IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID Query analysis | | | | |
| Date: 2022-01-14 | | | | |
| Author(s): | | | | |
| Name | Company | Address | Phone | email |
| Mark Hamilton | Ruckus/CommScope | 350 W. Java Dr  Sunnyvale, CA | +1 303 818 8472 | [mark.hamilton2152@gmail.com](mailto:mark.hamilton2152@gmail.com) |
|  |  |  |  |  |

Abstract

Analysis of the ID Query solution concept for TGbh, considering use cases and desired attributes.

R0 – Initial discussion document.

R1 – Updated, to match Issues Tracking 11-21/0332r29

R2 – Corrected analysis against criteria 15 and 17, per comments on Jan 11 teleconference.

# Introduction

This document evaluates the ID Query concept, being proposed in TGbh as one possible solution, discussing the applicability of the solution for the identified use cases as well as desirable attributes for a solution, per the 11-21/0332 (Issues Tracking) document.

# Solution analysis

## Applicability to Use Cases

The following analysis compares the ID Query proposal to those use cases that are agreed to be in scope, or possibly could be “nice to have” (but not required to be solved), per Issues Tracking document discussion.

Use cases that were agreed to result in “recommendations only” are not considered.

**Table 1 – Analysis against Use Cases**

|  |  |  |
| --- | --- | --- |
| Use Case(s) | In scope/description (per Table 1 of Issues Tracking)? | Client ID query analysis |
| 4.1 - Pre-association client steering | “Nice to have”, if can find sufficient privacy controls (opt-in, etc.) – maybe as a recommendation? Maybe if a solution to another problem happens to solve this? | Yes, when returning to a network that has previously been visited, and using PASN with authentication. |
| 4.2 - Post-association (returning device) device identification | Yes. Focus on a “returning device” needing identification on per network/SSID basis. | Yes. Provides, if the user does opt-in, a “user-friendly” or network assigned/understood identifier for the device, that can be used by various detection systems, etc. (to the same level of trust as currently for a MAC address). |
| 4.3 - Post-association home automation/arrival detection | Yes | Yes. Same analysis as for use case 4.2. |
| 4.6 - Grocery store frequent shopper notifications | Only in scope if criteria in Table 2 are not compromised | Yes. Same analysis for use case 4.2, or 4.1. |
| 4.10 – Approved client in secured environment. | Similar to 4.1 and 4.2, for pre-association and post-association situations, respectively. | Yes. Same analysis for use cases 4.1 and 4.2. |
| 4.13 – Mobile AP | Might add some recommendations? (But, might consider a solution, if one presented – would need to address the lack of this terminology in 802.11) | Not addressed by this proposal, but could be extended (in “reverse direction”) if identification of the Mobile AP is desired. |
| 4.15 - Customer Support and Troubleshooting | Aspects are within our scope, might be alternative interface(s) to access and/or control the MAC address behavior. | Yes, with user “opt in”, assuming the issue is not “my device will not connect at all, ever.” Good for the long-term troubleshooting needed by many common support cases. |

## Applicability to attributes/criteria

The following analysis compares the ID Query proposal to the attributes/criteria currently agreed to be useful, per Issues Tracking document’s Table 2 discussion.

