SLAAC - Stateless Address Autoconfiguration (IPv6)

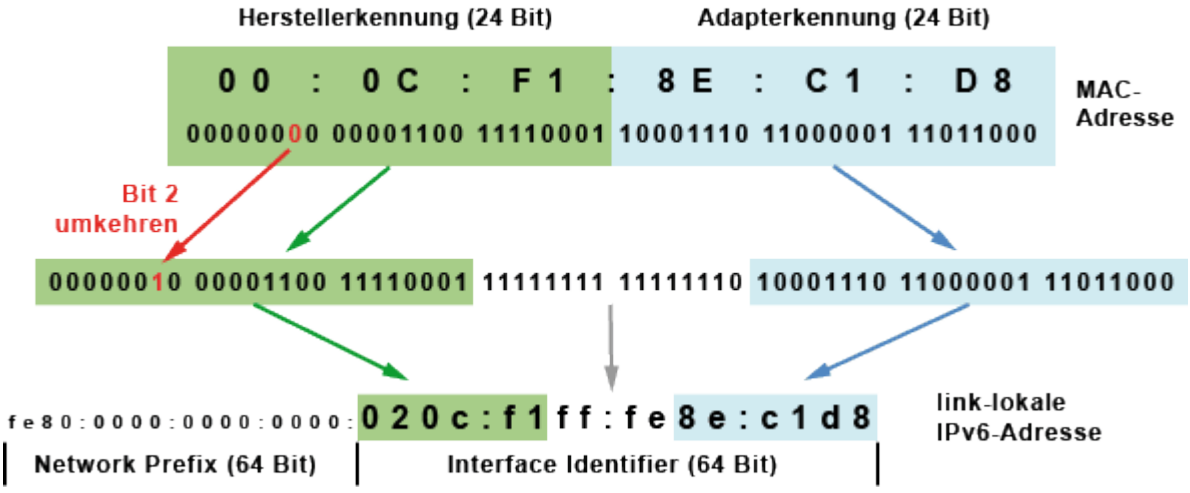
Stateless Address Autoconfiguration (SLAAC) ist ein Verfahren zur zustandslosen und automatischen Konfiguration von IPv6-Adressen an einem Netzwerk-Interface. Mit "stateless" bzw. "zustandslos" ist gemeint, dass die jeweilige IPv6-Adresse nicht zentral vergeben und gespeichert wird. Demnach erzeugt sich der Host seine IPv6-Adresse unter Zuhilfenahme zusätzlicher Informationen selbst. SLAAC ist die Weiterentwicklung von Verfahren für die klassische IP-Autokonfiguration unter IP4. Anders als bei IPv4 übernehmen IPv6-Router dabei eine aktive Rolle.

Man unterscheidet grob gesehen zwischen globalen IPv6-Adressen (Global Scope) und link-lokalen IPv6-Adressen (Local Scope). Mit der Stateless Address Autoconfiguration kann sich ein IPv6-Host sowohl eine link-lokale, als auch eine globale IPv6-Adresse erzeugen.
Damit bietet IPv6 den gleichen Komfort wie beim Betrieb eines sehr einfach gehaltenen DHCP-Servers.

Das Ziel von SLAAC ist, dass ein Host zumindest eine link-lokale IPv6-Adresse bekommt, mit der in jedem Fall eine Verbindung innerhalb des lokalen Netzwerks möglich ist. In einem weiteren Schritt würde sich ein Host per SLAAC ein globale IPv6-Adresse erzeugen, mit der er auch Verbindungen ins Internet aufbauen kann.

- Mehr Informationen über IPv6-Adressen
- Schreibweise/Notation von IPv6-Adressen
- IPv6-Address-Scopes (Gültigkeitsbereiche)

SLAAC für eine link-lokale IPv6-Adresse



Eine IPv6-Adresse besteht aus insgesamt 128 Bit. Eine link-lokale IPv6-Adresse wird aus einem Präfix (64 Bit) und einem Suffix (64 Bit) gebildet. Der Präfix für alle link-lokalen IPv6-Adressen ist immer "fe80:0000:0000:0000". Das Suffix (Interface Identifier) ist der EUI-64-Identifier oder IEEE-Identifier, der aus der MAC-Adresse (Hardware-Adresse des Netzwerkadapters) gebildet wird. In der Mitte der 48-Bit-MAC-Adresse (zwischen dem dritten und dem vierten Byte) werden mit "ff:fe" zwei feste Bytes eingefügt, damit es 64 Bit werden. Zusätzlich wird noch das zweite Bit im ersten Byte der MAC-Adresse invertiert. Das heißt, aus "1" wird "0" und aus "0" wird "1".
Warum? Als man den Adressraum für MAC-Adressen festgelegt hat, hat man vorausschauend einen Adressbereich festgelegt, den man sich selber ausdenken kann. Die also nicht zugewiesen

werden. Im zweiten Bit vom ersten Byte steckt ein Indikator drin, der diese Information enthält, ob die MAC-Adresse von der IEEE zugewiesen wurde oder ob sie selber ausgedacht ist. Wenn das Bit auf "0" ist, dann handelt es sich um eine MAC-Adresse, die von der IEEE zugewiesen wurde. Ist das Bit auf "1", dann ist es eine Phantasie-Adresse.
Wenn man sich jetzt die IPv6-Adresse bildet, dann können die Bits beliebig sein. Wenn man sich die MAC-Adresse ausgedacht hat, dann wird bei einer EUI-64 das Bit in der Regel zur "0" gedreht.

