IPv6-Tunnelbroker leicht gemacht: OpenVPN

40. DFN-Betriebstagung in Berlin

9.3.-10.3.2004

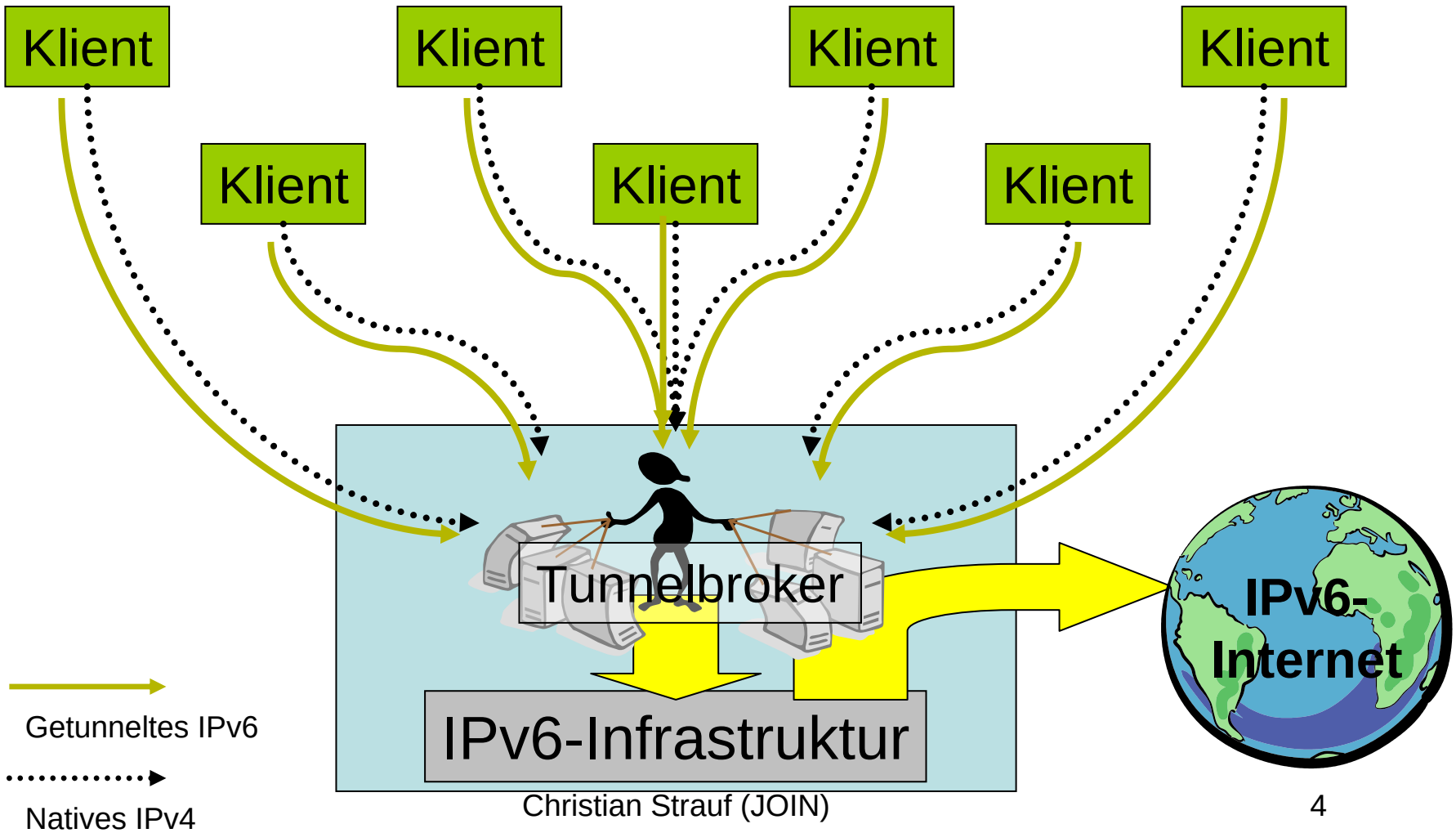
Agenda

- 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 unstabile 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 => kein Beeinflussung anderer Programme im Userspace
  - NAT-Traversierung (!)
  - Leichte Installation und Konfiguration (Client & Server)

