BWCAMPUSNETZ

Zukunftsfähige Konzepte für die Campusnetze
an Universitäten und Hochschulen

Zuordnung MAC- zu IP-Adressen in IPv6-Netzen

Inhalt

1 Motivation

In IPv6-Netzen erfolgt die Zuweisung von IPv6-Adressen generell nicht zentral, sondern über verschiedene Methoden auf dem Client. Dies bringt mit sich, dass in eine Zuordnung von IPv6-Adresse zu MAC-Adresse nicht an zentraler Stelle erfolgen kann, sondern dass mehr Informationen benötigt werden. Auch bei Stateful Verfahren ist die Zuordenbarkeit unter Umständen nicht gegeben. Deswegen müssen mehr Informationen aus verschiedenen Quellen im Netzwerk korelliert werden, um jeder IPv6-Adresse eine MAC-Adresse zuordnen zu können.

2 Adressierungsverfahren in IPv6

Grundsätzlich können in IPv6-Netzen verschiedene Verfahren zur Adressierung von Clients zum Einsatz kommen. Diese können grob in Stateless und Stateful Verfahren unterschieden werden. Zu den Stateless Verfahren zählt man all jene Verfahren, in denen der Client selbstständig eine Adresse generiert, während bei einem Stateful Verfahren eine Vergabestelle involviert ist. Die Art der Adressierung wird über Flags im Router-Advertisment fest gelegt.

2.1 Stateless Verfahren

Bei der Stateless Adressierung ist im Router-Advertisment für das jeweilige Präfix das Flag „autonomous address configuration“ gesetzt. Dies signalisiert einem Client, dass eine Adresse selbstständig gneriert werden darf. Das Verfahren der selbständigen Adresskonfiguration wird generell SLAAC, bzw. Stateless Address Autoconfiguration genannt.[1] Hierzu gibt es zwei Verfahren:

Bei **EUI-64** generiert ein Client durch ein spezielles Verfahren eine IPv6-Adresse aus seiner MAC-Adresse. Dadurch wird gewährleistet, dass die IPv6-Adresse auf jeden Fall eindeutig ist, sofern es keine Kollisionen bei den Hardware-Adressen gibt. Jedoch hat dieses Verfahren den entscheidenden Nachteil, dass ein Client unabhängig vom Netz, in dem er sich momentan befindet, verfolgbar ist, da seine MAC-Adresse idealerweise weltweit eindeutig ist. Diese Methode wird sowohl bei Link-Locale Adressen sowie vereinzelt noch für Global Unicast Adressen verwendet. Diese Adressen können auch vom Administrator eines Netzsegments wieder ein eine MAC-Adresse umgerechnet werden.

Um die Problematik der Identifizierbarkeit zu Umgehen wurden verschiedene weitere Methoden spezifiziert, eine IPv6-Adresse zu generieren. Zu nennen sind hier vor allem die **Privacy-Extensions**:[2] Zusätzlich zu einer EUI64-Adresse generieren Clients weitere randomisierte Adressen, die sie dann präferriert für den Datenverkehr benutzen. Die Eindeutigkeit dieser Adressen wird dabei über den Mechanismus der „Duplicate Address Detection“ geprüft.

Hier lässt sich vom Administrator nicht alleinig aufgrund der Kenntnis der IPv6-Adresse feststellen, welche MAC-Adresse zu Grunde lag.

2.2 Stateful Verfahren

Bei der Stateful Adressierung wird im Router-Advertisent das `managed` flag gesetzt. Dies sorgt beim Client dafür, dass dieser versucht, mittels Solicit Message einen zuständigen DHCPv6-Server [3] zu kontaktieren. DHCPv6 vergibt Adressen generell nicht aufgrund einer MAC-Adresse, sondern aufgrund eines DHCP Unique Identifiers (DUID). Diese DUID kann auf mehrere Arten synthetisiert werden: Zum einen gibt es Verfahren, die die MAC-Adresse eines Interfaces in die DUID kodieren (LL, LL+T), zum anderen gibt es auch Verfahren, die einen kompletten Unique String aus weiteren Hardware-Intentifiers generieren. Darüber hinaus ist nicht garantiert, dass bei den Typen `LL` oder `LL+T` tatsächlich diejenige Linklayer Adresse, also MAC-Adresse, des Interfaces verwendet wurde, von dem die Nachricht ausgingt. Somit ist hier keine eindeutige Zuordenbarkeit einer IPv6 Adresse zu einer MAC-Adresse gegeben.

