# Einführung in IPv6

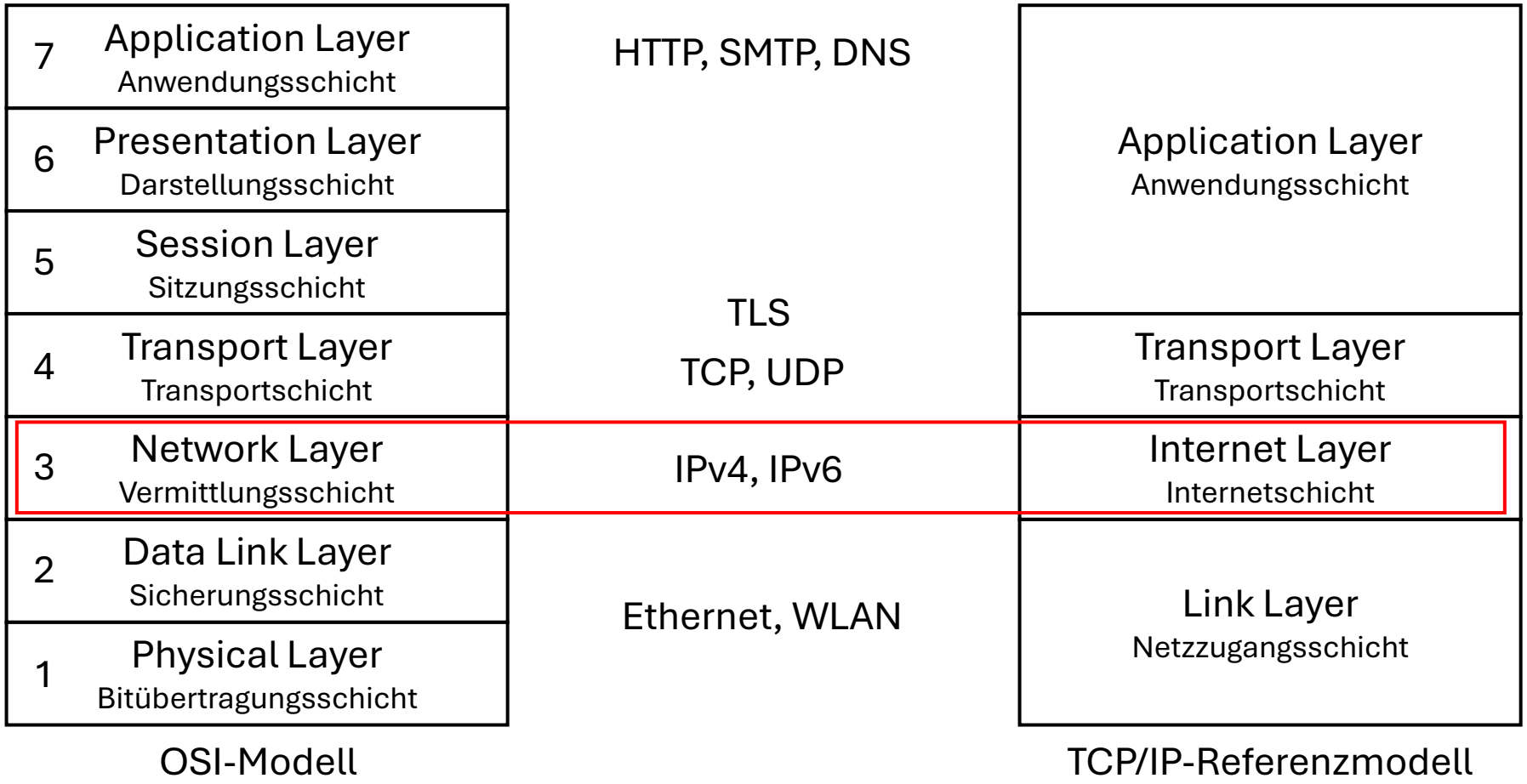
Matthäus Wander

# Inhaltsverzeichnis

# Grundlagen Internet Protocol

Kapitel 1

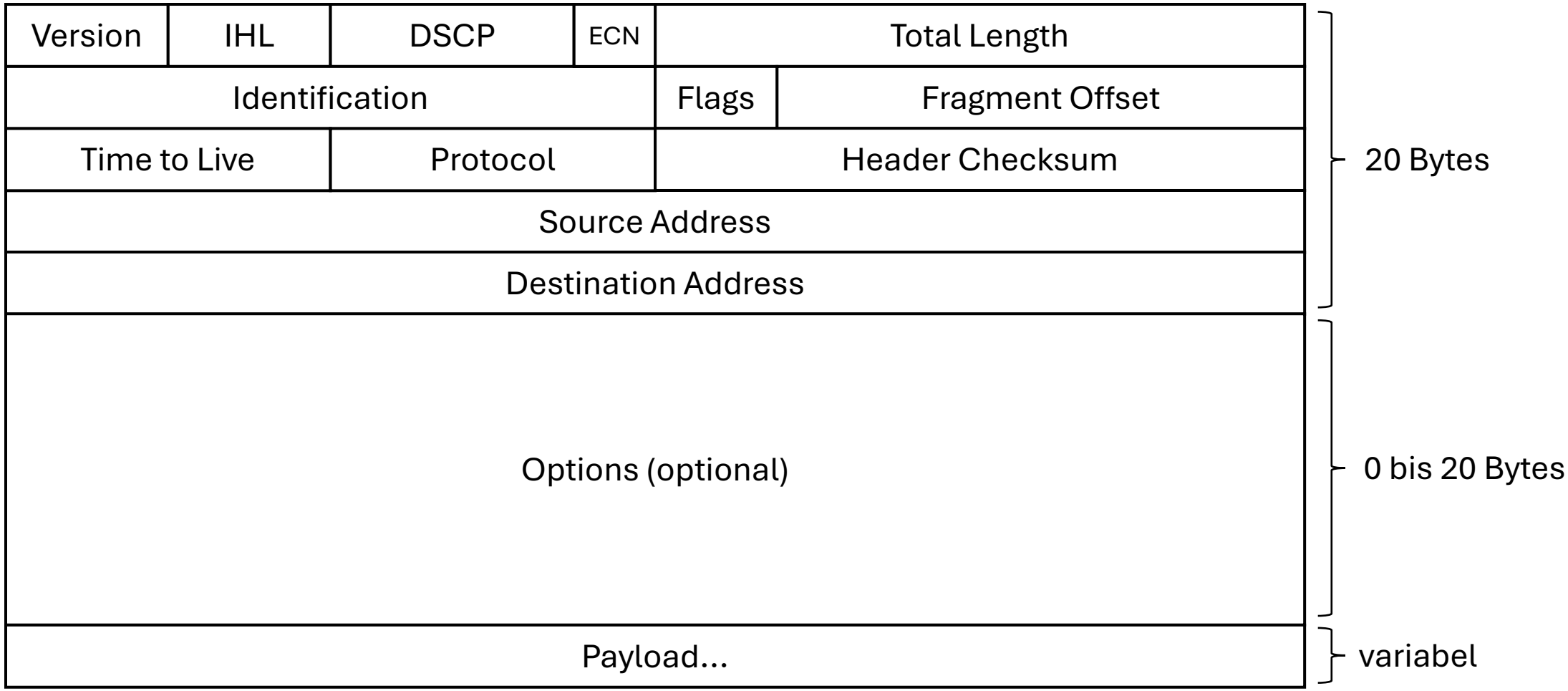
# Internet Protocol im Schichtenmodell



# Zweck des Internet Protocols (IP)

- Host-zu-Host-Kommunikation
  - Nicht zwischen Anwendungen → Aufgabe Transportschicht
- Paketvermittelte, verbindungslose Kommunikation
  - Keine garantierte Reihenfolge, keine Fehlerkorrektur
- Routing über Netzgrenzen hinweg
- Fragmentierung
  - Maximale Länge eines IP-Pakets: Maximum Transmission Unit (MTU)
  - IP-Fragmentierung zerlegt großes Paket in kleinere Fragmente
  - Häufige Fehlerquelle, sollte möglichst vermieden werden

