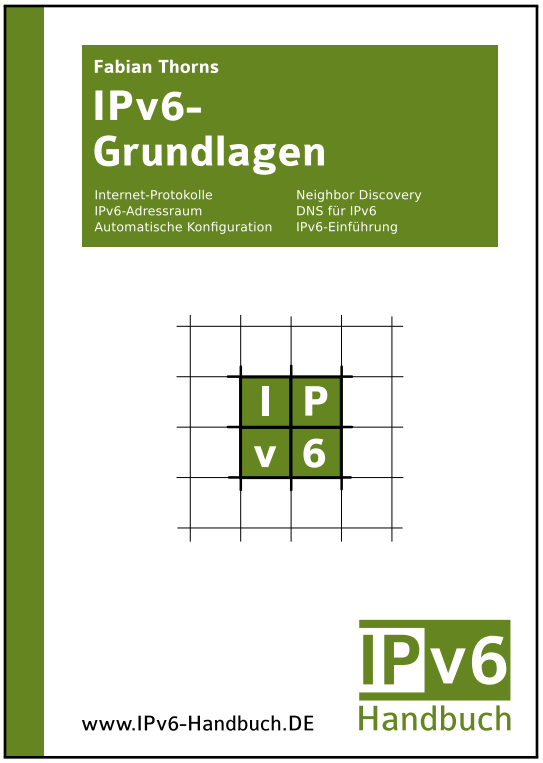
IPv6 Handbuch

Auszug / Leseprobe



Fabian Thorns

IPv6-Grundlagen

1. Auflage 2014
(Entspricht Version 20140204002 vom 4. Februar 2014)

Diese Datei ist ein Auszug aus dem E-Book *IPv6-Grundlagen* aus der Reihe *IPv6-Handbuch*. Das vollständige E-Book können Sie auf *www.IPv6-Handbuch.DE* erwerben. Dort finden Sie auch weitere Informationen über die anderen Bände dieser Reihe.

IPv6 Handbuch

Kapitel 3

Automatische Konfiguration und Neighbor Discovery

Von dem erweiterten Adressraum abgesehen bringt IPv6 die automatische Konfiguration aller Teilnehmer in einem Netzwerk und die Erneuerung verschiedener Verfahren, die im Hintergrund die Kommunikation in einem IP-Netzwerk erst ermöglichen. Beide Themen werden unter den Schlagwörtern *Automatische Konfiguration* und *Neighbor Discovery* zusammengefasst. Ihre Funktionsweise ist für die Konfiguration von Netzwerken und Routern sowie die Analyse von Fehlern von zentraler Bedeutung und deshalb Thema dieses Kapitels.

3.1 Automatische Konfiguration in IPv6-Netzen

3.1.1 Verfahren zur Adresskonfiguration

Wenn ein Gerät an ein Netzwerk angeschlossen wird, benötigt es verschiedene Informationen über das Netz, um darin kommunizieren zu können. Dazu zählen vor allem eine freie IP-Adresse sowie Informationen über die On-Link-Prefixe und ihre Länge, den Default-Router und die Namensauflösung. Im einfachsten Falle werden diese Daten manuell konfiguriert. Ab einer gewissen Anzahl an Teilnehmern ist dies aber nicht mehr praktikabel, zumal bei Änderungen jede einzelne Konfiguration manuell angepasst werden muss.

In einem IPv4-Netz befindet sich deshalb häufig ein Server für das *Dynamic Host Configuration Protocol*, kurz *DHCP*, der Teilnehmern auf Anfrage eine IPv4-Adresse zuweist und ihnen die Eckdaten des Netzes übermittelt. Dieser Dienst muss jedoch eingerichtet und gepflegt werden. Zudem ist DHCP kein einfaches Protokoll, da der DHCP-Server den Zustand aller von ihm vergebenen Adressen aktiv verwaltet, was mit einem gewissen Aufwand verbunden ist.

IPv6 überträgt die Aufgabe, die Teilnehmer mit den zur Konfiguration notwendigen Informationen zu versorgen, direkt den Routern des jeweiligen Netzes. Hinsichtlich der Adresskonfiguration machen sie sich dabei die Teilung von IPv6-Adressen in Prefix und Interface Identifier zunutze, indem sie in Form so genannter *Router Advertisements* lediglich Informationen darüber verbreiten, welche Prefixe in dem Netzwerk zur automatischen Konfiguration freigegeben sind, und es im Übrigen den einzelnen Teilnehmern überlassen, aus diesen Prefixen mit ihrem jeweiligen Interface Identifier IPv6-Adressen zusammenzusetzen. Die Anforderungen an die Router werden durch dieses Verfahren gegenüber den Anforderungen an einen DHCP-Server deutlich gesenkt. Trotzdem gibt es mit *DHCPv6* erweiterte Funktionen für die Konfiguration von Teilnehmern, die sowohl ergänzend als auch alternativ zu Router Advertisements eingesetzt werden können. Da ein DHCPv6-Server seine Clients im Gegensatz zu einem Router individuell verwaltet, wird die Konfiguration per Router Advertisements auch *Stateless Autoconfiguration*, kurz *SLAAC*, genannt, und die Konfiguration per DHCPv6 als *Stateful Autoconfiguration* bezeichnet.

Mit diesen Verfahren ergeben sich mehrere Möglichkeiten für die Konfiguration der Teilnehmer eines IPv6-Netzwerkes:

- **Statische Konfiguration:** Im einfachsten Falle werden die IPv6-Adressen fest auf dem Gerät hinterlegt, so dass das Betriebssystem sie lokal auslesen und einrichten kann. Dies ist vor allem für Server, Router und andere Infrastruktur-Komponenten sinnvoll, da sie so nicht von anderen Diensten abhängen und konstant adressierbar sind, was insbesondere im Fehlerfalle von zentraler Bedeutung ist. Zudem ist die manuelle Rekonfiguration bei genauer Dokumentation für diese – vergleichsweise – wenigen Geräte oftmals durchaus vertretbar.

- **Stateless Autoconfiguration über Router Advertisements:** Liegen einem Teilnehmer keine Informationen über seine IPv6-Adressen vor, muss er sich diese Informationen aus einer anderen Quelle erschließen. Dazu sendet er eine so genannte Router Solicitation in das Netzwerk, die von den dort befindlichen Routern mit je einem Router Advertisement beantwortet wird. Der Teilnehmer konfiguriert sich daraufhin selbst, ohne dass der Router eine Rückmeldung über die Konfiguration erhält. Router Advertisements können zudem Angaben zu Routern und anderen Eigenschaften des Netzes machen. Stateless Autoconfiguration ist Teil der Neighbor Discovery, die verschiedene weitere Funktionen eines IPv6-Netzes koordiniert.

- **Stateless Autoconfiguration mit zusätzlichen Informationen:** Router können in den Advertisements anzeigen, dass per DHCPv6 weitere Informationen über das Netzwerk verteilt werden. Zwar fragt ein Teilnehmer diese Informationen dann per DHCPv6 ab, seine IPv6-Adresse erhält er allerdings nicht per DHCPv6, sondern weiterhin auf Grundlage der Router Advertisements. Dieses Verfahren wird auch als Stateless DHCPv6 bezeichnet.

- **Stateful Autoconfiguration per DHCPv6:** Neben ergänzenden Konfigurationsdaten kann ein DHCPv6-Server auch selbst IPv6-Adressen vergeben. Auch hierauf wird in Router Advertisements hingewiesen. Der Client erhält dann eine einzelne, vollständige, ihm zugewiesene IPv6-Adresse, die er unverändert übernimmt. Ein DHCPv6-Server führt über seine Clients und ihre Adressen genauestens Buch, der Client muss sich die fortwährende Nutzung der Adresse

regelmäßig vom DHCPv6-Server genehmigen lassen. Neben einzelnen Adressen können auch ganze Prefixe per DHCPv6 verteilt werden.

