

Universität Osnabrück

SEMINARARBEIT

zum Seminar

IT-Sicherheit

im Sommersemester 2013

Thema:

IPv6 Privacy Extensions

Erstellt am 10.05.2013

Vorgelegt von:

Kevin Seidel
943147
Falkenstraße 43
49124 Georgsmarienhütte

Inhaltsverzeichnis

1	Einleitung	1
2	Das Internet Protocol Version 6	2
2.1	Warum IPv6?	2
2.2	Aufbau einer IPv6-Adresse	2
2.3	Vergabe von IPv6-Adressen	3
3	Stateless Address Autoconfiguration	3
3.1	Funktionsweise der Stateless Address Autoconfiguration	4
3.2	Probleme von Stateless Address Autoconfiguration	5
4	Fazit	5
5	Quellen	6

1 Einleitung

Diese Arbeit beschäftigt sich mit dem Nutzen und der Funktionsweise der Privacy Extensions im Internet Protocol Version 6.

2 Das Internet Protocol Version 6

2.1 Warum IPv6?

Durch den starken Anstieg von Netzwerkgeräten in den vergangenen Jahren, ist es nötig geworden, einen größeren Adressraum zu schaffen. Das Internet Protocol (IP) Version 4 stellt, aufgrund der Adressgröße von 32 Bits, nur einen Adressraum von 2^{32} Adressen zur Verfügung, was in etwa 4,3Mrd. Adressen entspricht. Da diese jedoch mittlerweile alle vergeben sind, ist es notwendig geworden einen größeren Adressraum zu schaffen.

IP Version 6 setzt deshalb auf eine Adresslänge von 128 Bits, wodurch sich der Adressraum enorm vergrößert (etwa $3.4 \cdot 10^{38}$ Adressen).

Eine weitere Veränderung von IP Version 6 (IPv6) gegenüber IP Version 4 (IPv4) ist ein Header mit festgelegter Größe, welcher die zwingend notwendigen Informationen enthält. Für zusätzliche Informationen gibt es einen Extension Header, welcher jedoch nur bei Bedarf genutzt wird.

2.2 Aufbau einer IPv6-Adresse

Die IPv6-Adresse unterscheiden sich deutlich von den bisher verwendeten IPv4-Adressen. IPv4-Adressen haben eine Größe von 32 Bits und werden meist in der "dotted decimal notation", das heißt in vier Blöcken von Dezimalzahlen zwischen 0 und 255, welche durch einen Punkt separiert werden, dargestellt. Dadurch lassen sich 2^{32} (ca. 4,3 Mrd.) verschiedene Adressen darstellen. Durch die Verwendung von IPv6-Adressen erhöht sich die Anzahl der Adressen drastisch, da man hier eine Adresslänge von 128 Bits verwendet, womit die Größe des Adressraumes auf 2^{128} angehoben wird. Da eine Darstellung dieser Adressen in "dotted decimal notation" aus 16 Blöcken bestehen würde und damit sehr schwer zu lesen wäre, entschloss man sich dazu die IPv6-Adressen in 8 Blöcken zu je 4 Hexadezimalziffern zusammenzufassen. Diese Blöcke werden, durch einen Doppelpunkt getrennt, notiert.

2001 : 0db8 : 1aAa : 0000 : CCcc : 0000 : 0000 : 0D01

Abbildung 1: Beispiel einer IPv6-Adresse.

Da diese Adressen im Vergleich zu IPv4-Adressen immernoch relativ lang und unübersichtlich sind, gibt es mehrere Möglichkeiten eine IPv6-Adresse zu verkürzen. So wird in [RFC 4291] vereinbart, dass man ein oder mehrere aufeinanderfolgende Blöcke, welche nur Nullen beinhalten durch "::" verkürzen kann. Dies jedoch nur einmal pro Adresse. Ausserdem ist es möglich auf führende Nullen innerhalb eines Blockes zu verzichten.

In [RFC 5952] wird eine Empfehlung für eine etwas striktere Darstellung von IPv6-Adressen gemacht. So ist es dort vorgeschrieben innerhalb von Adressen nur Kleinbuchstaben zu verwenden. Dies dient der besseren Lesbarkeit und verhindert eine versehentliche Verwechslung von 8 und B sowie 0 und D, die bei gemischter Groß- und Kleinschreibung oder durchgängiger Großschreibung entstehen könnte.

