# IPv6 Privacy Extensions for the GNRC Network Stack

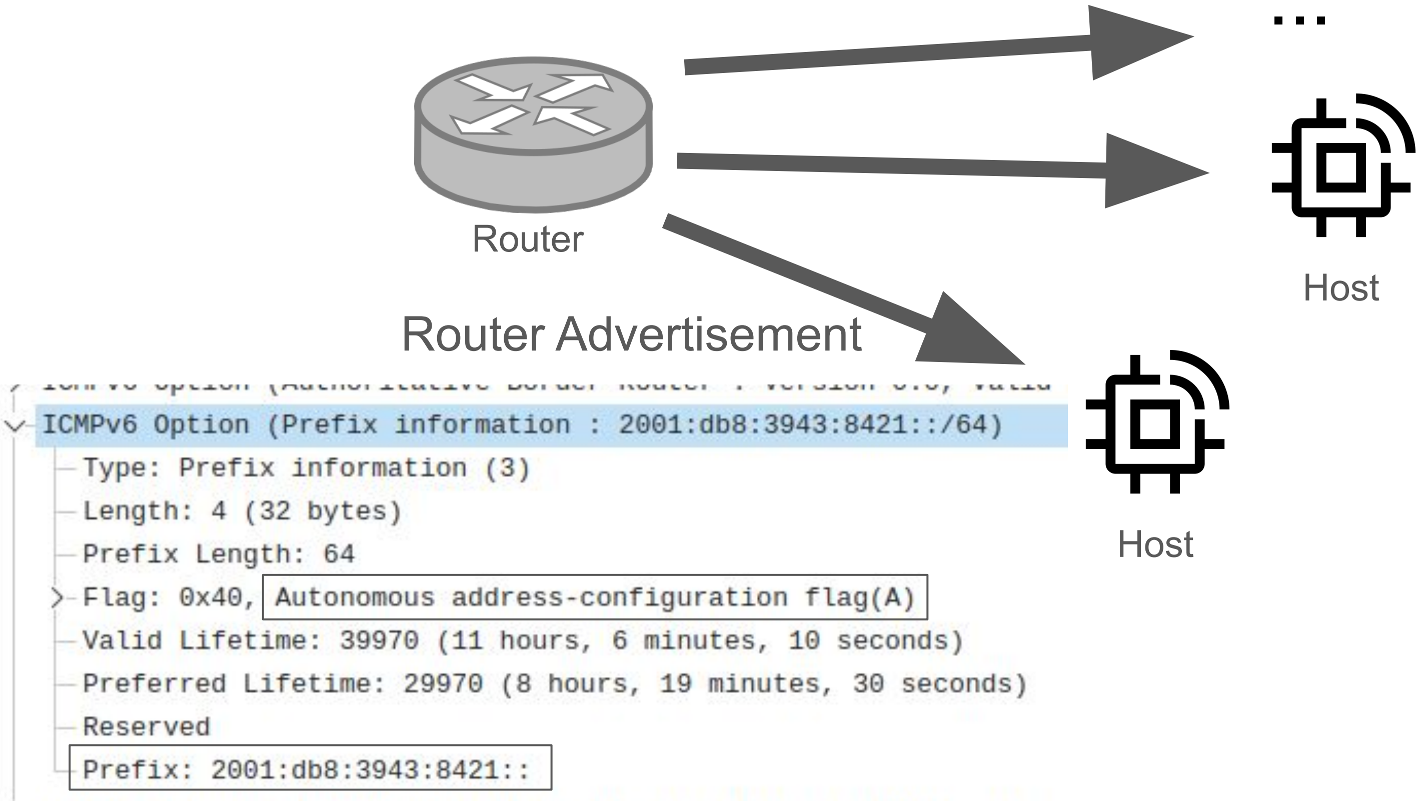
Nico Lick, Frankfurt University of Applied Sciences

