IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB203 MAC Resolution to Comments in D2.0 Subclause 10.3.5.11 and 10.3.8 | | | | |
| Date: 2014-8-25 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Zander Lei | I2R | 1 Fusionopolis Way #21-01 Connexis | +65 6408 2436 | leizd@i2r.a-star.edu.sg |
| Shoukang Zheng | I2R | 1 Fusionopolis Way #21-01 Connexis | +65 6408 2252 | skzheng@i2r.a-star.edu.sg |
| Yuan Zhou | I2R | 1 Fusionopolis Way #21-01 Connexis | +65 6408 2472 | yzhou@i2r.a-star.edu.sg |

Abstract

This submission proposes resolution to comments in D2.0 subclauses 10.3.5.11 and 10.3.8. There are 13 CIDs addressed: 3058, 3059, 3909, 3188, 3189, 3190, 3191, 3192, 3193, 3194, 4013, 3195, 4035

Revision History:

Rev1:

* Added in the doc # in the “instruction to editor” in the table
* CID3195: added resolution status
* CID4013: added clarification text in resolution status
* CID3058: replaced “may” with “can” in resolution text
* CID4035: made a correction to the MIB variable dot11S1GCACDeferral (“Unsigned32” to “TruthValue”) and added a sentence for updating the MIB value

Rev2:

* CID4035: amended the sentence for updating the MIB value
* Update the doc # in the “instruction to editor” in the table

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.***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page.Line** | **Clause** | **Comment** | **Propose Change** | **Resolution** |
| 3909 | 327.55 | 10.3.5.11 | This clause really just refers to a "sensor type" indicator, which looks more like a device type. It doesn't really look like a service. A traffic offload device/service isn't even defined. Furthermore the subclause does not describe what the STA and the no-AP STA do with this information. | Describe in details what Service Type is used for (consider renaming it to device type) and describe how this infomration is used during Association. | Revised  Agree in principle.  TGah editor to make the changes showin in 11-14/1115r2 under all headings that include CID 3909. |
| 3188 | 327.60 | 10.3.5.11 | The Service Type field in the AID Request element has the following subfields: Sensor, Offload, Critical Service. It is better to keep consistency when describing the service types per STA as specified by the field which is used to signal these services. | Replace "emergency services" with critical services" in P327L58. Replace "for emergency service type such as health care, home, industrical, alarm monitoring or emergency service devices" with for STAs that provide critical services such as health care, home, industrial, alarm monitoring, or emergency services." in P327L62. | Revised  Agree in principle.  TGah editor to make the changes showin in 11-14/1115r2 under all headings that include CID 3188. |
| 3189 | 328.1 | 10.3.5.11 | This paragraph contains some redundancy that can easily removed as suggested in the proposed change. | Replace the second paragraph with the following: " A non-AP STA may indicate the service types it provides by including the Service Type field in the AID Request element of a (Re) Association Request frame that it transmits to the AP with which it wants to associate. The AP may assign a particular AID to the STA taking into account the received service type information from the STA." | Revised  Agree in principle.  TGah editor to make the changes showin in 11-14/1115r2 under all headings that include CID 3189. |

**[CIDs 3909, 3188, 3189]**

**Instruction to TGah editor: Please modify subclause 10.3.5.11 (Service type indication during association) of TGah D2.1 as follows:**

A sensor type service is the service that a sensor type STA is able to provide. ~~A Sensor type STA supports only sensor services.~~ Non-sensor type ~~STAs may support different types of~~ services~~, for example~~ include offloading and ~~emergency~~ critical services. Different service types may have different requirements on QoS, packet size, duty cycle,(#3412) etc. An AP can optimize the system operating parameters with the knowledge of service type of each associated STA or provide a high priority on association/reassociation for a STA that provides critical services ~~emergency service type~~ such as health care, home, industrial, alarm monitoring or emergency service ~~devices~~.

