Chaos Computer Club Freiburg e.V.

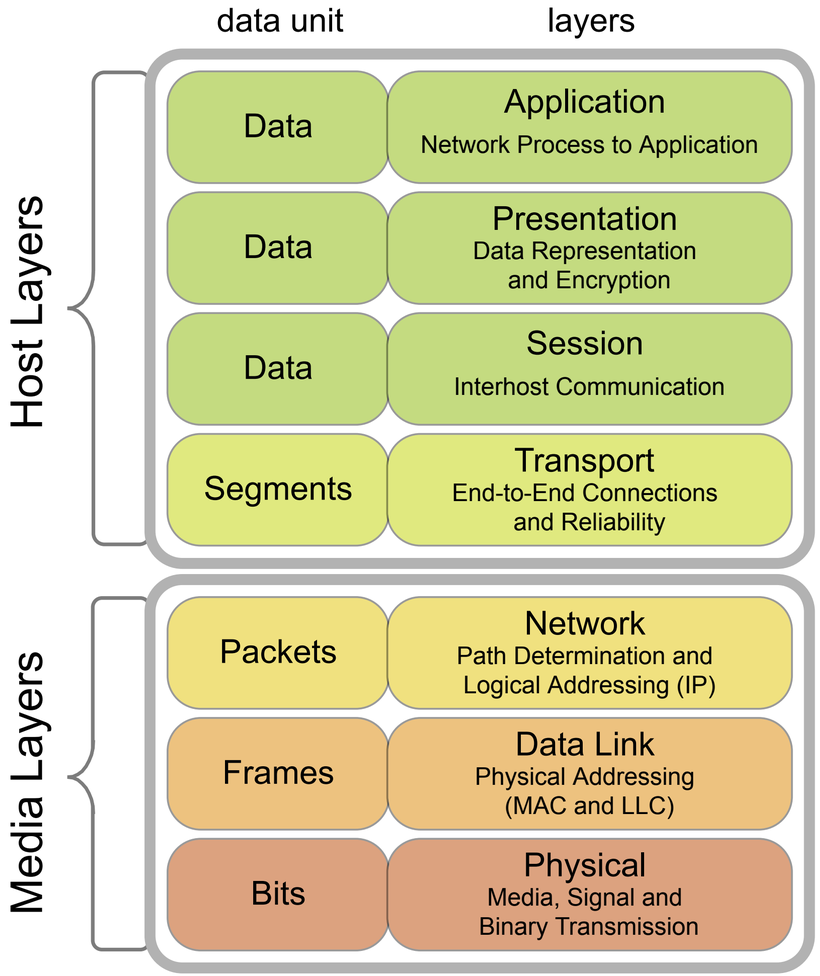
Netzwerke (Teil 2)

