SEMINARARBEIT

in der Fachrichtung
Wirtschaftsingenieurwesen
SoSe 2018

Thema

Was ist die MAC-Adresse eines Gerätes, wozu dient sie und wie kann man sie verschleiern?

Eingereicht von: Ersem Yildiz
Wing102745

Betreuer: Prof. Dr. Michael Anders

Inhaltsverzeichnis

1. Vorwort

Viele Menschen sorgen sich um ihre Privatsphäre, seitdem Whistleblower Edward Snowden offengelegt hat, wie Geheimdienste nicht nur verfeindeten, sondern auch ihre eigene Bevölkerung oder die verbündeten Länder überwachen und ausspionieren. Seit dieser Erkenntnis versuchen immer mehr Menschen, die ihre Privatsphäre schützen möchten, anonym im World Wide Web zu sein und Produktdienstleistungen zu meiden, die bezüglich Themen wie Datenschutz einen schlechten Ruf genießen.
In unserer heutigen Zeit hat so ziemlich jeder Mensch ein Smartphone, mit dem er/sie mit der ganzen Welt kommunizieren kann. Für die Kommunikation wird häufig Wi-Fi verwendet, welches man heutzutage generell überall (auch gratis) finden kann: sei es bei sich zuhause, in Geschäften, in Bussen, an Bahnhöfen und noch vielen anderen Orten. Für die Verbindung mit einem Wi-Fi Access Point wird eine MAC-Adresse des Endgerätes benötigt, welches das Gerät identifiziert.
Diese Identifizierung beherbergt jedoch nicht nur die Kommunikation mit der ganzen Welt, sondern auch die Nachverfolgung des Gerätes und somit die Person selber.

Im Folgenden werde ich deshalb nun erklären, was eine MAC-Adresse ist, wie sie aufgebaut ist, wieso sie gebraucht bzw. benutzt wird, wie Behörden und Unternehmen anhand dessen die Bewegungen der Bevölkerung herausfinden können und zu guter Letzt, wie man diese verschleiern kann um sich davor zu schützen.

2. Was ist eine MAC-Adresse?

Eine MAC-Adresse, was als Abkürzung für Media Access Control Adresse steht (nicht zu verwechseln mit dem macOS Betriebssystem oder den MacBook Geräten von Apple), ist eine Hardware-Adresse jedes Netzwerkadapters, dass eine eindeutige Identifikation eines Rechnernetzes liefert. Die MAC-Adresse wird auch als physische Adresse oder Geräteadresse bezeichnet.
Die IEEE 802 MAC-Adresse stammt originell von der *Xerox Ethernet* Adressschema.
Bei Konzernen wie Apple wird diese auch als *Ethernet-ID*, *Airport-ID* oder *Wi-Fi-Adresse* genannt, bei Microsoft geht die MAC-Adresse als *Physikalische Adresse* durch.
Die MAC-Adresse dient als Kommunikationswerkzeug zwischen dem Gerät und der *Data Link Layer*. Dieser **Data Link Layer** ist die zweite Schicht von 7 Schichten des OSI-Modells.
Meistens werden die Adressen von den Herstellern der Netzwerkkarten mit ihren OUI's (hierzu später mehr) zugewiesen

2.1 Erwerb einer MAC-Adresse

Unternehmen können MAC-Adressen bei der IEEE erwerben, die es in drei verschiedenen Größen gibt: MA-L, MA-M und MA-S Blöcke. L-Blöcke bieten hierbei die größte Anzahl an möglichen Adressen (2^{24}), M-Blöcke eine Möglichkeit von 2^{20} und S-Blöcke 2^{12}.
Die MAC-Adressen kann man entweder als öffentliche oder private Adressen erwerben. Öffentliche Adressen werden auf der Internetseite der IEEE veröffentlicht, sodass man die

Herstellerkennung der Adressen von den Unternehmen einsehen kann. Private Adressen werden hingegen nicht öffentlich kenntlich gemacht.
Die Preise variieren je nach Blöcken, von $705 bis $2.820 für öffentliche- und zwischen $1.855 und $6.080 für private Adressen, sowie eine jährliche Gebühr zwischen $1.150 und $3.260.

3. OSI-Modell

Das OSI-Modell (Open System Interconnection Model) ist ein Konzeptmodell zur Beschreibung der Telekommunikations- und Computersysteme. Sie beinhaltet die ganze Netzwerkkommunikation, ohne dabei auf deren internen Strukturen sowie Technologien einzugehen.

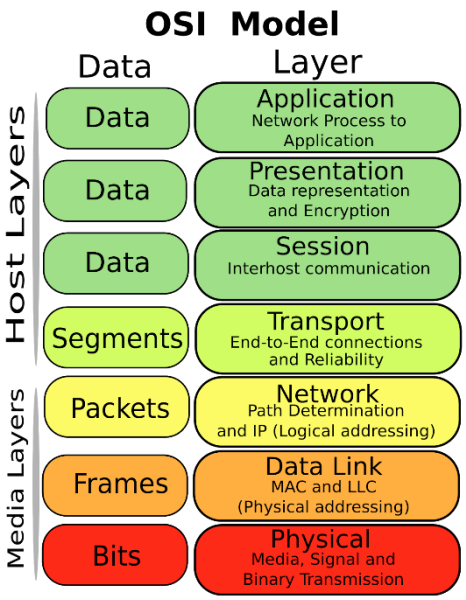


Abb. 1: OSI-Modell

Sie besteht aus sieben Schichten (engl. *Layers*), die aufeinander aufbauen. Wenn also beispielsweise die fünfte Schicht abgefragt wird, werden vorher die unteren Schichten abgerufen, um auf die fünfte Schicht zugreifen zu können.

Kurze Beispiele für jeden vorhandenen Layer:

1. Kabel, Netzwerkkarten, Hubs
2. Switches, MAC-Adresse
3. Router, IP-Adressen, Gateways
4. Transportprotokolle wie TCP und UDP
5. Herstellen und abbrechen von Verbindungen zwischen Geräten
6. Formatiert eingehende Daten, sodass die 7. Schicht sie versteht. Verschlüsselt und entschlüsselt Daten falls nötig
7. Kommunikation zwischen Applikation und User, z.B. durch SMTP (E-Mail) und FTP (Download)

4. IEEE

Das Institute of Electrical and Electronics Engineers (kurz *IEEE*) ist eine nicht-kommerzielle Organisation mit Sitz in New Jersey, US. Es ist ein Verband aus Elektro- und Informationstechnikern, die Fachtagungen anbieten, Herausgeber von diversen Fachzeitschriften sind sowie die Bildung von Gremien für die Standardisierung von Techniken, Hardware und Software.

4.1 IEEE 802

Die IEEE 802 ist eine Familie der IEEE Standards. Sie befasst sich mit dem Local Area Network (LAN) sowie dem Metropolitan Area Network (MAN), welches u.a. fürs Heim, Schulen, Campuse und auch ganze Städte zuständig ist.
Dieser Standard benutzt die ersten beiden Schichten des OSI-Modells, die Physical- und Data Link-Layer. Es sind u.a. die Ethernet- (IEEE 802.3) und Wi-Fi (IEEE 802.11) Protokolle in der IEEE standardisiert worden, sowie das Bluetooth Zertifikat (IEEE 802.15.1).
Es existieren noch viele andere Standards unter IEEE 802, wie *LLC*, *Token bus* und *Token ring*. Sie werden aber nicht mehr aktiv unterstützt und wurden aufgelöst.

5. Vorkommen

MAC-Adressen dienen zur Identifikation jeder Hardware, welche mit dem Internet in Verbindung tritt. Sie findet man auf jedem Gerät, welches eine *Network Interface Controller* (kurz NIC), auf Deutsch Netzwerkkarte, besitzt. Durch die Karte lassen sich Kommunikationen mit dem Internet bewerkstelligen, wie z.B. durch die Standards Ethernet und Wi-Fi.
Herkömmlich waren Netzwerkkarten als separate Hardware z.B. in Desktop PC's zu finden. Mit der Zeit und dem Fortschritt in der Technologie, existieren solche Karten nicht mehr. Der zuständige Chip für die Netzwerktauglichkeit wird auf das jeweilige Motherboard heutzutage aufgelötet.

Abb. 2: Netzwerkkarte

Einige Geräte mit einer MAC-48-Adresse:

- Smartphones, Notebooks, Spielekonsolen
- Smart-TVs
- Bluetooth Zahnbürsten
- Smart-Kühlschränke, Smart-Waschmaschinen
- PKW's

Grob zusammengefasst kann man sagen, dass Geräte die Ethernet, Wi-Fi und/oder Bluetooth bieten, auch eine MAC-Adresse besitzen. Wohlgemerkt sind diese dann auch unterschiedlich für **jede** Technologie und nicht dieselben MAC-Adressen.

6. Aufbau

Es existieren 3 Formen/Arten von MAC-Adressen, die im Grunde genau denselben Zweck erfüllen: MAC-48, EUI-48 und EUI-64.
Die derzeit gängigsten Formen sind die 48-Bit Adressen (EUI-48 und MAC-48) und werden (sowie die EUI-64) in hexadezimaler Schreibweise, Byteweise, geschrieben. Die Bytes werden hierbei durch Doppelpunkte oder Bindestriche voneinander getrennt. Da die Groß- und Kleinschreibung des Hexadezimalsystems irrelevant ist und für die Identifikation keinen Unterschied macht, stellen die verschiedenen Betriebssysteme MAC-Adressen entweder in Groß- oder Kleinbuchstaben dar. Beispiel wie so eine MAC-Adresse aussehen könnte:

f2:44:7b:18:ee:3a
F2-44-7B-18-EE-3A

Hexadezimal	Binär
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

Abb. 3

Ein Byte (z.B. das erste Byte “f2” im obigen Beispiel) besteht aus 8 Bits, welches für die bessere Lesbarkeit auch als *Oktett* geschrieben wird. Die MAC-48 und EUI-48 Adressen bestehen somit aus insgesamt 6 Oktetts, wie in der unteren Abbildung zu sehen ist.

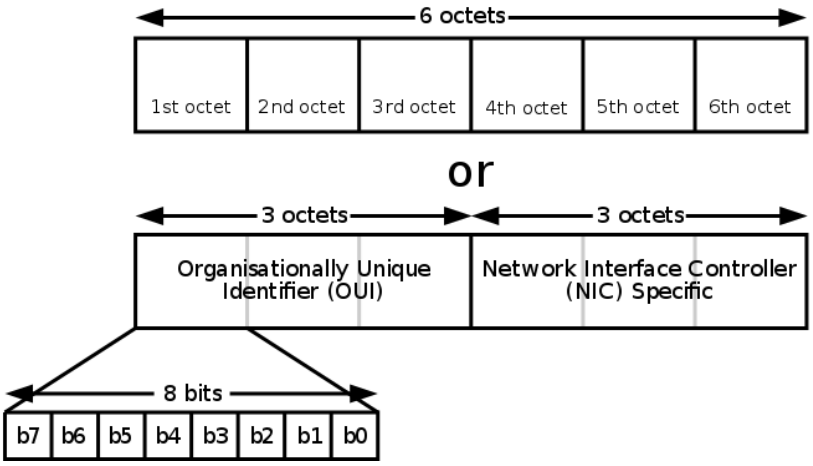


Abb. 4: Aufbau EUI-48

Die ersten drei Oktetts sind der sog. OUI (Organisationally Unique Identifier), welches die Herstellerkennungen der Hersteller widerspiegelt, Beispiel:

- Apple 04-F7-E4-xx-xx-xx
- Intel 00-07-E9-xx-xx-xx
- Cisco 00-60-2F-xx-xx-xx
- Asus 00-15-F2-xx-xx-xx

Die nächsten drei Oktetts, welche jeweils mit einem “x” versehen sind, stehen hierbei für eine beliebige Kombination aus Zahlen und Buchstaben von “a” bis “f”. Betriebssysteme stellen alle vorkommenden Buchstaben in einer MAC-Adresse entweder in Groß- oder Kleinschreibung dar. Es macht hinsichtlich der Identifikation jedoch keinen Unterschied, ob diese groß oder klein sind.

