

# IPv6 Schulung

Lutz Donnerhacke  
IKS Service GmbH

# Mythen

- Hat neue Servicequalität für Echtzeitübertragungen (TV, Sprache).
- Ist sicherer, weil IPSec mit drin ist.
- Wer IPv6 einsetzt, kann kein IPv4 mehr nutzen.
- Viel zu kompliziert.
- Kann unsere Technik eh' nicht.

# Vorurteile

- Wir fangen in 14 Jahren damit an. Mein Kollege geht da in Rente.
- Wir können wir uns ja nicht mehr auf NAT verlassen und müssen Firewall-Regeln bauen.
- Wann ist IPv6 so sicher wie IPv4?

# Grundlagen

# Was ist Internet ?

- Wie kommt eine Webseite in meinen Rechner?

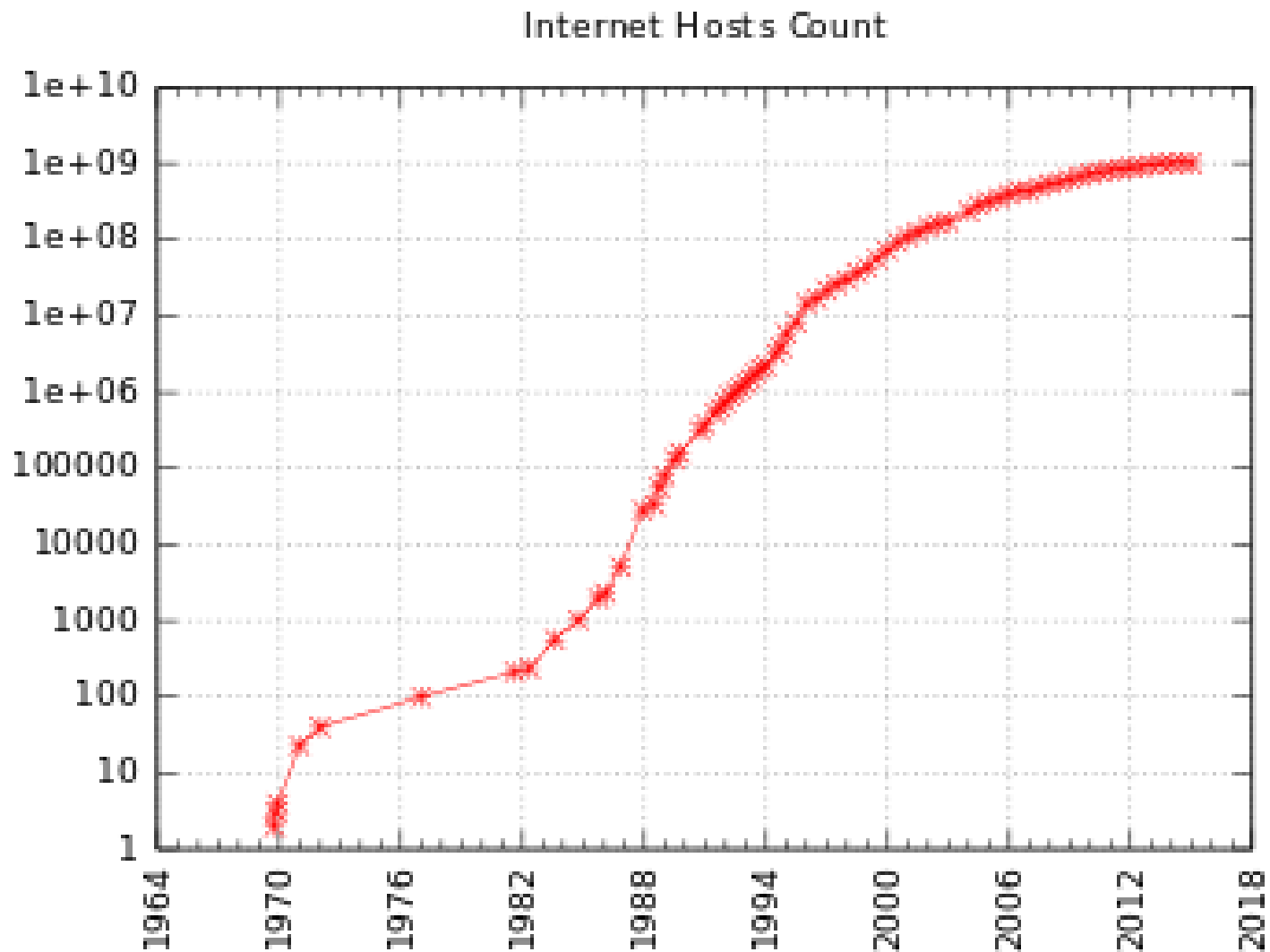
<http://www.wdrmaus.de/sachgeschichten/sachgeschichten/internet.php5>

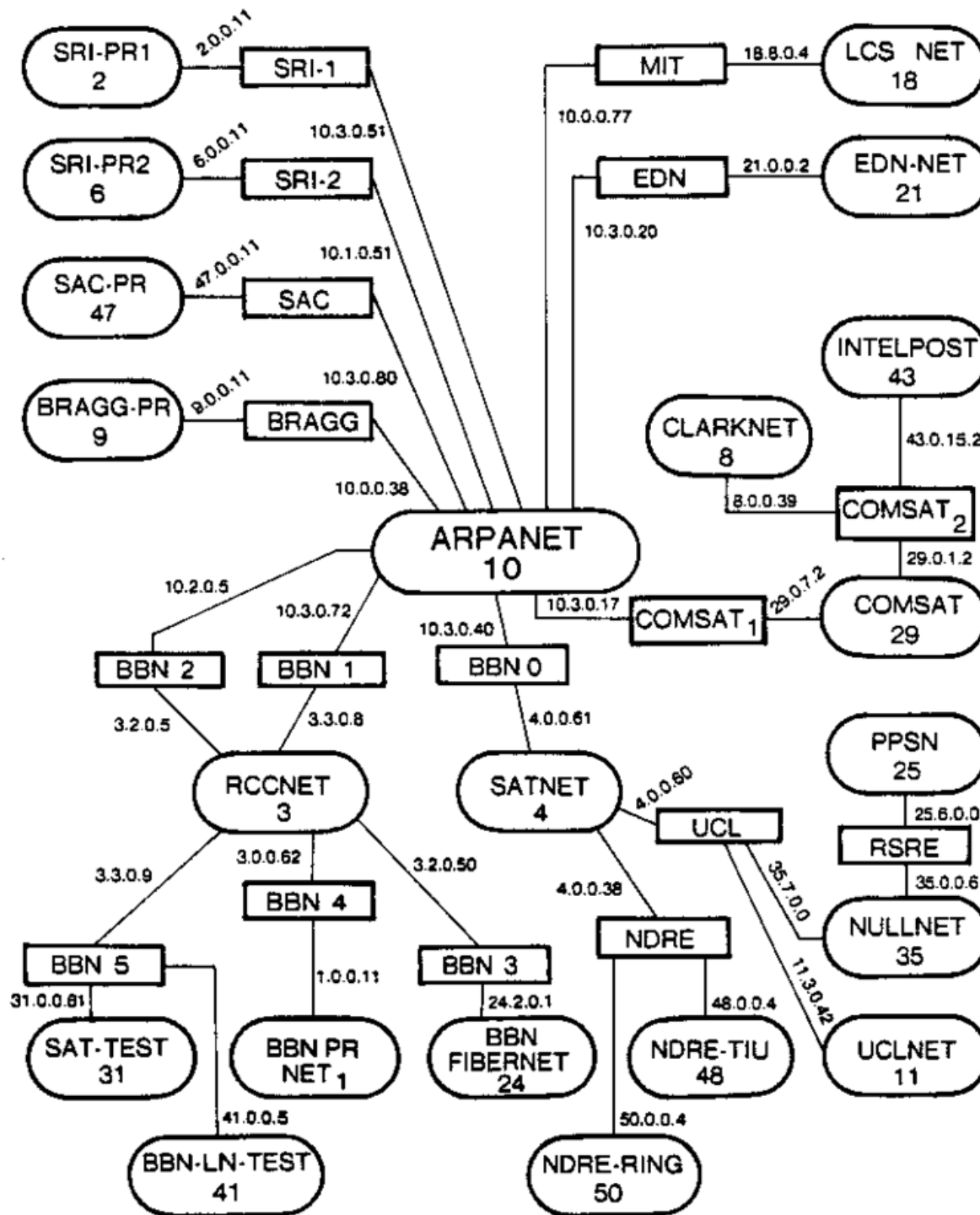
- Die Rolle des Providers
- IP-Adressen und Namensauflösung
- IP-Adressen und Routing
- Server und Kopien von Daten

# IP-Adressen

- Hierarchische Vergabe
  - Eindeutige Kennzeichnung
- Direkte Kommunikation von Endgeräten
  - Netzneutralität
- **Ein Internet** ist die *transitive Hülle* der Systeme, die sich per IP erreichen können.
- **Das Internet** ist ein Internet, in dem die *Root-Server* stehen.

# Zeitliche Entwicklung







# Situation 1991

- Dominanz im neuen Deutschland
  - Fido/Maus für Privatpersonen
  - IPX in Unternehmen
  - OSI in Universitäten
- Umschwung zu IP
  - Zentrale Adressvergabe **ermöglicht** Routing
  - Verbreitung von Linux und Trumpet Winsock
  - Aufkommen von FTP, Archie, Gopher und WWW

# Was kann man erzählen?

## Technik

- Header und Bits
- Software und Konfiguration
- Probleme und Lösungen
- Gesetze und Verträge
- Sicherheit und Hacking

Anleitung zum Bootsbau

## Vision

- Portale und Suchmaschinen
- Facebook und Twitter
- SIP und Skype
- Blogs und Podcasts
- Einkaufen und Revoluzzen

Sehnsucht nach dem Meer

# Erfolgskriterien für IPv6

- Kollegen erwarten
  - **Direkte** Erreichbarkeit von Systemen  
Mailserver, Remote Desktop, „internes“ DNS
  - **Einfache** Konfiguration: „ipv6 ospf 1 area 0“
  - HTTPS-Zugriff von **unterwegs** auf Intranetserver
  - **Gleichartige** Handhabung vom mobilen Gerät
- Kunden erwarten
  - Funktionalität trotz **Protokollignoranz**
  - IPv6 vom **neuen ISP** nach einem Umzug

# Was liefert IPv6?

- Endgeräte haben **öffentliche**, routbare IPs
  - Ohne Autoconfig tunneln Clients automatisch
- Server haben mehrere, **feste**, dienstbezogene IPs
  - Diensttrennung und Hardwaretausch
- Mediatoren wie NAT, DMZ und Portale entfallen
  - Zukünftige Protokolle erwarte **direkte** Kommunikation
  - Web 2.0: Daten direkt von den **Quellen**
  - **Verschlüsselte** Client-Client Kommunikation
  - **Kürzeste** Pfade für „gute Qualität“

