BWCAMPUSNETZ

Zukunftsfähige Konzepte für die Campusnetze
an Universitäten und Hochschulen

IPv6-only in Campusnetzen

Federführung bei der Erstellung dieses Dokuments: Karlsruher Institut für Technologie
Kontakt: team@bwcampusnetz.de

Inhalt

1 Einleitung **3**

2 IPv6-Rollout und erste Netzsegmente mit IPv6-only **4**

3 IPv6-only für Client-Netze **5**

3.1 NAT64 mit DNS64 5

3.2 464XLAT 6

3.3 Erkennung des NAT64-Präfix 7

3.3.1 DNS 7

3.3.2 Router Advertisements - PREF64 7

3.3.3 Vergleich der beiden Optionen 7

3.4 Unterstützung von CLAT auf verschiedenen Betriebssystemen 8

4 IPv6-Mostly **9**

5 Fazit **10**

6 Anhang: IPv6-only bei Unternehmen und der öffentlichen Hand **11**

7 Versionsverlauf **12**

Literaturverzeichnis **13**

1 Einleitung

Der Rollout von IPv6 wird in aller Regel zunächst als Dual-Stack-Setup durchgeführt, so dass die Teilnehmer im Netz beide Protokolle - IPv6 und IPv4 - sprechen. Zwei Stacks machen jedoch Verwaltung und Fehlersuche aufwendiger, so dass klar ist, dass dies nicht das Ziel sein kann.

IPv6 wird vor IPv4 präferiert, das heißt, wenn das Ziel per IPv6 erreichbar ist, wird die Verbindung prinzipiell über IPv6 aufgebaut. Bei Nutzung des Algorithmus „Happy Eyeballs“[1], beispielsweise in Browsern, kann es aber auch sein, dass die Verbindung per IPv4 aufgebaut wird. Hat das Ziel nur IPv4, dann ist das Ziel durch einen IPv6-only-Teilnehmer nicht ohne Weiteres erreichbar. Im Internet sind immernoch viele Websites und Dienste IPv4-only, auch die sehr prominente Plattform GitHub. [2]

In diesem Dokument soll der Fokus darauf liegen, wie man in Netzsegmenten mit Teilnehmern, die IPv4-only-Ziele erreichen müssen, dennoch IPv6-only ausrollen kann. Es wird IPv6-only in Campusnetzen betrachtet. Die meisten besprochenen Themen und Vorgehensweisen lassen sich aber auf jedes andere Netz übertragen.

2 IPv6-Rollout und erste Netzsegmente mit IPv6-only

Am Anfang steht der Rollout von IPv6. Alle Netzsegmente sollen mit einem IPv6-Präfix ausgestattet sein. Die Verwendung von zustandloser Autokonfiguration (SLAAC) ist zu empfehlen, da ausgehende Verbindungen dann ohne weiteres Zutun mit IPv6 aufgebaut werden können, sofern das Ziel per IPv6 erreichbar ist. Weiterhin sollen die zentralen Dienste mit IPv6-Adressen konfiguriert und AAAA-Records eingetragen werden.

Es ist nun möglich, an den ersten Stellen IPv6-only zu konfigurieren. Hat man die Dienste im Management für die Netzkomponenten wie z. B. RADIUS- oder TACACS-Server mit IPv6 ausgestattet, können z. B. die Management-Netze für die Netzkomponenten frühzeitig als IPv6-only-Netze realisiert werden, da diese nicht mit dem Internet kommunizieren. Genauso kann IPv6-only generell bei Diensten insbesondere im Backend praktiziert werden, die ausschließlich von IPv6-fähigen Systemen angesprochen werden und auch nur IPv6-fähige Dienste benötigen. So könnte dies z. B. beim RADIUS-Dienst für VPN möglich sein, wenn die VPN-Server selbst IPv6-fähig sind sowie der vom RADIUS-Server benötigte LDAP-Dienst ebenfalls IPv6 unterstützt.

