IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment Collection 09 MAC CIDs (Comment Resolutions for CC09) |
| Date: 2013-07-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Minynoung Park | Intel Corporation |  |  | minyoung.park@intel.com |
| Haiguang Wang | I2R |  |  | hwang@i2r.a-star.edu.sg |
| Zander Lei | I2R |  |  | leizd@i2r.a-star.edu.sg |

Abstract

This document provides resolutions for CIDs: 186, 482

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Clause**  | **Page** | **Line** | **Resn Status** | **Comment** | **Proposed Change** | **Resolution** |
| 186 | 10.3.7 | 174 | 6 | V | In section 10.3.7 of draft 0.1, behaviors of AP in Authentication Control is defined but the behavior of STA is still TBD. | Modify the test in 10.3.7 as follows:When a STA for which dot11S1GAuthenticationControlActivated is true receives a beacon from the AP that the STA intends to join including an Authentication Control element, the behavior is TBD., it may compare the Authentication Control threshold with a random number generated locally. If the random number is less than the Authentication Control threshold, it is allowed to transmit the Authentication Request to AP. Else, the STA shall listen to the beacon for further update on Authentication Control Threshold. | Revised – see document doc.: IEEE 802.11-13/0785r1 for the resolution. |
| 482 | 10.3.7 | 174 | 6 | V | The behavior of a STA below "A STA for which supports authentication control sets dot11S1GAuthenticationControlActivated to true and set dot11S1GAuthenticationControlPause to false when it is initialized.When a STA for which dot11S1GAuthenticationControlActivated is true receives a beacon from the AP thatthe STA intends to join including an Authentication Control element, the behavior is TBD.When a STA for which dot11AuthenticationControlActivated is true receives a beacon from an AP that it isintended to join does not include an Authentication Control element, it shall set dot11AuthenticationPauseto false." is not defined. Define the behavior of a STA so that the contention problem due to a large number of authentication request frames can be spread over a period of time, which can mitigate the contention. | Delete P174/L6 to P174/L16 and define a STA's behavor by adding the following paragraphs after P174/L4:"When dot11S1GAuthenticationControlActivated is true, an AP shall include an Authentication Control element in a beacon. Otherwise, the Authentication Control element shall not be included in a beacon.When a STA receives a beacon with an Authentication Control element from the AP with which the STA intends to join and if the STA intends to transmit an Authentication Request frame to the AP, the STA shall generate a random number m between [0, n], where n is the Authentication Control Threshold field value in the Authentication Control element and shall access the medium to transmit an Authentication Request frame not earlier than m TUs after the reception of a frame that contained the Authentication Control element." | Revised – see document doc.: IEEE 802.11-13/0785r1 for the resolution. |

**Discussion on CID 186 and 482:**

The STA's behavior under the association and authentication control was not defined in sub clause 10.3.7. This resolution provides the STAs' detailed behaviors which are dependent on either a centralized control approach or a distributed control approach. The STA's behavior in the centralized authentication and association control is specified in 10.3.7.1 whereas the behavior in the distributed control is specified in 10.3.7.2.

**Proposed changes:**

**[CID 186]**

* MLME-AUTHENTICATE.request
* Function
* Semantics of the service primitive
* When generated

 ***Modify section 6.3.5.2.3 as follows :***

When dot11S1G~~Option~~CentralizedAuthenticationControlActivated~~Implemented~~ is true, a STA for which dot11S1GAuthentication~~Pause~~RequestTransmission is ~~true~~ false shall not generate this primitive.

***Insert a subclause title 10.3.7.1 Centralized authentication control after the first paragraph of subclause 10.3.7 as follows:***

**10.3.7.1 Centralized authentication control**

When dot11S1GCentralizedAuthenticationControlActivated is true, AP may limit the number of STAs that can transmit Authentication Request to it by ~~broadcasting~~ including the Authentication Control element in a beacon or a Probe Response. AP can adjust the value of Authentication Control Threshold within the element from beacon to beacon.

When dot11S1GCentralizedAuthenticationControlActivated is false, AP shall not include the Authentication Control element with the Control field set to 0 in a beacon or Probe Response.

A STA for which supports ~~authentication control~~ Centralized Authentication Control sets dot11S1GCentralizedAuthenticationControlActivated to true and set dot11S1GAuthentication~~ControlPause~~RequestTransmission to ~~false~~ true when it is initialized.

A STA for which dot11S1GCentralizedAuthenticationControlActivated is true, it shall generate a random number for dot11S1GCentralizedAuthenticationControlValue when it is initialized. The generated random number is uniformly distributed between [0, 1022]. To avoid unfairness in opportunity of Authentication Request transmission in future, a STA may regenerate a random number for dot11AuthenticationCentralizedControlValue after receiving Authentication Response from AP.

When a STA for which dot11S1GCentralizedAuthenticationControlActivated is true receives a beacon or Probe Response from the AP that the STA intends to join including an Authentication Control element with the Control field set to 0, ~~the behavior is TBD.~~ if it intends to send an Authentication Request to an AP, it shall compare dot11S1GCentralizedAuthenticationControlValue with the Authentication Control Threshold value contained in the Authentication Control element received from the AP in last beacon. If dot11S1GCentralizedAuthenticationControlValue is less than the value of Authentication Control Threshold of the respective Authentication Control element, the STA may transmit Authentication Request to the AP and the STA shall set dot11S1GAuthenticationRequestTransmission to true. Otherwise, STA shall set dot11S1GAuthenticationRequestTransmission to false and STA shall not transmit Authentication Request to the AP.