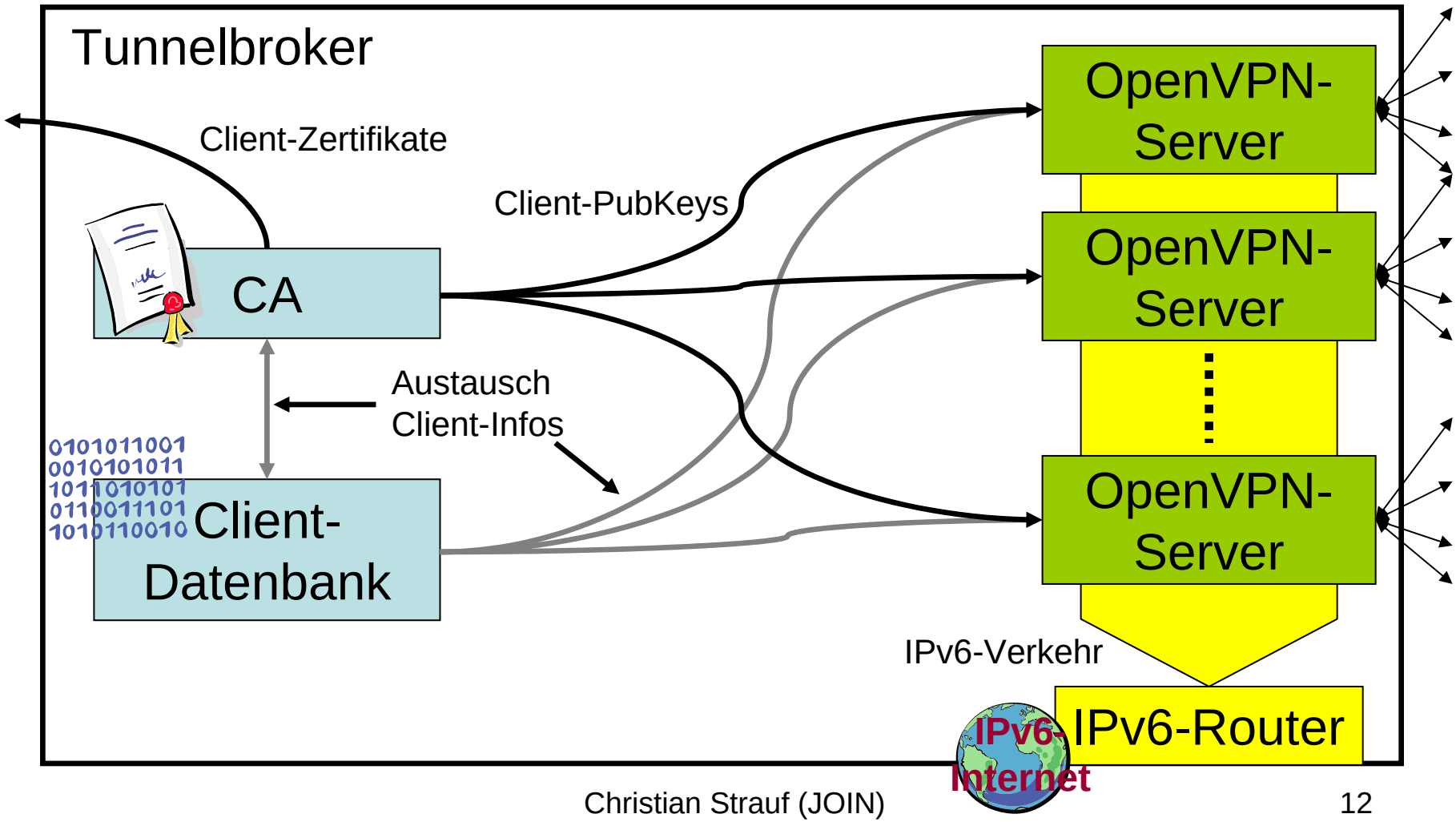
Was ist OpenVPN? (3)

