IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution of MAC Privacy CIDs | | | | |
| Date: 2017-07-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 3333 Scott boulevard, Santa Clara, California, United States of America | 408-555-1212 | spamme@gmail.com |
|  |  |  |  |  |

Abstract

This submission proposes resolutions to the CIDs from the 2nd recirculation of the 11aq draft in the tab labelled “MAC Privacy”.

***CID 8019***

Comment: “The MIB variable ‘dot11MACPrivacyActivated’ does not appear to have been defined”

Proposed Change: “Provide a definition of ‘dot11MACPrivacyActivated’ in clause C.3 within the OBJECT-TYPE definitions”

Proposed Resolution: Revised

***Instruct the editor to add the following to Annex C.3 as a new OBJECT-TYPE definition:***

dot11MACPrivacyActivated OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity or the SME. Changes take effect as soon as practical in the implementation. This attribute when true, indicates that the STA to enable MAC privacy considerations. The capability is disabled otherwise."

DEFVAL {false}

::= { dot11StationConfigEntry 170 }

***CID 8047***

Comment: “’a non-AP STA uses’ implies all non-AP STAs will always do this. But, these privacy enhancements are not universally used.”

Proposed Change: “Change ‘uses’ to ‘may use’”

Discussion: This sentence is in the context of a STA that is trying to mitigate traffic analysis. So the idea that it is implied that the text implies all STAs will do this is not universally recognized. “may” is normative and since the commentor (in fact all commetors) did not have a problem with the following “can”, to use that word.

Proposed Resolution: Revised

***Instruct the editor to modify the following text in section 4.5.4.10 as follows:***

To mitigate this sort of traffic analysis a STA can support the ability to periodically and randomly change its MAC addresses and reset counters and seeds prior to association. Post-association, a non-AP STA may use a unique random MAC address with a single sequence number space and seeded data scrambler for an established network connection. While discovering networks, a STA can refrain from gratuitously transmitting Probe Request frames containing SSIDs of favored BSS networks.

***CID 8053***

Comment: “Is this supposed to be a normative requirement?”

Proposed Change: “Change ‘invokes’ to ‘shall invoke’”

Proposed Resolution: Accept.

***CID 8055***

Comment: “This sentence sounds like the complete list of times when the STA shall defer changing its MAC address, but it is not complete.”

Proposed Change: “Add ‘during association to a BSS or ESS, or’ before ‘during a transactional exchange’"

Proposed Resolution: Accept.

***CID 8056***

Comment: “The requirement to change a STA's MAC address ‘prior’ to establishing a connection is: 1) contradictory with 2 paragraphs down that says it is static during association to an ESS; 2) breaks any pre-association negotiations (pre-auth, FT over-the-DS, etc.; and 3) is ambiguous in terms of how much prior to establishing the connection, and what point is determined to ‘establishing a connection’ (for example, should it be after the Authentication, but before Association? clearly, not.)”

Proposed Change: “Change ‘shall’ to ‘should’, and add explanation that the change can only occur if there are no persistent agreements in place with the new BSS's AP.”

Discussion: 1) The problematic text clearly says “prior to”. Two paragraphs down it says a STA “shall retain a single MAC address for the duration of its connection across an ESS.” You cannot be inside the duration of anything if you are doing it prior to entering the period of duration starting so there is no contradiction; 2) true; and, 3) text describing any recommended time would not have an impact on interoperability and it does not seem appropriate to constrain a device for no practical reason. Regarding after Authentication but before Association, Authentication advances the state machine and therefore has state to be maintained. It is therefore a transactional exchange and part of the “connection.”

Changing the “shall” to a “should” looks like comment bait in the belief that the next round someone else will request text explaining the circumstances under which a STA who wants to do privacy considerations would decide not to randomize the MAC address. Keeping in mind point 2, there does need to be some text to explain that there are transactional exchanges—pre-auth FT over-the-DS, etc—that contain state bound to the MAC address that generated it and the MAC address should not be changed.

Proposed Resolution: Revised

***Instruct the editor to modify the following text in section 12.2.10 as follows:***

To enable MAC privacy enhancements during discovery, BSS transition, and membership; a non-AP STA shall set dot11MACPrivacyActivated to true. When dot11MACPrivacyActivated is true, a non-AP STA shall periodically change its MAC address to a random value. However, the non-AP STA shall not change its MAC address during a transactional exchange, for example transmitting public action frames for pre-association discovery, or during the creation of state on an AP STA using pre-association capabilities, for example pre-authentication, FT over-the-DS, etc. The smaller the period of MAC address change, down to a single transmitted frame per MAC address, the greater the privacy these enhancements afford. The actual period used when changing a MAC address is implementation dependent and outside the scope of this standard.

A STA that discovers a BSS of interest, wishes to establish a connection, and does not have any transactional state bound to a random MAC address, shall change its MAC address to a random value prior to establishing a connection to the BSS. A STA that attemps to establish a connection using state established with an AP STA using a prior random MAC address—for instance pre-authentication state or FT state established over-the-DS—shall change its MAC address back to the MAC address used when the state was created. Once connected, it shall retain that MAC address for the duration of its BSS connection.

***CID 8057***

Comment: “No need to generate 48 bits of random value, and then bash 2 of them to fixed values. Just generate 46 bits.”

Proposed Change: “Change to ‘To set a random MAC address, a STA shall set the sixth bit ... and the seventh bit ... and shall assign a random 46-bit value to the remaining bits.’"

Discussion: As the 46-bits are not contiguous the suggested change is potentially confusing—how do you assign a 46-bit value to two distinct bits of memory?

Proposed Resolution: We could reject this because randomness is usually generated in units of 8 bits and the easiest thing to do is follow the existing text. Or we could choose: Revised,

***Instruct the editor to modify the following text in section 12.2.10 as follows:***

To construct a random MAC address, a STA shall set the sixth bit of the first octet to one (indicating a locally administered MAC address) and the seventh bit of the first octet to zero (indicating unicast) and shall assign random values to the remaining 46 bits. Using 46 bits of randomness ensures that the probability of random MAC address collision on even the largest networks remains acceptably small.

***CID 8059***

Comment: “Regarding ‘Post-association, a non-AP STA uses a unique random MAC address ... for an established network connnection.’, today, most STAs use their globally unique MAC addresses for post-association connection. Is the cited sentence meant to be a requirement (or at least a recommended practice) as a part of the MAC privacy enhancements in order not to reveal the globally unique MAC address of the STA? If it is intended to be a requirement or a recommended practice, should make it clear.”

Proposed Resolution: Please clarify.

Discussion: The MAC address used by a STA implememting privacy considerations has to be random, and not the globally unique MAC address, otherwise the traffic analysis qualities of privacy considerations are obviated. Should mention that the MAC address is locally generated and leave the uniqueness guarantees to the normative text that describes how to generate a MAC address.

Proposed Resolution: Revised

***Instruct the editor to modify the following text in section 4.5.4.10 as follows:***

To mitigate this sort of traffic analysis a STA can support the ability to periodically and randomly change its MAC addresses and reset counters and seeds prior to association. Post-association, a non-AP STA uses a locally-generated random MAC address with a single sequence number space and seeded data scrambler for an established network connection. While discovering networks, a STA can refrain from gratuitously transmitting Probe Request frames containing SSIDs of favored BSS networks.

**References:**