

Internet Protocol

1. IPv4

- 1.1 Adressierung
- 1.2 Subnetting
- 1.3 Datagramm-Aufbau
- 1.4 Fragmentierung
- 1.5 Kontrollprotokoll
- 1.6 Adressabbildung, DHCP

2. IPv6

- 2.1 Motivation + Übersicht
- 2.2 Adressierung
- 2.3 IPv6 Paketformate
- 2.4 Autokonfiguration
- 2.5 Weitere Eigenschaften
- 2.6 Migrationsszenarien

Zum Inhalt

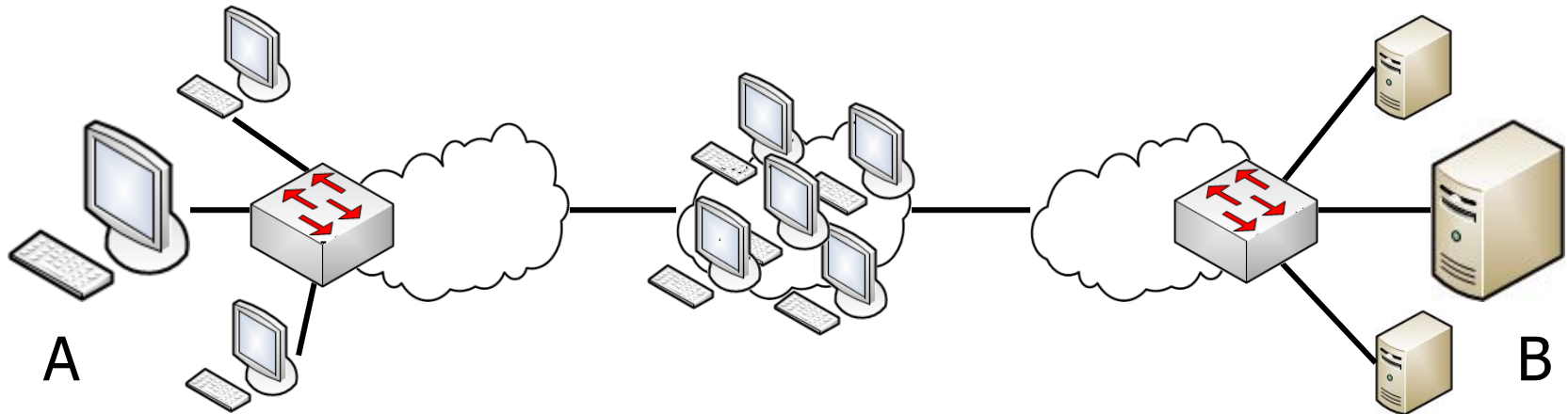
Dieses Kapitel stellt IP, „das“ Protokoll der Internet-schicht vor, welches nicht nur die Teilnetze untereinander zusammenhält, sondern auch allen Anwendungen erlaubt, alle Netzwerktechnologien einfach zu benutzen. Allerdings gibt es inzwischen mehrere Internetprotokolle: IPv4 und IPv6 – darauf müssen wir achten, wenn unsere Netzwerke & Programme weiterfunktionieren sollen.

Das zugehörige Kapitel im Tanenbaum ist 5. Vollständiger finden Sie den Inhalt im Bonaventure finden Sie die Inhalte in Teil 2.



1. Die Netzwerkschicht IP

- Bildet ein „Inter-Netzwerk“ zwischen LANs, MANs und WANs unterschiedlicher Technologien:
Universelles Paketformat mit einheitlichen Adressen

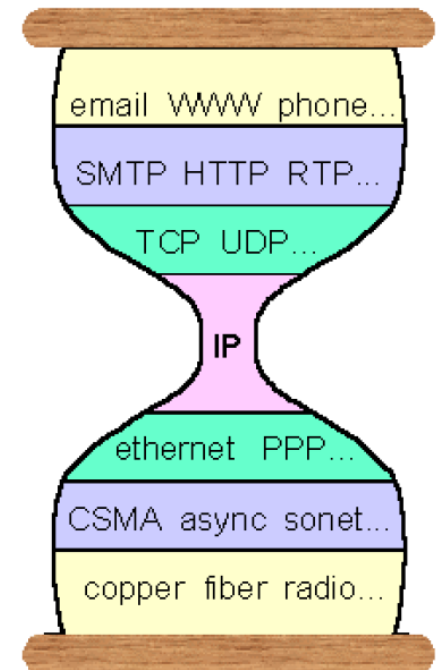


- Findet Wege und leitet Pakete zwischen Rechnern:
Routing und Forwarding



1. Aufgaben von IP

- Protokolldienst für einen verbindungslosen Datentransfer zwischen Rechnern und Netzen
- Inter-Networking: „Das verbindende Element“
- Regelt Paketverarbeitung und Fehlerbehandlung
- Legt das Format von Paketen fest
- Zerteilt Pakete bei Bedarf
- Spezifiziert das Internet Routing
- Ist festgelegt in RFC 791



1.1 Adressierung im Internet

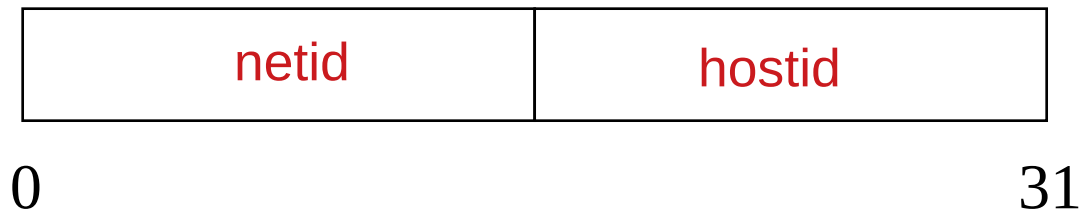
Anforderungen:

- Kompakt
- Universell (egal ob Host oder Gateway)
- Hardwareunabhängig (logische Adressierung)
- Automatische Abbildung von Hardwareadressen
- Unterstützung einer effizienten, dezentralen Wegefindung



1.1 Adressierungs-Schema

- Jeder Host hat eine 32-bit Adresse:
die **IP Adresse**
- Die Adresse ist hardwareunabhängig
- Die Adresse gliedert sich in zwei Teile:



1.1 Bestandteile der IP-Adresse

- **netid:** Netzwerkadresse als Prefix
 - alle Hosts in einem Netzwerk haben dieselbe netid
 - diese ist weltweit eindeutig und wird vom LIR zugeteilt
- **hostid:** Host-Adresse als Suffix
 - eindeutig in einem Netzwerk
 - wird vom lokalen Administrator eingestellt

Achtung: Adressen bezeichnen Netzwerkverbindungen!

Ein Gateway hat so viele Adressen, wie es Netzwerke verbindet.



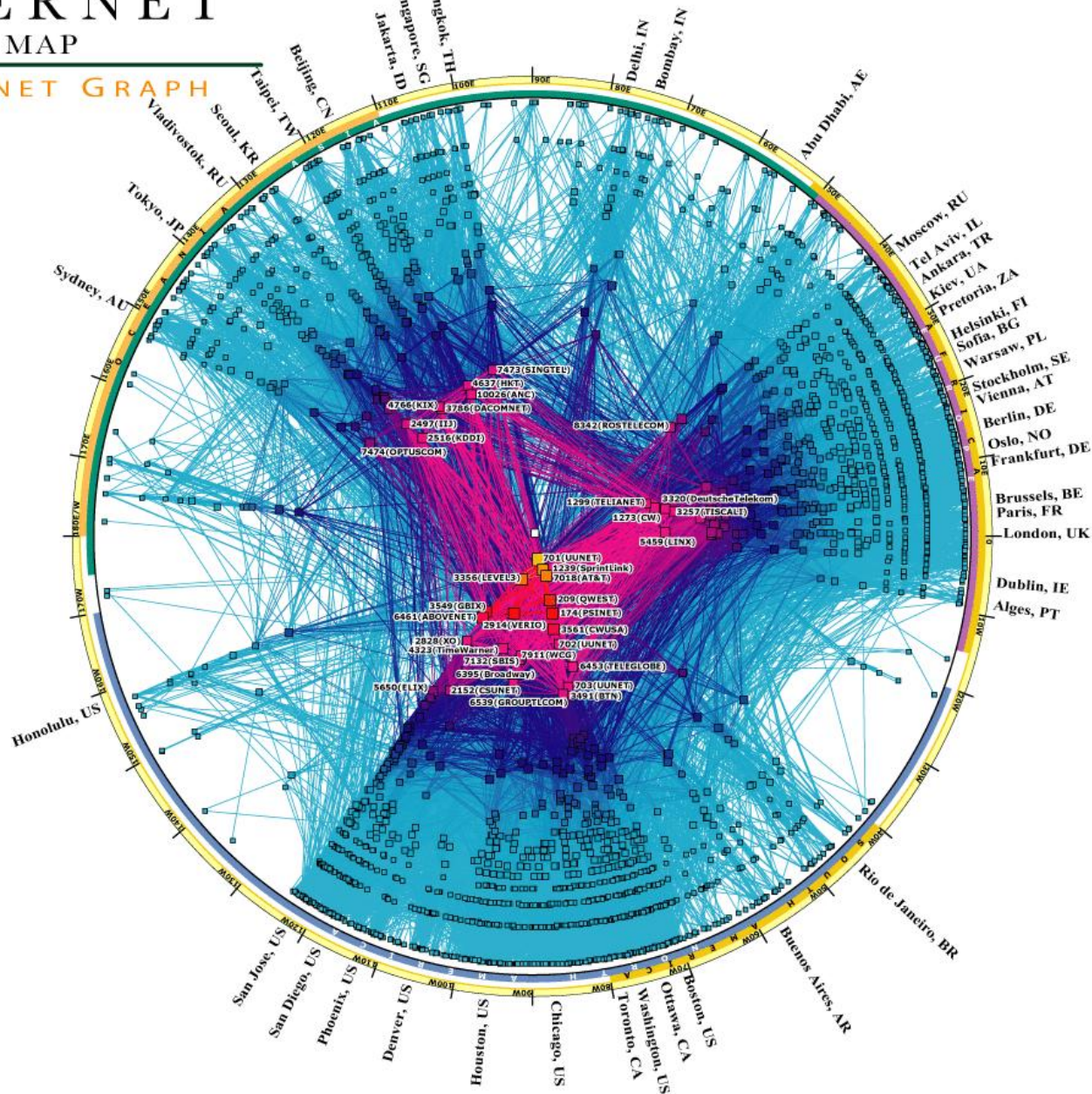
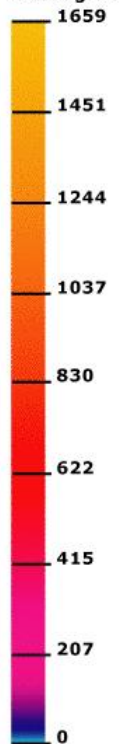
IPv4 INTERNET

TOPOLOGY MAP

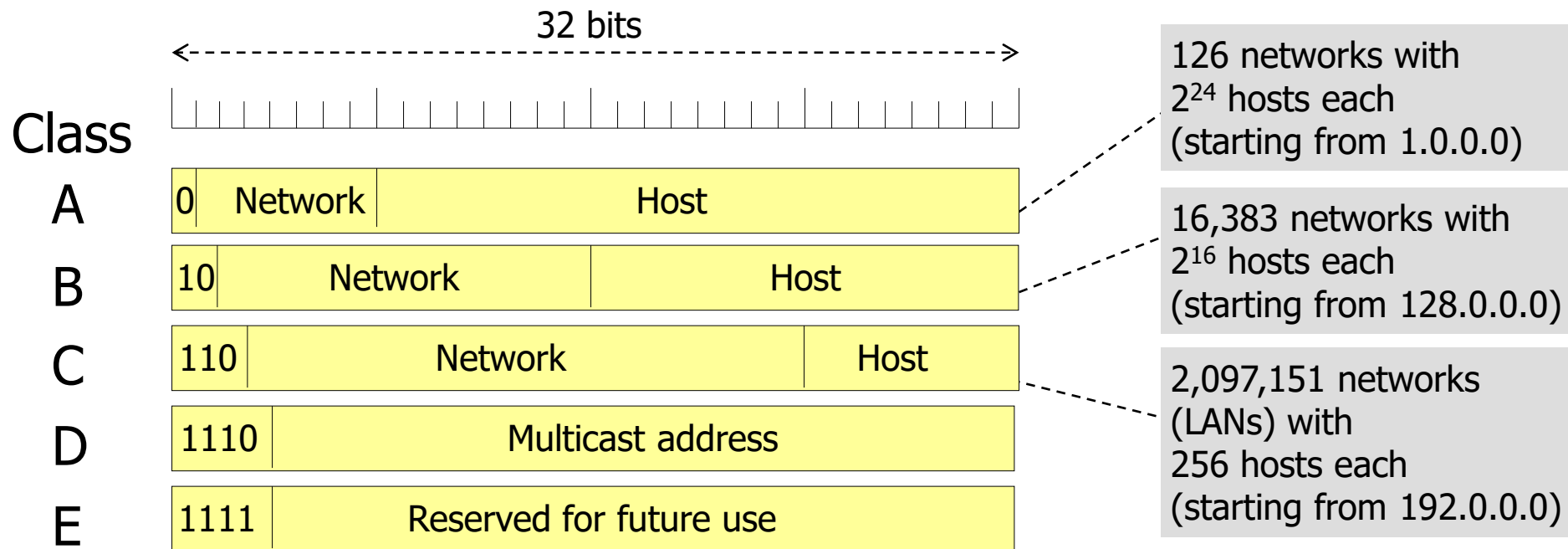
AS-level INTERNET GRAPH

copyright © 2005 UC Regents. all rights reserved.

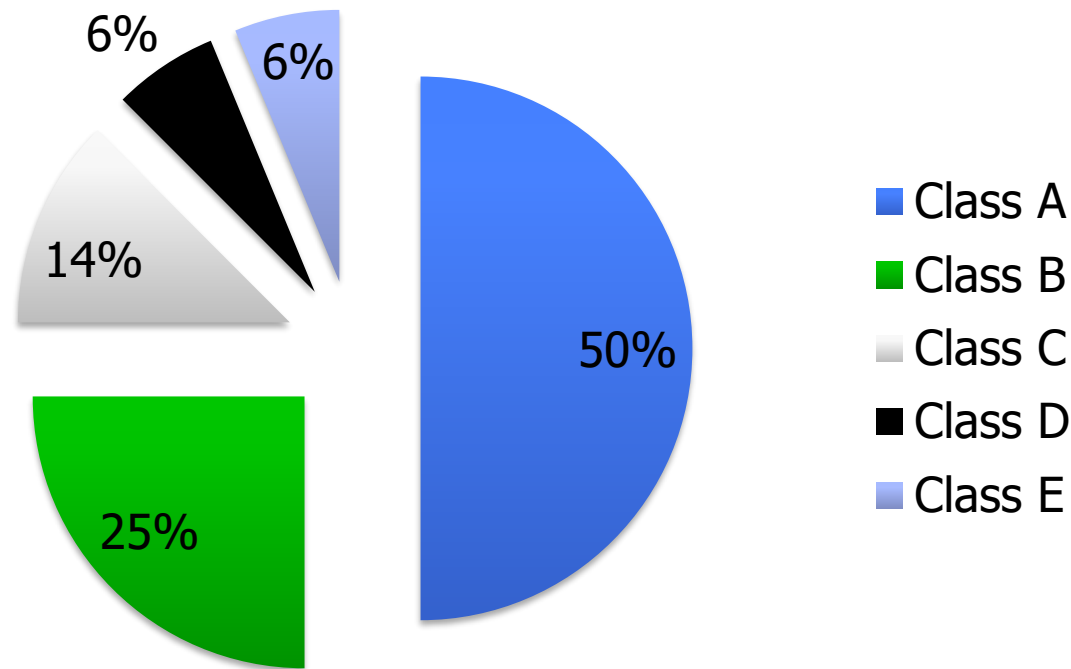
Peering:
OutDegree



1.1 Ursprüngliches Klassenkonzept der Internet-Adressierung



IPv4 Adressraum per Adressklasse



1.2 Subnetze

Adressierung von Subnetzen erweitert die Internet Adressierung (RFC 950):

- Ermöglicht eine einzelne Netzwerk Adresse auf verschiedene (physikalische) Netzwerke aufzuteilen
- Unterteilt den **hostid**-Anteil einer Adresse in
 - **subnetid**: (nachgeordnete Netzwerkadresse)
 - **hostid**: (Rechneridentifikation)

Subnetze werden von lokalen Gateways und Hosts interpretiert, nach außen jedoch wie eine normale Adresse behandelt.

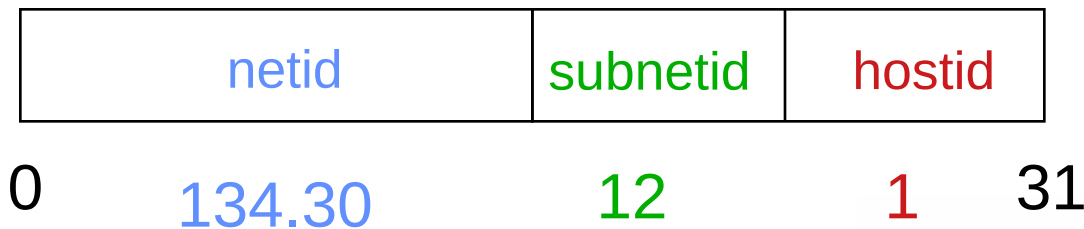


1.2 Internet im Internet

Gründe zur Subnetzbildung:

- Einfacherer Aufbau von Routing-Tabellen
- Verringerung von Broadcasts
- Abgrenzung von Rechnerbereichen (Sicherheit)
- Delegation von Administration

Bsp:



1.2 Notation der IP-Adresse

- IP-Adressen werden in der sog. **Dotted Decimal Notation** notiert, jedoch binär interpretiert:

- Bsp:

Dotted Decimal: 128.10.2.30

Binär: 10000000 00001010 00000010 00011110

Netid Subnetid Hostid



1.2 Subnetzmaske

Subnetze werden durch sog. Subnetzmasken bekanntgegeben: Diese kennzeichnet den der Netzwerkadresse zuzuordnen Adressteil in Form eines logischen AND-Filters

Bsp:

Adresse: 128.10.2.30 = 10000000 00001010 00000010 00011110

Netzmaske: 255.255.255.0 = 11111111 11111111 11111111 00000000

Host-ID: 30 = 00011110

Host-ID ohne 2.30 = 00000010 00011110

Subnetzmaske

Netzmasken werden in UNIX-Systemen mit dem Kommando **ifconfig**,
in Windows-Systemen mit **ipconfig** bzw. **netsh** verarbeitet.



IPv4 Addressierung: Variable-Length Subnet Masking

- Problem: Ineffiziente Adressnutzung durch Klassen
 - Class C Netzwerke (256 hosts) sind zu klein, Class A und B (65,536 hosts) Netzwerke zu groß
- Lösung: Variable-Length Subnet Masking (VLSM)
 - Ersetze statische Klassen durch variable Präfixe
 - IP Adressen tragen Präfixlänge: a.b.c.d/n
 - Die ersten n bits identifizieren das Netzwerk
 - Beispiel: 147.250.3/17

10010011.11111010.00000011.00000000

Network ID

Host ID

- VLSM ist die Basis für CIDR (Classless Inter-Domain Routing)



1.1 Spezielle Adressen

Einige Adressen im (Sub-)Netzwerk sind für spezielle Aufgaben reserviert:

- Alle bits = 0 bedeutet „dieser Host, dieses Netzwerk“
Bsp: 0.0.0.7 ist Host 7 in diesem Netzwerk
Bsp: 134.15.0.0 bedeutet „dieses (Class B-) Netzwerk“
- Alle bits = 1 bedeutet „Broadcast an alle“
Bsp: 255.255.255.255
- Hostid bits = 1 bedeutet „selected Broadcast“
Bsp: 134.15.255.255 oder 134.15.7.255
- 127.0.0.1 ist reserviert für das Loopback-Interface



1.2 Private Adressen

Werden willkürliche, ‚illegale‘ Adressen für den privaten IP-Bereich verwendet, so können diese legal nicht mehr angesprochen werden.

Deshalb gibt es reservierte ‚private Netzwerkadressen‘, die nie geroutet werden:

- | | |
|---------------|-------------------|
| - 10.0.0.0 | - 10.255.255.255 |
| - 172.16.0.0 | - 172.31.255.255 |
| - 192.168.0.0 | - 192.168.255.255 |



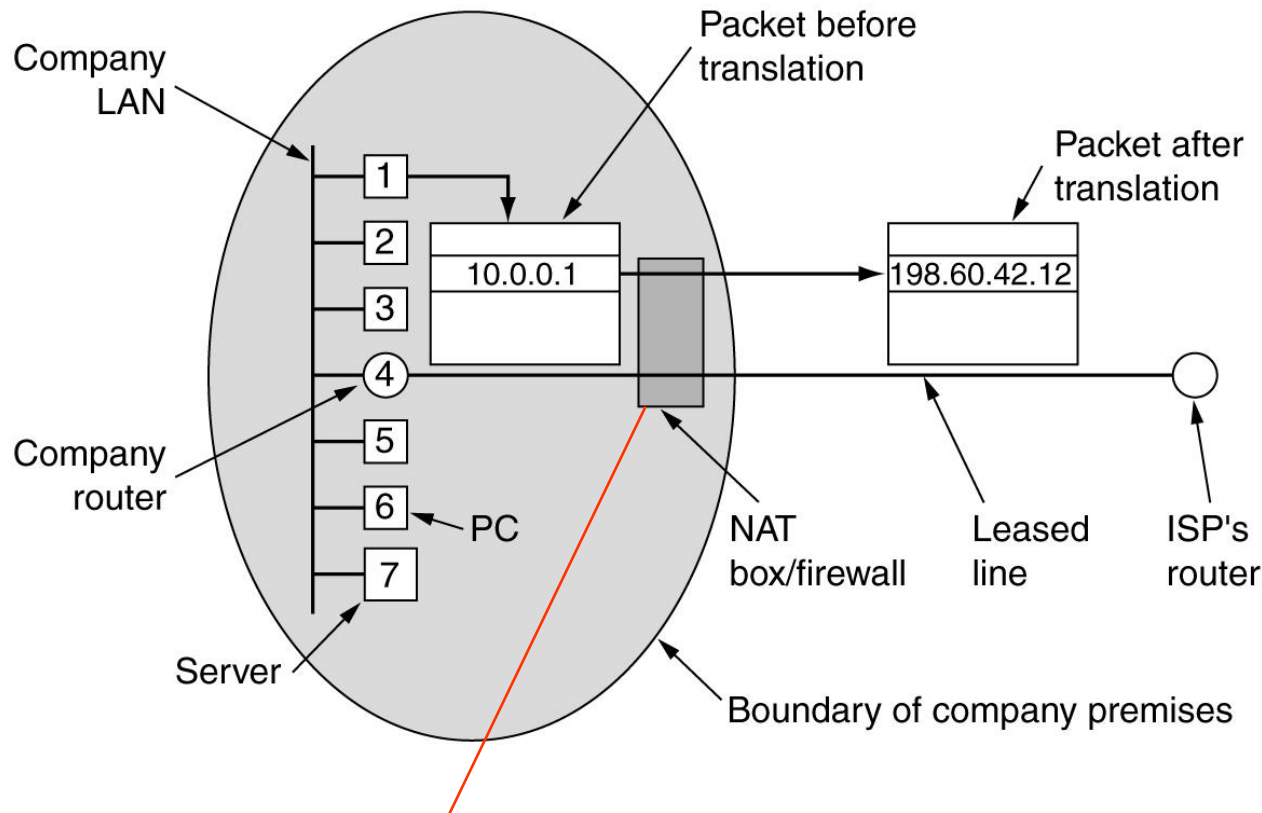
1.2 Private Netzwerke

Aufgrund der Knappheit von IP-Adressen oder aus Sicherheitsgründen können interne Netze mit ‚privaten‘ IP-Adressen versorgt werden:

- Ein zentrales Gateway (mit einer offiziellen Adresse) schreibt hierfür private Adressen in legale Datenpakete um. Hierfür existieren zwei Verfahren:
 - Network Address Translation (NAT)
 - Port Address Translation (PAT)
- Rechner/Dienste, welche nicht im Gateway konfiguriert sind, werden dabei von ‚außen‘ unerreichbar.



1.2 Network Address Port Translation (NAPT)



Protocol	Port (local)	IP (local)	Port (global)	IP (global)	IP (destination)	Port (destination)
TCP	1066	10.0.0.1	1066	198.60.42.12	147.216.12.221	21
TCP	1500	10.0.0.7	1500	198.60.42.12	207.17.4.21	80

1.3 IP Datagramme

Die Grundeinheit für den Internet Transfer von Daten ist das

IP Datagramm

Es besteht aus:

- Header mit Source- und Destination-Adress, ...
- Datenteil (Payload)

Datagramme werden von der Netzwerk-Software verarbeitet, sie benötigen keine spezielle Hardware



1.3 IP Datagramm Format

IP-Protokollkopf

1	4	8	16	19	24	32
Version	Länge	Servicetypen	Paketlänge			
Identifikation				D F	M F	Fragmenabstand
Lebenszeit		Transport	Kopfprüfsumme			
Senderadresse						
Empfängeradresse						
Optionen					Füllzeichen	

1.3 Felder des IP Protokollkopfs

Version: IP-Version (hier 4)

Länge: 32-bit Worte des Protokoll*kopfs* – default 5, länger durch Optionen

Paketlänge: Gesamtlänge des Pakets in Bytes ($< 2^{16}$)

Lebenszeit: Höchstzahl der IP Hops bei Paketbeförderung

Transport: Nachfolgendes Protokoll, i.d.R. Transport

Identifikation: ID für mögliche Fragmentierung - vom Absender vergeben

Flags: DF = don't fragment
MF = more fragments

Fragmentabstand: Relative Fragmentposition

Prüfsumme: nur IP Header

Optionen: Variable Erweiterungen für Spezialaufgaben, z.B. Source Routing



1.3 Servicetypen

- Definiert Qualitätsklassen bei der IP Paketverarbeitung (auch DiffServ Feld genannt):

Bits	Wert=0	Wert=1
0 - 2	Priorität	
3	Normale Wartezeit	Niedrige Wartezeit
4	Normaler Durchsatz	Hoher Durchsatz
5	Normale Zuverlässigkeit	Hohe Zuverlässigkeit
6 - 7	Reserviert	



1.3 Type of Service / Quality of Service

- Internet Datagramme werden gem. ‚best effort‘ - Prinzip ausgeliefert
 - Das TOS - Feld klassifiziert Pakete, keine (Daten-) Flüsse
- ⇒ Services können priorisiert, nicht garantiert werden

Service
Charakteristika:

Application	Low delay	High throughput	High reliability	Low cost
Telnet	⊗			
ftp (data)		⊗		
SNMP			⊗	
NNTP				⊗

1.3 Größe von Datagrammen

Die **Maximum Transfer Unit (MTU)** gibt die (medienabhängige) Maximalgröße von IP-Datagrammen an

Beispiel (Bytes):

► FDDI	4500
► Ethernet	1500
► IEEE 802.3	1492

IP Datagramme müssen kleiner/gleich der MTU des Netzwerks sein
Große MTU nutzen das Medium besser aus
aber: hoher Datenverlust bei Störungen

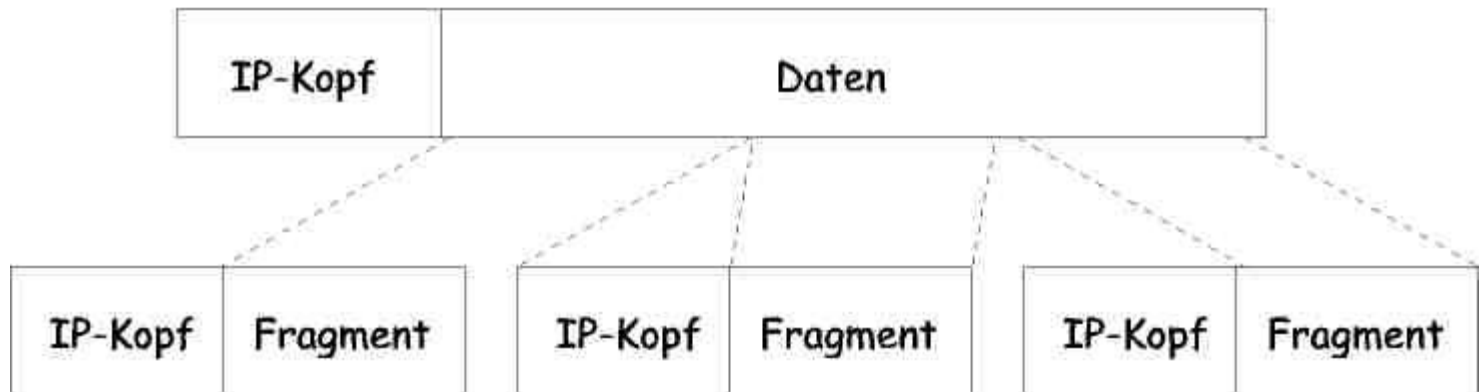


1.4 Fragmentierung von Datagrammen

Problem: IP-Datagramm größer als MTU

Lösung:

Fragmentierung eines IP-Pakets



Fragmentierung erfolgt am Router, Defragmentierung im Zielsystem

1.4 Ablauf einer Defragmentierung

- Beim Eintreffen des ersten Fragments im Ziel wird ein Timer gestartet
- Sind nach Ablauf des Timers noch nicht alle Fragmente eingetroffen, wird die unvollständige Nachricht verworfen (typischer Wert: 30 s)
- Eine Sendewiederholung muß von höheren Schichten (TCP) veranlaßt werden
- Fragmentinformationen im Header:
 - offset
 - identification, flags
 - MF = 0 identifiziert letztes Fragment



1.5 Kontrollfunktionen beim Versenden von Datagrammen

IP Datagramme bieten einen ungesicherten Dienst, d.h.

- Datagramme können verloren gehen
- Datagramme können dupliziert werden
- Datagramme können in ungeordneter Reihenfolge eintreffen
- Datagramme können verändert ankommen

Deshalb werden Mechanismen zur Fehlererkennung und -behebung benötigt:

Auf der IP-Ebene benachrichtigt das

ICMP - Internet Control Message Protocol



1.5 ICMP Messages

- Echo Request - Echo Reply

Überprüfen der Betriebsbereitschaft oder Performance (ping)

- Destination unreachable

Netzwerk, Rechner, Protokoll oder Port sind nicht erreichbar

- Source Quench

Empfänger hat keine Puffer mehr frei

- Redirect

Gateway teilt die IP-Adresse eines besser geeigneten Gateways mit

- Time Exceed

Benachrichtigung über vernichtetes Datagramm (TTL = 0)

- Parameter Problem

- Timestamp Request / Reply

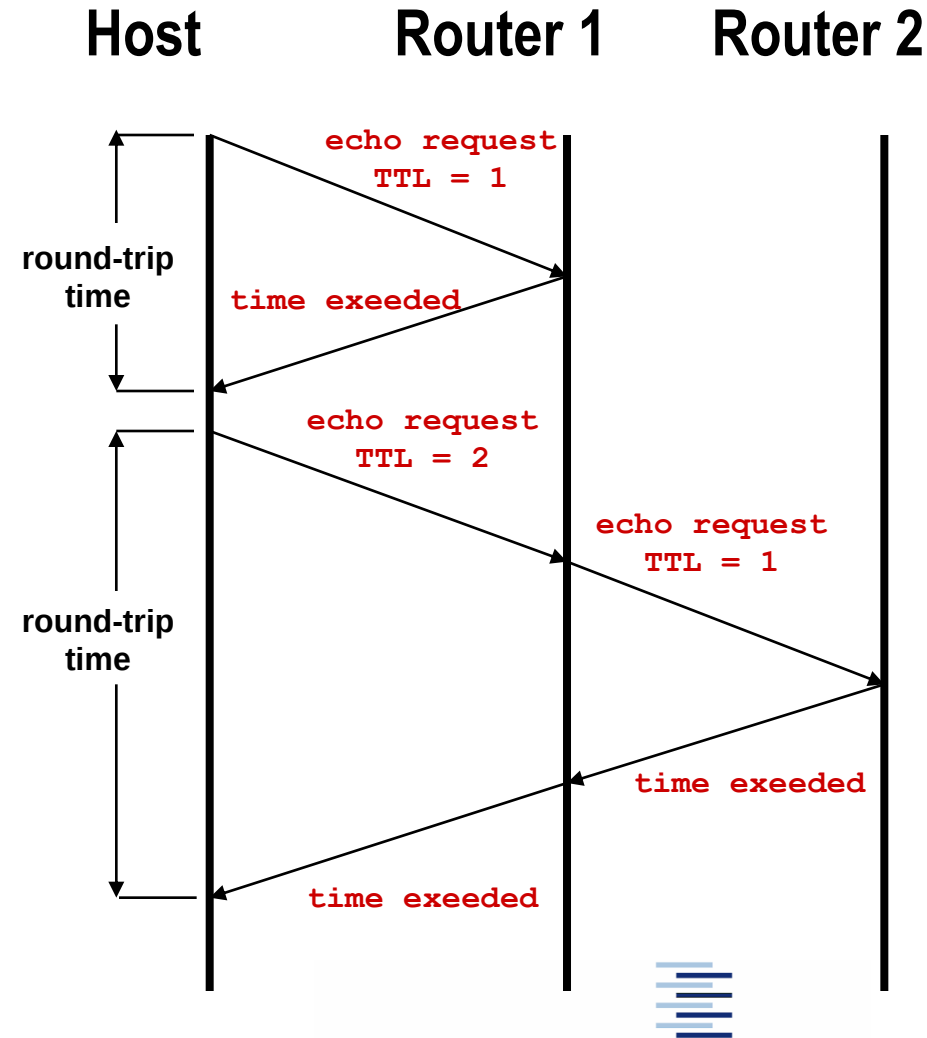


1.5 Beispiel: Jacobsons Traceroute

```

lucifer.rz.fhtw-berlin.de 17%
    traceroute www.hu-berlin.de
traceroute to webmania.rz.hu-berlin.de
(141.20.1.45), 64 hops max,
44 byte packets
 1  mitte004 (141.45.4.1)  0.268 ms
    0.238 ms  0.252 ms
 2  rand004 (141.45.4.2)  0.479 ms
    0.456 ms  0.434 ms
 3  ar-huberlin1-po4-3.g-win.dfn.de
    (188.1.33.101)  1.307 ms
    0.842 ms      0.824 ms
 4  194.94.12.101 (194.94.12.101)
    1.405 ms  0.966 ms  1.150 ms
 5  ER-IKA.mgmt.hu-berlin.de
    (141.20.16.2)      1.861 ms  1.338
ms  1.524 ms
 6  webmania.rz.hu-berlin.de
    (141.20.1.45)      2.414 ms *
1.903 ms

```



1. Forwarding im Internet

Forwarding bezeichnet die Weiterleitung der Pakete im Internet
Wichtigste Festlegungen:

- Die Forwarding-Entscheidung basiert allein auf der Zieladresse
- Jede Komponente bestimmt nur den nächsten Punkt des Weges (next hop), nicht den gesamten Weg zum Ziel
- Es gibt zwei Arten der Weiterleitung:
 - **Direktes Zustellen:** Der Zielrechner ist im gleichen Netz, d.h. direkt erreichbar
 - **Indirektes Weiterleiten:** Der Zielrechner ist nur über ein Gateway/Router erreichbar, an welchen das Paket zur Weiterleitung geschickt wird (**z.B. Defaultgateway**)



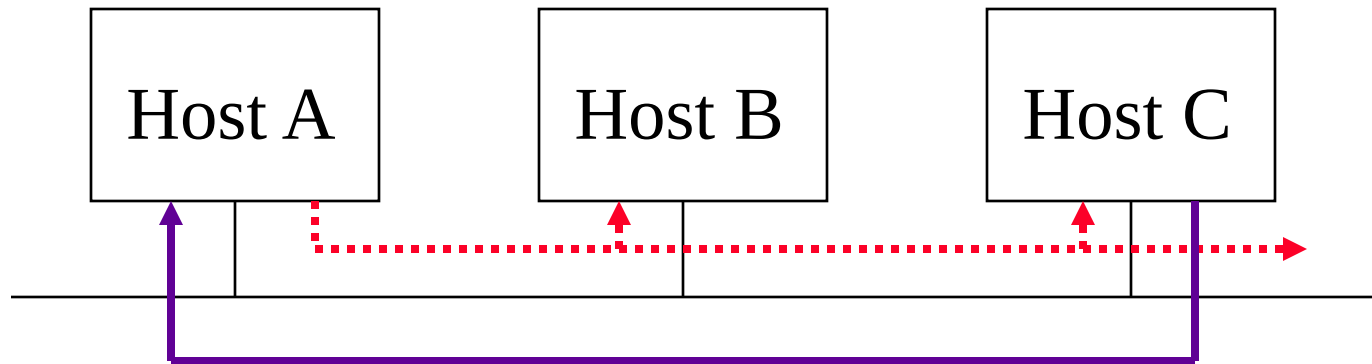
1.6 Abbildung von logischen auf physikalische Adressen

Beim Senden und Empfangen von Datenpaketen werden physikalische Adressen verwendet:

- Logische (IP) Adressen müssen auf physikalische abgebildet werden (**mapping**)
- Die Mapping-Methode gehört zur NIC-Software und hängt von der unterliegenden Hardware ab (z.B. Adressen)
- Der Internet Standard für dynamisches Address Binding ist das **Address Resolution Protocol (ARP)**



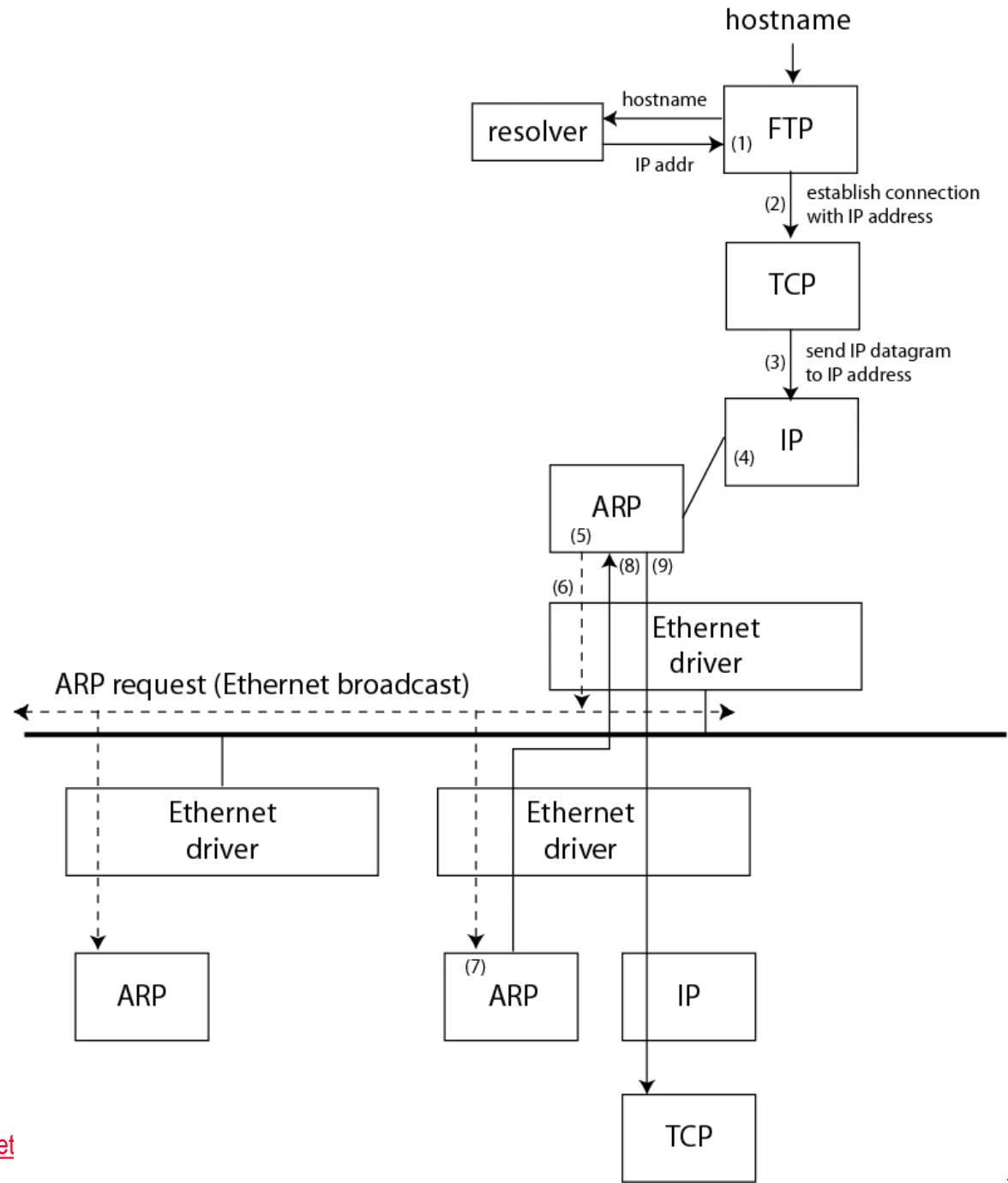
1.6 Funktionsweise von ARP



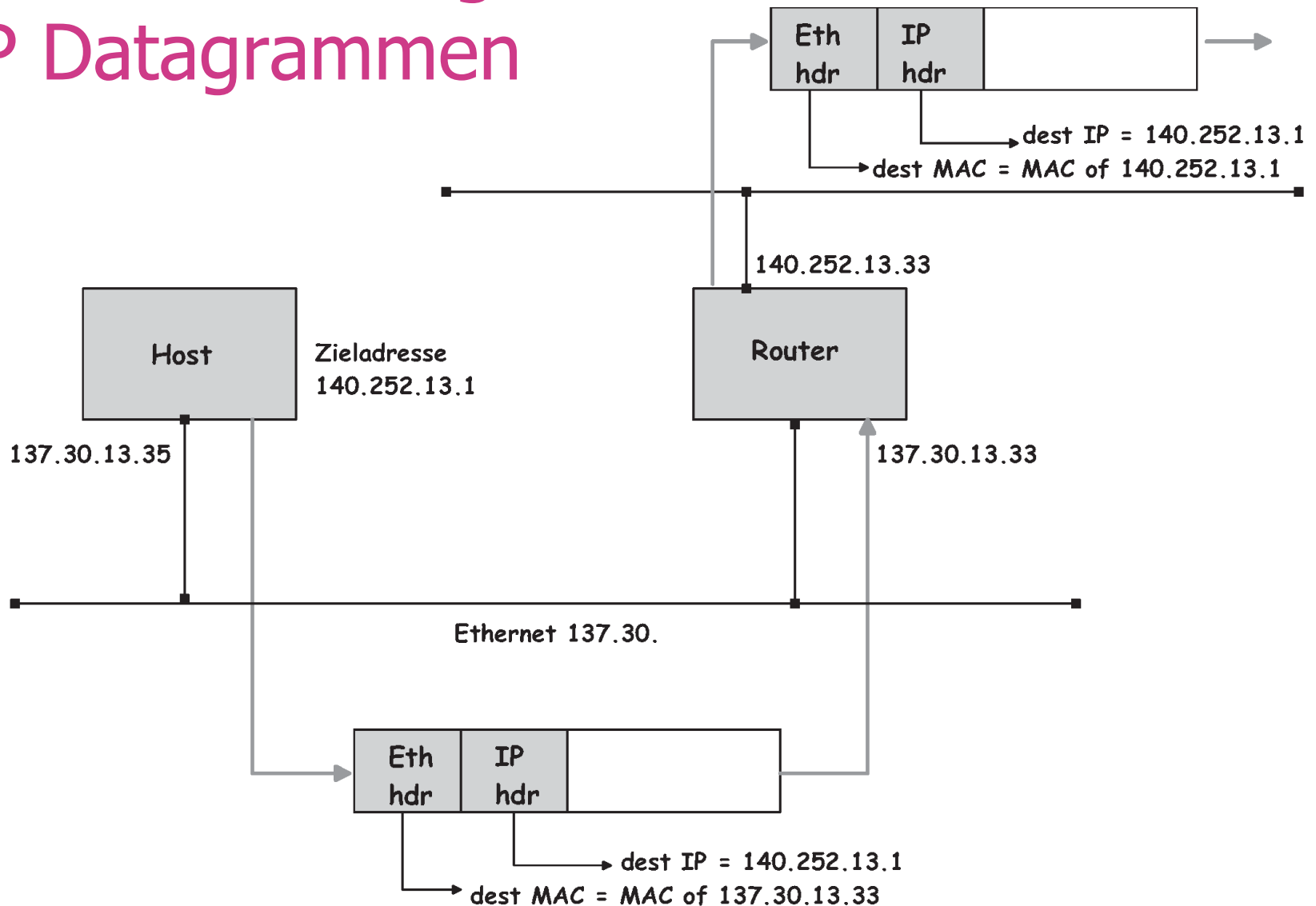
- A benötigt Mac-Adresse von C zum Senden
- A sendet per (Layer 2-) Broadcast ARP-Request mit der IP-Adresse von C
- Alle Rechner empfangen, aber nur C beantwortet den Broadcast mit seiner MAC-Adresse
- A sendet Daten direkt an C per Unicast



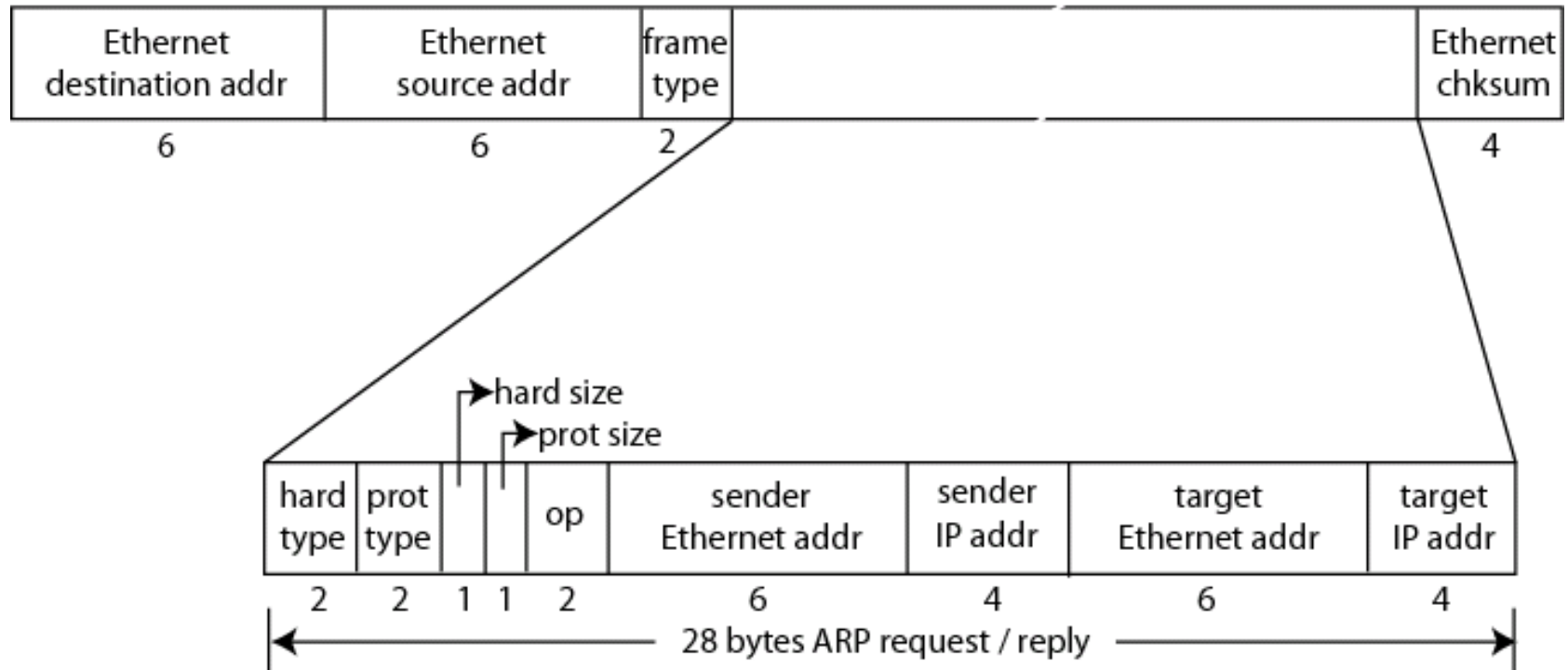
Schritte der ARP - Auflösung



1.6 Auslieferung von IP Datagrammen



1.6 ARP Paketaufbau



hard type – Typ der HW Adresse
prot type – Typ der SW Adresse

*size – Länge der jeweiligen Adresse
op – Operation (arp/rarp request/reply)

1.6 ARP Caches

Zur Verringerung der Broadcast-Last und Effizienzsteigerung werden einmal ermittelte HW Adressen in der ARP Table gemerkt.

- ARP Einträge verfallen nach ihrer Lebenszeit ($\approx$ 20 min)
- Mit dem **arp – Kommando** können Tabelleneinträge gelesen und manipuliert werden:

```
lucifer.rz.fhtw-berlin.de 13% arp -a
```

```
mitte004.rz.fhtw-berlin.de (141.45.4.1) at 00:00:5e:00:01:04 on xl0 [ethernet]
```

```
rand004.rz.fhtw-berlin.de (141.45.4.2) at 00:00:1d:e6:cf:e9 on xl0 [ethernet]
```

```
www.rz.fhtw-berlin.de (141.45.5.11) at 00:04:76:a3:b1:a7 on xl0 [ethernet]
```



1.6 Dynamic Host Configuration Protocol (DHCP)

IPv4 erwartet, dass für jeden Host eine IP Adresse, Netzmaske und ein Defaultgateway konfiguriert werden. Eine zentralisierte, dynamische Zuweisung kann durch DHCP erfolgen:

- ‚Vermietung‘ von IP Adressen, fest (per MAC) oder dynamisch
- Übermittlung von Subnetzmaske, Defaultgateway, Hostname
- Übermittlung von DNS Servern, Domainnamen, MTU-Size
- Verbreiten der Zeitzone, statischer Routen, des Printservers
- Viele weitere Attribute definiert ...



1.6 DHCP Funktionen

- DHCP Server discovery vom Client [UDP(67) broadcast]
- Ggfs Weiterleitung durch lokalen Relay Agent
- DHCP Offer von DHCP Server(n) [UDP(68) broadcast,TID]
- DHCP Request vom Client an Server [UDP(67) broadcast,TID]
- DHCP Acknowledge vom Server [UDP(68) broadcast, TID]



Praxisbeispiel: ICE4@bahn.de

Drahtlos-LAN-Adapter WLAN:

Verbindungsspezifisches DNS-Suffix:

```
Beschreibung. . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
Physische Adresse . . . . . : 58-1C-F8-06-9F-00
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
Verbindungslokale IPv6-Adresse . . : fe80::c1fc:195f:629f:cfbf%17(Bevorzugt)
IPv4-Adresse . . . . . : 172.18.232.58(Bevorzugt)
Subnetzmaske . . . . . : 255.255.0.0
Lease erhalten. . . . . : Dienstag, 3. Dezember 2024 10:19:01
Lease läuft ab. . . . . : Dienstag, 3. Dezember 2024 10:24:01
Standardgateway . . . . . : 172.18.0.2
DHCP-Server . . . . . : 172.18.0.2
DHCPv6-IAID . . . . . : 158378195
DHCPv6-Client-DUID. . . . . : 00-01-00-01-2D-70-C0-F6-00-50-B6-86-7F-AE
DNS-Server . . . . . : 172.18.0.2
NetBIOS über TCP/IP . . . . . : Aktiviert
```

1. Resümee

- IPv4 bildet seit $\approx$ 45 Jahren das alleinige Rückgrat des Internets
- Neuere Entwicklungen konzentrieren sich um die derzeitigen Kernprobleme von IPv4:
 - Erschöpfter Adressraum
 - Routing
 - Security
 - Multicasting / Anycasting
 - Mobility
- Neuere Entwicklungen & Deployments finden in IPv6 statt



Selbsteinschätzungsfragen

1. Gehört zu jeder IP Adresse eines Rechners auch eine eigene Netzwerkkarte?
2. Wie lauten Adressbereiche und Subnetzmasken, wenn die Netzadresse 135.30. in 128 gleich große Subnetze unterteilt wird?
3. Welche Forwarding-Entscheidung muss jeder Internet Teilnehmer treffen?
4. Kann mit dem ARP-Request eine HW Adresse eines benachbarten Subnetzes ermittelt werden?



Einführung in IPv6

Next Generation Internet Protocol

2.1 Motivation + Übersicht

2.2 Adressierung

2.3 Autokonfiguration

2.4 IPv6 Paketformate

2.5 Weitere Eigenschaften

2.6 Migrationsszenarien

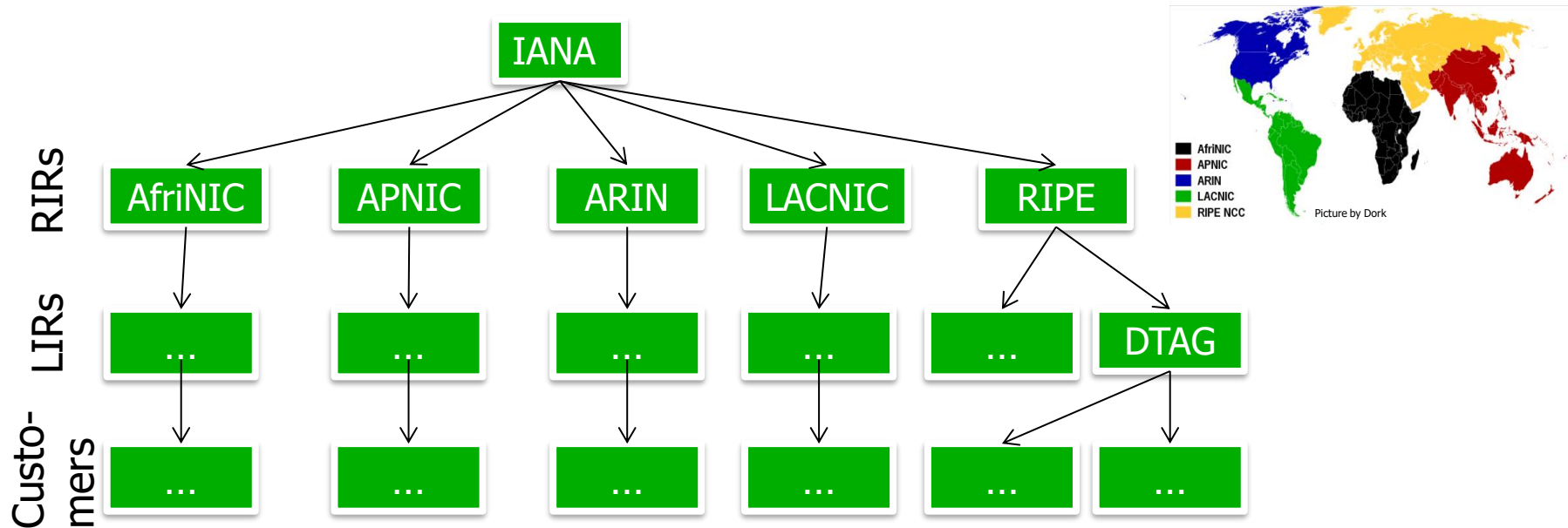


2. IPv6: Die Grenzen von IPv4

- Grunddesign etwa 50 Jahre alt
 - Paketformat, ... veraltet
 - Hardwareentwicklung der Netze überholt IP-Algorithmik
- Adressraum erschöpft
 - ‚Normales‘ Internetwachstum nicht mehr adressierbar
 - Neue Arten von vernetzten Geräten (Handys, intelligente Komponenten, „Internet of Things“ ...) verlangen neue Größenordnung von Adressen
 - Aufgrund des Adressengpasses NAT-ALGs
- Unterstützung neuer Services ‚mühsam‘



2. IP Adresszuweisung



- ▶ IANA – Internet Assigned Numbers Authority
- ▶ RIR – Regional Internet Registry
- ▶ LIR – Local Internet Registry
 - ▶ LIRs sind Internet Service Provider, Unternehmen oder Hochschulen
BSP: DTAG = Deutsche Telekom, die Adressen an Kunden weitergibt



2.1 IPv4 Addresses Shortage

- Problem: IANA vergab den letzten freien IPv4 Adressblock an RIRs in 2011



The screenshot shows the NRO (Number Resource Organization) website. At the top, there are logos for NRO, AFRINIC, APNIC, ARIN, lacnic, and RIPE NCC. Below the logos is a navigation bar with links: ABOUT, ACCOUNTABILITY, INTERNET GOVERNANCE, TECHNICAL COORDINATION, POLICY, and DOCUMENT ARCHIVE. The main content area features a headline "Free Pool of IPv4 Address Space Depleted" dated "3 FEB 2011". The text below the headline states: "IPv6 adoption at critical phase" and "Montevideo, 3 February 2011 – The Number Resource Organization (NRO) announced today that the free pool of available IPv4 addresses is now fully depleted. On Monday, January 31, the Internet Assigned Numbers Authority (IANA) allocated two blocks of IPv4 address space to APNIC, the Regional Internet Registry (RIR) for the Asia Pacific region, which triggered a global policy to allocate the remaining IANA pool equally between the five RIRs. Today IANA allocated those blocks. This means that there are no longer any IPv4 addresses available for allocation from the IANA to the five RIRs." On the right side, there is a "SEARCH" section with a search bar and a "SEARCH" button. Below that is a "QUICK LINKS" section with links to "NRO News", "ASO Review 2017", "Document Archives", "NRO FAQ", and "ASO Website". At the bottom right, there is a logo for the Hochschule für Angewandte Wissenschaften Hamburg.

NRO

AFRINIC

APNIC

ARIN

lacnic

RIPE NCC

ABOUT ACCOUNTABILITY INTERNET GOVERNANCE TECHNICAL COORDINATION POLICY DOCUMENT ARCHIVE

Free Pool of IPv4 Address Space Depleted

3 FEB 2011

IPv6 adoption at critical phase

Montevideo, 3 February 2011 – The Number Resource Organization (NRO) announced today that the free pool of available IPv4 addresses is now fully depleted. On Monday, January 31, the Internet Assigned Numbers Authority (IANA) allocated two blocks of IPv4 address space to APNIC, the Regional Internet Registry (RIR) for the Asia Pacific region, which triggered a global policy to allocate the remaining IANA pool equally between the five RIRs. Today IANA allocated those blocks. This means that there are no longer any IPv4 addresses available for allocation from the IANA to the five RIRs.

SEARCH

Search SEARCH

QUICK LINKS

NRO News

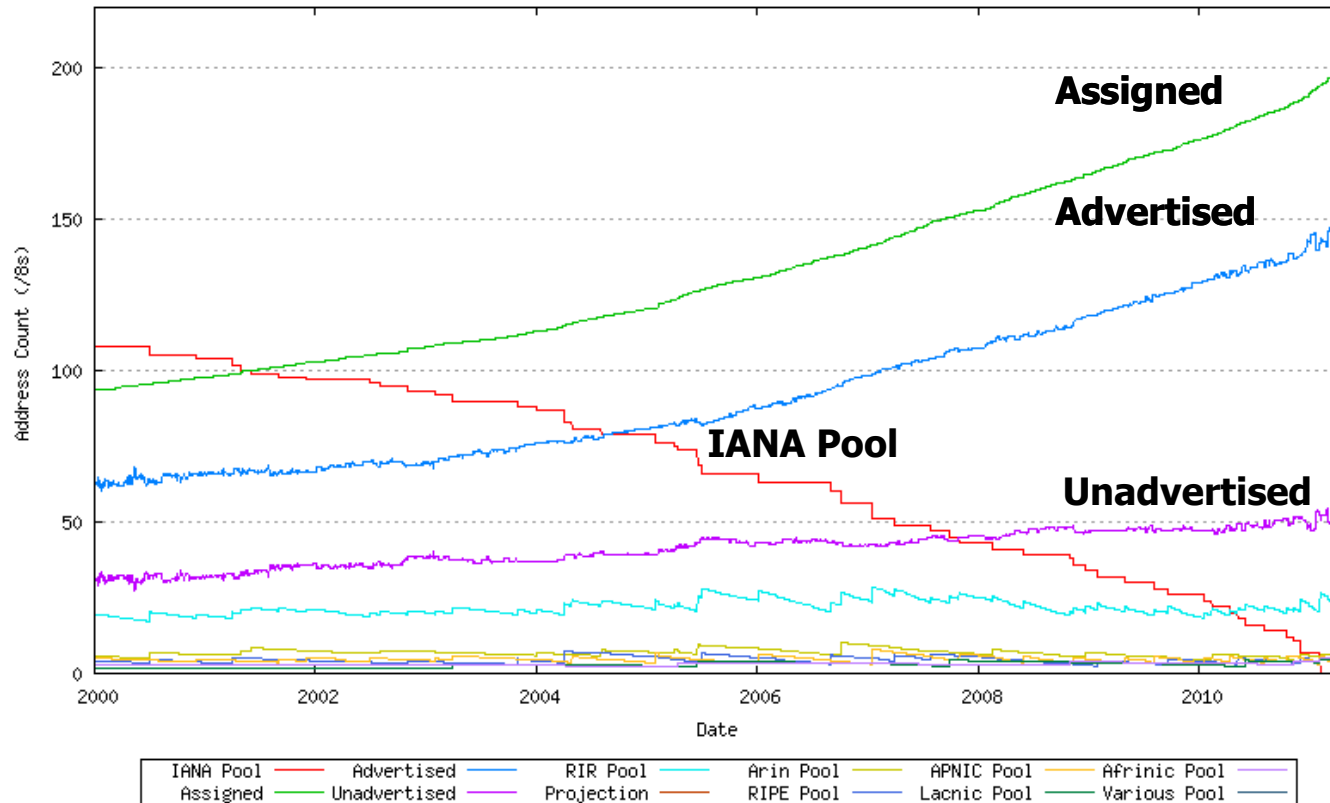
ASO Review 2017

Document Archives

NRO FAQ

ASO Website

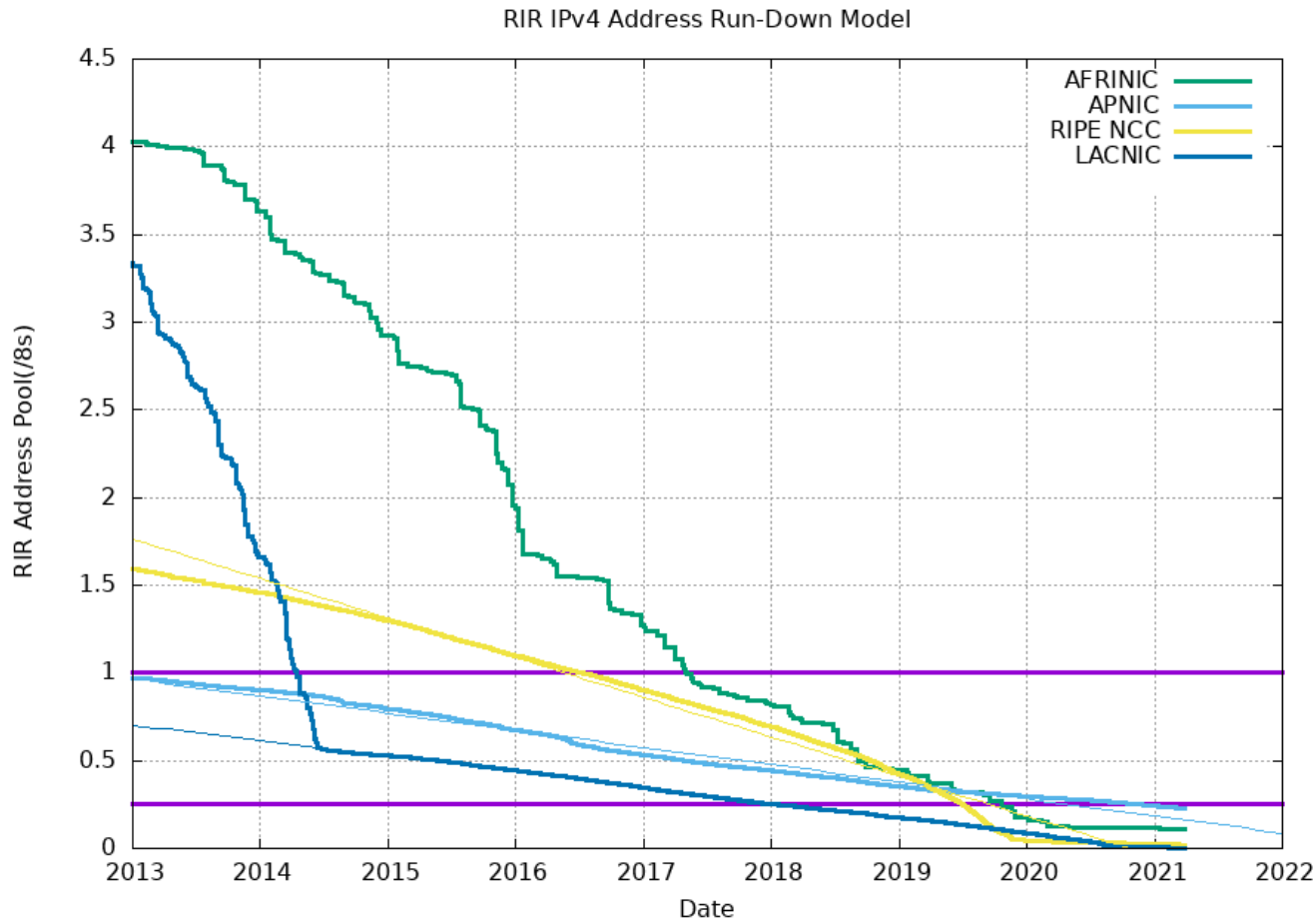
2.1 IPv4 Adresserschöpfung



- IANA Unallocated Address Pool Exhaustion: 3. Februar 2011
- RIPENCC Pool Exhaustion: 14. September 2012

Quelle: Geoff Huston, <http://www.potaroo.net/tools/ipv4/>

2.1 IPv4 Adresserschöpfung



➤ ARIN Exhaustion: 24. Sept. 2015 – remaining NULL

➤ RIPE NCC: April 2021 – remaining $0.02 * /8$

Source: Geoff Huston, <http://www.potaroo.net/tools/ipv4/>

2.1 IPng Geschichte

- IETF WG IPng begann Anfang der 90er zu arbeiten
- Winter 1992: 7 Vorschläge zur Weiterentwicklung von IP
 - CNAT, IP Encaps, Nimrod, Simple CLNP, PIP, SIP, TP/IX
- Herbst 1993: Verschiedene Zusammenschlüsse führen zu
 - ‚Simple Internet Protocol Plus‘ (SIPP) und ‚Common Architecture for the Internet‘ CATNIP
- Juli 1994: IPng Area Director empfiehlt Roadmap (RFC 1752) auf der Basis von SIPP (Steve Deering)
- Dez. 1995: S. Deering, R. Hinden, „Internet Protocol, Version 6 (IPv6) Specification“ (RFC 1883, jetzt RFC 2460)
- Sub-TLAs erhältlich (RIPE-NCC, APNIC, ARIN) seit 1999
- May 2007: ARIN ruft Internet Community zur Migration nach IPv6 auf



2.1 IPv6 Neuerungen

➤ Adressierung und Routing

- Behebung des Adressengpasses: 128 Bit lange Adressen
- Adresshierarchie kann Backbone-Routing vereinfachen
- Mehrere Adressen pro IP-Interface üblich

➤ Vereinfachte Administration

- Autokonfiguration auch ohne DHCPv6 vorgesehen
- Fließende Netzmasken, Renumbering durch Prefixänderung

➤ Sicherheit: IPSec

- Security Header Extension für Authentisierung, Integrität und Verschlüsselung



2.1 IPv6 Neuerungen (2)

➤ Protokollaufbau

- Schlankerer Header zur schnellen Verarbeitung
- Optional zusätzlich eingeschobene Header
- Festes Format für alle Header
- Verzicht auf Header Checksum
- Verzicht auf Fragmentierung in Routern
- Verbesserte Multicast-, Anycast-, QoS und Mobile Services
- Umstellungs- und Koexistenzkonzept IPv4 ↔ IPv6