… oder: wie unser Geraffel miteinander redet

Balrog, 10. November 2026

Rückblick auf Teil 1

OSI-Schichtenmodell



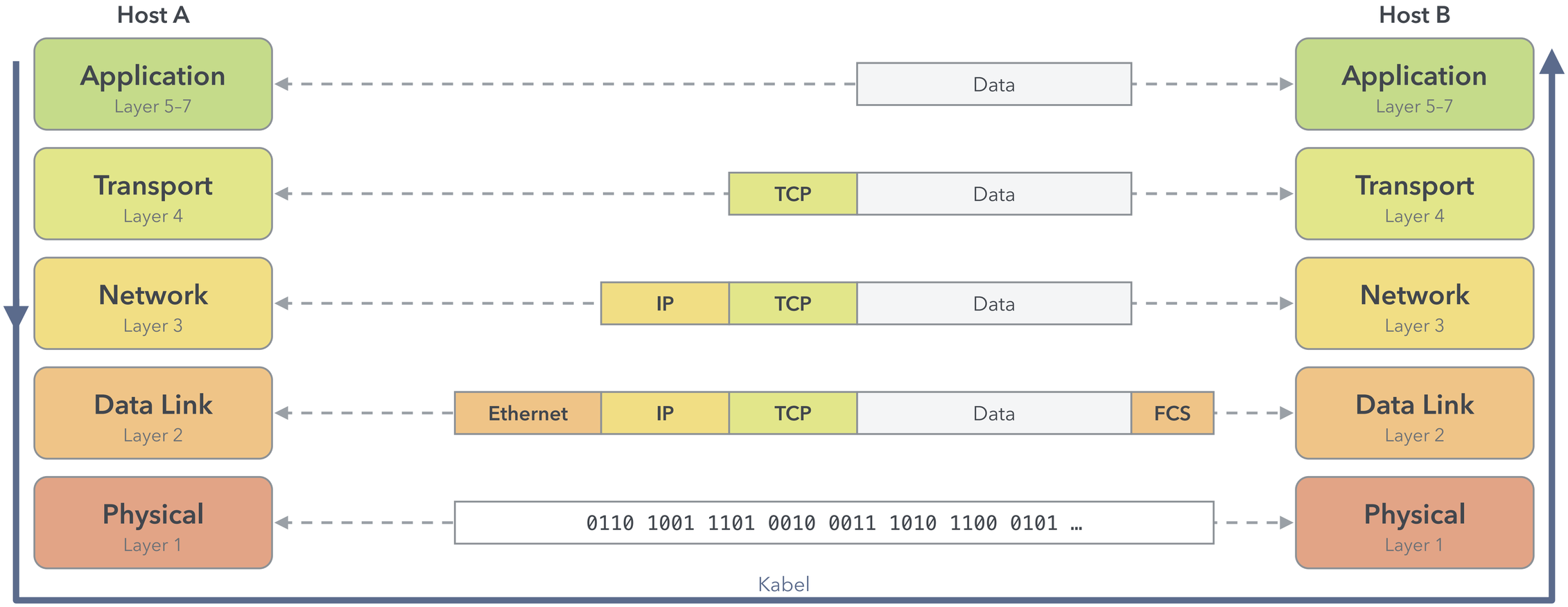
Away	
Pizza	
Salami	
Throw	TCP, UDP, SCTP, SPX, … Layer 4-7-Switch
Not	IP, IPSec, IPX, ICMP, IGMP, … / Router
Do	Ethernet, Token Ring, ARCNET, Bridge, Switch, Access Point, …
Please	Kabel, Hubs, Repeater, Antenne, …

https://commons.wikimedia.org/wiki/File:OSI_Model_v2.svg CC BY-SA 4.0

Chaos Computer Club Freiburg e.V.

OSI-Modell

Kapselung



logisch: jede Schicht spricht mit ihrem Gegenüber

tatsächlich: runter, über das Kabel, wieder rauf

IPv4

IP-Adressen

IPv4

- 32 Bit
- Repräsentation:
  - 4 Bytes, durch . getrennt
  - Binär
  - Dezimal

IP-Adressen

Repräsentation

172.16.0.1

Einschub

Logische Operatoren

- Jetzt wird’s ein bißchen theoretisch, aber zumindest das UND brauchen wir gleich:
  - Logisches UND (&): Eine Aussage A ist nur wahr, wenn Teilaussage B UND C wahr sind
  - Logisches ODER (|): Eine Aussage A ist wahr, wenn *mindestens* Teilaussage B ODER C wahr ist
  - Logisches NICHT (~): Eine Aussage A ist wahr, wenn Teilaussage B NICHT wahr ist
  - Logisches XOR (EXKLUSIV-ODER, ^): Eine Aussage A ist wahr, wenn EXKLUSIV Teilaussage B ODER Teilaussage C wahr ist

Einschub

Logische Operatoren

- Auf Bits übersetzt:
  - 1 & 1 → 1; 1 & 0 → 0; 0 & 1 → 0; 0 & 0 → 0
  - 1 | 1 → 1; 1 | 0 → 1; 0 | 1 → 1; 0 | 0 → 0
  - ~ 1 → 0
  - 1 ^ 1 → 0; 1 ^ 0 → 1; 0 ^ 1 → 1; 0 ^ 0 → 0

IP-Adressen

Repräsentation

172.16.0.1

10101100.00010000.00000000.00000001

IP-Adressen

Repräsentation

172.16.0.1

10101100.00010000.00000000.00000001

$$1*256^0+0*256^1+16*256^2+172*256^3=2886729729$$

IP-Adressen

Classless Inter-Domain Routing (CIDR)

172.16.0.1/24

IP-Adressen

CIDR verstehen

172.16.0.1/24

10101100.00010000.00000000.00000001

&

255.255.255.0

11111111.11111111.11111111.00000000

IP-Adressen

CIDR verstehen

172.16.0.1/24

10101100.00010000.00000000.00000001

&

11111111.11111111.11111111.00000000

=

10101100.00010000.00000000.00000000

IP-Adressen

CIDR verstehen

172.16.0.1/16

10101100.00010000.00000000.00000001

&

11111111.11111111.11111111.00000000

IP-Adressen

CIDR verstehen – so stimmt's tatsächlich 😏

172.16.0.1/16

10101100.00010000.00000000.00000001

&

11111111.11111111.00000000.00000000

IP-Adressen

CIDR verstehen

172.16.1.1/24

10101100.00010000.00000001.00000001

&

11111111.11111111.11111111.00000000

=

10101100.00010000.00000001.00000000

IP-Adressen

Chaos Computer Club Freiburg e.V.

