



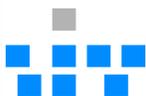
DHCPv6

Copyright © 2003 by

Christian Strauf (JOIN)

<strauf@uni-muenster.de>

39. Betriebstagung des DFN in Berlin
11.-12. November 2003



ZENTRUM FÜR
INFORMATIONEN
VERARBEITUNG



Westfälische Wilhelms-
Universität Münster



Agenda

- Die Welt ohne DHCPv6: IPv6 Stateless Address Autoconfiguration
- DHCPv6-Spezifikation
- Funktionsweise
- Betriebsszenarien
- Weitere Optionen
- DHCPv6 – mit oder ohne SAA?
- Sicherheit von DHCPv6
- Die Zukunft mit DHCPv6

Die Welt ohne DHCPv6: IPv6 Stateless Address Autoconfiguration

- Kurz: **SAA**; benutzt Router Advertisements (RA)
- Definiert in **RFC 2462**

Was funktioniert mit **SAA**?

- IP aus RA (keine Adresszuweisung!)
- Default-Router durch RA

Was funktioniert nicht mit **SAA**?

- DNS-/NTP-Server-Ermittlung
- Beeinflussung der Adressvergabe
- Zentrale Verwaltung von IPv6-Adressen
- Präfix-Delegation

Kleines
Netzwerk

Manuelle
Präfix-
Delegation

SAA
ausreichend!

Struktur des
Routings einfach

Adress-Auto-
konfiguration

Keine Beeinflussung
der IPv6-Adressen-
Vergabe nötig

Manuelle DNS-
Konfiguration

Manuelle NTP-
Server-Konfiguration

- Erweiterungen von SAA (exemplarische Drafts):

DNS-Discovery

draft-jeong-dnsop-ipv6-dns-discovery-00.txt
(„IPv6 DNS Discovery based on Router Advertisement“)

draft-beloeil-ipv6-dns-resolver-option-01.txt
(„IPv6 Router Advertisement DNS resolver Option“)

Dynamische
DNS-Konfiguration
aus RA

draft-jeong-ipv6-ra-dns-autoconf-00.txt
(„IPv6 Router Advertisement based DNS Autoconfiguration“)

Mehr Möglichkeiten
der
Host-Konfiguration



DHCPv6

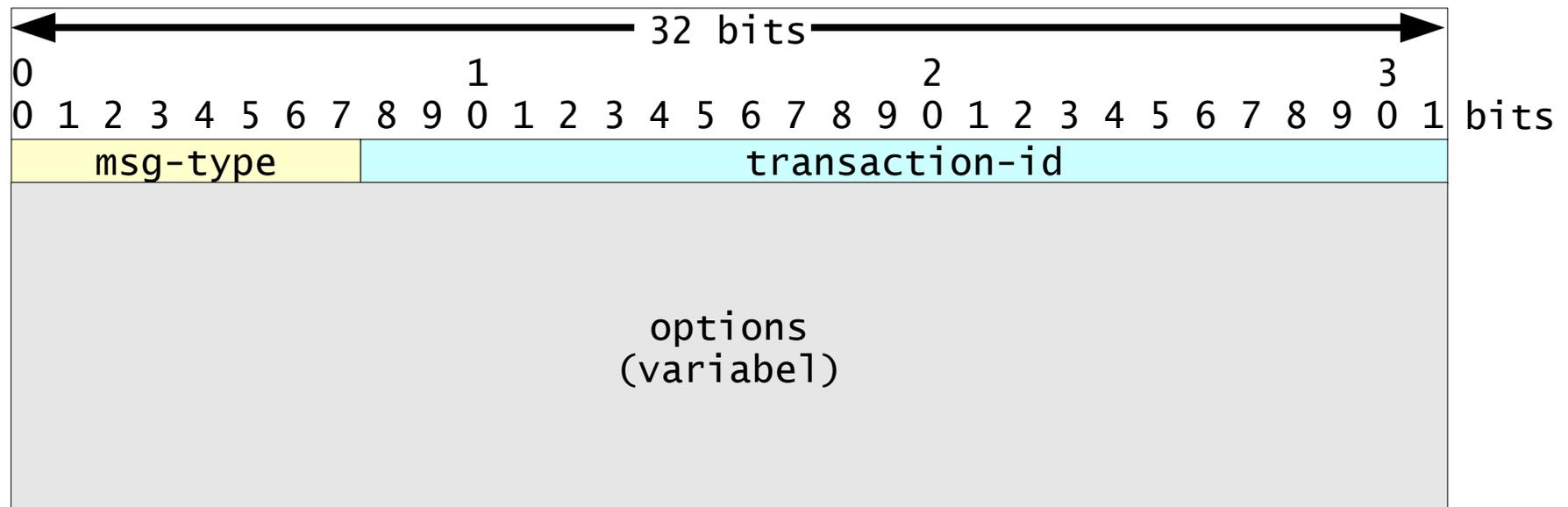
DHCPv6-Spezifikation

- Formale Definition: **RFC 3315** & darauf folgende Drafts/RFCs
- Wesentliche Aufgaben:
 - Adressvergabe
 - Präfix-Delegation (Präfixe für Announcements können an Router übermittelt werden)
 - DNS- und NTP-Server-Adressübermittlung
 - Temporäre Adresszuweisung (Adressen wie in RFC 3041)
 - Dynamische DNS-Updates