Mit den folgenden Links kann man seine eigene MAC-Adresse oder generell die OUI’s der Hersteller nachschauen:

- https://www.wireshark.org/tools/oui-lookup.html
- https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries

6.1 MAC-48 / EUI-48

MAC-48 und EUI-48 (EUI steht für *Extended Unique Identifier*) unterscheiden sich nur nominal voneinander: MAC-48 wird für Netzwerk-Hardware und EUI-48 für andere Geräte und Software eingesetzt.
Da die beiden Adressen im Prinzip genau dasselbe sind und der Unterschied zwischen den beiden zu gering war, hat die IEEE beschlossen, MAC-48 als obsolet zu erklären und die Bereiche von MAC-48 an die EUI-48 zu übertragen. Der Name MAC und MAC-Adresse an sich wird jedoch weiterhin im Gebräuchlichen genutzt und EUI-48 als dieser gehandelt, obwohl es diese nicht ist.
Die 48 Bit Adressen werden für IPv4 (Internet Protocol version 4) verwendet, wohingegen EUI-64 (64 Bit) ausschließlich für IPv6 (Internet Protocol version 6) Verwendung findet.
48-Bit Adressen besitzen die Möglichkeit 2^{48} (~281 Billionen) potenzielle Adressen zu erstellen, wohingegen 64-Bit Adressen 2^{64} mögliche Adressen bieten.

6.2 EUI-64

EUI-64 ist eine 64-Bit Adresse welches u.a. in IPv6 und Firewire zum Einsatz kommt. Sie hat im Grunde genau dieselben Funktionen wie eine EUI-48 Adresse. EUI-64 können wie EUI-48 von Firmen und Organisationen von der IEEE ausstellen lassen oder auch in eine *Modified* EUI-64 von MAC-48 und EUI-48 Adressen erstellt werden:

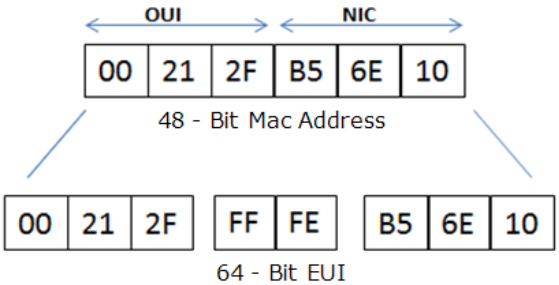


Abb. 5: Modified EUI-64

Wie aus der oberen Abbildung zu entnehmen ist, wird die 48-Bit große MAC-Adresse in zwei 24-Bit Blöcke geteilt. Zwischen den geteilten Blöcken wird - bei einer MAC-48, zwei Oktetts bestehend aus *FF-FF* eingesetzt oder wie im Schaubild bei einer EUI-48 Adresse, *FF-FE* eingefügt. Durch diese Erweiterung können 48-Bit Adressen unter IPv6 genutzt werden, ohne dabei jede "veraltete" 48-Bit Adresse durch die aktuelle EUI-64 mühsam ersetzen zu müssen.

6.2.1 EUI-48/EUI-64

Kurze Darstellung wie sich die 48-Bit-Adressen von 64-Bit-Adressen unterscheiden:

octet identifier	MSB 0	1	2	3	4	5 LSB
MA-L	24-bit OUI			24-bit extension		
MA-M	28-bit MA-M base			20-bit extension		
MA-S	36-bit OUI-36			12-bit extension		
example value (hex)	AC	DE	48	23	45	67
example value (binary)	1010 1100	1101 1110	0100 1000	0010 0011	0100 0101	0110 0111

Abb. 6: EUI-48 mit versch. Blöcken

octet identifier	MSB 0	1	2	3	4	5	6	7 LSB
MA-L	24-bit OUI			40-bit extension				
MA-M	28-bit MA-M base			36-bit extension				
MA-S	36-bit OUI-36			28-bit extension				
example value (hex)	AC	DE	48	23	45	67	01	9F
example value (binary)	1010 1100	1101 1110	0100 1000	0010 0011	0100 0101	0110 0111	0000 0000	1001 1111

Abb. 7: EUI-64 mit versch. Blöcken

6.3 Kanonische Darstellung / Bit-reversed-Darstellung

Verschiedene Protokolle interpretieren bei der Übermittlung eine MAC-Adresse auf unterschiedliche Weise - entweder mit der *Least Significant Bit* (LSB) zuerst oder mit der *Most Significant Bit* (MSB) zuerst. Die kanonische Darstellung ist hierbei LSB und die Bit-reversed-Darstellung MSB.
Die gängigste Form ist die LSB, da die Protokolle die mit der Bit-reversed-Darstellung arbeiten veraltet sind und nicht mehr

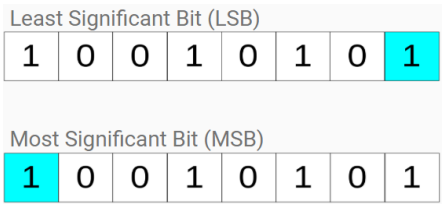


Abb. 8: Unterschied LSB und MSB

weitergeführt werden. Es wird jeweils immer Oktettweise übersetzt - bei LSB von rechts nach links gelesen und beim MSB von links nach rechts.
Man kann den Output einer MAC-Adresse z.B. durch die Kommandos *ifconfig*, *iproute2* und *ipconfig* sehen.
Da die Bitfolgen sich bei der Übersetzung ändern, können Verwechslungen und Irrtümer entstehen und eine falsche MAC-Adresse bei rauskommen.

Beispiel: Wir haben die MAC-Adresse **12-34-56-78-9A-BC**. Wenn wir sie jetzt jeweils in die beiden Formen übersetzen würden, käme für LSB die Bitfolge:
LSB = `01001000 00101100 01101010 00011110 01011001 00111101`
und für MSB die Bitfolge:
MSB = `00010010 00110100 01010110 01111000 10011010 10111100`

Wenn man nun diesen MSB Binärcode mit der LSB Reihenfolge in die Hexadezimale Schreibweise bringen würde, käme **48-2C-6A-1E-59-3D** heraus, die nicht unserer ersten MAC-Adresse entspricht. Es würde also eine *falsche* MAC-Adresse interpretiert werden, weswegen man darauf Acht geben sollte.