Die verschiedenen Verfahren schließen einander nicht aus. Ein Teilnehmer kann sie in beliebigen Kombinationen gemeinsam nutzen, um beispielsweise zusätzlich zu manuell konfigurierten Adressen auch Router Advertisements auszuwerten und Adressen per DHCPv6 zu beziehen. Auch muss die Konfiguration hinsichtlich der IPv6-Adressen nicht konsistent sein, grundsätzlich können etwa per DHCPv6 Adressen anderer Prefixe verteilt werden als über Router Advertisements. Zudem können in einem Netzwerk mehrere Router und DHCPv6-Server Konfigurationsdaten austeilen.

Neben den genannten Verfahren führt jede Netzwerkschnittstelle mit aktivem IPv6 zwangsweise eine link-lokale Adresse aus dem Prefix `fe80::/64`. Natürlich ist auch dies eine automatische Konfiguration, allerdings ist ihr Nutzen für den Anwender aufgrund des begrenzten Scopes der Adresse eher gering. Die hier besprochenen Konfigurationsverfahren kommunizieren allerdings fast ausschließlich über link-lokale Adressen, da sie garantiert verfügbar und unabhängig von den Adressen mit größerem Scope sind, die durch diese Verfahren ja erst erstellt beziehungsweise zugewiesen werden. Link-lokale Adressen sind zudem die einzige automatische Konfiguration, die auch Router auf ihren Interfaces durchführen.

3.1.2 Lebenszyklus von IPv6-Adressen

Eine IPv6-Adresse ist nicht sofort und für alle Zeit gültig. Sie durchläuft vielmehr verschiedene Zustände mit unterschiedlicher Bedeutung:

- **Tentative:** Eine neue IPv6-Adresse – egal, ob manuell zugewiesen, aus der lokalen Konfiguration ausgelesen, in Folge eines Router Advertisements generiert oder von einem DHCPv6-Server zugeteilt – hat zunächst den Zustand *tentative*. In diesem Zustand darf sie noch nicht genutzt werden, da noch nicht fest steht, ob nicht ein anderer Teilnehmer dieselbe Adresse bereits führt. Um dies herauszufinden, wird ein als *Duplicate Address Detection*, kurz *DAD*, bezeichneter Prozess durchgeführt. Er wird in Kapitel 3.2.3 im Detail beschrieben. An dessen Ende wird entweder die Eindeutigkeit der Adresse festgestellt oder die Adresse verworfen und gegebenenfalls eine andere Adresse ausgewählt und per DAD geprüft.
- **Preferred:** Wenn die Adresse eindeutig ist, wechselt sie in den Zustand *preferred*. Dann werden neue Verbindungen bevorzugt von dieser Adresse aus aufgebaut. Allerdings ist dieser Zustand an eine Gültigkeitsdauer geknüpft. Sofern diese *Preferred Lifetime* nicht unbegrenzt ist, verliert die Adresse nach Ablauf dieses Zeitraums ihren Zustand. Die Restlaufzeit wird allerdings immer dann wieder zurückgesetzt, wenn ein neues Router Advertisement für das Prefix der Adresse eintrifft oder ein DHCPv6-Server die Adresse bestätigt. Solange beispielsweise ein Router regelmäßig rechtzeitig vor Ablauf ein neues Router Advertisement mit der immer gleichen Preferred Lifetime für das Prefix sendet, läuft der Zustand nicht aus.