# IPv4-Paketformat



# IPv4-Adresse

- 32 Bit Adressraum
  - $2^{32} = 4.294.967.296 \approx 4{,}29 \cdot 10^9$ (4,29 Milliarden)

- Schreibweise: dezimal in 4 Blöcken á 8 Bit
  - Je Block 0 bis 255 (8 Bit)
  - Beispiel: 192.0.2.100

# Subnetting

- IP-Adresse besteht aus Netz- und Hostanteil
  - Größe der Anteile ist bei IPv4 variabel
- Beispiel: 24 Bit Netz- und 8 Bit Hostanteil
  - Dezimal: 192.0.2.100
  - Binär: 1100 0000 . 0000 0000 . 0000 0010 . 01100100
- CIDR-Notation
  - 192.0.2.100/24
  - Suffix: Länge des Netzteils in Bit
- Subnetzmaske
  - 192.0.2.100/255.255.255.0
  - Binär: 1111 1111 . 1111 1111 . 1111 1111 . 0000 0000

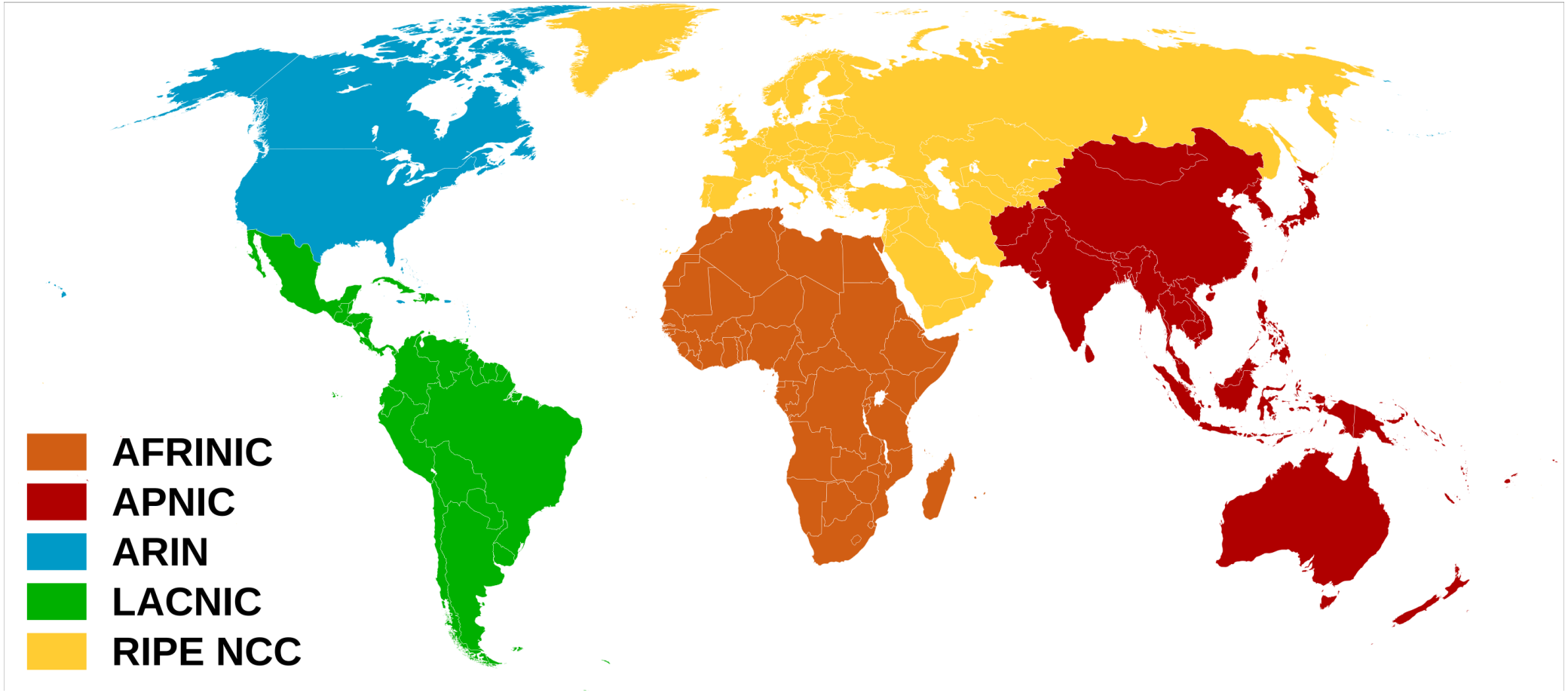
# Versionen des Internet Protocols

- IPv4 wurde 1981 spezifiziert (RFC 791)
- IPv5 war ein experimentelles Stream-Protokoll
- IPv6 ist ein neues Protokoll
  - Erstmals 1995 spezifiziert (RFC 1883, heute RFC 8200)
- IPv4 und IPv6 sind nicht kompatibel zueinander
  - Können aber parallel betrieben werden
  - Transitionsmechanismen ermöglichen den Übergang von IPv4 zu IPv6