**Table 2 – Analysis against features/attributes/criteria**

|  |  |
| --- | --- |
| Attribute/criteria | Client ID query |
| 1. User opt-in, per network | Yes. Includes recommendations for user configuration. |
| 2. Third-party can’t track – device can use a different address when returning/over time | Yes. Client ID and MAC address being used are completely de-coupled, so any MAC randomization scheme can be used to stop tracking. Client ID is entirely within the secured link. |
| 3. No exposure of PII that had been hidden by RCM? | Yes. All PII is within security context (so just as safe as all the other user data). |
| 4. Network can provide user services (automation, access control, etc.) – device can return to same ESS | Yes, with same level of trust as previous MAC address-based schemes. Does not add any new/better security of user identification. |
| 5. Network can use for troubleshooting | Yes, other than the “My device won’t connect to the network at all, ever” scenario. |
| 6. Network can provide QoS, DHCP, services | QoS, yes. DHCP depends on tight coupling between AP and DHCP server (not likely in practice), or just recommendations on identifier use. |
| 7. Pre-association client identification is possible (nice-to-have) | Yes, when PASN can be used. |
| 8. Is it “Extensible”? (Nice-to-have?) | Maybe/probably. This metric is not well defined, yet. |
| 9. Processing required on AP one-time/infrequent | Zero. |
| 10. Processing required on AP each association | Virtually zero. One simple message exchange. No computation required. |
| 11. Processing required on non-AP STA one-time/infrequent | Zero. |
| 12. Processing required on non-AP STA each association | Virtually zero. One simple message exchange. No computation required. |
| 13. Setup complexity for AP administrator | Zero. |
| 14. Setup complexity to configure non-AP STA | Only user configuration of desired identifier to share with each network. |
| 15. Memory/storage requirements on AP (consider large # of clients) | Storage of identifier, only for associated clients. No history required, beyond replacement of any prior storage of a MAC address replaced with storage of the identifier instead. |
| 16. Memory/storage requirements on non-AP STA | Storage of identifier as part of “network profile” (when user does opt in). |
| 17. Third-party can determine if non-AP STA is using the solution? | ID Query Capability is indicated in Extended Capabilities. Exchanges of ID Query information, and whether an identifier is provided or refused, are all within the secure link, and no more trackable than any other user data. |
| 18. Solution depends on an encrypted link? (Nice to have if ‘no’?) | Yes |
| 19. How strongly is the ID bound to a user, and giving the user access/capabilities/etc.? | Entirely up to the user, to choose the identifier to share with each network. The ID can only be trusted to the same level a MAC address was trusted in the past. |
| 20. Is it important/critical that the AP is trusted? | Entirely up to the user. Choice of an identifier that exposes PII can be controlled to be only on networks that have strong(er) trust. |
| 21. How “real” is the ID, in terms of getting to actual end-user identification versus a throwaway? | Entirely up to the user. |
| 22. How much the network can trust the ID, to re-establish context from last time? | 1. As much as it could have trusted MAC address in past 2. The network can control this, depending on the level of client device authentication used to establish the secure link. Although, with high trust in the device authentication, a client identifier is probably not needed, anyway. |
| 23. How does client know level of trust of the network (trust of AP/infrastructure/back-end entities)? | Up to the implementation and the user. The ID could be provided only on networks that have been validated. Or, the user can indicate that the ID is not “sensitive” and provide it more freely, for example based just on the SSID, if there is no significant concern of exposure to a spoof (for example, the grocery store case). |
| 24. Consider operation of the solution on networks that are “Open”, or PSK and could be exposed. (Note that protection of (post-association/SA) identifier is no higher than protection of the data exchange. Not a new problem caused by RCM.) | Similar to just above, the user can indicate which identifiers are sensitive, and which are not (or less so). Less sensitive identifiers can be used on Open or PSK networks, where the concern of exposure is low. Note: It should be a recommendation that the identifier is only shared over Enhanced Open (OWE) networks, and not truly Open networks, to avoid third-party tracking. |
| 25. Control over lifetime of the identifier? User control and/or network control? | Entirely at user control. |
| 26. Consider whether solution offers identifier per device, user or group. | The user can completely control the scope of the identifier, using a unique identifier per-device, or a shared identifier across all devices that user operates, or even more broadly shared if that’s appropriate to the use case. |
| 27. Network being spoofed can gain access to client identifier? | This is under user control, to decide the level of trust and verification needed from the network before the identifier is shared. Some identifiers might be very sensitive PII, and a high level of network validation can be required before proving the identifier (security and authentication context established). Or, an identifier might be “throw-away”/generally known/not sensitive, and can be shared more freely. |