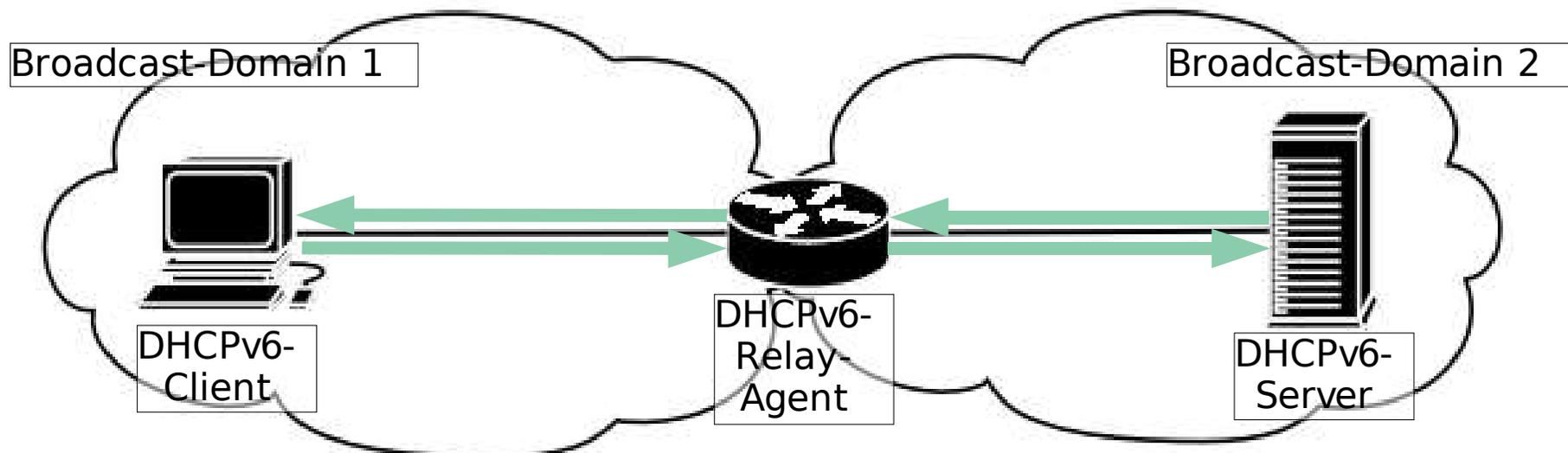
DHCPv6-Funktionsweise

- Verwendet UDP/IPv6, Ports 546 & 547
- Pakete über Link-Local- & Site-Local-Multicast-Adressen:
 - ff02::1:2 (Alle DHCP-Relay-Agents & -Server; link-local)
 - ff05::1:3 (Alle DHCP-Server; site-local)
- Ggf. Unicast-Verwendung

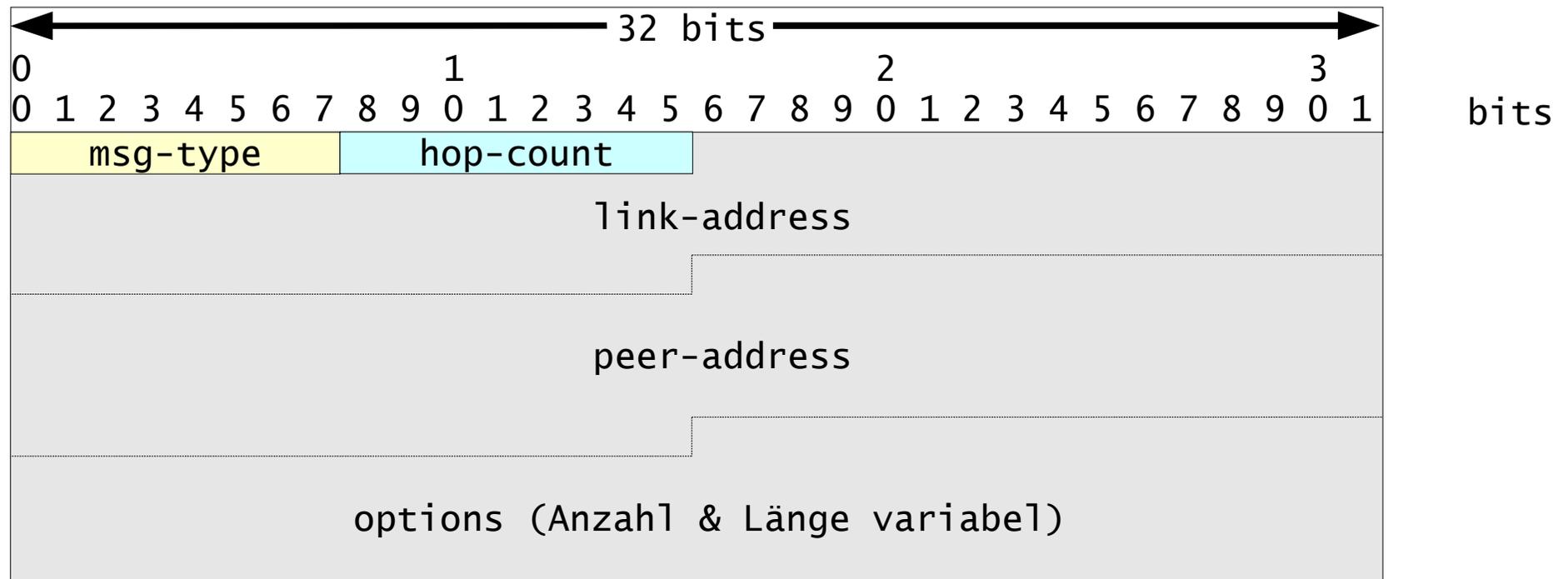
- DHCPv6-Paket (Server & Client):