2024-09-05

# Agenda

- Privacy exposures
- Privacy extensions
- Usage considerations

# Stateless Address Autoconfiguration

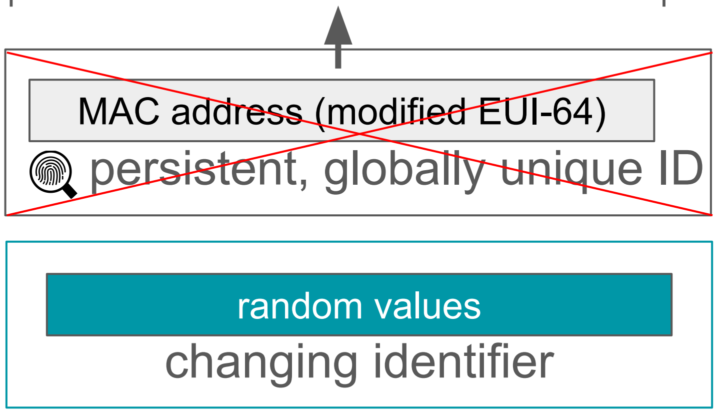


```
> ICMPv6 Option (Authoritative Border Router : Version 0.0, Valid
v ICMPv6 Option (Prefix information : 2001:db8:3943:8421::/64)
    Type: Prefix information (3)
    Length: 4 (32 bytes)
    Prefix Length: 64
  > Flag: 0x40, Autonomous address-configuration flag(A)
    Valid Lifetime: 39970 (11 hours, 6 minutes, 10 seconds)
    Preferred Lifetime: 29970 (8 hours, 19 minutes, 30 seconds)
    Reserved
    Prefix: 2001:db8:3943:8421::
```

# Interface Identifier

IPv6 address

```
|            64 bits             |            64 bits             |
+--------------------------------+--------------------------------+
|         subnet prefix          |          interface ID          |
+--------------------------------+--------------------------------+
```



~~MAC address (modified EUI-64)~~

~~persistent, globally unique ID~~

random values

changing identifier

**Privacy exposures** by exposing MAC address in IP address:

- Tracking within a prefix
- Tracking across prefixes
- Network re-identification
- Geolocation leak through Wi-Fi access points

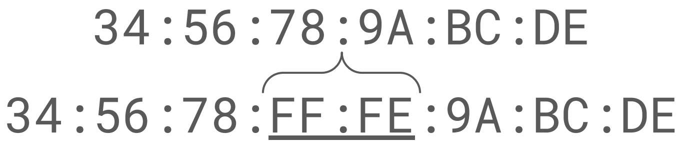
[RFC4291]

# Interface Identifier from MAC address (modified EUI-64)

MAC address / MAC-48

is a EUI-48 (Extended Unique Identifier)

1. Expand to 64 bits. EUI-48 becomes **EUI-64**



34:56:78:9A:BC:DE

34:56:78:FF:FE:9A:BC:DE

**2.** “Universal/Local bit” flip -> “***modified*** EUI-64” (only for use in IPv6 IID)

3**6**:56:78:FF:FE:9A:BC:DE

Notation in IPv6 address: 3656:78FF:FE9A:BCDE

[RFC4291]

# Tracking within a prefix

Temporal tracking inside a network

2001:0db8:3943:8421:**3656:78ff:fe9a:bcde**

Unchanged as long as connected to the network

-> Individual hosts in the same network are distinguishable -> temporal tracking

[RFC7721]

