

**Warum wir an der Universität
der Bundeswehr München IPv6
noch nicht eingeführt haben**



Über mich

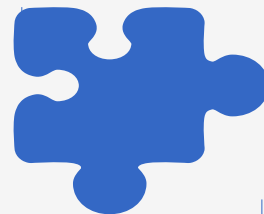
Dan Luedtke

B. Eng. Elektrotechnik
und technische Informatik



IT-Sicherheit, Netzwerke,
IPv6, OS-Entwicklung

Studentische Hilfskraft
im Rechenzentrum



www.danrl.de



Die Universität

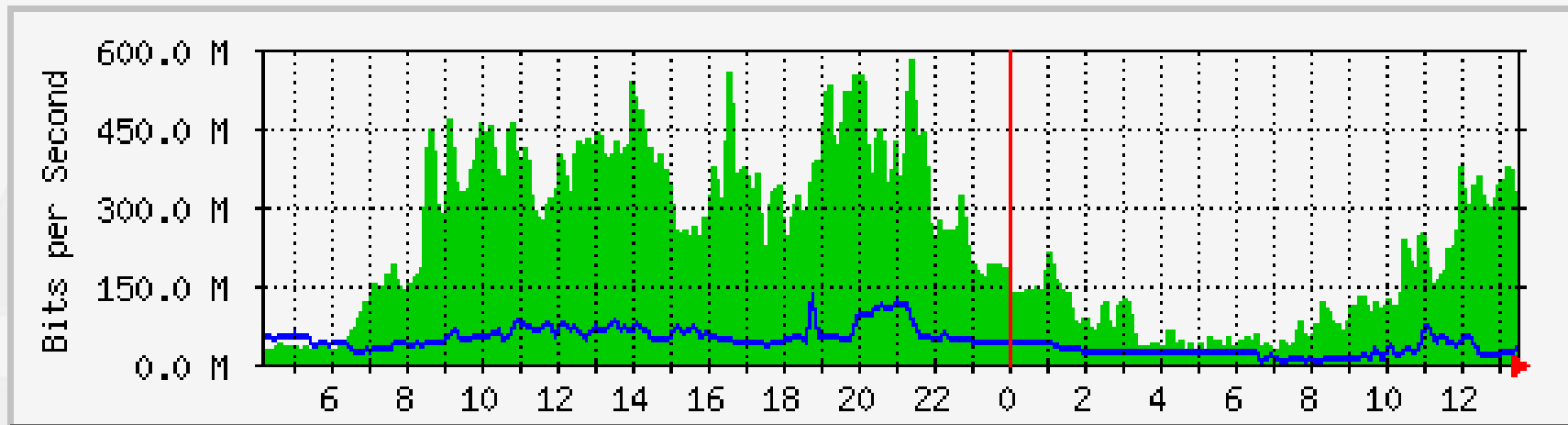
- Campus-Universität, gegründet 1973
- Dient der wissenschaftlichen Ausbildung von Offizieren und Offizieranwärtern
- ca. 3700 Studenten Stand: 2011
 - $\frac{3}{4}$ wohnen auf dem Campus
 - am HDN angeschlossen
- Mitglied im DFN-Verein
 - Upstream-Provider