- DHCPv6-Relay-Agents:
 - Aufgabe: DHCPv6-Messages zwischen Clients und Servern auf unterschiedlichen Links weiterleiten (mehrere Hops möglich):



- DHCPv6-Paket (Relay-Agent):



msg-type: RELAY-FORW

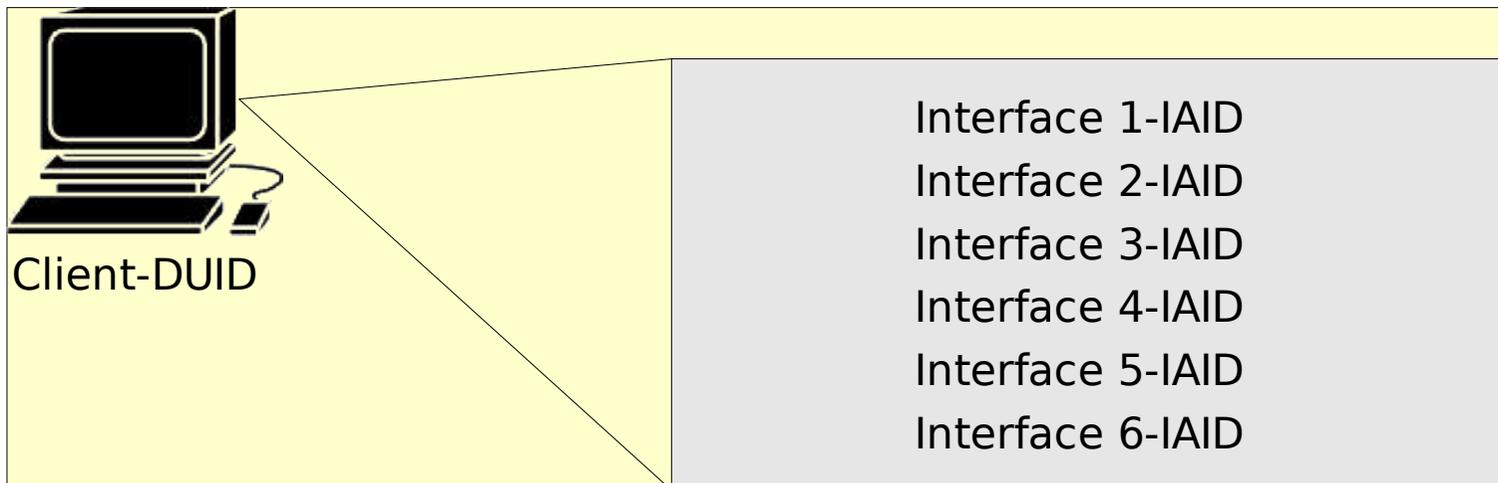
hop-count: #-Hops über Relay-Agents

link-address: Globale oder site-local Adresse zur Link-Identifizierung

peer-address: Adresse des Senders

- Identifizierung von DHCPv6-Clients/-Server:
 - früher: MAC-Adresse
 - heute: DUID + IAID(s)
- DUID = DHCP Unique Identifier
 - identifiziert Server und Clients
 - eindeutig
 - sollte sich nicht ändern
 - keine Änderung bei Austausch von Netzwerkkomponenten!

- IAID = Identity Association Identifier:
 - mindestens eine pro Interface
 - vom Client generiert
 - unverändert bei Neustarts des DHCP-Clients