# IP-Adressvergabe

Kapitel 2

# Regional Internet Registry

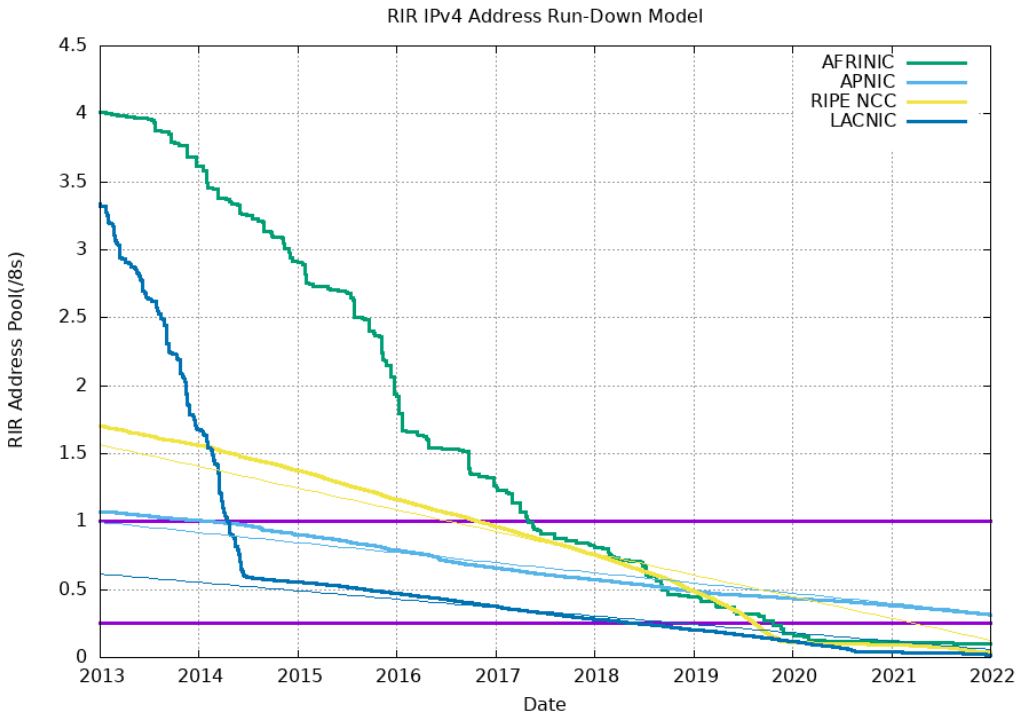


# Wer vergibt IP-Adressen?

- *Internet Corporation for Assigned Names and Numbers* (ICANN) definiert die weltweiten Richtlinien für IP-Adressvergabe
- *Internet Assigned Numbers Authority* (IANA) vergibt Adressblöcke an *Regional Internet Registry* (RIR)
  - Europa: Réseaux IP Européens Network Coordination Centre (RIPE NCC)
- RIR vergibt Adressblöcke an *Local Internet Registry* (LIR)
  - LIR ist üblicherweise ein Internet Service Provider (ISP)
- LIR vergibt Adressen an Endkunde
  - Provider-aggretable address space (PA): ISP besitzt Adressen
  - Provider-independent address space (PI): Endkunde besitzt Adressen

# IPv4-Adressverbrauch

- Feb 2011: IANA hat die letzten fünf /8 Blöcke an RIRs vergeben
- Nov 2019: RIPE NCC hat den letzten /22 Block vergeben
  - Seitdem Warteliste
- Ähnliche Situation bei anderen RIRs
- Privater Markt für IPv4-Adressen
  - Preis derzeit ca. 50€ pro Adresse



# IPv4-Adressknappheit

- IPv4 funktioniert nur durch Network Address Translation (NAT)
- Private Adressräume (RFC 1918) können frei verwendet werden
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- Praktisch alle Organisationen verwenden dieselben Adressräume
- Problem: Adressüberschneidung bei Netzkopplungen
  - Zusammenschluss von Organisationen
  - Anbindung von Private Clouds

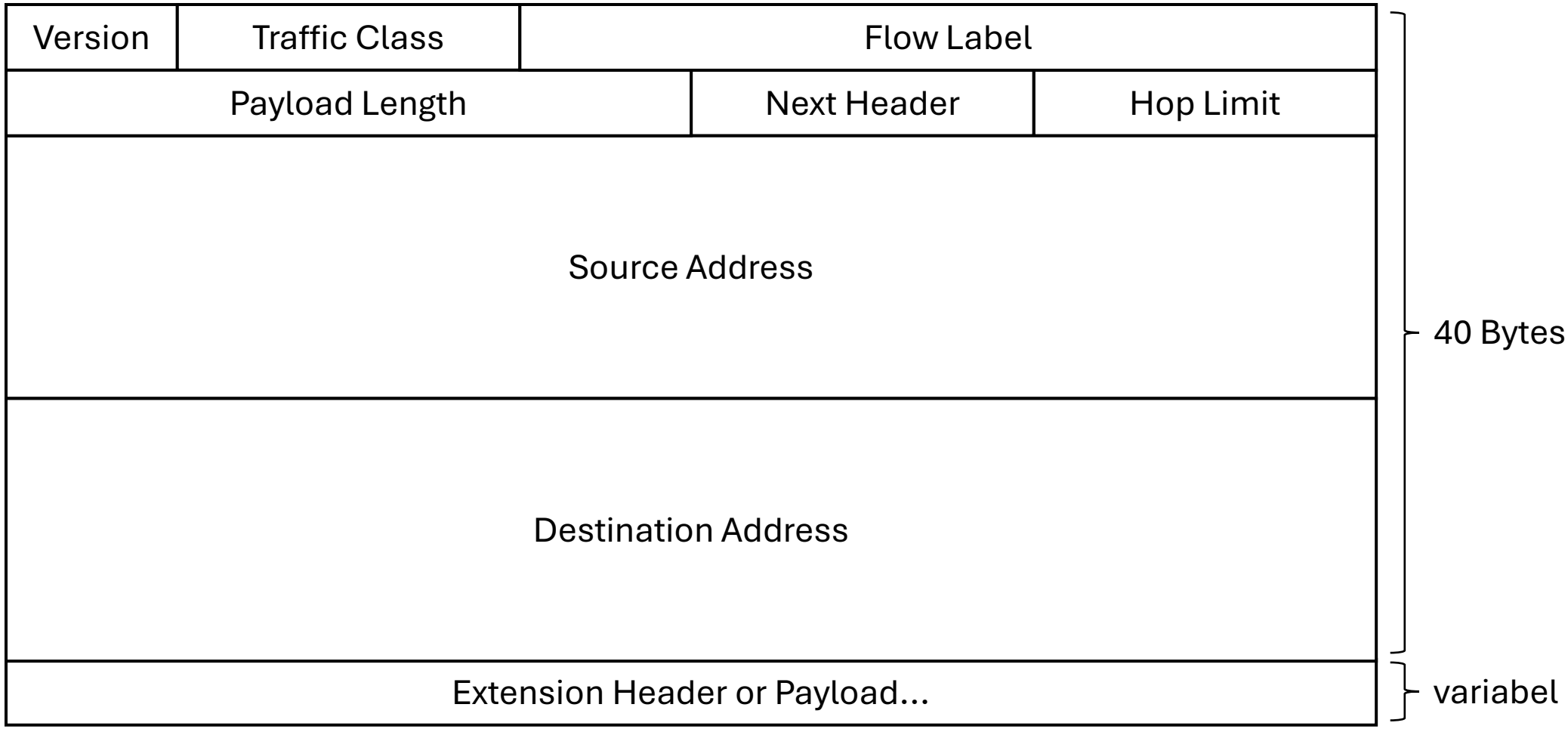
# IPv6: Konzept und Adressierung

Kapitel 3

# Konzeptionelle Neuerungen in IPv6

- Erheblich größerer Adressraum: 128 Bit
- Vereinfachter, aber längerer Header
  - Unterstützung für Erweiterungen über Extension Header
- Netz- und Hostanteil sind fix je 64 Bit lang
  - Keine Subnetzmaske notwendig
- Native Unterstützung mehrerer IPv6-Adressen gleichzeitig
  - Adressen haben verschiedene Scopes

# IPv6-Paketformat



# IPv6-Adresse

- 128 Bit Adressraum
  - $2^{128}$ = 340.282.366.920.938.463.463.374.607.431.768.211.456 ≈ $3{,}4 \cdot 10^{38}$
  - $6{,}67 \cdot 10^{17}$ (667 Billiarden) pro $mm^2$ der Erdoberfläche
  - Beachte jedoch Adressverschnitt durch Subnetting
    - 64 Bit Netzanteil ergibt $1{,}8 \cdot 10^{19}$ Netze

- Schreibweise: hexadezimal in 8 Blöcken á 16 Bit
  - Je Block 0000 bis ffff (16 Bit)
  - Beispiel: 2001:0db8:0000:0550:0000:0000:0000:baf1