Luftbild vom Campus UniBwM
Quelle: UniBwM Pressearchiv

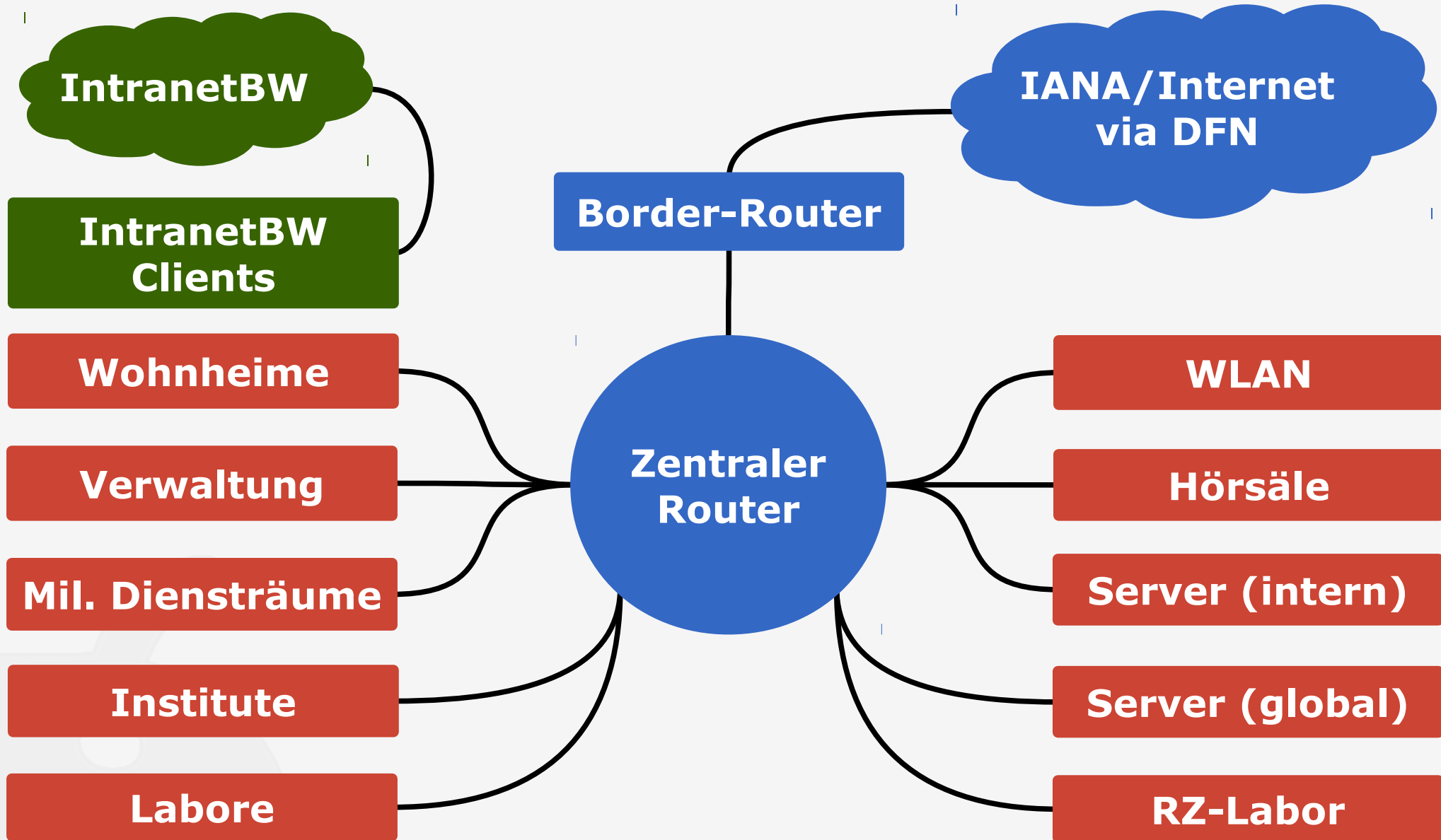
Hochschuldatennetz

- 272 Switches, überwiegend Edge-Switches
- 137.193.0.0/16
- 2001:638:103::/48
- >9000 Endsysteme