Zusätzlich kann ein DHCPv6-Server eine Adresse alleinig basierend auf der MAC-Adresse eines Clients vergeben, sofern entweder der DHCPv6-Server im gleichen Netzsegment wie der Client sitzt, oder an einem DHCPv6-Relay die Option79[4] verwendet wird, um die MAC-Adresse zu übertragen. Hier ist dann eine eindeutige Zuordnung gegeben.

Verkompliziert wird die Zuordenbarkeit aber auch in diesem Szenario dadurch, dass zusätzlich zu DHCPv6 (also dem `managed` flag), auch das `autonomous` Flag aktiv sein kann, um bspw. Privacy Extensions zu ermöglichen. Dann kann ein Client zusätzlich zur per DHCPv6 zugewiesenen Adresse weitere Adressen generieren. Bei diesen ist die Zuordenbarkeit dann wieder nicht gegeben.

3 Datenquellen

Grundsätzlich werden Daten aus den Layern 2 und 3 benötigt, um eine Zuordnung zu gewährleisten. Hier kommen vor allem die Neighbor-Tables (NDB) von beteiligten Routern sowie die Forwarding-Tables (FDB) von beteiligten Switches in Frage. Zusätzlich können auch die Informationen aus der Lease-Datenbank eines DHCPv6-Server hinzu gezogen werden. An dieser Stelle sei darauf hingewiesen, dass NDBs und FDBs bereits ausreichend sind. Zur Erhebung der Daten muss zwischen Pull-Verfahren und Streamin-Verfahren unterschieden werden. Bei einem Pull, bzw. der Abholung von Daten von einem Gerät, wir der Transfer von einer dritten Instanz von außen her initiiert. Dieses Verfahren kann leicht über bekannte Kommunikationsprotokolle realisiert werden. Beispielweise können Daten mittels SSH Command Exection, SNMP oder REST-APIs eingesammelt werden. Jedoch können bei diesem Verfahren, je nach Situation, Datenpunkte verloren gehen. Es empfielt sich sehr, ein Pull-Intervall zu wählen, dass sicher stellt, dass Einträge auch wirklich in die Datenbasis übernommen werden. Mindestens muss ein Abruf mit einer Frequenz kleiner oder gleich des halben aging-intervalls statt finden. Selbst dann ist jedoch nicht sicher gestellt, dass alle Datensätze erfasst werden können. Netzwerkereignisse (bspw. Topology Change Notifications) können einen vorzeitigen Flush von FDBs bewirken.

Den Pull-Verfahren stehen die Streaming-Verfahren gegenüber, bei denen ein kontinuierlicher Datenstrom vom zu überwachenden Gerät aus zu einem Collector besteht. Bei Änderungen in der Forwarding- oder Arp-Tabelle, wird sofort ein Update versandt. So werden alle Datenpunkte sicher erfasst. Als Beispiel ist hier Streaming Telemetry zu nennen. Setzt man eine Lösung auf Basis von EVPN/VXLAN ein, so kann aus den BGP-Updates auch jederzeit ein vollständiges Bild aller Information extrahiert werden.

Nachdem die notwendigen Informationen gesammelt wurden, müssen diese zeitlich korreliert werden. Zieht man die FDBs hinzu, so kann - als Nebeneffekt - auch zu jeder IPv6/Mac-Komination auch der jeweilige Switchport ermittelt werden.

4 Fallstudien

Im folgenden werden verschiedene Fallstudien präsentiert. Dazu wird das Netzdesign kurz erläutert, sowie Verfahren zur Verarbeitung der notwenigen Daten. Diese Fallstudien basieren jeweils auf der Lösung einzelner Institutionen und präsentieren kurz die eingesetzten Technologien zum Sammeln uns auswerten der Informationen.