- Hierarchisch aufgebaut
- Aggregierung über Netzmasken
- Konzept: Routing, siehe später.

IP-Adressen

Besondere Adressen 1

- Ist der Host-Teil 0, ist das die Netzadresse (172.16.0.0/24, aber: 172.16.0.128/25)
- Sind beim Host-Teil alle Bits 1, ist das die Broadcast-Adresse (172.16.0.255/24, aber: 172.16.0.255/25 und 172.16.0.127/25)
- RFC1918: zur privaten Verwendung, dürfen im Internet nicht geroutet werden:
  - 10.0.0.0/8 (2^{24}= 16.777.216 Adressen)
  - 172.16.0.0/12 (2^{20}= 1.048.576 Adressen)
  - 192.168.0.0/16 (2^{16}= 65.536 Adressen)
- 100.64.0.0/10 – CGNAT, Internetprovider (2^{22} = 4.194.304 Adressen, RFC 6598)
- 169.254.0.0/16 – Link Local Adressen (z.B. wenn kein DHCP-Server antwortet, RFC 3927)

IP-Adressen

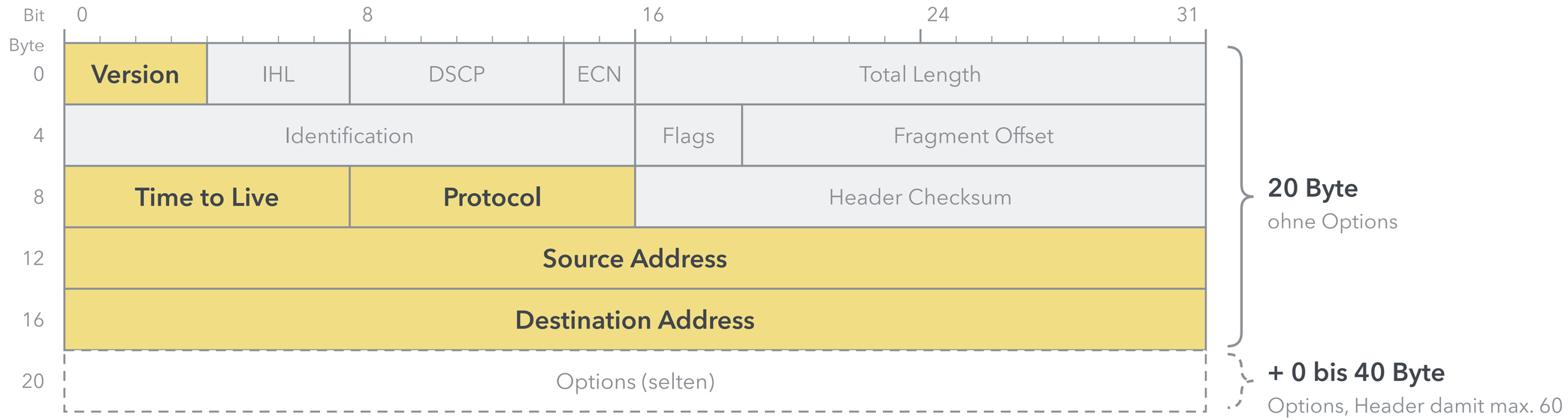
Besondere Adressen 2 (RFC 6890)

- 127.0.0.0/8 – Loopback, immer der lokale Host (there's no place like 127.0.0.1)
- 255.255.255.255/32 – Limited Broadcast (RFC 919, RFC 922)
- 192.0.2.0/24 – Reserviert für Dokumentationszwecke (TEST-NET-1, RFC 5737)
- 198.51.100.0/24 – reserviert für Dokumentationszwecke (TEST-NET-2, RFC 5737)
- 203.0.113.0/24 - reserviert für Dokumentationszwecke (TEST-NET-3, RFC 5737)
- 192.88.99.0/24 – reserviert für 6to4 anycast relay (RFC 3068, 2015 abgekündigt durch RFC 7526)
- 198.18.0.0/15 – reserviert für Benchmark tests (RFC 2544)
- 224.0.0.0/4 – reserviert für Multicast (RFC 5771)
- 240.0.0.0/4 – reserviert für zukünftige Benutzung (RFC 1112)

Chaos Computer Club Freiburg e.V.