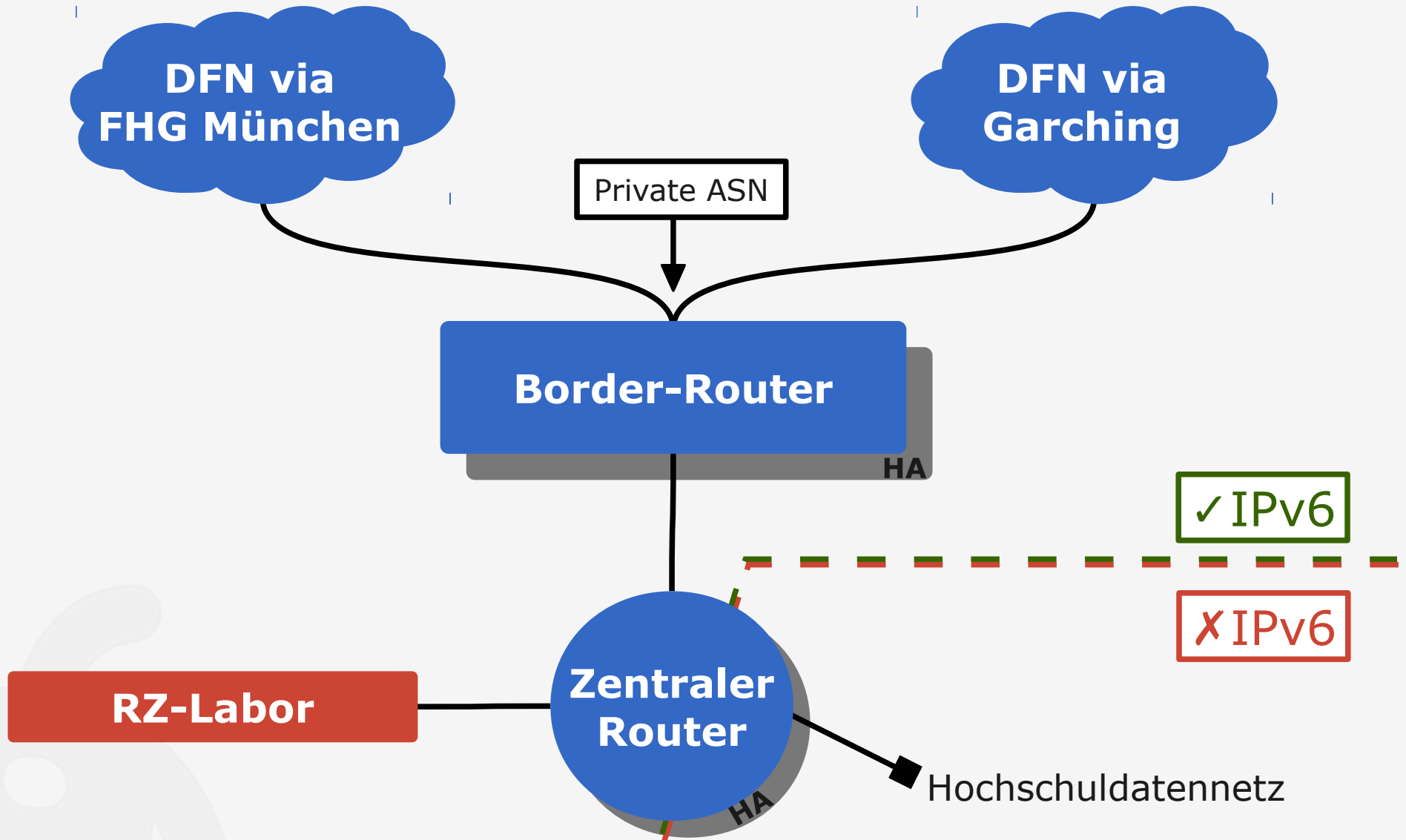


Datendurchsatz Upstream, typ. Bsp.
Quelle: UniBwM RZ NetMan

Netzzonen (vereinfacht)