2.2 Adressierung

- IPv6-Adressen sind 128-bit lang und variabel aufgebaut
- Adressarchitektur: RFC 1884, 4291 (Feb '06, Hinden, Deering)
- Automatische Adresskonfiguration
- Globale Adresshierarchie von der Top Level Vergabe bis zur Interface-ID vorgesehen
- Aggregation-based allocation zur Vereinfachung des weltweiten Routings möglich
- 3 Bit Format Prefix (FP) dient zur Identifikation des Adresstyps



2.2 Schreibweise von IPv6 Adressen

- **Standard Form:** 8 x 16 bit Hexadezimal

Bsp: 1080:0:FF:0:8:800:200C:417A

- **Verkürzte Form:** Folgen von Nullen ersetzt ::

Bsp: FF01:0:0:0:0:0:0:43 → FF01::43

- **IPv4 Kompatible Adressen:**

Bsp: 0:0:0:0:0:FFFF:13.1.68.3 → ::FFFF:13.1.68.3

- **CIDR-Notation für Präfixes:**

Bsp: 1080:645:FF::/48

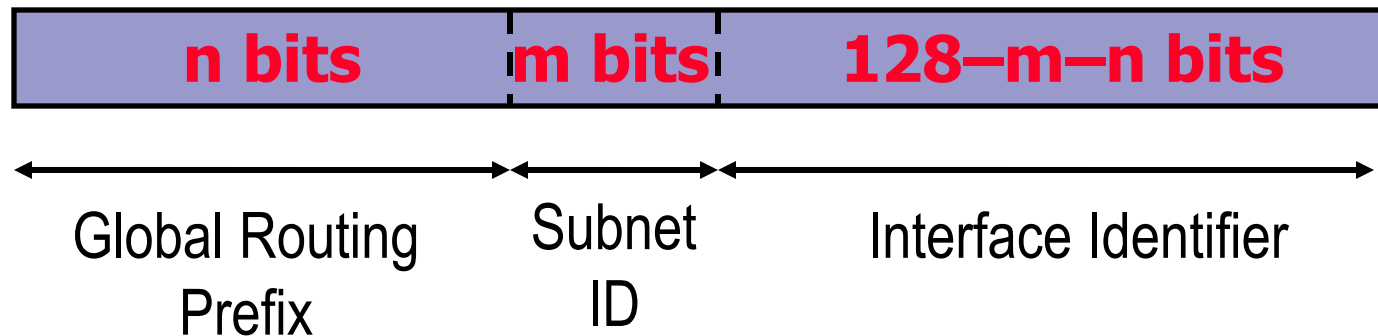


2.2 Adresstypen

<u>Type</u>	<u>Binäres Prefix</u>
■ Unicast (one-to-one)	
■ global	all not specified elsewhere
■ unique local addresses	1111 110 (FC00::/7)
■ link-local	1111 1110 10 (FE80::/10)
■ IPv4-mapped	000...0:FFFF ::FFFF:xxx.xxx.xxx.xxx
■ Loopback	0000..1 ::1/128
■ unspecified	0000...0 ::/128
■ Multicast (one-to-many)	1111 1111 (FF00::/8)
■ Anycast (one-to-nearest)	aus Unicast Prefixes
■ Keine Broadcast-Adressen (nur noch Multicast)!	



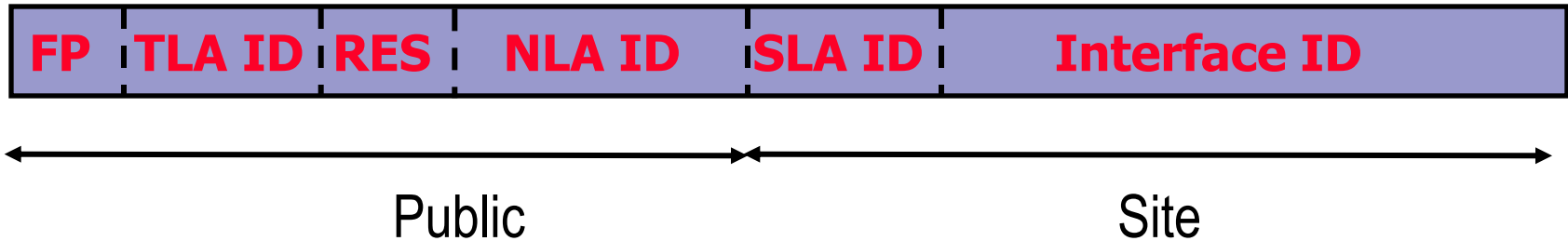
2.2 Globale Unicast Adressen (RFC 3513)



- Alle Teilfelder sind variabel lang und nicht ‚selbsterklärend‘ (keine Adressklassen)
- Alle globalen Unicast Adressen, die nicht mit 000 (binär) beginnen, besitzen eine 64 bit Interface ID, d.h. $m + n = 64$
- Mechanismen des automatischen Präfix-Tauschs vorgesehen



2.2 Historic – RFC2374: Aggregatable Global Unicast Format



- Früherer Ansatz: Standardisierte Präfixhierarchie von **Top/Next/Side Level Aggregator**
- Gegenwärtiger Ansatz: Den RIR Policies überlassen
cf. <http://www.ripe.net/ripe/docs/ipv6policy.html>



2.2 Lokale Unicast Adressen

- ▶ Link-lokale Adressen zum Gebrauch bei der Autokonfiguration und in Netzen ohne Router:



- ▶ Unique local addresses (RFC 4193), unabhängig von TLA/NLA:
 - ▶ Global eindeutig, für lokale Kommunikation (konfliktfrei)
 - ▶ Nicht für globales Routing gedacht (aber für gezielte Site-Verbindungen)



2.2 Beispiel:

Unser erstes IPv6 Netz in 2001

- 2001:: /16 - Vorgegebenes Präfix.
- 2001:0600:: /23 - Regionale Registry Europa (RIPE)
- 2001:0638:: /32 - DFN Präfix
- 2001:0638:0801:: /48 - unser Netz
- 2001:0638:0801:0001:: /64 - unser erstes Subnetz
- 2001:0638:0801:0001:0000:0000:0000:0001 /128
 - unsere erste IPv6 Rechneradresse in 2001 😊

Adressierung von Sub-TLAs (Ripe) nach RFC 2450

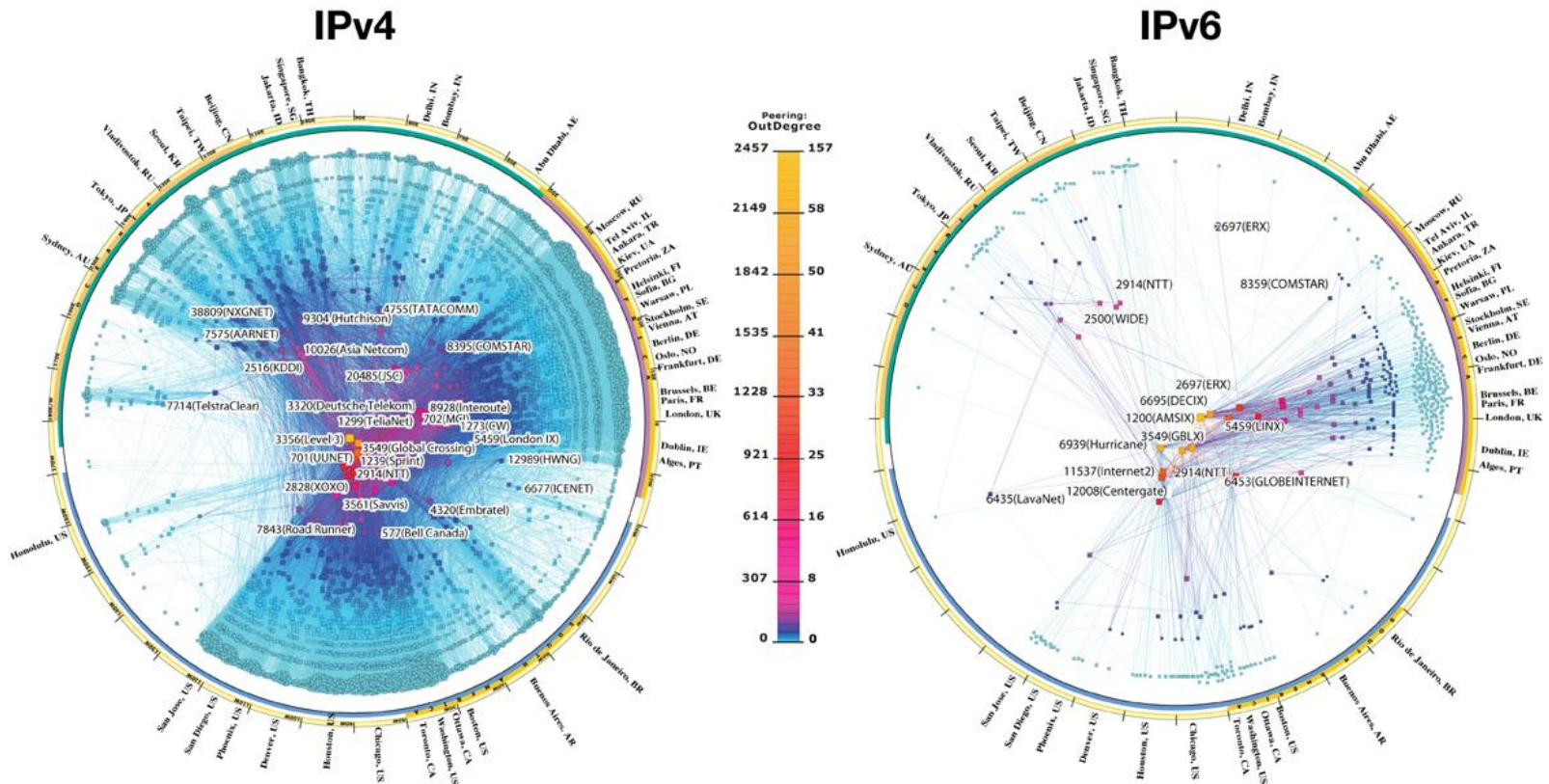


2.2 IPv6 Verbreitung (Jan '09)

IPv4 & IPv6

INTERNET TOPOLOGY MAP
JANUARY 2009

AS-level INTERNET GRAPH

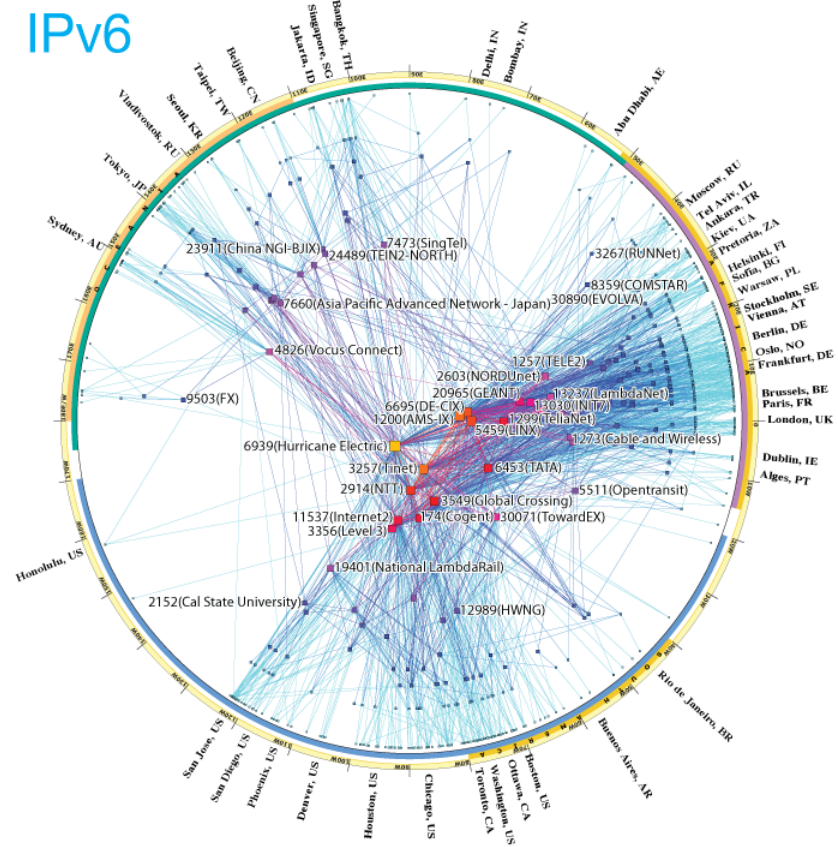
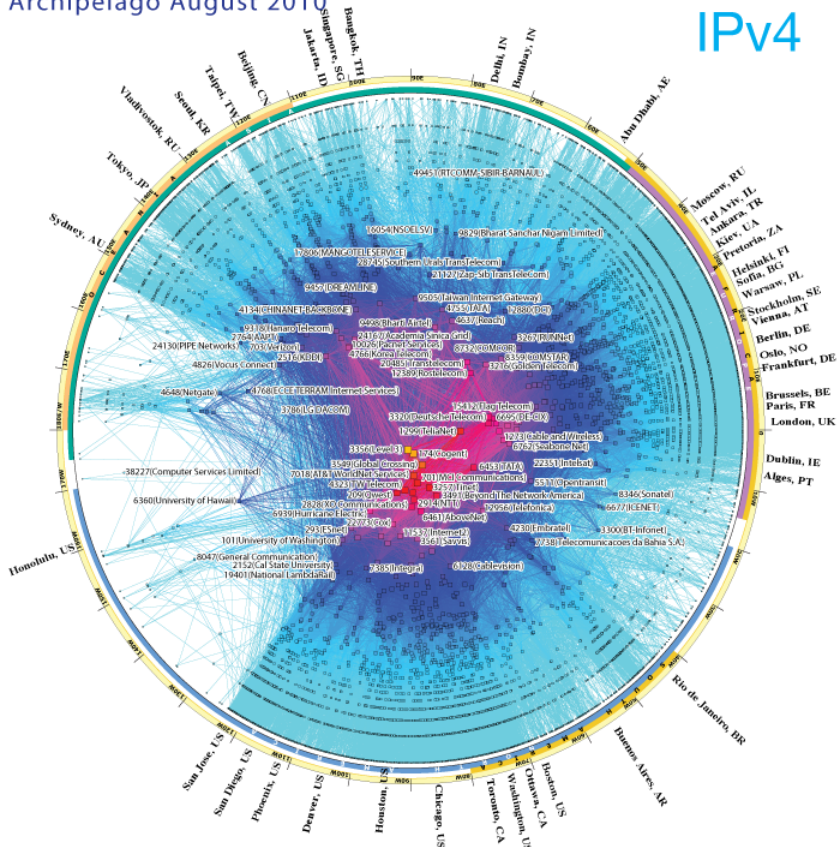


copyright © 2009 UC Regents. all rights reserved.