Nur intern erreichbare Dienste können ebenfalls IPv6-only konfiguriert werden, sofern man tatsächlich in allen Netzsegmenten IPv6 ausgerollt hat und keine Legacy Systeme ohne IPv6-Fähigkeit existieren, die den Dienst erreichen müssen. Es sei an dieser Stelle erwähnt, dass es sich empfehlt in der Organisation eine Policy zu etablieren, die keine Anschaffung von Geräten erlaubt, die nicht IPv6-fähig sind.

3 IPv6-only für Client-Netze

3.1 NAT64 mit DNS64

Clients müssen meist mit dem Internet kommunizieren und somit steht man vor dem oben beschriebenen Problem. Damit die IPv6-only-Clients IPv4-only-Ziele erreichen können, muss es einen Übergangsmechanismus geben. Mit NAT64 existiert ein solcher für die Übersetzung von IPv6 in IPv4. [3]

NAT64 ermöglicht die Kommunikation zwischen IPv6- und IPv4-Systemen durch eine Form der Netzwerkadressübersetzung (engl. Network Address Translation, kurz NAT). Hierfür wird ein IPv6-Netzwerksegment mit einem 32-Bit-Adressraum definiert, um damit die Übersetzung zu realisieren. Das für diesen Dienst reservierte „bekannte Präfix" lautet 64:ff9b::/96. Es kann aber auch jedes andere Präfix genutzt werden. Der Client bettet die IPv4-Adresse in den Hostteil des Netzsegments ein und erhält somit eine IPv6-Adresse, die die IPv4-Adresse enthält. An diese IPv6-Adresse sendet er die Pakete, die die IPv4-Adresse erreichen sollen.

Bevor die Pakete das Netz der Organisation verlassen, muss das IPv6-Paket in ein IPv4-Paket umgewandelt werden, wofür ein NAT64-Gateway benötigt wird. Als Quelladresse konfiguriert das Gateway genauso wie bei NAT44 eine auf dem Gateway konfigurierte IPv4-Adresse, damit die Antwortpakete auch wieder zu dem Gateway zurück gesendet werden. In einem Campusnetz bietet es sich an, die NAT64-Funktionalität auf der meistens ohnehin vorhandenen zentralen Firwall zu implementieren.

Damit der Client die Ziel-IPv4-Adresse in eine IPv6-Adresse umwandeln kann, so dass diese zum NAT64 Gateway gesendet wird, muss ihm der NAT64-Präfix bekannt sein. Ein Weg, der für den Client völlig transparent abläuft, ist DNS64. [4] Dafür muss der Client einen DNS-Resolver nutzen, der DNS64 implementiert. Für Domains ohne AAAA Record erhält der Client vom DNS64-Resolver einen AAAA-Record mit der IPv6-Adresse aus dem NAT64 Präfix mit der eingebetteten IPv4-Adresse. Ohne weitere Anpassungen auf dem Client, können so IPv4-only-Ziele von IPv6-only-Teilnehmern erreicht werden. Doch die Methode hat verschiedene Nachteile.

Zunächst funktioniert es auf diese Art und Weise nicht literale IPv4-Adressen erreichen. Auch wenn die Software, die die Verbindung zu dem IPv4-Server aufbauen möchte, kein IPv6 unterstützt und nur A-Records auswertet, ist DNS64 nutzlos. Weiterhin werden bei DNS64 DNS-Antworten modifiziert. Dies ist grundsätzlich schlecht und wird mit DNSSEC daher auch naturgemäß zum Problem. Neben dem Verzicht auf die DNSSEC-Validierung gibt es weitere Lösungen, um diesem Problem zu begegnen, die allerdings komplex sind. [5] Darüberhinaus muss für die DNS-Auflösung zwingend der Resolver der Organisation genutzt werden. Es wird aber für Nutzer immer üblicher, entweder öffentlich verfügbare Resolver zu nutzen oder auf ihrem Client selbst einen Resolver zu betreiben. Weiterhin ist in einem Setup mit mehreren Netzanschlüssen, wie beispielsweise bei der Nutzung von VPN, nicht klar, zu welcher Verbindung das NAT64-Präfix gehört. Es muss also der richtige Resolver pro Verbindung genutzt werden.