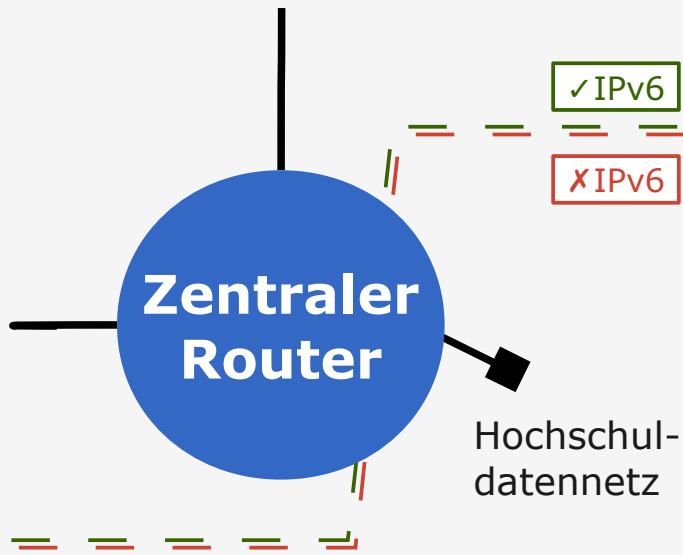
Border Link, RZ-Labor



FHG Fraunhofer Gesellschaft

HA High Availability

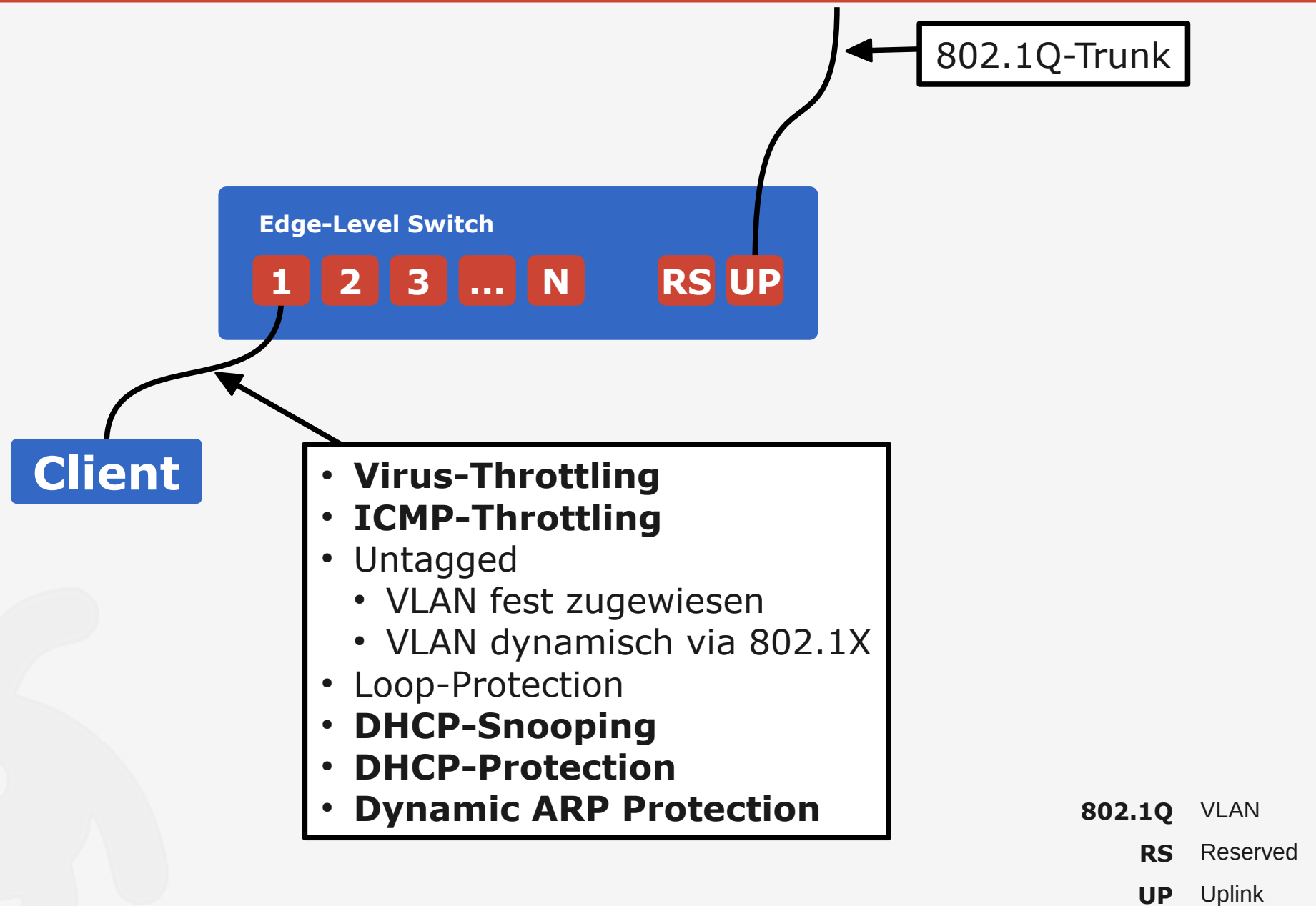
Zentraler Router



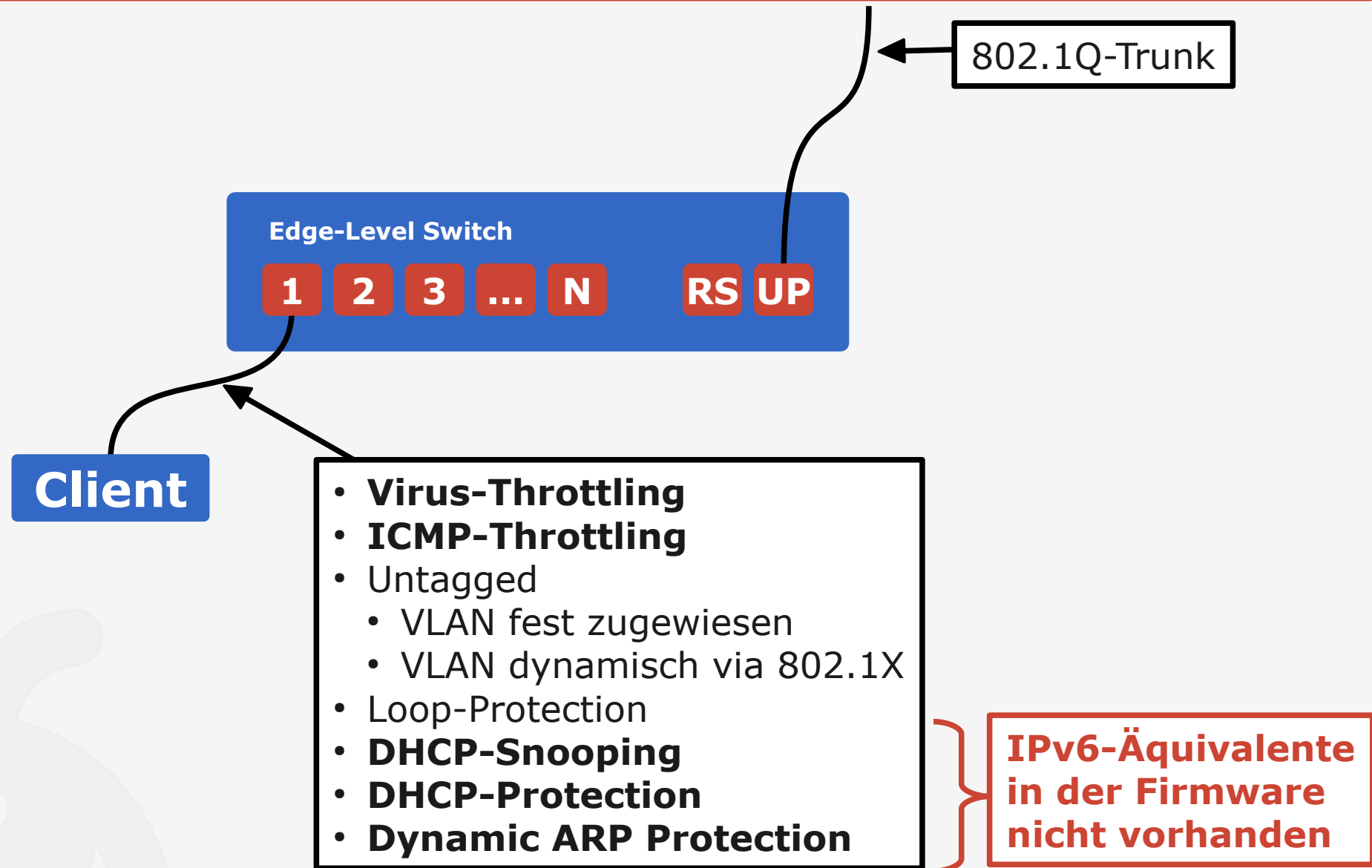
- IPv6-fähig
- IPv6 belastet die CPU stärker
- IPv6 entlastet die ASICs 😊
- Einige IPv4-Features gehen bei Nutzung von IPv6 verloren
- Austausch absehbar

