**IEEE P802.11
Wireless LANs**

|  |
| --- |
| **802.11****Active Scan Figure CID** |
| **Date:** 2019-04-08 |
| **Author(s):** |
| **Name** | **Affiliation** | **Address** | **Phone** | **Email** |
| Thomas Derham | Broadcom | 16340 W Bernardo Dr, San Diego CA |  | thomas.derham@broadcom.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Abstract**

This document provides comment resolution for REVmd letter ballot CIDs 2691 and 2008.

R0: Initial draft

R1: Also address CID 2008

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2691 | 11.1.4.3.2 | 2128 | 43 | Figure 11-4 shows "active scanning" with a probe request addressed to an individual address (i.e. where probe request is ACK'ed). However, as indicated in steps (d) and (e), in active scan the probe request(s) are sent to the broadcast destination address. Therefore this figure is very confusing | Modify Figure 11-4 to show an example where the probe request is addressed to broadcast destination address and BSSID is set to a non-wildcard BSSID. (This then correctly contrasts with Figure 11-5 where BSSID field is set to wildcard) |
| 2008 | 11.1.4.3.2 | 2127 | 27 | In active scanning, there is no expectation of an ACK response and as a result, the A1 field is always set to broadcast while the combination of A3 field and SSID determines whether the probe is sent to a single AP (A3=BSSID of the AP) or to a group of APs (e.g., A3=wildcard BSSID with SSID=specific SSID) or to any AP in the neighborhood (e.g., A3=wildcard & SSID=wildcard). | Clarify that reference to 'destination address' here refers to the RA (A1) field in the MAC header of the Probe Request frame.The following locations would also need additional clarification: Figure 11-4 (remove ACK sent in response to Probe Request), 11.1.4.3.10 (P2139L37), 11.46.2.2 (P2496L1) |

**Discussion:** Excerpt of the active scanning procedure in 11.1.4.3.2 where Probe Request frame is transmitted, is copied below. This text explicitly indicates that the Probe Request frame is sent to the broadcast address. These are the only references in this clause to transmission of a Probe Request frame (other than Figures 11-4 and 11-5 themselves). Hence, as far as this clause is concerned, a figure that refers to transmission of Probe Request frames to an individual address is not appropriate and confusing.

* Perform the basic access procedure as defined in 10.3.4.2 (Basic access).
* Send a probe request to the broadcast destination address. The probe request is sent with the SSID and BSSID from the received MLME-SCAN.request primitive. When the SSID List is present in the MLME-SCAN.request primitive, send one or more Probe Request frames, each with an SSID indicated in the SSID List and the BSSID from the MLME-SCAN.request primitive(11ai).
* When the SSID List is present in the invocation of the MLME-SCAN.request primitive, send zero or more Probe Request frames, to the broadcast destination address. Each probe request is sent with an SSID indicated in the SSID List and the BSSID from the MLME-SCAN.request primitive. The basic access procedure (10.3.4.2 (Basic access)) is performed prior to each probe request transmission.

As shown in text above, the SSID and BSSID fields in the Probe Request frame are the primary fields that determine the responder(s) to the Probe Request in active scan [note: in certain cases there are also other filtering criteria, e.g. FILS Request parameters]. Figure 11-5 shows a case with multiple responders, implying BSSID field of the Probe Request frame is set to wildcard address. Currently there is no figure showing the case where the Probe Request frame is sent to the broadcast destination address with a non-wildcard BSSID field, and therefore there is typically a single responder.

With regard to 11.46.2.2 and 11.1.4.3.10, which concern active scan by FILS STAs using APCSN, the text in 11.1.4.3.10 clearly refers to the STA setting A3 (BSSID) field of the Probe Request to the BSSID of the AP, and refers to an “individually addressed BSSID”, suggesting that the “individually addressed” reference is to the BSSID field (A3), not the RA/DA field (A1). However this is confusing because “individually addressed” usually refers to the DA (see definitions in 3.1). This ambiguity should be fixed by clarifying that, as per other active scan cases, the RA/DA is broadcast and it is the BSSID (A3) field that needs to be set to the non-wildcard value equal to the BSSID of the intended AP.

Note there are other clauses where transmission of an individually addressed Probe Request frame is specified. In these cases, the presence of the targeted peer is already assumed, e.g. 11.3.4.3 (obtaining peer’s security policy in IBSS), 11.5.2.2 (Block ACK agreement in IBSS), 11.29.2 (Peer service discovery). These exchanges do not appear materially different to any other acknowledged request/response type exchanges, and therefore do not seem to justify the need for a specific timing diagram. In any case, there are no other references in the standard to either Figure 11-4 or 11-5.

**Proposed Resolution:** Accept 2691, and revise 2008, making the following modifications:

*Request editor to modify Figure 11-4 as follows:*

* Change title to “Active scanning by a non-DMG STA with a probe request addressed to a specific BSSID” (and update reference in the text accordingly)
* Replace with the figure below (Visio files has been provided to Editor)

Note: Changes are: under “PROBE” (in Probe Request box), “RA = broadcast” and “BSSID = specific” is added; “ACK” and “G1” are removed and shifted start of G2 to align with end of Probe Request (same as Figure 11-5)



*Request editor to modify Figure 11-5 as follows:*

* Replace with the figure below (Visio file has been provided to Editor)
	+ Note: Changes are: under “PROBE” (in Probe Request box), add “RA = broadcast” and “BSSID = wildcard”



*Request editor to modify 11.1.4.3.10 as follows:*

A FILS non-AP STA may send~~, to an AP, an individually addressed~~  a Probe Request frame that includes an AP-CSN element (as defined in 9.4.2.181 (AP Configuration Sequence Number (AP-CSN) element(11ai))) if the STA has the BSS Configuration Parameter Set associated with the AP-CSN of ~~the~~ an AP. When sending such a Probe Request frame, the FILS non-AP STA shall send it to the broadcast destination address and set the Address 3 (BSSID) field in the Probe Request frame to the BSSID of the AP.

When a FILS AP receives a Probe Request frame with an AP-CSN element~~, an individually addressed~~ where the Address 3 (BSSID) field matches the BSSID of this AP, and the criteria for responding to a Probe Request frame(Ed) (11.1.4.3.4 (Criteria for sending a response(11ai))) are met, the AP sends a Probe Response frame according to comparison result, as follows: