IPv6 und die Privatsphäre

Secorvo White Paper

Möglichkeiten und Grenzen

Version 1.2
Stand 08. Januar 2015

Dr. Safuat Hamdy

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100

info@secorvo.de
www.secorvo.de

Inhaltsübersicht

Abkürzungen

APNIC	Asia-Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
CGA	Cryptographically Generated Address
CIDR	Classless Inter-Domain Routing
CSS	Cascading Style Sheets
DFN	Deutsches Forschungsnetz
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
EUI-64	64-Bit Extended Unique Identifier
HBA	Hash Based Address
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Taskforce
IP	Internet Protocol
IPsec	IP Security
ISP	Internet Service Provider
LAN	Local Area Network
LIR	Local Internet Registry
MAC	Media Access Control
NAT	Network Address Translation
RFC	Request for Comments
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIR	Regional Internet Registry
SEND	Secure Neighbor Discovery
SLAAC	Stateless Address Auto-Configuration
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

1 Zusammenfassung

Mit der Einführung von IPv6 soll erreicht werden, dass jedes System im Internet eine eigene global routbare Adresse erhält. Dadurch wird jedes System im Prinzip aus dem gesamten Internet erreichbar. Damit wird häufig assoziiert, dass Geräte eindeutig identifiziert und genaue Profile über Aktivitäten ihrer Besitzer erstellt werden können. Dies hat in verschiedenen Diskussionsforen und Blogs sowie bei Datenschützern zu Bedenken [DSBL 2011, Schaar 2011] oder sogar zu einer Ablehnung von IPv6 geführt. Um Datenschutz bei der Nutzung von IPv6 zu gewährleisten, wurden weitreichende Forderungen gestellt [DSBL 2012], die aber teilweise kaum erfüllt werden können. So wird beispielsweise gefordert, dass durchgängig IPsec verwendet wird, oder dass die IP-Adresse alle zehn Minuten erneuert werden kann. Beides ist technisch nicht machbar.

In diesem Artikel wird dargestellt, welche Zusammenhänge zwischen IPv6 und den Möglichkeiten zur Verfolgung und Identifikation von Benutzern bestehen. Die Bedrohung geht von unveränderlichen (statischen) IPv6-Adressen aus, die wie ein Identifizierungsmerkmal wirken. Aus Sicht des Datenschutzes ist eine möglichst hohe Wechselfrequenz erforderlich. Das Internet kann dann aber in vielen Szenarien nicht mehr sinnvoll genutzt werden. In der Praxis ist eine Verfolgbarkeit über eine minimale Dauer von einigen Stunden daher unvermeidlich. Bei der Bewertung dieser Folgen von IPv6 sollte man berücksichtigen, dass es zahlreiche andere Möglichkeiten gibt, Systeme zu verfolgen. Diesen Möglichkeiten kann man ohne Einschränkungen des Nutzerverhaltens kaum ausweichen. Unter diesem erweiterten Blickwinkel erscheint die Diskussion um IPv6-Adressen und die Forderung nach dynamischer Adressvergabe überbewertet.

Es zeigt sich außerdem, dass die Wirkung der Privacy Extensions überbewertet wird. Sie tragen in ihrer jetzigen Form weit weniger zur Privatsphäre bei, als die Bezeichnung dies vermuten lässt. Aus Sicht des Datenschutzes müssten ggf. neue Methoden zur Adressbildung entworfen und standardisiert werden, wobei die kürzlich verabschiedeten Opaque Interface Identifier ein Schritt in diese Richtung sein könnten.

2 Privatsphäre im Internet: Akteure und Schutzziele

Benutzer sollten Angebote und Dienste im Internet anonym nutzen können, wenn sie dies wünschen. Dadurch soll verhindert werden, dass umfassende Verhaltensprofile über diese Benutzer gebildet werden können. Die Interessen von Politik und Nachrichtendiensten, von Teilen der Wirtschaft und der Strafverfolgungsbehörden steht dem naturgemäß entgegen. Sie wünschen sich einfache Möglichkeiten, Anwender profilieren, verfolgen und identifizieren zu können.

Mit dem bisherigen Internetprotokoll IPv4 wurden in gewissem Umfang dynamische IP-Adressen für die Endgeräte eingesetzt. Trotzdem werden bereits diese Adressen von Datenschützern kritisch betrachtet. Mit dem neuen Internet-Protokoll IPv6 ist jedoch für jedes Endgerät zunächst eine statische IP-Adresse vorgesehen. Diese feste Zuordnung wird es Anbietern und Behörden im Internet erleichtern, Verhaltensprofile zu erstellen. IPv6 hat deshalb zu einigen Bedenken hinsichtlich der Privatsphäre der Nutzer geführt und gilt aus Datenschutzsicht als problematisch.

Inzwischen wurden Ergänzungen zu IPv6 definiert, die die Privatsphäre schützen sollen. Sie sollen im Weiteren vorgestellt und im Vergleich zur Situation mit IPv4 bewertet werden. Dazu ist es zunächst notwendig, die beteiligten Akteure vorzustellen und die Schutzziele zu identifizieren.

Private Endanwender nutzen das Internet mit einem Client auf einem Endgerät, beispielsweise einem Browser oder einem Chat-Client auf einem Smartphone, Tablet oder

Notebook. Endanwender verfügen in der Regel nicht über ausgeprägtes Interesse oder ausgeprägte Kompetenz in Fragen von Datenschutz und IT-Sicherheit. Ebenso verfügen sie nicht über die notwendigen Ressourcen, um ein hohes Schutzniveau aufzubauen und aufrechtzuerhalten.

Für die Diskussion in diesem Artikel werden ausschließlich Szenarien betrachtet, in denen der Anwender das Internet anonym und unverkettbar (siehe unten) nutzen möchte. Szenarien, in denen er sich an einem Dienst anmeldet oder aus anderen Gründen bewusst unveränderliche Informationen zu seiner Identifikation verwendet, etwa eine E-Mail-Adresse, sind daher von der weiteren Betrachtung ausgeschlossen.

Daneben spielen die folgenden Akteure eine Rolle:

- **Internet Service Provider** (ISP). Diese Akteure nehmen eine Sonderstellung ein, denn sie weisen den Anwendern ihre IP-Adressen zu (genauer gesagt, ihre Routingpräfixe, siehe Abschnitt A.1) und sind grundsätzlich in der Lage, Anwender zu identifizieren und ihr Verhalten zu analysieren. Ihr Interesse liegt vor allem in einem stabilen Betrieb effizienter Netze bei minimalen Kosten. Hier kann es zu Konflikten bei der „datenschutzfreundlichen“ Gestaltung von Mechanismen zur Adressvergabe kommen.
- **Dienst- und Inhalteanbieter**. Diese Akteure werden von Endanwendern gezielt aufgesucht. Die Betreiber der Sites können die Nutzung durch Clients protokollieren und auswerten, die Ausgangsbasis hierfür sind oft IP-Adressen und Cookies. Für fortgeschrittene Methoden der Auswertung werden aber zunehmend Analyse-Dienste in Anspruch genommen.
- **Analyse-Dienste**. Diese Akteure sind in der Regel über eingebetteten Script-Code bei vielen Dienst- und Inhalteanbietern im Einsatz und können damit Site-übergreifend das Nutzungsverhalten von Clients erfassen und auswerten. Die „Nutzung“ der Analyse-Dienste erfolgt vom Anwender unbemerkt und ohne dessen Zustimmung, wird aber in der Regel billigend in Kauf genommen. Die Methoden der Analyse-Dienste sind recht ausgefeilt und funktionieren auch ohne IP-Adressen, Cookies und dergleichen. Es ist jedoch davon auszugehen, dass IP-Adressen genutzt würden, wenn diese aus Sicht der Analyse-Dienste zur Verkettung von Anwenderaktivitäten geeignet wären.

  Wegen der zunehmenden Verbreitung dieser Dienste ist es kaum mehr möglich, ihnen aus dem Weg zu gehen, ohne erhebliche Einschränkungen der Internet-Nutzung in Kauf zu nehmen. Hier sind entsprechende Verteidigungsmethoden erforderlich, etwa die Blockade des Script-Codes.
- **Beobachter en-route**, z. B. Netzbetreiber und/oder Nachrichtendienste. Gemeint sind damit die Akteure, über deren Knoten Intenet-Nachrichten ausgetauscht werden oder die einen solchen Austausch mitlesen können. Beobachter en-route können ebenfalls umfangreiche Verhaltensprofile anlegen, besonders wenn die Beobachtung in Backbone-Netzen erfolgt.

Die Angriffsziele dieser Akteure bestehen darin, einzelne Benutzer zu verfolgen, zu profilieren oder zu identifizieren. In diesem Artikel werden die Möglichkeiten diskutiert, dies anhand der IP-Adresse zu erreichen. Das aus Sicht des Benutzers entsprechende Schutzziel wird in [DSBL 2012] als Unverkettbarkeit bezeichnet. Dieses Schutzziel kann in verschiedenen Szenarien unterschiedlich ausgeprägt sein, wie in Abschnitt 5 ausgeführt wird.

3 Hintergrund zu IPv6

IPv6 ist das Netzwerkprotokoll, das als Nachfolger für das bisher genutzte IPv4 entwickelt wurde. Die Aufgabe des Internet-Protokolls (IP) besteht im Wesentlichen darin, Datenpakete von einem Absender über verschiedene Netzwerke hinweg zu einem Empfänger zu

vermitteln. Diese Vermittlung erfolgt anhand von sogenannten IP-Adressen. Deshalb braucht jedes System im Internet eine eigene IP-Adresse, die einmalig ist. Ohne eine eigene, gültige IP-Adresse kann ein System nicht am Internet teilnehmen.