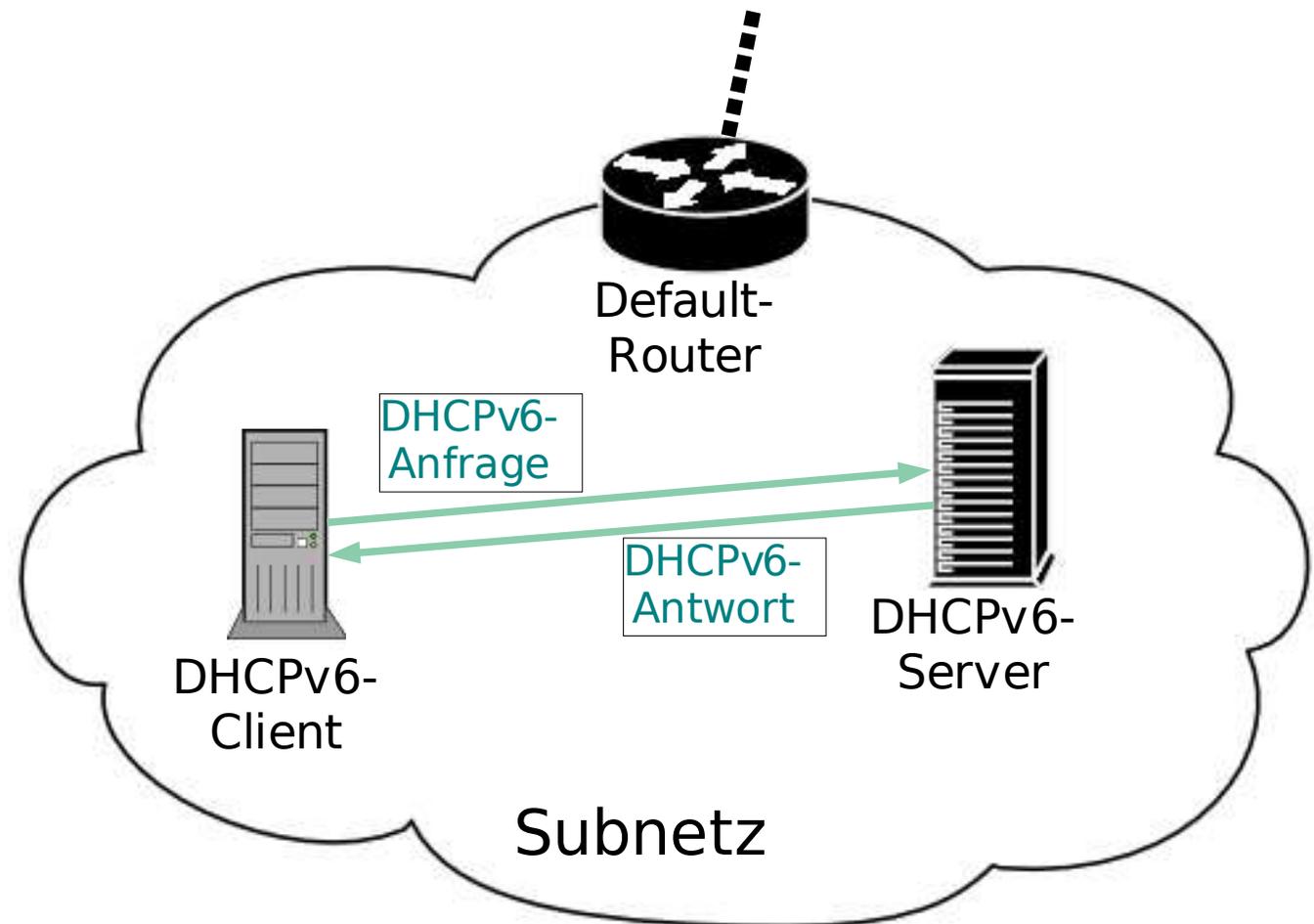


DHCPv6-Betriebsszenarien

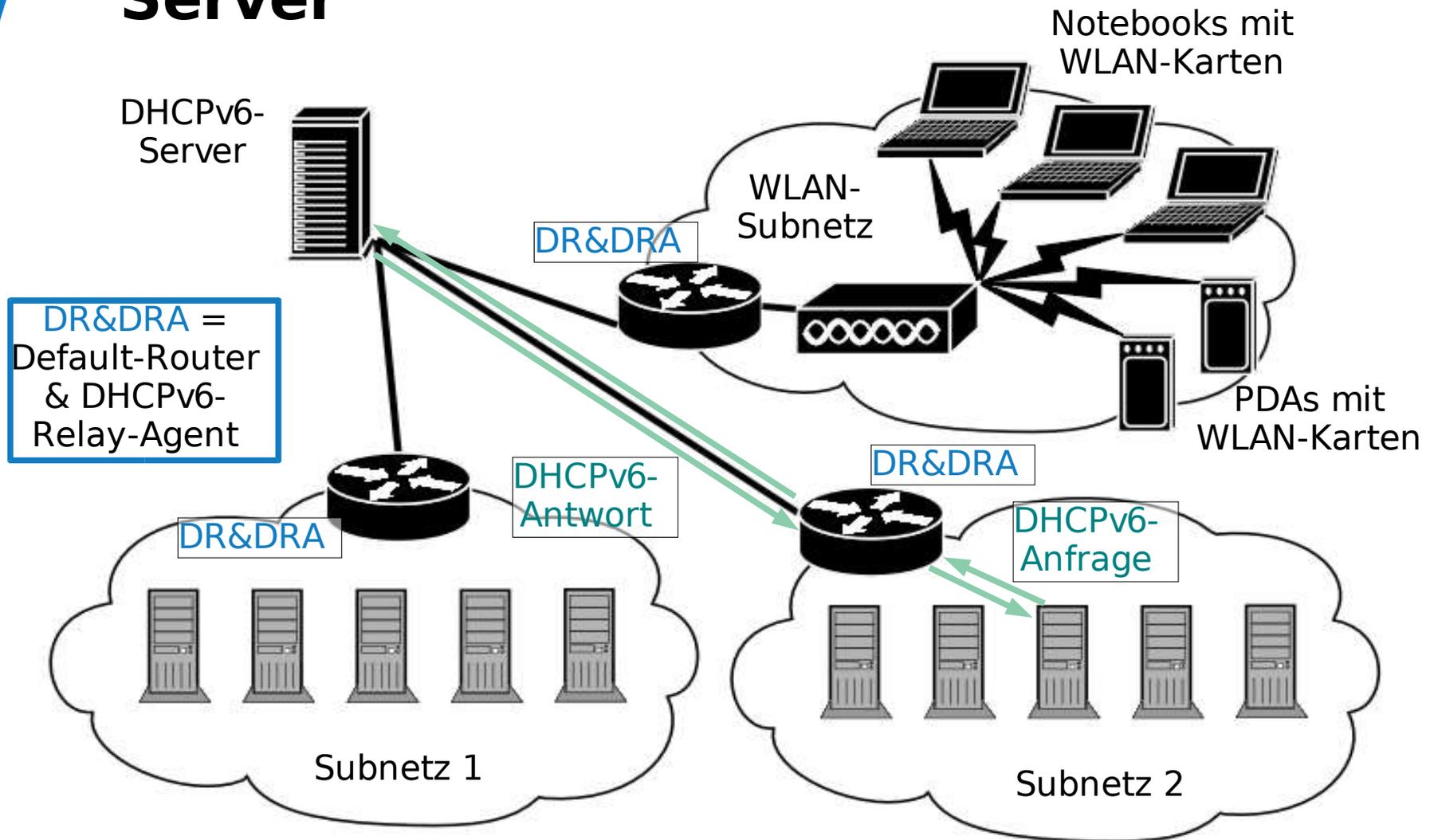
- Szenario 1: ein Subnetz & ein DHCPv6-Server
- Szenario 2: mehrere Subnetze & ein DHCPv6-Server
- Szenario 3: mehrere Subnetze & mehrere DHCPv6-Server
- (Szenario 4: ein Subnetz & mehrere DHCPv6-Server – siehe Szenario 3)

