

Netzwerk – IPv6

- IPv6 ist der Nachfolger von IPv4. Er erweitert die Adressierung von ca. 4 Milliarden Adressen auf unvorstellbar viele, damit jedes Gerät eine eindeutige Adresse bekommt.
- Aufbau: 128-Bit-Adressen (in hex), typischerweise als Subnetze mit /64, Router Advertisements/SLAAC oder DHCPv6 zur Zuweisung von Adressen, und ein neues DNS-Verhalten.
- Um ein Heimnetz von IPv4 auf IPv6 zu bringen, macht man meist Dual-Stack (gleichzeitig IPv4 und IPv6). Viele Provider unterstützen heute sowohl IPv4 als auch IPv6 am Kundenanschluss. Wichtig ist: kein NAT66 als Standard, sondern native IPv6-Adressen mit optionalen Übergangslösungen, falls nötig.

Was ist IPv6, in Kürze

- Adressformat: 128 Bit, hexadezimal gruppiert (z. B. 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Doppelpunkte trennen 16-Bit-Gruppen.
- Typen von Adressen:
 - Global Unicast: öffentlich routbare IPv6-Adressen (z. B. 2001:...).
 - Link-Local: nur im lokalen Link gültig (fe80::/10); wird verwendet, damit Geräte sich im gleichen Netz entdecken (NDP).
 - Unique Local Address (ULA): privat im Netzwerk, ähnlich wie IPv4-Privatadressen (fc00::/7, häufig als fd00::/8 verwendet).
- Subnetze und Präfixe:
 - Typischerweise wird ein /64-Subnetz pro LAN verwendet (eine IPv6-Adresse pro Gerät plus Router)
 - Der ISP liefert oft ein Delegated Prefix (z. B. ein /56 oder /48), aus dem man mehrere /64er im Heimnetz ableitet.
- Autokonfiguration:
 - SLAAC (Stateless Address Autoconfiguration) über Router-Ankündigungen (RA): Geräte bilden sich selbst eine IPv6-Adresse aus dem Präfix des Routers.
 - DHCPv6: Zuweisung von Adressen/ Optionen durch einen DHCPv6-Server (z. B. DNS-Server) – optional neben SLAAC.
- DNS: IPv6-fähige DNS-Server (AAAA-Einträge für Adressen anstelle von CNAME/ A) sind wichtig. Viele Systeme arbeiten automatisch mit IPv6-DNS.

Wie man ein lokales Heimnetz von IPv4 auf IPv6 umstellt (Praktische Vorgehensweise)

1) Voraussetzungen prüfen

- Internetanschluss/Provider unterstützt IPv6 am Kundenanschluss (WAN-Side): IPv6-Prefixdelegation oder statische IPv6-Adresse möglich?
- Router-Firmware unterstützt IPv6 (und DHCPv6/SLAAC). Idealerweise ein aktueller Router/Firewall mit IPv6-Unterstützung.
- Falls du hinter einem Glasfaser-/Kabelmodem bist: Kläre, ob Modem/ONT/router-kaskade IPv6 durchleitet oder ob du NAT66/6in4/Tunneling brauchst. Viele Provider liefern ein Modem/Router-Kombi, das IPv6 direkt unterstützt.

2) Grundkonzept wählen

- Native Dual-Stack-Variante (empfohlen): IPv4 + IPv6 gleichzeitig, kein NAT66, normales Routing im IPv6-Bereich.
- Falls nötig: Übergangslösungen wie DS-Lite, 6in4-Tunnel – das ist meist nur eine Zwischenlösung, nicht ideal für Heimnetze.
- Für Privaträume ist Native Dual-Stack meist die einfachste, zuverlässigste Lösung.

