IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB 200 Comment Resolutions for 10.3.8 and 8.4.2.170m | | | | |
| Date: 2014-01-15 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Shoukang Zheng | I2R | 1 Fusionopolis Way, #21-01 Connexis, Singapore | (65) 6408 2000 | skzheng@i2r.a-star.edu.sg |
| Zander Lei | I2R |  |  | leizd@i2r.a-star.edu.sg |
| Yuan Zhou | I2R |  |  | yzhou@i2r.a-star.edu.sg |

Abstract

This document provides resolutions for CID 1282, 1283, 1284, 1285, 1286, 1287, 1288, 1429, 1406, 2520, 2828, 2735, 2771.

The changes are in the following subclauses: 10.3.8 and 8.4.2.170m.

Table of Contents

[0 Revision Notes 2](#_Toc350888716)

# 0 Revision Notes

R0: First draft

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** | **Resolution** |
| 1282 | 10.3.8 | 223 | 31 | "expected to send Authentication Request to the AP" -- grammar, terminology | "expected to send and Authentication Request frame to the AP" | Revised  Tgah editor to make changes shown in 11-14-0071r0. |
| 1283 | 10.3.8.1 | 223 | 36 | I stopped commenting on 10.3.8.1, because I discovered I was rewriting it para by para. It is full of grammatical errors, particularly articles. | Have a qualified reviewer adjust the language. | Revised  Tgah editor to make changes shown in 11-14-0071r0. |
| 1284 | 10.3.8.1 | 223 | 37 | "When dot11S1GCentralizedAuthenticationControlActivated is true, AP may limit the number of STAs that can transmit Authentication Request to it by 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." - various article errors | "When dot11S1GCentralizedAuthenticationControlActivated is true, an AP may limit the number of STAs that can transmit an Authentication Request frame to it by including an Authentication Control element in a Beacon or a Probe Response frame. The AP can adjust the value of the Authentication Control Threshold field within the element from beacon to beacon." | Revised  Tgah editor to make changes shown in 11-14-0071r0. |
| 1285 | 10.3.8.1 | 223 | 43 | "When dot11S1GCentralizedAuthenticationControlActivated is false, AP shall" - grammar | AP -> an AP | Accepted  Tgah editor to make changes shown in 11-14-0071r0. |
| 1286 | 10.3.8.1 | 223 | 46 | "A STA for which supports Centralized Authentication Control sets dot11S1GCentralizedAuthenticationControlActivated to true and set dot11S1GAuthenticationRequestTransmission to true when it is initialized." -- various errors | "A STA that supports centralized authentication control sets dot11S1GCentralizedAuthenticationControlActivated to true and sets dot11S1GAuthenticationRequestTransmission to true when it is initialized." | Revised  Tgah editor to make changes shown in 11-14-0071r0. |
| 1287 | 10.3.8.2 | 224 | 19 | "shall set the Distributed Authentication Control bit to 1"  According to WG11 style, this is a subfield. Only structures that are bitfields, where the size of the item is relevant should explicitly be called bits. Others are subfields. | bit -> subfield.  Review all use of "bit" in the draft. Where it names a subfield that is not a bitfield or bit array, change to "subfield". | Revised  Tgah editor to make changes shown in 11-14-0071r0. |
| 1288 | 10.3.8.2 | 224 | 40 | "The STA accesses the medium to transmit an Authentication Request frame at the beginning of the lth authentication control slot in the m-th BI, where m=0 is the current BI." This is a good example of the reason not to use ordinals in this context. | Replace with: "The STA accesses the medium to transmit an Authentication Request frame at the beginning of authentication control slot l in BI m, where m=0 is the current BI." | Revised  Tgah editor to make changes shown in 11-14-0071r0. |
| 1406 | 10.3.8.1 | 223 | 34 | Better wording may be needed throughout this subclause and some clarificaitons are proposed in the resolution of this comment. | Replace " A STA for which supports Centralized Authentication Control" with "A STA that supports Centralized Authentication Control" throughout the subclause. Add at the end of the third paragraph: "A STA that does not support Centralized Authentication Control sets the dot11S1GCentralizedAuthenticationControlValue to false." And move the last sentence of the subclause to the end of the third paragraph. And replace "A STA for which dot11..." with "A STA with dot11..." throughout the subclause. | Revised  Tgah editor to make changes shown in 11-14-0071r0. |
| 2520 | 10.3.8 | 223 | 27 | Authentication control seems like another solution to a problem that P802.11ai is resolving. | Either justify why this is required, or work with Tgai to adapt their solution to solve this problem. | Reject.  Please see the justification in the discussion session |
| 2828 | 10.3.8.1 | 223 |  | Even though a STA regenerate a random number after receiving Authentication Response from AP, there still exists unfairness. There should be a STA which has been successful at the first try while other STAs still being failed continuously at the multiple tries. Since the Centralized athentication control mechanism is STA voluntary, multiple trier has more priority or probability to transmit authetication request. | Add the mechanisme for the multiple tried STA to have higher priority than the first tried STA in the draft. Detatils are TBD. | Rejected.  The method in the current draft is simple and achieves long term fairness. The proposal providing additional fairness in Authentication Control incurs a lot of unexpected complexity and behavior. |
| 2771 | 10.3.8.1 | 223 | 34 | Centralized authentication control should support a large number of active scanning STAs to migitate the contention in a more power saving manner | provide a simple deferred channel access after active scanning: AP is able to give an deferred channel access time for active scanning STA when there is a lot of STAs performing probing and doing authentication/association. Details see the proposed comment resolution | Revised  Tgah editor to make changes shown in 11-14-0071r0. |
| 1429 | 8.4.2.170m | 111 | 36 | Description the Authentication Contorl element should not include "may" which is used for protocol behavior. Also is the control field needed? The differentiation of the two cases can be performed by simply looking at the length value. | As in comment. | Rejected  Please see discussions below |
| 2735 | 8.4.2.170m | 111 | 17 | Centralized authentication control should support a large number of active scanning STAs to migitate the contenion in a more power saving manner | provide a simple deferred channel access after active scanning: AP is able to give an deferred channel access time for active scanning STA when there is a lot of STAs performing probing and doing authentication/association. Details see the proposed comment resolution | Revised  Tgah editor to make changes shown in 11-14-0071r0. |