Die Vergabe von IP-Adressen an End-Sites[1] erfolgt über *Local Internet Registrys* (LIRs). Dies sind typischerweise Internet Service Provider (ISP). Die LIRs weisen ihren Kunden Adressen oder Adressbereiche aus den Adressblöcken zu, welche die LIRs ihrerseits von sogenannten *Regional Internet Registrys* (RIRs) erhalten. Das für Europa zuständige RIR ist RIPE NCC. Die RIRs erhalten ihre Zuweisungen wiederum von der Internet Assigned Numbers Authority (IANA).

Benötigt ein Kunde mehr Adressen als die LIR zur Verfügung stellen kann, dann fragt die LIR bei ihrer zuständigen RIR nach der Zuweisung eines weiteren Adressblocks. Ist auch der Pool der RIR erschöpft, dann fragt sie bei IANA nach einem weiteren Adressblock. Im Jahr 2011 vergab die IANA ihren letzten /8-Block des IPv4-Adressraums und erreichte einen wichtigen „Meilenstein" im Lebenszyklus von IPv4. Es können also keine weiteren IPv4-Adressblöcke an die RIRs vergeben werden. Zwar verfügen die RIRs noch über freie Adressblöcke, jedoch werden auch diese in absehbarer Zeit verbraucht sein.[2]

Theoretisch gibt es knapp 4,3 Milliarden IPv4-Adressen, allerdings sind einige Adressblöcke für Sonderfunktionen reserviert. Nach Abzug aller Sonderadressen verbleiben etwa 3,7 Milliarden *global routbare* Adressen. Global routbare Adressen können weltweit eindeutig zugeordnet werden; sie werden landläufig auch als öffentliche IP-Adressen bezeichnet. Der IPv4-Adressraum ist relativ dicht belegt, dennoch wird eine signifikante Anzahl dieser Adressen nicht genutzt. Es sind verschiedene Vorgehensweisen denkbar, um beispielsweise ungenutzte Adressen oder Adressblöcke wieder einzuziehen und neu zu vergeben. Dabei ergeben sich jedoch verschiedene Probleme,[3] deren Details für die weitere Diskussion in diesem Artikel nicht von Belang sind.

Die Situation der Adressknappheit war bereits seit der enormen Expansion des Internets ab Mitte der neunziger Jahre absehbar. Aus diesem Grund wurden seit 1993 mehrere Maßnahmen ergriffen, um das Problem anzugehen. Als langfristige Maßnahme wurde mit IPv6 ein neues Internet-Protokoll entworfen, welches unter anderem über einen so großen Adressraum verfügt, dass Engpässe bei der Adressvergabe auf absehbare Zeit nicht mehr auftreten sollten.

Als kurzfristige Maßnahme zur Linderung des Problems wurde *Network Address Translation* (NAT) im Zusammenspiel mit dynamischer Adressvergabe für Privatanwender eingeführt.[4] Es gibt verschiedene Formen von NAT. Im Kontext der nachfolgenden Diskussion ist allein One-to-Many-NAT[5] von Interesse, bei dem ein komplettes Netzwerk nach außen hin auf eine

---

1 Eine End-Site stellt eine administrative Einheit dar, die keinen Verkehr an andere Netzwerke weiterleitet. Dies kann beispielsweise das Netz eines Anbieters von Diensten und Inhalten sein, aber auch das Netz eines Heimnutzers.

2 Die großen RIRs ARIN, RIPE NCC und APNIC haben ihren jeweils letzten /8-Block bereits angebrochen, siehe https://www.arin.net/announcements/2014/20140423.html, http://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8 und http://www.apnic.net/publications/news/2011/final-8.

3 Hierbei sind beispielsweise Netzwerke neu zu nummerieren, d. h. den jeweiligen Systemen muss eine neue IP-Adresse zugewiesen werden, was bei IPv4 zu signifikanter Ausfallzeit führt.

4 Vorher wurde bereits das starre Schema der Netzklassen zugunsten von Classless Inter-Domain Routing (CIDR) aufgegeben, um den bestehenden Adressraum effizienter aufzuteilen.

5 Auch als Cone NAT bzw. als Source NAT bekannt.

IP-Adresse abgebildet wird. Wenn in dem Netzwerk private IP-Adressen nach RFC 1918 verwendet werden, dann kann auf diese Weise der Adressraum künstlich gedehnt werden. Es können also mehr Systeme an das Internet angeschlossen werden als global routbare Adressen vorhanden sind.

One-to-Many-NAT hat aus Sicht der Sicherheit und des Datenschutzes einige interessante Nebenwirkungen: Erstens wirkt das System, auf dem das NAT erfolgt, quasi wie eine rudimentäre und nicht konfigurierbare Firewall, siehe Kasten. Zweitens kann von außen nicht mehr anhand der IP-Adresse zwischen verschiedenen Systemen des inneren Netzes unterschieden werden.

Aus technischer Sicht werden NAT und dynamische Adressvergabe mit IPv6 obsolet. Dies führt bei Datenschützern zu Bedenken, da NAT und dynamische Adressvergabe einen – zumindest subjektiv wahrgenommenen – Beitrag zur Privatsphäre der Anwender leisten.

Sicherheit durch NAT?

One-to-Many-NAT wird verschiedentlich als Sicherheitsmechanismus missverstanden. Tatsächlich hat NAT einige interessante Eigenschaften. Bei One-to-Many-NAT wird ein „inneres“ Netz mit mehreren Clients über ein NAT-Gateway an das Internet angebunden. Dazu muss das Gateway für jedes ausgehende IP-Paket die interne Absenderadresse durch die IP-Adresse seines auswärtigen Interfaces ersetzen und für jedes eingehende IP-Paket die Empfängeradresse durch die interne IP-Adresse des Clients ersetzen. Um eingehende Pakete den Clients korrekt zuordnen zu können, muss das Gateway eine NAT-Tabelle führen, in der die jeweils laufenden Kommunikationsvorgänge eingetragen sind.

Im Grundzustand sind die einzelnen Clients von außen nicht sichtbar und können nicht angesprochen werden; alle Kommunikationsversuche mit einem Client im inneren Netz terminieren am Gateway. Erst wenn ein Client im inneren Netz einen Kommunikationskanal nach außen etabliert, kann dieser Client von außen aus angesprochen werden, und das auch nur im Kontext des Kommunikationskanals.

Das Gateway wirkt dadurch quasi wie ein rudimentärer Paketfilter. Dies ist ein Nebeneffekt von NAT, es ersetzt jedoch keinen vollwertigen Paketfilter, der den Verkehr nach weiteren Kriterien filtern und steuern kann. So kann ein NAT-Gateway beispielsweise weder ausgehenden Verkehr beschränken, noch eingehenden Verkehr einem Rate-Limit unterwerfen. Als Sicherheitsmechanismus ist ein NAT-Gateway in der Regel nicht ausreichend und wird selbst auf einfachen Heimroutern mit einem konfigurierbaren Paketfilter gekoppelt.

4 Der Stein des Anstoßes – IP-Adressen

Ein neuralgischer Punkt bezüglich der Unverkettbarkeit ist die IP-Adresse. Bei unveränderlichen (statischen) Adressen oder Adressen mit unveränderlichen Anteilen, die eindeutig zugeordnet werden können, besteht die Gefahr, dass verschiedene Kommunikationsvorgänge miteinander verkettet werden können. Über den Bezug von IP-Adressen zu geografischen Regionen können Benutzer zudem geortet werden (Geolocation). Dadurch ist es bei mobilen Geräten möglich, Bewegungsprofile zu erstellen.

4.1 IPv4

Man unterscheidet zwischen statischen und dynamischen IP-Adressen. Statische IP-Adressen werden fest vergeben und ändern sich praktisch nie. Diese Adressen werden bei IPv4 in der Regel an Systeme vergeben, auf denen öffentlich erreichbare Dienste betrieben

werden. Dynamische IP-Adressen ändern sich[6] dagegen mehr oder weniger oft und werden in der Regel an Endkunden vergeben, die nur Clients betreiben; die überwiegende Mehrheit der Privatanwender fällt hierunter.

Der Grundgedanke bei der Vergabe dynamischer Adressen war wie bei NAT eine optimale Nutzung eines knappen Adressraumes. In der Regel sind nicht alle Privatanwender gleichzeitig online, außerdem sind Privatanwender in der Regel nicht darauf angewiesen, eine bestimmte IP-Adresse zu verwenden. Daher können momentan nicht genutzte IP-Adressen frei an andere Privatanwender vergeben werden. Dadurch erhalten Privatanwender mit einiger Wahrscheinlichkeit jeweils eine andere IP-Adresse. Diese technische Notlösung erweist sich aus Sicht des Datenschutzes als interessant, weil dadurch ein Tracking auf Grundlage der IP-Adresse erschwert wird.

Mittlerweile sind viele Nutzer durch Angebote wie DSL oder Internet über Kabelnetze permanent online. Ohne weitere Maßnahme behält ein solcher Anschluss über einen längeren Zeitraum dieselbe IP-Adresse. Bei DSL kommt es in der Regel zu einer Zwangstrennung, beispielsweise nach 24 Stunden, um IP-Adressen von ungenutzten Anschlüssen wieder „einzusammeln“ und neu vergeben zu können.[7] Mit der zunehmenden Verbreitung von Triple-Play, also Internet sowie Telefon und Fernsehen über Internet aus einer Hand, scheint aber auch die Zwangstrennung abgeschafft zu werden. Die Kabelnetz-Anbieter führen keine Zwangstrennung durch, so dass ein Kabelnetz-Anschluss für eine längere Dauer (Wochen oder Monate) tatsächlich dieselbe IP-Adresse haben kann. Die unterstellte Dynamik von IPv4-Adressen für Endanwender ist also tatsächlich nur begrenzt gegeben.