# Bits und Bytes

# Aufbau der Adressen

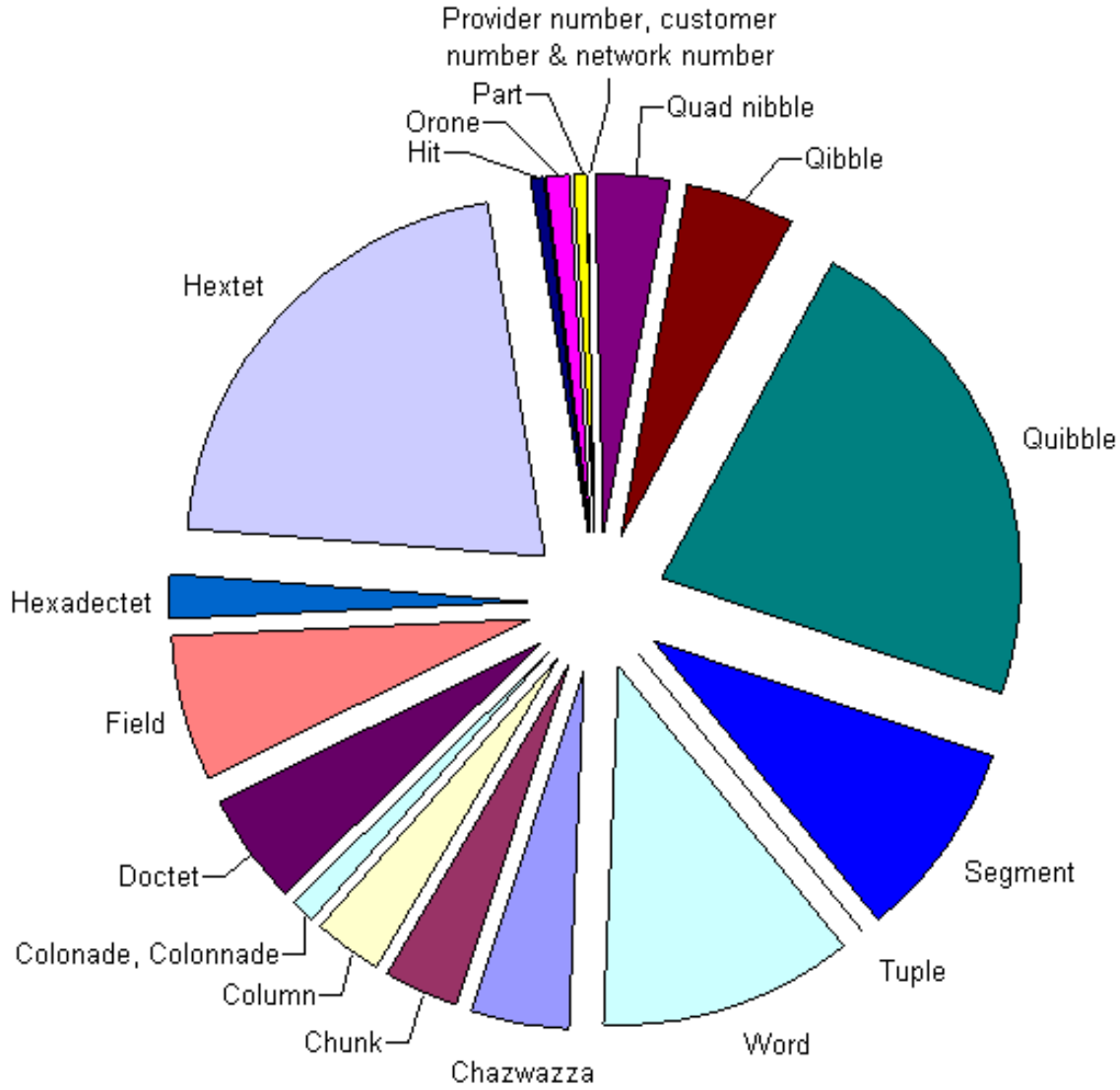
- 128bit lang, also  $2^{128}$  Möglichkeiten
  - 6700 IP Adressen pro Atom Erdoberfläche
- Nicht alle Möglichkeiten genutzt
  - Große Teile des Adressraums noch frei
  - Nur  $\frac{1}{4}$  der Adressen sind global nutzbar
- Großzügige Vergabe
  - 64bit pro Netz (MAC hat 48bit)
  - 4, 8 oder 16bit Netze pro Kunde
  - Mehr als 32bit Netze (soviel IPs hat v4) pro LIR

# Aufbau der Adressen

- 128 bit in hexadezimal: 32 Nibbles
- 32 Nibbles in 4er-Gruppen: 8 Hextets
  - Erste 4 Hextets (64bit): Netz
  - Zweite 4 Hextets (64bit): Hostanteil
- Vereinfachen
  - Führende Nullen weglassen: 2001:db8:0:1061:0:0:0:0
  - Mehrere Nullen zusammenfassen: 2001:bd8:1061::

RIR	LIR	Kunde	VLAN	Hostanteil, z.B. MAC Adresse			
2001	0db8	0000	1061	0248	54ff	fe12	ee3f

# Benennung der Gruppen



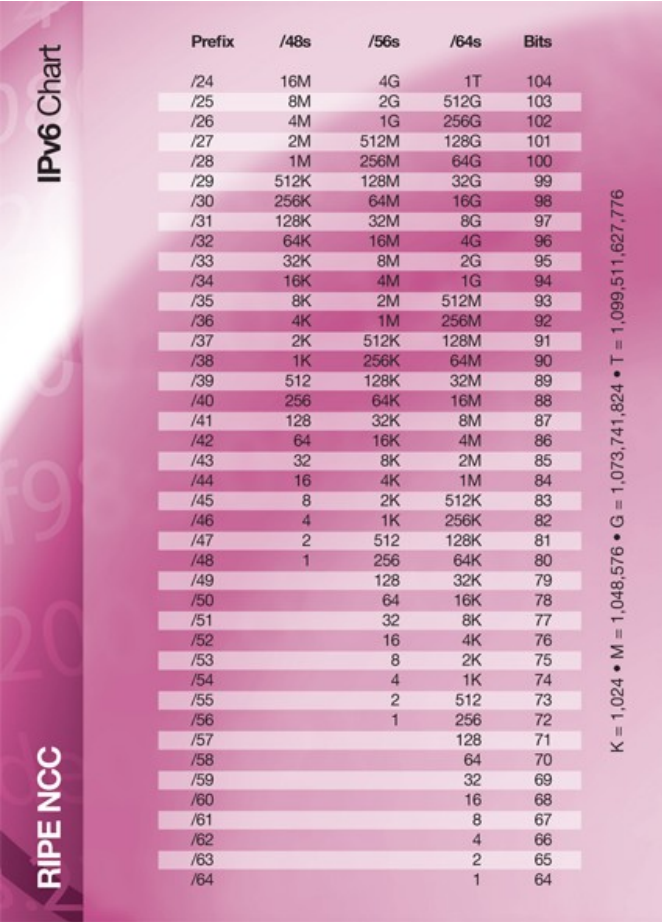


# Netzformat

- An CIDR-Format angelegt
  - Bits des Netzanteil werden gezählt
  - Hostanteil konstant 0, dadurch als :: geschrieben
- Beispiele
  - 2001:db8::/32
  - ::1/128
  - ::/0
  - fe80::/64

# Netzformat

- Gängige Größen
  - /29 – aktives LIR
  - /32 – LIR Start
  - /48 – Großkunde
  - /56 – Kleinkunde
  - /60 – Massenkunde
  - /64 – Netz
  - /112 – shared Host(ing)
  - /127 – P2P-Netz
  - /128 – Einzeladresse



The image shows a vertical chart titled 'IPv6 Chart' and the 'RIPE NCC' logo. The chart is a table with 5 columns: Prefix, /48s, /56s, /64s, and Bits. It lists IPv6 prefixes from /24 to /64. The background of the chart is a gradient of purple and pink with faint circular patterns.

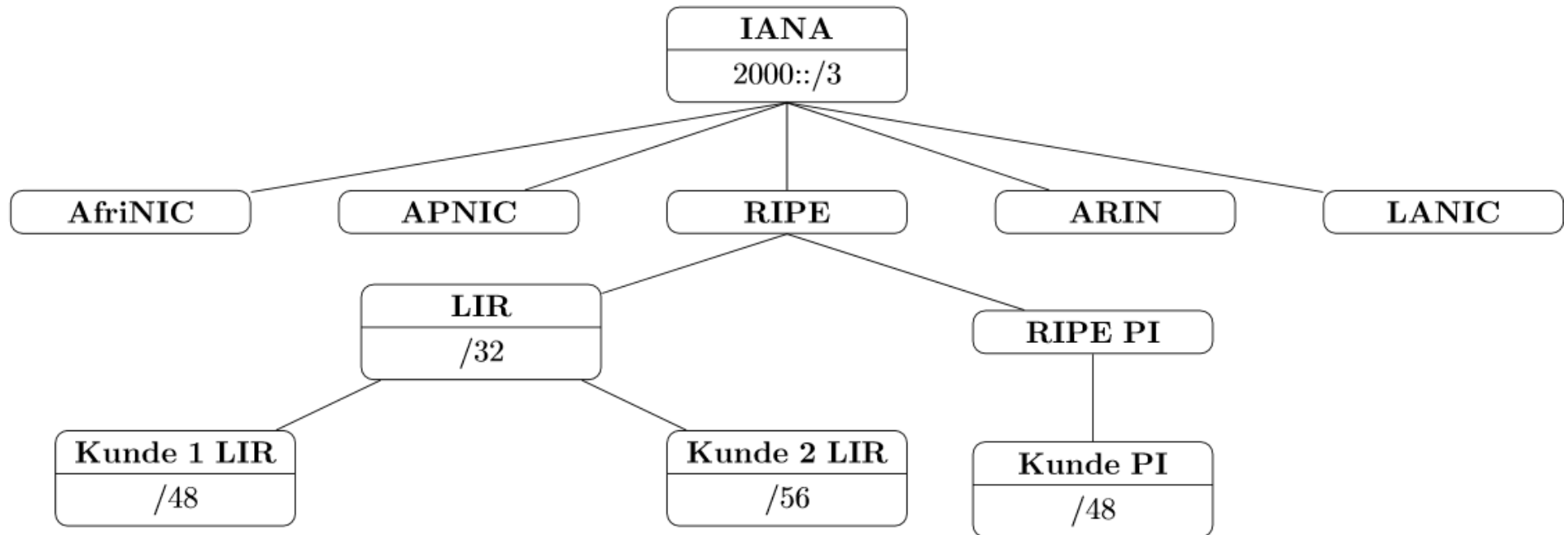
Prefix	/48s	/56s	/64s	Bits
/24	16M	4G	1T	104
/25	8M	2G	512G	103
/26	4M	1G	256G	102
/27	2M	512M	128G	101
/28	1M	256M	64G	100
/29	512K	128M	32G	99
/30	256K	64M	16G	98
/31	128K	32M	8G	97
/32	64K	16M	4G	96
/33	32K	8M	2G	95
/34	16K	4M	1G	94
/35	8K	2M	512M	93
/36	4K	1M	256M	92
/37	2K	512K	128M	91
/38	1K	256K	64M	90
/39	512	128K	32M	89
/40	256	64K	16M	88
/41	128	32K	8M	87
/42	64	16K	4M	86
/43	32	8K	2M	85
/44	16	4K	1M	84
/45	8	2K	512K	83
/46	4	1K	256K	82
/47	2	512	128K	81
/48	1	256	64K	80
/49		128	32K	79
/50		64	16K	78
/51		32	8K	77
/52		16	4K	76
/53		8	2K	75
/54		4	1K	74
/55		2	512	73
/56		1	256	72
/57			128	71
/58			64	70
/59			32	69
/60			16	68
/61			8	67
/62			4	66
/63			2	65
/64			1	64