IPv4

Header



die Felder für den Anfang

gibt es, später

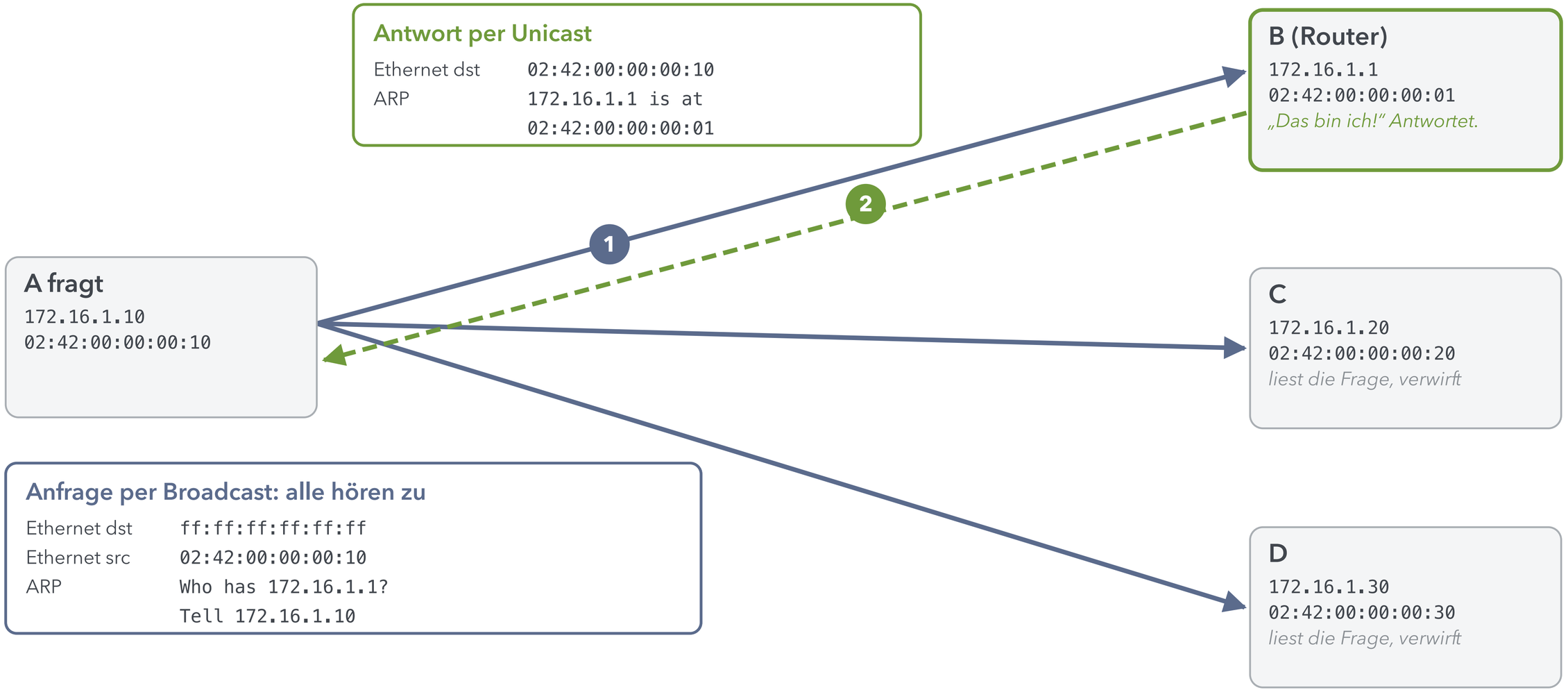
ARP

Klebstoff zwischen Layer 2 und Layer 3

Chaos Computer Club Freiburg e.V.

ARP

Adressauflösung



ARP

Mitschnitt

Paketliste

```
1  02:42:00:00:00:10 → Broadcast           ARP  Who has 172.16.1.1? Tell 172.16.1.10
2  02:42:00:00:00:01 → 02:42:00:00:00:10   ARP  172.16.1.1 is at 02:42:00:00:00:01
```

Paket 1 aufgeklappt

```
Ethernet II, Dst: ff:ff:ff:ff:ff:ff, Src: 02:42:00:00:00:10
    Type: ARP (0x0806)                ← kein IP-Header, ARP sitzt direkt auf Ethernet
Address Resolution Protocol (request)
    Opcode: request (1)               ← Antwort: reply (2)
    Sender MAC address: 02:42:00:00:00:10
    Sender IP address:  172.16.1.10
    Target MAC address: 00:00:00:00:00:00  ← gesucht
    Target IP address:  172.16.1.1
```

Chaos Computer Club Freiburg e.V.