6.4 Universal / Lokal

Eine MAC-Adresse ist entweder immer eine universelle oder eine lokale Adresse. Wie man aus der Abbildung entnehmen kann, ist die 2. LSB im 1. Oktett ausschlaggebend hierfür - wenn dieser Bit eine **0** ist, ist sie universell, bei einer **1** hingegen lokal.

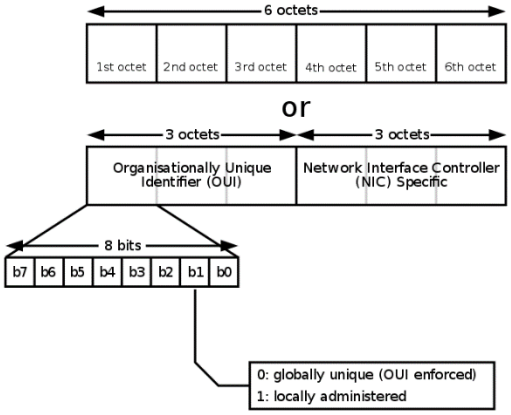


Abb. 9: Aufbau Global/Lokal

Universelle Adressen werden immer vom Hersteller festgelegt, mit ihrer OUI sowie den restlichen zufällig generierten drei Oktetts. Sie kommen so ziemlich (fast) überall zum Einsatz.
Lokale Adressen wiederum sind veränderte universelle Adressen, um sehen zu können, dass es sich eben um eine veränderte Adresse handelt. Diese werden z.B. von einem Netzwerk-Administrator verändert oder können sogar auch von der IEEE als CID (Company ID) statt einer OUI erworben werden. Lokale Adressen dürfen bzw. sollten nicht wie die universellen Adressen in der Öffentlichkeit verwendet werden, da dies zu gleichen MAC-Adressen und evtl. Missverständnissen führen kann.
Ein Anwendungsbeispiel von lokalen Adresse wäre die Nutzung in *MAC-Randomization*. Was dies genau ist, werde ich in *Punkt 8* näher erläutern.

6.5 Unicast / Multicast

Man kann MAC-Adressen noch auf eine andere unterscheiden: ob sie eine Unicast oder eine Multicast Adresse ist. Sie befindet sich wie die globale/lokale Bitfolge im 1. Oktett, diesmal jedoch an der 1. LSB. Wenn die Bitnummer an der Stelle eine 0 besitzt, ist die Adresse eine Unicast MAC-Adresse. Bei dem Bit 1 wäre sie also eine Multicast MAC-Adresse. Das Schaubild (rechts) verdeutlicht das ganze nochmal.

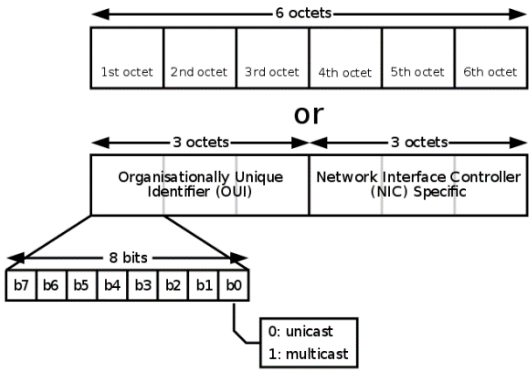


Abb. 10: Aufbau Unicast/Multicast

Unicast ist eine 1 zu 1 Übertragung. In demselben Netzwerk werden von einem Punkt zu einem anderen Punkt Datenpakete verschickt, jeweils mit einem Sender und Empfänger.

Multicast ist eine 1 zu vielen bzw. von vielen zu vielen. Im selben Netzwerk würde z.B. der Sender Datenpakete verschicken, die von mehreren Empfängern mit Multicast Adressen erhalten werden. Dies passiert automatisch, da von den gesendeten Daten Kopien erstellt werden, um sie direkt weiterzuleiten.

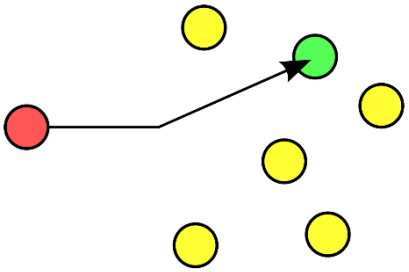


Abb. 11: Unicast

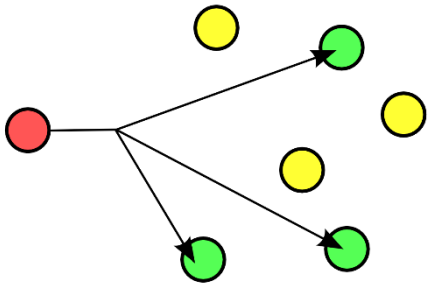


Abb. 12: Multicast

7. Kommunikation

Wie schon anfangs in *Punkt 3* erwähnt, kommen MAC-Adressen in der Data Link Layer (2. Schicht), genauer gesagt in der MAC-Sublayer, des OSI-Modells vor.
Um eine Verbindung mit den höheren Schichten aufzubauen, u.a. die IP-Adresse, gibt es zwei verschiedene Protokolle:

1. Address Resolution Protocol (ARP)
2. Neighbor Discovery Protocol (NDP)

Beide Adressen nutzen die 3. Schicht des OSI-Modells.
ARP wird u.a. bei IPv4, DECnet und ChaosNET eingesetzt. Die häufigste Verwendung findet die ARP unter IPv4 mit Ethernet und Wi-Fi, da sie generell mit Abstand am weitesten verbreitet sind.
NDP wird bei IPv6 eingesetzt. Ich werde im Folgenden den Prozess von ARP erklären.

Wenn ein Host mit einem anderen Host im selben Netzwerk kommunizieren möchte, braucht er neben der IP-Adresse auch die MAC-Adresse. Die IP-Adresse wird jeweils vom Router/Switch o.ä. jedem verbundenen Gerät automatisch (man kann dies auch manuell zuweisen) zugewiesen. Die MAC-Adresse kennt der Host derzeit nicht.
Der Sender möchte mit dem Gerät, der die IP: *192.168.1.120* besitzt, kommunizieren. Bei dem Versuch, sendet er dabei eine *ARP Request* (Anfrage) an alle Geräte die sich im selben Netzwerk befinden, um die MAC-Adresse des Geräts herauszufinden und Datenpakete mit ihm austauschen zu können. Der Host mit der IP: *192.168.1.120* meldet sich mit einem *ARP Reply* (Antwort) zurück und sendet dabei seine MAC-Adresse. Bei dem Prozess speichern die beiden Hosts die jeweiligen MAC-Adressen mit ihren jeweiligen IP-Adressen in eine sog. *ARP Tabelle*, um für zukünftige Kommunikationen den Prozess nicht wiederholen zu müssen.

