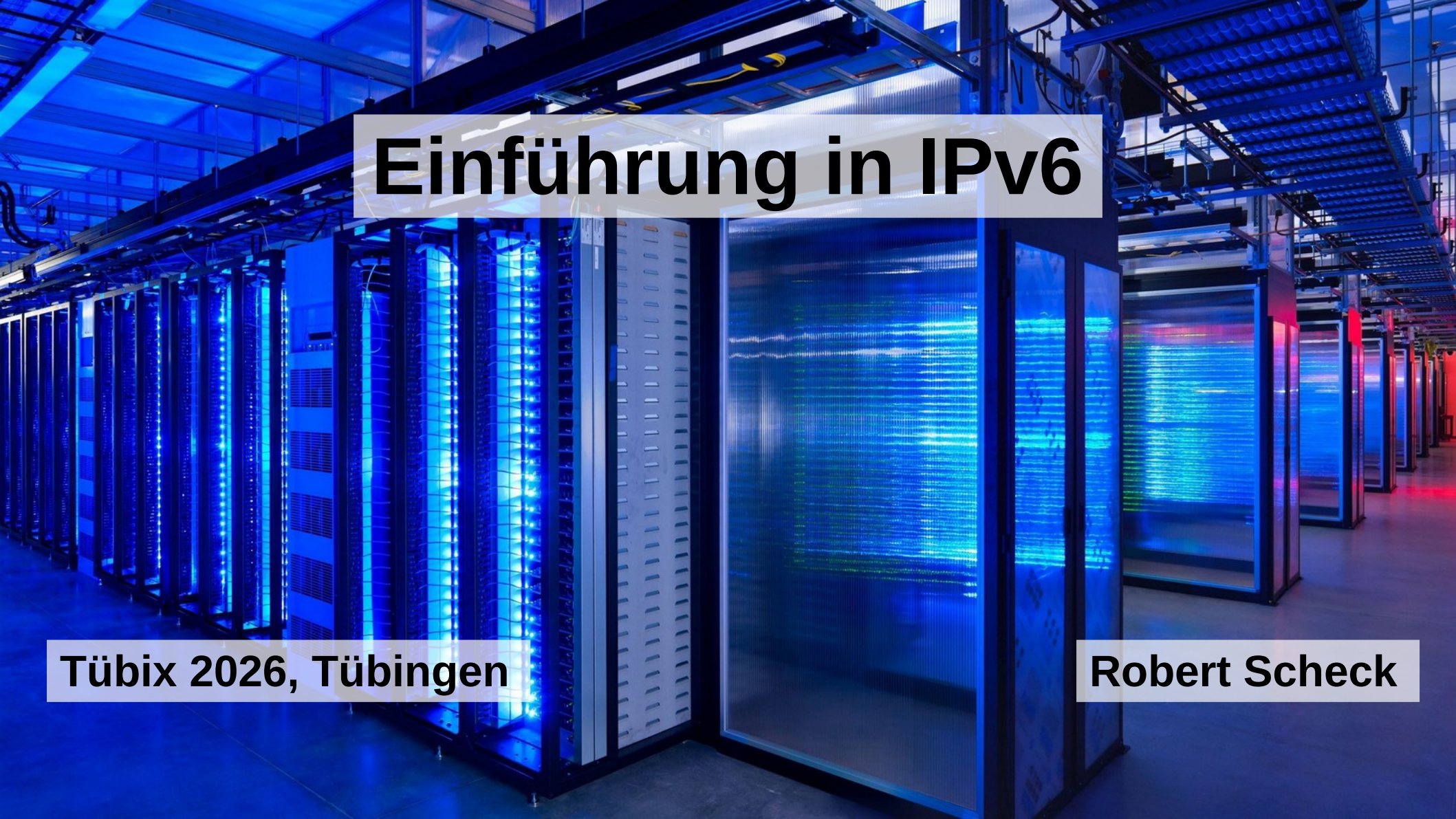


Einführung in IPv6

Tübix 2026, Tübingen

Robert Scheck

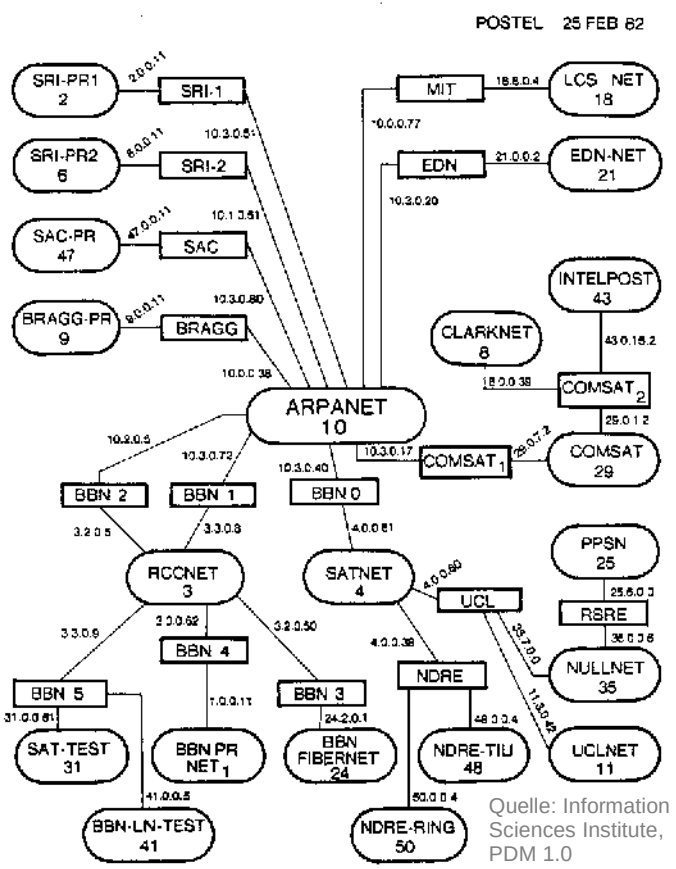
Robert Scheck

- Mitwirkender beim Fedora Project (seit 2005)
  - Package Maintainer (ca. 250 Pakete) mit Fokus auf EPEL
  - Provenpackager und Packager Sponsor
- Mitwirkender bei diversen anderen Open-Source-Projekten
  u.a. aggregate6, bgpdump, bgpq4, iputils, jwhois, rpki-client, systemd
- Verwendung von IPv6: Getunnelt seit 2002, nativ seit 2005
- Unterstützung des RPM-Paketbaus der RIPE Atlas Probe

- Mail: robert@fedoraproject.org
- Web: https://fedoraproject.org/wiki/RobertScheck

Es war einmal…

- 1981: RFC 791
  - Internet Protocol version 4 („IPv4“)
  - RFC 755, Seite 6 für IPv0 bis IPv3
  - Ab 1982 im SATNET (Atlantic Satellite Packet Network) mit `4.0.0.0/8` verwendet
  - Ab Januar 1983 im ARPANET (Advanced Research Projects Agency Network) mit `10.0.0.0/8` verwendet



Quelle: Information Sciences Institute, PDM 1.0

...aber warum IPv6?

- IPv4: 32-Bit-Adressierung ermöglicht ≈ 4,3 Mrd. Adressen
  - Heute:
    - ≈ 8,3 Mrd. Menschen, mehr als die Hälfte mit Smartphone
    - Angeblich mehr als 100 Mio. physische Server
  - Viele IPv4-Adressen ineffizient vergeben oder historisch reserviert
    - `127.0.0.0/8`: ≈ 16 Mio. Adressen für Loopback-Adressen auf „localhost“
    - 12x /8 für US Department of Defense, 1x /8 für jeweils Apple, Ford, Daimler
    - `224.0.0.0/4`: ≈ 270 Mio. Adressen reserviert für Multicast, früher „Class D“
    - `240.0.0.0/4`: ≈ 270 Mio. Adressen reserviert für zukünftige Nutzung, „Class E“
  - Internet ist deutlich größer geworden als ursprünglich geplant
    - z.B. Smartphones/Tablets, Internet of Things (IoT)

Aber es gibt doch NAT!