- 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

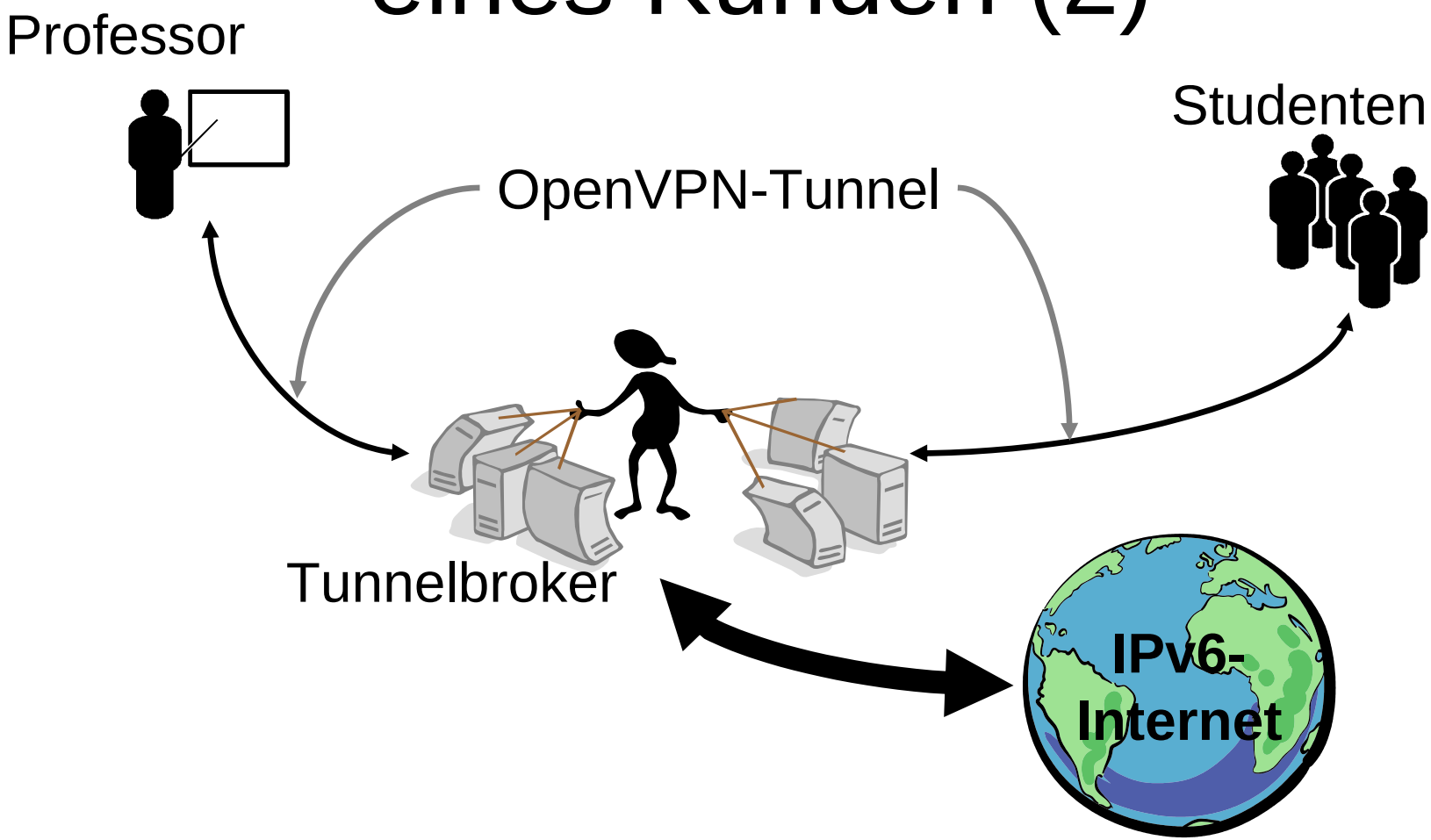
Tunnelbroker: Bestandteile (2)



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)



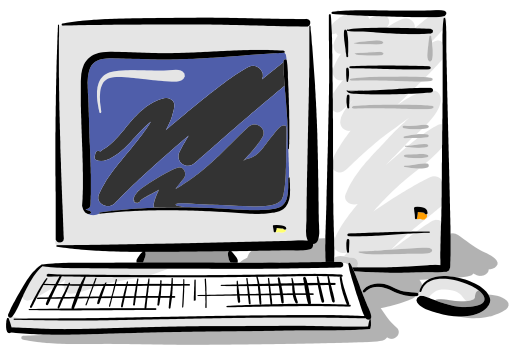
Exemplarisch: Anbindung eines Kunden (3)