ASIC anwendungsspezifische integrierte Schaltung

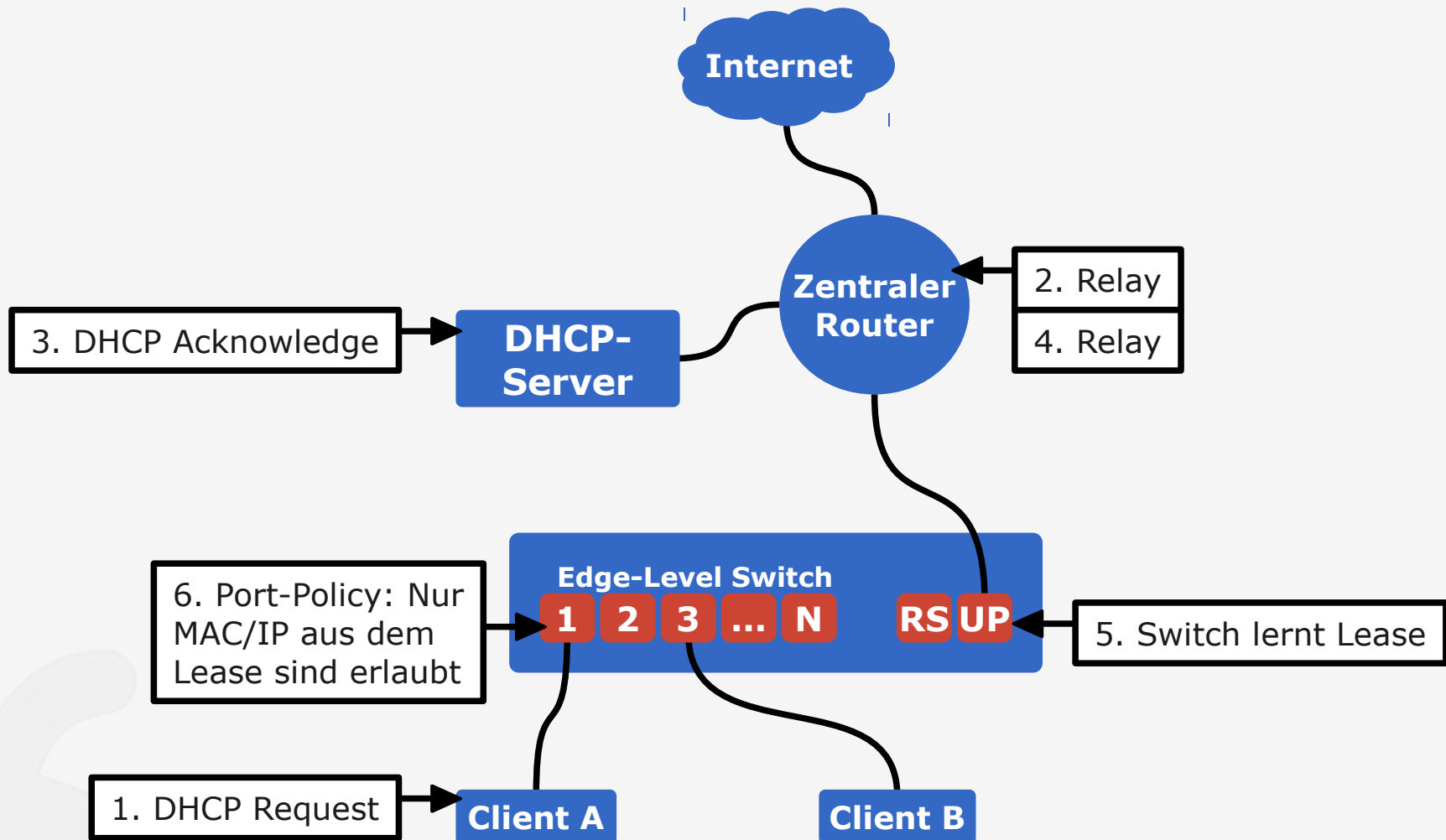
Edge-Level Sicherheit



Edge-Level Sicherheit

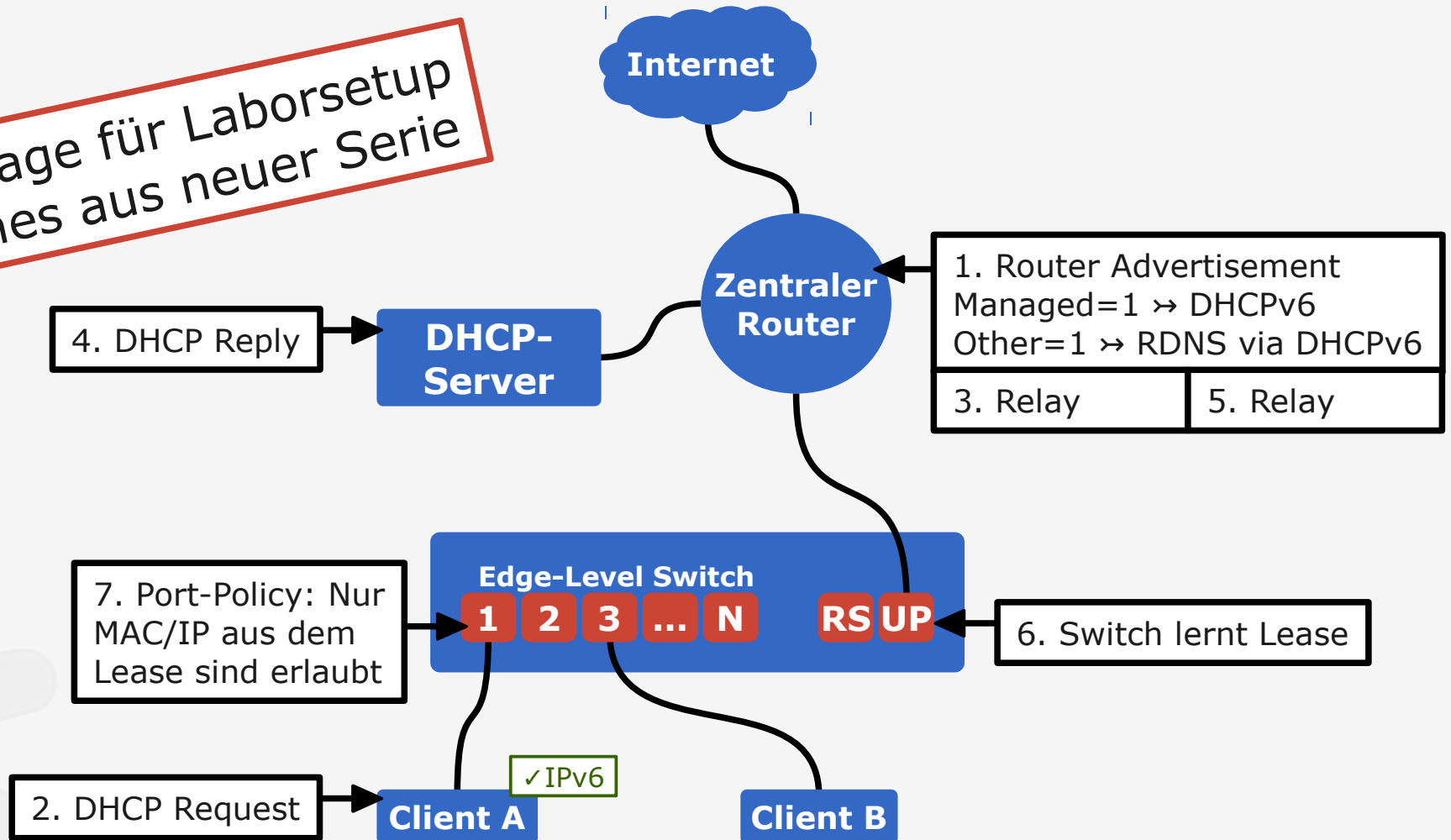


