IEEE 802.11bh and 802.11bi

- Short Introduction and Update -

Jerome Henry, Juan Carlos Zuniga

November 2021

v 01

Context

- Randomized and Changing MAC Address (RCM) is becoming common practice in mobile client devices
  - The Whole Industry is wondering about the impact on network services
    - WBA, WFA, IEEE, IETF
  - Following IETF work in 2013-2015 on privacy, IEEE 802 (under the umbrella of the IEEE 802.1 Security Workgroup) published a *Recommended Practice for Privacy Considerations for IEEE 802 Technologies* https://standards.ieee.org/standard/802E-2020.html
  - 802.11aq (2018) allows usage of RCM outside of association, but forbids it during active associations
  - In 2019, a Topic Interest Group (TIG) was formed to “consider the merits and challenges presented by randomized and changing MAC addresses within an 802.11-based network” -> the outcome is 802.11bh and 802.11bi Task Groups

802.11bh

- ***802.11bh: Enhanced service with randomized MAC addresses***
  - *The goal: given RCM, are there services that break with current 802.11?*
    - *Note that the goal is not to fix the entire world, not to 'encourage' or 'discourage' RCM, not to address privacy aspects (although the proposed solution should not degrade privacy in 802.11)*
  - *The group is examining which services, which use cases may break*
  - *Once the relevant use cases/services will have been identified, remediations will be proposed (either recommendations or enhancements to the IEEE 802.11 Standard)*
  - *Group work is expected to be rather short (publication by mid-2023)*

802.11bh Status

- ***802.11bh: Enhanced service with randomized MAC addresses***
  - *Primary use cases "possibly broken" by RCM: enterprise IT support and troubleshooting, roaming efficiency, accounting and billing, post-association access control*
  - *Likely out of scope: 802.1X, DHCP resource exhaustion, pre-association access control, steering*
  - *Group is working on a stable L2 representation of the STA (e.g. Identifiable Random MAC), so the AP can recognize the associated RCM STA as it rotates its MAC*
  - *Goal is to start text proposals before EoY*

802.11bi

- ***802.11bi: Enhanced service with Data Privacy Protection***
  - *The goal: can 802.11 be enhanced to offer better privacy?*
    - *Note that the goal is not to look at the consequences of RCM, although it is understood that RCM has a positive impact on privacy for personal devices*
  - *The group is examining which elements have an impact on privacy, which elements could improve privacy*
  - *The group will publish enhancements to the IEEE 802.11 Standard*
  - *Group work is expected to be longer than 802.11bh (publication by mid-2025)*

802.11bi Status

- ***802.11bi: Enhanced service with Data Privacy Protection***
  - *Group is listing issues: Information Element fingerprinting, password identifier sent in the clear, same for other identifiers (PMKID etc.), STA MAC address persistence ('and' visible in DA, SA), soft/mobile AP privacy, behavioral fingerprint, PHY/RF (e.g. CSI reports in the clear)*
  - *Already point-proposals (PMKSA persistence beyond RCM, STA persistence in roaming with RCM), etc.)*

  - Goal is to complete use cases by March 2022, then start looking at common requirements, then text