3.2 464XLAT

464XLAT ist ein IPv4-IPv6-IPv4-Übersetzungsverfahren und behebt einige Probleme von NAT64/DNS64. [6] XLAT wird als Abkürzung für das englische Wort „translate“ genutzt und bedeutet daher „Übersetzung“.

464XLAT setzt sich zusammen aus CLAT (customer-side translator) und PLAT (provider-side translator). PLAT unterscheidet sich nicht von NAT64. Neu ist CLAT, was auf dem Client selbst implementiert wird und die IPv4-Adresse mit dem NAT64-Präfix zu einer IPv6-Adresse synthetisiert. Hierbei handelt es sich also um NAT46. CLAT kann auch auf dem Default Gateway des Clients implementiert werden, hier betrachten wir aber nur den Fall von CLAT auf dem Client selbst.

464XLAT benötigt DNS64 nicht, da der Host die Pakete weiterhin an die IPv4-Adresse des Ziels senden kann und diese durch den CLAT übersetzt werden. Hierdurch werden die oben angesprochenen Probleme wie das Erreichen von Literalen und Software, die nur IPv4 implementiert, behoben. Darüber hinaus müssen auch keine DNS Records modifiziert werden. Allerdings ist nun die Übersetzung für den Client nicht mehr transparent, sondern es muss die CLAT-Funktionalität implementiert werden.

3.3 Erkennung des NAT64-Präfix

Damit der CLAT die IPv4-Adresse in die IPv6-Adresse übersetzen kann, muss das NAT64-Präfix bekannt sein. Zur Erkennung gibt es verschiedene Möglichkeiten, DNS und PREF64, die im folgenden beschrieben werden.

3.3.1 DNS

Mit RFC 7050 [7] (*Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis*) wurde 2013 die Domain ipv4only.arpa eingeführt, mit Hilfe dieser ein Client das NAT64-Präfix erkennen soll. Hierfür hat diese Domain genau zwei im RFC definierte well-known A Records, die der Resolver dann zu den entsprechenden AAAA-Records synthestisiert. Allerdings wurde die Domain mit diesem RFC nicht als special use domain deklariert. Daher war es weder dem Client noch dem Server möglich, eine spezielle Behandlung der Domain zu implementieren. 2020 wurde dies mit RFC 8880 [8] (*Special Use Domain Name 'ipv4only.arpa'*) nachgeholt. 'ipv4only.arpa' ist eine special-use domain [9] nach RFC 6761 (*Special-Use Domain Names*) [10]. Dadurch kann man einen Resolver implementieren, der ausschließlich für die well-known Domain die Synthetisierung durchführt. Auf Client-Seite muss nur dieser Record beim DNS64-Resolver abgefragt werden. Für die eigentliche DNS-Auflösung können weiterhin beliebige Resolver verwendet werden.

3.3.2 Router Advertisements - PREF64

In RFC 8781 [11] (*Discovering PREF64 in Router Advertisements*) wurde 2020 eine Neighbor-Discovery-Option eingeführt, mit der NAT64-Präfixe im Router Advertisement (RA) an die Hosts kommuniziert werden können. Hiermit ist 464XLAT vollkommen unabhängig von DNS, aber der Router muss diese Option implementieren. PREF64 bezeichnet das NAT64-Präfix, wird aber auch als Bezeichnung für die RA-Option verwendet.

3.3.3 Vergleich der beiden Optionen

Auch wenn die RA-Option grundsätzlich eleganter erscheint, ist man beim Verwenden von Netzkomponenten von Herstellern mit nicht offener Firmware darauf angewiesen, dass diese

die Option implementieren. Einen entsprechenden Resolver bereitzustellen, ist hingegegen relativ einfach. Als Vorteil von der RA-Option ist noch zu nennen, dass sich hiermit das Präfix durch ein weiteres Router Advertisement aktualisieren lässt. Bei HPE Juniper[12][13] wird die Option seit 2022, bei Arista [14] und Cisco Catalyst (IOS-XE) [15] seit 2023 unterstützt. Für Cisco Nexus (NX-OS) ist die Option Stand heute (Oktober 2025) nicht implementiert.

RFC 9872 (*Recommendations for Discovering IPv6 Prefix Used for IPv6 Address Synthesis*) vom September 2025 [16] gibt die Empfehlung für die Hosts, PREF64 über DNS zu bevorzugen. Netzwerkadministratoren sollten PREF64-Information in Router Advertisements bereitstellen. RFC 9872 nennt weitere Probleme mit der Erkennung des NAT64-Präfixes über DNS.

3.4 Unterstützung von CLAT auf verschiedenen Betriebssystemen

Da Mobilfunkprovider schon längere Zeit auf IPv6-only setzen, hat sich die CLAT-Funktionalität sowohl auf Android als auch auf iOS bereits gut etabliert. Auf Windows ist diese nur für Verbindungen im Mobilfunk implementiert. Microsoft hat 2024 angekündigt, CLAT auf allen Netzwerkschnittstellen einzuführen. [17] Gemäß unserer 2024 durchgeführten Tests ist CLAT auch auf macOS vollständig implementiert. Dies deckt sich auch mit den Ergebnissen einer am 21. Juli 2025 veröffentlichten Survey. [18] Auf Android, iOS und macOS funktionieren die Erkennung des NAT64-Präfixes sowohl mit PREF64 als auch DNS.

Für Linux gibt es mit clatd [19] eine CLAT-Implementierung. Diese funktioniert allerdings Stand heute (Oktober 2025) noch nicht vollständig mit PREF64. Im Januar 2025 wurde eine Implementierung für den Linux-Kernel angekündigt. [20] Mehr Informationen zu Linux und IPv6-only finden sich in dem Vortrag *Improving IPv6-only experience on Linux* (FOSDEM 2024). [21]

4 IPv6-Mostly

Ein IPv6-Mostly-Netzwerk [22] stellt IPv6 mit NAT64 als auch IPv4 zur Verfügung, gibt aber gleichzeitig IPv6-only-fähigen Clients die Möglichkeit, auf IPv4 zu verzichten, ohne dass der Nutzer die Fähigkeiten des Netzwerks manuell überprüfen und IPv4 dann aktiv dekonfigurieren muss. Hierzu bietet die DHCPv4-Server-Infrastruktur die DHCPv4-Option 108 gemäß RFC 8925 (*IPv6-Only Preferred Option for DHCPv4*) [23] an. Der IPv6-only fähige Client fragt mit dieser Option an und der entsprechend konfigurierte Server gibt die Option ebenfalls zurück. Als IP-Adresse wird entweder eine noch nicht belegte Adresse aus dem Pool oder 0.0.0.0 angeboten (DHCPOFFER). Der Client sendet nach dem DHCPOFFER in diesem Fall keinen DHCPREQUEST und bleibt somit IPv6-only. Hiermit wird für den DHCPv4-Server auch die Möglichkeit geschaffen, IPv4-Adressen einzusparen.

Ein IPv6-Mostly-Netzwerk ist also einem Dual-Stack-Netzwerk ähnlich, gibt aber IPv6-fähigen Clients die Möglichkeit, per IPv6-only zu kommunizieren.

5 Fazit

Es gibt verschiedene Möglichkeiten, IPv6-only im Campusnetz anzubieten. Hier sollen mögliche Startpunkte aufgezeigt werden.

In Netzen, in denen die Teilnehmer nicht bekannt sind und keine Kontrolle über die Installation herrscht, sollte besser IPv6-mostly als IPv6-only angeboten werden. Andernfalls werden Clients, die keine CLAT-Implementierung haben (Stand heute: Windows und Linux bei fehlender manuellen Installation von clatd), an Literalen und Software ohne IPv6-Unterstüzung scheitern. Bietet man IPv6-mostly an, sollte das Präfix mit PREF64 oder wenn nicht möglich über DNS verteilt werden. Die Probleme von DNS64 wurden dargestellt, daher ist die Empfehlung, keinen DNS64-Resolver zu implementieren, sondern lediglich bei fehlender Möglichkeit von PREF64 einen Resolver bereitzustellen, der ausschließlich die Domain ipv4only.arpa synthetisiert.