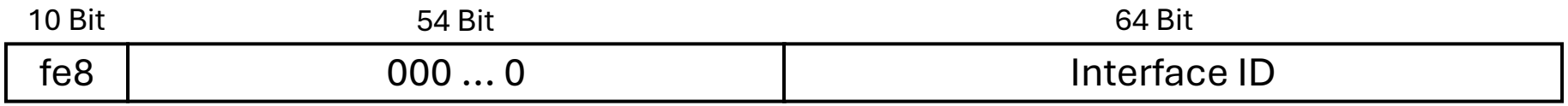
# IPv6-Adresse

- Führende Nullen können pro Block weggelassen werden
  - 2001:0db8:0000:0550:0000:0000:0000:baf1
  - 2001:db8:0:550:0:0:0:baf1
- Aufeinanderfolgende Nullblöcke können durch :: ersetzt werden
  - 2001:db8:0:550:0:0:0:baf1
  - 2001:db8:0:550::baf1
  - Aber nur ein mal (ungültig: ~~2001:db8::550::baf1~~)
- Gängige Schreibweisen in Anwendungen mit Portnummer:
  - Eckige Klammern um IPv6-Adresse: http://[2001:db8:0:550::baf1]:80
  - Port mit Punkt abtrennen: 2001:db8:0:550::baf1.80

# IPv6-Adresstypen

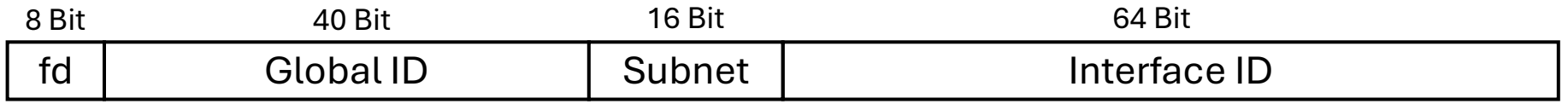
- Loopback ::1
  - Kommunikation mit sich selbst
  - Ähnlich wie 127.0.0.1 bei IPv4
- Unicast (1:1)
  - Link-local Address
  - Unique Local Address (ULA)
  - Global Unicast Address (GUA)
- Anycast (1:1 aus n)
- Multicast (1:n)

# Link-local Address



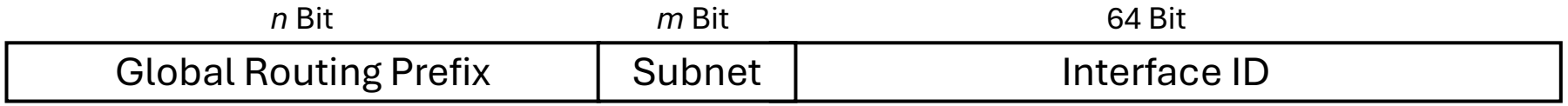

- Adressraum: fe80::/10
- Kommunikation nur im lokalen Netzsegment, wird nie geroutet
  - Ähnlich wie 169.254.0.0/16 bei IPv4 (APIPA)
- Anwendungsfälle:
  - Lokale Netzwerkdienste
  - Feste Adressen für das Heimnetz trotz wechselndem IPv6-Präfix
- Jede Netzwerkschnittstelle hat eigenen link-local Adressraum
  - Zone ID an Adresse zur Unterscheidung von Netzwerkschnittstellen
  - Beispiel: fe80::9386:9dd6:858f:4d9b%5 (link-local Adresse an Adapter „5“)

# Unique Local Address (ULA)




- Adressraum: fc00::/7 bzw. fd00::/8
- Wird im Internet nicht geroutet, kann aber in privaten Netzen geroutet werden
  - Ähnlich wie private Adressen bei IPv4 (RFC1918)
- 40 Bit Global ID **muss** zufällig gewählt werden, um Adresskollisionen bei Netzvereinigungen zu vermeiden
- 16 Bit Subnet ID zur freien Vergabe
- Ersetzt die frühere ~~Site-local Address fec0::/10~~ (deprecated)

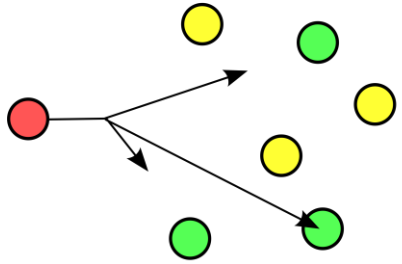
# Global Unicast Address (GUA)




- Adressraum 2000::/3 (2000:: bis 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff)
  - Global eindeutige Zuweisung
  - Kann im Internet geroutet oder nicht geroutet werden
- ISP weist Kunden Präfix mit *n* Bit Länge zu
  - Privatkunde: meist /56 pro Anschluss
  - Geschäftskunde: meist /48 pro Standort
  - Restliche 8 oder 16 Bit verfügbar für Subnetting auf Kundenseite

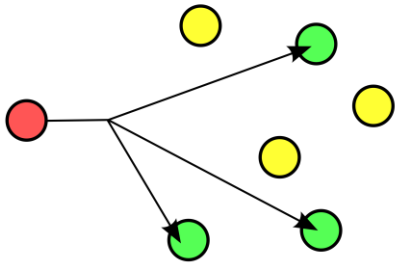
⇨ Für den Kunden ist die Subnet-Bitanzahl die relevante Kenngröße

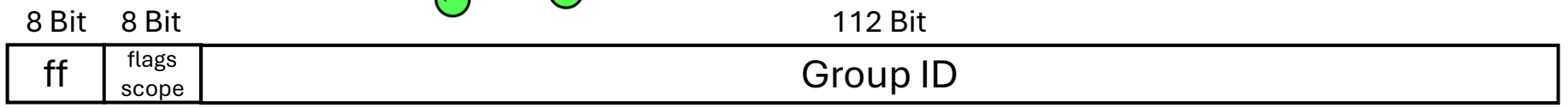
# Anycast



- Anycast adressiert 1 Ziel aus einer Gruppe von identischen Zielen
  - Verhält sich für den Client wie normale Unicast-Kommunikation
  - Verkehrssteuerung erfolgt durch Router
- Anwendungsfall global im Internet, weniger im lokalen Netz
  - Beispiel: Lastverteilung bei DNS Root Servern
- IPv6 reserviert einige Adressen für lokales Anycast
  - /64 Subnetzadresse soll an einen Subnetz-Router zugestellt werden
  - Beispiel: 2001:db8:0:550:: (Interface ID = 0)
  - Praktische Verbreitung unklar

# Multicast






- Multicast adressiert eine Gruppe von Zielen gleichzeitig
  - IPv6 Multicast löst den Broadcast ab
  - Zielgerichtete Gruppenkommunikation per Group ID
- Verschiedene Scopes
  - Link-Local: ganzes Netzsegment (essentiell für IPv6)
  - Admin-Local: konfigurierbares Netz
  - Site-Local: ganze Liegenschaft
  - Organization-Local: ganze Organisation

# IPv6: Netznahe Protokolle

Kapitel 4

# Netznahe Protokolle

- ICMPv6
- Neighbor Discovery Protocol
- Automatische IP-Adresszuweisung
  - Stateless Address Autoconfiguration (SLAAC)
  - DHCPv6
- Path MTU Discovery
- Extension Headers
  - Fragment Header

# ICMPv6

- ICMPv6 ist ein neues Protokoll ähnlich zu ICMP bei IPv4
  - Essentiell für eine funktionierende IPv6-Kommunikation
- Hilfreich zur Netzwerkdiagnose
  - Destination unreachable
  - Echo request/reply (Ping)
  - Time exceeded (Traceroute)
- Notwendig für:
  - Neighbor Discovery Protocol
  - Path MTU Discovery

