tunnelbroker-Servers
- Kunde installiert OpenVPN-Client und Konfigurationsdateien, die vom Tunnelbroker automatisch generiert wurden

Exemplarisch: Anbindung eines Kunden (2)

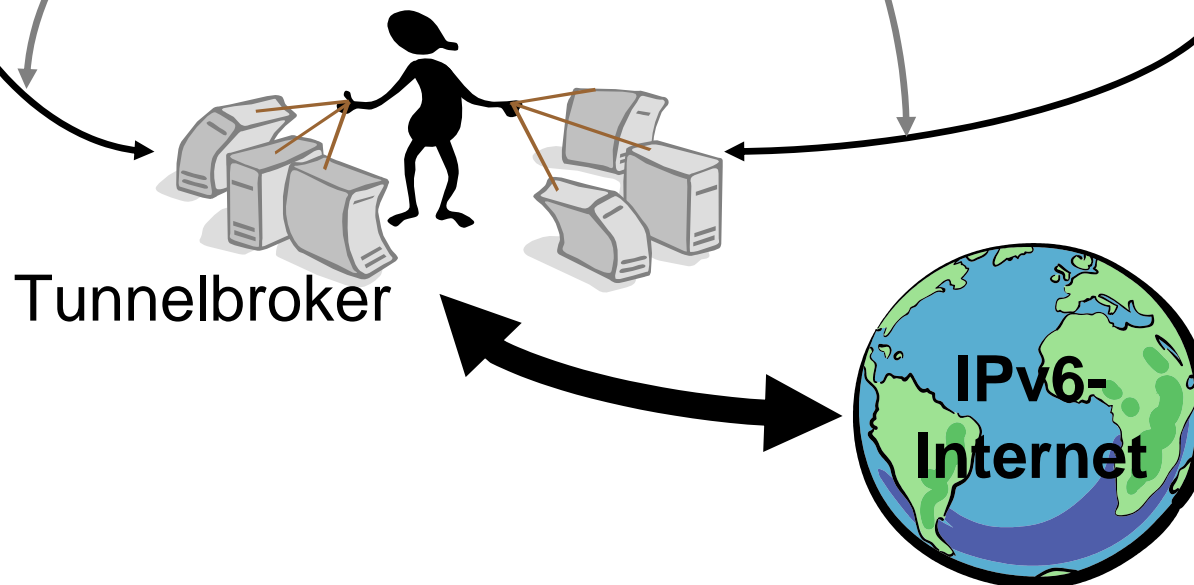
Professor



Studenten



OpenVPN-Tunnel



Exemplarisch: Anbindung eines Kunden (3)



OpenVPN-Tunnel

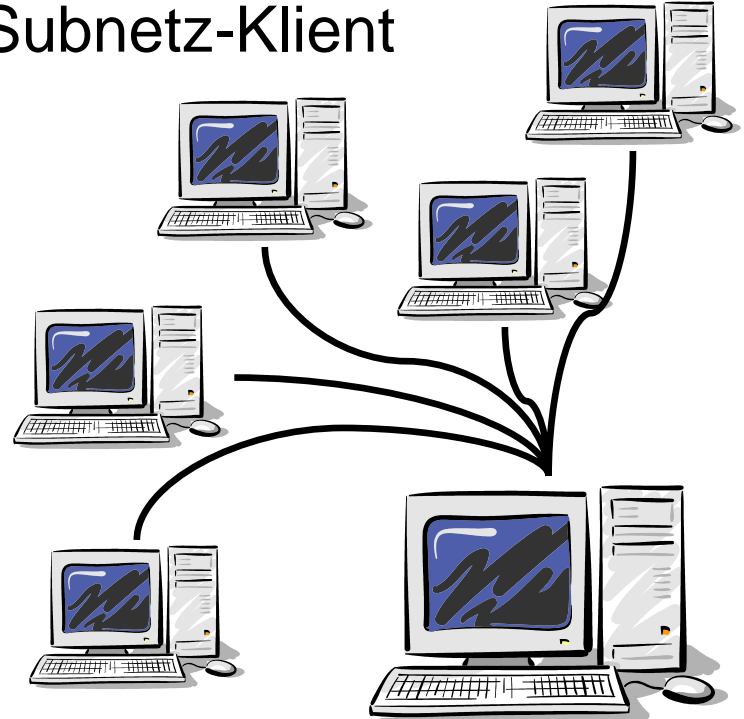
Natives IPv6

Zwei Typen von Klienten:

Einzel-Host-Klient



Subnetz-Klient



Tunnelbroker aufbauen

- Gestaltung der CA je nach Anforderung:
 - skriptbasiert (Beispiele bald auf JOIN-Homepage frei verfügbar)
 - OpenPKI-basiert
- Nutzerdatenbank je nach Anforderung:
 - Textfile
 - LDAP-basiert
 - Datenbank-System (MySQL, Oracle, etc.)