- 1994: RFC 1631 beschreibt NAT als **kurzfristige Übergangs-lösung** → Verlust eindeutiger IP-Adressen und Peer-to-Peer
- 1995: RFC 1883 spezifiziert Internet Protocol version 6 („IPv6“)
  - Damals noch häufig auch „IP Next Generation“ (IPng) genannt
- 1996: RFC 1918 definiert private IPv4-Adressbereiche
  - `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`
- 2011: RFC 6264 beschreibt Carrier-Grade NAT (CGN, CGNAT)
  - „Provider-NAT“ verhindert eingehende Portweiterleitungen
  - Spürbare (VPN-) Probleme während COVID-19-Lockdowns

IPv6

- 128-Bit-Adressierung ermöglicht 340 Undezillionen Adressen
  - 340.282.366.920.938.463.463.374.607.431.768.211.456 Adressen
  - Genügend IPv6-Adressen um jedem Sandkorn eine zuzuweisen
- Genügend eindeutige öffentliche Adressen für jedes Gerät
- Direkte Erreichbarkeit (Ende-zu-Ende-Prinzip) wieder möglich
- Moderne Protokollmechanismen von Anfang an eingeplant
  - Multicast statt Broadcast, automatische Adresskonfiguration
- IPv6 ist keine Erweiterung von IPv4
  - Neues Internetprotokoll und einigen grundlegend anderen Konzepten

Warum reden wir überhaupt über IPv6?

- Erforderliche Umstellungen wurden und werden hinausgezögert
- IPv6 ist seit über 30 Jahren standardisiert
- IPv4 wird durch Übergangslösungen seit 30 Jahren verlängert
- Viele Altsysteme (vor 1995) unterstützen weiterhin nur IPv4
- Ein Teil moderner Software ist leider weiterhin IPv4-zentriert
- IPv6 wird in Ausbildung und Lehre oft nachrangig behandelt
- Einige Internet-/Hosting-Provider bieten weiterhin nur IPv4 an
- Mittlerweile wirtschaftliche und technische Grenzen bei IPv4

IPv6-Adressen

- Aufbau und Darstellung:
  - 128 Bit Länge, komprimierte Darstellung möglich
  - Darstellung in 8 Blöcken zu je 16 Bit (Hextets)
  - Hexadezimale Schreibweise: 0-9, a-f
  - Beispiel: `2001:0db8:0407:0000:0000:c215:1200:1250`
- Führende Nullen dürfen in jedem Hextet weggelassen werden
  - Beispiel: `2001:db8:407:0:0:c215:1200:1250`
- Ersetzung des längsten zusammenhängenden Nullblocks durch `::`
  - Beispiel: `2001:db8:407::c215:1200:1250`
  - Wichtig: Kürzung auf `::` nur einmal je IPv6-Adresse erlaubt!

IPv6-Adressbildung im Detail

- IPv6-Adresse besteht aus Netzpräfix und Interface Identifier
  - Typisch: 64 Bit Netzpräfix (vom Router/Provider) + 64 Bit Hostanteil
  - Beispiel: `2001:db8:abcd:1200:0211:22ff:fe33:4455/64`
- Herkunft des Interface Identifiers (IID):
  - EUI-64: Klassisch, heutzutage eher seltener verwendet
    - Basiert auf der MAC-Adresse, wird automatisch erzeugt
  - Privacy Extensions: Temporäre Adressen, heutzutage Standard
    - Zufällig generierter Interface Identifier (IID)
    - Regelmäßig wechselnde IPv6-Adresse um Tracking zu verhindern
- Ein Gerät besitzt oft mehrere IPv6-Adressen gleichzeitig

IPv6-Netzpräfixe

- Typische IPv6-Netzpräfixe:
  - /64: Standardgröße für ein einzelnes Netzwerk
  - /56 bzw. /52: Häufige Zuweisung für Privatkunden und Selbstständige
  - /48: Typische Zuweisung für Unternehmen und Organisationen
- IPv6 hat riesige Netze:
  - /64: 18.446.744.073.709.551.616 IPv6-Adressen
  - /56: 4.722.366.482.869.645.213.696 IPv6-Adressen
  - /52: 75.557.863.725.914.323.419.136 IPv6-Adressen
  - /48: 1.208.925.819.614.629.174.706.176 IPv6-Adressen

IPv6-Adressverschwendung?!