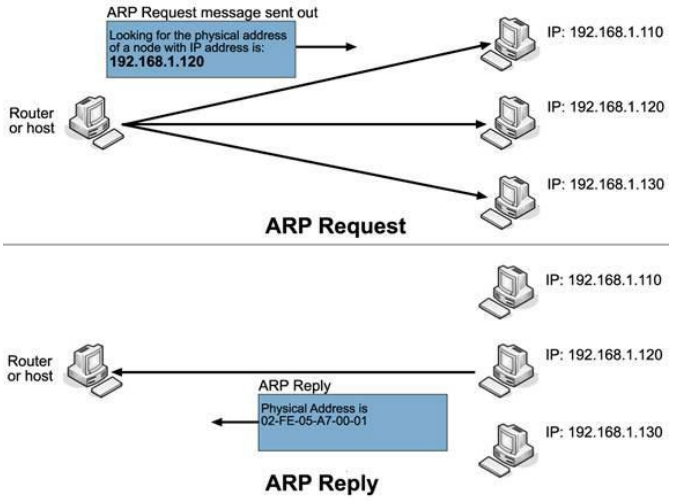


Abb. 123: Address Resolution Protocol

8. Verschleierung

Kommen wir nun zur Geheimhaltung der MAC-Adresse, dem sog. MAC-Spoofing. Durch das MAC-Spoofing kann man entweder gezielt die MAC-Adresse für ein bestimmtes Netzwerk oder durch eine zufällige Generierung von MAC-Adresse für jedes Netzwerk ändern lassen.
Es gibt mehrere Gründe, wieso man sie geheim halten sollte.

8.1 MAC-Spoofing - Warum?

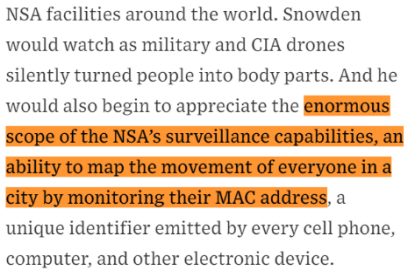

NSA facilities around the world. Snowden would watch as military and CIA drones silently turned people into body parts. And he would also begin to appreciate the enormous scope of the NSA's surveillance capabilities, an ability to map the movement of everyone in a city by monitoring their MAC address, a unique identifier emitted by every cell phone, computer, and other electronic device.

Abb. 134

Abb. 145

Abb. 156

Solche Schlagzeilen nehmen seit dem Whistleblow von Edward Snowden immer mehr zu. Snowden hat 2013 u.a. erwähnt, dass die National Security Agency (NSA) die Fähigkeit besitzt, die Bevölkerung anhand derer MAC-Adressen nachzuverfolgen. Wie? Im Vorwort habe ich erwähnt gehabt, dass so ziemlich jede Person auf der Welt heutzutage ein Smartphone besitzt. Da die Smartphones sich mit Netzwerken verbinden, um mit dem World Wide Web kommunizieren zu können, besitzen sie eine MAC-Adresse und wir wissen jetzt, dass MAC-Adressen einzigartig und individuell für jedes einzelne Smartphone sind. Das Smartphone trägt man jedes Mal bei sich. Wir schlussfolgern also:

"Das unentbehrliche Smartphone ist wegen seiner MAC-Adresse zu einem Tracking-Device geworden. Das Ausschalten von Ortungsdiensten/Ortungssystem per Satelliten schafft hierbei keine Abhilfe."

Abb. 15 und Abb. 16 zeigen deutlich, wie auch zwei “nicht-behördliche” Unternehmen die Londoner Bevölkerung anhand der MAC-Adresse verfolgen können. Beide Unternehmen setzen hierfür auf Tracking per Wi-Fi Scanning von Smartphones/Notebooks/Smartwatches usw.
Was Wi-Fi Scanning genau ist, kann man an Bild 4 sehen: Man sieht hier mehrere, sich in der Nähe befindende Wi-Fi Access Points. Um diese Darstellung überhaupt angezeigt zu bekommen, wird Wi-Fi Scanning eingesetzt. Bei dem Scan Vorgang sendet das Smartphone sog. *probe request frames* an die sich in der Nähe befindenden Access Points, wo u.a. auch die MAC-Adresse mit übertragen wird. Das Unternehmen “Renew London” würde also mit ihren Mülleimern, gezielt alle Bürger mit einem eingeschalteten Smartphone, die sich in der Nähe von solchen Mülleimern befinden, verfolgen können. Sie würden herausfinden, wie die individuelle Person sich in dem jeweiligen Ort fortbewegt, wie viel Zeit er/sie dabei benötigt und wo die Person ggfs. Stopps einlegt.
Durch diese Datenquelle besteht die Möglichkeit, gezielt individuelle Werbung zu generieren. Aus einem Blogeintrag des Unternehmens geht sogar hervor: “*It provides an unparalleled insight into the past behavior of unique devices -- entry/exit points, dwell times, places of work, places of interest, and affinity to other devices -- and should provide a compelling reach data base for predictive analytics (likely places to eat, drink, personal habits etc.)*“

Abb. 167: Nahliegende Wi-Fi Access Points

Wi-Fi Scanning kommt hierbei immer zum Einsatz. Man kann sie in den Systemeinstellungen zwar ausschalten, dennoch ist sie von Standard aus aktiviert.