A non-AP STA may indicate to the AP its service type information during association by including the ~~adding a~~ ~~s~~Service ~~t~~Type field in the AID Request element in ~~a~~ the (Re) Association Request frame ~~or a Reassociation Request frame as described in 8.3.3.5 (Association Request frame format) and 8.3.3.7 (Reassociation Request frame format).~~ ~~After receiving the service type information from the STA, the~~ The AP may assign a particular AID to ~~this~~ the STA ~~based on its~~ ~~service type~~ taking into account the received service type information from the STA.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3058 | 328.13 | 10.3.8 | "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 tothe AP at about the same time."  This mixes a normative requirement and an explanation of why you might want to do it." | "Separate into information and normative sentences.  Ditto at line 26. | Revised  Agree in principle.  TGah editor to make the changes showin in 11-14/1115r2 under all headings that include CID 3058. |
| 3190 | 328.13 | 10.3.8 | Some suggested changes to make this paragraph clearer: "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." | Replace the paragraph with: " In an infrastructure BSS, an S1G AP may use the Authentication Control element to alleviate WM contention when a large number of STAs are trying to or are expected to send Authentication Request frames to the AP at about the same time." | Accept.  TGah editor to make the changes showin in 11-14/1115r2 under all headings that include CID 3190. |
| 3059 | 328.11 | 10.3.8 | I am not convinced we need any form of authentication rate control.  But we certainly don't need two of them. | Remove 10.3.8, or remove one of its subclauses. | Reject.  As specified in the specification requirement document, 11ah task group is required to address the issue that a large number of STAs reset and re-authenticate / associate may congest or down the network. This subclause provides such solutions. |
| 4013 | 328.18 | 10.3.8.1 | Having first 3 paragraphs, all starting with "When dot11S1GCentralizedAuthenticationControlActivated is true at an AP" is confusing. | Combine into one paragraph and simplify the language. | Revised  Combine part of 4th paragraph and 1st paragraph.  TGah editor to make the changes showin in 11-14/1115r2 under all headings that include CID 4013. |
| 3191 | 328.18 | 10.3.8.1 | It seems that this subclause needs some logical organization. Move the 4th paragraph after the 2st paragraph. And move the last paragraph of this subclause as the second paragraph of subclause 10.3.8. | As in comment. | Revised  Agreed partially and moved part of 4th paragraph to the end of 1st paragraph.  TGah editor to make the changes showin in 11-14/1115r2 under all headings that include CID 3191. |
| 3192 | 328.20 | 10.3.8.1 | There is a capability indication for this feature in the S1G Capabilities element but there is no normative behavior specified in this subclause | Insert the following: "When dot11S1GCentralizedAuthenticationControlActivated is true, an S1G STA shall set the Distributed 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 the Distributed Authentication Control subfield equal to 0 shall not follow the rules defined in this subclause." | Revised  Agreed in principle.  TGah editor to make the changes showin in 11-14/1115r2 under all headings that include CID 3192. |
| 3193 | 328.20 | 10.3.8.1 | An AP that activates Centralized auth. Ctrl does not necessarily include the Authentication Control element in all transmitted Beacons ..." Clarify that shall set the CTRL subfield to 0 in the elements THAT it includes in the frames. See suggested change. | Replace the first paragrap of this subclause with: "When dot11S1GCentralizedAuthenticationControlActivated is true at an AP, the AP shall set the Control subfield to 0 in the Authentication Control elements that it includes in transmitted S1G Beacon and Probe Response frames. | Revised  TGah editor to make the changes showin in 11-14/1115r2 under all headings that include CID 3193. |
| 3194 | 328.29 | 10.3.8.1 | Authentication Control Threshold subfield in each Beacon and Probe Response... Add "of the Authenticaiton Control element included in the Beacon and Probe Resposne frames" | As in comment. | Revised  Agreed in principle.  TGah editor to make the changes showin in 11-14/1115r2 under all headings that include CID 3194. |
| 3195 | 329.31 | 10.3.8.2 | Distributed authentication control defines a procedure to enable the AP alleviate medium contention when a large number of STAs are sending Authentication Request frames. But if the signaling is in the S1G Capabilities element doesn't this mean that this procedure is activated all the time by the AP? Or can the value of this field in capabilities element change? | If the S1G Capabilities element values can be changed by an AP during its BSS existence then this should be fine. But if this is not the case we may need to find another way to signal this (not in the S1G Capabilities element). | Reject.  For the supporting STA, the capability is set to 1 through out the operation. |
| 4035 | 329.62 | 10.3.8.2 | The MIB values mentioned in "An S1G STA receiving such an Authentication Control element shall update its MIB values of the DAC parameters based on the values received in the Authentication Control element." are not defined. | Please define the concerned MIBs. | Revised  Agreed in principle.  TGah editor to make the changes showin in 11-14/1115r2 under all headings that include CID 4035. |
|  |  |  |  |  |  |

**[CIDs 3058, 3190]**

**Instruction to TGah editor: Please modify subclause 10.3.8 (Authentication Control) of TGah D2.1 as follows:**

In infrastructure mode, ~~when dot11S1GOptionImplemented is true,~~ an S1G AP ~~and STA~~ ~~may~~ can use the Authentication Control element to alleviate ~~media~~ WM contention when a large number of STAs are trying to or are expected to send Authentication Request frames to the AP at about the same time.