# Tracking across prefixes

Prefix change due to different network

2001:0db8:3943:8421:**3656:78ff:fe9a:bcde** (prefix1:**iid1**)

at some other point, in a different prefix

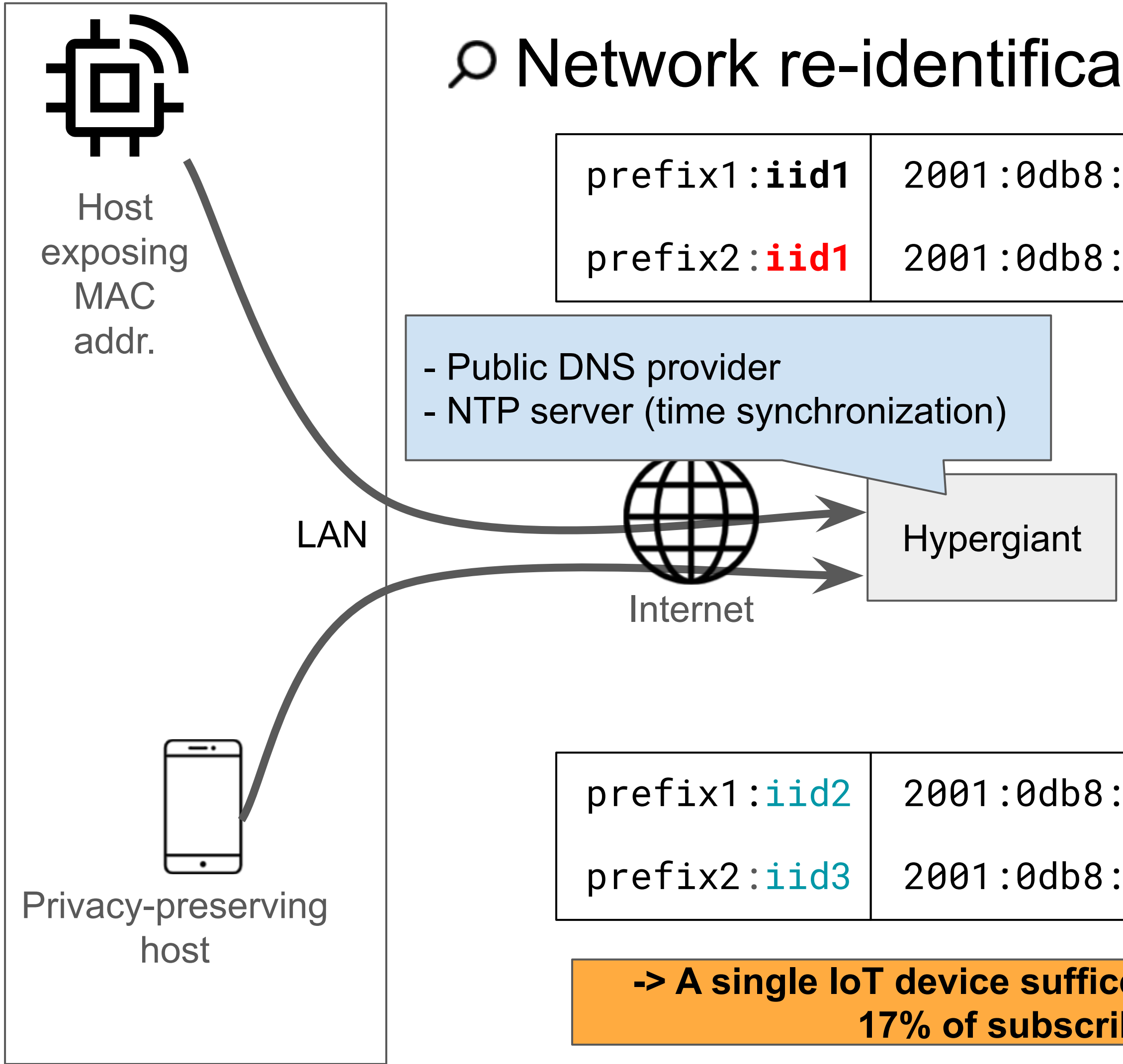
2001:0db8:3364:7387:**3656:78ff:fe9a:bcde** (prefix2:**iid1**)

Prefix change due to prefix rotation ->

[RFC7721]

# Network re-identification

[Bad-Apple]



| | |
|---|---|
| prefix1:**iid1** | 2001:0db8:3943:8421:**3656:78ff:fe9a:bcde** |
| prefix2:**iid1** | 2001:0db8:3364:7387:**3656:78ff:fe9a:bcde** |

