IEEE P802.11
Wireless LANs

|  |
| --- |
| ID Query analysis |
| Date: 2021-11-11 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Mark Hamilton | Ruckus/CommScope | 350 W. Java DrSunnyvale, CA | +1 303 818 8472 | 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 –

# 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? | Client ID query |
| 4.1 - Pre-association client steering 4.10 - Approved client detection in secured infrastructure network (pre-association) | Pre-association identification is not clearly in scope as something we need to solve, but it might be “nice to have” as long as no privacy concerns are created. | Yes, when returning to a network that has previously been visited, and using PASN. |
| 4.2 - Post-association access control (Parental controls, etc.)4.10 - Approved client detection in secured infrastructure network (post-association) | Yes | Yes. Provides, if the user does opt-in, a “user-friendly” or network assigned/understood identifier for the device, that can be used by parental controls and other access control/detection systems, etc. (to the same level of trust as currently for a MAC address). |
| 4.3 - Post-association home automation (including arrival detection) | Yes | Same analysis as for use case 4.2. |
| 4.6 - Grocery store frequent shopper notifications | Yes, for post-association.Possibly “nice to have” for pre-association (no association), similar to use case 4.1 | Yes. Same analysis for use case 4.2, or 4.1. |
| 4.14 - Onboarding a “known” MAC address (secure environment, or controlled/managed), but does anyone know the address? | Not decided.If using MAC address currently, that has limited security, but is easy to use. | Yes, provides similar “easy to use” interaction, but only to the same level of trust as currently for a MAC address. |
| 4.15 - Customer Support and Troubleshooting | Not decided/haven’t completed discussion. Enterprise versus residential use cases, pre- and post-association scenarios.Includes “long duration” (days to weeks) troubleshooting. | Yes, with user “opt in”, assuming the issue is not “my device will not connect at all, ever.” Good for the long-term troubleshooting. |
| 4.21 - Accounting and billing issues (WBA) | Yes | Yes. Similar to use case 4.2 |
| 4.22 - QoS and QoE (WBA) | Not decided yet. Might be the same as use case 4.2, for scenarios that are within 11bh scope. | Yes. Similar to use case 4.2 |
| 4.23 - DHCP pool exhaustion (WBA)4.24 - Inconsistent DHCP address assignment (WBA) | Not decided yet. Might just be recommendations on DHCP configuration (lifetime, DHCP identifier use). | Probably not covered, although recommendation could be to use same “identifier” for ID Query and DHCP client id, which might solve.Alternatively, implementations could do tight coupling between APs and DHCP server, but that is out of scope and seems complicated in practice. |
| 4.25 - ACLs/firewalls (MAC-address based) (WBA) | Yes | Yes. Similar to use case 4.2 |
| 4.25 - ACLs/firewalls (IP-address based) (WBA) | Not decided yet. | Probably not, but is similar to use case 4.23. |

## 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 discussion.

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

|  |  |
| --- | --- |
| Attribute/criteria | Client ID query |
| User opt-in | Yes. Includes recommendations for user configuration. |
| 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. |
| 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). |
| 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. |
| Network can use for troubleshooting | Yes, other than the “My device won’t connect to the network at all, ever” scenario. |
| 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. |
| Pre-association client identification is possible (nice-to-have??) | Yes, when PASN can be used. |
| Is it “Extensible”? (Nice-to-have?) | Maybe. This metric is not well defined, yet. |
| Processing required on AP one-time/infrequent | Zero. |
| Processing required on AP each association | Virtually zero. One simple message exchange. No computation required. |
| Processing required on non-AP STA one-time/infrequent | Zero. |
| Processing required on non-AP STA each association | Virtually zero. One simple message exchange. No computation required. |
| Setup complexity for AP administrator | Zero. |
| Setup complexity to configure non-AP STA | Only user configuration of desired identifier to share with each network. |
| Memory/storage requirements on AP (consider large # of clients) | Zero. |
| Memory/storage requirements on non-AP STA | Storage of identifier as part of “network profile” (when user does opt in). |
| Third-party can determine if non-AP STA is using the solution? | No. All exchanges are within secure link, no more trackable than any other user data. |
| Solution depends on an encrypted link? (Nice to have if ‘no’?) | Yes |
| 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. |
| 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. |
| How “real” is the ID, in terms of getting to actual end-user identification versus a throwaway? | Entirely up to the user. |
| 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.
 |
|  |  |