- Machen wir jetzt den gleichen „Fehler“ wie bei IPv4? Nein!
- IPv6 ist nicht auf maximale Adressausnutzung optimiert
- Wichtiger ist eine einfache und einheitliche Netzstruktur
- Vorteile durch neues Adressierungsmodell:
  - Einfache Netzplanung und einfaches Subnetting
  - Effizientes Routing durch Präfix-Aggregation
  - Keine sparsame Adressvergabe mehr erforderlich
  - /64 ist das Standardnetz – unabhängig von der Anzahl der Geräte

IPv6-Subnetz-Matrix

IPv6-Präfix	Anzahl /48-Subnetze	Anzahl /56-Subnetze	Anzahl /64-Subnetze	Nutzbare Bits
/19	536.870.912	137.438.953.472	35.184.372.088.832	109
/29	262.144	134.217.728	34.359.738.368	99
/32	65.536	16.777.216	4.294.967.296	96
/48	1	256	65.536	80
/52		16	4.096	76
/56		1	256	72
/60			16	68
/64			1	64

- Formel zur Berechnung: $2^{(\text{Subnet-Präfix} - \text{Supernet-Präfix})} \rightarrow 2^{(64-48)} \rightarrow 2^{16}$

IPv6-Adresstypen

- Global Unicast (GUA)
  - `2000::/3` für öffentlich routbare IPv6-Adressen („Internet“)
  - Aktuell ist nur ⅛ aller IPv6-Adressen für das Internet vorgesehen
- Link Local (LLA)
  - `fe80::/10` nur im lokalen Netzwerk gültig (nicht routbar)
  - Automatisch auf jeder Netzwerkschnittstelle vorhanden
- Unique Local Address (ULA)
  - `fc00::/7` (praktisch `fd00::/8`) für nicht öffentlich routbare Netze
- Multicast
  - `ff00::/8` für Kommunikation mit Empfängergruppe, da kein Broadcast

Global Unicast vs. Unique Local Address

- `2000::/3` für Global Unicast (GUA):
  - Ermöglicht Ende-zu-Ende-Kommunikation ohne NAT („Internet“)
  - Benötigt allerdings weltweit routbaren IPv6-Präfix vom Provider
  - Interne Server bei statischem IPv6-Präfix einfach zu betreiben
- `fc00::/7` für Unique Local Address (ULA):
  - Ähnlich zu privaten IPv4-Adressen (nicht global/öffentlich routbar)
  - Geräte ohne GUA, aber mit ULA + IPv4, nutzen für Internetzugang IPv4
  - Dynamischer GUA-Präfix macht ULA primär attraktiv, wenn feste IPv6-Adressen (also mit statischem Präfix) für interne Systeme, z.B. Server, benötigt werden

ARP vs. Neighbor Discovery

IPv4: ARP

- Address Resolution Protocol
- Broadcast: „Wer hat IP X?“
- Antwort vom Zielgerät direkt

IPv6: NDP

- Neighbor Discovery Protocol
- Basiert auf ICMPv6
- Nutzt Multicast statt Broadcast
- Übernimmt mehrere Aufgaben:
  - Address Resolution
  - Router Discovery
  - Duplicate Address Detection

IPv6 ersetzt ARP durch ein erweitertes Protokoll (NDP) auf Basis von ICMPv6 und Multicast

Wie erhalten Geräte IPv6-Adressen?