RIPE NCC

IPv6 Chart

K = 1,024 • M = 1,048,576 • G = 1,073,741,824 • T = 1,099,511,627,776

# Vergabehierarchie



# Adressarten

- Es gibt
  - Unicast: Das physische Ziel
    - Global: Überall im WAN (2000::/3)
    - Link-local: Nur im LAN (fe80::/10)
  - Anycast: Einen Dienst (Adresse wie Global)
  - Multicast: Alle Interessierten (ff00::/8)
  - Unique Local: Private Nutzung (fc00::/8 zentral, fd00::/8 zufällig)
- Ein Interface hat
  - eine link-local Unicast Adresse
  - eine oder mehrere Multicast Adressen (ff01::1 – all hosts)
  - null oder mehrere globale Adressen haben

# Adressplanung

- Relevant sind nur die 32bit, die der LIR vergibt
- Geplant werden nur ganze Netze /64
  - Anzahl der Hosts ist praktisch unbeschränkt
- Planziele
  - Aggregation der Routen
  - Einfache Firewallregeln
  - „Sprechende“ Adressen

# Adressplanung (Alternativen)

- Direktes Mapping existierender Nummern
  - IPv4: 10.4.15.0/24 → 2001:db8:0:040f::/64
  - VLAN: vlan-id 12 → 2001:db8:0:0d::/64
- Konvertierung von Dezimal nach Hex
- Trick beim Einbinden von IPv4
  - 2001:db8:0:co:ff:ee:10.4.15.192  
2001:db8:0:co:ff:ee:0a04:0fc0
  - Leicht zu schreiben, schwer zu lesen
  - Schreibweise wird nicht überall verstanden

# Adressplanung (richtig)

- Erste Bits für verschiedene Standorte
- Primäres Arbeitsmittel festlegen
  - Router: Nächste Bits nach Struktur
  - Firewall: Nächste Bits nach Funktionsgruppen
- Weitere Bits auffüllen mit Struktur/Funktion
- 2001:db8:LLOO:TTVV::/64
  - L – Land, O – Ort, T – Typ, V – VLAN
  - Firewall kann auf /56 filtern, egal welches VLAN

# Adressplanung (richtig)

- Mut zur Lücke
  - Wachstum einkalkulieren
- Trennung auf Nibblegrenzen
  - Netzmaske durch 4 teilbar
  - Andernfalls Ärger mit DNS und Anschauung
- Bifurkation als Zuteilungsplan
  - Immer maximale Abstände nehmen und halbieren
  - Immer genug Luft für ungeplante Erweiterungen
  - Anwenden, wenn völlig unplanbar



# Hostanteil

- Manuell mit vielen Nullen → x::<1>
- EUI-64: 48-bit MAC Adresse → 64bit
  - Sonderbits der MAC stören (invertieren)
  - Erkennung der Bitreihenfolge mit fffe in der Mitte
  - Neue Geräte im Netz haben vorhersagbare IP-Adressen
- Privacy Extensions
  - Mehrfache zufällige IPs pro Ziel und Datenmenge
  - Offene Frage: Woher Abuse-Informationen?
- Stable Random Identifiers
  - Windows, abhängig von GW-MAC und AD

# Hostanteil

- Manuell für Server und Router
- SLLAC für einfache Clients
  - Router annouciert Netz (und DNS)
  - Host wählt selbst mit Duplicate Address Detection
- DHCPv6 für besondere Clients und Server
  - Oft nur die fehlenden Infos (DNS, NTP, ...)
  - Prefixdelegation möglich
  - Zentrale Adressvergabe möglich

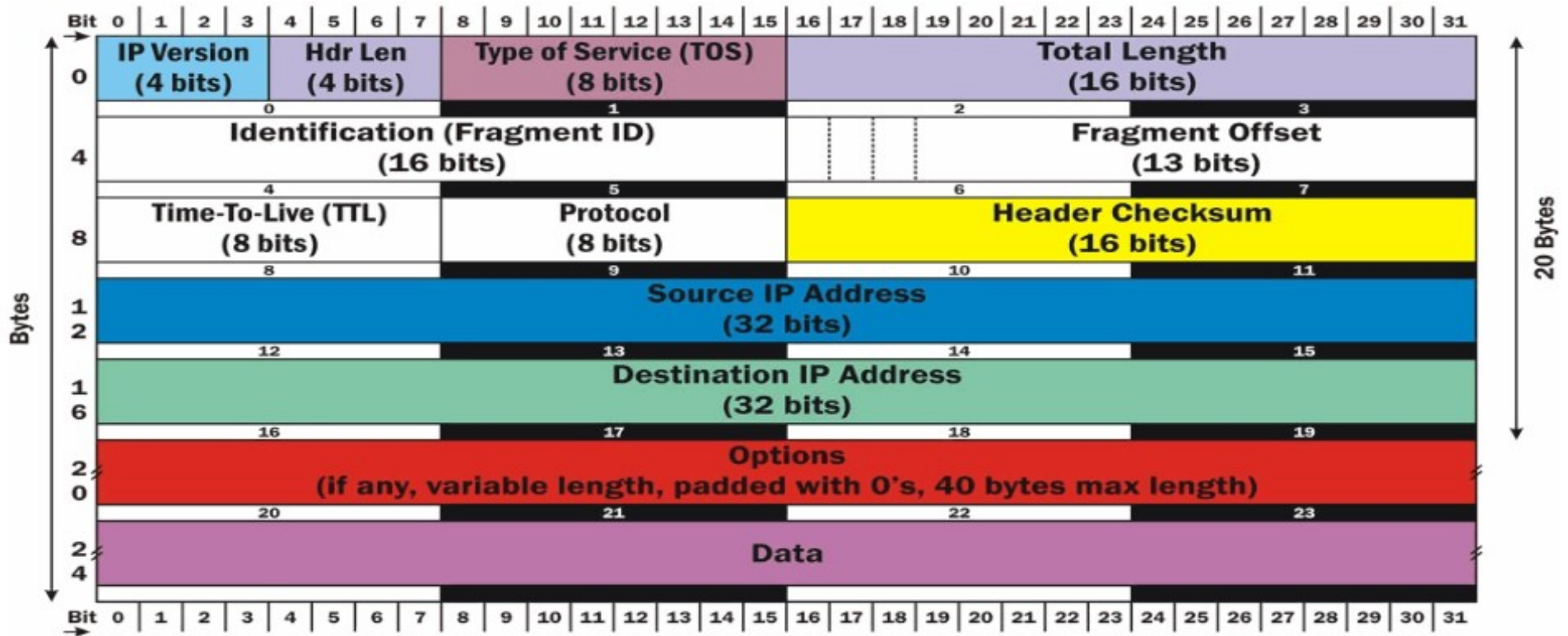
# Hostanteil

- Manuelle Adressen kurz halten
  - Eintippen wird weniger fehleranfällig
  - Dienst kodieren X::53, X::123
- Bei Routern auch Link-Lokal manuell setzen
  - Windows ändert sonst eigene IP
  - Routingtabelle wird übersichtlicher
  - fe80::routerid:vlan (zentral managed /112)
- Bei Dual-Stack-Servern IPv4 kodieren
  - 192.0.2.1 → 2001:db8:0:0:192:0:2:1 (kein Hex)

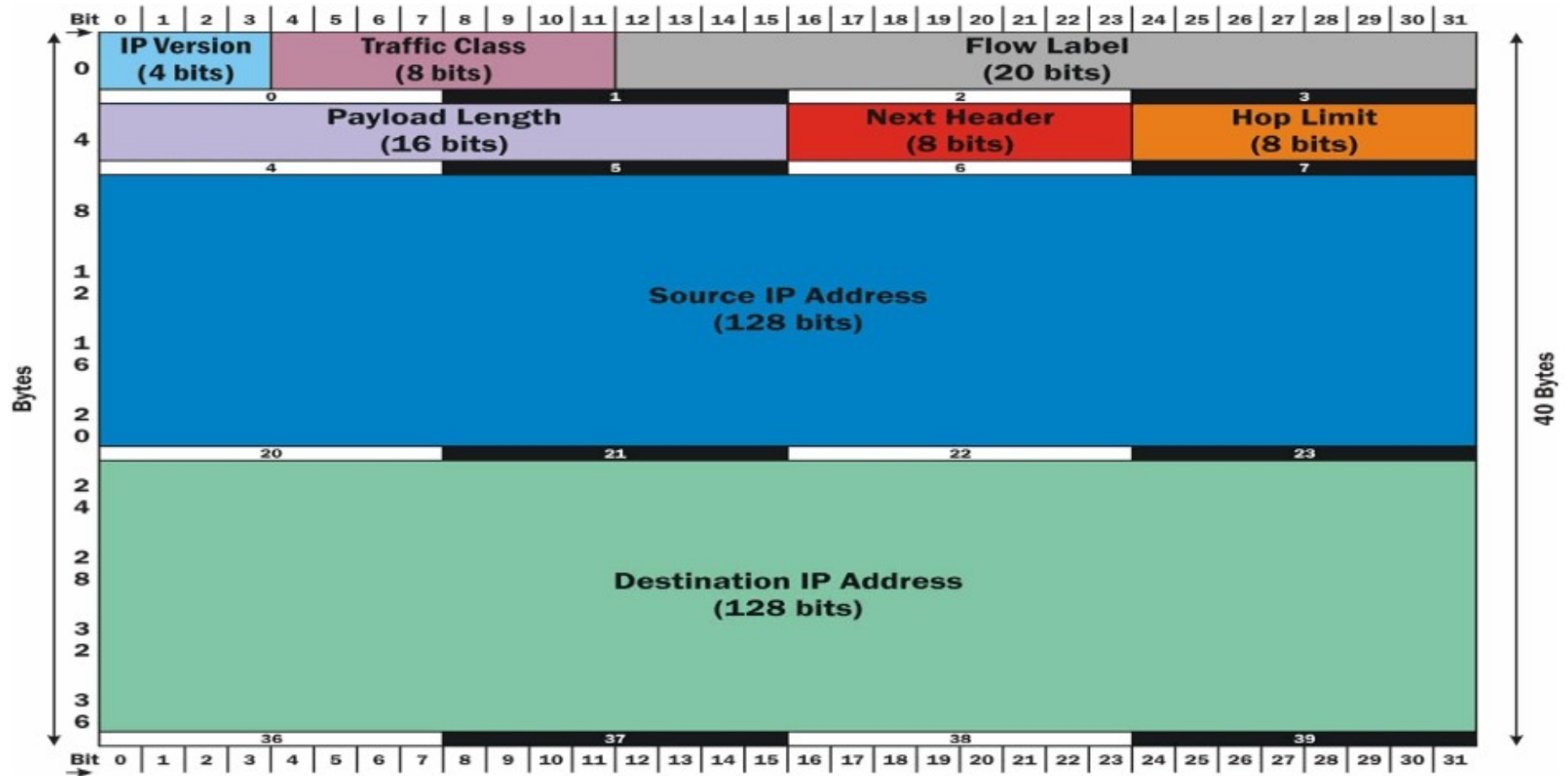
# Transport im Ethernet

- Eigener Ethernettype: 86DD
- kleinste MTU: 1280 Byte
- Path MTU Discovery (PMTUD)
  - Router fragmentieren nicht mehr (DF=1)
  - ICMPv6 zwingend aus dem Internet annehmen
- Neighbor Discovery für IP->MAC Mapping
- Multicast muss die MAC enthalten: letzte 24bit