Tunnelbroker aufbauen (2)

- OpenVPN-Tunnelbroker-Server:
 - Beginn mit einer Maschine
 - bei guter Akzeptanz des Services weitere hinzufügen
 - Konfigurationen des Servers über Nutzerdatenbank (jeder Nutzer bekommt eigene Konfiguration & ggf. eigenes Logfile)
 - Benutzung des neuesten OpenVPN-Servers nötig (CVS bzw. bald stabil)

Tunnelbroker aufbauen (3)

- Nutzerdatenbank & CA werden zentral gesteuert und leisten:
 - Zertifikatserstellung für Clients
 - Vergabe der IP-Adressen bzw. -Präfixe
 - Erstellung der Konfiguration für OpenVPN-Server & -Client
 - Ggf. DNS-Einträge für Client-Systeme

Tunnelbroker an der WWU Münster

- Motivation:
 - „Friendly IPv6 Users“ gewinnen (Studenten, Mitarbeiter, Professoren)
 - Instituten und Administratoren Möglichkeit geben, sich mit IPv6 an isolierten Maschinen vertraut zu machen
 - Umgehung von Problemen mit nativer IPv6-Einwahl mit vorhandener Hardware

Tunnelbroker an der WWU Münster (2)

- Per OpenVPN-Tunnel möglicher Service:
 - globale und statische (!) IPv6-Adressen für Einzelrechner und ganze Netze, die sich per OpenVPN verbinden (Studenten-WGs)
 - Feste Eintragung in DNS mit (fast 😊) beliebigen Hostnamen (name.tbv6.uni-muenster.de)
 - Statische IPv6-Adr. & Verbindung überlebt kurze Unterbrechung der v4-Verbindung (z.B. 24h-Disconnect bei T-Online)

Tunnelbroker an der WWU Münster (3)

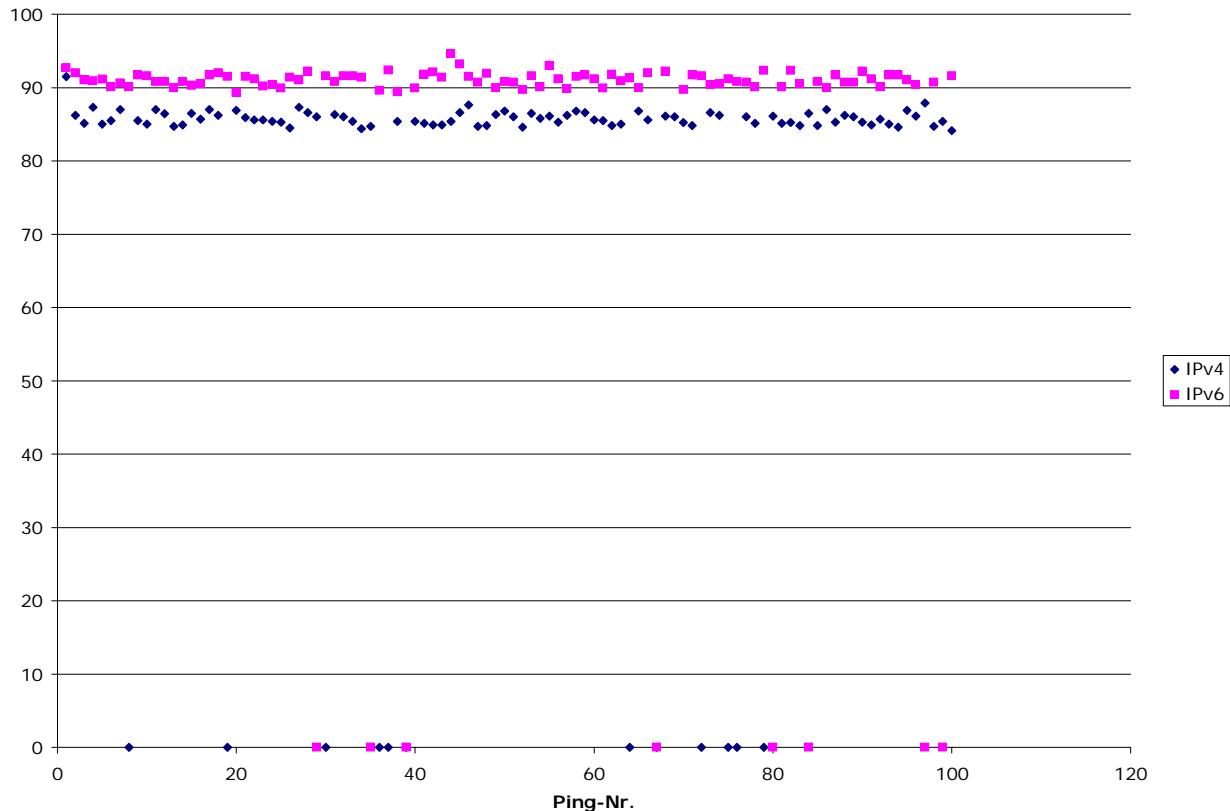
- Tests, die in naher Zukunft von JOIN durchgeführt werden:
 - Stabilität bei vielen simultanen Verbindungen zum Tunnelbroker-Server
 - Skalierbarkeit und Performanz
 - Quantitative Tests zu Jitter, Ping und Bandbreitenverbrauch (Tunnel-Overhead)