2.2 IPv6 Verbreitung (Aug '10)

CAIDA's IPv4 & IPv6 AS Core AS-level INTERNET GRAPH

Archipelago August 2010



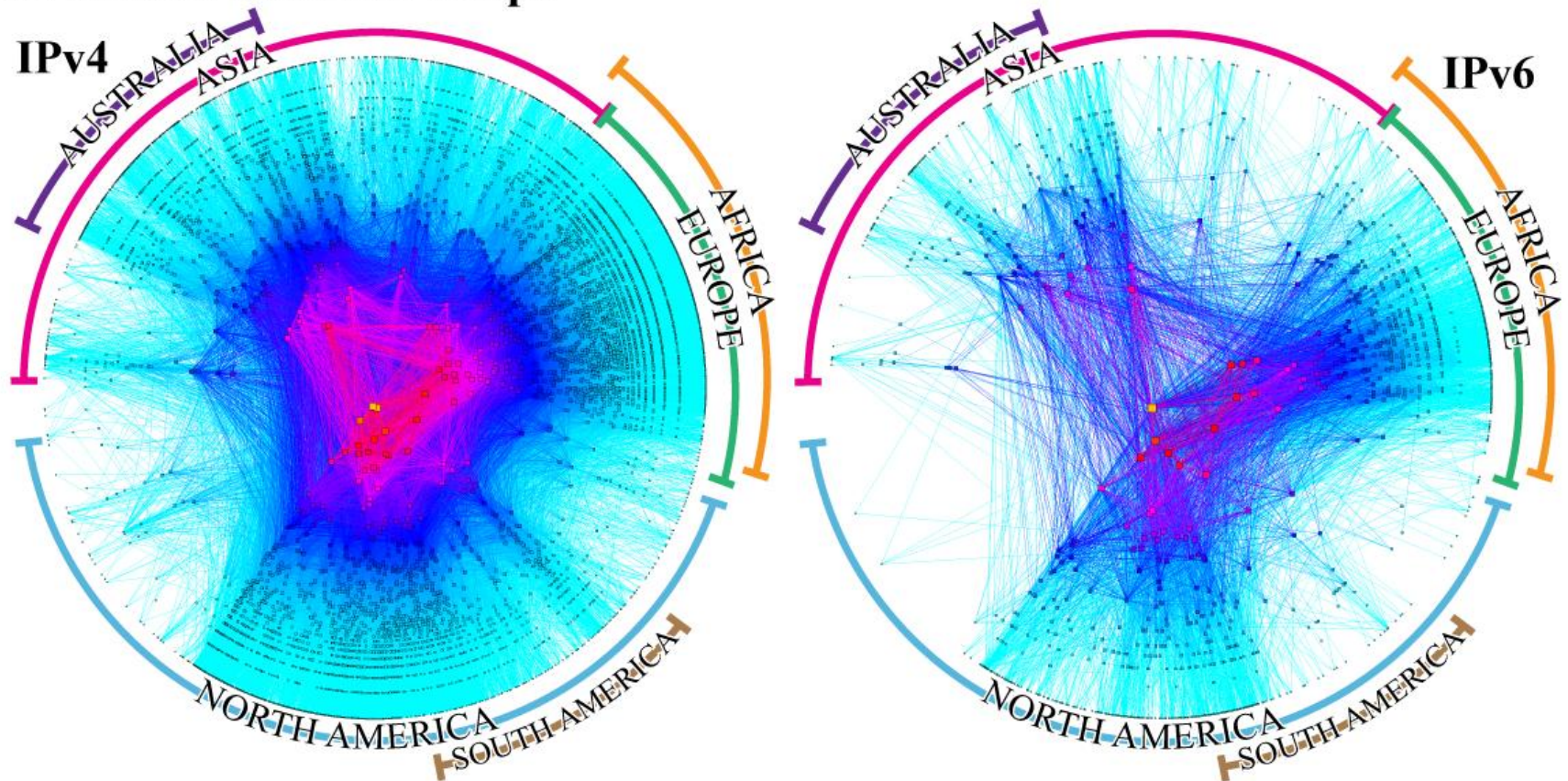
copyright © 2010 UC Regents. all rights reserved.

- Source: CAIDA
(http://www.caida.org/research/topology/as_core_network/ipv6.xml)

2.2 IPv6 Verbreitung (Jan '13)

CAIDA's IPv4 & IPv6 AS Core
AS-level INTERNET Graph

Archipelago
Jan 2013

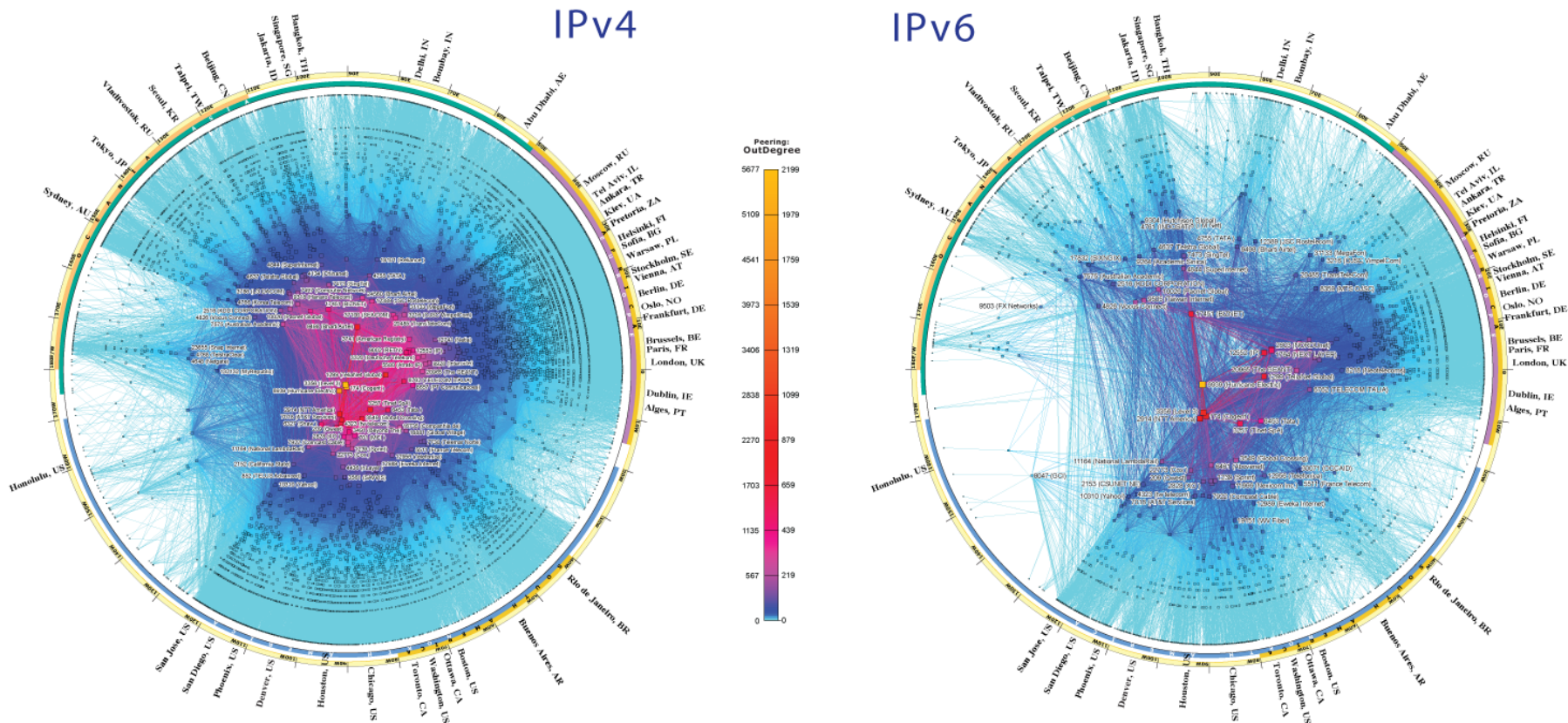


Copyright 2013 UC Regents. All rights reserved.

2.2 IPv6 Verbreitung (Jan '15)

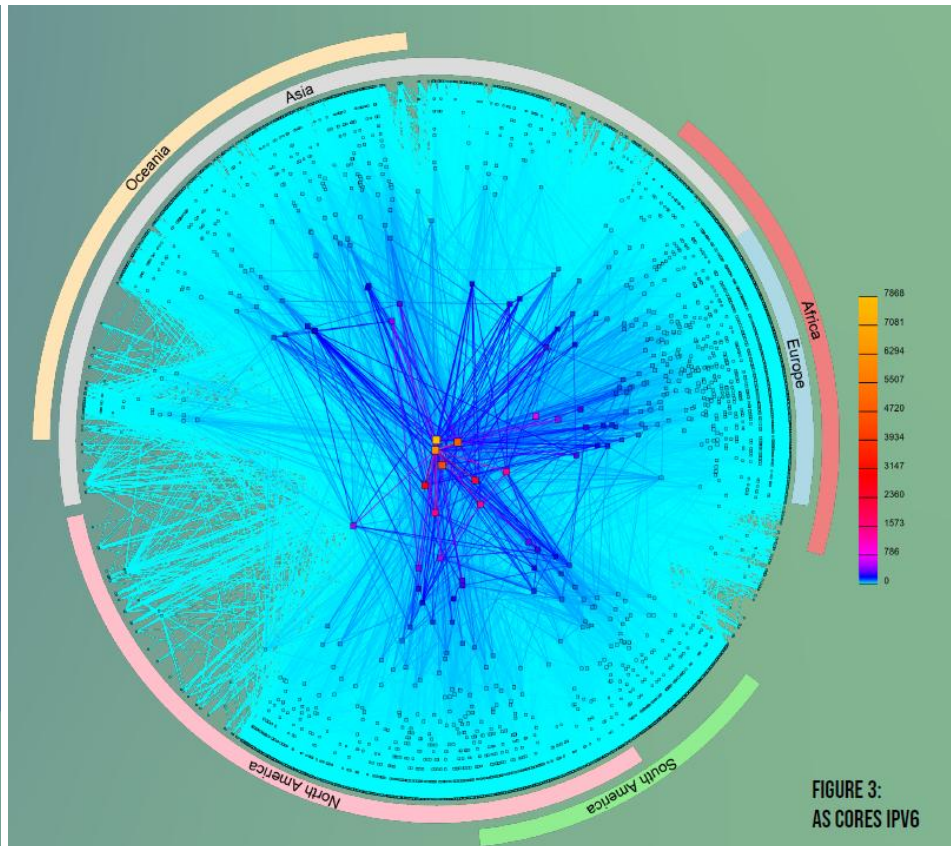
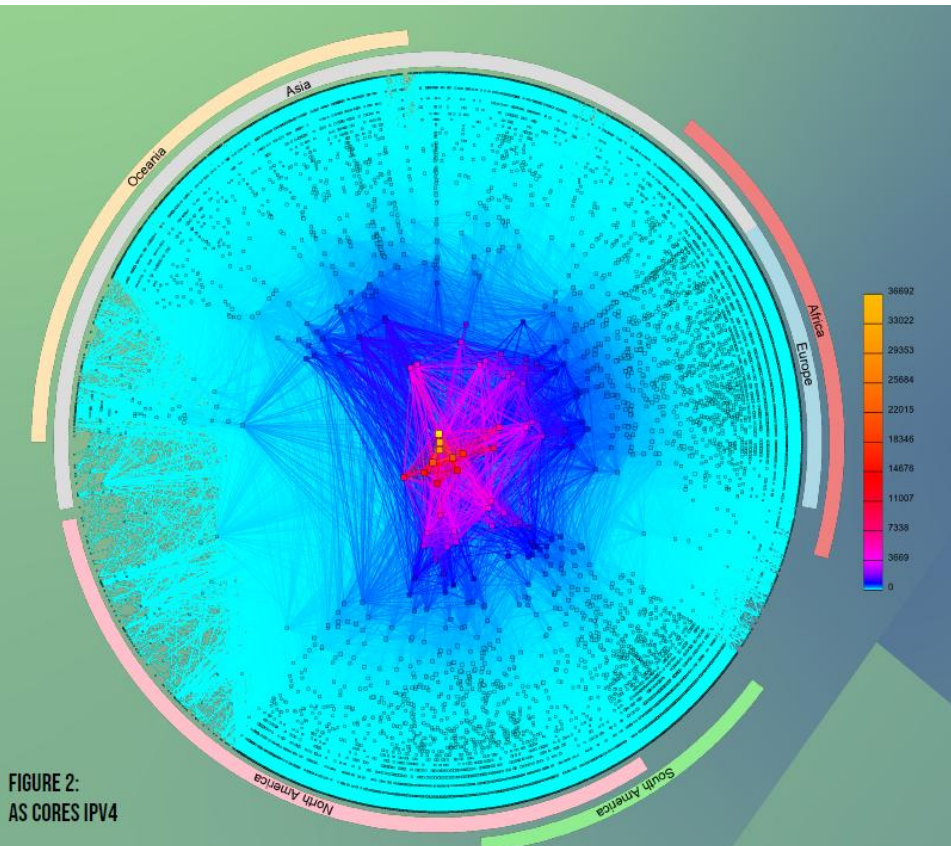
CAIDA's IPv4 & IPv6 AS Core AS-level INTERNET GRAPH

Archipelago January 2015



Copyright © 2015 UC Regents. All rights reserved.