**[CIDs 4013, 3191, 3192, 3193, 3194, 4035]**

**Instruction to TGah editor: Please modify the subclause 10.3.8.1 (Authentication Control) of TGah D2.1 as follows:**

* 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 the Centralized Authentication Control subfield equal to 0 shall not follow the rules defined in this subclause.

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 frames. When dot11S1GCentralizedAuthenticationControlActivated is false at an AP, the 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 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 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 AP may include, within an individually addressed (#3066, Ed) 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~~which~~ begins immediately following the reception of the Probe Response, the receiving STA with dot11S1GCentralizedAuthenticationControlActivated equal 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 an Authentication Control element with the Control field equal 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 that supports Centralized Authentication Control sets dot11S1GCentralizedAuthenticationControlActivated to true and sets the local MAC variable AuthenticationRequestTransmission to true when it is initialized.

A 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 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 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 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.

… …

**[CID 4035]**

**Instruction to TGah editor: Please insert the following MIB details into Annex C (C.3). Please note that the number for dot11S1GStationConfigEntry should be assigned accordingly:**

dot11S1GCACEntry OBJECT-TYPE

SYNTAX Dot11S1GCACEntry

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the MAC upon receiving an Authentication Control Element with Control subfield equal to 0.

Changes take effect as soon as practical in the implementation.

This attribute specifies the parameters that are used by the Centralized Authentication Control operation. "

::= { dot11S1GStationConfigEntry xx }

Dot11S1GCACEntry ::=

SEQUENCE {

dot11S1GCACDeferral TruthValue,

dot11S1GCACThreshold Unsigned32}

dot11S1GCACDeferral OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the MAC upon receiving an Authentication Control Element with Control subfield equal to 0.

Changes take effect as soon as practical in the implementation.

This attribute specifies whether the deferred channel access is used by the Centralized Authentication Control operation. "

DEFVAL { 0 }

::= { dot11S1GCACEntry 1}

dot11S1GCACThreshold OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the MAC upon receiving an Authentication Control Element with Control subfield equal to 0.

Changes take effect as soon as practical in the implementation.

This attribute specifies the threshold value that is used by the Centralized Authentication Control operation. "

DEFVAL { 1024 }

::= { dot11S1GCACEntry 2 }

dot11S1GDACEntry OBJECT-TYPE

SYNTAX Dot11S1GDACEntry

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the MAC upon receiving an Authentication Control Element with Control subfield equal to 1.

Changes take effect as soon as practical in the implementation.

This attribute specifies the parameters that are used by the Distributed Authentication Control operation. "

::= { dot11S1GStationConfigEntry xx }

Dot11S1GDACEntry ::=

SEQUENCE {

dot11S1GDACTac Unsigned32,

dot11S1GDACTImin Unsigned32,

dot11S1GDACTImax Unsigned32}

dot11S1GDACTac OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the MAC upon receiving an Authentication Control Element with Control subfield equal to 1.

Changes take effect as soon as practical in the implementation.

This attribute specifies the Authentication Slot Duration that is used by the Distributed Authentication Control operation. "

DEFVAL { 10 }

::= { dot11S1GDACEntry 1 }

dot11S1GDACTImin OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the MAC upon receiving an Authentication Control Element with Control subfield equal to 1.

Changes take effect as soon as practical in the implementation.

This attribute specifies the minimum transmission interval that is used by the Distributed Authentication Control operation. "

DEFVAL { 8 }

::= { dot11S1GDACEntry 2}

dot11S1GDACTImax OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the MAC upon receiving an Authentication Control Element with Control subfield equal to 1.

Changes take effect as soon as practical in the implementation.

This attribute specifies the maximum transmission interval that is used by the Distributed Authentication Control operation. "

DEFVAL { 256 }

::= { dot11S1GDACEntry 3 }