IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB205 MAC Resolution to Comments in D3.0 Subclauses 8.4.2.170m and 10.3.8.1 | | | | |
| Date: 2014-12-1 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Zander Lei | I2R | 1 Fusionopolis Way #21-01 Connexis, Singapore | +65 6408 2436 | leizd@i2r.a-star.edu.sg |
| Shoukang Zheng | +65 6408 2252 | skzheng@i2r.a-star.edu.sg |
| Yuan Zhou | +65 6408 2472 | yzhou@i2r.a-star.edu.sg |

Abstract

This submission proposes resolution to comments in D3.0 subclauses 8.4.2.170m and 10.3.8.1. There are 8 CIDs addressed: 5192, 5450, 5338, 5462, 5463, 5464, 5465, and 5466

Revision History:

Rev1:

**Interpretation of a Motion to Adopt:** A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGah Draft. This introduction is not part of the adopted material.

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

***TGah Editor: Editing instructions preceded by “TGah Editor” are instructions to the TGah editor to modify existing material in the TGah draft. As a result of adopting the changes, the TGah editor will execute the instructions rather than copy them to the TGah Draft.***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5192 | 162.10 | 8.4.2.170m | When is the start time of deferral time? | Clarify it. | Revised.  Agreed in principle.  (A link to 10.3.8.1 is provided instead of repeating text.)  TGah editor to make the changes shown in 11-14/1576r0 under all headings that include CID 5192. |
| 5450 | 162.27 | 8.4.2.170m | The fragment "is used by the recipient STA to determine whether or not it is permitted to transmit an Authentication-Request frame." is ambiguous as to what entity controls this permission | Replace "is used by the recipient STA to determine whether or not it is permitted to transmit an Authentication-Request frame." with "is used by the recipient STA to determine whether or not the AP is permitting it to transmit an Authentication-Request frame." | Revised.  Agreed in principle.  TGah editor to make the changes shown in 11-14/1576r0 under all headings that include CID 5450. |

**[CID 5192,5450]**

**Instruction to TGah editor: Please modify the subclause 8.4.2.199 (Authentication Control element) of TGah D3.1 as follows:**

(Pg162)

The Element ID and Length fields are defined in 8.4.2.1 (General).

The Information field starts with a 1-bit Control subfield.

When the Control subfield is equal to 0, the Authentication Control element format is as shown in Figure 8-575a32 (Authentication Control element format (Control subfield=0)). The Authentication Control element indicates ~~to~~ whether the recipient STA ~~whether it~~ can transmit an Authentication Request frame to the AP which sends the element. The ~~Information field~~ remaining part of the Centralized Authentication Control Parameters field following the Control subfield contains the Deferral, Reserved and the Authentication Control Threshold subfields. The Deferral subfield ~~is 1 bit~~ and the Authentication Control Threshold subfield are ~~is~~ 1 bit and 10 bits in length respectively. ~~See Figure 8-575a32 (Authentication Control element format (Control subfield = 0)).~~

The Centralized Authentication Control Parameters field format is shown in Figure 8-575a33 (Centralized Authentication Control Parameters format).

(Figure 8-575a33)

The Authentication Control Threshold subfield contains a number with a range from 0 to 1023. When the Deferral subfield is equal to 0, the value of the Authentication Control Threshold subfield is used by the recipient STA to determine whether or not ~~it is permitted~~ AP is permitting it to transmit an Authentication-Request frame. When the Deferral subfield is equal to 1, the Authentication Control Threshold subfield value is a time value, expressed in TUs, indicating a minimum amount of deferred time for channel access which is required before the transmission of an Authentication-Request frame, as described in 10.3.8.1 (Centralized authentication control).