Des Weiteren müssen führende Null innerhalb eines Blockes ausgelassen werden und Blöcke, welche nur aus Nullen bestehen durch eine einzelne Null repräsentiert werden.

Ausserdem ist es nun nicht mehr erlaubt einzelne Null-Felder durch "::" zu repräsentieren. Diese Schreibweise ist nurnoch auf mehrere aufeinanderfolgende Null-Felder anwendbar und muss in dem Fall auch genutzt werden. Gibt es mehrer Möglichkeiten Felder

durch ":" zu verkürzen, muss das mit dem größten Nutzen, das heißt mit den meisten aufeinanderfolgenden Nullen, gewählt werden. Gibt es mehrere gleichgroße Möglichkeiten, ist die erste zu wählen.

2001 : db8 : 1aaa : 0 : cccc :: d01

Abbildung 2: Beispieladresse aus Abb. 1 unter Berücksichtigung der Empfehlung

Durch die Befolgung dieser Regeln zu Darstellung von IPv6-Adressen in Textform hat sich die Lesbarkeit stark verbessert.

Die Netzmasken werden bei IPv6 durch Suffixe dargestellt, das heißt die Anzahl der Einsbits in der Netzmaske wird, abgetrennt durch einen Schrägstrich, hinten an die Adresse angehängen.

2001 : db8 : 1aaa : 0 : cccc :: d01/64

Abbildung 3: Beispieladresse aus Abb. 2 mit Netzmaske

Durch diese Netzmaske wird angegeben, welcher Teil der Adresse das Netzwerk identifiziert und welcher Teil das Interface repräsentiert. Der vordere Teil der Adresse, auch Präfix genannt, dient dabei zur Bestimmung des Netzes. Der hintere Teil, Interface Identifier genannt, dient zur Identifizierung eines Gerätes im Netz. Beim Beispiel in Abbildung 3 wäre der Präfix 2001:db8:1aaa:0::/64 und der Interface Identifier ::cccc:0:0:d01/64.

2.3 Vergabe von IPv6-Adressen

Bei der Vergabe von IPv6-Adressen in einem Netzwerk gibt es mehrere Vorgehensweisen. Zum einen die manuelle Vergabe von Adressen, was in kleinen Netzen schnell und einfach funktioniert, bei größeren Netzen jedoch einen enormen Aufwand bedeutet. Eine Alternative für größere Netze wäre die Verwendung des Dynamic Host Configuration Protocols (DHCP), welche schon für IPv4 existiert. Für IPv6 gibt es eine angepasste Version mit dem Namen DHCPv6, welches, identisch zum klassischen DHCP, dynamisch Adressen an im Netzwerk befindliche Interfaces verteilt und die Adressen auf dem DHCP-Server speichert. Durch die Speicherung der Adressen handelt es sich um eine Stateful Address Configuration im Gegensatz zur letzten Möglichkeit, der Stateless Address Autoconfiguration. Diese erzeugt IPv6-Adressen direkt auf dem Gerät, welches diese später verwendet. Die Funktionsweise wird im Folgenden näher erörtert.

3 Stateless Address Autoconfiguration

Die Stateless Address Autoconfiguration(SLAAC) ist ein Verfahren zur eigenständigen Erzeugung von IP-Adressen von Netzwerkgeräten. Dies ermöglicht eine einfache und konfigurationslose Einrichtung von Netzwerken, da zum Beispiel auf manuelle Adressvergabe oder den Einsatz von Dynamic Host Configuration Protocol(DHCP)-Servern verzichtet werden kann. Selbst bei mehreren verbundenen Netzwerken ist ein DHCP-Server nicht nötig, da mittels Router Advertisement die einzelnen Adressen für die Subnetze vergeben werden können.

3.1 Funktionsweise der Stateless Address Autoconfiguration

Für die Erzeugung einer globalen IPv6-Adresse sind mehrere Schritte nötig, welche im folgenden genauer erörtert werden. Der Autokonfigurationsprozess wird mit der Aktivierung des Netzwerkgerätes gestartet. Dazu wird zuerst eine link-local Adresse erstellt. Diese erlaubt grundlegende Kommunikation im Netzwerk. Sie setzt sich aus einem festgelegtem Präfix (fe80::/64) und dem gerätespezifischen Interface Identifier zusammen. Die Interface Identifier wird in der Regel aus der Media Access Control(MAC)-Adresse des Netzwerkgerätes gebildet. Um diese 48 Bits lange MAC-Adresse auf die für den Interface Identifier vorgesehene Länge von 64 Bits zu bringen, wird die MAC-Adresse in der Mitte geteilt und dort wird der Wert "FF:FE" eingesetzt. Ausserdem wird das siebte Bit von links invertiert, welche angibt, ob die MAC-Adresse global oder lokal administriert wird.