IPv4-Konnektivität herstellen



IPv6-Konnektivität herstellen

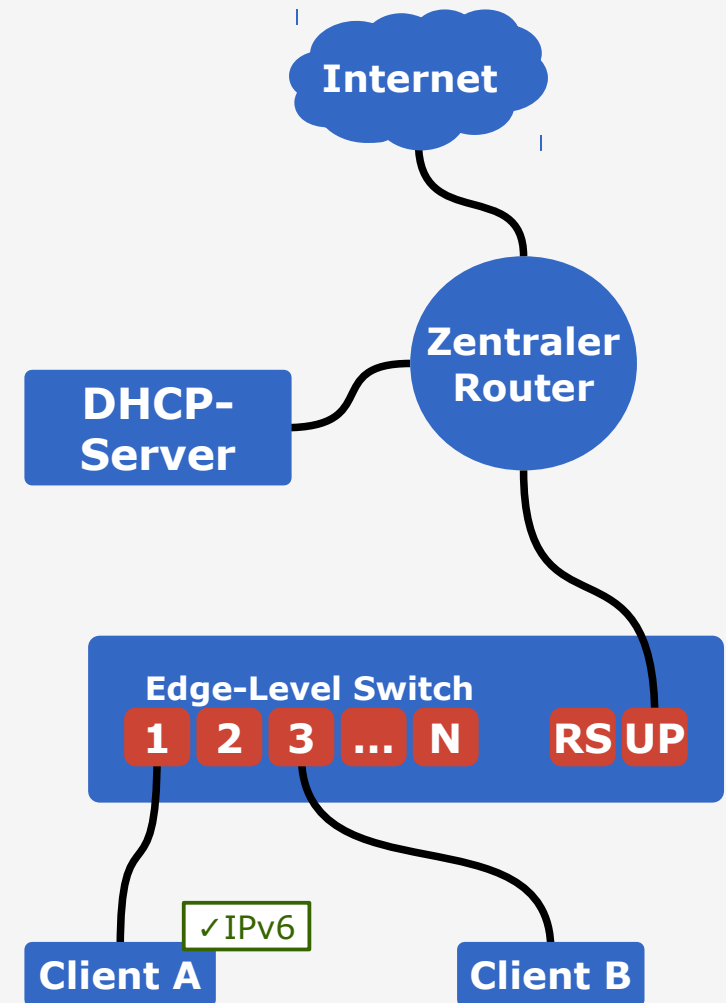
Grundlage für Laborsetup
Switches aus neuer Serie