# Neighbor Discovery Protocol

- Neighbor Discovery (ND) erbringt essentielle IPv6-Funktionen
  - Verwendet ICMPv6 link-local Multicast
- Neighbor Solicitation und Advertisement
  - Zuordnung von IPv6-Adresse zu MAC-Adresse (ersetzt ARP von IPv4)
  - Erkennung von IPv6-Adresskonflikten (Duplicate Address Detection)
- Router Solicitation und Advertisement
  - Bekanntmachung der IPv6-Basiskonfiguration
  - IPv6-Präfix, MTU, Default Router, DNS-Resolver
- Redirect
  - Umleitung auf anderen Router

# IP-Adresszuweisung für Hosts

- Manuelle Zuweisung
  - Statische IPv6-Adresse
  - Präfixlänge: /64 (andere Werte funktionieren nicht zuverlässig)
  - Default Router
  - DNS-Resolver
- Automatische Zuweisung
  - Zustandslos per SLAAC
  - Zustandsbehaftet per DHCPv6

# Stateless Address Autoconfiguration (SLAAC)

- SLAAC ermöglicht automatische IPv6-Adresskonfiguration
  - Ohne DHCP-Server und ohne Zuweisungstabelle
- Ablauf:
  1. Host leitet 64 Bit Interface ID aus seiner MAC-Adresse ab (EUI-64)
  2. Host sendet Router Solicitation
  3. Host empfängt Router Advertisement mit IP-Präfix
  4. IP-Präfix und Interface ID ergeben IPv6-Adresse
  5. Host prüft Adresskonflikt per Neighbor Solicitation

# Privacy Extensions

- Nachteil von SLAAC: Datenschutz
  - Aus fester MAC-Adresse ergibt sich feste Interface ID
  - Ermöglicht Nutzerverfolgung auch bei wechselndem IPv6-Präfix
- Lösung: Privacy Extensions for SLAAC in IPv6 (RFC 4941)
  - Wähle die 64 Bit Interface ID zufällig
  - Erzeuge alle paar Stunden eine neue Interface ID
- Gleitender Wechsel zwischen temporären IPv6-Adressen
  - Offene Verbindungen über $IP_{alt}$, neue Verbindungen über $IP_{neu}$
- Sinnvoll für Heimnutzer, weniger sinnvoll für Regierungsnetz

# Beispiel: Fritzbox und Windows 10

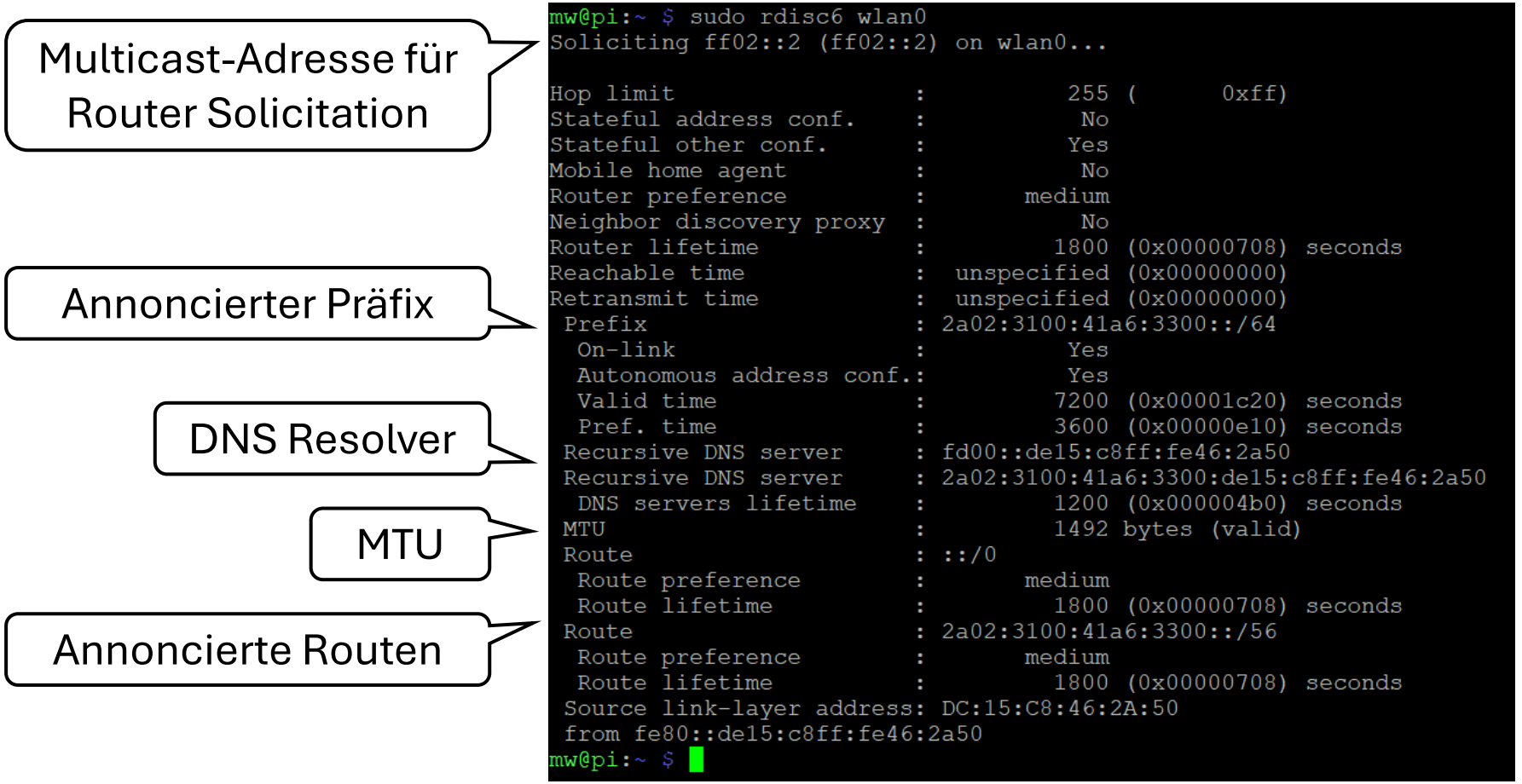
| | | |
|---|---|---|
| DSL | 🟢 | verbunden, ↓ 95,1 Mbit/s ↑ 35,3 Mbit/s |
| Internet, IPv4 | 🟢 | verbunden seit 07.01.2025, 03:21 Uhr<br>IPv4-Adresse: 2.243.238.176 |
| Internet, IPv6 | 🟢 | verbunden seit 07.01.2025, 03:21 Uhr<br>IPv6-Adresse: 2a02:3100:3203:ddcd:de15:c8ff:fe46:2a4d/64, Gültigkeit: 258125/171725s<br>IPv6-Präfix: 2a02:3100:41a6:3300::/56, Gültigkeit: 178143/91743s |
| Genutzte DNS-Server | | 62.109.121.2<br>62.109.121.1<br>2a01:c30::531 (aktuell genutzt für Standardanfragen)<br>2a01:c30::530 |