Für mobile Geräte, die über Mobilfunk mit dem Internet verbunden sind, stellt sich allerdings eine andere Situation dar. Ihnen werden in der Regel privaten Adressen nach RFC 1918 zugewiesen, und der Provider übernimmt das NAT für Verkehr ins Internet. Da mobile Geräte in der Regel nicht permanent online sind sondern nur nach Bedarf Zugang zum Internet erhalten, wird diesen Geräten besonders häufig eine neue IP-Adresse zugewiesen. Aus Sicht des Datenschutzes stellt IPv6 für dieses Szenario daher eine Verschlechterung der Situation dar – sofern man unterstellt, dass eine Verfolgung nur über IP-Adressen erfolgt.

4.2 IPv6

Eine IPv6-Adresse umfasst 128 Bits. Diese werden in acht durch Doppelpunkte getrennte Gruppen zu je vier Hexadezimalziffern dargestellt, wobei führende Nullen entfernt werden dürfen. Eine typische IPv6-Unicast-Adresse sieht beispielsweise so aus:

```
2001:db8:5e4:c084:20c:29ff:fe78:50a1
```

Eine Unicast-Adresse besteht aus zwei Teilen, nämlich dem *Netzpräfix* und dem *Interface Identifier*. Netzpräfix und Interface Identifier umfassen jeweils 64 Bits. Im Beispiel oben ist `2001:db8:5e4:c084` das Netzpräfix und `20c:29ff:fe78:50a1` der Interface Identifier. Das Netzpräfix ist in der Regel nochmals unterteilt in ein *Routingpräfix* und eine *Subnet-ID*; in dem Beispiel könnte `2001:db8:5e4` das Routingpräfix und `c084` die Subnet-ID sein. Die näheren Details zu IPv6-Adressen und -Präfixen sind in Anhang A beschrieben.

Mit IPv6 ist zunächst keine dynamische Vergabe von IP-Adressen vorgesehen. Provider vergeben Routingpräfixe in der Regel statisch an ihre Kunden. Da den Providern große

6 D. h. sie werden zufällig aus einem Pool vergeben.

7 Andere Gründe für die Zwangstrennung sind die Geschäftsmodelle der Provider: der Betrieb von Diensten auf Privatkunden-Anschlüssen ist in der Regel unerwünscht und wird durch die dynamische Vergabe von IP-Adressen gestört. Dies kann durch Verwendung von dynamischen DNS-Diensten jedoch durchkreuzt werden.

Adressblöcke zugewiesen werden, entfällt der Grund für die dynamischen Wechsel wie bei IPv4. Zudem markiert die Vergabe eines Routingpräfixes, etwa eines /48-Präfix, dass die Provider nicht einzelne Adressen sondern ein oder mehrere Netze vergeben. Jedes einzelne Netz ist so groß, dass der Grund für NAT aus technischer Sicht ebenfalls entfällt. Daher sind sowohl Präfix als auch Interface Identifier bei IPv6 in der Regel statisch.

Im Jahr 2007 wurden für IPv6 die sogenannten Privacy Extensions (PEX) eingeführt [RFC 4941]. Mit Privacy Extensions wird für jedes Netzpräfix *zusätzlich* zum statischen Interface Identifier in regelmäßigen Abständen ein zufälliger Interface Identifier erzeugt – die daraus gebildete IP-Adresse wird auch als temporäre IP-Adresse bezeichnet. Mit temporären IP-Adressen sollte den berechtigten Bedenken begegnet werden, dass Geräte beim Wechsel zwischen verschiedenen Netzen anhand der statischen IP-Adresse verfolgt werden können.

Die sogenannten Opaque Interface Identifier sind eine weitere Entwicklung, die aus Sicht des Datenschutzes interessant sind [RFC 7217]. Sie werden in Abhängigkeit des Präfix gebildet. Wenn also das Präfix gewechselt wird, dann wird auch gleichzeitig der Interface Identifier gewechselt. In Anhang A.2 werden weitere Details zu allen Mechanismen zur Adressbildung erläutert.

Da Privacy Extensions und Opaque Interface Identifier sich nur auf die Interface Identifier beziehen, reicht der Einsatz dieser Mittel allein nicht aus, um alle Bedenken auszuräumen. Tatsächlich wurden Privacy Extensions vor allem für mobile Systeme entwickelt, wie unten in Szenario 3 dargestellt. Der Wechsel des Präfixes ergibt sich dann durch den Wechsel des Netzes.

Sicherheit ohne NAT?

Mit IPv6 wird das Ende-zu-Ende-Prinzip wieder eingeführt, da jedes System eine eigene IP-Adresse bekommt. Diese IP-Adresse ist eindeutig in dem Sinn, dass kein anderes System im Internet diese IP-Adresse hat. Es bedeutet jedoch nicht, dass diese IP-Adresse nicht auch gewechselt werden kann.

Aus dem Ende-zu-Ende-Prinzip folgt, dass grundsätzlich jedes System mit jedem anderen System im Internet kommunizieren *kann*. Dies hat in Foren und Blogs, und selbst bei IT-Betreibern gelegentlich zu der Ansicht geführt, dass mit IPv6 ohne NAT jedes System von jedem System aus erreichbar *ist*. Dies ist falsch. Die Einschränkung von Verkehr über Paketfilter und Firewalls ist natürlich genauso möglich und notwendig wie bei IPv4.

Wechselfrequenz

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Möglichkeit, eine Wechselfrequenz von zehn Minuten einstellen zu können [DSBL 2012]. Diese Forderung ist aus Sicht des Datenschutzes verständlich. Vor allem zur Verteidigung gegen Analyse-Dienste wäre eine möglichst hohe Wechselfrequenz wünschenswert. Aus technischer Sicht ist diese Forderung jedoch nicht machbar, wie in Abschnitt A.3 erläutert wird. Selbst eine Frequenz von dreißig oder sechzig Minuten stellt eine große Herausforderung dar. Entweder werden mehrere Präfixe gleichzeitig an eine Site gebunden, oder Anwendungen müssen damit umgehen können, dass IP-Adressen in bestehenden Kommunikationsbeziehungen gewechselt werden.

Dem steht die Annahme gegenüber, dass Provider aus technischen und wirtschaftlichen Gründen einem Benutzer nicht mehr als ein Präfix gleichzeitig zuteilen können oder wollen. Zudem erwarten Anwendungen in der Regel unveränderliche IP-Adressen. Wenn eine Anwendung beispielsweise dauerhafte TCP-Verbindungen nutzt, dann führt ein Wechsel der

IP-Adresse zum Verbindungsabbruch. Darüber hinaus beenden viele Webanwendungen aus Sicherheitsgründen eine Benutzeranmeldung, wenn sich die IP-Adresse des Clients ändert.

Je nach Nutzungsszenario ist für eine sinnvolle Nutzung des Internets eine Wechselfrequenz von mindestens einigen Stunden erforderlich. Verschiedene Anwendungsszenarien legen unterschiedliche Wechselfrequenzen nahe – ein sinnvoller einheitlicher Wert lässt sich nicht festlegen. Für Anwender, die ihre Datenschutz-Interessen durchsetzen wollen, sollte die Möglichkeit eingerichtet werden, den Wechsel des Präfix zu einer vom Anwender bestimmten Zeit zu veranlassen.

5 Wirksamkeit von Privacy-Mechanismen bei IPv6

In diesem Abschnitt wird für drei unterschiedliche Szenarien die Tauglichkeit verschiedener Mechanismen zur Wahrung der Privatsphäre diskutiert, siehe auch [BVA 2013, Abschnitt 8.5]. Für jedes Szenario ist zunächst zu definieren, was genau „Wahrung der Privatsphäre“ bedeutet.

5.1 Szenario 1 – Heimnutzer

In diesem Szenario wird ein beispielhafter Heimanschluss betrachtet, der von seinem ISP etwa ein /56-Routingpräfix erhält. Das Schutzziel besteht darin, dass die Kommunikationsvorgänge eines Client anhand der IP-Adresse nicht einer End-Site zugeordnet werden kann. Ein Dienstanbieter, beispielsweise eine Nachrichtenseite, oder ein Analyse-Dienst soll Aufrufe des Dienstes von einer End-Site zu unterschiedlichen Zeiten nicht miteinander korrelieren können.

Dafür ist es von Bedeutung, dass bereits unveränderliche Anteile der Adresse zur Verfolgung von Systemen ausreichen können, wenn sie eindeutig sind:

- Das Routingpräfix ist eindeutig in dem Sinn, dass keine zwei End-Sites dasselbe Routingpräfix haben können. Ein statisches Routingpräfix identifiziert also bereits die End-Site, dies verletzt aber das Schutzziel dieses Szenarios.
- Der Interface Identifier ist quasi eindeutig in dem Sinn, dass mehrere Endgeräte zwar denselben Interface Identifier bilden könnten, dies ist mit den gängigen Methoden zu ihrer Bildung (siehe Abschnitt A.2) jedoch sehr unwahrscheinlich. Ein statischer Interface Identifier identifiziert also bereits den Client (und in diesem Szenario damit auch die End-Site), dies verletzt aber das Schutzziel dieses Szenarios.

Mit IPv4 wurden in diesem Szenario dynamische IP-Adressen vergeben. Um den Effekt einer dynamischen IPv6-Adresse zu bekommen, müssen daher drei Dinge erfolgen:

- Das Routingpräfix muss regelmäßig gewechselt werden. Da das Routingpräfix vom Provider zugewiesen wird, ist der Provider dafür verantwortlich.
- Die Subnet-ID sollte regelmäßig gewechselt werden. Da die Subnet-ID auf der Seite der End-Site vergeben wird, ist der Anwender bzw. dessen Administrator dafür verantwortlich. Die Subnet-ID soll dafür verwendet werden, das interne Netz zu strukturieren. Die Wahlfreiheit ist bei der Subnet-ID daher stark eingeschränkt. Bei einem /56-Routingpräfix ist die Subnet-ID ein Wert zwischen `00` und `ff`, bei einem so kleinen Wertebereich könnte notfalls auch darauf verzichtet werden.
- Der Interface Identifier muss regelmäßig gewechselt werden. Da der Interface Identifier vom System zugewiesen wird, ist der Anwender bzw. dessen Administrator dafür verantwortlich.

Um im Sinne des Datenschutzes wirksam zu sein, müssen Präfix und Interface Identifier gleichzeitig gewechselt werden, andernfalls ergibt sich eine Möglichkeit der Verkettung, wie nachstehend beispielhaft dargestellt ist:

```
2001:db8:cafe:123:fef2:6ee6:d24a:ad72
2001:db8:cafe:123:b4f8:37f8:e8ee:7d64
2001:db8:ace:4567:b4f8:37f8:e8ee:7d64
```

Ändert sich zeitlich versetzt erst der Interface Identifier (zweite Zeile) und dann das Präfix (dritte Zeile), dann ergibt sich die Verkettung über die hier farbig markierten Teile der IP-Adresse. Der Wechsel ist dann wirkungslos im Sinne des Schutzziels.

Es stellt sich heraus, dass Privacy Extensions in diesem Szenario nur eingeschränkt dafür tauglich sind, Privatsphäre herzustellen, denn in den Standards dazu ist nicht vorgesehen, dass alleine beim Wechsel des Präfix auch der temporäre Interface Identifier gewechselt wird, siehe hierzu auch Anhang A.2. Ein neuer Interface Identifier wird nur erzeugt, wenn die Gültigkeitsdauer abläuft oder wenn das Netzwerkinterface neu konfiguriert wird. Werden Privacy Extensions in stationären Netzen verwendet, dann ergibt sich in der Regel eine Verkettung wie oben dargestellt.

Die Wirksamkeit verschiedener Mechanismen der Adressbildung[8] sowie von NAT für IPv6 und der Nutzung eines externen Proxys gegen eine Verfolgung über IP-Adressen ist in der nachstehenden Tabelle zusammengefasst.

Methode	Wirksam gegen Verfolgung der End-Site bei		
	Wechsel nur des Interface Identifiers	Wechsel nur des Präfix	Wechsel des Präfix und des Interface Identifiers
EUI-64	Nicht anwendbar	Nein	Nicht anwendbar
Windows	Nicht anwendbar	Nein	Nicht anwendbar
PEX	Nein	Nein	Nein
Opaque	Nein	Nicht anwendbar	Ja
DHCPv6	Nein	Nein	Abhängig von der Implementierung
Explizit	Nein	Nein	Abhängig von der Implementierung
NAT[9]	Nein	Nein	Abhängig von der Implementierung
Externer Proxy	Ja	Ja	Ja

Dies zeigt, dass aus Sicht eines Endanwenders mit einem Heimanschluss die Möglichkeit zum Wechsel des Präfixes notwendig ist. Darüber hinaus haben Anwender mit ausgeprägtem Datenschutz-Interesse keine große Auswahl an Mechanismen. NAT ist nur Hilfreich, wenn das NAT-Gateway den Interface Identifier seines auswärtigen Netzwerkinterfaces synchron mit dem Präfix wechselt. Wird DHCPv6 verwendet, dann hilft das nur dann, wenn der DHCPv6-Server beim Wechsel des Präfixes die Clients zur Neukonfiguration auffordert und dabei neue Interface Identifier erzeugt. Darüber hinaus sind Privacy Extensions in diesem Szenario nicht hilfreich, während Opaque Interface Identifier noch nicht verbreitet sind.

8 Siehe Abschnitt A.2 für eine genauere Beschreibung der einzelnen Mechanismen. Die Mechanismen CGA und HBA sind hier nicht aufgeführt, da sie in der Praxis nicht relevant sind.

9 Die Bewertung bezieht sich auf das Interface des NAT-Gateways.

Eine Alternative dazu ist die Verwendung eines externen Proxys, der von vielen Anwendern genutzt wird. In dem Fall ist es unerheblich, ob und wie die Adresse gewechselt wird. Dies ist dann der Einstieg zur Nutzung von Anonymisierungsdiensten.

5.2 Szenario 2 – Client einer Site mit vielen Clients

In diesem Szenario wird eine End-Site mit statischem Präfix und einer hohen Anzahl von Nutzern betrachtet, zwischen denen von außen eine Differenzierung aufgrund der IP-Adresse nicht möglich sein soll. Das Ziel besteht also darin, als Client in einer Gruppe von anderen Clients innerhalb einer End-Site nicht verfolgt werden zu können. Ein Dienstanbieter kann dann zwar feststellen, dass ein Client einer End-Site den Dienst nutzt; er kann aber nicht nachvollziehen, welcher Client innerhalb der End-Site dies ist.

In diesem Szenario ist es nicht von Bedeutung, dass eine End-Site an ihrem Präfix erkannt werden kann. Daher braucht nur betrachtet zu werden, ob die Methode zur Bildung von Interface Identifiern aus Sicht des Datenschutzes wirksam ist.

Die Wirksamkeit verschiedener Mechanismen der Adressbildung sowie von NAT für IPv6 und der Nutzung eines internen Proxys gegen eine Verfolgung über IP-Adressen ist in der nachstehenden Tabelle zusammengefasst.

Methode	Wirksam gegen Verfolgung
EUI-64	Nein
Windows	Nein
PEX	Ja
Opaque	Abhängig von der Implementierung[10]
DHCPv6	Abhängig von der Implementierung
Explizit	Abhängig von der Implementierung
NAT	Ja
Interner Proxy	Ja

Auch hier gibt es nicht viele Möglichkeiten. Da das statische Präfix in diesem Szenario irrelevant ist, sind Privacy Extensions wirksam gegen eine Verfolgung. Aus demselben Grund ist auch NAT wirksam. Opaque Interface Identifier sind dagegen keine Option, es sei denn, der zur Bildung des Opaque Interface Identifiers verwendete geheime Schlüssel würde regelmäßig gewechselt. Bei der Verwendung von DHCPv6 kommt es darauf an, ob der DHCPv6-Server für jeden Lease einen zufälligen Interface Identifier vergibt.

Eine Alternative dazu ist die Verwendung eines internen Proxys. In dem Fall ist es unerheblich, ob und wie die Adresse gewechselt wird. Da im Unternehmensumfeld ohnehin Proxys zur Content- und Malware-Filterung verwendet werden, ist die Verwendung von Proxys gegenüber NAT oder Privacy Extensions im Unternehmensumfeld die einfachste und beste Wahl.

10 Opaque Interface Identifier wären nur dann wirksam, wenn auch der Schlüssel (siehe Anhang) regelmäßig gewechselt wird, da andernfalls ein Opaque Interface Identifier bei einem statischen Präfix konstant bleibt.

5.3 Szenario 3 – Mobile Systeme (Roaming)

Dieses Szenario hat Ähnlichkeit zu Szenario 1 mit dynamischer Vergabe des Präfixes. Hierbei wird ein einzelnes mobiles System betrachtet, das sich von Netz zu Netz bewegt, beispielsweise ein Smartphone. Das Ziel besteht hier darin, als einzelner *mobiler* roaming Client nicht örtlich verfolgt werden zu können.

Ein umherwanderndes System kann durch einen unveränderlichen Interface Identifier über die Netzgrenzen hinweg verfolgt werden. Neben den Möglichkeiten zur Verfolgung und Profilierung eines Nutzers kann über den festen Interface Identifier deshalb auch ein räumliches Bewegungsprofil des Nutzers erstellt werden.

Die Wirksamkeit verschiedener Mechanismen der Adressbildung sowie von NAT für IPv6 und der Nutzung eines externen Proxys gegen eine Verfolgung über IP-Adressen ist in der nachstehenden Tabelle zusammengefasst.

Methode	Wirksam gegen Verfolgung
EUI-64	Nein
Windows	Nein
PEX	Ja
Opaque	Ja
DHCPv6 (beim ISP)	Abhängig von der Implementierung
Explizit	Abhängig von der Implementierung
NAT (beim ISP)	Ja
Externer Proxy	Ja

In diesem Szenario sind die Privacy Extensions am besten dazu geeignet, um sich wirksam gegen eine Verfolgung zu schützen. Opaque Interface Identifier sind ein gute Alternative dazu, sofern der Schlüssel gewechselt wird,[11] sie sind aber noch nicht verbreitet. NAT oder auch DHCPv6 ist dahingehend problematisch, als dass deren Betrieb in der Verantwortung der Netzbetreiber liegt. Mit Privacy Extensions kann der Anwender dagegen eigenverantwortlich für die Durchsetzung seiner Privatsphäre sorgen.

Wie in Szenario 1 stellt die Verwendung eines externen Proxys eine Alternative dar, wenn er von vielen Anwendern genutzt wird. Es ist dann ebenfalls unerheblich, ob und wie die Adresse gewechselt wird, oder wie sich der Netzbetreiber verhält.

6 Jenseits von IP-Adressen

Es gibt viele Möglichkeiten zur Identifizierung oder Verfolgung von Nutzern, von denen die IP-Adresse nur eine Möglichkeit darstellt. Einige dieser Möglichkeiten zur Identifizierung oder zur Verfolgung lassen sich kaum vermeiden.

11 Andernfalls würde beim Betreten eines Netzes ein jeweils unveränderlicher Interface Identifier gebildet werden.

6.1 Weitere Möglichkeiten zur Identifizierung

6.1.1 Fingerprinting

Clients verhalten sich je nach Hardware- und Software-Ausstattung unterschiedlich. Eine Möglichkeit zur Verfolgung eines bestimmten Clients besteht darin, diese Unterschiede auszuwerten und einen sogenannten Fingerprint zu erzeugen. Wird bei verschiedenen Kommunikationsvorgängen der gleiche Fingerprint erkannt, ist der jeweilige Client identifiziert. Die Unterschiede entstehen unter anderem, weil Standards für Protokolle oft mehrdeutig sind oder bewusst einen Spielraum zur Implementierung lassen. Dies führt in der Regel zu unterschiedlichen Implementierungen, aus denen sich Unterschiede im Verhalten ergeben. Eine weitere Quelle zum Fingerprinting sind individuelle Konfigurationseinstellungen, die das Verhalten des Clients beeinflussen.