4.1 Fall 1: Collapsed Backbone mit Firewalls

Im Falle eines collapsed Backbones sind nur wenige Geräte am Routing beteiligt. Dies hat den Vorteil, dass die entscheidenden Informationen zur IPv6/Mac-Zuordnung nur auf wenigen Geräten gesammelt werden muss. Zusätzlich sind einzelne Netzbereiche noch durch Firewalls, auf denen jeweils Netze terminieren, abgetrennt. Neighbor-Tables können hier auf den zentralen Routern sowie Firewalls abgerufen werden. Beispielsweise können Cisco-Geräte mit dem Befehl `sh ipv6 neigh vlan xxx` den Inhalt ihrer Neighbor-Table ausgeben. Beispielhaft sieht der Output aus wie folgt:

```
star# sh ipv6 neighbor vlan 2

Flags: # - Adjacencies Throttled for Glean
       G - Adjacencies of vPC peer with G/W bit
       R - Adjacencies learnt remotely
       CP - Added via L2RIB, Control plane Adjacencies
       PS - Added via L2RIB, Peer Sync
       RO - Re-Originated Peer Sync Entry
       CC - Consistency check pending

IPv6 Adjacency Table for VRF default
Total number of entries: 26
Address         Age       MAC Address     Pref Source     Interface       Flags
XXXX::3
```

```
                00:11:59  2c4f.YYYY.ffff  50   icmpv6     Vlan2
XXXX::15
                   2d20h  d401.YYYY.b737  50   icmpv6     Vlan2
XXXX::23
                    8w6d  0019.YYYY.a74a  50   icmpv6     Vlan2
XXXX::29
                00:19:49  0019.YYYY.5aa4  50   icmpv6     Vlan2
XXXX::58
                    3w0d  901b.YYYY.7709  50   icmpv6     Vlan2
XXXX::85
                    2w3d  00d2.YYYY.f073  50   icmpv6     Vlan2
```

Die Ausgabe wurde pseudonymisiert. Hier sind schon alle Informationen enhalten, die benötigt werden. Diese können per SSH Command-Execution abgeholt und geparst werden. Das gleiche Verfahren kann auf jedem Router verwendet werden.

Zusätzlich, um Geräte zuverlässig im Netzwerk verorten zu können, können die Forwarding-Tables der beteiligten Switches ausgelesen werden. Verschiedene Hersteller bieten die Option, die Informationen über eigene MIBs per SNMP abzufragen. Hierzu kann eigenes Tooling entwickelt werden. Die Universität Ulm benutzt hierfür Mixin-Klassen, zu finden unter [5] [6]

Werden nun die Einträge aus der Neighbor-Tables sowie die Einträge aus den Forwarding-Tables zeitlich korelliert, kann eine Datenbank erstellt werden, die enhält, welche IPv6-Adresse wann von welcher MAC-Adresse verwendet wurd und an welchem Switchport diese zuletzt gesehen wurde. Auch sieht man MAC-Adressen, die noch nie eine IPv6-Adresse hatten.

Nachteil des Verfahrens ist, dass man nur Zuordnungen von Client vornehmen kann, die tatsächlich schonmal mit einer ihnen konfigurierten Adresse kommuniziert haben. Sollten bspw. Privacy-Extensions Adressen konfiguriert sein die der Client aber nur in der lokalen Kommunkation, nicht aber in der Kommunikation mit dem Router nutzt, so taucht diese Adresse auch nie in der Neighbor-Table auf.

4.2 Fall 2: Layer 2 zentrisches Netz mit verteiltem Routing

Die Architektur ähnelt der Collapsed Backbone Architektur aus Fall 1. Das Netzwerk besteht größten Teils aus Layer 2 Komponenten und Vlans. Einzelne Subnetze terminieren entweder auf Firewalls (Cisco ASA, Palo Alto) oder auf Core Routern (Cisco Nexus). Somit sind alle relevanten Informationen für die MAC-IP-Zuordnung auf Firewalls und Core Router verteilt und weniger zentral wie im ersten Fall. Das Auslesen der ARP-/ND-Caches auf den Layer 3 Geräten erfolgt mitels Ansible Playbook und Cron-Jobs die dieses ausführen. Ansible ermöglicht hierbei eine Abstraktion der Abfragemethode und stellt eine vordefinierte Pipeline zur Aufbereitung der Daten zur Verfügung. So werden in diesem Beispiel die gesammelten Zurodnungen in eine Influx-Datenbank geschrieben. Die Daten werden je nach Vendor verschieden abgefragt: Für **Cisco Nexus** wird die Abfrage mit CLI-aufruf im JSON-format von den verschiedenen Geräten geholt. Die Palo Alto Firewalls werden über ihre API abgefragt. Jedoch liefern Palo Alto hier nur Daten im XML-format, die erst durch ein eigens geschriebenes Ansible-Modul geparst werden müssen. Das Vorgehen ist fpr IPv4 und IPv6 jeweils analog. Nachteil des Verfahrens ist die relativ lange Ausführzeit von Ansible. Das führt dazu, dass keine zu kurzen Abfrageintervalle gewählt werden dürfen, da sich ansonsten die Jobs überschniden und zu Lestungsproblemen führen. Grundsätzlich wäre denkbar das Prinzip ohne Ansible Framework umzusetzen eventuell mittels NAPALM in Python.