***Discussion:***

**CID 1282**

Authentication Request and Authentication Response are used in the subclauses 10.3.8 and 8.4.2.170m. They refer to Authentication-Request and Authentication-Response defined in Subclause 12 (Fast BSS transition) (802.11REVmc D1.1).

**CID 1287**

This CID gives a comment on how to use subfield and bits. Accept the proposed change in principle. However, this document only handles the subclauses 8.4.2.170m and 10.3.8.

**CID 1429**

Rejected. Although the differentiation of the two cases (Control subfield set to 0 and 1) can be performed by simply looking at the length value, it is abnormal. As the redefinition of Reserved subfield (Control subfield set to 0) may introduce other possible values for the length of the Authentication Control element, the proposed method won’t work for this case.

**CID 2520**

Tgah is trying to solve a problem where there could be a large number of STAs (could be up to 6,000STAs) that may be reset and need to authenticate/associate with the AP at the same time, which is not solved by the fast initial link setup in Tgai.

Firstly, the use cases in11ai are different from that in 11ah. Specifically, 11ai addresses the congestion caused by tens to a couple of hundreds STAs trying to access the channel in a short period of time. However, 11ah's authentication control is to support up to 6000 STAs for association in emergence cases (e.g STAs power outage) where STAs access channel at the same time.  Secondly, the work in the 802.11ai is still ongoing. It is not a requirement for 11ah to follow 11ai.

**CID 2828**

Rejected. The method in the current draft is simple and achieves long term fairness. The proposal providing additional fairness in Authentication Control incurs a lot of unexpected complexity and behavior.

**CID 2735, 2771**

A simple deferred channel access for active scanning STA is feasible when the AP experience a heavy traffic load or a very busy channel: AP may respond to the active scanning STA’s response request with an deferred channel access time when there is a lot of STAs performing probing and doing authentication/association. When the STA receives this information, it shall defer its transmission of Authentication-Request frame until the indicated deferred time is due.

***Proposed changes:***

**Instruction to Editor: *Please make the following changes in clause 8.4.2.170m:***

**8.4.2.170m Authentication Control element**

The notation of *Authentication-Request* and *Authentication-Response* refers to *the definition in Clause 12 (Fast BSS transition)*.

The Authentication Control element contains the information required to mitigate contention among

Authentication Request frames (see 10.3.8).

When the Control subfield is set to 0, the Authentication Control element format is as shown in Figure 8-

401dm (Authentication Control element format (Control subfield = 0)). The Authentication Control element indicates to the recipient STA whether it may transmit an Authentication Request frame to the AP which sends the element. The Information field contains ~~only one field,~~ the Deferral, Reserved and Authentication Control Threshold subfields. The total length of the Information field is 2 octets. The Deferral subfield is 1 bit in length and the Authentication Control Threshold is 10 bits in length. See Figure 8-401dm (Authentication Control element format (Control subfield = 0)).

The Authentication Control Threshold subfield ~~is~~ contains a number ~~and varies~~ with a range from 0 to 1023. When the Deferral subfield is set to 0, the value of the Authentication Control Threshold subfield is used by the recipient STA to determine whether or not it is permitted to transmit an Authentication-Request frame. When the Deferral subfield is set to 1, the Authentication Control Threshold subfield value is a time value, expressed in TUs, indicating a minimum amount of deferred channel access which is required before the transmission of an Authentication Request frame.

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

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Bits: | B0 B1 B7 B8 B15 B16 B23 | | | | | |
|  | Element ID | Length  (=3) | Control  (1) | Authentication  Slot Duration | Maximum  Transmission  Interval | Minimum  Transmission  Interval |
| Octets: | 1 1 3 | | | | | |
|  | Figure 8-401dn – Authentication Control element format (Control subfield = 1) | | | | | |

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

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

The Maximum Transmission Interval subfield is a 9-bit unsigned integer, expressed in BIs, and indicates the maximum transmission interval.