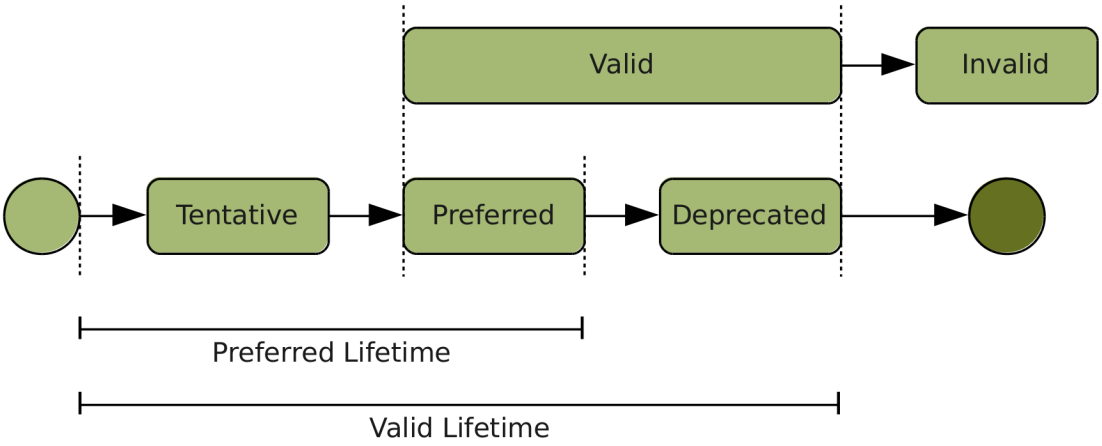


Abbildung 3.1: Abfolge der Phasen im Lebenszyklus einer IPv6-Adresse (Schematische Darstellung).

- **Deprecated:** Zusätzlich hat jede IPv6-Adresse eine so genannte *Valid Lifetime*, die größer oder gleich der Preferred Lifetime ist. Läuft letztere aus, verliert die Adresse zwar den Zustand preferred, bleibt aber bis zum Ablauf der Valid Lifetime im Zustand *deprecated*. Die Adresse ist dann zwar noch gültig und darf insbesondere für bestehende Verbindungen weiter genutzt werden. Neue Verbindungen werden dann aber bevorzugt von einer anderen Adresse im Zustand preferred aufgebaut, da davon auszugehen ist, dass auch die Valid Lifetime ohne Verlängerung verstreicht. Bis dahin können Anwendungen jedoch weiter auf die Adresse zurückgreifen, wenn der Wechsel auf eine andere Adresse für sie beispielsweise mit dem Abbruch bestehender Verbindungen verbunden wäre.
- **Invalid:** Nach Ablauf der Valid Lifetime verliert die Adresse ihre Gültigkeit, ist fortan im Zustand *invalid* und verschwindet aus der laufenden Systemkonfiguration. Sie kann jedoch jederzeit etwa über ein neues Router Advertisement wieder aktiviert werden. Dann durchläuft die Adresse den gesamten Lebenszyklus erneut.

Mit den verschieden Zuständen lassen sich IPv6-Adressen in zwei Kategorien aufteilen:

- **Gültige** Adressen (*valid*) sind entweder preferred oder deprecated und dürfen von einem Teilnehmer genutzt werden.
- **Ungültige** Adressen (*invalid*) sind auf keinem Interface aktiv, weil sie entweder noch tentative sind oder ihre Valid Lifetime abgelaufen ist.

Die verschiedenen Zustände einer IPv6-Adresse sind in Abbildung 3.1 zusammengefasst. Die Verlängerung der Lebenszeiten einer IPv6-Adresse illustriert Abbildung 3.2 auf der nächsten Seite.

Manuell zugewiesene Adressen sowie die obligatorische link-lokale Adresse aus dem Prefix `fe80::/64` haben stets eine unbegrenzte Gültigkeit und bleiben so auch ohne weiteres Zutun dauerhaft in dem Zustand preferred. Auch diese Adressen werden mittels DAD geprüft, bevor sie valid werden.

