IEEE P802.19
Wireless Coexistence

|  |
| --- |
| Proposed resolution to comment to clause 5.2.1.1 WSO authentication procedure |
| Date: 2012-07-17 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Stanislav Filin | NICT |  |  | sfilin@nict.go.jp |
| Hiroshi Harada | NICT |  |  |  |

Abstract

This document is a submission to IEEE 802.19 TG1 proposing resolution to comment to clause 5.2.1.1 WSO authentication procedure.

**Notice:** This document has been prepared to assist IEEE 802.19. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

# Comment

WSO authentication procedure is not described, only figure is provided.

# Proposed resolution

*It is proposed to modify the text in the clause 5.2.1.1 WSO authentication procedure as shown below:*

* + - 1. WSO authentication procedure

The CE shall perform the WSO authentication procedure when it has received a request to start operation. An illustrative example of this procedure is shown in Figure 1. GetAuthInfo.request, GetAuthInfo.response, and GetAuthInfo.comfirm primitives are defined in clause 4.2.2.1 Authentication service. AuthenticationRequest and AuthenticationResponse messages are defined in clause 5.3 Messages.



Figure 1 WSO authentication procedure

After a CE has received a request to start operation, it shall send GetAuthInfo.request to WSO it serves and shall wait for the corresponding GetAuthInfo.response from the WSO. If the CE has not received the GetAuthInfo.response from the WSO within a given time, the CE shall retransmit the GetAuthInfo.request to the WSO. If the CE has not received the GetAuthInfo.response from the WSO after a given number of attempts, the CE shall indicate that the WSO is not responding and stop operation until the next request to start operation.

When the CE has received the GetAuthInfo.response from the WSO, the CE shall send an AuthenticationRequest to the CM using the CP\_PACKET\_SEND.request primitive of the coexistence transport SAP and shall wait for the corresponding AuthenticationResponse from the CM. If the CE has not received the AuthenticationResponse from the CM within a given time, the CE shall retransmit the AuthenticationRequest to the CM. If the CE has not received the AuthenticationResponse from the CM after a given number of attempts, the CE shall indicate that the CM is not responding and stop operation until the next request to start operation.

When sending the AuthenticationRequest to the CM, the CE shall set the parameters of the CP\_PACKET\_SEND.request primitive as described in the Table 1.

Table 1 CP\_PACKET\_SEND.request parameter values for the AuthenticationRequest

|  |
| --- |
| transportType parameter value shall be set to tcp. |
| sourceID parameter value shall be set to a combination of the IP address and port number of the CE. |
| destinationID parameter value shall be set to a combination of the serverIPAdress and serverPortNumber parameters from the received GetAuthInfo.response. |
| coexProtocolPDU parameter value shall be set to the AuthenticationRequest to be transmitted. |

The CE shall set the parameters of the header of the AuthenticationRequest as described in Table 2.

Table 2 AuthenticationRequest header parameter values

|  |
| --- |
| sourceIdentifier::type parameter value shall be set to ce. |
| sourceIdentifier::id parameter value shall be set to the ID of the CE. |
| destinationIdentifier::type parameter value shall be set to cm. |
| destinationIdentifier::id parameter value shall be set to the cmID from the received GetAuthInfo.response. |
| ackPolicy parameter value shall be set to true. |
| messageIdentification parameter value shall use requestID that shall be set to 0 for the first AuthenticationRequest to be sent and shall be incremented by 1 for each new AuthenticationRequest to be sent. |

The CE shall set the parameters of the payload of the AuthenticationRequest as described in Table 3.

Table 3 AuthenticationRequest payload parameter values

|  |
| --- |
| clientID parameter value shall be set to clientID from the received GetAuthInfo.response. |
| clientPW parameter value shall be set to clientPassword from the received GetAuthInfo.response. |

When the CM has received the AuthenticationRequest from the CE, the CM shall process the content of the AuthenticationRequest and then shall send an AuthenticationResponse to the CE using the CP\_PACKET\_SEND.request primitive of the coexistence transport SAP.

When sending the AuthenticationResponse to the CE, the CM shall set the parameters of the CP\_PACKET\_SEND.request primitive as described in the Table 4.

Table 4 CP\_PACKET\_SEND.request parameter values for the AuthenticationResponse

|  |
| --- |
| transportType parameter value shall be set to tcp. |
| sourceID parameter value shall be set to a combination of the IP address and port number of the CM. |
| destinationID parameter value shall be set to a combination of the serverIPAdress and serverPortNumber parameters of the CE that has sent the AuthenticationRequest. |
| coexProtocolPDU parameter value shall be set to the AuthenticationResponse to be transmitted. |

The CM shall set the parameters of the header of the AuthenticationResponse as described in Table 5.

Table 5 AuthenticationResponse header parameter values

|  |
| --- |
| sourceIdentifier::type parameter value shall be set to cm. |
| sourceIdentifier::id parameter value shall be set to the ID of the CM. |
| destinationIdentifier::type parameter value shall be set to ce. |
| destinationIdentifier::id parameter value shall be set to the ceID of the CE that has sent AuthenticationRequest. |
| ackPolicy parameter value shall be set to true. |
| messageIdentification parameter value shall use multipleResponse in which requestID shall be sent to the value from the received AuthenticationRequest, sequenceNumber shall be set to 0, and isLastResponse shall be set to true. |

The CM shall set the parameters of the payload of the AuthenticationResponse as described in Table 6.

Table 6 AuthenticationResponse payload parameter values

|  |
| --- |
| If the CM cannot process the AuthenticationRequest due to wrong state, the status parameter value shall be set to errorInvalidEntityStatus. |
| If the values of the clientID and clientPW in the received AuthenticationRequest are equal to the values recorded in the CM, the status parameter value shall be set to noErrorAccepted. |
| If the values of the clientID and clientPW in the received AuthenticationRequest are not equal to the values recorded in the CM, the status parameter value shall be set to noErrorRejected. |

When the CE has received the AuthenticationResponse from the CM, the CE shall process the content of the AuthenticationResponse and then shall send a GetAuthInfo.confirm to the WSO.

If the status parameter value in the received AuthenticationResponse is set to errorInvalidEntityStatus, the CE shall retransmit the AuthenticationRequest to the CM.

If the status parameter value in the received AuthenticationResponse is set to errorInvalidArgument, errorProcessFailure, errorNetworkFailure or errorUnknow, the CE shall indicate that the CM is not responding properly and stop operation until the next request to start operation.

For any other value of the status parameter in the received AuthenticationResponse, the CE shall proceed to sending the GetAuthInfo.confirm to the WSO.

The CE shall set the parameters of the GetAuthInfo.confirm as described in Table 7.

Table 7 GetAuthInfo.confirm parameter values

|  |
| --- |
| If the status parameter value in the received AuthenticationResponse is set to noErrorAccepted and the values of the serverID and serverPassword parameter from the received AuthenticationResponse are equal to the values of the serverID and serverPassword parameter from the received GetAuthInfo.response,the status parameter value shall be set to noErrorAccepted. |
| If the status parameter value in the received AuthenticationResponse is set to noErrorAccepted and either of the values of the serverID and serverPassword parameter from the received AuthenticationResponse is not equal to the values of the serverID and serverPassword parameter from the received GetAuthInfo.response,the status parameter value shall be set to noErrorRejected. |
| If the status parameter value in the received AuthenticationResponse is set to noErrorRejected, the status parameter value shall be set to noErrorRejected. |