ARP

ARP-Cache

Linux

```
$ ip neigh
172.16.1.1 dev eth0 lladdr 02:42:00:00:00:01 REACHABLE
```

macOS

```
$ arp -an
? (172.16.1.1) at 2:42:0:0:0:1 on en0 ifscope [ethernet]
```

Windows

```
> arp -a
  Internetadresse       Physische Adresse     Typ
  172.16.1.1            02-42-00-00-00-01     dynamisch
```

Eintrag löschen, die nächste Verbindung fragt neu

```
Linux: ip neigh flush dev eth0   macOS: arp -d 172.16.1.1   Windows: arp -d 172.16.1.1
```

ICMPv4

Chaos Computer Club Freiburg e.V.

ICMPv4

Internet Control Message Protocol

- Metadaten für IP-Verkehr
- Steuerung von IP-Verkehr
- Am wichtigsten:
  - ICMP Echo Request („ping“)
  - ICMP Echo Reply („pong“)
  - Time Exceeded
  - Destination unreachable

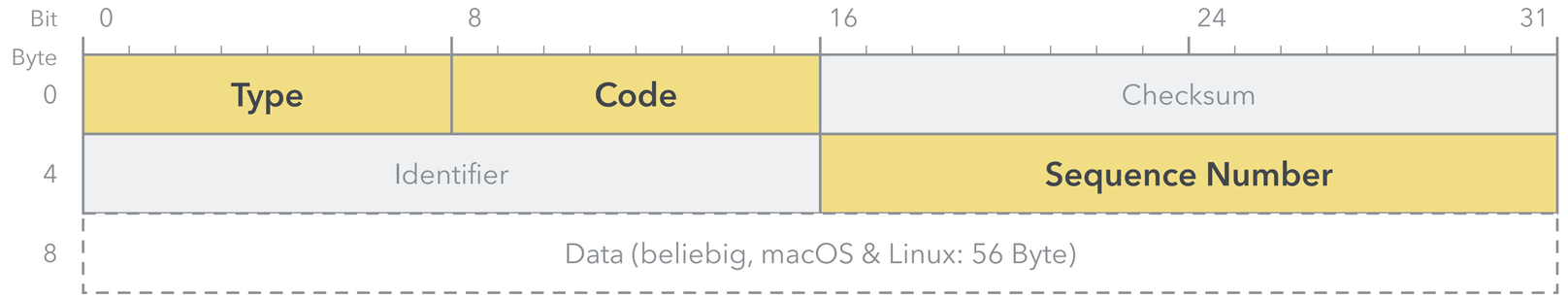
ICMPv4

Typen & Codes

Type	Code	Name	Bedeutung
8	0	Echo Request	ping fragt
0	0	Echo Reply	ping-Antwort
3	0	Net Unreachable	Router: keine Route zum Zielnetz
3	1	Host Unreachable	letzter Router: ARP ohne Antwort
3	3	Port Unreachable	Ziel: niemand lauscht auf dem UDP-Port
3	4	Fragmentation Needed	Paket > MTU, aber Don't Fragment gesetzt
3	13	Administratively Prohibited	Firewall lehnt ab
11	0	Time Exceeded	TTL abgelaufen → traceroute