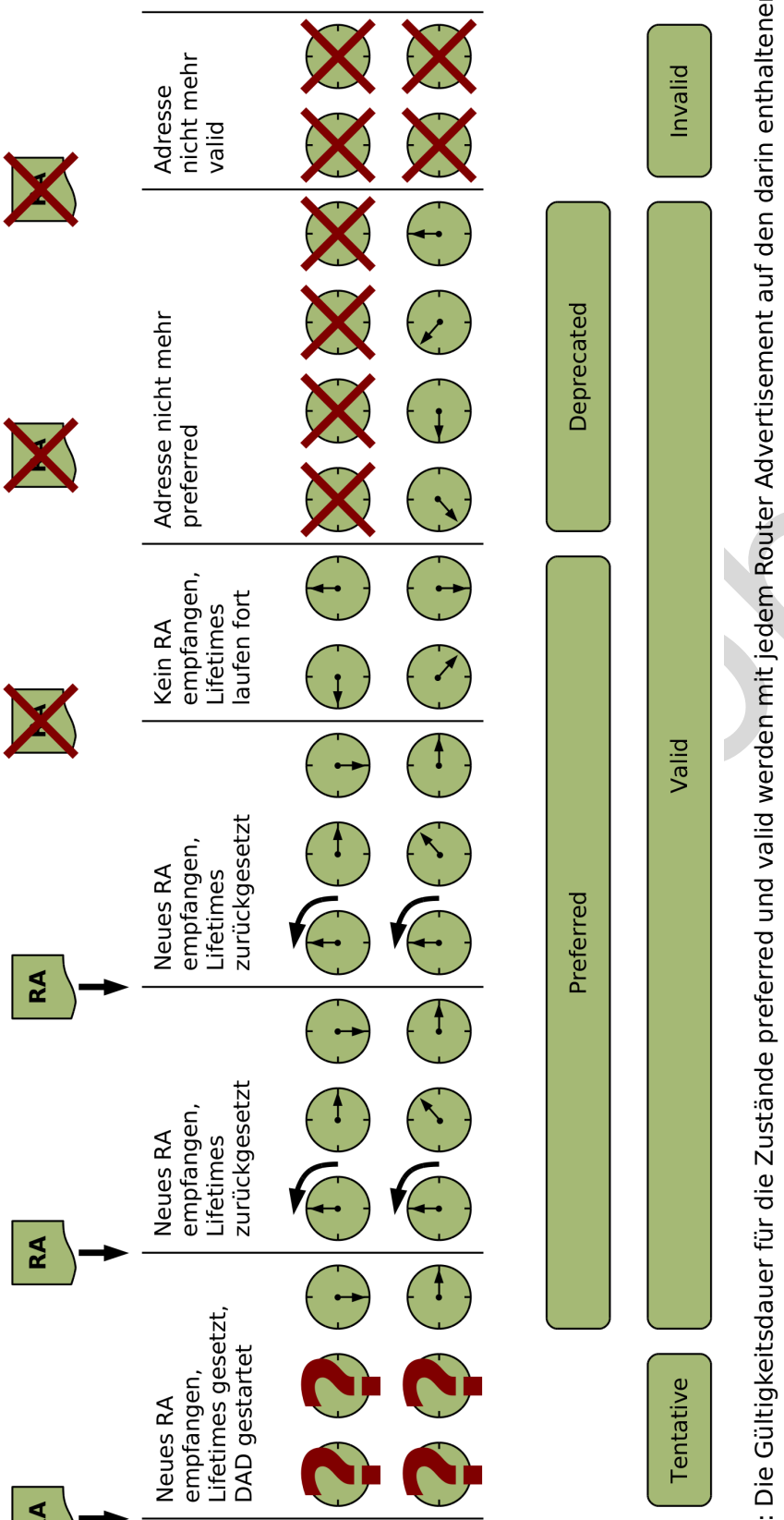


Abbildung 3.2: Die Gültigkeitsdauer für die Zustände preferred und valid werden mit jedem Router Advertisement auf den darin enthaltenen Wert zurückgesetzt (Schematische Darstellung).

Jede temporäre Adresse, deren Interface Identifier wie in Kapitel 2.4.3 beschrieben gemäß der Priacy Extensions berechnet wurde, erhält zwei weitere Zeitzähler, um den regelmäßigen Wechsel der temporären Adresse zu steuern. Die beiden zusätzlichen Zeitzähler werden bei der Inbetriebnahme der Adresse gesetzt und zählen fortan herunter, wie lange die Adresse mit ihrem aktuellen zufälligen Interface Identifiers noch im Zustand preferred respektive valid verbleiben darf.

So lange die temporäre Adresse mit ihren zusätzlichen Zeitzählern im Zustand preferred ist, verlängern Router Advertisements für das Prefix die reguläre Laufzeit der temporären Adresse immer wieder. Die zusätzlichen Zeitzähler der Adresse werden hingegen nicht zurückgesetzt. Läuft eine der beiden Preferred Lifetimes ab, wird die Adresse zunächst deprecated, bis schließlich auch entweder die reguläre Valid Lifetime des Prefixes oder die zusätzliche Valid Lifetime der temporären Adresse abläuft und die Adresse invalid wird.