# IPv4 Header



# IPv6 Header



# IPv6 Header

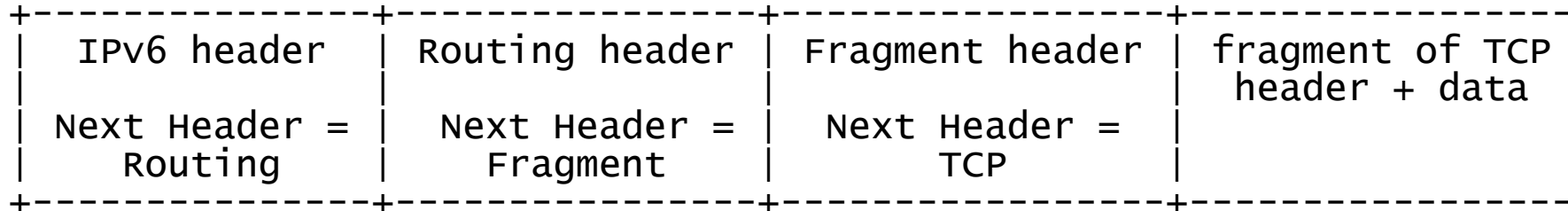
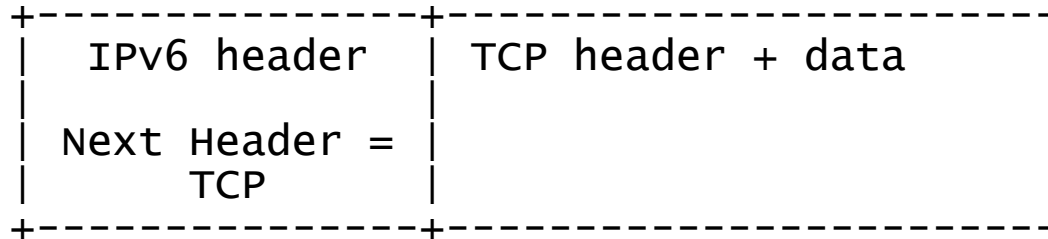
- Feste Größe des Headers
  - Kein Durchmischen von variablen Optionen
- Beim Erreichen des Ziels Header wegnehmen
  - Evtl. weitere Header vorhanden, sonst Payload
- Vereinfachtes Processing auf Routern

# IPv6 Header

- Hop-by-Hop Option Header
- Routing Header
  - Einige davon für Mobile IPv6 (nicht blocken)
  - Andere inzwischen als gefährlich eingestuft
- Fragment Header
- Authentication Header
- Privacy Header



# IPv6 Header



# ICMPv6

- Andere Protokollnummer als ICMP
  - Firewall ACL mit „icmp6“ statt „icmp“
- Zentrales Managementwerkzeug in IPv6
  - Nachbarschaftserkennung (ehemals ARP)
  - Multicast verwalten (ehemals IGMP)
  - Router Advertisements
  - Renumbering

# ICMPv6

- Fehlermeldungen

- 1 Destination unreachable
- 2 Packet Too Big
- 3 Time Exceeded
- 4 Parameter Problem

- Nicht blocken

- Management

- 128 Echo Request
- 129 Echo Reply
- 130 Group Membership Query
- 131 Group Membership Report
- 132 Group Membership Reduction
- 133 Router Solicitation
- 134 Router Advertisement
- 135 Neighbor Solicitation
- 136 Neighbor Advertisement
- 137 Redirect
- 138 Router Renumbering

- Im LAN wichtig

# Neighbor Discovery

- Aus dem Prefix ff02::1:ff00:0/104 und den letzten 24Bit der Ziel IP wird eine Multicast Adresse gebaut
- An diese Adresse wird ein ICMP Paket vom Typ 135 geschickt
- Der Zielhost antwortet mit Layer2 Adresse in einem ICMP Paket vom Typ 136

# Duplicate Address Detection

- Vermeidet die mehrfache IP Adressen
  - Unicast, ICMP Typ 135, von ':::' an die Zieladresse
  - Wenn Adresse schon vorhanden, Antwort an ff02::1
- IP Adressen nicht sofort nutzbar (tentative)
  - Startup-Verhalten von Servern beachten
- Wird auch bei manuellen Adressen gemacht
  - Server können u.U. gar nicht mehr erreichbar sein

# Router Advertisements

- Verteilen von Prefixen mit Lebenszeiten
- Managed-Flag: Client Adresse per DHCPv6
- Other-Config Flag: Weitere Infos per DHCPv6
- Verteilen von Recursive DNS Servern
- Ideal für Renumbering
- Clients mit feste IP können den Router lernen

# SLAAC

- SLAAC ist einer der Vorteile von IPv6. Ein Host
  - wählt eine Interface ID, z.B. seine MAC Adresse
  - generiert aus der MAC eine EUI64 Adresse
  - erzeugt daraus seine link-local Adresse (Prefix: FE80::/64)
  - prüft, via DAD ob die Adresse schon einmal vorhanden ist
  - fragt per ICMP (Router Solicitation) alle Router nach weiteren Prefixen
  - fügt für jedes empfangene Prefix eine weitere Interface Adresse hinzu
  - hört weiter auf Router Announcements und ändert ggf. die Adressen
  - lernt die Router als default Gateway
- Problem:
  - kein automatischer Eintrag ins DNS

# Sicherheitswarnung

- Jeder Router annunciert Prefixe
- Auch defekte Router, Server oder Angreifer
- Manuelle RA Priorität setzen
- First Hop Security nötig
  - RA-Guard verhindert Router Advertisements
  - DHCP-Guard ist seltener nötig
  - Neighbor Discovery nur, wenn schon ARP Schutz



# DNS

- Aus A wird AAAA
  - `www AAAA 2001:db8:dead:beef::1`
- Reverse DNS an Nibble-Grenzen
  - `1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.e.e.b.d.a.e.d.8.b.d.0.1.0.0.2.ip6.arpa`
  - PTR Records wie gehabt
  - Kein \$GENERATE möglich, aber wildcards
- Keine Probleme mit Subnetzdelegation
  - Wenn nicht mit krummer Netzmaske gebaut
  - RIPE delegiert ein /19, also mehr als eine DNS-Zone

# Happy eyeballs

- Clients fragen parallel nach A und AAAA
  - Wer schneller antwortet gewinnt
- Funktion aller Dienste auf allen IPs nötig
  - IPv6-Tag: Hoster setzt AAAA, Kunde zieht A um
  - Wenn Dienst nicht auf v6 lauscht, Timeouts möglich
- Tipp: Normal benutzen
  - Es ist eine Adresse wie jede andere
  - Dual-Stack sollte einfach tun

# Firewalls

- Kein NAT mehr
  - Alle internen Maschinen haben globale IPs
  - Grundsätzlich aus dem Internet erreichbar
- Firewallregeln
  - ICMPv6 durchlassen (Fehlercodes)
  - Filtern nach Netzen (Funktionsgruppen)
  - Viel Link-Local Multicast Traffic nötig

# Multicast

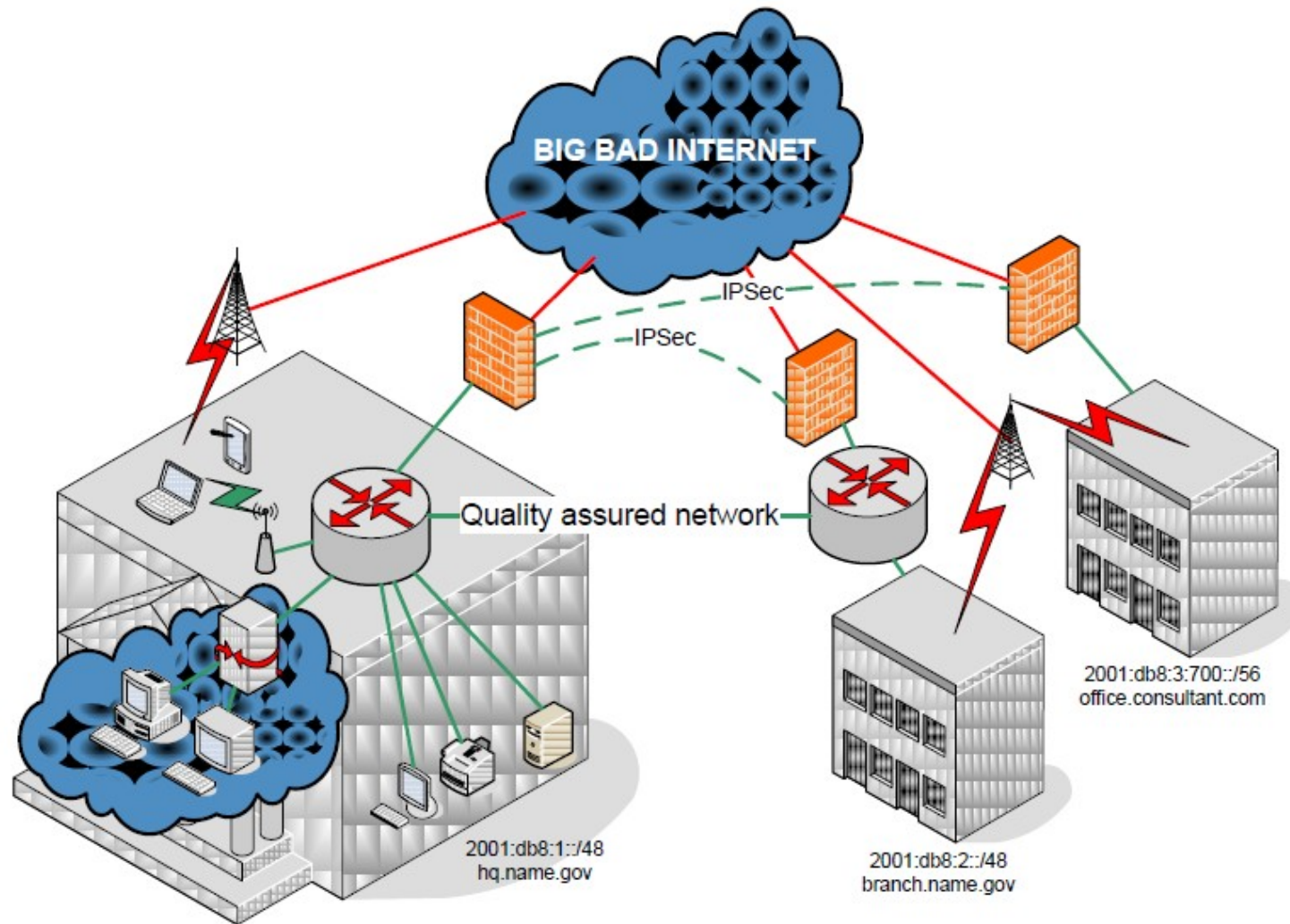
- Basisfunktionalität von IPv6 ersetzt Broadcast
- IGMP Teil von ICMP
- PIM (sparse/dense) für größere Netze
- Verschiedene Adressen
  - ff0x::/8 – Multicast, ohne Source
  - ff3x::/8 – Multicast, Source eingebettet
  - ffx1:/8 – Host-Lokales Multicast
  - ffx2:/8 – Link-Lokales Multicast
  - ffx8:/8 – Organisations-Lokales Multicast
  - ffxe:/8 – Globales Multicast