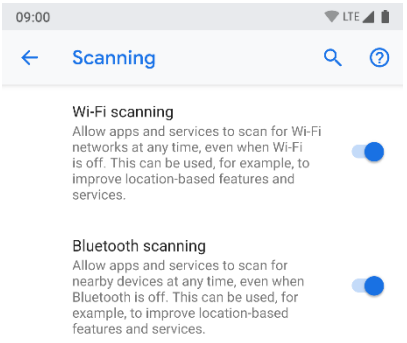


Abb. 178: Wi-Fi Scanning Option

Hier noch einige Beispiele, wieso man die MAC-Adresse ändern sollte:

1. Statische Zuweisung von IP-Adresse
    - Router bieten die Möglichkeit statische IP-Adressen den Geräten zuzuweisen. Wenn ein Gerät sich mit dem Router wieder verbindet, bekommt es wieder dieselbe IP-Adresse, sofern es die passende MAC-Adresse hierzu hat.
2. MAC-Adresse Filtering
    - Netzwerke können hiermit explizit Geräte durch deren MAC-Adressen von der Verbindung stoppen

3. MAC Authentication
    - Manche Internet-Provider wollen, dass man sich mit der MAC-Adresse authentifiziert. Im Anschluss können sich dann nur Geräte mit dem Internet verbinden, deren MAC-Adressen beim Provider hinterlegt sind.
4. Device Identification
    - Öffentliche Wi-Fi Netzwerke nutzen die MAC-Adresse zur Identifikation der Geräte. Hierdurch können die Netzwerke z.B. Timelimits von 30 min. setzen um die Geräte danach zu sperren. (limitierte Wi-Fi können auch durch Browser-Cookies oder Account-Systemen verfolgt werden)

Es sollte beachtet werden, dass jede Netzwerkschnittstelle eine eigene MAC-Adresse besitzt. Ein Laptop mit einem Ethernet, Wi-Fi und Bluetooth Anschluss besitzt somit drei MAC-Adressen.

8.2 MAC-Adresse herausfinden

Bevor man sich darauf stürzt, seine MAC-Adresse ändern zu wollen, sollte man erstmal wissen wie die aktuelle Adresse des Gerätes ist, da man sich vergewissern will ob diese sich nun wirklich geändert hat. Eventuell möchte man auch nach der Änderung der Adresse, diese auf die Originale MAC-Adresse zurücksetzen.
Um sie herauszufinden, muss man erstmal wissen was für ein Betriebssystem das Gerät besitzt, da es hierzu verschiedene Methoden existieren.

- Windows 10
    - Einstellungen → Netzwerk und Internet → WLAN → Hardwareeigenschaften → Physische Adresse (MAC)
    - Im Terminal mittels “ipconfig /all” oder “getmac”
- macOS
    - Systemeinstellungen → Netzwerk → Erweitert → Hardware
- Linux
    - #ip link show interface
- Android / iOS
    - Einstellungen → System → Über das Handy/Info

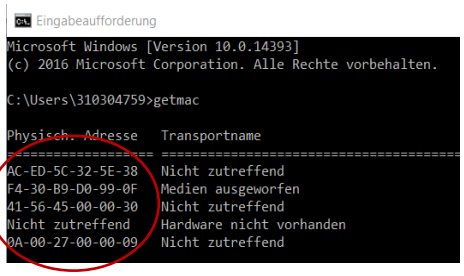


Abb. 189: Windows 10 MAC-Adressen im Terminal

8.3 MAC-Spoofing

Nachdem man die MAC-Adresse herausgefunden hat, können wir unsere MAC-Adresse ändern/verschleiern. Die Änderung der Adresse wird auch als *MAC-Spoofing* bezeichnet.
Wie auch bei der Anzeige der MAC-Adresse, ist auch hier die Vorgehensweise für das Spoofing abhängig vom Betriebssystem.
Es sollte beachtet werden, dass jede Netzwerkschnittstelle eine eigene MAC-Adresse besitzt. Ein Laptop mit einem Ethernet, Wi-Fi und Bluetooth Anschluss besitzt somit drei MAC-Adressen.

8.3.1 Im Betriebssystem

Man kann die MAC-Adresse auf ausgewählten Betriebssystem ohne die Hilfe von jeglicher Software selber ändern. Meist geht es dabei aber nur über das Terminal:

- Windows 10
  - Geräte-Manager → Netzwerkadapter → Netzwerk-Interface auswählen → Eigenschaften → Erweitert → Network Address / Locally Administered Address
    (Diese Einstellung findet man auf neueren Geräten oft nicht mehr, da Intel und Microsoft dies aus unerklärlichen Gründen einschränken.)
- Linux
  - # ip link set dev interface down
    # ip link set dev interface address xx:xx:xx:xx:xx:xx
    # ip link set dev interface up
- macOS
  - sudo ifconfig en(x) ether xx:xx:xx:xx:xx:xx
- Android / iOS
  - iOS nicht änderbar
  - Ab Android 8.1 nicht änderbar (evtl. auf älteren Versionen änderbar)

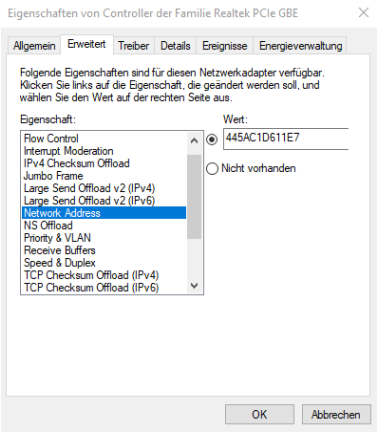


Abb. 20: Änderung MAC-Adresse in den Einstellungen des NIC

8.3.2 Software

Falls man Schwierigkeiten haben sollte die MAC-Adresse mittels Terminal zu ändern, kann man auch auf Software zurückgreifen.
Leider ist das Angebot hierfür sehr sporadisch, da viele nicht funktionieren.
Für Windows 10 gibt es eine Software namens *Technitium MAC Address Changer* die wie folgt aussieht:

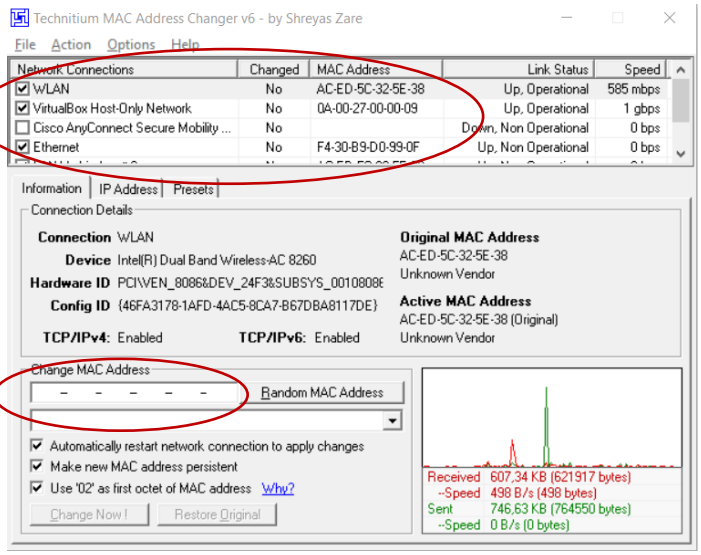


Abb. 191: Technitium MAC Address Changer

Technitium greift auf die *Registry-Datenbank* von Windows zurück und verpackt sie in eine übersichtliche Oberfläche. Man kann hier zwischen den verschiedenen Adaptern wie Wi-Fi und Ethernet wählen und so die jeweilige MAC-Adresse dafür ändern. Dies kann man in dem Feld unter *Change MAC Address* machen oder rechts daneben mit dem Button sich eine zufällige MAC-Adresse generieren lassen.

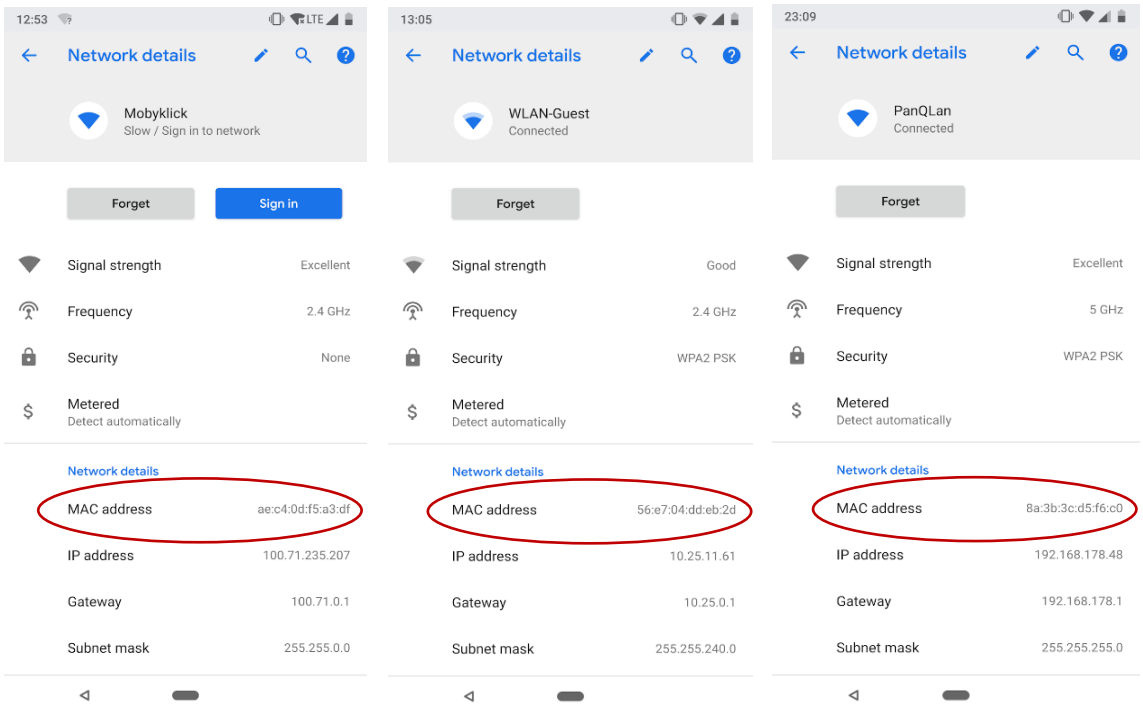
Es existiert noch eine andere Software: *Tails*.
Tails wird für Windows, Linux und macOS angeboten. Dabei ändert sie allerdings nicht nur die MAC-Adresse, welches nur vorübergehend ist, sondern ist ein eigenständiges Betriebssystem auf einem USB-Stick. Sofern also Tails an dem PC/Notebook ausgeführt wird, ändert sich auch die MAC-Adresse des Rechners. Wenn man nun aber Tails nicht mehr ausführt, verändert sich die Adresse des Gerätes wieder in ihre einzigartige, globale 48-Bit langen Binärcode.

Für Android (ab Version 8.1 mit Root-Zugriff) und iOS existieren keine Apps, die für eine Veränderung der MAC-Adresse sorgen. Eventuell ist es möglich dies auf älteren Softwareversionen zu ändern, ich konnte dies jedoch selbst nicht testen.

8.4 MAC-Randomization

Neben dem MAC-Spoofing wie wir eben kennengelernt haben, bieten Hersteller wie Apple, Google und Microsoft auch eine *zufällige* Änderung der MAC-Adresse an. Dabei bekommen alle Geräte ab iOS 8, Android 5 (Nexus und Pixel) und Windows 10 jedes Mal *pseudo* MAC-Adressen, wenn sie nach Wi-Fi Access Points scannen. Wenn wir uns den Artikel von Renew London mit den Mülleimern nochmal verdeutlichen, werden hierdurch genau solche gezielten Verfolgungen vermieden. Der Prozess für die zufällige Generierung von MAC-Adresse geschieht automatisch, allerdings ist sie auf Windows erst aktiv, wenn man es in den Systemeinstellungen einschaltet.
Daneben bieten Windows 10 und seit jüngstem auch Android 9 (befindet sich noch in der Betaversion) MAC-Randomization mit *verbundene*n Access Points an. Zufällige Adressen werden also nicht nur für das passive Scanning eingesetzt, sondern auch wenn man sich z.B. Zuhause, bei der Arbeit und beim Kollegen sich mit dem Wi-Fi verbindet.
Die zufällige Änderung mit einem verbundenen Access Point findet dabei nur einmal statt, da ansonsten bei jeder neuen Generierung der Router das “neue” Gerät nicht kennen würde und man ansonsten sich jedes Mal aufs Neue verbinden müsste. Das tut der Privatsphäre aber keinen Schaden, da man trotzdem überall anders eine andere MAC-Adresse besitzt.