When a STA for which dot11S1GCentralizedAuthenticationControlActivated~~Implemented~~ is true receives a beacon or Probe Response from an AP that it is intended to join does not include an Authentication Control element with the Control field set to 0, it shall set dot11S1GAuthentication~~Pause~~RequestTransmission to ~~false~~true.

A STA for which dot11S1GCentralizedAuthenticationControlActivated is false is not constrained by the Authentication Control rules defined in this subclause when it transmits Authentication Request to AP.

**[CID 482]**

***Insert a new subclause 10.3.7.2 at the end of subclause 10.3.7 as follows:***

**10.3.7.2 Distributed authentication control**

When dot11S1GDistributedAuthenticationControlActivated is true, an S1G AP shall set the Distributed Authentication Control bit to 1 in the S1G Capabilities Info field of the S1G Capabilities element. Otherwise, the bit is set to 0.

When an S1G STA receives an S1G Capabilities element with the Distributed Authentication Control field set to 1, the STA shall determine when to access the medium to transmit an Authentication Request frame based on the following procedure:

1. The STA maintains the following distributed authentication control (DAC) parameters:
	1. Authentication control slot duration (Tac) in TU units. The default value is set to 10 TUs.
	2. Minumum transmission interval (TImin) in BI units. The default value is set to 8 BIs.
	3. Maximum transmission interval (TImax) in BI units. The default value is set to 256 BIs.
2. The STA maintains a transmission interval (TI) in BI units.
	1. The TI is initialized to TImin.
3. The STA chooses a random number *m* from [0, TI].
4. The STA chooses a random number *l* from [0, L], where $L=\left⌊BI/T\_{ac}\right⌋$, *l*=0 is the first authentication control slot
5. The STA accesses the medium to transmit an Authentication Request frame at the beginning of the *l*-th authentication control slot in the *m*-th BI, where *m*=0 is the current BI.
6. If the transmission of the Authentication Request frame fails, the TI is increased as follows:
TI = min{2×TI, TImax}.

An S1G AP may assign DAC parameters different from the default values by sending to the STA an Authentication Control element with the Control field set to 1. An S1G STA receiving the Authentication Control element shall update its MIB values of the DAC parameters based on the values received in the Authentication Control element.

**8.4.2.170k.1 S1G Capabilities element structure**

***Modify Figure 8-401df – S1G Capabilities element format in subclause 8.4.2.170k.1 as follows:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element ID | Length | S1G Capabilities Info | TBD |
| Octets: | 1 | 1 | 2 | m (TBD) |
| * **S1G Capabilities element format**
 |

**8.4.2.170k.2 S1G Capabilities Info field**

***Modify Figure 8-401dg – S1G Capabilities Info field in subclause 8.4.2.170k.2 as follows:***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | B0 | B1 | B2 | B3 | B4 | B5 | B6 B7 |
|  | Uplink Synch Capable | DynamicAID | BATSupport | TIM ADESupport | Non-TIMSupport | TWTSupport | STA TypeSupport |
| Bits: | 1 | 1 | 1 | 1 | 1 | 1 | 2 |

|  |  |  |
| --- | --- | --- |
|  | B8 | B9 B10 B15 |
|  | Centralized Authentication Control | Distributed Authentication Control | reserved |
| Bits: | 1 |  1 6 |
| * **S1G Capabilities Info field**
 |

***Insert a row at the end of Table 8-191d – Subfields of the S1G Capabilities Info field as follows:***

|  |
| --- |
| * **Subfields of the S1G Capabilities Info field**
 |
| Subfield | Definition | Encoding |
| Centralized Authentication Control | This field indicates support of the centralized authentication control defined in 10.3.7.1. | Set to 1 if dot11S1GCentralizedAuthenticationControlActivated is true. Set to 0 otherwise. |
| Distributed Authentication Control | This field indicates support of the distributed authentication control defined in 10.3.7.2. | Set to 1 if dot11S1GDistributedAuthenticationControlActivated is true. Set to 0 otherwise. |

**8.4.2.170o Authentication Control element**

***Modify the first paragraph in subclause 8.4.2.170o:***

The Authentication Control element contains the information required to mitigate contention among Authentication Request frames (see 10.3.7).

When the Control subfield is set to 0, the Authentication Control element format is as shown in Figure 8-401dj. The Authentication Control element indicates to STA whether it may transmit an Authentication Request frame to the AP which sends the element. The Information field contains only one field, the Authentication Control Threshold. The total length of the Information field is 2 octets. See Figure 8-401dj (Authentication Control element format).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Bits: |  |  | B0 | B1 B5 | B6 B15 |
|  | Element ID | Length(=2) | Control(0) | Reserved | AuthenticationControl Threshold |
| Octets: | 1 | 1 |  | 2 |
|  | Figure 8-401dj – Authentication Control element format (Control subfield = 0) |

The Authentication Control Threshold is a number and varies from 0 to 1023.

When the Control subfield is set to 1, the Authentication Control element contains the distributed authentication control (DAC) parameters as shown in Figure 8-401dj1.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Bits: |  |  | B0 | B1 B7 | B8 B15 | B16 B23 |
|  | Element ID | Length(=3) | Control(1) | AuthenticationSlot Duration | MaximumTransmissionInterval | MinimumTransmissionInterval |
| Octets: | 1 | 1 | 3 |
| Figure 8-401dj1 – Authentication Control element format (Control subfield = 1) |

The Authentication Slot Duration subfield is 6-bit unsigned integer, expressed in TUs, and indicates the authentication slot duration.

The Minimum Transmission Interval subfield is 1-octet unsigned interger, expressed in BIs, and indicates the minimum transmission interval.

The Maximum Transmission Interval subfield is 9-bit unsigned interger, expressed in BIs, and indicates the maximum transmission interval.**References:**