Für das Fingerprinting können z. B. die folgenden Eigenschaften ausgewertet werden:

- Die spezifische Verwendung der Protokolle IP, ICMP, TCP und UDP
  Die Implementierung oder Konfiguration von Details wie Fragmentierung (IP) oder Window Size (TCP) ermöglicht es, einen Client zumindest einzugrenzen. Die entsprechenden Techniken sind vom System-Fingerprinting her bekannt [Kapitel 8, Lyon 2008].[12]
- Der SSL/TLS-Handshake des Systems
  Details wie die Auswahl der Cipher-Suites ermöglichen es ebenfalls, einen Client einzugrenzen.[13]
- HTTP-Header
  HTTP-Header wie `Accept`, `Accept-Charset`, `Accept-Encoding`, `Accept-Language`, `User-Agent`, `Etag` und andere können ebenfalls einen Client eingrenzen. Wenn Cookies im Browser zulässig sind, dann kann ein Client über Cookies mit Sicherheit identifiziert werden [Tillmann 2013].
- Cascading Style Sheets (CSS)
  Bestimmte Stil-Element können dazu genutzt werden, einen Client einzugrenzen, weil sie vom Browser unterschiedlich behandelt werden und ggf. dazu führen, dass weitere Inhalte nachgeladen werden.
- Canvas Fingerprinting
  Über das Canvas-Element von HTML 5 kann ein System über die Pixel-Darstellung bestimmter Elemente wie Text und Grafik identifiziert werden, denn diese erfolgt je nach installierter Hard- und Software relativ eindeutig [MoSh 2012, AEEJND 2014].
- Browser-Konfiguration einschließlich aktiver Erweiterungen

Bei allen aufgeführten Punkten findet lediglich eine Eingrenzung statt, aber über die Kombination aller Merkmale könnte man einen bestimmten Client bereits identifizieren.[14]

6.1.2 Aktive Inhalte

Über JavaScript oder Flash kann ein Browser veranlasst werden, von sich aus sehr viele Informationen preisgeben. Diese umfassen z. B. Systeminformationen, installierte Schriften,

---

12 Siehe auch http://nmap.org/book/osdetect.html.

13 Siehe auch https://www.ssllabs.com/projects/client-fingerprinting/ oder https://isc.sans.edu/diary/Browser+Fingerprinting+via+SSL+Client+Hello+Messages/17210.

14 Siehe beispielsweise https://panopticlick.eff.org oder auch http://ip-check.info/.

Zeitzone und Informationen zu Bildschirmauflösung und -Größe. Mit diesen Daten kann ein Client mit hoher Wahrscheinlichkeit identifiziert werden [Tillmann 2013, Biselli 2014].

6.1.3 Nutzerverhalten

Schließlich ist es auch möglich, dass ein Benutzer seine Identität durch sein Verhalten preisgibt. Wenn ein Benutzer eine Webseite auf sehr individuelle Weise nutzt, dann könnte sowohl der Seiten-Betreiber als auch ein Beobachter en-route einen Client identifizieren.

Einem Beobachter en-route stehen sogar noch weitere Möglichkeiten zur Verfügung. Wenn der Benutzer bestimmte Dienste in Anspruch nimmt, die einzeln oder in Kombination individuell sind, dann kann der Client auch daran identifiziert werden. Beispiele hierfür sind die Nutzung einer individuellen Menge von Nachrichten-Seiten oder die Nutzung individueller Dienste, etwa der Abruf von HTTP von einem bestimmten Server.

6.1.4 Malware

Denkbar ist auch eine Identifizierung über spezielle Malware, die entweder bei der Nutzung zufällig oder gezielt über Social Engineering eingebracht wird. Es sind auch Fälle bekannt geworden, in denen Geheimdienste oder kriminelle Organisationen Geräte bereits vor ihrer Auslieferung mit Malware infiziert haben.

6.2 Gegenmaßnahmen

Die Abwehr der genannten Möglichkeiten ist nicht trivial. Wirksame Abwehrmaßnahmen führen in vielen Fällen zu einer schlechteren Benutzbarkeit oder zu erheblichen funktionalen Einschränkungen. Einige Beispiele:

- Um CSS-Fingerprinting zu verhindern, müsste CSS deaktiviert werden. Viele Webseiten weisen ohne CSS ein unattraktives Design auf oder sind unbenutzbar. Die bestehenden Mechanismen, mit denen man CSS selektiv erlauben oder verweigern kann, überfordern die Benutzer in der Regel.
- Dasselbe gilt sinngemäß für JavaScript und Flash. Browser-Plug-Ins wie beispielsweise Request Policy und NoScript (für Firefox) zum selektiven Laden bzw. Ausführen von JavaScript erfordern oft einigen Rechercheaufwand, um eine funktionierende aber tracker-freie Ansicht zu bekommen. Ein etwas benutzerfreundlichere Alternative steht mit Plug-Ins wie Ghostery zur Verfügung.
- Auf Cookies kann ein Benutzer dagegen in der Regel verzichten, wenn er anonym bleiben möchte. Dies führt nur dann zu einer Einschränkung der Benutzbarkeit einer Web-Seite, wenn eine Anmeldung erforderlich ist und die Session über Cookies verwaltet wird. In vielen Fällen dienen Cookies auch der Speicherung von Benutzereinstellungen, solche Cookies können besonders gut zur Benutzerverfolgung eingesetzt werden. Allerdings gibt es mittlerweile zahlreiche andere Möglichkeiten, einen Benutzer auch ohne Cookies zu verfolgen [Tillmann 2013].
- Über Browser-Plug-Ins kann man HTTP-Header unterdrücken oder fälschen. Dies ist aber in der Regel wiederum auffällig, so dass ein neues Unterscheidungsmerkmal geschaffen würde. Auch bei der Fälschung von `User-Agent` sollten keine ungewöhnlichen Werte verwendet werden.
- Das eigene Benutzerverhalten so umzustellen, dass man in der Masse untergeht, könnte dazu führen, dass der Benutzer im Internet erheblich eingeschränkt wird. Dabei wäre noch zu definieren, wie ein solches Verhalten aussehen könnte. Darüber hinaus wird diese Maßnahme angesichts der anhaltenden Beliebtheit von sozialen Netzwerken und ähnlichen Angeboten kaum Akzeptanz finden. Insgesamt würde solch eine Maßnahme

eine massive Einschränkung der persönlichen Entfaltung im Internet darstellen und den Zielen einer freiheitlichen Grundordnung widersprechen.

- Die Feststellung, ob ein erworbenes Gerät frei von Malware ist, übersteigt die Kompetenz der Privatanwender.

Mögliche Maßnahmen zum Schutz vor Profilbildung sind im Privacy-Handbuch ausführlich beschrieben [Privacy].

Als Fazit lässt sich festhalten, dass auch ohne statische IP-Adressen die Möglichkeiten zur Verfolgung von Nutzern bereits sehr umfangreich gegeben sind. Die Bedeutung statischer IP-Adressen für die Bedrohung der Privatsphäre wird daher in der Regel überbewertet, andererseits bietet IPv6 auch neue Chancen zur Steigerung des Datenschutzes und der informationellen Selbstbestimmung [Donn 2011].

7 Schlussfolgerungen

Der Schutz vor Verfolgung durch IP-Adressen ist selbst bei IPv4 zumindest für Endanwender nur gering, denn die aktuelle Praxis bei der Vergabe von IP-Adressen weist einerseits eine geringere Dynamik auf als allgemein unterstellt, und andererseits können Dienstanbieter Anwender oft anhand ihres jeweils individuellen Nutzungsprofils wiedererkennen. Im Verhältnis dazu erleichtern statische IPv6-Adressen die Verfolgung eines Benutzers zwar etwas, aber nicht gravierend.

Die Konstruktion von EUI-64-Identifiern ist aus Datenschutzsicht unglücklich. Dies wurde aber durch die Einführung von Privacy Extensions und Opaque Interface Identifiern teilweise behoben. Tatsächlich stellt sich aber heraus, dass Privacy Extensions weniger wirksam sind, als deren Name es vermuten lässt. Eine im Sinne des Datenschutzes vollständig befriedigende Konstruktion der Interface Identifier existiert noch nicht. Je nach Implementierung der Opaque Interface Identifier könnten diese aber ein Schritt in die richtige Richtung sein.

Für die Unverkettbarkeit muss unterschieden werden zwischen einem Privatanwender (hier vor allem Szenarien 1 und 3) sowie einem Mitarbeiter einer Organisation (hier vor allem Szenario 2). Um als Privatanwender die Verfolgung anhand der IP-Adresse weitgehend auszuschließen, müssten die Provider die Präfixe dynamisch vergeben und gleichzeitig muss der Benutzerclient seinen Interface Identifier wechseln. Eine Verbesserung wird beispielsweise dann erreicht, wenn Präfixwechsel durch den Anwender explizit ausgelöst werden können. Zur durchgängigen Unterstützung müssten dann noch Mechanismen zur Anforderung eines neuen Routingpräfix entworfen und standardisiert werden.

Zu überlegen wäre auch, ob für eine datenschutzfreundliche Nutzung des Internets nicht die (zusätzliche) Vergabe von /64-Netzen aus speziellen Pools mit kurzen Gültigkeitsdauern durch die Provider sinnvoller wäre. Diese müssten dann geeignet gekennzeichnet werden (beispielsweise über ein Flag im Router Advertisement), so dass nur die dafür bestimmten Geräte eine Adresse für das entsprechende Netzpräfix konfigurieren.