Kurzes Beispiel, dass MAC-Randomization funktioniert:



8.5 Probleme

MAC-Adressen waren dafür bestimmt, einzigartig und individuell für jedes Gerät zu sein. Durch das MAC-Spoofing entsteht das Problem, dass es mehrere Geräte geben kann, welches dieselbe MAC-Adresse aufweist. Dies kann evtl. zu Problemen führen, wenn sie im selben Netzwerk verbunden sind. Zwar bekommt jedes Gerät eine individuelle IP-Adresse vom Netzwerk zugewiesen, dennoch sieht das Netzwerk nur eine MAC-Adresse, welches dann zu Verwirrungen führen kann.

MAC-Adressen die vom Betriebssystem durch das MAC-Randomization verändert werden, haben an der 2. LSB im 1. Oktett die Bitfolge 1, was bedeutet, dass es lokale Adressen sind. Wenn man also eine MAC-Adresse von ihrem Hexadezimalsystem in die Binärform umschreiben würde, würde man sofort erkennen, dass es nicht mehr die originale Adresse ist. So können Dritte, die von außen lauschen direkt erkennen, dass es sich um eine veränderte MAC-Adresse handeln muss.
Passive Attacken von *Lauschern* funktionieren also bei randomized Adressen nicht. Jedoch gibt es einige aktive Attacken, wie bspw. *Karma*, die es erlauben, die globale MAC-Adresse zu bekommen. Aktive Attacken basierend auf Karma simulieren einen Access Point, welches vom Gerät zur Verbindung bevorzugt wird. Hierdurch kann das Gerät welches mit Karma ausgestattet ist, jegliches aufnehmen und belauschen. Das solche Attacken in erster Linie funktionieren, ist auf eine Sicherheitslücke in Wi-Fi Chips zurückzuführen.

Als letzte Problemzone kann ein Lauscher von außen evtl. die globale Adresse anhand von Wi-Fi Frames einsehen. Wie man an der Abb. 22 sehen kann, wurde in dem linken rot umrandeten Rechteck die MAC-Adresse geändert. Im rechten Rechteck kann man nun auch sehen, dass jene MAC-Adresse dieselbe sein muss, da die Sequenznummer von den Wi-Fi Frames nicht zurückgesetzt werden. Hieraus kann ein Lauscher dann zurückführen, dass es sich um dieselbe Adresse handeln muss.

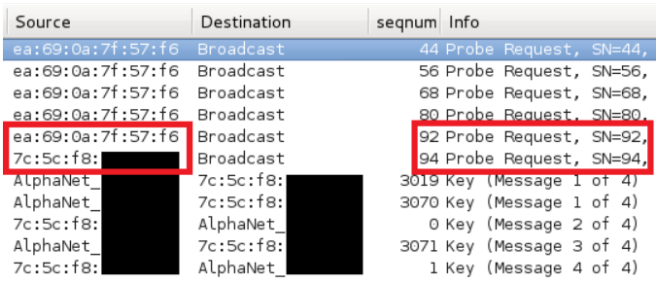


Abb. 202: MAC-Spoofing Wi-Fi Frames

Quellenverzeichnis

- https://de.wikipedia.org/wiki/MAC-Adresse *Zuletzt: 02.05.2018*
- https://en.wikipedia.org/wiki/MAC_address *Zuletzt: 02.05.2018*
- http://accc.uic.edu/answer/what-my-ip-address-mac-address *Zuletzt: 11.03.2018*
- https://www.youtube.com/watch?v=UrG7RTWIJak *Zuletzt: 11.03.2018*
- https://www.howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows-linux-and-mac/ *Zuletzt: 11.03.2018*
- https://en.wikipedia.org/wiki/MAC_spoofing *Zuletzt: 01.05.2018*
- *https://www.giac.org/paper/gsec/3199/mac-spoofing-an-introduction/105315 Zuletzt: 01.05.2018*
- https://searchnetworking.techtarget.com/definition/Data-Link-layer *Zuletzt: 12.04.2018*
- https://searchenterprisewan.techtarget.com/definition/WAN *Zuletzt: 07.04.2018*
- https://tails.boum.org/doc/first_steps/startup_options/mac_spoofing/index.de.html *Zuletzt: 11.03.2018*
- https://www.youtube.com/watch?v=9yYqNqTNngI&t *Zuletzt: 15.04.2018*
- https://www.youtube.com/watch?v=HEEnLZV2wGI *Zuletzt: 15.04.2018*
- http://standards.ieee.org/faqs/regauth.html *Zuletzt: 26.03.2018*
- https://supportforums.cisco.com/t5/network-infrastructure-documents/understanding-ipv6-eui-64-bit-address/ta-p/3116953 *Zuletzt: 26.04.2018*
- https://www.vultr.com/tools/mac-converter/ *Zuletzt: 26.04.2018*
- https://kwallaceccie.mykajabi.com/blog/how-to-calculate-an-eui-64-address *Zuletzt: 26.04.2018*
- https://en.wikipedia.org/wiki/Network_interface_controller *Zuletzt: 26.03.2018*
- https://www.electronics-tutorials.ws/binary/bin_3.html *Zuletzt: 30.03.2018*
- https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries *Zuletzt: 03.04.2018*
- https://en.wikipedia.org/wiki/Bit_numbering 09*.04.2018*
- https://www.cybrary.it/0p3n/karma-mitm-attack/ *22.04.2018*
- https://www.com-magazin.de/bilderstrecke/mac-adressen-id-eines-netzwerkadapters-322081.html?bid=198762 *01.04.2018*
- https://www.theregister.co.uk/2017/03/10/mac_address_randomization/ *24.04.2018*
- https://petsymposium.org/2017/papers/issue4/paper82-2017-4-source.pdf *28.04.2018*
- https://tools.ietf.org/html/rfc2469 *28.04.2018*
- https://standards.ieee.org/develop/regauth/oui28/index.html *22.03.2018*
- https://www.wired.com/2014/08/edward-snowden/ *22.04.2018*
- http://www.wired.co.uk/article/recycling-bins-are-watching-you *22.04.2018*
- https://networkengineering.stackexchange.com/questions/36843/do-bluetooth-devices-have-mac-address-with-the-same-specification-as-the-mac-add *10.04.2018*
- http://www.mathyvanhoef.com/2016/03/how-mac-address-randomization-works-on.html *22.04.2018*

Bilderverzeichnis