Internetzugangsanbieter vergibt dynamisch /56

```
Connection-specifi
Description . . . .                          ) I219-V
Physical Address. . . . . . . . . : 30-9C-23-8B-EB-70
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . . . . . . . : 2a02:3100:41a6:3300:8c7e:8811:fe17:1df1(Preferred)
Temporary IPv6 Address. . . . . . : 2a02:3100:41a6:3300:10e2:3cd8:3a94:6eb9(Preferred)
Link-local IPv6 Address . . . . . : fe80::9386:9dd6:858f:4d9b%5(Preferred)
IPv4 Address. . . . . . . . . . . : 192.168.178.31(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : 2. Januar 2025 21:38:29
Lease Expires . . . . . . . . . . : 17. Januar 2025 19:06:54
Default Gateway . . . . . . . . . : fe80::de15:c8ff:fe46:2a50%5
                                    192.168.178.1
DHCP Server . . . . . . . . . . . : 192.168.178.1
DHCPv6 IAID . . . . . . . . . . . : 103848995
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-4D-70-C0-30-9C-23-8B-EB-70
DNS Servers . . . . . . . . . . . : fd00::de15:c8ff:fe46:2a50
                                    2a02:3100:41a6:3300:de15:c8ff:fe46:2a50
                                    192.168.178.1
                                    fd00::de15:c8ff:fe46:2a50
                                    2a02:3100:41a6:3300:de15:c8ff:fe46:2a50
NetBIOS over Tcpip. . . . . . . . : Enabled
```

Privacy Extensions standardmäßig aktiv

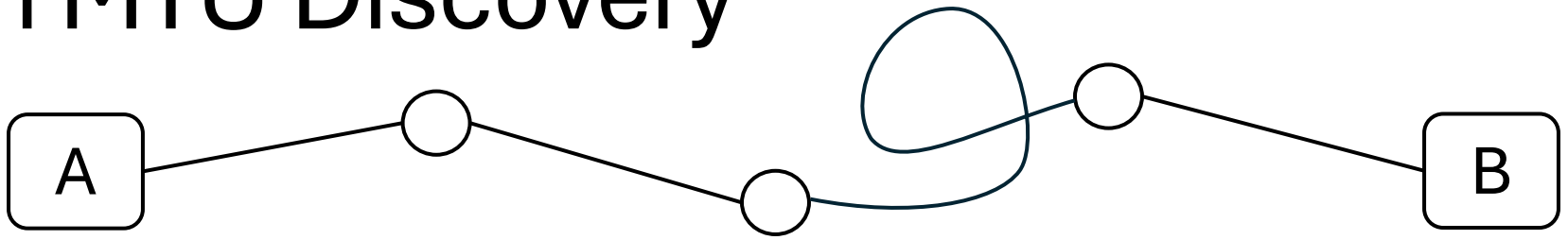
# Beispiel: Router Advertisement



# DHCPv6

- DHCPv6 ermöglicht zustandsbehaftete IPv6-Adresszuweisung
  - Zuweisung stabiler Adressen ähnlich wie DHCP bei IPv4
  - Dynamische DNS-Updates des Gerätenamens
  - Zuweisung temporärer Adressen prinzipiell auch möglich
- Zuweisung DNS-Resolver per DHCPv6 oder Router Adv. möglich
- DHCPv6 kann parallel zu SLAAC betrieben werden
  - Sinnvoll in heterogenen Umgebungen mit Systemen, die nicht beides voll unterstützen
  - Android unterstützt nur SLAAC

# Path MTU Discovery

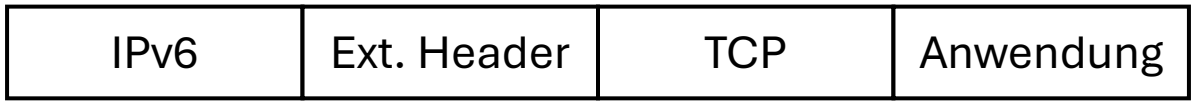



- Auf dem Weg zum Ziel durchläuft ein Paket verschiedene Netze
  - Netze verwenden potentiell unterschiedliche MTU-Werte
- Interface MTU ist der einstellbare Wert einer Netzwerkschnittstelle
- Path MTU ist die funktionierende MTU der Gesamtstrecke
  - Ergibt sich aus dem Minimum aller Interface MTUs der Strecke
  - Es gilt: Path MTU ≤ Interface MTU
- Path MTU Discovery (PMTUD) reagiert auf ICMPv6 „Packet too big“
  - … indem es die maximale Paketgröße für dieses Ziel reduziert

# Fragmentierung in IPv6

- Alle IPv6-Geräte müssen MTU ≥1280 Bytes unterstützen
  - Bei IPv4: ≥576 Bytes
- IPv6-Fragmentierung findet nur durch den sendenden Host statt
  - Bei IPv4: durch Host oder Router möglich
  - IPv6-Router fragmentieren nie, sondern senden ICMPv6 „Packet too big“
- IP-Fragmentierung soweit wie möglich vermeiden
  - TCP hat Maximum Segment Size und braucht keine Fragmentierung
  - UDP und IPsec brauchen evtl. IP-Fragmentierung
  - Möglichst auf Anwendungsebene segmentieren
- Fragmentierung bei IPv6 verwendet einen Extension Header

# Extension Header




- Erweiterungen werden als Extension Header hinter dem IPv6-Header eingefügt
  - Es können mehrere Extension Header hintereinander folgen
  - Geräte können unbekannte Extension Header überspringen
- Liste einiger Extension Header:
  - Fragment Header: IPv6-Fragmentierung
  - Hop-by-Hop Options: Optionen zum Auslesen durch Router
  - Destination Options: Optionen zum Auslesen durch Ziel-Host
  - Routing Header: ermöglicht Source Routing
  - Authentication Header und ESP: für IPsec-VPN

# Domain Name System

- DNS unterstützt IPv4- und IPv6-Adressen nebeneinander
- A Record für IPv4-Adresse
  - example  IN A  192.0.2.100
- AAAA Record für IPv6-Adresse
  - example  IN AAAA  2001:db8:0:550::baf1
- Rückwärtsauflösung über PTR Record
  - 100.2.0.192.in-addr.arpa
  - 1.f.a.b.0.0.0.0.0.0.0.0.0.0.0.0.0.5.5.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa
- Verbindung zum DNS-Server über IPv4 oder IPv6 möglich
  - DNS-Server kann über IPv4 auch AAAA Records transportieren

# Übergangsmechanismen und Verbreitung

Kapitel 5

# Dual Stack

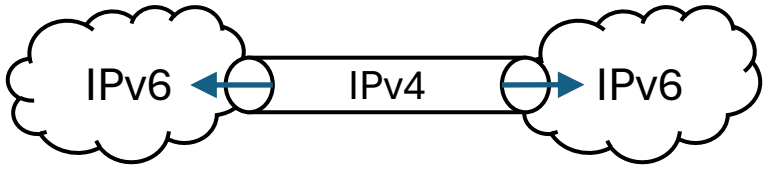
- Dual Stack (DS) ist der Parallelbetrieb von IPv4 und IPv6
  - Funktioniert auf nahezu allen IPv6-fähigen Geräten
- Vor- und Nachteile
  - ☺ Native Unterstützung beider Protokolle
  - ☺ Schleichender Übergang möglich
  - ☹ Doppelter Konfigurationsaufwand
- Dual Stack Lite (DS-Lite) für Breitband-Privatkunden
  - IPv6 nativ – IPv4 per Carrier-grade NAT
  - Eingeschränkte IPv4-Konnektivität führt zu Problemen mit VPN-Einwahl

# Dual Stack

- Wie entscheiden, ob Verbindung über IPv4 oder IPv6 erfolgt?
  - Default Address Selection for IPv6 (RFC 6724)
  - Präferenzalgorithmus wählt die „beste“ Quell- und Zieladresse
- Dual-Stack Client fragt gleichzeitig A und AAAA im DNS ab
  - Bei Vorliegen eines AAAA Records wird IPv6 bevorzugt