… …

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5338 | 345.04 | 10.3.8.1 | The same MIB variable appears literally in almost every paragraph of this subclause which creates a lot of redundancy and does not help much. Suggest using the terminology proposed to resolve this issue. | Insert the following sentence at the end of this paragraph: "An S1G STA with dot11S1GCentralizedAuthenticationControlActivated equal to true is a CA controller AP if the STA is an AP and is a CA controlled STA if the STA is a non-AP STA."  Use the new terminology throughout the subclause to avoid calling the MIB valiable again and again. | Revised.  Agreed in principle.  TGah editor to make the changes shown in 11-14/1576r0 under all headings that include CID 5338. |
| 5463 | 345.06 | 10.3.8.1 | "equal to 0 shall not follow the rules in this subclause": how is this a requirement? Is the STA required to violate every rule in the subclause? A STA that doesn't violate one of the rules is nonconformant? Also, does "this subclause" mean 10.3, 10.3.8 or just 10.3.8.1. | Either specify exactly which rules the STA shall violate or replace the fragment "equal to 0 shall not follow the rules in this subclause" with "equal to 0 is not constrained by the requirements specified in 10.3.8.1." | Revised.  Agreed in principle.  TGah editor to make the changes shown in 11-14/1576r0 under all headings that include CID 5463. |
| 5464 | 345.09 | 10.3.8.1 | "When dot11S1GCentralizedAuthenticationControlActivated is true at an AP" implies that there is some repository of dot11 variables out there for which STAs/APs may set values. Replace this with a clearer indication the STA/AP may implement this variable (or not). | Replace "When dot11..." with "When the AP's dot11..." and delete "at an AP" on lines 9, 12, 15 and 24. On page 346 line 21 replace "When dot11... is true, an S1G AP shall set" with "When an S1G AP's dot11... is true, it shall set". | Revised.  Agreed in principle (following suggestion in CID5338).  TGah editor to make the changes shown in 11-14/1576r0 under all headings that include CID 5464. |
| 5465 | 345.19 | 10.3.8.1 | The following is obviously true, since an AP can always do this: "The AP can transmit a different value in the Authentication Control Threshold subfield ...." The importance of this concept is that this amendment is giving the AP \_permission\_ to do this -- so the "can" should be a "may". | Replace "can" with "may". | Revised.  Agreed in principle.  TGah editor to make the changes shown in 11-14/1576r0 under all headings that include CID 5465 |
| 5466 | 345.30 | 10.3.8.1 | A standard is much clearer if it varies phrasing in descriptions only when it is specifying variations in the requirements it is presenting. (In other words, boring repetition is needed when the specifications are not varying -- a standard is not high literature.) The various forms of the statements that begin "A STA with the value of true for dot11..", "A STA with dot11... equal to true", etc. need to be reduced to one form (and that form should be similar to the form of the statements about APs, except only the differences necessary to express the different specifications. | On line 30 replace "the receiving STA with dot11... equal to true shall not" with "the receiving STA whose dot11... is true shall not". On line 33 replace "STA with the value of false for dot11.. Is not" with "STA whose dot11... is false is not". On line 33 replace "A STA that has a value of true for dot11... shall generate" with "A STA whose dot11... is true shall generate". On line 47 replace "A STA with a value of true for dot11... shall compare" with "A STA whose dot11... is true shall compare". On line 55 replace "The STA with dot11... equal to true shall" with "The STA whose dot11... is true shall". On line 60 replace "A STA with dot11... equal to true shall" with "A STA whose dot11... is true shall". And on page 346 line 6 replace "A STA with dot11... equal to true shall" with "A STA whose dot11... is true shall". | Revised.  Agreed in principle (following suggestion in CID5338).  TGah editor to make the changes shown in 11-14/1576r0 under all headings that include CID 5466 |
| 5462 | 345.06 | 10.3.8.1 | The value of the Centralized Authentication Control subfield is not a property of the STA, but something that the STA transmits. | Replace "A STA with the Centralized Authentication Control subfield equal to 0 shall" with "A STA that transmits 0 as the value of the Centralized Authentication Control subfield of the S1G Capabilities Info field shall". | Revised.  Agreed in principle.  TGah editor to make the changes shown in 11-14/1576r0 under all headings that include CID 5462 |

**[CID 5338, 5462, 5463, 5464, 5465, 5466]**

**Instruction to TGah editor: Please insert the following definitions in the subclause 3.2 (Definitions specific to IEEE 802.11) of TGah D3.1 as follows:**

**centralizd authentication controller access point (CAC AP):** An S1G AP with dot11S1GCentralizedAuthenticationControlActivated equal to true.

**centralizd authentication controlled station (CAC STA):** An S1G non-AP STA with dot11S1GCentralizedAuthenticationControlActivated equal to true.

**[CID 5338, 5462, 5463, 5464, 5465, 5466]**

**Instruction to TGah editor: Please modify the subclause 10.3.8.1 (Centralized authentication control) of TGah D3.1 as follows:**

**10.3.8.1 Centralized authentication control**

When dot11S1GCentralizedAuthenticationControlActivated is true, an S1G STA shall set the Centralized Authentication Control subfield to 1 in the S1G Capabilities Info field of the S1G Capabilities element. Otherwise, the STA shall set it to 0. A STA ~~with~~ that transmits 0 as the value of the Centralized Authentication Control subfield of the S1G Capabilities Info field ~~equal to 0~~ ~~shall not follow the rules defined in this subclause~~ is not constrained by the requirements specified in 10.3.8.1 (Centralized authentication control). An S1G STA with dot11S1GCentralizedAuthenticationControlActivated equal to true is a CAC AP if the STA is an AP and is a CAC STA if the STA is a non-AP STA.