RDNS Resolving Nameserver

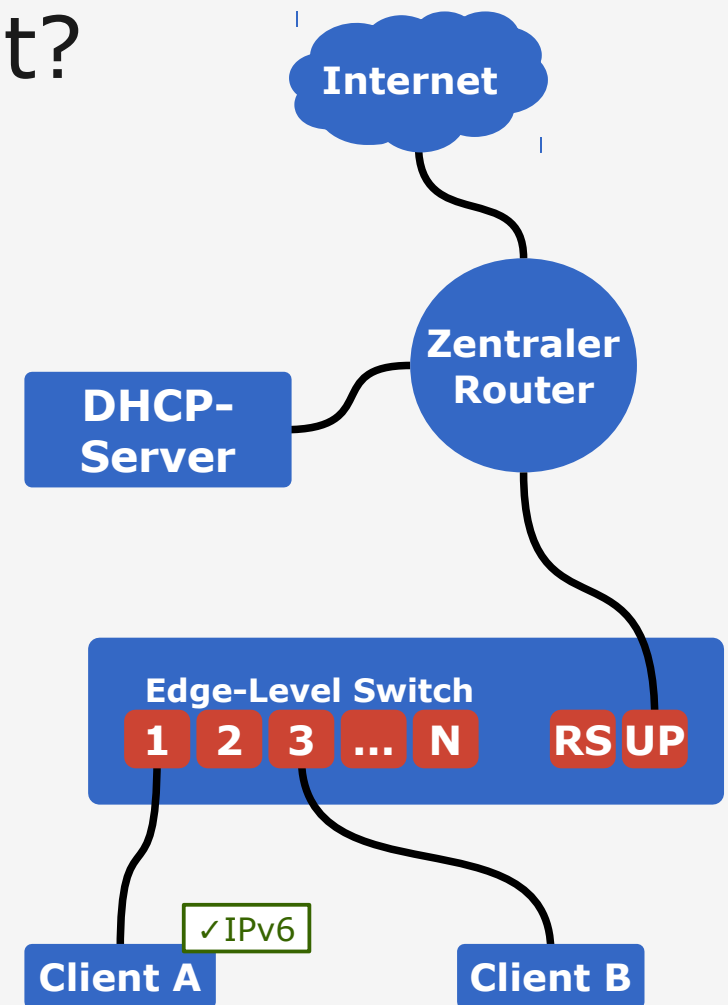
Probleme

- Manche Betriebssysteme beherrschen kein DHCPv6
- Manche Betriebssysteme ignorieren das Other-Flag
- Unsere Switches können DHCPv6-Snooping etc. (noch) nicht!
- Austausch der Switches aus Kostengründen derzeit nicht möglich



Offene Fragen (Edge-Level)

- Privacy Extensions am Client?
- Aufwand und Nutzen der DUID-Verwaltung?
- Relay einsparen?
 - site-local multicast
 - ff05::1:3 All-dhcp-servers RFC3315