Auf diese Weise wird zum Beispiel die MAC-Adresse "00:0C:F1:8E:C1:D8" zum Interface Identifier "020c:f1ff:fe8e:c1d8". Und der Host bildet sich so die link-lokale Adresse "fe80:0000:0000:0000:020c:f1ff:fe8e:c1d8".

Bevor der Host diese link-lokale Adresse nutzen kann muss er eine Duplicate Address Detection (DAD) durchführen, um festzustellen ob die Adresse im lokalen Netz womöglich schon existiert.

DAD - Duplicate Address Detection

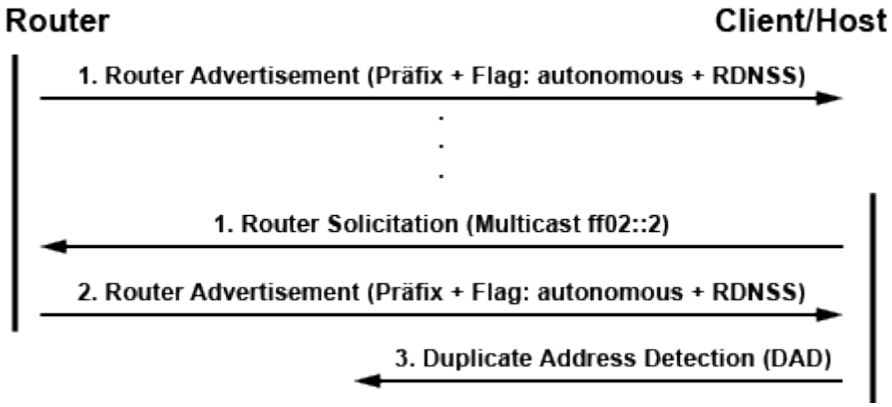
Um Adresskollisionen zu vermeiden sollte der Host bei einer neu generierten IPv6-Adresse eine Duplicate Address Detection (DAD) durchführen.

1. Neighbor Solicitation: Dazu schickt der Host eine Anfrage an die generierte Adresse ins lokale Netz. Als Antwort-Adresse dient eine Multicast-Adresse.
2. Neighbor Advertisement: Falls eine andere Station die IPv6-Adresse bereits nutzt, kommt eine Antwort zurück.

Erst wenn keine Antwort von dieser Adresse zurückkommt bindet sich das Interface an diese Adresse und kann sie für die Kommunikation nutzen.

Weil es keine Pflicht gibt eine DAD durchzuführen, sind Adresskollisionen durchaus möglich. Aufgrund des sehr großzügigen Adressraums und der weltweit eindeutigen MAC-Adressen aber eher unwahrscheinlich.
Sollte es doch einmal zu einer Kollision kommen und die IPv6-Adresse tatsächlich schon existieren, dann muss die IPv6-Adresse vom Anwender manuell geändert werden.
Dann sollte man gleich das ganze Netzwerk überprüfen. Es könnte dann sein, dass jemand eine MAC-Adresse gekapert hat und per MAC-Spoofing ins Netzwerk eingedrungen ist.

SLAAC für eine globale IPv6-Adresse (ohne Privacy Extensions)



Mit seiner link-lokalen IPv6-Adresse kann der Host nur im lokalen Netzwerk kommunizieren. Für das Internet braucht er eine zusätzliche IPv6-Adresse, die er sich ebenfalls selber generiert. Dazu muss der Host beim Standard-Gateway (nächster Router) nachfragen, was der Präfix des globalen Adressblocks ist. Dabei handelt es sich um den Adressraum, den man vom Netzzugangsprovider (ISP) zugeteilt bekommen hat. Der Präfix ist in der Regel 64 Bit lang. Diesen Präfix gibt der Router in regelmäßigen Abständen per Router Advertisement bekannt.

Sofern der Client oder Host diesen noch nicht erhalten hat, kann er den Präfix auch per Solicitation Message (Router Solicitation) anfordern. Als Antwort kommt ein oder auch mehrere Router Advertisements mit dem globalen Präfix zurück.

1. Router Solicitation (Solicitation Message): Mit seiner link-lokalen IPv6-Adresse bittet der Host auf der Multicast-Adresse "ff02::2" um den globalen Präfix (optional).
2. Router Advertisement (Advertisement Message): Der Router schickt daraufhin eine Nachricht mit dem globalen Präfix für dieses Netzwerk, der MTU (Größe der IP-Pakete) und dem Flag "autonomous".