# Routing

- Router immer im lokalen Netz erreichbar
  - Routing i.d.R. auf link-lokal Adressen
  - Manuelle Routen können globale Ziele nehmen
- OSPF, ISIS, RIPng, BGP etc. verfügbar
- Konfiguration Cisco
  - Fehler der Zuordnung behoben
  - Interface-Konfiguration am Interface

Einfluss auf interne Netze

# Mobilfunk als Problem

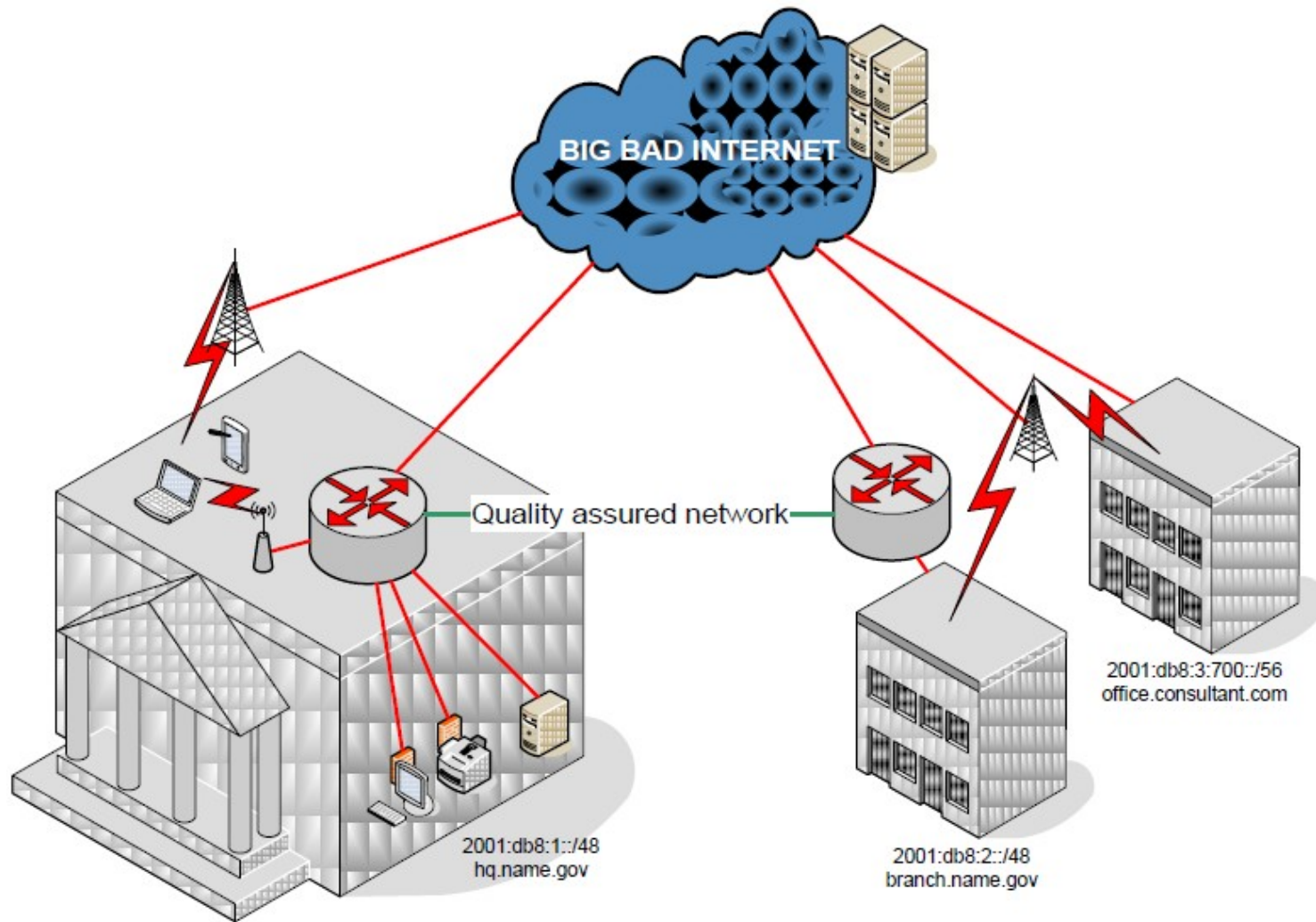


# DNS und Mobile Endgeräte

- IPv6 Anwendungen brauchen DNS
  - Dynamische Updates bei Autoconfig
  - Dynamische CNAMEs für Privacy Extensions
- Interne DNS Server extern sichtbar
  - Bei DirectAccess, SSH, Active Directory zwingend
  - DNSSEC verhindert Modifikationen
- Mobile Clients wechseln intern/extern
  - DNSSEC Root hartkodiert
  - Cloudaffin



# IPv6 als Chance



# IPv6 – Konsequenzen

- **Konsistentes Erscheinungsbild**
  - Egal ob lokales WLAN oder Mobilfunk
  - REST Web-Anwendungen statt VPN
- Absicherung der Dienste, nicht der Netze
- Absicherung der Daten, nicht der Server (cloud)
- Identifizierung des Nutzers, nicht des Computers
- DNS ist vertrauenswürdige, verteilte Datenbank
- Nur direkte, verschlüsselte Kommunikation

# Zusammenfassung

- Abschneiden alter Strukturzöpfe
  - Zentraler Firewall und DMZ Ansatz scheitert
  - Rein interne Information gibt es nicht mehr
- Konzentration auf die Vorteile
  - Stabile, global erreichbare Netzwerke
  - Datensicherheit ist ein Eigenschaft der Daten
  - Vertraut den Nutzern, nicht der Technik

# Gesellschaftliche Auswirkungen

# Technosoziale Implikationen

## IPv4 (heute)

- 32bit für alles
- Netze dynamisch geteilt
- 300k globale Routen (frag.)
- **Private** Adressen mit NAT
- Services als Relays über Dienstleister (Hoster)
- **Kunde-Dienstleister-Modell**
- Trend zu neuen Diensten (soziale Netze, Portale)

## IPv6

- 64bit für Hosts
- 64bit für Netze
- 4k globale Routen (aggr.)
- Alles mit **globalen** Adressen
- Services am Endgerät möglich (Eigenbetrieb)
- **Ende-Ende-Kommunikation**
- Trend zu neuen Protokollen (Peer2Peer, verschlüsselt)

# Technosoziale Implikationen

## IPv4 (heute)

- Dynamische Adresspools
  - für selten aktive, viele Zugänge
- Statische IP als Geschäft
- Dynamische IP trotz always on als **Protektionismus:**
  - Hosting statt Kundenrechner
  - Trennung Business vs. Privat
- Suggestieren von
  - Anonymität
  - Providerunabhängigkeit
  - Sicherheit (NAT statt Firewall)

## IPv6

- 8-16bit für Netze beim Kunden
- Netzteil wird gelernt
  - Hostteil (64bit) frei wählbar
  - Mehrere Adressen Pflicht
  - **Privacy Extensions** mit je einer IP pro Gegenstelle
  - Mehrere Netze parallel für Providerwechsel ohne Ausfall
  - **Zweckabhängige IPs** parallel
- Sicherheit durch Filtern
  - Firewall notwendig

# Adresszuteilung im Massenmarkt

- Dynamik Pflicht, da Marketing-Indoktrination
  - Zwei Teile: *Hostadresse* und *zugeteiltes Netz*
  - Ende-Ende-Kommunikation erfordert *feste* IPs
- Mögliche Lösung
  - **Drei** Prefixe verteilen: 1x statisch, 2x dynamisch
  - Altes zugeteiltes Prefix bleibt noch 24h im Routing
- Mobile IPv6 lokal in den CPEs
  - Roaming leichtgemacht durch automatische VPNs

# Mittlerfreie Kommunikation

- Internet als Reduktion der Publikationskette
  - Leser greift **direkt** auf die Erstveröffentlichung zu
- Technikfolgeabschätzung
  - *Redefreiheit* mangels Redaktion, Drucker, Vertrieb
  - *Rezipientenfreiheit* mangels DPI (oder ?)
  - Potentiell *unbegrenzte* Leserzahlen
  - *Real*: Reduktion des Netzes auf „bekannte Seiten“
  - Leicht merkbare **URLs** als entscheidender Vorteil



# Mittlerfreie Kommunikation

- Triviale Lösung
  - *Alle haben alles*
  - Flood fill und Limitierung durch Kategorien
  - NNTP für **Usenet News**
- Netzaffine Lösung
  - *Semantisches Routing*
  - Mapping von Texten in IPs
  - Query per Multicast, Response per Unicast
  - **Wilder Vorschlag ?**

# Traditionelle Mittler

- Archie
  - **Sammlung** von anonymous FTP Server Inhalten
- Nachschlagewerke
  - Regelmäßiges Telefon**buch** des WWW
  - Strukturierte **Verzeichnisse** von DEC, Altavista
- Aggregatoren
  - Thematische **Linklisten** zu anderen Angeboten
  - Heute in Blogs wichtig (mangels eigener Inhalte?)

# Gute Suche

- Klassische Suchmaschine
  - Verwendet nur **Suchanfrage** für das Ergebnis
  - IP für *Geolokation*: Sprache und Sperren
  - *Anonymität* per Default
  - Individuelle Einstellungen nach *Login / Cookie*
  - Verdienst durch **Anzeigenverkauf** (Adword)
  - Beliebtheit durch *großen Suchindex*

# Böse Suche

- Moderne Suchmaschine
  - **Selbstlernendes** System über **alle** Parameter
    - Suchbegriff, Tippgeschwindigkeit, -fehler, IP, Uhrzeit, ...
    - Korrektur: Wo geklickt, welche Vorschau, Alternativen
  - Beliebtheit durch *Do what I mean*
    - Suchergebnis entspricht dem **Verhaltensprofil**
    - Techniker sehen anderes als Marketing (IPv6 Bits!)
  - Monetarisierung
    - **Personalisierte Anzeigen** anhand des Kontextes
    - *Ads auf Webseiten*: Wie eine Suche ohne Suchbegriffe

# Böse Portale

- Soziale Netzwerke
  - Umfassende **Erfassung** persönlicher Daten
  - **Abwicklung** persönlicher Kommunikation
  - Monetarisierung
    - Verkauf von **Anzeigen** anhand von *Nutzerprofilen*
    - Zentralisierte **Zahlungsabwicklung** für *Gimmicks*
  - Nutzer haben „Kneipenfeeling“
    - Anzeigen lästig wie der „Rosenverkäufer“

# Vision für soziale Netzwerke

## IPv4

- Daten hochladen auf **Portal**
- Zugriffsberechtigungen nach **Portalvorgabe**
- Interaktion der Nutzer durch **Portalprogramm**
  - Werbung einblenden
  - Attraktivität per Nutzerzahl
- Zentralisierung auf wenige große Portale

## IPv6

- Daten durch **Nutzersystem** veröffentlicht (always on)
- Zugriffssteuerung und Löschung durch direkte **Nutzereinstellung**
- Interaktion über direkten (Web2.0) Zugriff auf andere **Nutzersysteme**
- Viele Softwareanbieter durch Interoperabilität