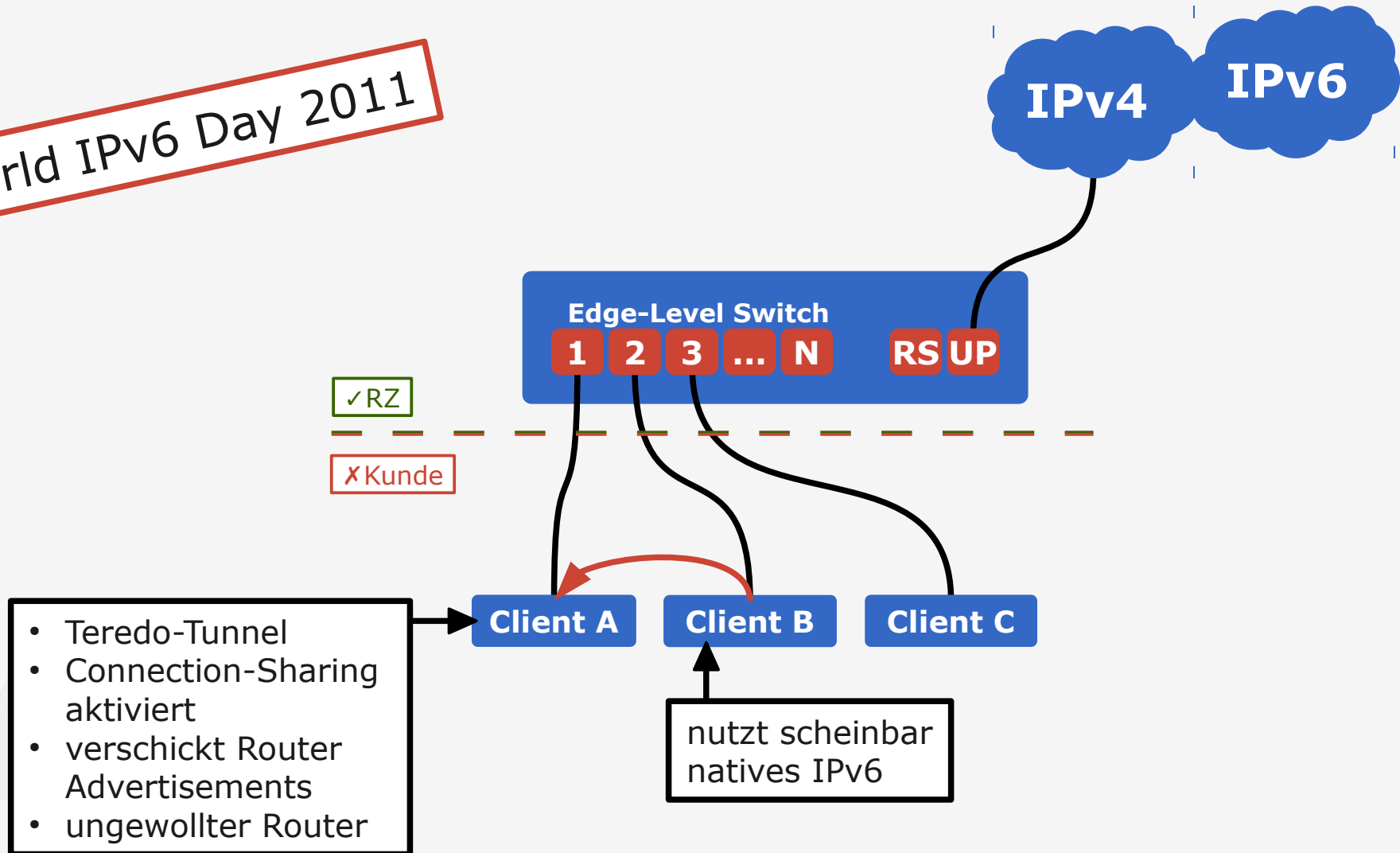
DUID DHCP Unique Identifier

Probleme ohne IPv6

- gesunkene Kundenzufriedenheit
- Kunden finden *workarounds*
 - Teredo (z.T. automatisch)
 - Tunnelbroker
- Getunnelter Verkehr entzieht sich unserer "Kontrolle"!
 - Wir lassen nicht jeden tunneln 😊

Probleme ohne IPv6 (Bsp.)

World IPv6 Day 2011



Offene Punkte

- **Kein IPv6 ist keine Lösung!**
- Wo wäre eine zentrale Adressvergabe sinnvoll?
 - Server
 - verwaltete Systeme
- Wo wäre die Nutzung von SLAAC statt DHCPv6 sinnvoll?
 - Wohnbereiche
 - Wireless
 - *Bring-Your-Own-Device*-Netze
- Kann uns OpenFlow weiterhelfen?
- Wollen und können wir Kunden eigene Netze geben?
 - Layer-2 → ISP
- Gibt es einen Konflikt zwischen Privacy Extensions und Sicherheit?
 - Falls ja, wie lösen wir diesen?

Lösungsvorschlag BYOD-Netze

- Router Advertisements
 - mit RDNS-Option
- SLAAC
- Neighbor Discovery Snooping
- Neighbor Discovery Detection
- Erweitertes Logfile
 - Zeitstempel
 - IPv6-Adresse
 - Switchport

BYOD Bring-Your-Own-Device

SLAAC Stateless Address Autoconfiguration

Fragen?

**Vielen Dank für Ihre
geschätzte Aufmerksamkeit!**

Quellen

- RFC 2675, 5095, 3122, 4443, 4884, 4007, 2460, 5942
- Netzkonzept für die UniBwM ab 2008; Winfried Thalmeier (CSO)
- IT-Sicherheitsstrategie an der UniBwM; 2008; Winfried Thalmeier (CSO)
- Projektstudie IPv6 im Hochschuldatennetz; 2011; Dan Luedtke
- IPv6 Border-Link and Edge-Level Packet Filtering; 2011; Dan Luedtke

IN EIGENER SACHE

AS57821 is looking for peers!
www.nonattached.net