OpenVPN-Tunnel

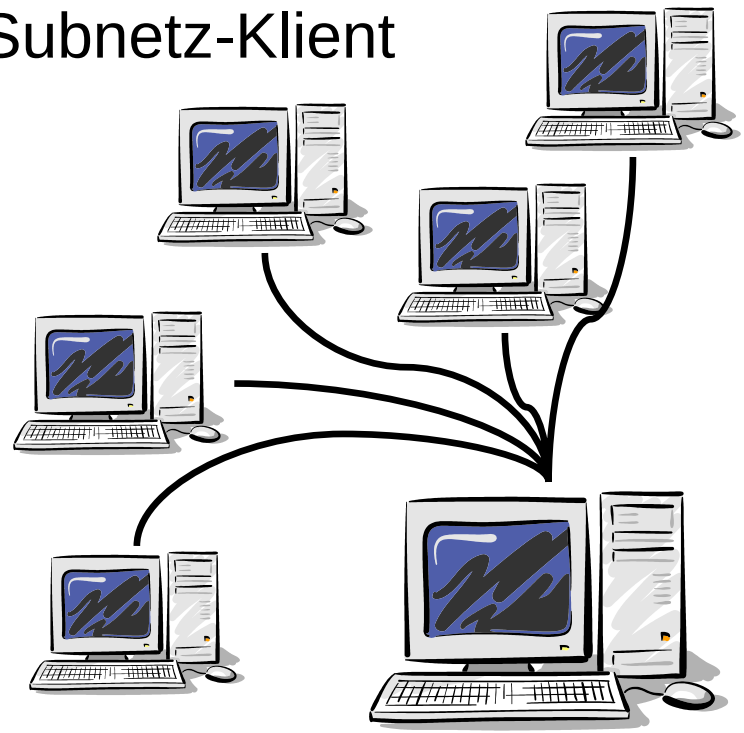
Natives IPv6

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)

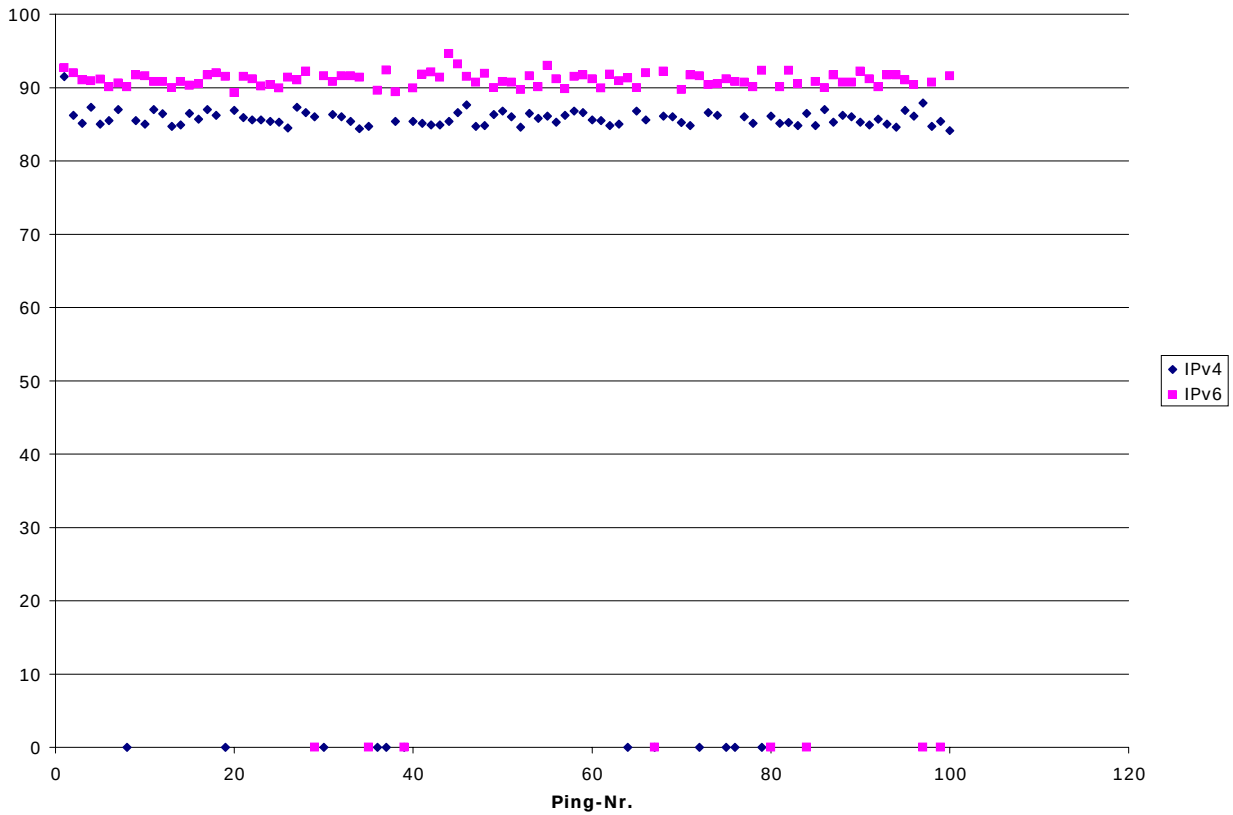
- Tests, die in naher Zukunft von JOIN durchgeführt werden:
  - Stabilität bei vielen simultanen Verbindungen zum Tunnelbroker-Server
  - Skalierbarkeit und Performanz
  - Quantitative Tests zu Jitter, Ping und Bandbreitenverbrauch (Tunnel-Overhead)

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:

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