Bevor diese vorläufige Adresse, egal ob manuell zugewiesen oder durch DHCP oder SLAAC, an ein Interface gebunden wird, muss deren Eindeutigkeit im Netzwerk überprüft werden. Dies geschieht mittels Duplicate Address Detection. Einzige Ausnahmen eine Duplicate Address Detection sind Anycast Adressen oder explizite Deaktivierung des Vorgangs. Zur Überprüfung der Eindeutigkeit von Adresse werden sogenannte Neighbor Solicitations und Neighbor Advertisements verwendet. Neighbor Solicitations haben als Empfänger unsere generierte vorläufige Adresse und als Sender die nicht spezifizierte Adresse. Um eine Antwort auf diese Nachricht zu erhalten ist es noch nötig, dass das Interface zunächst dem all-nodes Multicast, welcher einem Broadcast in IPv4 entspricht und an alle angebundenen Adressen verschickt, und dem solicited-node Multicast, welcher speziell für die Duplicate Address Detection zuständig ist, beitreten. Falls nun schon ein Interface diese vorläufige Adresse besitzt, erhält es die Neighbor Solicitation und antwortet mit einem Neighbor Advertisement. Unser Interface empfängt dieses Neighbor Advertisement, wodurch es weiß, dass die vorläufige Adresse nicht eindeutig ist und damit nicht an das Gerät gebunden werden kann.

Falls das Interface während der Duplicate Address Detection eine Neighbor Solicitation von einem anderen Gerät erhält, versuchen zwei Geräte gleichzeitig die gleiche Adresse zu verwenden. In diesem Fall sollte keines der Geräte seine vorläufige Adresse an das Gerät binden. Es kann jedoch auch vorkommen, dass die Neighbor Solicitation von unserem Gerät kommt, falls der Multicast die Pakete auch an den Sender zurückschickt.

Wenn die Duplicate Address Detection fehlschlägt und unser Interface Identifier aus der Hardware-Adresse gebildet wurde, sollten alle IP Operationen eingestellt werden.

Nachdem die link-local Adresse gebildet wurde, ist es nun möglich eine globale Adresse zu generieren. Dies geht jedoch nur, falls sich ein Router im Netzwerk befindet, da hierfür sogenannte Router Advertisements nötig sind. Die Router Advertisements enthalten Informationen über das Netzwerk, wie zum Beispiel den zu verwendenden Präfix. Sie werden

vom Router automatisch in periodischen Abständen geschickt, können jedoch auch durch Router Solicitation angefragt werden.

Ein Gerät sendet also zuerst eine Router Solicitation und wartet auf ein Router Advertisement als Antwort. Nach einem vorgegebenen Zeitraum ohne Antwort wird dies noch einmal ausgeführt. Dies geschieht so lange bis ein Router antwortet oder die vorgegebene Maximalanzahl von Anfragen erreicht ist. Antwortet der Router, wird aus dem in dem Router Advertisement enthaltenen Präfix und dem vom Gerät vorher gebildeten Interface Identifier eine globale Adresse gebildet.

3.2 Probleme von Stateless Address Autoconfiguration

Durch die Erzeugung des Interface Identifiers aus der MAC-Adresse ist dieser eindeutig und statisch. Das führt dazu, dass man ihn sehr einfach zurückverfolgen kann.

4 Fazit

5 Quellen

RFC 5952 RFC 3513 RFC 4941 RFC 4291 <https://supportforums.cisco.com/docs/DOC-24485>

Literatur

[RFC 4291] R. Hinden and S. Deering, *IP Version 6 Addressing Architecture*, RFC 4291 (Draft Standard), February 2006, Updated by RFCs 5952, 6052.

[RFC 4862] S. Thomson and T. Narten and T. Jinmei, *IPv6 Stateless Address Autoconfiguration*, RFC 4862 (Draft Standard), September 2007.

[RFC 5952] S. Kawamura and M. Kawashima, *A Recommendation for IPv6 Address Text Representation*, RFC 5952 (Proposed Standard), August 2010.