Ubiquitous WiFi may pose a serious treat to user privacy: take care of it with NetworkManager!

Francesco Giudici - fgiudici@redhat.com

Jan 25th 2019 – DevConf.CZ 2019
A TRIP TO THE MALL
CAPTURE (filter: !beacon frames)
MAC address:

- ALWAYS EXPOSED IN THE AIR
- USED ALSO WHEN NOT CONNECTED
- SOLUTION? RANDOMIZE IT!
NetworkManager: cloned-mac-address property

Randomization enabled by default during scanning

Controlled by the **cloned-mac-address** property when associating:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;hex value&gt;</td>
<td>custom value</td>
</tr>
<tr>
<td>preserve</td>
<td>don’t touch the MAC address (default)</td>
</tr>
<tr>
<td>permanent</td>
<td>use the burned in MAC address</td>
</tr>
<tr>
<td>stable</td>
<td>random stable MAC address</td>
</tr>
<tr>
<td>random</td>
<td>a new MAC address at each activation</td>
</tr>
</tbody>
</table>

```bash
$> nmcli connection modify MyConn cloned-mac stable
```
NetworkManager: cloned-mac-address property (II)
PROBE REQUESTS
CAPTURE (filter: probe requests)
CAPTURE (filter: probe requests)
NetworkManager:
no SSID in probe requests (by default)
DHCP OPTIONS
DHCP client-identifier

**DHCPv4 (RFC 2132)**
Option 61
“**MUST be unique among the client-identifiers used on the subnet to which the client is attached**”

**DHCPv6 (RFC 8415)**
Option 1
DUID: identifies the client
Options 3 and 4
IAID: identify the interface

**DHCPv4 (RFC 4361)**

<table>
<thead>
<tr>
<th>Code</th>
<th>Len</th>
<th>Type</th>
<th>IAID</th>
<th>DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>61</td>
<td>n</td>
<td>255</td>
<td>i1</td>
<td>i2</td>
</tr>
</tbody>
</table>

SOLUTION? RFC 7844 “Anonymity Profiles for DHCP Clients”
**CAPTURE (filter: DHCP client msgs)**

```
<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>154.987414725</td>
<td>172.16.154.226</td>
<td>1.1.1.1</td>
<td>DHCP</td>
<td>DHCP Request - Transaction ID 0x4f4f78e0</td>
</tr>
<tr>
<td>154.987992053</td>
<td>172.16.154.226</td>
<td>1.1.1.1</td>
<td>DHCP</td>
<td>DHCP Request - Transaction ID 0x4f4f78e0</td>
</tr>
<tr>
<td>154.988468418</td>
<td>172.16.154.226</td>
<td>1.1.1.1</td>
<td>DHCP</td>
<td>DHCP Request - Transaction ID 0x4f4f78e0</td>
</tr>
<tr>
<td>174.683952315</td>
<td>0.0.0.0</td>
<td>255.255.255</td>
<td>DHCP</td>
<td>DHCP Request - Transaction ID 0x62211c3c</td>
</tr>
<tr>
<td>566.634063300</td>
<td>0.0.0.0</td>
<td>255.255.255</td>
<td>DHCP</td>
<td>DHCP Discover - Transaction ID 0x7dc2c97a</td>
</tr>
<tr>
<td>605.834009367</td>
<td>172.16.154.226</td>
<td>1.1.1.1</td>
<td>DHCP</td>
<td>DHCP Request - Transaction ID 0x469fbac3</td>
</tr>
<tr>
<td>608.596977567</td>
<td>0.0.0.0</td>
<td>255.255.255</td>
<td>DHCP</td>
<td>DHCP Request - Transaction ID 0x44b99895</td>
</tr>
</tbody>
</table>
```

Transaction ID: 0x7dc2c97a
Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)
- Client IP address: 0.0.0.0
- Your (client) IP address: 0.0.0.0
- Next server IP address: 0.0.0.0
- Relay agent IP address: 0.0.0.0
- Client MAC address: 00:1c:11:00:00:00
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (Discover)
- Option: (61) Client Identifier
  - Length: 7
  - Hardware type: Ethernet (0x01)
  - Client MAC address: 00:1c:11:00:00:00
- Option: (57) Maximum DHCP Message Size
- Option: (60) Vendor class identifier
- Option: (12) Host Name
  - Length: 14
  - Host Name: HUAWEI_P9_lite
- Option: (55) Parameter Request List
- Option: (255) End
- Option: (255) End