# Neue Soziale Netze

[en.wikipedia.org/wiki/Distributed\\_social\\_network](http://en.wikipedia.org/wiki/Distributed_social_network)

## Persönliche Wunschliste

- *Webseiten* als typische (RSS-)Datenquelle
- Freie Editorwahl: *Standard Webtools*
- Server leichtgewichtig genug für *IPv6-CPEs*
- Struktur *optional* per FOAF, nicht proprietär
- Dezentrale Suche per *Multicast*

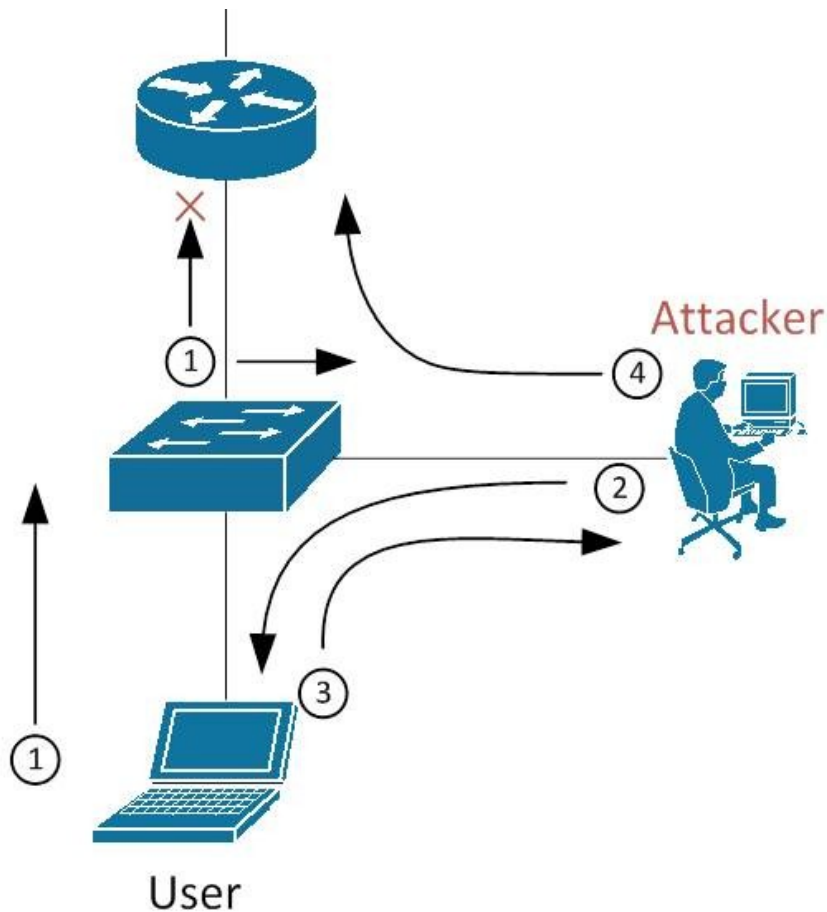
# IPv6 statt Zuckerberg

Es bedarf Druck auf Provider und Hersteller für *datenschutzkonforme Lösungen*, die **Visionen befördern**



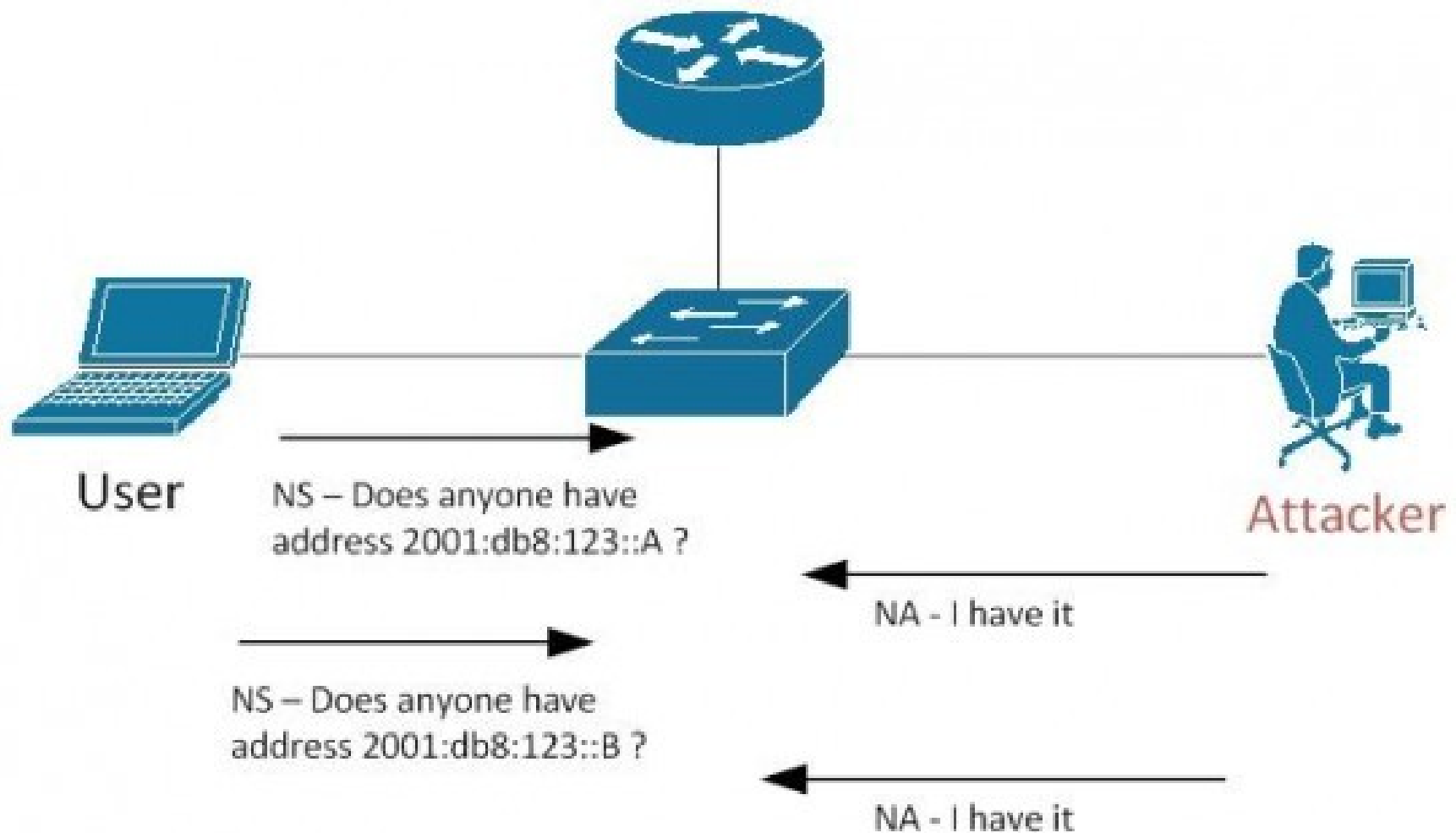
Cool Stuff  
Crypto Adressen

# Als Router ausgeben

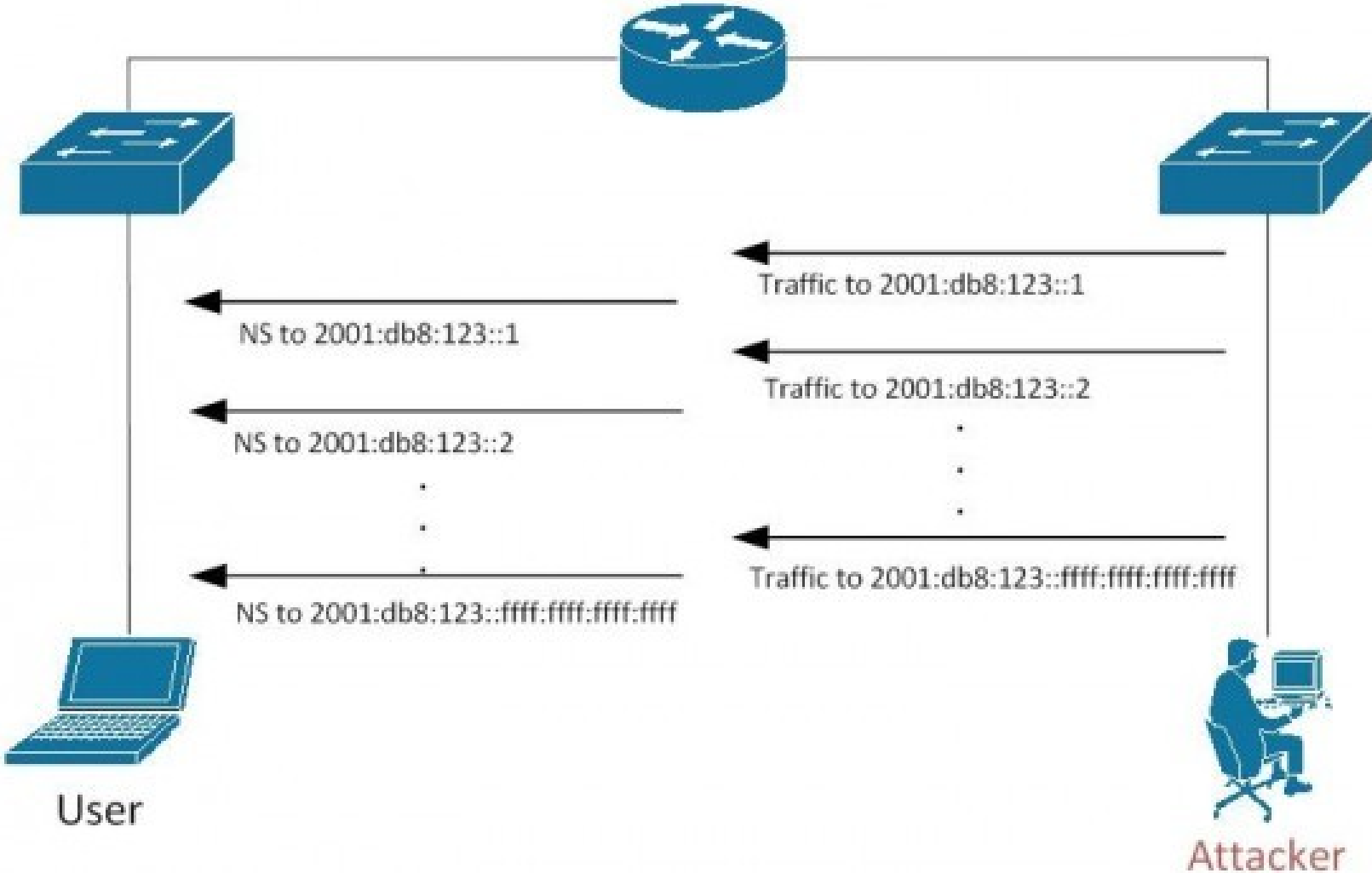


- 1) Router Solicitation
- 2) Router Advertisement
- 3) intercepted data
- 4) reinjected data

