IEEE P802.11
Wireless LANs

|  |
| --- |
| TSID Proposal Analysis |
| Date: December 29 2021 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom | 250 Innovation Drive, San Jose CA | +1 408 391 2159 | nehru.bhandaru@broadcom.com |
| Thomas Derham | Broadcom |  |  |  |

**Abstract**

This document contains an analysis of Transient Station Identification proposal in 11-21-1839r0 with respect to the use cases and analysis criteria in 11-21-0332r27 tentatively agreed upon by TGbh for evaluating proposed solutions.

*Note: In this document TSID refers to the Transient Station Identification and not the traffic stream identifier defined in Draft P802.11REVme\_D1.0.*

Revision Notes

R0 – initial version

References

[1] 11-21-0332r27 – TGbh Issues Tracking

[2] 11-21-1839r0 – Transient Station Identification (TSID) proposal

[3] Draft P802.11REVme\_1.0

Based on Table in § 5 Issues and analysis… of TGbh issues tracking document 11-21-0332r27, the following table summarizes how the TSID proposal addresses the use cases that are in scope.

|  |  |  |
| --- | --- | --- |
| Use Case # | Use Case/Status | TSID Proposal |
| 4.1 | Pre-association client steering - Nice to have | Yes, the mechanism applicable post-association is the same as the one pre-association. The TSID is derived from the security context; PASN (11az) can be used pre-association – which allows MAC address to change while un-associated via a TSID update (via SA Query or Unicast Probe Request) |
| 4.2 | Post-association access control (returning) device identification per network/SSID basis – In scope | Yes, the device is identified by the permanent MAC address or entity named in the security context that is established first time the device associates; that identity is bound to the TSID generated from the security context and the device can (at its choice) use the TSID in the next association to identify itself to the network. Real/permanent Identity is treated as abstract and is managed by higher layers while allowing access control to be possible. |
| 4.3 | Post-association home automation/arrival detection – In scope | Yes, see above. |
| 4.4 | Airport security queue – Out of scope | N/A |
| 4.5 | Grocery store customer (movement) analysis – Out of scope | N/A |
| 4.6 | Grocery store frequent shopper – In scope | Yes. The use case in scope, per description in § 4.6 of 11-21-0332r7, seems to be the same as the post-association case. TSID even allows pre-association identification, at the discretion of the device. In the pre-association case, identification may be authenticated or not (e.g., PASN without authentication). Higher layer policies would decide whether authentication is required. |
| 4.7 | Infrastructure with different SSIDs – Out of scope | N/A |
| 4.8 | Infrastructure use of probes – Only recommendations | N/A |
| 4.9 | Unapproved client detection – Out of scope | N/A |
| 4.10 | Approved client in secured environment – Maps to post-association and pre-association use cases | Yes. Approved client can be identified by the TSID. The network and the client agree on the TSID to use next time as they both generate the TSID in the same way from the security context. |
| 4.11 | Approved and secured client taking unexpected actions – Out of scope | N/A |
| 4.12 | Unapproved AP detection – Out of scope | N/A |
| 4.13 | Mobile AP – Out of scope |  |
| 4.14 | Onboarding a “known” MAC address – Out of scope | N/A |
| 4.15 | Customer support and troubleshooting – May be in scope | Not sure about this, is it really in scope. Perhaps MAC randomization could be disabled temporarily for this case. PASN + TSID could be used if basic frame exchange is possible, but it is likely there will be cases where it is not. |
| 4.16 | Residential gateway with public hotspot – Out of scope | N/A |
| 4.17 | Lawful surveillance – Out of scope | N/A |
| 4.18 | Emergency services – Out of scope | N/A |
| 4.19 | Public Wi-Fi hotspot roaming – Out of scope | N/A |
| 4.20 | MAC address collisions (WBA) – Out of scope | N/A |
| 4.21 | Accounting and billing issues (WBA) – Out of scope | N/A |
| 4.22 | QoS and QoE (WBA) – Out of scope | N/A |
| 4.23 | DHCP pool exhaustion – Might add recommendations | Yes. Perhaps DHCP assignment can be based on device identification that TSID facilitates, but this can be totally handled at higher layer. |
| 4.24 | Inconsistent DHCP address assignment (WBA) – Out of scope | N/A |
| 4.25 | ACLs/firewalls (WBA) – Already covered by 4.2, Out of scope otherwise | N/A |

Based on Table 2 in § 6.4 Solutions Analysis, the following table summarizes evaluation of TSID proposal relative to the criteria listed in the table.