Der dynamischen Vergabe von Präfixen sind jedoch technische Grenzen gesetzt. Eine hohe Wechselfrequenz führt entweder dazu, dass eine entsprechend große Zahl von Präfixen an eine Site gebunden wird, oder dass Anwendungen mit im laufenden Betrieb wechselnden IP-Adressen umgehen müssen. Letzteres scheitert zumindest heute daran, dass viele Anwendungen Verbindungen mit unveränderter Adresse erwarten. Die Wechselfrequenz wird daher mindestens im Bereich mehrerer Stunden liegen müssen.

Im Unternehmensumfeld können Proxys zur Wahrung der Privatsphäre der Mitarbeiter gegenüber einem externen Anbieter von Inhalten beitragen. In diesem Umfeld erfolgen in der Regel ohnehin Inhaltsanalysen zur Abwehr von Malware und eine Filterung unerwünschter

URLs auf einem Proxy. Die Verfolgung der Nutzer anhand deren IP-Adressen lässt sich dort somit ohne großen Aufwand verhindern.

Doch auch wenn ein Benutzer nicht mehr über die IP-Adresse verfolgt werden kann, sollte man Folgendes bedenken: Die IP-Adresse ist nur eine Möglichkeit, Benutzer zu verfolgen. Auf Anwendungsebene hinterlassen vor allem Browser weitere Spuren, die zur Verfolgung von Benutzern gut geeignet sind. Die Privatsphäre wird deshalb durch IPv6 nur etwas mehr bedroht als durch IPv4. Wer gezielt Anonymität im Netz sucht, sollte unabhängig vom verwendeten Netzwerkprotokoll einen Anonymisierungsdienst in Anspruch nehmen.

8 Literatur

[Biselli 2014] A. Biselli: *How-To Analyze Everyone – Teil VIII: Browser-Fingerprints und Informationskrümel ohne Cookies*. netzpolitik.org, 09.07.2014, https://netzpolitik.org/2014/how-to-analyze-browser-fingerprinting-bhaviour-tracking/.

[Donn 2011] L. Donnerhacke: *Kommentar: IPv6 und der Datenschutz*. Heise Online, 2011, http://heise.de/-1375692.

[DSBL 2011] Konferenz der Datenschutzbeauftragten des Bundes und der Länder: *Datenschutz bei der Einführung des Internet-Prokolls Version 6 (IPv6)*. Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz, 2011.

[DSBL 2012] Konferenz der Datenschutzbeauftragten des Bundes und der Länder: *Orientierungshilfe: Datenschutz bei IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft*. Der Landesbeauftragte für den Datenschutz Brandenburg, Oktober 2012.

[Hamdy 2014] S. Hamdy: *IPv6 – Die grundlegenden Funktionen, Bedrohungen und Maßnahmen*, Version 1.3. Secorvo White Paper, Februar 2014.

[AEEJND 2014] G. Acar et al.: *The Web never forgets: Persistent tracking mechanisms in the wild*. https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf .

[MoSh 2012] K. Mowery and H. Shacham: *Pixel Perfect: Fingerprinting Canvas in HTML5*. Beitrag zu *Web 2.0 Security & Privacy 2012*.

[Lyon 2008] G. Lyon: Nmap Network Scanning: *The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure Press, 2008.

[Privacy] Ohne Verfasser: *Privacy-Handbuch*. Fortlaufende Überarbeitung, letzter Stand 28. Juni 2014, verfügbar unter https://www.privacy-handbuch.de/ (siehe auch http://de.wikibooks.org/wiki/Privacy-Handbuch).

[RFC 1918] Y. Rekhter et al.: *Address Allocation for Private Internets*. IETF Best Current Practice, Februar 1996.

[RFC 3972] T. Aura: *Cryptographically Generated Addresses (CGA)*. IETF Proposed Standard, März 2005.

[RFC 4291] R. Hinden, S. Deering: *IP Version 6 Addressing Architecture*. IETF Draft Standard, Februar 2006.

[RFC 4941] T. Narten, R. Draves, S. Krishnan: *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*. IETF Draft Standard, September 2007.

[RFC 5535] M. Bagnulo: *Hash-Based Addresses (HBA)*. IETF Proposed Standard, Juni 2009.

[RFC 7217] F. Gont: *A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)*. IETF Proposed Standard, April 2014.

[Schaar 2011] P. Schaar (Hrsg.): *Internetprotokoll Version 6 (IPv6) – Wo bleibt der Datenschutz?*

[Tillmann 2013] H. Tillmann: Browser Fingerprinting: *Tracking ohne Spuren zu hinterlassen*. Diplomarbeit, Humboldt-Universität zu Berlin, 2013,

ANHANG

A Technische Details

In diesem Abschnitt werden einige technische Sachverhalte dargestellt. Die notwendigen Grundlagen mit zahlreichen Verweisen auf die jeweiligen Standards sind beispielsweise in dem Secorvo White Paper *IPv6 – Die grundlegenden Funktionen, Bedrohungen und Maßnahmen* [Hamdy 2014] dargestellt.

A.1 Adressen

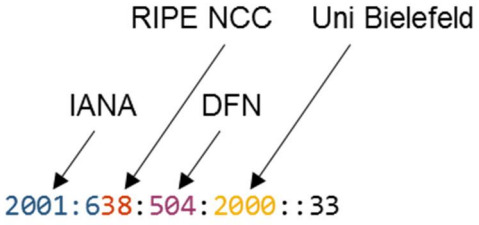
Der Adressraum von IPv6 ist unvorstellbar groß. Um dies zu verdeutlichen, reicht es, sich einmal in Erinnerung zu rufen, dass beispielsweise die kürzesten AES-Schlüssel ebenfalls 128 Bits haben. Allein die Aufzählung des Adressraums gilt als praktisch aussichtslos. Jedoch wird der Adressraum nur dünn besetzt werden, d. h. nur ein verschwindend geringer Bruchteil aller IPv6-Adressen wird je an Systeme vergeben werden. Aufgrund der Erfahrungen mit IPv4 mag das wie grob fahrlässiger Leichtsinn erscheinen, doch hat diese Strategie einen Sinn, und selbst bei sehr großzügiger Vergabe der Adressblöcke reicht der IPv6-Adressraum auf absehbare Zeit aus.

Präfixe werden in der von IPv4 her bekannten CIDR-Schreibweise notiert. Die korrekte Schreibweise des Präfix aus dem Beispiel in Abschnitt 4.2 lautet daher `2001:db8:5e4:c084::/64`. Ein /64-Präfix wird auch als Netzpräfix bezeichnet, da der Interface Identifier immer 64 Bits einnimmt und einzelne Netze unter IPv6 immer /64-Netze sind – die von IPv4 her bekannte Klasseneinteilung oder Subnetting gibt es bei IPv6 nicht. Aus demselben Grund sind längere Präfixe bei IPv6 grundsätzlich nicht vorgesehen. Kürzere Präfixe bezeichnen größere Adressblöcke und sind zur Adressbildung unvollständig. Sie enthalten aber Routinginformationen (siehe unten) und werden als Routingpräfix bezeichnet. Das Routingpräfix `2001:db8:5e4::/48` enthält die 65536 Netze `2001:db8:5e4:0:/64` bis `2001:db8:5e4:ffff:/64`.

Das Präfix enthält Routinginformationen, die für ein effizientes Routing notwendig sind. Unter IPv6 wird ein hierarchisches Routing angestrebt, um die Routingtabellen übersichtlich zu halten. Dies wird erreicht, indem das Präfix von links nach rechts immer feinere topologische Details enthält. Man kann dies in etwa mit einer Postanschrift vergleichen, die aus Angaben für Land, Stadt, Postleitzahl, Straße und Hausnummer aufgebaut ist.

In der Hierarchie IANA – RIR – LIR – ISP – Kunde ist jeder der Beteiligten für einen Teil des Präfixes verantwortlich. Unter IPv6 ist ein /64-Netz die kleinste Einheit. Jedoch vergeben die LIRs und ISPs keine Präfixe für einzelne /64-Netze an ihre Kunden, sondern kürzere Präfixe für größere Netze, beispielsweise /56-Netze oder /48-Netze. Die dementsprechend unteren 8 bzw. 16 Bits für die Subnet-ID werden durch den Kunden festgelegt.

Am Beispiel des NTP-Servers der Universität Bielefeld kann man das Prinzip gut veranschaulichen:



IANA hat das Präfix `2001:600::/23` an RIPE NCC vergeben, daraus hat RIPE das Präfix `2001:638::/32` an das DFN vergeben, das DFN hat das Präfix `2001:638:504::/48` an die Uni Bielefeld vergeben usw.

A.2 Interface Identifier

In Fortführung der Analogie zur Postanschrift stellt der Interface Identifier den Namen des Adressaten dar. Während das Präfix ein /64-Netz kennzeichnet, wird ein System in einem /64-Netz durch seinen Interface Identifier gekennzeichnet. Interface Identifier können auf verschiedene Weisen gebildet werden. Aus Datenschutzsicht sind die Methoden interessant, bei denen der Interface Identifier regelmäßig auf unvorhersehbare Weise gewechselt werden kann.

Für den störungsfreien Betrieb eines IPv6-Netzes ist es notwendig, dass jedes angeschlossene Interface über eine individuelle IP-Adresse und somit über einen individuellen Interface Identifier verfügt. Dabei spielt es keine Rolle, ob der Interface Identifier veränderlich ist oder nicht – entscheidend ist vielmehr, dass es nicht zu einer Adresskollision kommt.

A.2.1 Wahl des Interface Identifier durch den Client

Mit IPv6 kann ein System sich selbst ohne Hilfe einer zentralen Instanz eine Adresse zuweisen. Dies wird als Stateless Address Autoconfiguration (SLAAC) bezeichnet. Hierzu bildet das System einen Interface Identifier und mit einem oder mehreren Präfixen die entsprechenden Adressen.

EUI-64 [RFC 4291, Abschnitt 2.5.1]

Diese Interface Identifier werden aus der MAC-Adresse des Netzwerk-Interfaces gebildet. Der Hintergrund für diese Konstruktion ist die Annahme, dass MAC-Adressen im LAN eindeutig sind, so dass auf einfache Weise ein eindeutiger Interface Identifier gebildet werden kann. Aus der Konstruktion des EUI-64-Identifiers ergibt sich, dass der so gebildete Interface Identifier unveränderlich ist. Ein Gerät kann daher an diesem Interface Identifier erkannt werden.

Außerdem lässt sich die MAC-Adresse aus dem EUI-64-Identifier bestimmen, so dass aus diesem Interface Identifier Rückschlüsse auf die Hardware des Clients gezogen werden können. Diese Form der Interface Identifier gilt daher unter dem Aspekt des Datenschutzes als besonders problematisch.

Microsoft Windows

Unter Windows wird seit Windows Vista ein pseudo-zufälliger Interface Identifier verwendet. Dieser Interface Identifier lässt zwar keine Rückschlüsse auf die verwendete Hardware zu, ist aber darüber hinaus unveränderlich, so dass ein Gerät an seinem Interface Identifier erkannt werden kann.

Privacy Extensions [RFC 4941]

Die Konstruktion des EUI-64-Identifiers hat besonders im Zusammenhang mit Mobile IPv6 zu Bedenken geführt, dass ein Gerät verfolgt werden kann, das sich zwischen verschiedenen Netzen bewegt (Roaming). Um dies zu verhindern, wurden die Privacy Extensions entwickelt.

Bei Privacy Extensions wird in regelmäßigen Abständen, typischerweise täglich, ein pseudo-zufälliger Interface Identifier bestimmt, d. h. dieser Interface Identifier wird zwar algorithmisch

bestimmt, ist aber praktisch nicht vorhersagbar. Die daraus gebildete Adresse wird auch als temporäre Adresse bezeichnet. Der Idee nach sollen neue Verbindungen jeweils über die neueste temporäre IP-Adresse erfolgen, d. h. die neue temporäre Adresse wird bevorzugt, sofern beim Verbindungsaufbau keine andere Adresse spezifiziert wird, denn temporäre Adressen werden *zusätzlich* zu anderen Adressen gebildet.

Über Router Advertisements können mehrere Netzpräfixe gleichzeitig vergeben werden. Grundsätzlich ist vorgesehen, für jedes Netzpräfix denselben Interface Identifier zu verwenden. Dies hat Performance-Gründe, denn für jeden Interface Identifier muss das System einigen Multicast-Gruppen beitreten. Es ist aber auch zulässig für eine Implementierung, für jedes Präfix einen anderen Interface Identifier zu wählen [RFC 4941, Abschnitt 3].

Privacy Extensions haben jedoch einen Haken, der ihren Beitrag zur Wahrung der Privatsphäre signifikant schmälert: *Wird über ein Router Advertisement das Netzpräfix gewechselt, dann ändert sich der Interface Identifier in der Regel nicht*.[15] Erst wenn das Netzwerkinterface neu konfiguriert wird, ändert sich der Interface Identifier. Mit anderen Worten, Privacy Extensions sind wirksam bei einem echten Wechsel des Netzes, nicht aber bei einem Wechsel des Präfix. Experimente mit verschiedenen Betriebssystemen bestätigen dieses Verhalten. Ändert sich nur das Präfix, aber nicht der Interface Identifier, etwa im Rahmen der dynamischen Vergabe von Präfixen, dann ist dieser Wechsel aus Sicht des Datenschutzes unwirksam, siehe Abschnitt 4.2. Dieses technische Detail zeigt, dass Privacy Extensions bei der Diskussion um Datenschutz mit IPv6 überbewertet werden.

Opaque Interface Identifier [RFC 7217]

Opaque Interface Identifier sind als Ersatz zu EUI-64-Identifiern entwickelt worden. Sie werden mit Hilfe einer Einweg-Funktion gebildet, d. h. sie lassen keinen Rückschluss auf die MAC-Adresse oder andere Merkmale zu. Opaque Interface Identifier werden in Abhängigkeit vom Netzpräfix und einem geheimen Schlüssels erzeugt.

Bleibt der geheime Schlüssel konstant, dann bleibt auch die Interface-ID für ein festes Netzpräfix konstant; wird der Schlüssel dagegen regelmäßig gewechselt, dann ergibt sich derselbe Effekt wie bei Privacy Extensions. Ob der Schlüssel gewechselt werden kann, ist der jeweiligen Implementierung überlassen. RFC 7217 ist noch relativ jung und noch nicht verbreitet. Wie Schlüsselwechsel in der Praxis gehandhabt werden, wird sich noch zeigen.

Werden mehrere Netzpräfixe auf einem Interface verwendet, etwa bei Multihoming, dann haben Opaque Interface Identifier gegenüber Privacy Extensions den Vorteil, dass für unterschiedliche Netzpräfixe ein individueller Interface Identifier gebildet wird, während bei Privacy Extensions derselbe Interface Identifier über alle Netzpräfixe eines Interfaces verwendet wird.

Cryptografically Generated Addresses [RFC 3972]

Im Zusammenhang mit der Secure Neighbor Discovery (SEND) wurden Cryptographically Generated Addresses (CGA) eingeführt. Die Konstruktion dieser Adressen führt zu Interface Identifiern, die vom Präfix abhängen und unvorhersagbar sind. Aus Datenschutzsicht ist das

---

15 Siehe auch Abschnitt 3.3 aus RFC 4941: *When processing a Router Advertisement with a Prefix Information option carrying a global scope prefix for the purposes of address autoconfiguration (i.e., the A bit is set), the node MUST perform the following steps: […] 6. New temporary addresses MUST be created by appending the interface's* ***current randomized interface identifier*** *to the prefix that was received.*

zwar interessant, bietet aber keinen Vorteil zu Opaque Interface Identifiern. SEND ist in der Praxis bisher nicht relevant, und vermutlich wird sich das auch nicht mehr ändern, daher wird für die Diskussion in diesem Artikel nicht weiter darauf eingegangen.

Hash-Based Addresses [RFC 5535]

Um die Zugehörigkeit von Adressen im Fall von Multihoming nachweisen zu können, wurden Hash-Based Addresses (HBA) eingeführt. Multihoming bezeichnet die Konstruktion, eine Site über mehrere Provider an das Internet anzubinden. Diese Konstruktion wird typsicherweise aus Gründen der Hochverfügbarkeit einer Internet-Anbindung gewählt. Wie bei CGA werden auch hier Adressen mit zufälligen Interface Identifiern gebildet, die von den jeweiligen Präfixen abhängen. Multihoming kommt im Privatkundengeschäft nicht vor, und HBA ist in der Praxis bisher nicht aufgetreten, so dass auch darauf für die Diskussion in diesem Artikel nicht weiter eingegangen wird.

A.2.2 Andere Formen der Adressvergabe

Alternativ zur Adressvergabe über SLAAC stehen die von IPv4 bekannten Methoden zur Verfügung:

DHCPv6

Anders als DHCP für IPv4 kann DHCPv6 zur Adressvergabe (stateful DHCPv6) oder nur zur Verteilung anderer Parameter wie IP-Adressen von DNS- und NTP-Servern (stateless DHCPv6) verwendet werden. Wird DHCPv6 zur Adressvergabe verwendet, dann werden nicht Interface Identifier sondern vollständige IPv6-Adressen verteilt. Diese sind für eine Lease-Dauer gültig, der entsprechende Lease muss regelmäßig erneuert werden. DHCPv6 hat den Vorteil, dass Adressen zentral verwaltet werden und ein Eintrag im Domain Name Service (DNS) zuverlässig gegeben ist. Mit DHCPv6 ist die Adressvergabe allerdings von einem Dienst abhängig. Nach dem Grunddesign von IPv6 wäre das nicht notwendig.

Prinzipiell ist es mit DHCPv6 möglich, über eine begrenzte Lease-Dauer Adressen mit zufälligem Interface Identifier zu vergeben. Damit kann die Wirkung von temporären Adressen auch mit DHCPv6 erzielt werden. Die Vergabe von Adressen mit zufälligem Interface Identifier wird jedoch erst von neueren DHCPv6-Implementierungen angeboten.

Ein vergebener Lease kann über DHCPv6 nicht zurückgezogen werden. Wenn sich Parameter ändern, beispielsweise das Netzpräfix, dann kann der DHCPv6-Server die Clients über eine RECONFIGURE-Nachricht dazu auffordern, neue Leases zu beziehen.

Explizit

Adressen können stets explizit zugewiesen werden, wobei dies auch automatisiert über ein Skript erfolgen kann. In der Regel werden Adressen explizit vergeben, um einfach strukturierte Adressen verwenden zu können, beispielsweise `2001:db8:cafe::80` für einen Webserver oder `2001:db8:cafe::53` für einen DNS-Server. Für Endgeräte ist dies jedoch ungewöhnlich und bedeutet zusätzlichen Aufwand. In der Praxis wird dies nur in seltenen Einzelfällen relevant sein, daher wird nicht weiter darauf eingegangen.

A.2.3 Übersicht der Mechanismen zur Bildung von Adressen

In der nachstehenden Tabelle sind die Eigenschaften der einzelnen Methoden zur Bildung von Interface Identifiern und Adressen zusammengefasst.