# Andere Gerät übernehmen



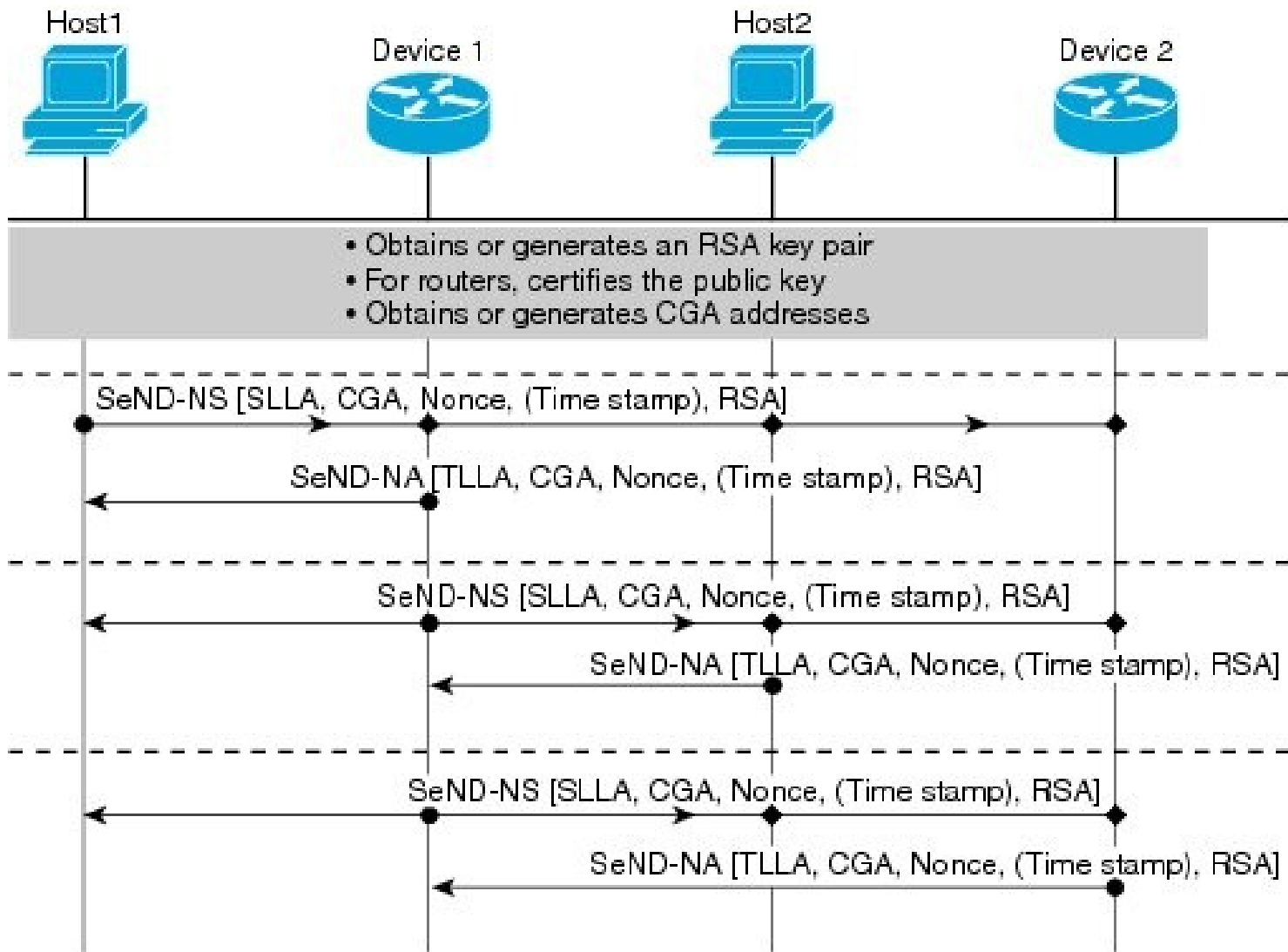
# Caches überlaufen lassen



# Cryptographically Generated Address

- Hostanteil der IPv6 Adresse als Token
  - Quelladresse ist Hash über public Key und Nonces
  - Pakete sind signiert mit privatem Schlüssel (Header)
  - Eigentlich nur 59bit nutzbar → Doppelter Hash
  - Effektiver Schutz:  $O(2^{59+16*s})$  mit s als Securityparameter
  - Test auf doppelt vergebene IP
- Pakete nicht mehr spoofbar
- Verwendung bei SeND
  - Schutz vor spoofenden Angreifern existierender IPs
  - Kein Schutz vor neuen Adressen des Angreifers

# SeND



Cooler Kram  
Mobilität

# Techniken im Vergleich

Anforderung	IPv6	VPN	DirectAccess	Mobile IPv6
Zugriff Internet	Ja	Split-Tunnel	Ja	Ja
Zugriff Intranet	Firewall	Ja	Ja	Ja
Feste Client IP	Nein	Im LAN	Im LAN	Ja
Nutzer bekannt	Nein	Ja	Ja	Nein
Automatisch an	Ja	Nein	Ja	Ja
Effizienter Datenfluss	Ja	Nein	Nein	Ja
Unterbrechungsfrei	Nein	Nein	Nein	Ja
Moderner Server	Ja	Nein	Ja	Ja
Legacy Server	Nein	Ja	NAT64	Nein
Moderner Client	Ja	Nein	Ja	Ja
Public Legacy Client	6to4	Ja	6to4	6to4
Private Legacy Client	Teredo	NAT-Traversal	Teredo	Teredo



# Mobile IPv6 – unterwegs daheim

- Sicherstellen der Erreichbarkeit
  - Anrufe auf die Firmennummer sollen immer den richtigen Mitarbeiter erreichen
- Netz stellt die Erreichbarkeit sicher
  - Nur noch Handys erlaubt
- Mitarbeiter meldet sich mit aktueller Nummer
  - Sekretariat stellt Anrufe durch
  - Mitarbeiter gibt aktuelle Nummer weiter

# Mobile IPv6 – Annahmen

- Native IP-Adressen sind regional verschieden
  - Trotz Roaming sollen Verbindungen bleiben
- IP Routing ist sicher und geht nur nach Ziel
  - Sicherheit nicht besser als ohne Mobilität
  - Feste System-Adresse auch Mobil erreichbar
- Ende-zu-Ende statt Änderungen am Netz
- Mobiles Gerät nur daheim vorab bekannt
- Hauptgefahren: Mobiler MitM, Flooding

# Mobile IPv6 – Meld' Dich An

- MN sucht HA: „Wer macht Sekretariat?“
  - Dynamic HA Discovery per ICMP Anycast
  - *Eine* Antwort mit Liste aller HA
  - Alternativ Autoconfig im LAN, H-Bit
- MN bereitet Weggang vor: Hinterläßt Kennung
  - Vereinbarung einer IPSec SA für ESP (manuell)
- MN am Ziel: Hinterlegt neue Nummer
  - BindungsUpdate per IPSec mit CoA

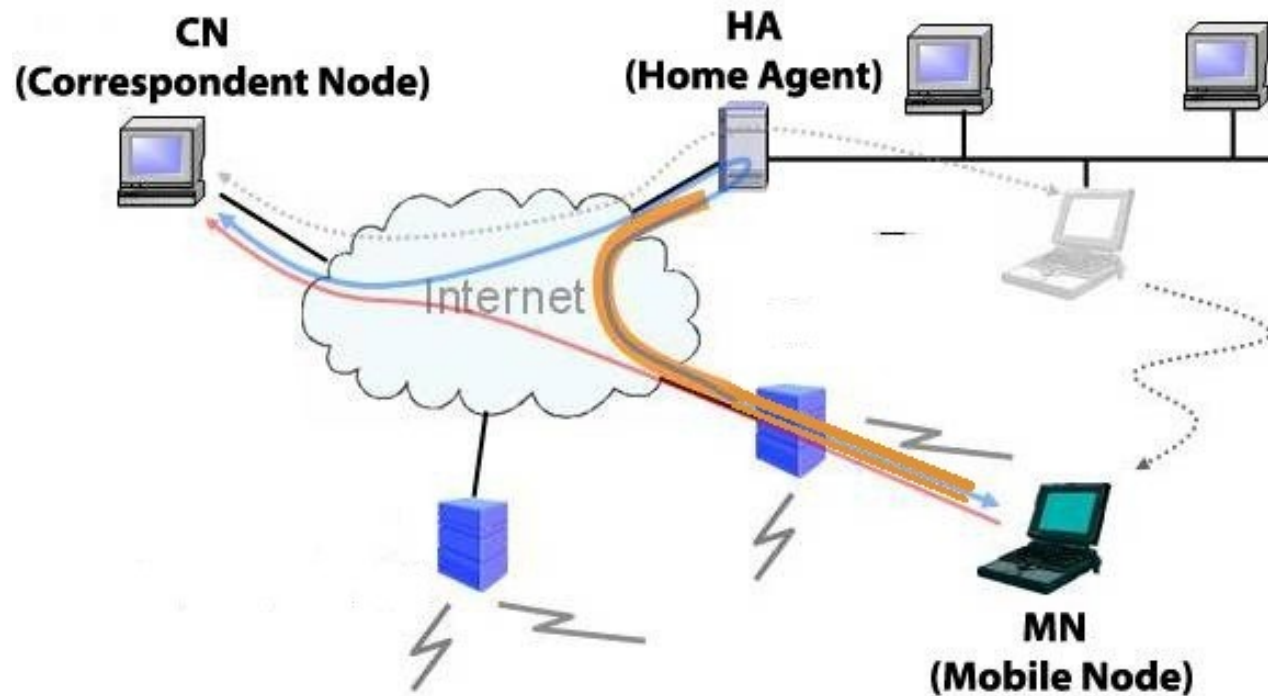
# Mobile IPv6 – ineffizient arbeiten

- HA simuliert MN im Heimnetz
  - Nimmt alle Kommunikation von CN an
  - auch Link Local und Multicast!
- HA leitet abgefangene Daten an MN
  - Verschlüsselt und authentisiert mit ESP
- MN antwortet klassisch
  - Verschlüsselt und authentisiert per ESP
- HA sendet getunnelte Daten klassisch an CN

# Mobile IPv6 – effizient arbeiten

- MN informiert CN über direkte Erreichbarkeit
  - CN würde die Information anzweifeln
- MN informiert CN auf beiden Wegen
  - Direkt mit CoA und via HA
- CN antwortet mit geteiltem Geheimnis
  - Direkt an CoA und via HA
- MN baut Geheimnis zusammen, sendet BU
  - Direkte Kommunikation zwischen MN und CN

# Mobile IPv6 – Datenfluss



<http://www.youtube.com/watch?v=N2kvPCwJkLU>

# Mobile IPv6 – Mit fremden Federn

- Routing Header (2)
  - Alle Applikationen sehen nur Heimatadresse
  - Nutzung von Ingress Filter da topologisch korrekt
  - Erlaubnis trotz Verbots von Source Routing (RH0)
- Alternative CoA bei Topologieproblemen
- Kaum State auf CN, da Indizes in Noncetabelle
- Aktualisierung der Bindung kurzfristig möglich
  - Kein Return Routability Test nötig, nur ein Paket
  - Häufige Updates, Bindung nur für Minuten

# Mobile IPv6 – Veränderungen daheim

- Wechsel des HA: „Vertretung im Sekretariat“
  - Dynamic HA Discovery -> Neuer HA
- Renumber: „Wechsel des Dienstleisters“
  - Regelmäßiger BU beim HA enthält Umzugshinweis
  - Dynamic Prefix Discovery -> Neue Heimatadresse
  - Parallelbetrieb möglich
- Returning Home Konflikt: „Wer ist wer?“
  - Rückmeldung per Multicast, dann erst Übernahme