- Stateless Address Autoconfiguration (SLAAC)
  - Gerät konfiguriert sich selbstständig ohne zentrale Vergabe
  - Router kündigt nur den Netzpräfix (/64) an
  - Gerät erzeugt daraus seine eigene IPv6-Adresse
  - Funktioniert ohne zentralen DHCP-Server
- Vereinfachter Ablauf:
  - Router sendet Router Advertisement (RA) → Teil von NDP (ICMPv6)
  - Enthält: Netzpräfix (/64) und Standard-Gateway
  - Gerät bildet eigene IPv6-Adresse selbst aus:
    - Netzpräfix und Interface Identifier, z.B. MAC-Adresse oder zufällig

Und was ist mit DHCP?

- DHCPv6 wird oft ergänzend/zusätzlich zu SLAAC eingesetzt
  - Für reine Adressvergabe ist DHCPv6 bei IPv6 nicht zwingend erforderlich
- DHCPv6 vergibt optional:
  - IPv6-Adresse oder nur Zusatzparameter
  - Domain-Suffix / Suchdomänen
  - DNS-Server, weitere Netzwerkinformationen
- Vereinfachter Ablauf:
  - Gerät erkennt Router über Router Advertisement (RA),
  - entscheidet sich für SLAAC und/oder DHCPv6,
  - holt sich zusätzliche Konfigurationsdaten vom DHCPv6-Server

IPv6-Werkzeuge auf der Linux-Konsole

- Grundsätzlich die gleichen Werkzeuge wie bei IPv4:
  - `ip address show` → IPv6-Adressen anzeigen
  - `ip -6 route show` → IPv6-Routingtabelle anzeigen
  - `ip -6 neigh show` → Neighbor Discovery (NDP) anzeigen
  - `host -t AAAA example.net` → DNS AAAA-Record abfragen
  - `ping -6 example.net` → IPv6-Erreichbarkeit testen
  - `traceroute -6 example.net` → IPv6-Route verfolgen
  - `mtr -6 example.net` → Kombination aus Ping und Traceroute
  - `ss -6` → IPv6-Sockets anzeigen
- Alternative Befehle teilweise vorhanden, z.B. `traceroute6`, `ping6`

Wie siehts auf der Linux-Konsole aus?

```
[root@tux ~]# ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:00:5e:00:53:42 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 192.0.2.29/24 brd 192.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86390sec preferred_lft 86390sec
    inet6 2001:db8:abcd:1200:200:5eff:fe00:5342/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86390sec preferred_lft 14390sec
    inet6 2001:db8:abcd:1200:7c2a:91ff:fe11:3b4d/64 scope global temporary dynamic
       valid_lft 86390sec preferred_lft 86390sec
    inet6 2001:db8:abcd:1200:9f11:33aa:be22:77cc/64 scope global temporary dynamic
       valid_lft 86390sec preferred_lft 86390sec
    inet6 fd12:3456:789a:1::10/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::200:5eff:fe00:5342/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@tux ~]#
```

Link-Local benötigt meist Zonen-IDs

```
[root@tux ~]# ping fe80::1
PING fe80::1(fe80::1) 56 data bytes
^C
--- fe80::1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2032ms
[root@tux ~]#
```

- `fe80::/64` liegt an jedem Netzwerk-Interface an → keine Eindeutigkeit ohne Zonen-ID

```
[root@tux ~]# ping fe80::1%eth0
PING fe80::1%eth0(fe80::1%eth0) 56 data bytes
64 bytes from fe80::1%eth0: icmp_seq=1 ttl=64 time=0.679 ms
64 bytes from fe80::1%eth0: icmp_seq=2 ttl=64 time=0.222 ms
64 bytes from fe80::1%eth0: icmp_seq=3 ttl=64 time=0.280 ms
^C
--- fe80::1%eth0 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2030ms
rtt min/avg/max/mdev = 0.222/0.393/0.679/0.203 ms
[root@tux ~]#
```

Woher bekommt man IPv6?