2.2 IPv6 Verbreitung (2020)



2.3 Internet Control Message Protocol (ICMPv6)

- RFC 2463 (Conta, Deering)
- Definiert zwei (erweiterbare) Nachrichtenklassen:

Informational Messages

- Echo Request (128)
- Echo Reply (129)

Error Messages

- Destination Unreachable (1)
- Packet Too Big (2)
- Time Exceeded (3)
- Parameter Problem (4)



2.3 Neighbor Discovery (RFC 4861)

Implementiert lokale Netzkonfigurationen mittels ICMP:

- Router und Präfix Entdeckung
 - Ermöglicht zustandslose Autokonfiguration
- Adressauflösung, Unerreichbarkeitserkennung
 - Ablösung von ARP (auf Schicht 3!)
- Umleitungsfunktion (Redirect)
- Definiert **fünf neue ICMP-Nachrichten**:
 - Router Solicitation – Router Advertisement
 - Neighbor Solicitation – Neighbor Advertisement
 - Redirect



2.3 State-Less Address Auto-Configuration (SLAAC)

1. Interface erhält (bei Aktivierung) eine link-lokale Adresse (z.B. aus der Hardwareadresse gebildet).
 2. Interface sendet *router solicitation*, um nicht auf Router Advertisements warten zu müssen.
 3. Router sendet *router advertisement* (Präfix, Defaultgateway, ...).
 4. Das Interface bildet aus Präfix und link-lokaler Adresse eine globale Adresse.
 5. Zur Verifikation der Eindeutigkeit wird noch eine ICMP *neighbor solicitation* versandt (Duplicate Address Detection).
- ➔ Interface hat eine global gültige Unicast Konfiguration gebildet (ohne DHCP)



2.3 Neighbour Discovery Protocol (NDP)

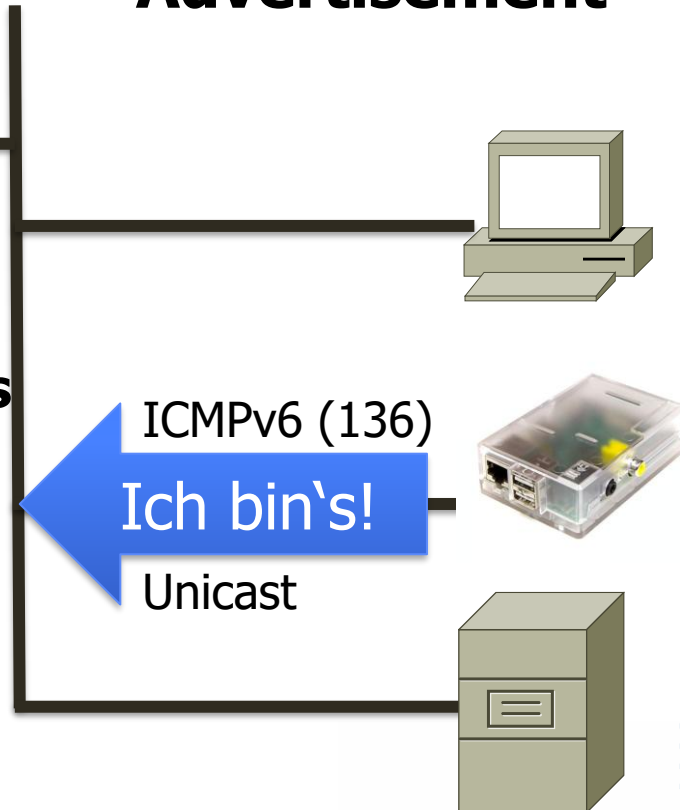
- Adresse meines Nachbarn?

Suche **FE80::ba27:ebff:FE3b:7def**,64

Solicitation



Advertisement

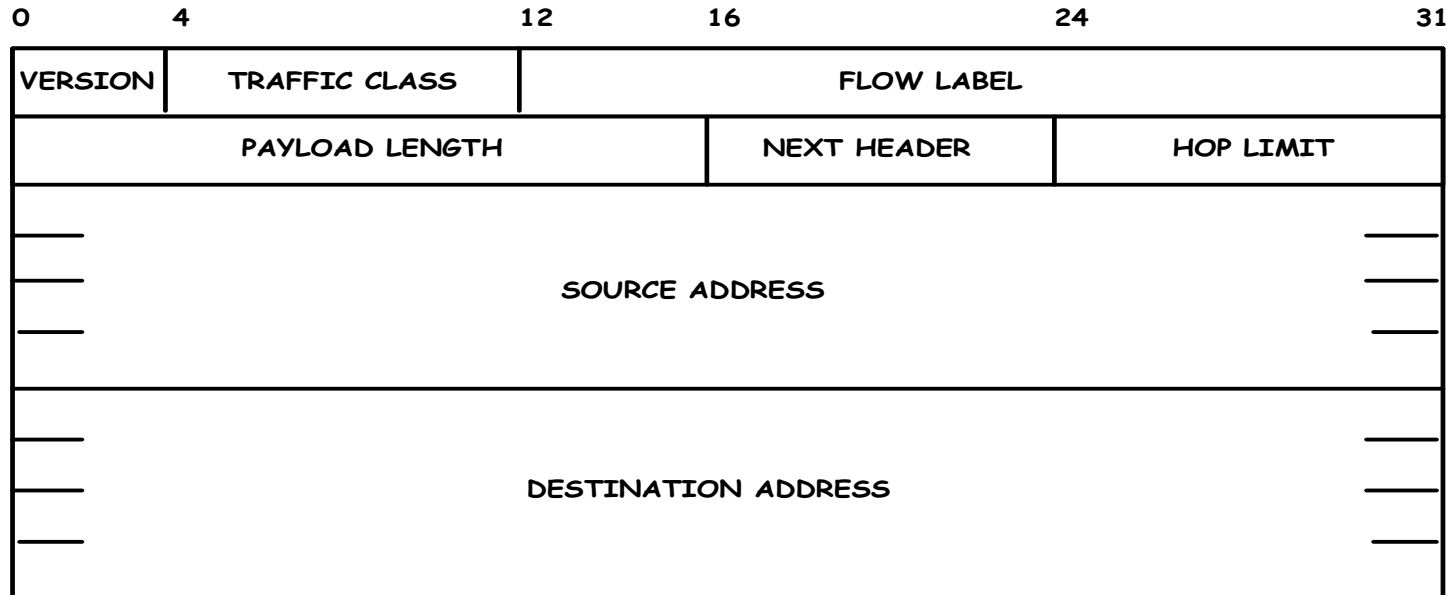


NDP nutzt
Solicited-node Multicast Address
Prefix: ff02::1:ff00:0000/104

Verbleibende 24 Bits stammen von
Interface ID

Unser Beispiel: **ff02::1:ff3b:7def**

2.4 IPv6 Paketformat: Basisheader



VERSION	4 Bit	Internet Protocol Version number = 6
TRAFFIC CLASS	8 Bit	Type-of-Services
FLOW LABEL	20 Bit	Qos-Informationen für Routerverarbeitung
PAYLOAD LENGHT	16 Bit	Oktettanzahl des Paketes ohne IPv6-Header
NEXT HEADER	8 Bit	Type des "encapsulated protocol"
HOP LIMIT	8 Bit	TTL-Zähler wird dekrementiert je Router
SOURCE ADDRESS	128 Bit	Adresse des Ausgangsknoten (128 Bits)
DESTINATION ADRESS	128 Bit	Adresse des Ausgangsknoten (128 Bits)

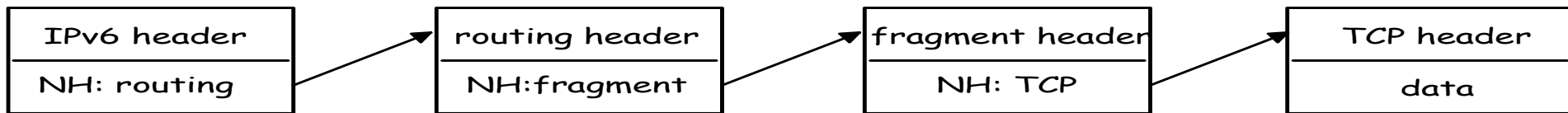
2.4 Streichungen aus IPv4 Header

1 4 8 16 19 24 32

Version	Länge	Servicetypen	Paketlänge			
Identifikation				D	M	Fragmenabstand
				F	F	
Lebenszeit	Transport		Kopfprüfsumme			
Senderadresse						
Empfängeradresse						
Optionen					Füllzeichen	

2.4 IPv6 Paketformat: Optionsheader

- Erweiterter Optionsmechanismus: Jeder Header verweist auf eventuell nachfolgende Header oder auf Daten, z.B:



- Optionsheader haben keine Längenbeschränkung (IPv4: 40 Oktetts), Padding auf 8 Oktetts
- Optionsheader werden von Hosts, nicht von Routern verarbeitet. Ausnahme: Hop-by-Hop Options Header



2.4 Basis Options-Header

- **Routing**
Erweiterte Routinginformationen (source routing)
- **Fragmentation**
Fragmentierungs-/Defragmentierungsinformationen
- **Authentication**
Sicherheitsinformationen: Authentizität und Integrität
- **Encapsulation**
,Tunneling`, z.B. für vertrauliche Daten
- **Hop-by-Hop Option**
Spezielle Optionen, die an jedem Router verarbeitet werden
- **Destination Option**
Informationen für den Empfänger-Host (Headererweiterung)

2.5 QoS: Traffic Class + Flow Label

Traffic Class wie IPv4 TOS-Feld.

20-bit Flow Labels können von der Quelle genutzt werden, um zusammenhängende Pakete zu markieren.

- Markiert Flows allein im IP(v6) Header
- Zielstellung: Beschleunigte, uniforme Behandlung von Paketströmen durch Router
- Flowlabel: Random per Flow
- Headerinformationen einheitlich per Flow (Router Caching)
- Kann Zustände auf Routern definieren, aber auch zustandslos prozessiert werden



2.5 Weiteres zu IPv6

- Domain Name System, abgeschlossene Debatte
 - A-Record → AAAA - Record versus
 - A-Record → [A6 - Record (Speicherung von Adressteilen)]
- IPsec ist Pflichtbestandteil von IPv6
- Secure Neighbour Discovery (Send)
- IPv6 over 3GPP
- Mobile IPv6
- Multihoming in der Diskussion



2.6 IPv4 → IPv6 Portierung

- IPv6 ist ein *anderes* Internet-Protokoll:
 - Teilnehmer sprechen **entweder IPv4 oder IPv6**
- Adress-Datenstrukturen:
 - Neu für IPv6 (Adressliste)
- Name-to-address Übersetzung:
 - Neue Funktionen zur Unterstützung von IPv6 und IPv4
- Adress-Konvertierungsfunktionen
 - Neue Funktionen zur Unterstützung von IPv6 und IPv4
- DNS resolver
 - Gibt IPv6 oder IPv4 Adresse oder beide zurück



2.6 IPv4 → IPv6 Migration

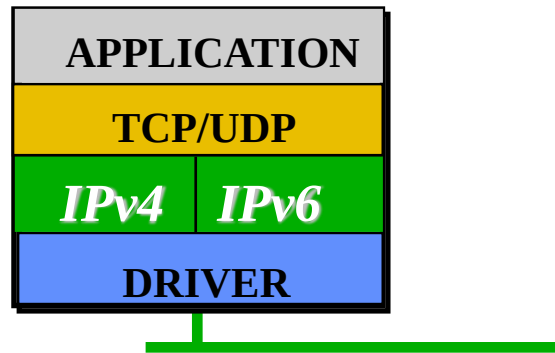
Vielfältige Techniken zur Migration wurden konzipiert und implementiert nach folgenden Ansätzen:

- **Dual-Stack** Techniken, welche die Koexistenz von IPv4 und IPv6 für dieselben Geräte und Netze erlauben
- **Tunnel**, welche IPv6-Regionen über IPv4-Regionen hinweg verbinden. Bsp.: 6-to-4 automatisch über Anycast Gateway
- **Protokollübersetzer (NATs)**, welche IPv6-Geräte mit IPv4-Geräten sprechen lassen

In der Migrationszeit ist der kombinierte Einsatz all dieser Methoden wahrscheinlich.



2.6 Dual Stack



- Beim Aktivieren von IPv6 kann der IPv4-Stack einfach weiterbetrieben werden (Multiprotokoll-Ansatz)
- Geräte können Ihre Adressen behalten (IPv4 in IPv6)
- Anwendungen/Bibliotheken wählen die IP-Version aus:
 - Bei der Kontaktaufnahme in Abhängigkeit zur DNS-Antwort
 - Bei der Beantwortung in Abhängigkeit vom den eingegangenen Paketen
- Der Dual-Stack Betrieb kann unbeschränkt fortgeführt werden und erlaubt die schrittweise Portierung der Applikationen



Selbsteinschätzungsfragen

1. Welche Möglichkeiten bietet IPv6, um automatisch eine link-lokale Interface Adresse zu konfigurieren?
2. Wie kann die IPv6 Adressstruktur zur Vereinfachung des Routings beitragen?
3. Was tritt in IPv6 an die Stelle des ARP Requests? Was ist protokollseitig anders?
4. Warum benötigt die IPv6 Software (API) neue Adressfunktionen? Was müssen diese zusätzlich zu den IPv4-Funktionalitäten können?