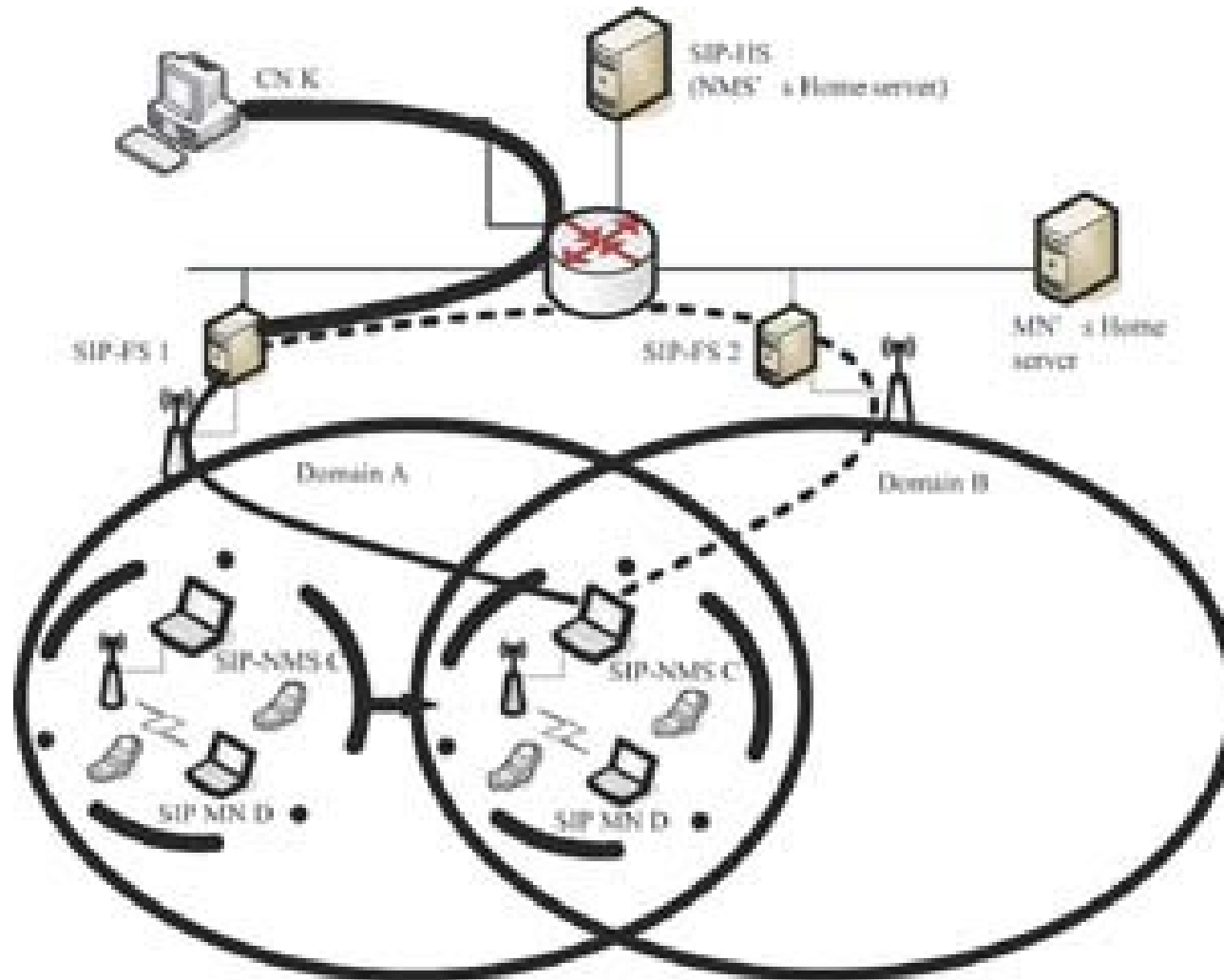
# Mobile IPv6 – Standortwechsel

- Bei Wechsel der IP Anbindung (neuer Prefix)
  - Schnelle Umschaltung durch 1-Paket BU
  - Neuer Return Routability Test: sechs Zyklen
- Verbindungen reißen nicht ab
  - CoA nicht für Applikationen sichtbar
- Umschaltzeiten hängen von Layer 2 ab
  - Kein Netz, keine Daten
  - Neues Netz schnell detektieren, Altes lange halten
  - Router Announcements alle 50ms statt alle 2min?

# Fast Mobile IPv6 – Schnelle Wechsel

- MN fragt alten Router nach direkten Nachbarn
- MN wählt neuen Router, z.B. anhand Stärke
  - Fast BU an alten Router, authentisiert mit SEND (CGA)
- Router informieren sich über den Wechsel
  - Duplizieren Datenverkehr zum neuen Router
- MN wechselt die Netze
  - Neue L3 Adressen, BUs an HA und CNs
- MN informiert neuen Router über Abschluß
  - Quertraffic zwischen Routern erstirbt

# Mobile IPv6 – Schnelle Wechsel



# HMIPv6 – Türme im Netz

- Verstecken der Mikromobilität
  - MN lernt vom Router regionale Gateways (MAP)
  - MN bindet sich lokal und den MAP global
  - Roaming innerhalb des MAP-Bereichs sehr schnell
- MAP fungiert als Proxy für MN
  - CoA des MN nicht mehr extern sichtbar
- MN kann sich bei mehreren MAP melden
  - Topologie bzgl. CN bestimmt Nutzung

# Mobile IPv6 – Firewall Nightmare

- MIPv6 Support praktisch vernachlässigbar
- Firewall vor MN
  - ESP Traffic eingehend verboten, HA evtl. möglich
  - Spontaner Verbindungsaufbau durch CN verboten
  - Route Optimization generiert stateless Traffic
  - Roaming zu anderer Firewall: MN stateless
- Übungsaufgabe: Firewall vor HA oder CN
- Lösungen?

# Mobile IPv6 – praktische Probleme

- Replay Angriffe verhindern mit IKE
- Mobilität in vertrauenswürdigen Netzen
  - IPSec viel zu teuer: Einfache Authentifizierung
- HA Downtime, Überlast, Renumber
  - Proaktive Signalisierung vom HA an den MN
- Mobile IPv6 fähige Anwendungen: API
- Multicast: IPTV (restricted access)
- Datenschutz bzgl. MN: Lokation möglich
  - Heimadresse oder CoA verstecken (topologisch)

# Mobile IPv6 – praktische Probleme

- FMIP pro 802.11, 802.16 (WIMAX), 3G, ...
  - 802.21 – Media independent Handover
- Roaming zu langsam
  - Preshared Key zwischen MN und CN
  - CN und HA Ummeldungen gleichzeitig
  - Paralleler Netzzugriff und multiple CoA
  - Temporärer Fallback auf HA allein
  - Datenversand auf Kredit durch CN
  - Kryptographische Adressen mit Authentikator

# Mobile IPv6 – praktische Probleme

- Standard zu starr für Entwicklungen
  - Proprietäre Vendor Options
  - Experimentelle Protokolle
- Einfacheres Bootstrapping: AAA statt Manuell
  - MN eindeutig identifizieren (ISMI, FQDN, ...)
  - Support für multiple Provider, Zertifikate, ...
- Betrieb mehrerer Mobilitätsprovider
  - Auswahl nach angebotenen Services: voip, im, ...
- Ressourcenlast des MN im Fremdnetz
  - 802.1x Authentisierung durch ISPs zum Heimnetz



# Mobile IPv6 – praktische Probleme

- NASA/Boeing: Nutzbarkeitsstudie (RFC 5522)
  - Untersuchungen in Flugzeugen mit VDL 2
    - In der Luft alle 30-60min Handover
    - „Up“-Bandbreite nur 1% der „Down“-Bandbreite
    - Anforderungen an Latenz, Verfügbarkeit, Overhead
    - Route Optimization zwingend nötig
  - Zukunft
    - 802.16: Boden, P34, LDL: Land, Satcom: Ozean
    - Internet und VoIP für Passagiere

# NEMO – Netze auf Reisen

- MN wird Mobile Route mit (Sub)Netz
  - Systeme im mobilen Netz merken gar nichts
- Roaming durch mobile Netze
  - Beliebige Verschachtelung von MR
  - MN funktionieren auch hinter NEMO
- Bidirektionaler Tunnel zwischen HA und MR
  - Keine Route Optimization
- Multihoming und Location Privacy
- IPv4 und NAT-Traversal

# Proxy Mobile IPv6

- Mobilität als Aufgabe des Netzwerkes
  - Endknoten haben trotz Roaming feste Anbindung
  - Netzwerk stellt mobiles Heimnetz bereit
  - Keine Unterstützung bei den Endknoten nötig
  - Mehrere Netzwerke pro Gerät möglich
  - Viele Features (ECN) durch homogene Technik
- Nur noch ein zentraler HA pro PMIPv6 Domain
- Kein Roaming zwischen PMIPv6 Domains
  - Separate Authentisierung und Provisionierung

# Standards



- RFC 4225; Mobile IPv6 Design; 2001–2002
- RFC 3775; Mobility Support in IPv6; June 2004
- RFC 3776; Home Agent IPsec; June 2004
- RFC 3963; NEMO Basic Support; January 2005
- RFC 4260; 802.11 Fast Handover; November 2005
- RFC 4283; MN Identifier Option; November 2005
- RFC 4285; Authentication Protocol; January 2006
- RFC 4449; Shared Data for CN-BU; June 2006
- RFC 4487; MIPv6 and Firewalls; May 2006
- RFC 4584; Socket-API for MIPv6; July 2006

# Standards



- RFC 4866; Enhanced Route Optimization; May 2007
- RFC 4877; Mobile IPv6 with IKEv2; April 2007
- RFC 4882; MIPv6 Location Privacy; May 2007
- RFC 4885; NEMO Terminology; July 2007
- RFC 4886; NEMO Goals; July 2007
- RFC 4887; NEMO Home Network Models; July 2007
- RFC 4908; Multihoming with NEMO; June 2007
- RFC 5026; MIPv6 Bootstrapping; October 2007
- RFC 5094; MIPv6 Vendor Specific Option; December 2007

# Standards



- RFC 5096; Experimental Messages; December 2007
- RFC 5142; Home Agent Switch; January 2008
- RFC 5149; Service Selection; February 2008
- RFC 5213; Proxy Mobile IPv6; August 2008
- RFC 5269; FMIPv6 Security; June 2008
- RFC 5270; FMIPv6 over 802.16e; June 2008
- RFC 5271; FMIPv6 over 3G CDMA; June 2008
- RFC 5380; Hierarchical MIPv6; October 2008
- RFC 5447; Diameter MIPv6 NAS; February 2009

# Standards



- RFC 5555; Dual Stack Mobility; June 2009
- RFC 5568; MIP6 Fast Handovers; July 2009
- RFC 5677; IEEE 802.21 Mobility; December 2009
- RFC 5678; DHCPv6 Mobility Service; December 2009
- RFC 5679; DNS Mobility Service; December 2009
- RFC 5726; MIP6 Location Privacy; February 2010
- RFC 5757; Mobile Multicast Problem; February 2010
- RFC 5778; Diameter MIPv6 HA; February 2010
- RFC 5779; Diameter PMIPv6; February 2010