Szenario 1: Einzelnes Subnetz

- DHCPv6-Server & -Clients in derselben Broadcast-Domain (per Link-Local zu pinggen)
- Kein DHCPv6-Relay-Agent nötig



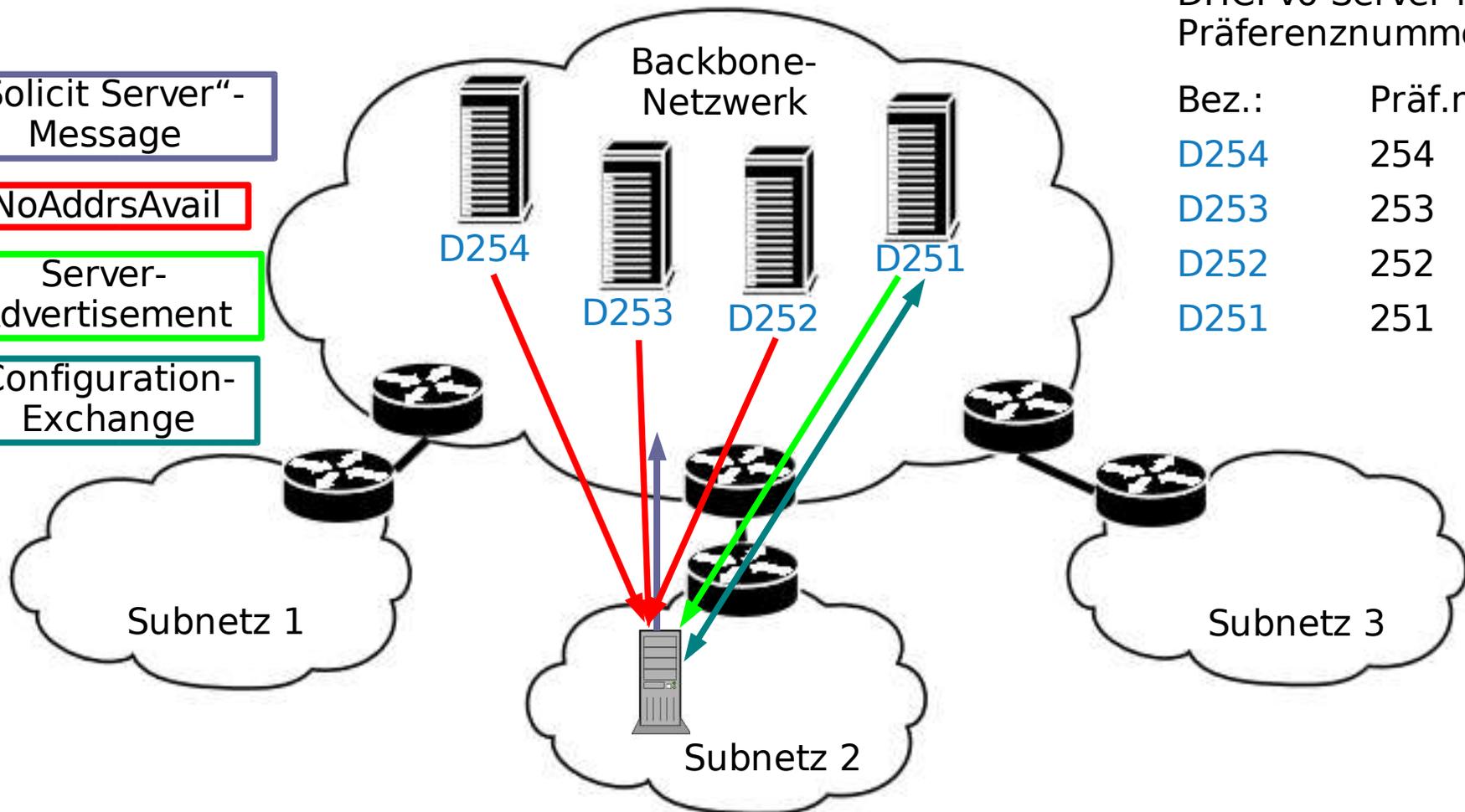
Szenario 2: Mehrere Subnetze, ein DHCPv6-Server



Szenario 3: Mehrere Subnetze, mehrere DHCPv6-Server



- „Solicit Server“-Message
- NoAdrrsAvail
- Server-Advertisement
- Configuration-Exchange

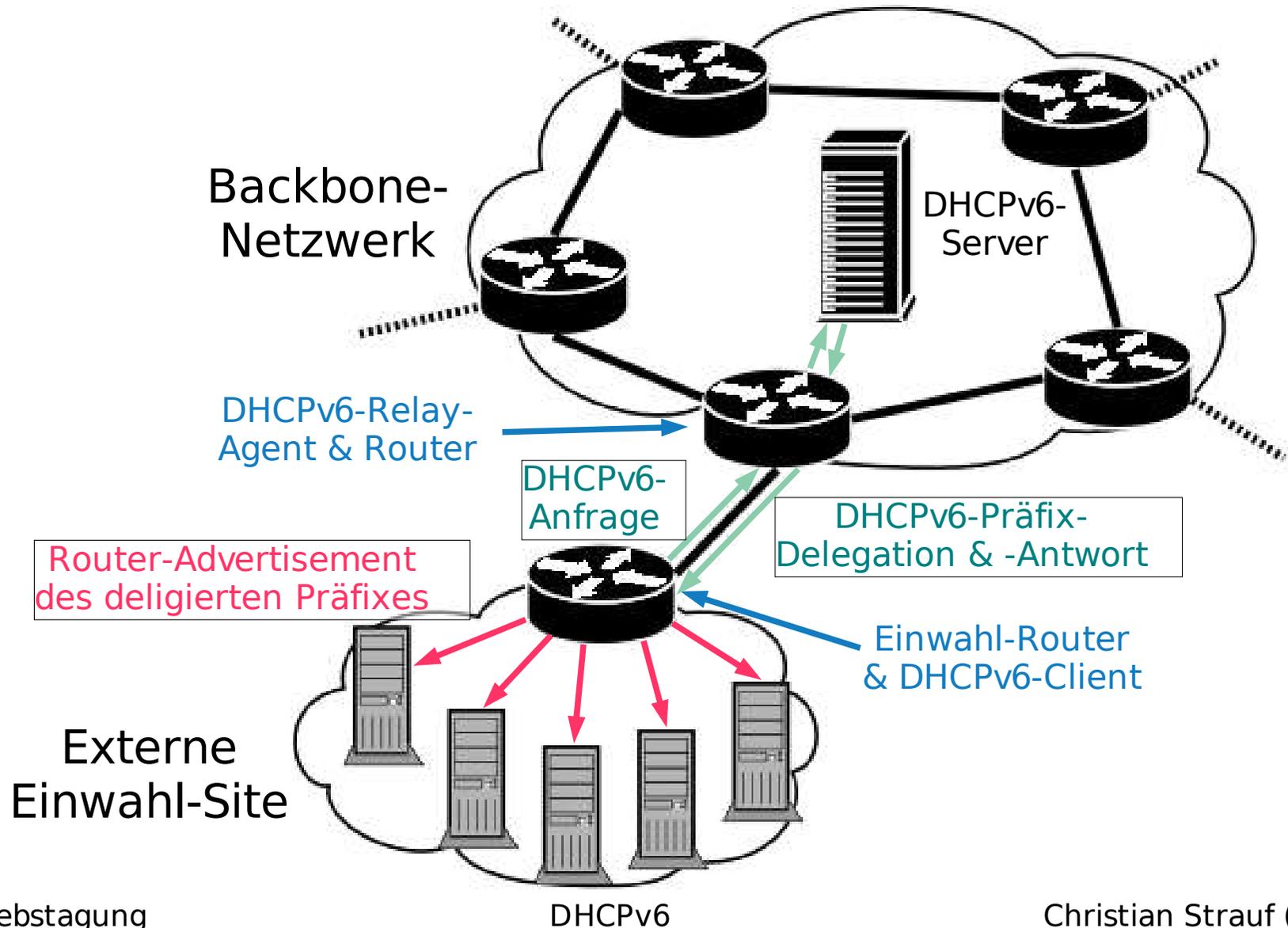


DHCPv6-Server mit Präferenznummer

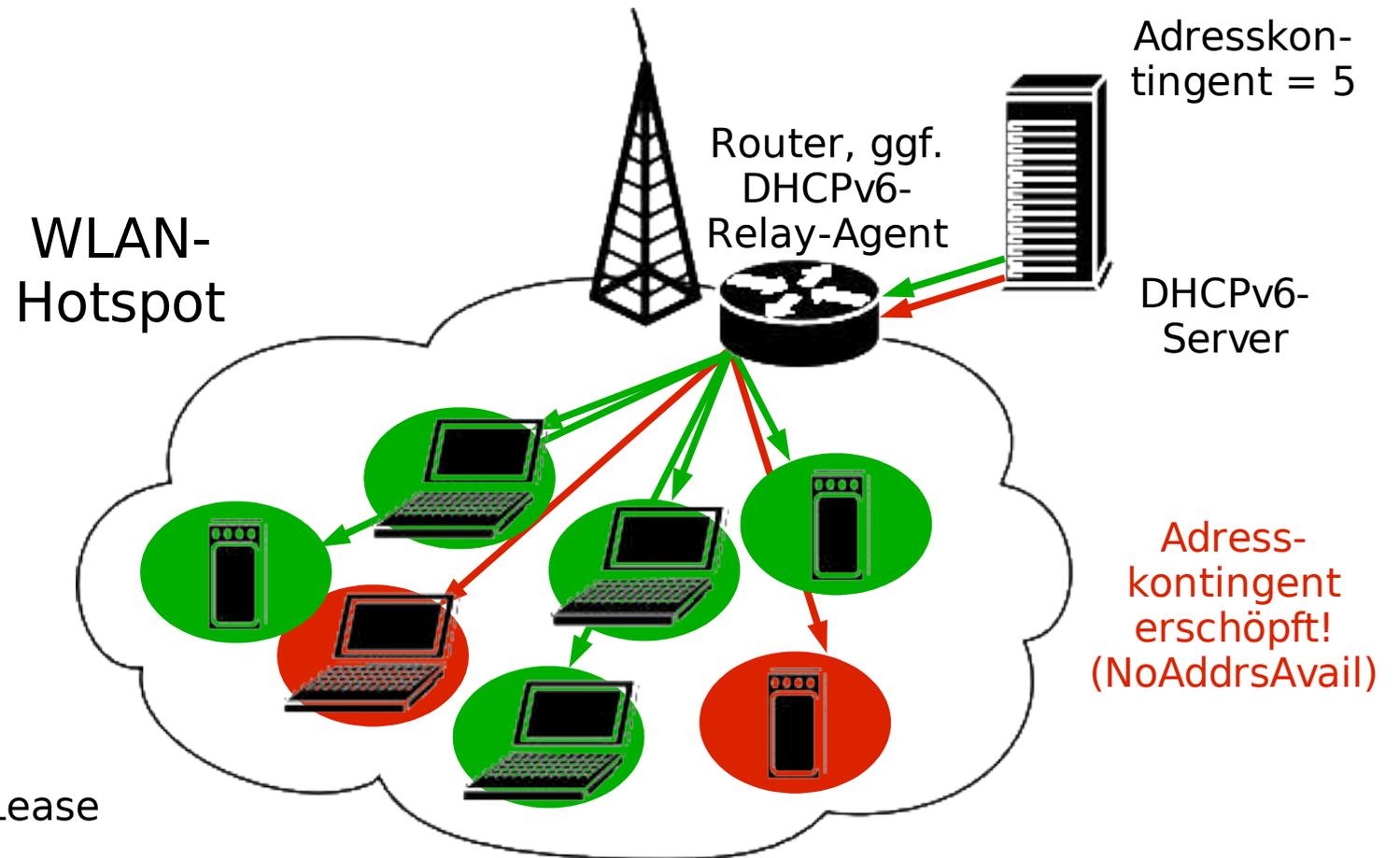
Bez.:	Präf.nr.:
D254	254
D253	253
D252	252
D251	251

DHCPv6 – weitere Optionen

Präfix-Delegation



Begrenzte Adressvergabe



- = Gültige DHCP-Lease
- = Keine DHCP-Lease

DHCPv6 – mit oder ohne SAA?

DHCPv6 bei Stateless Address Autoconfiguration

- In RFC festgelegt: DHCPv6-Server & -Clients funktioniert parallel zu SAA
- DHCPv6 im **Stateless-Betrieb**:
 - DNS- & NTP-Server-Adress-Übermittlung, evtl. Präfix-Delegation
 - Restliche Konfiguration vollständig mit SAA

DHCPv6 im Stateful-Betrieb

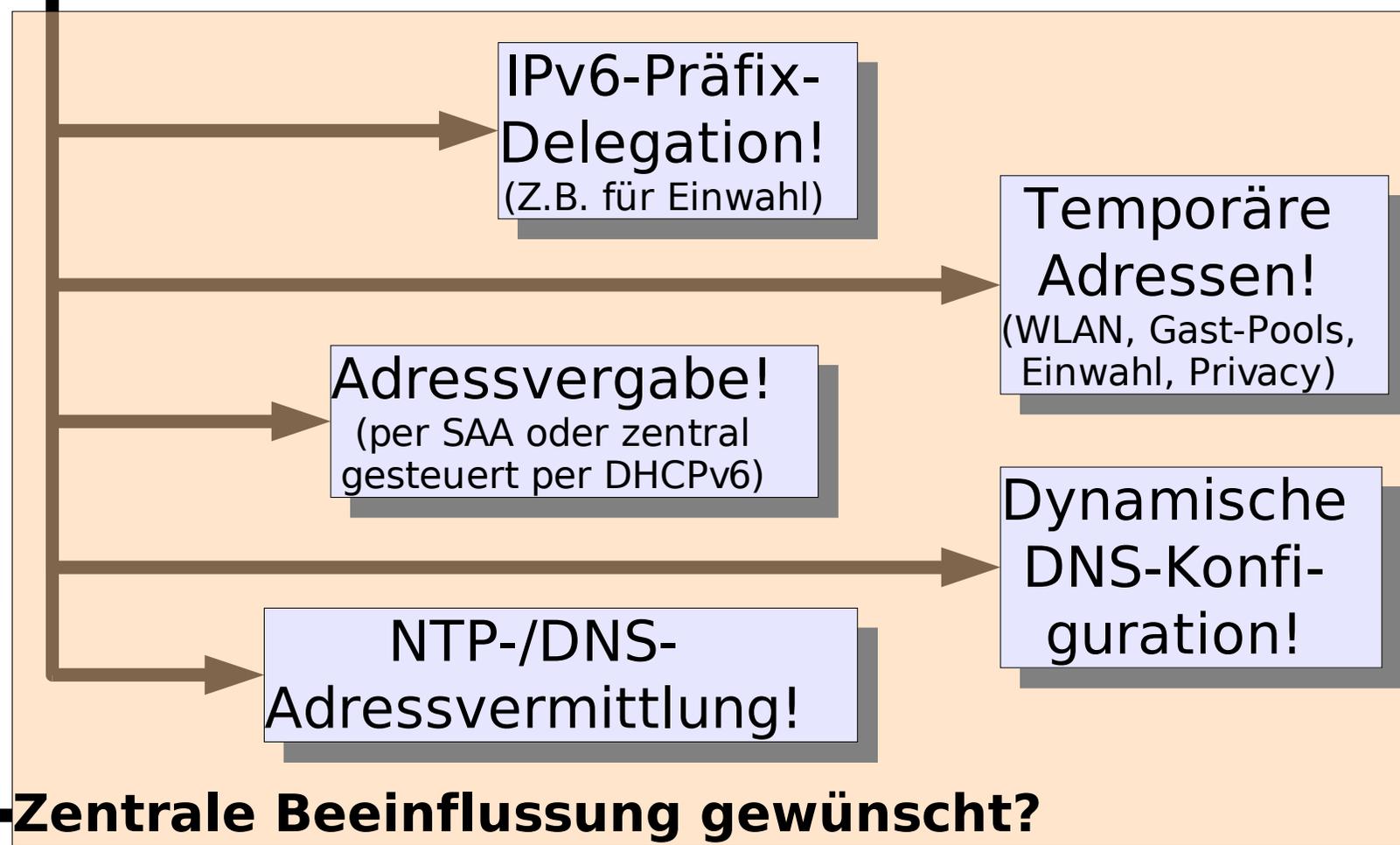
- **Stateful-Betrieb** mit...
 - ... „pro-interface“ Adress-Vergabe und Konfiguration
 - ... Beschränkung von Adress-Leases
- **ACHTUNG:** DHCPv6 \neq erhöhte Sicherheit:
Trotzdem möglich: manuelle Konfiguration von...
 - ... IPv6-Adressen
 - ... Routern
 - ... DNS-Servern, etc.!
- Sicherheit von Server Richtung Client existiert!