**Instruction to Editor: *Please make the following changes in clause 10.3.8, 10.3.8.1, 10.3.8.2:***

**10.3.8 Authentication Control**

In infrastructure mode, when dot11S1GOptionImplemented is true, AP and STA may use the Authentication

Control element to alleviate media contention when a large number of STAs are trying to or expected to send Authentication Request frames to the AP at about the same time.

**10.3.8.1 Centralized authentication control**

When dot11S1GCentralizedAuthenticationControlActivated is true at an AP, the AP shall set the Control subfield to 0 in the Authentication Control element in all transmitted beacons and Probe Responses.

When dot11S1GCentralizedAuthenticationControlActivated is true at an AP, the AP may ~~limit the number of STAs that can transmit Authentication Request to it by~~ include~~ing the~~ an Authentication Control element with the Control subfield set to 0 and Deferral subfield set to 0 in a beacon or a p~~P~~robe r~~R~~esponse frame to attempt to limit the number of STAs that can transmit an Authentication Request frame to it. The AP can ~~adjust~~ transmit a different~~the~~ value in~~of~~ the Authentication Control Threshold subfield in each ~~within the elementfrom beacon to~~ beacon and Probe Response that it transmits.

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

When dot11S1GCentralizedAuthenticationControlActivated is false at an AP, the AP shall not include ~~the~~an Authentication Control element with the Control field set to 0 in a beacon or Probe Response frame. A STA with the value of false for dot11S1GCentralizedAuthenticationControlActivated is not constrained by the Authentication Control rules defined in this subclause when it transmits an Authentication Request frame to the AP.

A STA ~~for which~~that supports Centralized Authentication Control sets dot11S1GCentralizedAuthenticationControlActivated to true and sets the local MAC variable AuthenticationRequestTransmission~~dot11S1GAuthenticationRequestTransmission~~ to true when it is initialized.

A STA ~~for which~~that has a value of true for dot11S1GCentralizedAuthenticationControlActivated ~~is true, it~~ shall generate a random number *v*~~for dot11S1GCentralizedAuthenticationControlValue~~ when it is initialized. The generated random number ~~is~~ *v* shall be uniformly distributed between 0 and 1022(inclusive) ~~[0, 1022]~~. ~~To avoid unfairness in opportunity of Authentication Request transmission in future, a~~The STA may ~~re~~generate a new random value for ~~number for dot11AuthenticationCentralizedControlValue~~*v* after receiving an Authentication Response from an 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, 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.~~A STA with 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 set to 0. If ~~dot11S1GCentralizedAuthenticationControlValue~~*v* is less than the value of the Authentication Control Threshold subfield ~~of the respective Authenccation Control element~~, the STA may transmit an Authentication Request frame to the AP and ~~the STA~~ shall set ~~dot11S1GAuthenticationRequestTransmission~~ the local MAC variable AuthenticationRequestTransmission to true. Otherwise, the STA shall set the local MAC variable AuthenticationRequestTransmission~~dot11S1GAuthenticationRequestTransmission~~ to false and the STA shall not transmit an Authentication Request frame to the AP.

A STA with dot11S1GCentralizedAuthenticationControlActivated set 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 a unicast Probe Response if the Probe Response contains an Authentication Control element with the Control subfield set to 0 and the Deferral subfield set 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.

~~When a STA for which dot11S1GCentralizedAuthenticationControlActivated 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 dot11S1GAuthenticationRequestTransmission to true.~~

A STA with dot11S1GCentralizedAuthenticationControlActivated set 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.

~~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.~~

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.

**10.3.7.2 Distributed authentication control**

When dot11S1GDistributedAuthenticationControlActivated is true, an S1G AP shall set the Distributed Authentication Control ~~bit~~subfield to 1 in the S1G Capabilities Info field of the S1G Capabilities element. Otherwise, the ~~bit~~subfield 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 it is permitted to access the medium to transmit an Authentication Request frame to the AP from which it received the S1G Capabilities element based on the following procedure:

1. The STA maintains the following distributed authentication control (DAC) parameters:

* Authentication control slot duration (Tac) in TU units. The default value is set to 10 TUs.
* Minumum transmission interval (TImin) in BI units. The default value is set to 8 BIs.
* Maximum transmission interval (TImax) in BI units. The default value is set to 256 BIs.

1. The STA maintains a transmission interval (TI) in BI units.
2. 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*=0 is the first authentication control slot
5. The STA may initiate normal EDCA accesses procedures~~the medium~~ for the transmission of ~~to transmit an~~ the Authentication Request frame ~~at the~~ beginning ~~of~~at the *~~l~~*~~-th~~ authentication control slot *l* in the *~~m~~*~~-th~~ BI *m*, 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 subfield set to 1. An S1G STA receiving ~~the~~ such an Authentication Control element shall update its MIB values of the DAC parameters based on the values received in the Authentication Control element.