  ⇨ AAAA Record ist ein Signal dafür, dass der Server IPv6 wünscht
- „Happy Eyeballs“ Algorithmus ermöglicht schnellen Rückfall
  - Starte IPv6-Verbindungsversuch
  - Nach ca. 200 ms starte zusätzlichen IPv4-Verbindungsversuch
  - Vermeidet lange Verzögerung durch Verbindungs-Timeout

# Tunneling

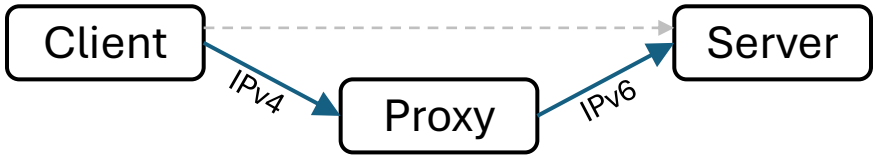



- Tunneling ermöglicht die Anbindung von IPv6-Inseln über IPv4
- IPv6-Historie hat viele Tunnelmechanismen hervorgebracht
  - 6in4, 6over4, 6to4, 6rd, AYIYA, ISATAP, Teredo
  - Mit Verbreitung von nativem IPv6 nicht mehr notwendig

⇨ Dual Stack ist die bessere Wahl

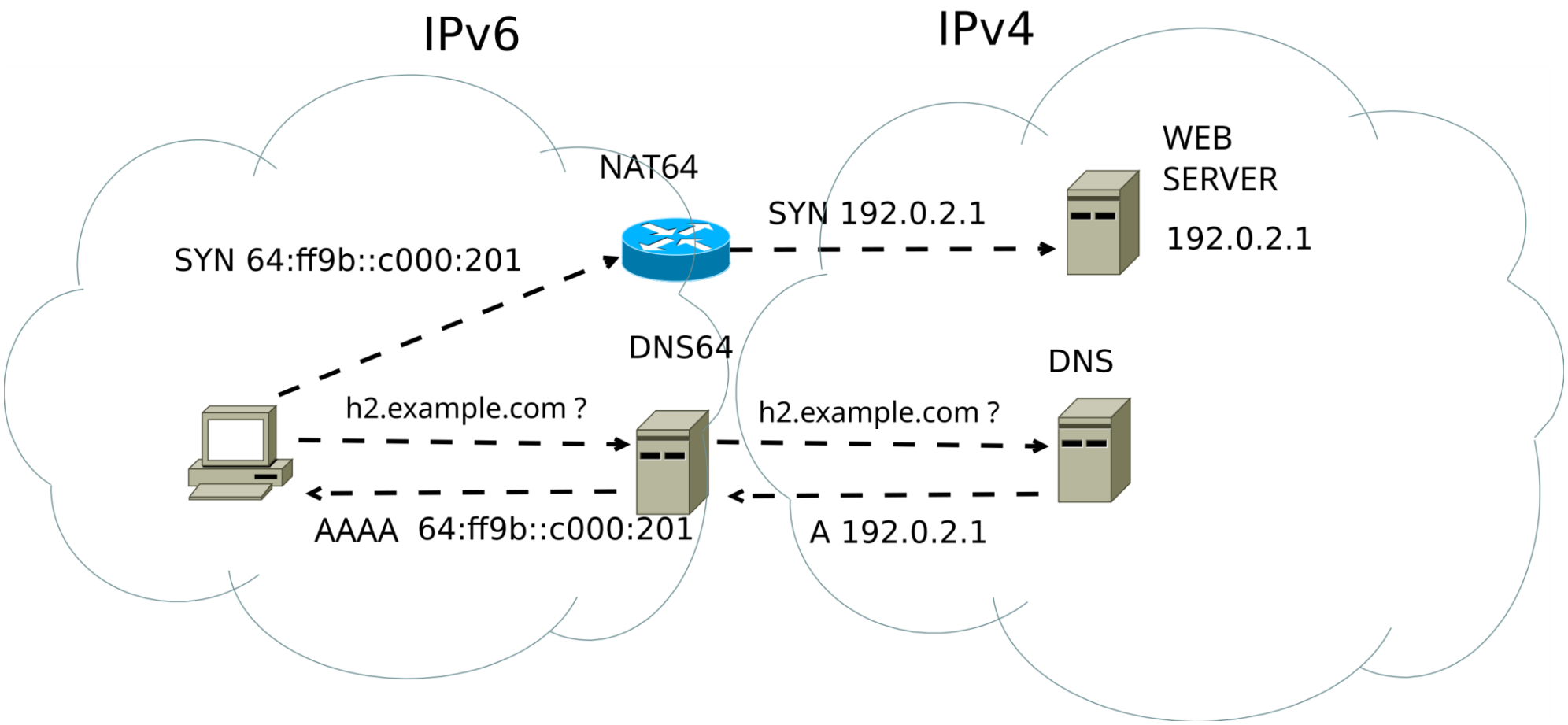
- In VPN-Szenarien kann 6in4 oder 4in6 Tunneling sinnvoll sein

# Adressübersetzung



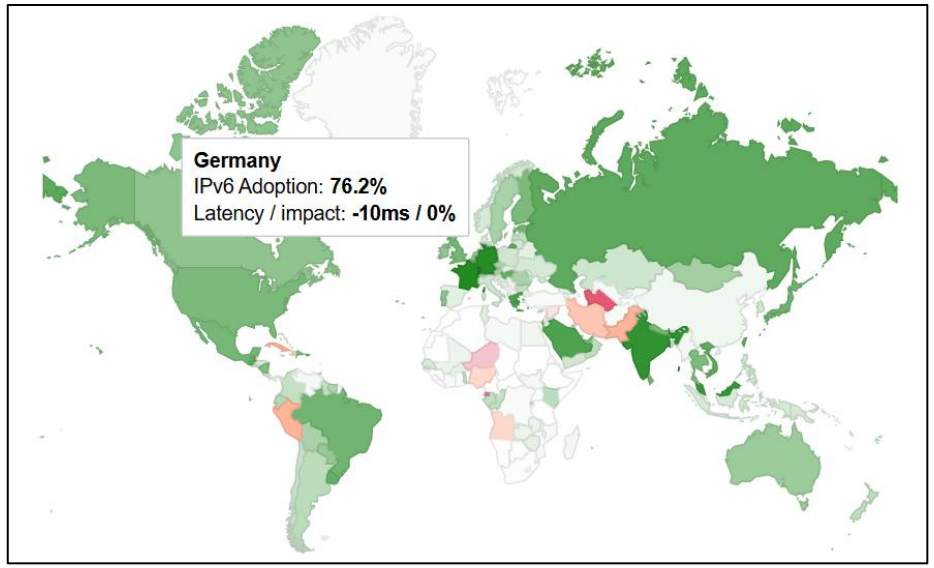

- Proxy kann zwischen IPv4 und IPv6 übersetzen
  - Setzt proxy-fähige Anwendung voraus
- NAT kann zwischen IPv4 und IPv6 übersetzen
  - Setzt NAT-fähige Anwendung voraus
- NAT64: Übersetzung von IPv6-Client zu IPv4-Server
  - Adressraum 64:ff9b::/96 zur Abbildung von IPv4-Adressen in IPv6
  - Beispiel: 64:ff9b::c000:0264 oder 64:ff9b::192.0.2.100
  - IPv6 kann per NAT64 beliebige IPv4-Zieladressen erreichen
  - DNS64 zur Umsetzung von A Record auf passenden AAAA Record

