IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Text for ID Query Action Frame  |
| Date: 2021-08-29 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Mark Hamilton | Ruckus/CommScope | 350 W. Java DrSunnyvale, CA 94089 | +1-303-818-8472 | mark.hamilton@commscope.com |
| Carol Ansley | Self |  | +1-404-229-1672 | carol@ansley.com  |
| Kurt Lumbatis | CommScope |  |  | kurt.lumbatis@commscope.com |
|  |  |  |  |  |

Abstract

This submission proposes a new action frame exchange to allow an AP and non-AP STA can use to exchange a unique identifier for the non-AP STA (within a secured link). The proposal is based on IEEE P802.11-2020.

Revisions:

* Rev 0: Initial version, prepared for TGbh consideration.
* Rev 1: Corrected typos; clarified “non-AP” on some occurrences of (unqualified) “STA”

***Editing instructions formatted like this (with highlight) are instructions to the TGbh editor.***

***Editing instructions formatted like this are intended to be copied into the TGbh Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***Insert new row in Table 9-51 in 9.4.1.11 (Action field), after the last non-vendor specific entry***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Code** | **Meaning** | **See Subclause** | **Robust** | **Group Addressed Privacy** |
| <ANA> | ID Query | 9.6.30a | Yes | No |
| <ANA+1> - 125 | Reserved | - | - | - |

***Insert new row in Table 9-153 (Extended Capabilities field) in 9.4.2.26***

|  |  |  |
| --- | --- | --- |
| **Bits** | **Information** | **Notes** |
| <ANA> | ID Query Capability | The STA sets ID Query Capability subfield to 1 to indicate the STA supports the ID Query action frame. It is set to 0 to indicate that it does not support this action frame exchange. |

***Add a new subclause at the end of subclause 9.6 (Action frame format details)***

**9.6.30a ID Query Action frame details**

**9.6.30a.1 ID Query Action field**

Two Action frame formats are defined, to allow an AP to query a non-AP STA for a unique identifier and for the non-AP STA to provide a response or unsolicited response. An ID Query Action field, in the octet field immediately after the Category field differentiates the formats. The ID Query Action field values associated with each frame format are defined in Table 9-aaa (ID Query Action field values).

**Table 9-aaa – ID Query Action field values**

|  |  |
| --- | --- |
| ID Query Action field value | Description |
| 0 | ID Query Request |
| 1 | ID Query Response |
| 2-255 | Reserved |

**9.6.30a.2 ID Query Request frame**

The ID Query Request frame uses the Action frame body format. It is transmitted from an AP to a non-AP STA to request that the non-AP STA provide an identifier that the AP may store, and may be used by the AP and infrastructure network for future identification of the non-AP STA. The format of the Action field in the ID Query Request frame is shown in Figure 9-bbb.

|  |  |  |
| --- | --- | --- |
| Category | ID Query Action | Vendor Specific (optional) |

 Octets: 1 1 Variable

**Figure 9-bbb – ID Query Request frame Action field format**

The Category field is defined in 9.4.1.11 (Action field).

The ID Query Action field is defined in 9.6.30a.1 (General).

The ID QueryVendor Specific field is optionally present and includes one or more vendor-specific elements, as defined in 9.4.2.25 (Vendor Specific element).

**9.6.30a.3 ID Query Response frame**

The ID Query Response frame uses the Action frame body format. It is transmitted from a non-AP STA to an AP to provide a unique non-transitory identifier, either unsolicited or in response to a request from the AP. The format of the Action field in the ID Query Request frame is shown in Figure 9-ccc.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Category | ID Query Action | ID Query Response | Length | ID (optional) | TTL (optional) | Vendor Specific (optional) |

Octets: 1 1 1 2 Variable 2 Variable

**Figure 9-ccc – ID Query Response frame Action field format**

The Category field is defined in 9.4.1.11 (Action field).

The ID Query Action field is defined in 9.6.30a.1 (General).

The ID Query Response field is defined in table 9-ccc (ID Query Response field values). The non-AP STA has the option to indicate that it will not provide an ID value or that an ID is provided.

**Table 9-ccc – ID Query Response field values**

|  |  |
| --- | --- |
| ID Query Response field value | Description |
| 0 | Decline to provide ID |
| 1 | ID Provided |
| 2-255 | Reserved |

The Length field indicates the combined length of the ID and TTL fields, in octets.

When the ID Query Response field value is 0, the ID and TTL fields are not present, and the Vendor Specific field is optionally present. When the ID Query Response field value is 1, the ID and TTL fields are present, and the Vendor Specific field is optionally present.

The ID field provides the identification value that the requesting AP may use to identify this non-AP STA without regard to the MAC address used by the STA in the MAC header.

The TTL field is defined in Table 9-ddd (Time to Live field values). The lifetime of the ID is as indicated.

**Table 9-ddd – Time to Live field values**

|  |  |
| --- | --- |
| ID QueryTTL field value | Description |
| 0 | The ID is usable for the duration of this ESS association |
| 1-65533 | The ID is usable for the indicated time to live, in minutes |
| 65534 | The ID is usable for a vendor- or provider-specific period, specified outside the scope of this standard. |
| 65535 | The ID is permanent. |

The ID QueryVendor Specific field includes one or more vendor-specific elements, as defined in 9.4.2.25 (Vendor Specific element).

***Add a new subclause at the end of clause 11 (MLME)***

**11.aa Identification Management**

A non-AP STA may use a local MAC address or an otherwise randomized MAC address before or after association. For some APs and network services, a local MAC address identification of the non-AP STA that may change with each ESS association (or more quickly) will restrict the services that an AP can offer without additional identification.

An AP may use the ID Query Request frame to request that a non-AP STA provide an identifying value that can be used in an implementation-specific manner, across association events, or optionally while not associated, to consistently identify the particular non-AP STA, even if its MAC address changes. The ID Query Request frame may also include Vendor Specific information.

A non-AP STA may respond to an ID Query Request frame with an ID Query Response frame that carries an ID, or a non-AP STA may provide an ID Query Response frame without AP soliticitation. The ID Query Response frame also indicates the amount of time that the AP may expect that ID to be valid in the time to live field. The ID Query Response frame may also include Vendor Specific information.

The ID Query Response frame that carries an ID should be sent after a security context is in place and management frame protection has been negotitated between the requesting AP and the target STA, then the ID in the response will be secure and kept private. If the non-AP STA is associated to the AP, the security context is established as defined in 12.6.19 (Protection of Robust Management Frames), and 12.6.20 (Robust management frame selection procedure). If the non-AP STA is not associated to the AP, the security context is established using the Pre-Association Security Negotiation mechanism as defined in 12.12 (Pre-Association Security Negotiation).

Alternatively, a non-AP STA may respond to an ID Query Request frame with an ID Query Response frame that declines to provide the requesting AP with an ID, for example, if the STA does not trust the AP.

NOTE—The AP’s SME may make the ID available to higher layers. Based on the query response or lack thereof from the non-AP STA, the AP or higher layer facilities might restrict the non-AP STA’s access in an implementation specific manner.

**TBD: Some PASN facilities explicitly mention Fine Timing Measurement frames, and need to be modified to support both Fine Timing Measurement and ID Query Request/Response frames.**