Laut dem Privacy Extension-Standard in RFC 4941 ist eine temporäre Adresse standardmäßig einen Tag preferred und eine Woche valid. Rund fünf Sekunden vor Ablauf der Preferred Lifetime wird eine neue Adresse mit demselben Prefix und einem neuen zufälligen Interface Identifier generiert, um einen Wechsel der Adressen einzuläuten. Unabhängig von den Zeitzählern werden neue temporäre Adressen zudem bei dem Wechsel eines Netzwerkes gebildet.

3.1.3 On-Link- und Off-Link-Eigenschaft von Adressen und Prefixen

In einem Netzwerk gelten üblicherweise mehrere IPv6-Prefixe: Neben den obligatorischen link-lokalen Adressen sind zumeist auch lokale und globale Prefixe – letztere möglicherweise von verschiedenen Providern – gleichzeitig im Umlauf. Aus Sicht eines Teilnehmers sind alle Prefixe und Adressen, die in einem Netzwerk gelten mit dem er direkt verbunden ist, *on-link*. Alle anderen Prefixe werden hingegen als *off-link* bezeichnet.

Obwohl alle Teilnehmer in der Regel mehrere Adressen führen, müssen sie nicht zwangsweise Adressen aus allen On-Link-Prefixen haben. Es kann auf einem Link IPv6-Prefixe geben, aus denen nur einige der mit dem Link verbundenen Teilnehmer Adressen nutzen.

Wirksam trennen lassen sich die Teilnehmer an einem Link durch verschiedene IPv6-Prefixe nicht: Allen gemein sind mindestens das Prefix `fe80::/64` für die obligatorischen link-lokalen Adressen sowie die Multicast-Adresse aller Nodes. Auch treten alle Teilnehmer ihren Solicited Node Multicast-Gruppen bei, die ebenfalls unabhängig von Prefixen sind.

Über die jeweilige Solicited Node Multicast-Adresse lässt sich für jede On-Link-Adresse die dazugehörige Link Layer-Adresse ausfindig machen, so dass jeder Teilnehmer prinzipiell mit allen auf seinen Links gültigen Adressen direkt kommunizieren kann, auch wenn er selbst keine Adresse aus dem jeweiligen Prefix führt. Vorausset-

zung dafür ist, dass der Teilnehmer weiß, dass das jeweilige Prefix auf einem Link gültig ist und zunächst eine direkte Zustellung versucht, anstatt sofort einen Router mit der Übermittlung zu beauftragen.

Voraussetzung für eine wechselseitige direkte Kommunikation ist ferner, dass auch die Gegenseite spiegelbildlich Kenntnis über die ihr fremden On-Link-Prefixe hat. Diese Information kann sie einerseits aus Neighbor Advertisements lernen. Andererseits können Router Advertisements Prefixe unabhängig von der automatischen Adresskonfiguration als auf dem Link gültig und somit als on-link kennzeichnen. Ein Teilnehmer kann dann eine Netzwerk-Route auf das jeweilige Interface setzen. Die Bekanntgabe von On-Link-Prefixen wird auch als *Prefix Discovery* bezeichnet.

Zudem können Router nachhelfen, indem sie mit einem *Redirect* einem Teilnehmer den Hinweis geben, dass ein anderer Teilnehmer des lokalen Netzwerkes das Paket besser zustellen kann. Wenn ein vermeintlich off-link befindliches Ziel tatsächlich on-link ist und der Absender das Paket direkt ausliefern soll, kann der Router anstatt eines anderen Routers den ursprünglichen Empfänger des Paketes als Ziel im Redirect angeben. Redirects werden in Abschnitt 3.2.6 genauer betrachtet.