- IPv6 wird vom Provider oder Netzbetreiber als Präfix delegiert
- Zuteilung erfolgt hierarchisch über Internet-Registries
  - IANA (ICANN) vergibt große IPv6-Blöcke an Regional Internet Registries
  - RIRs (z.B. RIPE NCC) verteilen diese an Provider
  - Provider delegieren daraus Präfixe an Kunden
- Kunden erhalten Netzpräfixe (z.B. /64, /56, /52, /48)
  - Es werden keine einzelnen IPv6-Adressen vergeben
  - Ausnahmen bei einigen Hosting-Anbietern für virtuelle Maschinen
- Unterschiedlich bei Heimnetz, Firmennetz und Hosting-Anbietern

Woher bekommt man IPv6 im Heimnetz?

- Provider für DSL, Kabel und Glasfaser stellen meist IPv6 bereit
  - Zuteilung eines dynamischen /56- oder /52-Präfixes per DHCPv6-PD
  - Router verteilt IPv6-Präfixe, Geräte konfigurieren sich per SLAAC
  - In der Praxis ist IPv6 meist bereits vorhanden und wird bereits genutzt
  - Hinweise aus der Praxis:
    - Vodafone DSL ist häufig leider IPv4-only
    - Regionale oder kleine Provider teilweise IPv4-only
- IPv6 auf älteren Routern nicht immer standardmäßig aktiviert
  - IPv6 wird im Heimnetz teilweise auch aus Unkenntnis deaktiviert
- Notlösung: IPv6-Tunnel zu Tunnelbroker oder Hosting-Anbieter

IPv6 auf Root-Servern / gemieteten VMs

- Hosting-Anbieter stellen IPv6 fast immer standardmäßig bereit
  - Zuteilung eines statischen /64-Präfixes (teilweise mehr zubuchbar)
  - Gebuchte Systeme meist mit Dual-Stack (IPv4 + IPv6) vorkonfiguriert
  - IPv6-only-Instanzen sind günstiger verfügbar (z.B. Hetzner, netcup)
- Vorkonfiguration meist statisch, d.h. kein SLAAC/DHCPv6-PD
- Deaktiviertes IPv6 oftmals aufgrund Unkenntnis des Kunden
- Sehr alte Produkte/Setups erfordern teilweise Support-Anfragen
- Sonderfälle bei Low-End-Produkten oder Wiederverkäufern
  - Gänzlich fehlendes IPv6 oder sehr kleine Präfixes, z.B. /80 - /124