Performanzstichprobe

- Aufbau:
 - T-DSL & T-Online über Hardware-DSL-Router (Linksys WRT54G)
 - OpenVPN-Client hinter DSL-Router
 - OpenVPN-Server & Router im JOIN-Netz
 - Ping (IPv4 & IPv6) auf dual-stack Host im JOIN-Netz
 - **Achtung:** Pingtests erfolgten nicht zeitgleich, Graphen dienen nur zum Vergleich der Größenordnungen der Ping-Zeiten!

Performanzstichprobe (2)

Größenordnung der Ping-Zeiten IPv4 / IPv6 über OpenVPN
(nicht zeitgleich gemessen!)



Debugging-Hilfe

Shell-Skript
mit Sanity-
Checks zur
Unterstützung
der User:

```
Terminal — ssh — 89x51
[gargoyle:~] # /etc/openvpn/join-openvpn-sanity-check.sh

JOIN OpenVPN Tunnelbroker Client Sanity Check      Version 0.3
-----
Copyright (C) 2004 by Christian Strauf <strauf@uni-muenster.de>
                                <join@uni-muenster.de>
                                http://www.join.uni-muenster.de

Please note: this script only works for a Linux OpenVPN Client
            that announces a /64 prefix to a local subnet.

Checking existence of a configuration file... OK
Checking client ID... (christian.strauf) OK
Checking existence and executability of up-script... OK
Checking existence of SSL certificate... OK
Checking existence of SSL key... OK
Checking permissions of SSL key... OK
Checking existence and executability of tls-verify script... OK
Checking existence of CA certificate... OK
Checking reachability of tunnelbroker over IPv4... OK
Checking IPv6 connectivity to ftp.ipv6.join.uni-muenster.de... OK
Checking if OpenVPN is running... OK
Checking that OpenVPN port is not occupied by other app... OK
Checking presence of "sysctl"... OK
Checking presence of "ip"... OK
Checking if IPv6 packet forwarding is enabled... OK
Checking if correct address+prefix has been configured for eth0... OK
Checking if tunnel device has correct IPv6 address... OK
Checking that there is only one IPv6 default route... OK
Checking default route is via tunnel device... OK
Checking for tun driver support in kernel... OK
Checking for IPv6 support in kernel ;-)... OK

System infos:
-----
Kernel:      Linux 2.6.3-gentoo-r1 #1 SMP Fri Feb 20 15:08:52 CET 2004
Hardware:    i686 AMD Athlon(tm) Processor AuthenticAMD
OS:          GNU/Linux
OpenVPN version:
  OpenVPN 1.6_beta1 i686-pc-linux-gnu [SSL] [LZO] built on Jan 29 2004
  Copyright (C) 2002-2004 James Yonan <jim@yonan.net>
ip tool version: ip utility, iproute2-ss010824

Test summary:
-----
No. of tests: 21
PASSED tests: 21
FAILED tests: 0
SKIPPED tests: 0

[gargoyle:~] #
```


Fazit

- Gewinnung von Studenten für IPv6-Einsatz wichtig (innovative Ideen, Umgang mit dem IP der Zukunft); wird durch OpenVPN-Tunnelbroker gefördert
- OpenVPN-Tunnelbroker geeignete Migrations-/Transitionsmethode für Einwahlsysteme mit geringem Konfigurations- & Kostenaufwand

Zukunft

- Tests von Multicast über OpenVPN-Tunnel
 - pim6sd für Linux wird benötigt
- Tests für Präfix-Delegation mit DHCPv6

Links

- OpenVPN-Homepage:
<http://openvpn.sourceforge.net>
- JOIN-Homepage:
<http://www.join.uni-muenster.de>



Fragen?

Danke für Ihre Aufmerksamkeit!

Christian Strauf

Kontakt:

strauf@uni-muenster.de

join@uni-muenster.de

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