Methode	Zeitlich Veränderlich	Zufällig	Wechsel bei Präfixwechsel	Wechsel bei Netzwechsel	Verbreitung
EUI-64	Nein	Nein	Nein	Nein	Hoch
Windows	Nein	Ja	Nein	Nein	Hoch
PEX	Ja	Ja	Nein	Ja	Hoch
Opaque	Abhängig von Implementierung	Ja	Ja	Ja	Niedrig
CGA	Nein	Ja	Ja	Ja	Keine
HBA	Nein	Ja	Ja	Ja	Keine
DHCPv6	Abhängig von Implementierung	Abhängig von Implementierung	Über RECONFIGURE	Abhängig von Implementierung	Hoch
Explizit	Abhängig von Nutzung	Abhängig von Nutzung	Abhängig von Nutzung	Abhängig von Nutzung	Hoch

A.3 Gültigkeitsdauer

Wenn ein Interface konfiguriert wird, dann erhält es eine IPv6-Adresse. Dies geschieht in der Regel automatisch. Die gängigen Methoden für die Adresszuweisung sind SLAAC oder stateful DHCPv6. Bei SLAAC bildet das System eine IP-Adresse aus einem vom Router bestimmten Präfix und einem vom System bestimmten Interface Identifier, bei stateful DHCPv6 hingegen wird dem System die komplette IP-Adresse vom DHCP-Dienst zugewiesen.

Bei SLAAC verteilen die Router-Informationen über Präfixe mittels sogenannter Router Advertisements. Dies sind spezielle ICMPv6-Nachrichten, die von Routern in regelmäßigen Abständen versendet werden. Sie können aber auch über sogenannte Router Solicitations von einem System angefordert werden.

Ein Router Advertisement kann Informationen für ein oder mehrere Präfixe enthalten. Sie enthalten unter anderem auch zwei Gültigkeitsdauern für die jeweiligen Präfixe, die als Preferred Lifetime und Valid Lifetime bezeichnet werden. Mit diesen Parametern kann die Gültigkeit der aus dem Präfix gebildeten Adresse begrenzt werden.

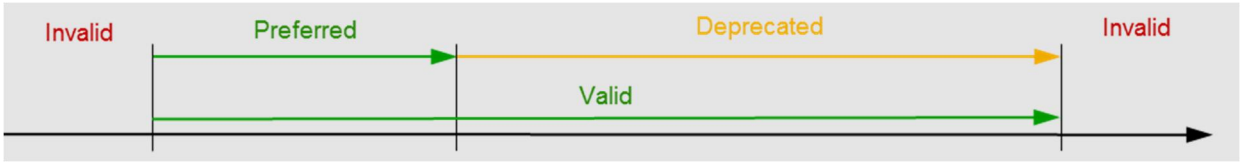


Abbildung 1: Zustände einer IPv6-Adresse (vereinfacht)

Nach der Zuweisung zu einem Interface ist die Adresse im Zustand Preferred (Bevorzugt). In diesem Zustand kann die IP-Adresse frei genutzt werden. Dieser Zustand wird durch regelmäßige Router Advertisements aufrechterhalten.

Ohne Auffrischung geht die Adresse nach Ablauf der Preferred Lifetime in den Zustand Deprecated (Abgelaufen) über. In diesem Zustand sollte auf dem Interface keine ausgehende Verbindung[16] unter dieser IP-Adresse veranlasst werden. Eingehende und bestehende Verbindungen können jedoch angenommen bzw. weiterhin genutzt werden.

16 Für IP existiert das Konzept einer Verbindung nicht; „Verbindung“ ist hier daher im Sinn eines Kontextes gemeint, innerhalb dessen IP-Pakete ausgetauscht werden.

Erfolgt bis zum Ablauf der Deprecated Lifetime keine Auffrischung, dann geht die IP-Adresse in den Zustand Invalid (Ungültig) über. In diesem Zustand darf die IP-Adresse nicht genutzt werden, auch nicht für bestehende Verbindungen.

Privacy Extensions

Eine Neuerung von IPv6 gegenüber IPv4 besteht darin, dass einem Interface mehrere Adressen gleichzeitig zugewiesen werden können. Dies ist vor allem beim Wechsel von IP-Adressen interessant, da mehrere Adressen im Zustand Deprecated und eine Adresse im Zustand Preferred nebeneinander genutzt werden können. Dieses Konzept ermöglicht es überhaupt erst, dass Privacy Extensions genutzt werden können (siehe Abschnitt A.2).

Für Privacy Extensions existieren neben den Parametern Preferred und Valid Lifetime zusätzlich die Parameter Temporary Preferred Lifetime (im Folgenden t_p) und Temporary Valid Lifetime (im Folgenden t_v) sowie der Desync Factor (im Folgenden d). Es gilt, dass unabhängig von den Angaben in einem Router Advertisement ein Interface Identifier niemals länger als $t_p - d$ bevorzugt und insgesamt niemals länger als t_v gültig ist. Der Desync Factor wird als zufälliger Wert zwischen 0 und 600 Sekunden beim Systemstart gewählt.[17] Er verhindert, dass mehrere Systeme ihre IP-Adresse nach einem festen Muster wechseln. Ein regelmäßiger Wechsel der IP-Adressen in der Größenordnung von 10 Minuten (wie in [DSBL 2012] vorgeschlagen) ist daher technisch nicht sinnvoll.

Die maximale Anzahl der für ein Präfix geltenden Adressen kann aus der Temporary Preferred Lifetime und der Temporary Valid Lifetime errechnet werden. In der nachstehenden Abbildung wird beispielhaft gezeigt, wie viele Adressen zu einem bestimmten Zeitpunkt gültig sind.

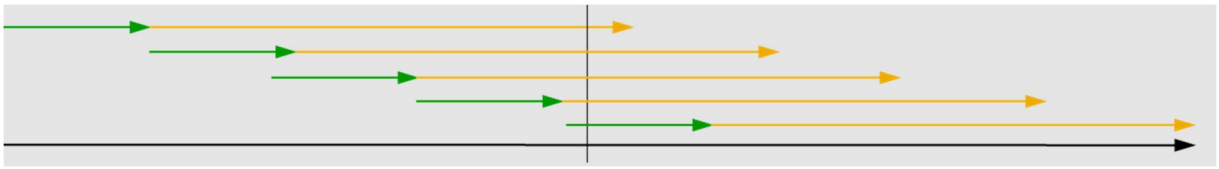


Abbildung 2: Überlappende Gültigkeitszeiträume

Die maximale Anzahl n_a der für jeweils ein Präfix geltenden Adressen ist bestimmt durch

$$n_a = \left\lceil \frac{t_v}{t_p - 600\text{s}} \right\rceil \leq \frac{t_v}{t_p - 600\text{s}} + 1$$

Werden mehrere Präfixe verwendet, dann ist das entsprechende Vielfache anzusetzen.

Dabei wird deutlich, dass das Betriebssystem sehr viele Adressen für ein Interface vorhalten muss, wenn die Adressen an diesem Interface sehr oft gewechselt werden. Die optimale Wahl der Parameter t_v und t_p hängt vom Nutzerverhalten ab. Aus Sicht des Datenschutzes sind jeweils kleine Werte optimal. Langlebige Verbindungen, etwa für Media Streaming oder Online-Spiele, erfordern aber ein entsprechend großes t_v. Selbst wenn keine Dauerverbindungen genutzt werden, erwarten viele Anwendungen, dass die eigene IP-Adresse sich nicht verändert, d. h. dann muss t_p entsprechend groß gewählt werden. Die nachstehende Tabelle zeigt beispielhaft einige Werte für die Anzahl der aktiven Adressen bei unterschiedlicher Wechselfrequenz für jeweils nur einer Adresse.

[17] Jedoch so, dass $d < t_p$.

Tabelle 1: Anzahl der aktiven temporären Adressen für verschiedene Werte der Preferred und der Valid Lifetime bei Verwendung von Privacy Extensions

Preferred Lifetime	Valid Lifetime	Maximale Anzahl der Adressen
15 min	2 Std	24
15 min	8 Std	96
20 min	8 Std	48
30 min	8 Std	24
30 min	12 Std	36
1 Std	12 Std	15
2 Std	3 Std	2
2 Std	12 Std	7
2 Std	24 Std	14
6 Std	8 Std	2
1 Tag	1,5 Tage	2
1 Tag	2 Tage	3
1 Tag	7 Tage	8

Die Grundeinstellung vieler Betriebssysteme entspricht dem letzten Eintrag. Mit den entsprechenden Werten für die Preferred und die Valid Lifetime verfügt ein Interface über acht temporäre Adressen zusätzlich zu der statischen Adresse – und zwar pro Präfix, einschließlich des Link-Local-Präfixes `fe80::`. Neben den Unicast-Adressen ist jedem Interface zusätzlich für jeden Interface Identifier die entsprechende Link-Local Solicited-Node Multicast-Adresse zugewiesen [RFC 4291, Abschnitt 2.8]. Nimmt man stattdessen einen Wert von fünfzehn Minuten bzw. acht Stunden an, dann ist es denkbar, dass ein Gerät mit beschränkten Ressourcen wie etwa ein Smartphone mit einigen hundert Adressen pro Interface schnell überfordert ist.

Daneben ist noch eine weitere Überlegung zu berücksichtigen: Wie in Abschnitt 4.2 gezeigt, reichen Privacy Extensions zur Wahrung der Privatsphäre in einem festen Netz nicht aus. Datenschützer fordern die dynamische Vergabe von Präfixen durch die Provider. Das ist aus Sicht des Datenschutzes nur dann sinnvoll, wenn es gleichzeitig mit dem Wechsel des Interface Identifiers geschieht. *In diesem Fall ist nicht ein einzelnes Präfix sondern die entsprechende Anzahl von Präfixen an eine End-Site gebunden*. Es ist kaum vorstellbar, dass ein Provider ohne weiteres acht oder mehr Präfixe gleichzeitig an einen Kunden vergibt. Es ist höchstens denkbar, dass die Valid Lifetime nicht oder nur unwesentlich größer als die Preferred Lifetime ist (siehe dritt- oder viertletzter Eintrag der Tabelle). Dies ist allerdings nur dann sinnvoll, wenn die Preferred Lifetime nicht zu klein gewählt wird, da andernfalls Anwendungen wie Media Streaming gestört werden.