4.3 Fall 3: EVPN-Fabric mit Anycast Gateway

Im EVPN-Standard sind die MAC-IP-Zuordnungen bereits im Protokoll enthalten. Insbesondere wenn für alle Netzsegmente das Gateway auf Routern der EVPN-Fabric konfiguriert sind, wie es beispielsweise am KIT realisiert ist, können die MAC-IP-Zurodnungen augelesen werden. Hierzu muss eine BGP-Verbindung zur EVPN-Fabric aufgebaut und die BGP EVPN-Route-Type 2 Announcement protokolliert werden. Da nur Änderungen, aber dafür alle, gestreamt werden, erfolgt das einsammeln der MAC-IP-Daten so sehr effizient und insbesondere auch zeitnah.

Die bringt den Vorteil gegenüber Fall 1 und 2, dass Updates garantiert ankommen, was bei periodischem Abfragen nicht der Fall ist. Zudem funktioniert diese Lösung herstellübergreifend und es ist nur eine Implementierung notwendig. Eine Einschränkung gegenüber Fall 1

und 2 ist, dass nur die MAC-IP-Adress-Zuordnungen von Global-Unicast-Addresses (GUA) gelernt werden. Link-local-Adressen bleiben unberücksichtigt.

Kürzlich wurde am KIT eine Bachelorarbeit verfasst, die sich mit einer Softwarearchitektur befasst, mit der genau dies realisiert werden könnte.[7] In einer Masterarbeit wurden die MAC-IP-Zuordnung aus dem EVPN-Protokoll genutzt, um ein Dual-Stack-Captive-Portal zu implementieren, bei dem alle IP-Adressen eines Endgeräts in der Firewall freigeschaltet werden.[8]

5 Fazit

Auch in Netzen mit stateless Konfiguration kann die Zuordnung von Mac zu IPv6-Adressen erfolgen. Dazu müssen allerdings in aller Regel Informationen aus dem Netzwerklayer verfügbar sein. Allein aufgrund der Informationen, die ein DHCPv6-Server vorhält, ist diese Zuordnung nicht möglich. Allerdings haben die Verfahren auch ihre Schwächen, die nicht unbedingt zu umgehen sind. So können nur Adressen in Neighbor-Tables auftauchen, die tatsächlich nicht nur für die lokale Kommunikation genutzt werden.

Literaturverzeichnis

[1] *IPv6 Stateless Address Autoconfiguration*, Sep. 2007. Adresse: `https://datatracker.ietf.org/doc/html/rfc4862`.

[2] *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, Sep. 2007. Adresse: `https://datatracker.ietf.org/doc/html/rfc4941`.

[3] *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, Nov. 2018. Adresse: `https://datatracker.ietf.org/doc/html/rfc8415`.

[4] *Client Link-Layer Address Option in DHCPv6*, Mai 2013. Adresse: `https://datatracker.ietf.org/doc/html/rfc6939`.

[5] Adresse: `https://metacpan.org/dist/Net-SNMP-Mixin-NXOSDot1qFdb`.

[6] Adresse: `https://metacpan.org/pod/Net::SNMP::Mixin::Dot1qFdb`.

[7] Gregor Czubayko, *Softwarearchitektur zur Aufzeichnung von MAC/IP-Adresszuordnungen mithilfe von EVPN/VXLAN unter Berücksichtigung von Datenschutz- und Datensicherheitsaspekten*, Bachlorarbeit, 2025.

[8] Benedikt Neuffer, *Moderner Ansatz für ein IPv6-fähiges Captive Portal in einer EVPN-Umgebung*, Masterarbeit, 2019.