|  |  |  |
| --- | --- | --- |
| ID | Attribute/criteria | TSID Proposal |
| 1 | User opt-in, per network |  |
| 2 | Third-party (attackers/parties not intended to have the identification) can’t track – device can use a different address when returning/over time | Yes. TSID is updated with each secure association and whenever a MAC address needs to change. An observer cannot tell from the OTA frames whether TSID is being updated. |
| 3 | No exposure of PII that had been hidden by RCM? | No. PII is not exposed. TSID generation and update are protected cryptographically (current RSN mechanisms or otherwise). |
| 4 | Network can provide user services (automation, access control, etc.) – device can return to same ESS | Yes. See notes on TSID proposal in case 4.2 in the use case table above. |
| 5 | Network can use for troubleshooting | Yes, the last TSID may be kept on the device and in the network. |
| 6 | Network can provide QoS, DHCP, services | Yes, TSID may be used to identify the client – it is up to the client to use/identify itself or not. Just like a new permanent MAC address gets a new IP address, a new unknown TSID could be assigned a new IP address. |
| 7 | Pre-association client identification is possible (nice-to-have??) | Yes. See use case table above. |
| 8 | Is it “Extensible”? (Nice-to-have?) | Yes. Not exactly sure what this criterion means, but TSID proposal can work with an arbitrary identity or identity exchange protocol. It extends current RSN mechanisms. Perhaps this question might make more sense for proposals that introduce additional protocols to support the feature requirements. |
| 9 | Processing required on AP one-time/infrequent | Infrequent. Frequency is only governed by how often a client wishes to update the TSID – perhaps to start using a new random MAC address. |
| 10 | Processing required on AP each association | Yes. No additional protocol, but small amount of computation; TSID is derived from the security context established using already defined mechanism. The computation itself uses a small number of HMAC-Hash operations where Hash is usually SHA256. AP does not need to perform an exhaustive hash computation and searching through all the clients. |
| 11 | Processing required on non-AP STA one-time/infrequent | Infrequent. Frequency is only governed by how often a client wishes to update the TSID – perhaps to start using a new random MAC address |
| 12 | Processing required on non-AP STA each association | Yes. No additional protocol, but some computation; TSID is derived from the security context established using already defined mechanism. |
| 13 | Setup complexity for AP administrator | Not complex. Needs an entity on the AP to collect TSID information. Typically, this would be the Authenticator. TSID information could be exposed via MLME. |
| 14 | Setup complexity to configure non-AP STA | Not complex. Needs an entity on the non-AP STA to derive TSID information. Typically, this would be the Supplicant. This functionality may be enabled by default based on AP/Network capability and thus there is no setup really. |
| 15 | Memory/storage requirements on AP (consider large # of clients) | 30 octets/client with 128 bit keys. |
| 16 | Memory/storage requirements on non-AP STA | 30 octets/network with 128 bit keys. |
| 17 | Third-party can determine if non-AP STA is using the solution? | Yes. |
| 18 | Solution depends on an encrypted link? (Nice to have if ‘no’?) | Yes. An encrypted link can be setup using PASN or an RSN association. PASN can setup an encrypted link without any prior credentials. |
| 19 | How strongly is the ID bound to a user, and giving the user access/capabilities/etc.? | Strongly and securely. Derived from the security context. |
| 20 | Is it important/critical that the AP is trusted? | Yes. If the AP is not trusted, the client can be tracked. |
| 21 | How “real” is the ID, in terms of getting to actual end-user identification versus a throwaway? | As real as the client/use case warrants. It is bound to the security context and thus can identify the user. It can be a throwaway – e.g., can be generated on first access to the network and can be updated until some future time and/or restricted to a location. TSID also does not by itself leak any identity or its relation with its predecessor for the same identity. |
| 22 | How much the network can trust the ID, to re-establish context from last time? (Spoofing protection) Level of trust of the ID should match the trust of the data exchange with this network. | Fully trusted. Only the entity that used the TSID last can produce it. Spoofing protection of TSID on the AP or the non-AP STA is no different than spoofing protection for data exchange e.g., key compromise or spoofing. |
| 23 | How does client know level of trust of the network (trust of AP/infrastructure/back-end entities)? | RSN mechanisms and authentication are leveraged. No new mechanisms. |
| 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.) | PASN can be used with the mechanism to protect open networks. |
| 25 | Control over lifetime of the identifier? User control and/or network control? | User control. User can stop using a TSID. Some status indication from the AP/network to indicate TSID has expired may help. |
| 26 | Consider whether solution offers identifier per device, user or group. | One per device. When group credentials (e.g., PSK) are used, the security context (PTKSA) that is setup will drive further identification of the non-AP STA by the AP/network. No mechanism is proposed to share TSID among multiple devices. |
| 27 | Network being spoofed can gain access to client identifier? | No. When a client derives TSID with a genuine AP, there is no way for the rogue network to obtain the TSID unless the network access is unauthenticated, or the client uses the TSID (say in PASN or secure association) and a rogue device intercepts the transmission. A rogue device cannot obtain the TSID from the AP. |

The following table outlines how the TSID proposal compares to the other proposals

|  |  |
| --- | --- |
| Other Proposal | How TSID Proposal Compares |
| 11-21-1585 Identifiable Random MAC addresses | * Auto transient ID and key generation/distribution without additional messages
* Replay protection
* Binding to address (chain) and security context
* Better performance with faster validation
* No check field that can be trackable
* Leverage Std 802.11 SA query support
* TSID update – implicit and explicit, pre and post association
* Fewer new protocol messages
 |
| 11-21-1083 Signature based identification schemes | * Does not use public keys
* Does not leak identity (public key signatures leak the public key)
* More efficient
 |
| 11-21-1379 ID Query Action Frame | * No (additional) ID exchange is needed
	+ But can be used in conjunction to retrieve ID to bind to TSID
* Uses Std 802.11 SA query support
* Supports Identity recovery with TSID – higher layers can do the mapping
* Works when there is no association, after first secure association or PASN
* BTSID is bound to security context
* Fewer new protocol messages
 |