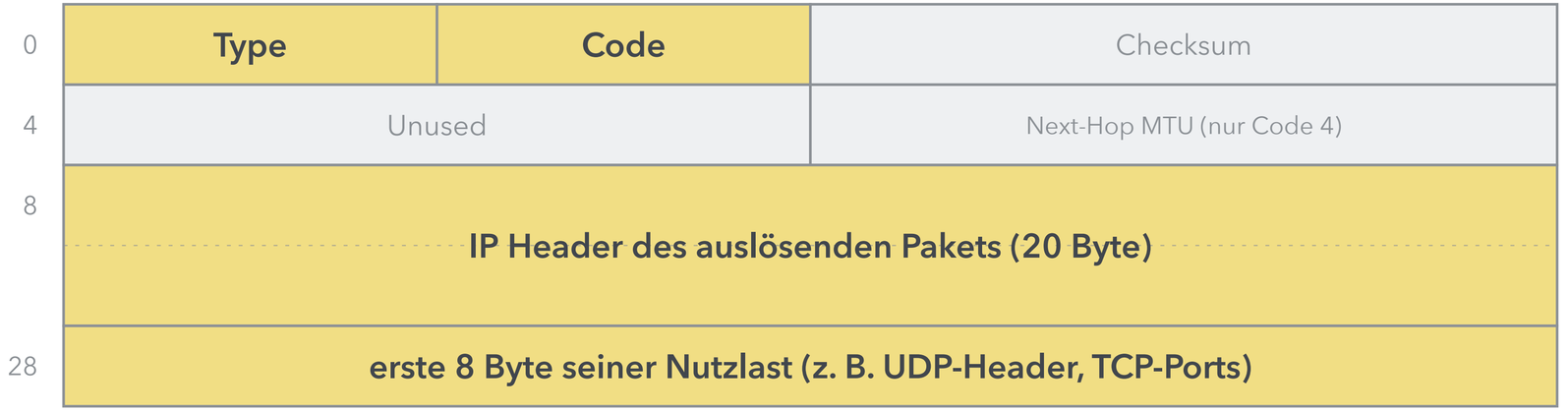
ICMPv4

Header



Echo Request / Reply
Type 8 / 0, ping

Data
kommt in der Antwort zurück



Fehlermeldungen
Type 3: Destination Unreachable
Type 11: Time Exceeded

die Felder für den Anfang

gibt es, später

ICMPv4

Bitte nicht wegfiltern

- Firewalls verwerfen ICMP gern pauschal: „Sicherheit“
- Jede Leitung hat eine Höchstgröße für Pakete: *Maximum Transmission Unit* (MTU), Ethernet 1500 Byte, DSL 1492
- Absender schickt 1500 Byte mit „Don't Fragment“
- Router vor der DSL-Leitung: „passt nicht, max. 1492“ (ICMP Fragmentation Needed)
- Absender verkleinert seine Pakete: *Path MTU Discovery* (PMTUD)
- Meldung weggefiltert → große Pakete verschwinden still
- Symptom: Verbindung steht, Webseite lädt halb, SSH hängt nach dem Login
- Durchlassen: Destination Unreachable & Time Exceeded

Routing…

… oder: wie komme ich zu ccc.de?

Hier geschieht Magie

(Magie: DNS)

(Domain Name System)

(eigener Vortrag)

Routing…

… oder: wie komme ich zu 185.106.84.100?

Routing

Klebstoff für das Internet

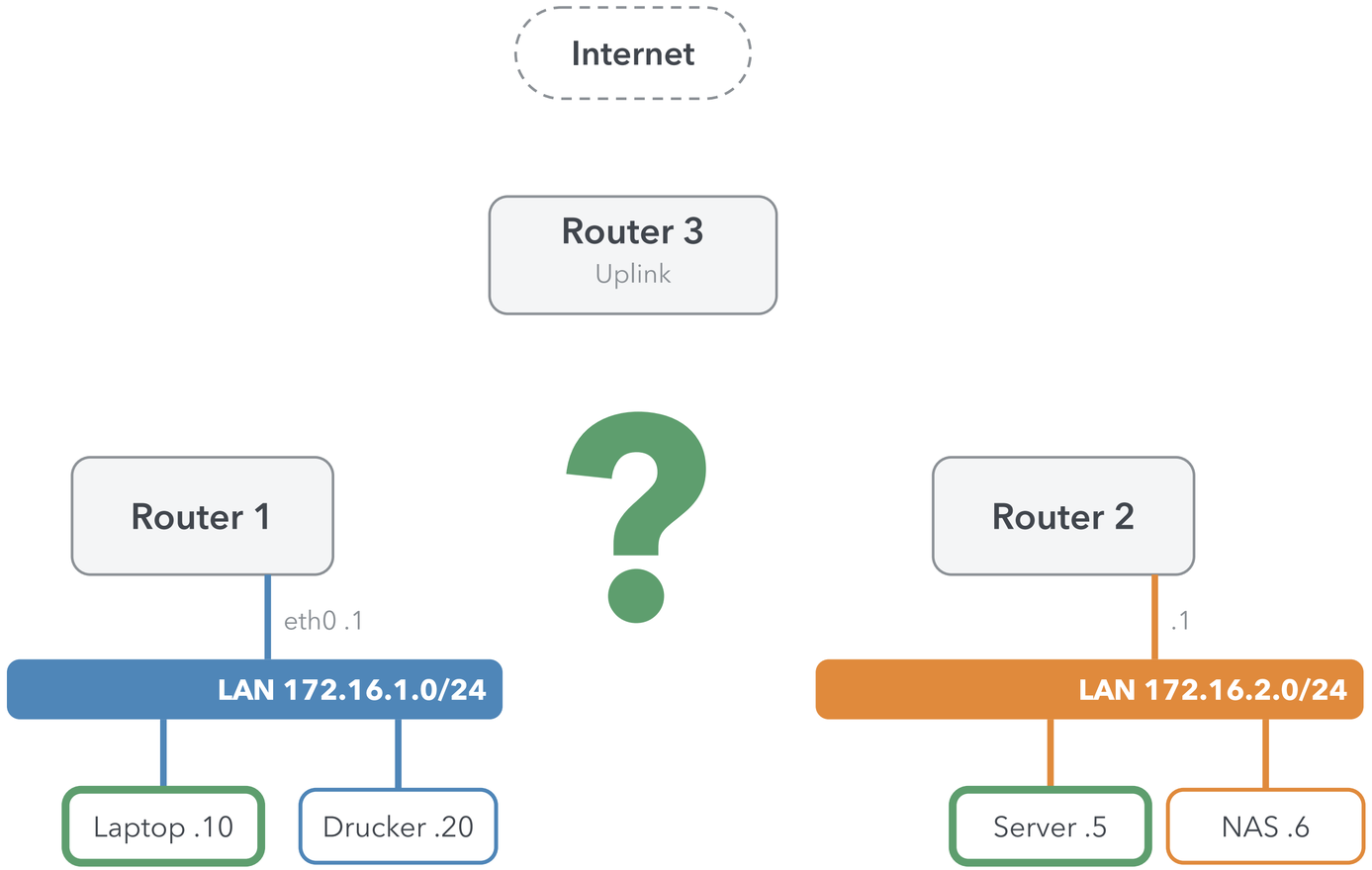
- Internet: kein einheitliches Netz, sondern *„ein Netz von Netzen“*
- Verbunden durch
  - Layer 1: Leitungen
  - Layer 2: Ethernet
  - Layer 3: Routing