Für IPv6 gibt es keinen direkten Zusammenhang zwischen den IPv6-Adressen, die ein Teilnehmer auf einem Interface führt, und den IPv6-Prefixen, die auf dem mit dem Interface verbundenen Link gültig sind. Der Umstand, dass ein Teilnehmer eine IPv6-Adresse führt, impliziert nicht, dass das Prefix, aus dem die Adresse stammt, auf dem jeweiligen Link gültig ist. Ein Teilnehmer darf unabhängig von seinen eigenen IPv6-Adressen nur jene Prefixe als on-link erachten, für die ihm diese Eigenschaft eindeutig mitgeteilt wurde. Ausgenommen davon ist lediglich das obligatorische link-lokale Prefix, das auf jedem Link gültig ist. In Router Advertisements lassen sich Prefixe deshalb explizit als On-Link-Prefixe kennzeichnen, bei der manuellen Konfiguration von IPv6-Adressen muss gegebenenfalls ausdrücklich die Länge des Prefixes angegeben oder zusätzlich eine Route für das On-Link-Prefix gesetzt werden.

Vor allem bei der manuellen Konfiguration von IPv6-Adressen ist dies ein wichtiger Unterschied zu IPv4. Ohne weitere Angabe wird bei IPv4 oft die – veraltete – Netzwerk-Klasse der Adresse herangezogen, und das entsprechend große Netzwerk als on-link konfiguriert. Obwohl einzelne IPv6-Netze praktisch immer /64-Prefixe haben, erfordert IPv6 immer die Angabe der Prefix-Länge und geht ansonsten von einer einzelnen Adresse, also einem /128-Prefix, aus.

RFC 5942 befasst sich eingehend mit dem Subnet- und On-Link-Begriff für IPv6 und konkretisiert ihn gegenüber RFC 4861.

Eine inzwischen veraltete Version der Neighbor Discovery – RFC 2461 – sah vor, dass ein Teilnehmer ohne Default-Router alle nicht durch genauere Routen erfassten IPv6-Prefixe als on-link ansieht. Diese Annahme führt unter anderem zu Problemen, wenn etwa ein IPv4-Teilnehmer ohne Anbindung an das IPv6-Internet auf einem Interface IPv6 aktiviert. Erhält er für einen DNS-Eintrag sowohl eine IPv4- als auch eine IPv6-Adresse, würde er zunächst vergeblich die direkte Zustellung