Ein Startpunkt für IPv6-only könnte sein, das Gästenetz eduroam als ein IPv6-mostly-Netzwerk realisieren.

Sollte Microsoft seine Ankündigung umsetzen, und CLAT auf allen Netzwerkinterfaces implementieren, könnte man beispielsweise ein Netz der Verwaltung, bei dem alle Clients mit Windows installiert sind und unter der Kontrolle von zentralen IT-Administratoren stehen, mit IPv6-only ausstatten.

6 Anhang: IPv6-only bei Unternehmen und der öffentlichen Hand

Im folgenden soll ein Eindruck vermittelt werden, wie es mit IPv6-only an verschiedenen Stellen aussieht. Es werden Fundstücke aus dem Internet gelistet, es besteht kein Anspruch auf Vollständigkeit.

Bei den großen Unternehmen sieht man die Richtung IPv6-only schon lange sehr deutlich:

- Apple (2016): "Starting June 1, 2016 all apps submitted to the App Store must support IPv6-only networking" [24]
- Facebook (2017): "Today, 99 percent of our internal traffic is IPv6 and half of our clusters are IPv6-only" [25]
- Microsoft (2019): "We are now focusing on having a single stack in our network" [26]
- Mobilfunkprovider wie T-Mobile nutzen seit einiger Zeit IPv6-only im Mobilfunk. [27]

Bei der öffentlichen Hand sieht es etwas weniger gut aus, aber immerhin hat sich der tschechische Staat kürzlich committet, bis 2032 alle seine Angebote IPv6-only anzubieten. [28] In Deutschland wurde 2023 zumindest eine Initiative der öffentlichen Verwaltung in Richtung Dual-Stack gestartet. [29]

Beim Imperial College London geht man in Richtung IPv6-only, wie 2020 in einem Vortrag berichtet wurde. [30]

7 Versionsverlauf

Version	Datum	Änderungen
1.0	06.10.2025	Initiale Veröffentlichung
1.1	01.12.2025	Rechtschreibfehler korrigiert und Fazit klarer dargestellt.
1.2	13.03.2026	Rechtschreibfehler korrigiert.

Literaturverzeichnis

[1] *RFC 8305: Happy Eyeballs Version 2: Better Connectivity Using Concurrency*, Dez. 2017. Adresse: https://datatracker.ietf.org/doc/html/rfc8305.

[2] *Discussion on GitHub 2022-2025: "IPv6 support for cloning Git repositories"*, 2024. Adresse: https://github.com/orgs/community/discussions/10539.

[3] *RFC 6146: Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*, Apr. 2011. Adresse: https://datatracker.ietf.org/doc/html/rfc6146.

[4] *RFC 6147: DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*, Apr. 2011. Adresse: https://datatracker.ietf.org/doc/html/rfc6147.

[5] *IEEE: DNSSEC in the networks with a NAT64/DNS64*, 2024. Adresse: https://ieeexplore.ieee.org/document/8501446.

[6] *RFC 6877: 464XLAT: Combination of Stateful and Stateless Translation*, Apr. 2013. Adresse: https://datatracker.ietf.org/doc/html/rfc6877.

[7] *RFC 7050: Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis*, Nov. 2013. Adresse: https://datatracker.ietf.org/doc/html/rfc7050.

[8] *RFC 8880: Special Use Domain Name 'ipv4only.arpa'*, Aug. 2020. Adresse: https://datatracker.ietf.org/doc/html/rfc8880.

[9] *IANA: Special-Use Domain Names*. Adresse: https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xhtml.

[10] *RFC 6761: Special-Use Domain Names*, Feb. 2013. Adresse: https://datatracker.ietf.org/doc/html/rfc6761.

[11] *RFC 8781: Discovering PREF64 in Router Advertisements*, Apr. 2020. Adresse: https://datatracker.ietf.org/doc/html/rfc8781.