Entscheidung: Stateless oder Stateful DHCPv6?



Anforderungen einer großen Site

Ersetze SAA durch DHCPv6, wo nötig!



Sicherheit von DHCPv6

Sicherheit zwischen Server und Relay Agents

- Verwendung von IPsec:
 - Transport-Mode oder ESP
 - Authentifizierung der Verbindung
 - DHCP-Messages nicht vertraulich, keine Verschlüsselung nötig

Authentifizierung v. DHCP-Messages

- Verwendung der Authentifizierungs-Option (OPTION_AUTH) mit:
 - Replay-Detection-Mechanism (RDM)
 - versch. Authentifizierungsprotokollen
 - versch. Algorithmen zur Authentifizierung
- Mögliches Protokoll: Delayed Authentication Protocol

Delayed Authentication Protocol

- Schützt Client vor feindlichen DHCPv6-Servern
- Schlüssel wird vom Server „out-of-band“ (z.B. per Diskette) einmal zum Client übertragen
- Client bittet um Authentifizierungs-Protokoll in Solicit-Messages
- Verwendung der HMAC-MD5-Funktion zur Authentifizierung von DHCP-Messages

Reconfigure Key Authentication Protocol

- Schützt Client vor falschen Reconfigure-Messages
- Key-Übertragung mit erstem DHCPv6-Exchange
- Reconfigure-Message-Generierung auf Server:
 - HMAC-Digest-Berechnung der Reconfigure-Message mit Key
 - Reconfigure-Message-Versand inkl. HMAC-Digest
- Bei Empfang auf Client:
 - Berechnung HMAC-Digest mit vorhandenem Key
 - Vergleich mit empfangenen HMAC-Digest

Die Zukunft mit DHCPv6

DHCPv6 – das Mittel der Wahl

- Erleichterung des Managements
- Beseitigung von Nachteilen von SAA:
 - DNS- & NTP-Server-Übermittlung möglich
 - Präfix-Delegation z.B. für Einwahl-Router
 - Leichtere Verwaltung komplexer Netze mit Relay-Agents
- Charmante Möglichkeiten bei Einwahl bzw. Einbindung kleiner externer Sites

DHCPv6-Implementierungen

- Noch wenige Implementierungen
- Client-/Server-Implementierungen für PCs/Server:
 - <http://dhcpv6.sourceforge.net> (Linux, *BSD, möglicherweise andere Unix-Flavours)
 - DHCPv6-Support in HP-UX
 - DHCPv6-Support in Kame (*BSD) – muss extra aktiviert werden (kein stateful DHCPv6!)
- Router-Implementierungen:
 - Cisco IOS (rudimentär – bald mehr)

DHCPv6-Implementierungen (2)

- Kommerzielle Implementierung für Windows
- Aber:
 - RFC und abstammende RFCs/Drafts noch jung
 - Diskussionen in IETF-Kreisen zeigen Wichtigkeit von DHCPv6
 - Router-Hersteller stecken Energie in DHCPv6
 - Betriebssystemhersteller ziehen nach
 - Kommerzielle DHCPv6-Software-Anbieter gibt es schon

Ausblick

- DHCPv6 wichtig für Betrieb
- Positive Entwicklungen (Router- und Betriebssystemhersteller gehen Richtung DHCPv6)
- Theoretische Anwendung und Deployment von DHCPv6 klar
- Interoperabilitätstests wichtig
- Prefix-Delegation charmantes Feature
- DHCPv6-Implementierungen müssen gefördert werden



Fragen?

Vielen Dank für Ihre Aufmerksamkeit!

JOIN-Projekt-Team
Westfälische Wilhelms-Universität Münster
Zentrum für Informationsverarbeitung
Röntgenstraße 9-13
D-48149 Münster

Web: <http://www.join.uni-muenster.de>
Email: join@uni-muenster.de
Email: strauf@uni-muenster.de