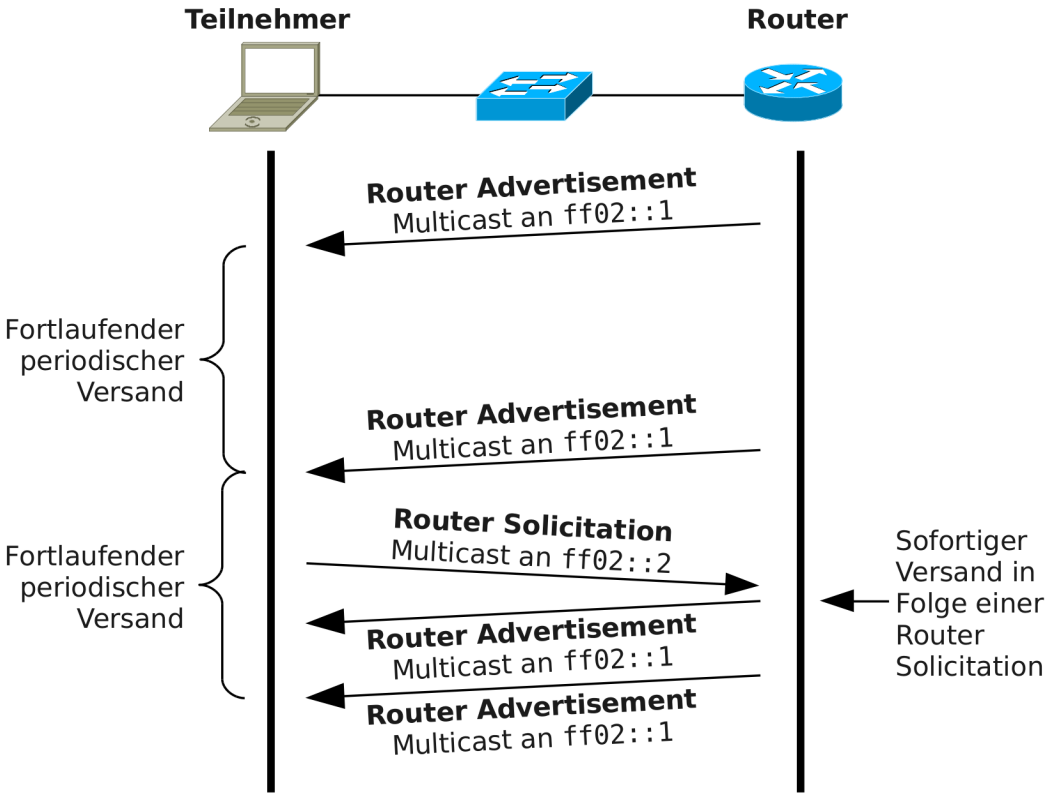


Abbildung 3.3: Nachrichtenaustausch während der automatischen Konfiguration per Stateless Address Autoconfiguration (Schematische Darstellung).

an die vermeintlich on-link befindliche IPv6-Adresse versuchen, was zu einer merklichen Verzögerung führt. RFC 4943 beschreibt diese Probleme unter dem Titel *IPv6 Neighbor Discovery On-Link Assumption Considered Harmful*. RFC 4861 enthält eine aktualisierte Fassung der Neighbor Discovery, die auf diese Vermutung verzichtet.

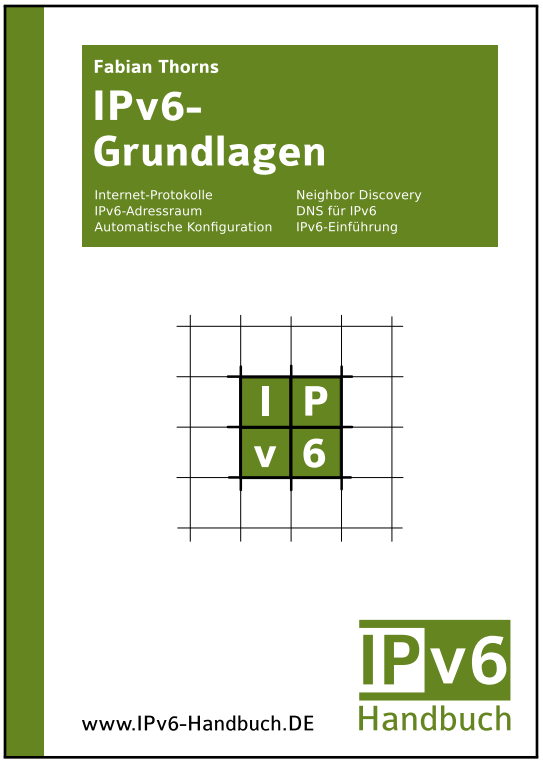
3.1.4 SLAAC – Stateless Autoconfiguration über Router Advertisements

Router Solicitations und Router Advertisements

Das grundlegende Verfahren für die automatische Konfiguration aus Router Advertisements wurde bereits zu Beginn dieses Kapitels skizziert: Die Router in einem Netzwerk versenden periodisch *Router Advertisements* an die Multicast-Adresse `ff02::1`, unter der alle Teilnehmer des Links erreichbar sind. Statt auf den nächsten periodischen Versand zu warten, kann ein Teilnehmer eine *Router Solicitation* an die Multicast-Adresse `ff02::2` senden, die alle Router an dem Link zusammenfasst. Als Reaktion auf die Solicitation sendet jeder Router sofort ein Advertisement per Multicast. Dieses Verfahren ist in RFC 4862 definiert und in Abbildung 3.3 dargestellt.

IPv6 Handbuch

Auszug / Leseprobe



Fabian Thorns

IPv6-Grundlagen

1. Auflage 2014
(Entspricht Version 20140204002 vom 4. Februar 2014)

Diese Datei ist ein Auszug aus dem E-Book *IPv6-Grundlagen* aus der Reihe *IPv6-Handbuch*. Das vollständige E-Book können Sie auf *www.IPv6-Handbuch.DE* erwerben. Dort finden Sie auch weitere Informationen über die anderen Bände dieser Reihe.