- Public DNS provider
- NTP server (time synchronization)

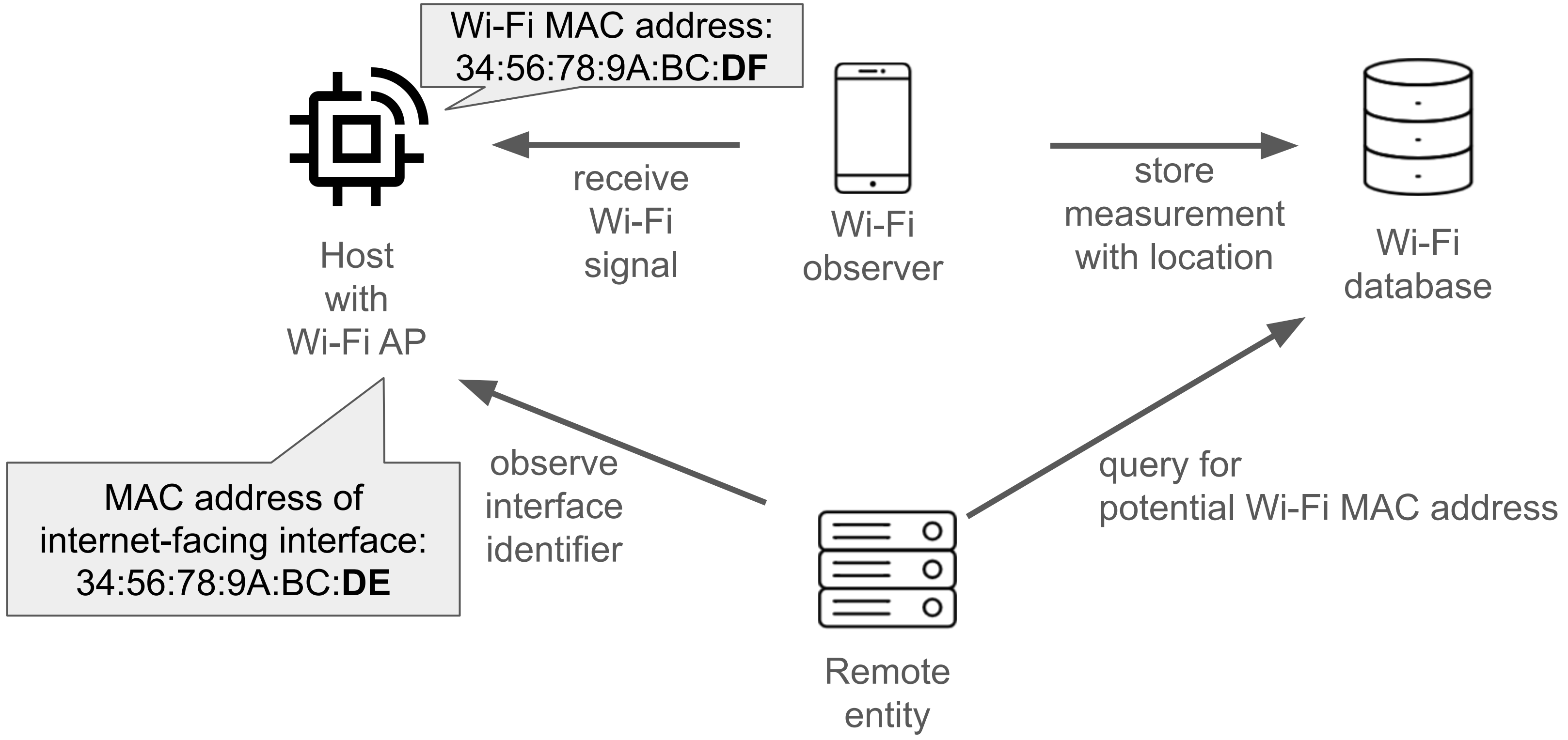
Host exposing MAC addr. is re-identified across prefixes. (**prefix1 => prefix2**)