Aus dem per Router Advertisement erhaltenen Präfix und dem Interface Identifier der link-lokalen Adresse wird dann die globale IPv6-Adresse gebildet. Danach prüft der Host, ob diese Adresse im lokalen Netzwerk schon vergeben ist (Duplicate Address Detection, DAD). Wenn sie frei ist, weist er die globale Adresse seiner Netzwerkschnittstelle zu.

SLAAC für eine globale IPv6-Adresse mit Privacy Extensions (Lösung des Datenschutz-Problems)

Der Hostanteil bzw. Interface Identifier einer per SLAAC erzeugten globalen IPv6-Adresse ist weltweit eindeutig, sofern die dafür verwendete MAC-Adresse weltweit eindeutig ist. Das bedeutet, am Interface Identifier kann man einen Host identifizieren. Unabhängig in welchem Netz (Präfix) er sich befindet. Da alle Computer und Computer-ähnlichen Geräte über eine oder mehrere Hardware-Adressen verfügen ist jeder Host über seinen Interface Identifier identifizierbar.
Da viel Hosts, zum Beispiel Smartphones und Tablets, nur von einer Person genutzt werden, sind IPv6-Adressen mit einem auf eine MAC-Adresse bezogenen Interface Identifier personenbezogene Daten. Somit wäre jeder Nutzer jederzeit identifizierbar. Mit der Einführung von IPv6 ist damit die Angst um den Verlust der Privatsphäre gestiegen.

Deshalb gibt es aus Gründen des Datenschutzes die Erweiterung "Privacy Extensions", die standardmäßig in allen IPv6-Clients aktiviert sein sollte. Statt die eindeutige MAC-Adresse für den Interface Identifier zu verwenden, generiert der Host für den Interface Identifier einen pseudozufälligen Hash-Wert.
Ein anderes Verfahren erzeugt Cryptographically Generated Addresses (CGAs). Auch CGN verhindert die Identifizierung eines Hosts anhand seiner IPv6-Adresse.

- SLAAC für eine globale IPv6-Adresse mit Privacy Extensions (RFC 4941)

Unvollständige Autokonfiguration

Leider fehlt in manchen Betriebssystemen eine vollständige Unterstützung von IPv6. Das betrifft Windows 7 und 8, sowie das veraltete Windows XP. Auch ältere Linux-Distributionen und mobile Betriebssysteme sind nur eingeschränkt IPv6-tauglich.

- Weitere Details zur IPv6-Fähigkeit und -Autokonfiguration

SLAAC bei Servern und Routern

Jeder IPv6-Client richtet automatisch eine eigene link-lokale und globale IPv6-Adressen ein. Für die meisten Endgeräte ist das eine praktische Lösung. Doch bei einem Server oder Router sollten sich die IP-Adressen nicht ändern. Insbesondere dann nicht, wenn dem Server per DNS ein Host- oder Domain-Name zugeordnet ist. Und fürs IP-Routing muss ein Router zwangsläufig eine feste IP-Adresse haben. Hier sollte man die IPv6-Adresse manuell zuweisen oder zentral per DHCPv6 eine statische IP-Adresse vergeben.
Bei Servern empfiehlt es sich daher, die Autokonfiguration (SLAAC) zu deaktivieren bzw.

serverseitig zu ignorieren und eine statische IPv6-Adressen nach dem Zufallsprinzip zu erzeugen und nicht durchnummeriert vergeben.

SLAAC: NDP und ICMPv6

Die gesamte Kommunikation von SLAAC basiert auf den Protokollen NDP und ICMPv6.

- NDP - Neighbour Discovery Protocol
- ICMPv6 - Internet Control Message Protocol Version 6

Aufgaben und Übungen mit dem Raspberry Pi

Wer mit IPv6 experimentieren will, der kann das zum Beispiel auf einem Raspberry Pi tun. Dazu gibt es ein paar Aufgaben und Übungen speziell für IPv6.

- IPv6 auf dem Raspberry Pi einschalten und konfigurieren
- IPv6 Privacy Extensions im Raspberry Pi aktivieren
- Feste IPv6-Adresse für den Raspberry Pi einrichten
- IPv6-Tunnel für SixXS mit aiccu einrichten (Raspberry Pi)
- IPv6-Firewall für einen IPv6-Tunnel einrichten (Raspberry Pi)
- IPv6-Gateway einrichten (Raspberry Pi)

Übersicht: IPv6

- IPv6 - Internet Protocol Version 6
- IPv6-Adressen
- Schreibweise/Notation von IPv6-Adressen
- IPv6-Autokonfiguration
- IPv6-Multihoming und -Renumbering

Weitere verwandte Themen:

- TCP/IP
- IPv4 - Internet Protocol Version 4
- DHCPv6 (Stateful Address Autoconfiguration)
- DNS - Domain Name System