Beispiel bei einer gemieteten VM

- Beispielkonfiguration bei netcup mit systemd-networkd:

```
[root@tux ~]# networkctl cat ens3.network
# /etc/systemd/network/ens3.network
[Match]
Name=ens3

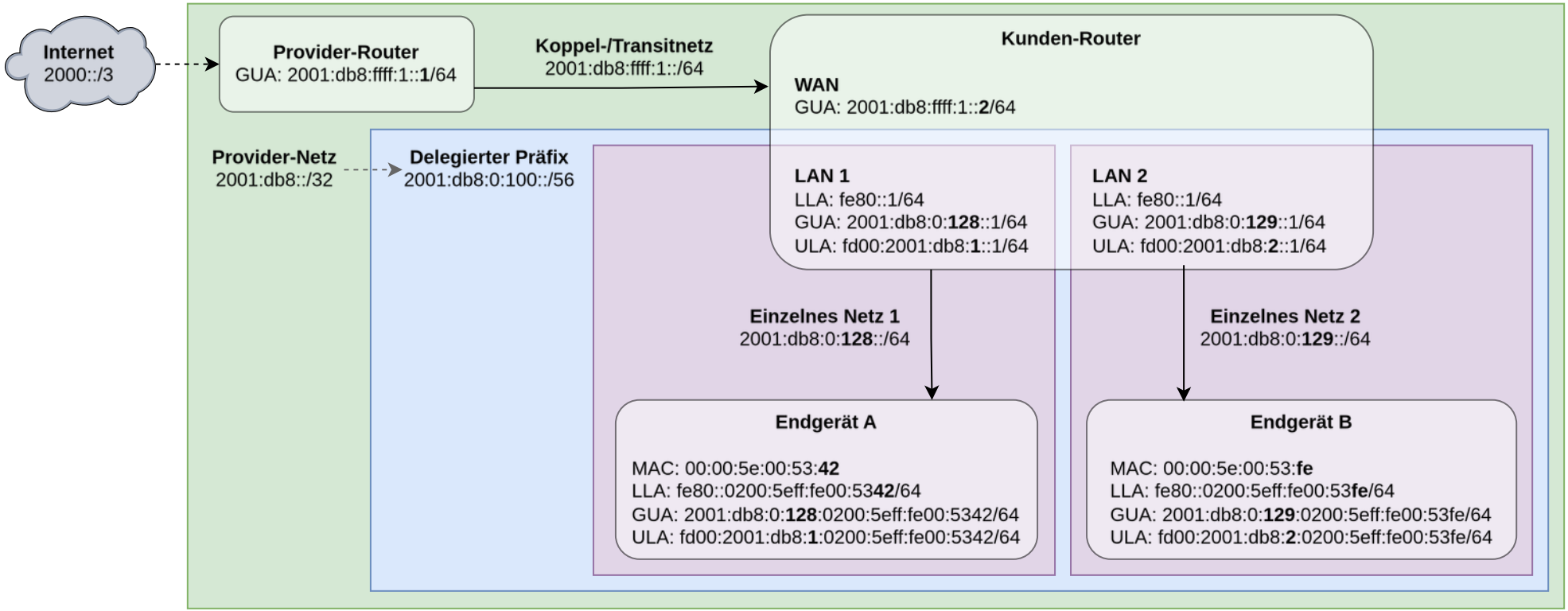
[Network]
Address=192.0.2.29/24
Address=2001:db8:1234:5678:0200:5eff:fe00:5342/64
Gateway=192.0.2.1
Gateway=fe80::1
IPv6AcceptRA=no
[root@tux ~]#
```

- Bei Hetzner ähnlich (mit zusätzlicher Hostroute für 172.31.1.1/32)

Woher bekommt man IPv6 im Firmennetz?

- Provider für DSL, Kabel und Glasfaser stellen meist IPv6 bereit
  - Oft Zuteilung eines statischen /48-Präfixes (teilweise gegen Aufpreis)
  - Geschäftskunden-Tarife unterscheiden sich typischerweise in:
    - Selbstständige und kleine Firmen: Nahe an Privatkunden-Produkten
    - Mittelständische und große Unternehmen: Leistungsfähige Enterprise-Tarife
  - In der Praxis ist IPv6 im Firmennetz meist bereits vorhanden…
    - …aber außer auf dem Provider-Router (Edge) leider nirgends konfiguriert!
- Sehr alte Produkte/Tarife erfordern teilweise Support-Anfragen
- Hinweis: Wechsel des Providers führt zu IPv6-Renummerierung
  - Provider-Independent (PI) IPv6-Adressen ab gewisser Größe sinnvoll

Das große Ganze



IPv4 durch IPv6 ersetzen?

- Häufigste bzw. erste Migrationsstrategie: Dual-Stack
  - Paralleler Betrieb aller Dienste mit IPv4 und IPv6 gleichzeitig
    - Private und/oder öffentliche IPv4-Adressen, öffentliche IPv6-Adressen
  - Schrittweise Migration möglich, reduziert Risiko bei Legacy-Systemen
- Weitere Migrationsansätze:
  - IPv6-mostly, NAT64 / DNS64, CLAT (464XLAT), IPv6-only
  - Migrationsstrategie muss unbedingt zum jeweiligen Netzwerk passen
    - Server bleiben häufig noch langfristig im Dual-Stack-Betrieb
    - Reine Client-Netzwerke können zunehmend IPv6-mostly werden
- Empfehlung: IPv6 aktiv ausbauen statt IPv4 abrupt abzulösen

IPv6: Firewall statt NAT

- NAT bietet keine Sicherheit, sondern nur Adressübersetzung
  - IPv4: NAT wird oft fälschlich als „Schutz“ wahrgenommen
  - IPv6: Standardmäßig keine NAT-Schicht → Ende-zu-Ende-Prinzip
- Sicherheit entsteht ausschließlich durch Firewall-Regeln (Filter)
- Gängige Praxis:
  - IPv4: NAT bei privaten IP-Adressen oder Routing – und Firewalling
  - IPv6: Routing und Firewalling
- IPv6-Firewalling nicht vergessen
  - ICMPv6 nicht pauschal filtern: Neighbor Discovery, Path MTU Discovery
  - Filtern von ICMP Echo Requests („ping“) erhöht die Sicherheit nicht

IPv6-Umstellungsstrategie?

- Einfach anfangen – nicht perfekt starten wollen!
  - Klein starten, Erfahrungen sammeln, schrittweise erweitern
  - Grober Adressplan statt Overengineering
  - Entscheidungen treffen statt zu überanalysieren
  - Flexibilität einplanen, da sich Anforderungen ändern
  - Eventuell nur einen Teil der IPv6-Zuteilung initial verplanen
- Einstiegsmöglichkeiten zur Umstellung:
  - Einzelne unkritische Systeme: DNS-, Web-, Monitoring-, Mail-Server
  - Interne Netzwerke, beginnend mit Test- oder Gäste-Netzen

IPv6-Security in Kürze angerissen…

- …weil viele IPv4-Netzwerke bereits heute nicht abgesichert sind:
  - First-Hop Security: RA Guard, DHCPv6 Guard, Rogue RA
  - Neighbor Discovery Protection: NDP, Spoofing, SLAAC-Sicherheit
  - SLAAC vs. DHCPv6: Kontrolle der Adressvergabe
  - Firewalling für IPv6: Separate Regeln für IPv4 und IPv6 erforderlich
  - Dual-Stack-Risiken: IPv6 oft schlechter überwacht als IPv4
  - Ungefilterte IPv6-Interfaces auf Clients/Servern
  - Monitoring und Logging für IPv6 sicherstellen
  - IPv6 in „IPv4-only“-Netzen: Angreifer bringt einfach IPv6 mit
- Sicherheit bestehender Netzwerke generell auf Prüfstand stellen!

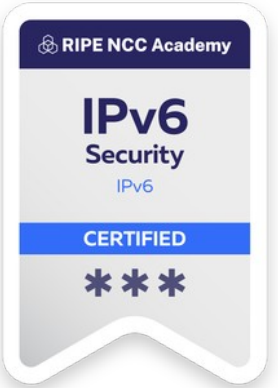
Fazit

- IPv6 ist seit mehr als 30 Jahren standardisiert
  - Aber leider noch immer nicht überall konsequent umgesetzt
- Einführung von IPv6 erfolgt nicht als Umbruch oder „Big Bang“
  - Schrittweiser Migrations- bzw. kontinuierlicher Evolutionsprozess
- Dual-Stack ist aktuell meist die wichtigste Übergangsstrategie
- IPv6 bei Hosting-Anbietern, im Heim-/Firmennetz meist verfügbar
  - Wird jedoch leider unterschiedlich konsequent (oder gar nicht) genutzt
- Wer IPv6 ignoriert, betreibt Netzwerke zunehmend unvollständig
- IPv6 bitte sukzessive aktivieren bzw. konfigurieren und benutzen

Noch mehr über IPv6 lernen?

- RIPE NCC Academy Summer School:
  - E-Learning-Kurs im Juli oder August absolvieren,
  - kostenlosen Gutschein für Zertifikatsprüfung erhalten
- Kostenlose E-Learning-Kurse für IPv6:
  - IPv6 Fundamentals: 15h, Zertifikatsprüfung möglich
  - IPv6 Advanced: 22h, *noch keine* Zertifikatsprüfung
  - IPv6 Security Expert: 25h, Zertifikatsprüfung möglich
- Weitere Informationen:
  - https://academy.ripe.net/
  - https://www.ripe.net/training/summer-school-2026/





In diesem Sinne…



Quelle: vv01f @ GNU MediaGoblin, CC BY-SA 3.0


Fragen?


Vielen Dank!