**IEEE P802.11
Wireless LANs**

|  |
| --- |
| **802.11****Individually addressed probes CID2216** |
| **Date:** 2019-05-02 |
| **Author(s):** |
| **Name** | **Affiliation** | **Address** | **Phone** | **Email** |
| Thomas Derham | Broadcom | 16340 W Bernardo Dr, San Diego CA |  | thomas.derham@broadcom.com |
| Laurent Cariou | Intel |  |  |  |
| Po Kai Huang | Intel |  |  |  |
|  |  |  |  |  |

**Abstract**

This document provides comment resolution for REVmd letter ballot CID 2216.

R0: Initial draft

R1: Add figure and co-authors

R2: Language improvements

R3: Fix figure

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2216 | 11.1.4.3.2 | 2127 | 27 | The definition of active scanning is still confusing, it is covering all probe request transmissions or only a category of them? In this subclause, it is a requirement for the STA to send a  probe request to the Broadcast address. However, it is possible to send a unicast probe request and STAs on the field today do send unicast probe requests. | Unicast probe request should be allowed in section 11.1.4.3.2 or the definition of what active scanning is in this section 11.1.4.3.2 should be clarified in order to reflect the situation on the field today. |

**Discussion:** Excerpt of the active scanning procedure in 11.1.4.3.2 for non-DMG STAs 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. Therefore, agree with commenter that, when sending non-DMG probe requests in active scan (i.e. when triggered by an MLME-SCAN.request primitive with ScanType parameter indicating active scan), the clause requires that probe requests are always sent to the broadcast DA/RA. The A3 (BSSID) field, among others, determines whether or not an AP responds to a probe request as specified in 11.1.4.3.4 (Criteria for sending a response).

* 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.

Active scan is used by a STA to discover the presence of APs, as described in:

* 4.5.3.3 (Association): “For details of how a STA learns about what APs are present, see 11.1.4 (Acquiring synchronization, scanning).”
* 6.3.3.2.1 “[MLME-SCAN.request] primitive requests a survey of potential BSSs that the STA can later elect to try to join.”

Since, in active scan, the (in-range) presence of an AP is unknown a-priori, even in cases where only a single AP is targeted, the current active scan requirements are appropriate, in order to avoid airtime overhead caused by invoking the retransmit mechanism if the targeted AP is not present.

However, there are use cases where the presence of an AP is already confirmed but it is still desirable or necessary to send a probe request to that AP. In some such cases it may be preferred to send an individually addressed probe request for reliable delivery. Note there are multiple clauses in the current standard where the STA is recommended or required to send a probe request frame outside the context of active scan, and in some cases it is explicitly stated that this is individually addressed. Examples:

* 12.6.1.1.1 – “In order to set up a security association to a peer STA, a SME that does not know the security policy of the peer should send a Probe Request frame to the peer STA to find its security policy before setting up a security association to the peer STA”
* 10.2.3.2 – “If the EDCA Parameter Set update count value in the QoS Capability element is different from the value that has been stored, the QoS STA shall query the updated EDCA parameter values by sending a Probe Request frame to the AP.”
* 10.47.2 – “The S1G STA shall either be awake to receive the next S1G Beacon frame that is transmitted at a TBTT or shall queue for transmission a Probe Request frame when it receives a Change Sequence field that contains a value that is different from the previously received Change Sequence field.”
* 11.2.4.4 – “A STA shall indicate its power management mode in the Power Management subfield of the Frame Control field of frames containing all or part of a BU or individually addressed Probe Request frame, or (QoS) Null frames, that it transmits.”
* 11.5.2.2 – “If the initiating STA is an HT STA, is a member of an IBSS, and has no other existing block ack agreement with the recipient STA, then the initiating STA shall transmit a Probe Request frame to the recipient STA and shall not transmit an ADDBA Request frame unless it receives a Probe Response frame from the recipient.”
* 11.29.2 – “To query available services in a BSS, a non-AP and non-PCP STA shall send either an Information Request frame or a Probe Request frame to the AP or PCP (11.29.1 (Information Request and Response)).”

There may be other similar use cases that are not explicitly documented and, as the commenter mentions, are implemented in commercial devices.

In order to clarify the conditions under which individual and broadcast addressed Probe Request frames can be transmitted, it is proposed to resolve the comment by (a) generalizing the title of 11.1.4.3 to cover probing procedures in general (not just active scan), and (b) adding a subclause that explicitly permits transmission of a probe request to a peer STA that has already been discovered with either individual or broadcast destination address, and a note clarifying that the active scan procedure (using broadcast DA in non-DMG case) is used when presence of the peer STA has not yet been determined.

Note MinChannelTime and MaxChannelTime are specified in MLME-Scan.request primitive, so (unlike similar figures in the active scan clause) are not shown in the figure in this subclause.

**Proposed Resolution:** Revise 2216 by making the following modifications:

*Request editor to modify the title of 11.1.4.3 from “Active scanning” to “Active scanning and probing procedures”*

*Request editor to add the following section between 11.1.4.3.7 and 11.1.4.3.8: (Note: Visio file for the figure is available)*

**11.1.4.3.7a. Non-scanning probe request transmission**

A STA may send an individually addressed or broadcast addressed Probe Request frame to a peer STA that it has determined is within range of itself, in order to solicit information contained within a response frame, see 11.1.4.3.8 (Contents of a probe response). When the Probe Request frame is sent to the broadcast address, Address 3 (BSSID) field shall be set to the MAC address of the peer STA.

NOTE – A STA might determine that a peer STA is within range of itself by, for example, successfully receiving a frame from that peer STA or, if the peer STA is an AP, by successfully receiving a frame from another AP that corresponds to a co-located BSS of the AP.

NOTE -- Transmission of an individually addressed frame can provide more reliable delivery to a peer STA since it is acknowledged (as shown in Figure 9-XX (Probe request addressed to an individual address)) and retransmit procedures apply. When a STA has not determined that a peer STA is in range of itself, Probe Request frames it sends to discover the peer STA are transmitted in accordance with the active scanning procedures in 11.1.4.3. For a non-DMG STA, such Probe Request frames are always sent to the broadcast address.



Figure 9-XX -- Probe request addressed to an individual address