*Some other hosts moved along with it*, which therefore likely are the same devices as in the previously observed prefix. (**iid2 => iid3**)

| | |
|---|---|
| prefix1:iid2 | 2001:0db8:3943:8421:1648:7c92:5f79:c22e |
| prefix2:iid3 | 2001:0db8:3364:7387:c37d:1165:1b41:ab16 |

**-> A single IoT device suffices to track prefix rotation, 17% of subscribers affected**

# Geolocation leak through Wi-Fi access points



**-> IPv6 address to geolocation**

[IPvSeeYou]

# Agenda

- Privacy exposures
- **Privacy extensions**
- Usage considerations

# Privacy mechanisms

☑ Use stable address

 ☐ Use stable privacy adressing (RFC7217)

  (instead of MAC address for interface identifier)

☐ Use temporary addresses (RFC8981, previously RFC4941)

 (independent of stable addresses)

**Temporary addresses**:

*Periodically change* IID. Immediately change if prefix changes.

```
IID = random()
```

lifetime = 2 days, actively used for 0.4-1 days

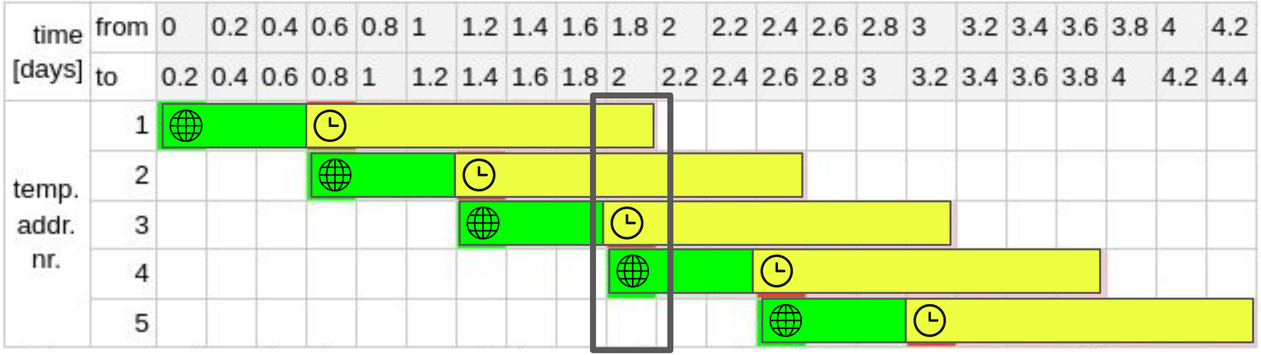
**Stable privacy addresses**:

Recommended as default since 2017 by IETF.

fixed IID per prefix, different across prefixes

```
IID = hash(Prefix, secret_key, Net_Iface, DAD_Counter)
```

# Max. configured temporary addreses



| time [days] | from | 0 | 0.2 | 0.4 | 0.6 | 0.8 | 1 | 1.2 | 1.4 | 1.6 | 1.8 | 2 | 2.2 | 2.4 | 2.6 | 2.8 | 3 | 3.2 | 3.4 | 3.6 | 3.8 | 4 | 4.2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | to | 0.2 | 0.4 | 0.6 | 0.8 | 1 | 1.2 | 1.4 | 1.6 | 1.8 | 2 | 2.2 | 2.4 | 2.6 | 2.8 | 3 | 3.2 | 3.4 | 3.6 | 3.8 | 4 | 4.2 | 4.4 |
| temp. addr. nr. | 1 | 🌐 | 🟩 | 🟩 | 🕒 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | | | | | | | | | | | | |
| | 2 | | | | 🌐 | 🟩 | 🟩 | 🕒 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | | | | | | | | | |
| | 3 | | | | | | | 🌐 | 🟩 | 🟩 | 🕒 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | | | | | | |
| | 4 | | | | | | | | | | 🌐 | 🟩 | 🟩 | 🕒 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | | | |
| | 5 | | | | | | | | | | | | | 🌐 | 🟩 | 🟩 | 🕒 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 |

States: 🌐 = preferred, 🕒 = deprecated

Timeline of address states
in the case of most simultaneous temporary addresses
when using default lifetime limits

# Agenda

- Privacy exposures
- Privacy extensions
- **Usage considerations**

# Device output

```
# ifconfig
# Iface  7  HWaddr: 03:11  Channel: 26  NID: 0x23  PHY: O-QPSK
#           Long HWaddr: BA:10:F8:D9:6A:AF:03:11
#            State: IDLE
#           ACK_REQ  L2-PDU:102  MTU:1280  HL:64  6LO
#           IPHC
#           Source address length: 8
#           Link type: wireless
#           inet6 addr: fe80::b810:f8d9:6aaf:311  scope: link  VAL
#           inet6 addr: 2001:db8:3943:8421:f5f1:e5d0:cc31:5fec  scope: global  VAL
#           inet6 addr: 2001:db8:3943:8421:d1cf:a650:e1f7:e1e7  scope: global  VAL TMP
```

6LoWPAN: 16 compression contexts shared among network nodes

```
# 6ctx
# cid|prefix                                     |C|ltime
# ----------------------------------------------------------
#   0|                   2001:db8:3943:8421::/64 |1|  664min
#   1| 2001:db8:3943:8421:f5f1:e5d0:cc31:5fec/128|1|   13min
#   2| 2001:db8:3943:8421:d1cf:a650:e1f7:e1e7/128|1|   13min
```

# 6LoWPAN: Scaling beyond 16 compression contexts

Host only:

- **Random MAC addresses**.
    - (minor operational changes)
    - Change address
    - - each time you connect to a network,
    - - or in the same network
        - Some overlap as grace period? Cooperation from the router helpful.

Router only:

- **Network Address Translation** (modify IP addresses)

Both host and router:

- **Short address hashing**
    - (moderate operational changes)
- **Compression context per device**
    - (non-standard, IETF WG had not much interest due to complexity) (SLAAC or DHCPv6)

# How to use it in your app

https://github.com/RIOT-OS/RIOT/**pull/20370**: **stable privacy addresses**

Makefile:
```
CFLAGS += -DCONFIG_GNRC_IPV6_STABLE_PRIVACY=1
```

https://github.com/RIOT-OS/RIOT/**pull/20369**: **temporary addresses**

Makefile:
```
CFLAGS += -DCONFIG_GNRC_IPV6_NIB_SLAAC_TEMPORARY_ADDRESSES=1
```

**Which ones should I choose?**

Stable privacy addresses:

- No expected complications when switching. Recommended as default by IETF.

Temporary addresses:

- Useful if mobile device
- break long-lived connections: limited by valid lifetime of temporary address. Transport layer keep-alive interval to detect broken connectivity = max. unreachable time.

# Conclusion: Privacy Extensions

- Prevent tracking through your IP address
- Relevant for IoT
- Available in RIOT

# Sources / Literature

[RFC8981]

F. Gont, S. Krishnan, T. Narten, and R. P. Draves, “Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6,” Internet Engineering Task Force, Request for Comments RFC 8981, Feb. 2021. doi: 10.17487/RFC8981.

[RFC7217]

F. Gont, “A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC),” Internet Engineering Task Force, Request for Comments RFC 7217, Apr. 2014. doi: 10.17487/RFC7217.

[RFC7721]

A. Cooper, F. Gont, and D. Thaler, “Security and Privacy Considerations for IPv6 Address Generation Mechanisms,” Internet Engineering Task Force, Request for Comments RFC 7721, Mar. 2016. doi: 10.17487/RFC7721.