[12] *HPE Juniper Feature Explorer: NAT64 router advertisement*, 2022. Adresse: https://apps.juniper.net/feature-explorer/feature/5951?fn=NAT64%5C%20router%5C%20advertisement.

[13] *Junos OS Dates & Milestones*. Adresse: https://support.juniper.net/support/eol/software/junos/.

[14] *ARISTA: PREF64 option in Router Advertisements (RFC8781)*, 2023. Adresse: https://www.arista.com/en/support/toi/tag/rfc8781.

[15] *Cisco IOS XE 17.11.1 for Catalyst Switching*, 2023. Adresse: https://community.cisco.com/t5/networking-blogs/cisco-ios-xe-17-11-1-for-catalyst-switching/ba-p/4811370.

[16] *RFC 9872: Recommendations for Discovering IPv6 Prefix Used for IPv6 Address Synthesis*, Sep. 2025. Adresse: https://datatracker.ietf.org/doc/html/rfc9872.

[17] *Microsoft extends Windows 11 464XLAT support to include fixed-line networks*, 2024. Adresse: https://www.sidn.nl/en/news-and-blogs/microsoft-extends-windows-11-464xlat-support-to-include-fixed-line-networks.

[18] *A Survey of the Current State of CLAT Availability and Performance on Non-Mobile Systems*, Juli 2025. Adresse: https://www.ietf.org/archive/id/draft-nbrr-v6ops-clat-status-00.html.

[19] *clatd - a CLAT / SIIT-DC Edge Relay implementation for Linux*. Adresse: https://github.com/toreanderson/clatd.

[20] *Systemd Issues: Built-in 464XLAT implementation*, 2025. Adresse: https://github.com/systemd/systemd/issues/23674#issuecomment-2625544068.

[21] *Improving IPv6-only experience on Linux*, 2024. Adresse: https://archive.fosdem.org/2024/events/attachments/fosdem-2024-1798-improving-ipv6-only-experience-on-linux/slides/22113/FOSDEM2024-Improving_IPv6-only_experience_on_Li_DXG1q8n.pdf.

[22] *Internet-Draft: IPv6-Mostly Networks: Deployment and Operations Considerations*, 2024. Adresse: https://datatracker.ietf.org/doc/draft-ietf-v6ops-6mops/.

[23] *RFC 8925: IPv6-Only Preferred Option for DHCPv4*, Okt. 2020. Adresse: https://datatracker.ietf.org/doc/html/rfc8925.

[24] *Apple Requires All iOS Apps To Work in IPv6-ONLY Networks*, 2016. Adresse: https://www.internetsociety.org/blog/2016/05/starting-june-1-apple-requires-all-ios-apps-to-work-in-ipv6-only-networks/.

[25] *Legacy support on IPv6-only infra*, 2017. Adresse: https://engineering.fb.com/2017/01/17/production-engineering/legacy-support-on-ipv6-only-infra/.

[26] *Microsoft Works Toward IPv6-only Single Stack Network*, 2019. Adresse: https://www.arin.net/blog/2019/04/03/microsoft-works-toward-ipv6-only-single-stack-network/.

[27] *Case Study: T-Mobile US Goes IPv6-only Using 464XLAT*, 2014. Adresse: http://www.internetsociety.org/resources/deploy360/2014/case-study-t-mobile-us-goes-ipv6-only-using-464xlat.

[28] *Michal Hrušecký: More details about the end of IPv4 in state service*, 2024. Adresse: https://social.hrusecky.net/@michal/statuses/01HMDKVBZ246WMFVR3PW74N8RF.

[29] *Der Bund ist Vorreiter bei der IPv6-Migration*, 2023. Adresse: https://blogs.pwc.de/de/oeffentlicher-sektor-zukunft-gestalten/article/240425/der-bund-ist-vorreiter-bei-der-ipv6-migration/.

[30] *IPv6 Only at Imperial*, 2024. Adresse: https://www.ipv6.org.uk/wp-content/uploads/2020/04/IPv6OnlyAtImperial.pdf.