Chaos Computer Club Freiburg e.V.

Routing

Rahmenbedingungen

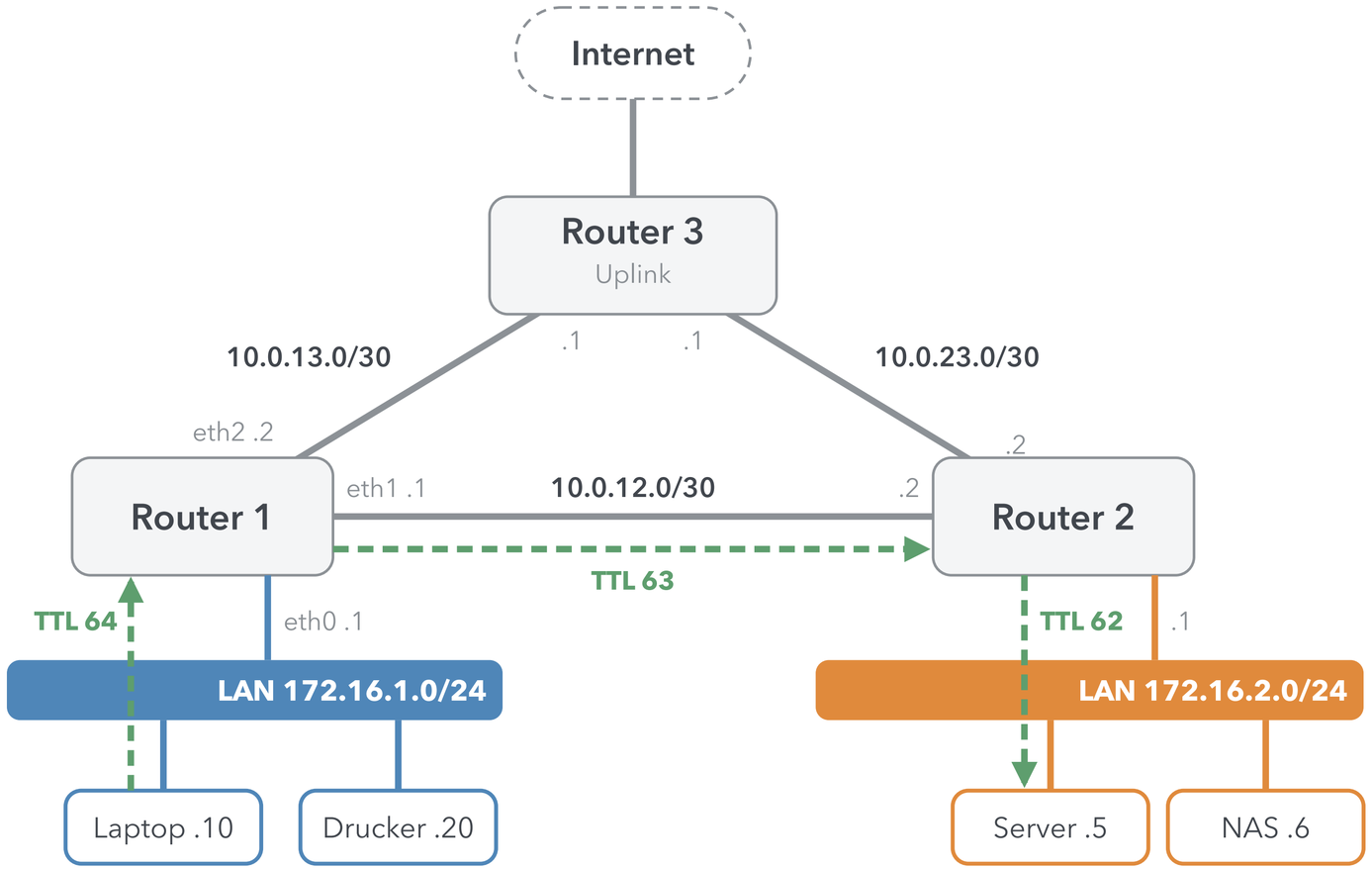
- Routing-Tabelle(n)
- Longest match wins
- Transport-/Transfernetze/Interlink



Wie kommt der Laptop zum Server?

172.16.1.10 → 172.16.2.5

Routing



Routing Table Router 1

Destination	Next Hop	Interface
172.16.1.0/24	connected	eth0
10.0.12.0/30	connected	eth1
10.0.13.0/30	connected	eth2
172.16.2.0/24	**10.0.12.2**	**eth1**
0.0.0.0/0	10.0.13.1	eth2

Longest Prefix Match: Von allen passenden Einträgen gewinnt der mit der längsten Maske. 0.0.0.0/0 passt auf jede Adresse: die Default Route.

Paket vom Laptop an 172.16.2.5

Jeder Router entscheidet für sich, nur anhand der Zieladresse und seiner Routing Table. Pro Hop sinkt die TTL um 1.

Chaos Computer Club Freiburg e.V.

Routing

So wird die Routing-Entscheidung getroffen

Paket an `172.16.2.5` `10101100.00010000.00000010.00000101`

Für jede Zeile der Routing Table: Zieladresse & Netzmaske. Kommt die Netzadresse der Zeile heraus, passt die Route.

Destination	Netzmaske	172.16.2.5 & Netzmaske	passt?	Prefix	
172.16.1.0/24 Next Hop: connected	11111111.11111111.11111111.00000000 /24 = 255.255.255.0	10101100.00010000.00000010.00000000 = 172.16.2.0 ≠ 172.16.1.0	**nein**		
10.0.12.0/30 Next Hop: connected	11111111.11111111.11111111.11111100 /30 = 255.255.255.252	10101100.00010000.00000010.00000100 = 172.16.2.4 ≠ 10.0.12.0	**nein**		
10.0.13.0/30 Next Hop: connected	11111111.11111111.11111111.11111100 /30 = 255.255.255.252	10101100.00010000.00000010.00000100 = 172.16.2.4 ≠ 10.0.13.0	**nein**		
172.16.2.0/24 Next Hop: 10.0.12.2	11111111.11111111.11111111.00000000 /24 = 255.255.255.0	10101100.00010000.00000010.00000000 = 172.16.2.0	**ja**	**/24**	**längster Prefix gewinnt**
0.0.0.0/0 Next Hop: 10.0.13.1	00000000.00000000.00000000.00000000 /0 = 0.0.0.0	00000000.00000000.00000000.00000000 = 0.0.0.0	**ja**	**/0**	

Zwei Zeilen passen: /24 und /0. Die /24 ist genauer, also geht das Paket an 10.0.12.2 (Router 2).

Die Default Route 0.0.0.0/0 passt immer: Maske aus lauter Nullen, Ergebnis 0.0.0.0. Sie greift nur, wenn nichts Genaueres passt.

IPv6

Ausblick

- IPv4: $2^{32} \approx 4{,}3$ Mrd. Adressen → aufgebraucht (IANA 2011, RIPE 2019)
- Notlösung: NAT, beim Provider sogar doppelt (CGNAT)
- IPv6: 128 Bit, hexadezimal: 2001:db8::1
- Präfix, Routing Table, Longest Prefix Match: alles wie gehabt
- … aber: kein ARP, kein Broadcast, Adressen per SLAAC, meist kein NAT

Nächstes Mal: IPv6, TCP & UDP