Packets: 44925 - Displayed: 13 (0.0%)
NetworkManager: IPv4 dhcp-client-id property

<table>
<thead>
<tr>
<th>&lt;hex value&gt;</th>
<th>custom value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac</td>
<td>actual MAC address (RFC 7844)</td>
</tr>
<tr>
<td>perm-mac</td>
<td>permanent MAC address</td>
</tr>
<tr>
<td>stable</td>
<td>stable random value</td>
</tr>
<tr>
<td>duid</td>
<td>IAID + DUID (RFC 4361)</td>
</tr>
</tbody>
</table>

$> nmcli conn mod MyConn ipv4.dhcp-client-id mac

Default can be configured

[connection-anon]
ipv4.dhcp-client-id=mac

NetworkManager.conf
# NetworkManager: IPv6 dhcp-duid property

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;hex value&gt;</td>
<td>custom value</td>
</tr>
<tr>
<td>lease</td>
<td>DUID from the lease or global DUID-UUID (RFC 6355)</td>
</tr>
<tr>
<td>llt</td>
<td>DUID-LLT</td>
</tr>
<tr>
<td>ll</td>
<td>DUID-LL (RFC 7844)</td>
</tr>
<tr>
<td>stable-llt</td>
<td>stable random DUID-LLT</td>
</tr>
<tr>
<td>stable-ll</td>
<td>stable random DUID-LL</td>
</tr>
<tr>
<td>stable-uuid</td>
<td>stable random DUID-UUID</td>
</tr>
</tbody>
</table>

```
$> nmcli conn mod MyConn ipv6.dhcp-duid ll
```

Default can be configured

```
[connection-anon]
ipv6.dhcp-duid=ll
```

NetworkManager.conf
CAPTURE (filter: DHCP client msgs)

Transaction ID: 0x7dc2c97a
Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)
- Client IP address: 0.0.0.0
- Your (client) IP address: 0.0.0.0
- Next server IP address: 0.0.0.0
- Relay agent IP address: 0.0.0.0
- Client MAC address: d6:4b
- Client hardware address padding: 00000000000000000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP

- Option: (53) DHCP Message Type (Discover)

- Option: (61) Client Identifier
  - Length: 7
  - Hardware type: Ethernet (0x01)
  - Client MAC address: d6:4b

- Option: (57) Maximum DHCP Message Size

- Option: (60) Vendor class identifier

- Option: (12) Host Name
  - Length: 14
  - Host Name: HUAWEI P9 lite

- Option: (55) Parameter Request List
- Option: (255) End

Packets: 44925 - Displayed: 13 (0.0%)
NetworkManager:
DHCPv4 option 12 (hostname)
DHCPv6 option 39 (FQDN)

NetworkManager sends out system hostname by default.

DROP THE OPTIONS

```
$> nmcli conn mod MyConn \
ipv4.dhcp-send-hostname no \
ipv6.dhcp-send-hostname no
```

CHANGE THE OPTIONS

```
$> nmcli conn mod MyConn \
ipv4.dhcp-hostname ‘nemo’\nipv6.dhcp-hostname ‘nemo.dom’
```
SO, WHAT ARE YOU GOING TO DO IF YOU SPOT ME AT THE MALL?
NetworkManager: enforcing privacy

MAC address = random

DHCPv6 client-id = 11

DHCPv4 client-id = mac

Hostname: don’t send

https://gitlab.freedesktop.org/NetworkManager/NetworkManager/blob/master/examples/nm-conf.d/30-anon.conf
QUESTIONS?

https://wiki.gnome.org/Projects/NetworkManager

gitlab: https://gitlab.freedesktop.org/NetworkManager
github: https://github.com/NetworkManager
ML: networkmanager-list@gnome.org
IRC: #nm