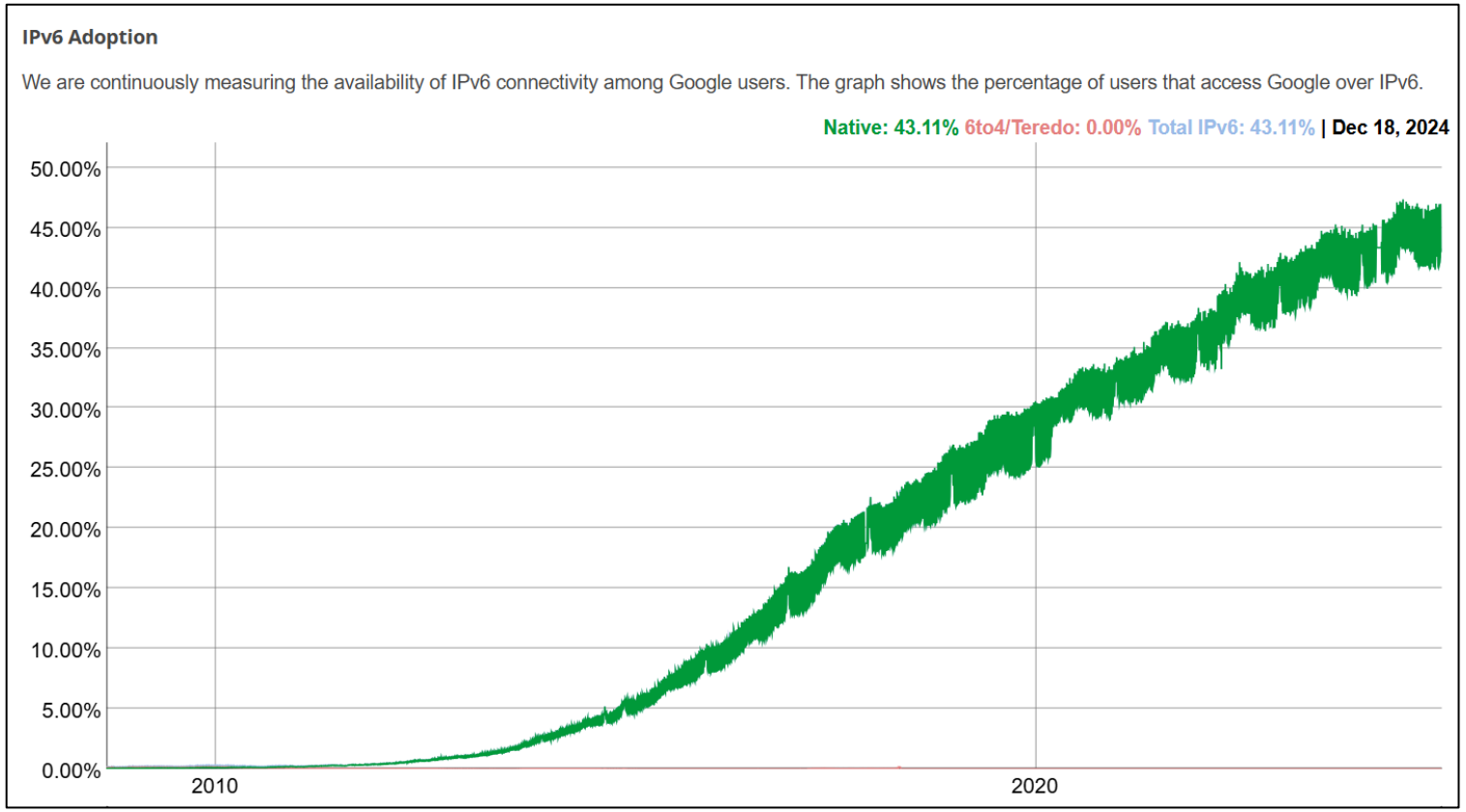
# NAT64 mit DNS64



# IPv6-Verbreitung

- Anteil an IPv6-Nutzern im Dezember 2024 laut Google:
  - 43 % weltweit
  - 76 % in Deutschland



# IPv6 beim Bund

- Bund hat LIR „de.government“ gegründet
  - 2a02:1000::/23 für Bund und Länder
  - Verschiedene untergeordnete Sub-LIRs
- Sub-LIR Bund vergibt Präfixe der Länge /36, /40, /44 oder /48 an Bundesbehörden zur freien Nutzung in eigenen Netzen

| Bereich | Name | Beschreibung |
|---|---|---|
| 2a02:11c0::/28 | **de.gov** | Routing nur innerhalb von Verwaltungsnetzen |
| 2a02:11f0::/28 | **de.non-gov** | Routing ins Internet |

- Beide Global Unicast (GUA), aber nur einer für Routing ins Internet

# IPv6 beim Bund

- Politischer Auftrag zur Einführung von IPv6 beim Bund
  - KoITB (heute CIO Board) Beschluss 2020/13 und 2020/14
- Netze des Bundes (NdB) unterstützen noch kein IPv6
- Bund-Länder-Verbindungsnetz (VN) unterstützt IPv6
- Der geplante Informationsverbund Öffentliche Verwaltung (IVÖV) soll IPv6 unterstützen
- BMI und BDBOS unterstützen die Einführung mit einem IPv6-Programm des Bundes

# Sicherheitsbetrachtung

Kapitel 6

# Sicherheitsbetrachtung

- Neuerungen bieten Potential für neue Sicherheitsprobleme
  - Sicherheitsimplikationen müssen neu bedacht werden
- IPv6-Herstellerunterstützung ist nicht so bewährt wie IPv4
  - Testen, testen, testen
- Umgehung von Schutzmaßnahmen
  - Können mit IPv6 bestehende Schutzmaßnahmen umgangen werden?
  - Filterung von Tunneling durch Firewall
  - Abschaltung von jeweils nicht konfiguriertem IPv4/IPv6 Stack

# Sicherheitsbetrachtung

- Extension Header
  - Welche sind notwendig/erwünscht, welche an der Firewall gefiltert?
  - Prüfung von Fragment Headern durch Firewall
- ICMPv6 ist essentiell für das Funktionieren von IPv6
  - Welche ICMPv6-Nachrichten sind erwünscht und welche nicht?
  - Gezielte Filterung an Netzgrenzen
- Filterung von IPv6-Adressen
  - Welche Adressen sind intern? (ULA und auch GUA)
  - Filterung von internen Unicast- und Multicast-Adressen an Netzgrenzen
  - Sowohl aus- als auch eingehend (Source Spoofing)

# Spezifische Angriffe

- Neighbor Discovery Spoofing
  - Kryptographische Absicherung mit Secure Neighbor Discovery (SEND)
- Rogue DHCPv6 und Rogue Router Advertisement
  - DHCPv6 Guard und RA Guard
- Rogue Source Routing und Redirect
  - Funktionen deaktivieren
- Allgemeine Gegenmaßnahmen
  - 802.1x Access Control
  - Mikrosegmentierung und internes Firewalling
  - Software-Defined Networking mit Sicherheitsrichtlinien

# Literatur

- Bundesamt für Sicherheit in der Informationstechnik:
  - Leitfaden für eine sichere IPv6-Netzwerkarchitektur (ISi-L-IPv6)
  - Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)
- National Institute of Standards and Technology:
  - Guidelines for the Secure Deployment of IPv6 (800-119)
- Internet Engineering Task Force:
  - Enterprise IPv6 Deployment Guidelines (RFC 7381)
  - Operational Security Considerations for IPv6 Networks (RFC 9099)