[Bad-Apple]

S. J. Saidi, O. Gasser, and G. Smaragdakis, “One bad apple can spoil your IPv6 privacy,” *SIGCOMM Comput. Commun. Rev.*, vol. 52, no. 2, pp. 10–19, Jun. 2022, doi: 10.1145/3544912.3544915.

[IPvSeeYou]

E. Rye and R. Beverly, “IPvSeeYou: Exploiting Leaked Identifiers in IPv6 for Street-Level Geolocation.” arXiv, Sep. 15, 2022. doi: 10.48550/arXiv.2208.06767.

[RFC4291]

S. E. Deering and B. Hinden, “IP Version 6 Addressing Architecture,” Internet Engineering Task Force, Request for Comments RFC 4291, Feb. 2006. doi: 10.17487/RFC4291.

**Requirements for IID for stable privacy addresses**:

A device generates a different address for different prefixes
A device uses the same address for the same prefix (for the same prefix: same stability as MAC addresses)
-> **Prefix**

Shall be unpredictable for observer whether 2 given IIDs belong to the same secret.
*Prefix->randomIID mapping*
*Or more efficient: Hash (one-way) + Secret (different per device, randomly initialized once)*
*Predictably random, but only predictable if you know secret, which only device itself knows*

Devices in the same LAN should not collide -> **DAD_Counter**
to force generation of a different one when there is a duplicate address

**F(Prefix, Net_Iface, secret_key, DAD_Counter)**

**Net_Iface**: ifindex, name or even MAC address.
Should still be an _interface identifier_, i.e. be different across interfaces.
E.g. you connect to the same subnet simultaneously with multiple interfaces. Only needs to uniquely identify an interface for a single host, not necessarily across hosts.

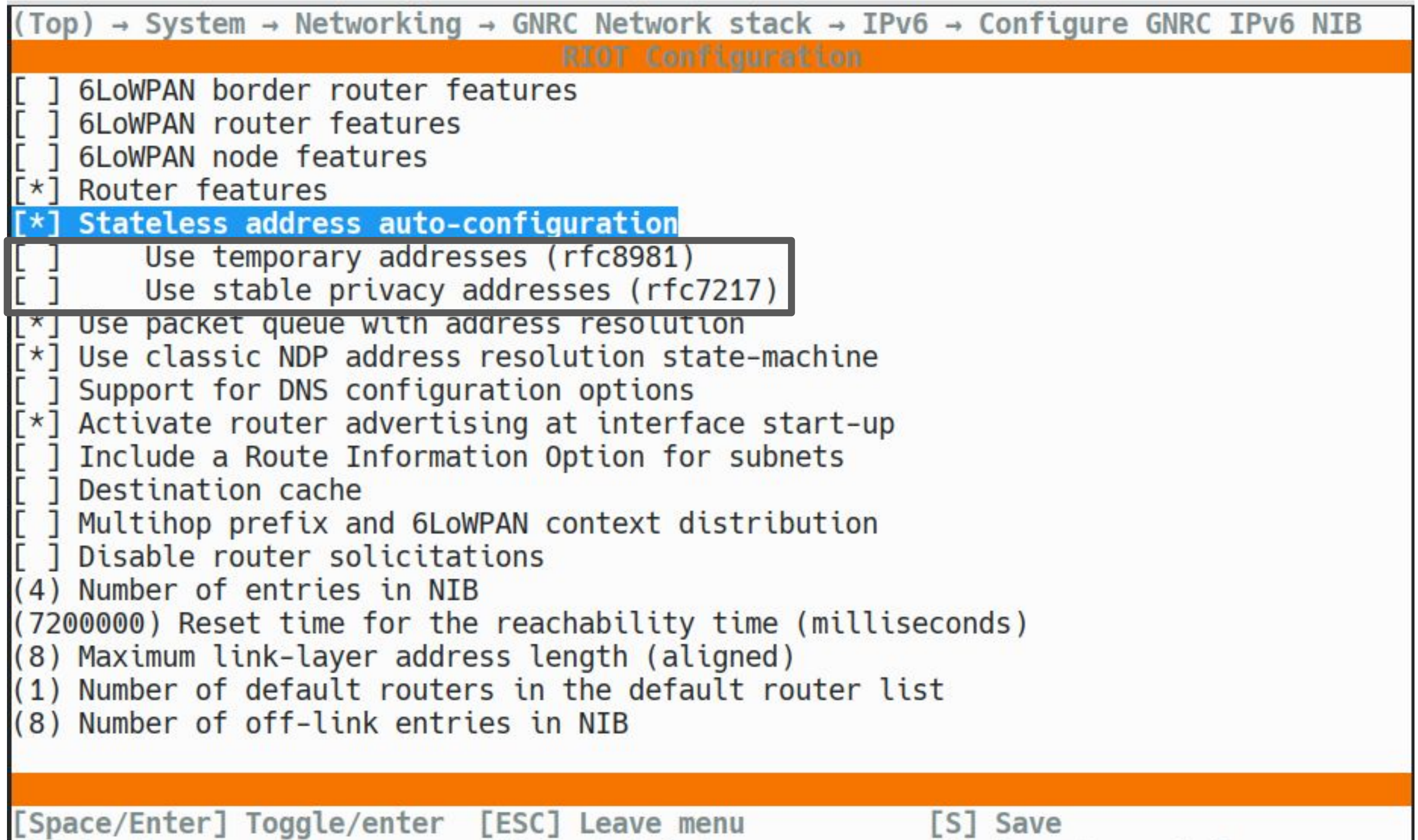
IETF Internet Architecture Board (IAB) committee:

*In the late 1990's when IPv6 stateless autoconfiguration was being developed,
notions of what constituted "personally identifiable information" (PII)
were limited to identifiers such as name, address, and telephone number.*

*If [...] the privacy implications of persistent re-use of stable identifiers had been better understood,
the temporary addressing mechanism would have been more likely to have emerged sooner
and with a stronger normative default.*

- https://www.iab.org/media/documents/IPv6-addresses-privacy-review.txt

# KConfig (make menuconfig):



```
(Top) → System → Networking → GNRC Network stack → IPv6 → Configure GNRC IPv6 NIB
                                   RIOT Configuration
[ ] 6LoWPAN border router features
[ ] 6LoWPAN router features
[ ] 6LoWPAN node features
[*] Router features
[*] Stateless address auto-configuration
[ ]     Use temporary addresses (rfc8981)
[ ]     Use stable privacy addresses (rfc7217)
[*] Use packet queue with address resolution
[*] Use classic NDP address resolution state-machine
[ ] Support for DNS configuration options
[*] Activate router advertising at interface start-up
[ ] Include a Route Information Option for subnets
[ ] Destination cache
[ ] Multihop prefix and 6LoWPAN context distribution
[ ] Disable router solicitations
(4) Number of entries in NIB
(7200000) Reset time for the reachability time (milliseconds)
(8) Maximum link-layer address length (aligned)
(1) Number of default routers in the default router list
(8) Number of off-link entries in NIB

[Space/Enter] Toggle/enter  [ESC] Leave menu          [S] Save
```

# Icon sources

https://uxwing.com/finger-print-icon/

https://iconduck.com/icons/293829/time
https://www.iconpacks.net/free-icon/location-pointer-2961.html
https://www.iconpacks.net/free-icon/search-2906.html
https://uxwing.com/wifi-line-icon/

https://openclipart.org/detail/171415/router-symbol
https://www.svgrepo.com/svg/340470/iot-platform

https://www.iconpacks.net/free-icon/mobile-phone-2642.html
https://www.iconpacks.net/free-icon/globe-4286.html
https://www.iconpacks.net/free-icon/server-12259.html
https://www.iconpacks.net/free-icon/database-server-black-outline-20310.html