3) Router vorbereiten und aktivieren

- Zugang zum Router: Admin-Oberfläche.
- IPv6 aktivieren:
 - WAN-Sektion: Anbieterpräfixdelegation aktivieren (z. B. Prefix Delegation/PD, oft DHCPv6-PD oder SLAAC).
 - Falls der Provider kein Prefix delegiert: statische IPv6-Adresse am WAN oder 6to4/DS-Lite-Laufzeit je nach Provider. Die meisten modernen Router unterstützen DHCPv6-PD und SLAAC automatisch.
- LAN/Subnetz-Konfiguration:
 - Router lässt normalerweise automatisch ein /64-LAN-Subnetz aus dem Provider-Prefix erstellen. Falls der Provider ein /56 oder /48 liefert, kann man daraus mehrere /64er ableiten (z. B. 2001:db8:1:1::/64, 2001:db8:1:2::/64 usw.).

4) Adressvergabe im Heimnetz

- SLAAC verwenden (Standard bei vielen Routern):
 - Geräte erhalten IPv6-Adressen automatisch vom Router, meist zusätzlich eine temporäre Privacy-Adresse.
- DHCPv6 optional nutzen:

- Falls du gezielt IPv6-Adressvergabe oder DNS-Server konfigurieren willst, aktiviere DHCPv6.

- DNS beachten:

- Stelle sicher, dass IPv6-DNS-Server konfiguriert sind (entweder via SLAAC/DHCPv6 oder manuell in jedem Gerät). Prüfe AAAA-Einträge für die gewünschten Domains.

5) Sicherheit und Firewall

- IPv6-Firewall aktivieren. Viele Router setzen IPv6-Firewallregeln standardmäßig.

- Für Dienste, die von außen erreichbar sein sollen (z. B. Heim-Server), plane Port-Öffnungen bzw. Firewallregeln für IPv6 separat. Beachte, dass IPv6 kein NAT verwendet; daher gelten andere Sicherheitsüberlegungen.

- Privatsphäre verbessern:

- Viele OSes erzeugen temporäre IPv6-Adressen (privacy extensions). Das ist gut für Privatsphäre, kann aber Troubleshooting erschweren.

6) Geräte testen und Fehlerbehebung

- Prüfe, ob Geräte IPv6-Adressen bekommen:

- Windows: ipconfig /all, Linux/macOS: ip -6 addr

- Router-Statusseite: DHCPv6/SLAAC-Status.

- Teste Konnektivität:

- Ping IPv6-Adressziele (z. B. ping6 google.com oder ping -6 google.com)

- Browser-Aufruf über IPv6 (z. B. <https://ipv6.google.com>)

- Prüfe DNS:

- Stelle sicher, dass DNS-Abfragen IPv6-fähige Adressen zurückliefern (AAAA-Einträge prüfen).

7) Typische Stolpersteine

- Nicht alle Geräte unterstützen IPv6 gleichzeitig (besonders ältere IoT-Geräte).

- Manche Internet-Dienste oder Apps funktionieren schlechter über IPv6, daher bevorzugt Dual-Stack mit IPv4-Unterstützung, falls Probleme auftreten.

- Falls du ein Hauptmodem eines Providers hast, musst du ggf. die Modem/Router-Kette korrekt konfigurieren, damit das IPv6-Prefix delegiert wird.

Was man technisch im Detail sieht (Beispiele)

- Adressbeispiel globaler IPv6-Adresse: 2001:db8:abcd:0012:0000:0000:abcd:1234
 - Typisch: 2001:db8... ist der globale Provider-Prefix; der Rest wird per SLAAC/DHCPv6 zugewiesen.
- Link-Local Beispiel (immer vorhanden): fe80::1ff:fe23:4567:890a
- ULA-Beispiel: fd12:3456:789a:1:2:3:4:5

Checkliste in Kürze

- Anbieter IPv6-Verfügbarkeit? Ja -> Schritt 2
- Router IPv6-fähig? Ja -> Schritt 3
- IPv6 aktivieren (WAN): Prefix Delegation aktiviert? Ja -> Schritt 4
- LAN-Subnetz (/64) zugewiesen? Ja
- SLAAC oder DHCPv6 konfiguriert? Beide möglich, SLAAC standardmäßig ok
- DNS IPv6 aktiviert? Ja
- Firewall IPv6 aktiv? Ja
- Tests gelaufen (IPv6-Adressen, DNS, Ping6)? Bestanden