~~When dot11S1GCentralizedAuthenticationControlActivated is true at an AP, the~~ A CAC AP shall set the Control subfield to 0 in the Authentication Control element in all transmitted Beacons and Probe Responses frames. ~~When dot11S1GCentralizedAuthenticationControlActivated is false at an AP, the~~ A non-CAC AP shall not include an Authentication Control element with the Control field equal to 0 in a Beacon or Probe Response frame.

~~When dot11S1GCentralizedAuthenticationControlActivated is true at an AP, the~~ A CAC AP may include an Authentication Control element with the Control subfield equal to 0 and the Deferral subfield equal to 0 in a Beacon or a Probe Response frame to attempt to limit the number of STAs that can transmit an Authentication Request frame to it. The AP ~~can~~may transmit a different value in the Authentication Control Threshold subfield in the Authenticaiton Control element included in each of Beacon and Probe Response frames that it transmits.

~~When dot11S1GCentralizedAuthenticationControlActivated is true at an AP, the~~ A CAC AP may include, within an individually addressed Probe Response frame that is transmitted in response to a Probe Request frame from a STA, an Authentication Control element that has the Control subfield equal to 0, the Deferral subfield equal to 1 and the Authentication Control Threshold subfield equal to a deferred channel access time. During the deferred channel access time that begins immediately following the reception of the Probe Response, ~~the~~ a CAC receiving STA ~~with dot11S1GCentralizedAuthenticationControlActivated equal to true~~ shall not transmit an Authentication Request frame to the AP that transmitted the Probe Response.

A non-CAC STA ~~with the value of false for dot11S1GCentralizedAuthenticationControlActivated~~ is not constrained by the Authentication Control rules defined in ~~this subclause~~ 10.3.8.1 (Centralized authentication control) when it transmits an Authentication Request frame to the AP. A CAC STA ~~that supports Centralized Authentication Control sets dot11S1GCentralizedAuthenticationControlActivated to true and~~ sets the local MAC variable AuthenticationRequestTransmission to true when it is initialized.

A CAC STA ~~that has a value of true for dot11S1GCentralizedAuthenticationControlActivated~~ shall generate a random number *v* when it is initialized. The generated random number *v* shall be uniformly distributed between 0 and 1022 (inclusive). The STA may generate a new random value for *v* after receiving an Authentication Response from an AP.

A CAC STA ~~that has a value of true for dot11S1GCentralizedAuthenticationControlActivated~~ shall compare *v* with the Authentication Control Threshold subfield value in the most recently received Authentication Control element from the AP to which it intends to send an Authentication Request frame if the Control and the Deferral subfields are equal to 0. If *v* is less than the value of the Authentication Control Threshold subfield, the STA may transmit an Authentication Request frame to the AP and shall set the local MAC variable AuthenticationRequestTransmission to true. Otherwise, the STA shall set the local MAC variable AuthenticationRequestTransmission to false and the STA shall not transmit an Authentication Request frame to the AP. ~~The~~ A CAC STA ~~with~~ ~~dot11S1GCentralizedAuthenticationControlActivated equal to true~~ shall update its MIB values of the CAC parameters based on the values received in the Authentication Control element.

A CAC STA ~~with dot11S1GCentralizedAuthenticationControlActivated equal to true~~ shall set the local MAC variable AuthenticationRequestTransmission to false and shall defer the transmission of an Authentication Request frame to an AP from which it has received an individually addressed Probe Response if the Probe Response contains an Authentication Control element with the Control subfield equal to 0 and the Deferral subfield equal to 1. The deferral begins at the end of the reception of the Probe Response and extends for a period of time equal to the value contained in the Authentication Control Threshold subfield value in the Probe Response. At the end of the deferral time period, the STA shall set the local MAC variable AuthenticationRequestTransmission to true and may transmit an Authentication Request frame to the AP.

A CAC STA ~~with dot11S1GCentralizedAuthenticationControlActivated equal to true~~ shall set the local MAC variable AuthenticationRequestTransmission to true when it receives a Beacon or Probe Response frame that does not include an Authentication Control element from the AP that it intends to join.

An S1G AP shall not set the Deferral subfield in the Authentication Control element of the Beacon frames or the broadcast Probe Response frames to 1.

An S1G STA does not follow the Authentication Control rules defined in this subclause if it receives a Beacon or Probe Response frame that includes an Authentication Control element from the AP that it does not intend to join, or is not intended to the STA.