IEEE P802.22
Wireless RANs

|  |
| --- |
| CID7 Resolution - LB2 Recirculation  |
| Date: 2014-11-18 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Ranga Reddy | Self |  |  | Ranga.reddy@me.com  |
|  |  |  |  |  |

Abstract

This document provides comment resolutions for CID 7 in LB2 re-circulation contained 22-14/130r1.

R0: initial version of this document

**Notice:** This document has been prepared to assist IEEE 802.22. 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.

**Release:** The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE’s name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE’s sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.22.

**Patent Policy and Procedures:** The contributor is familiar with the IEEE 802 Patent Policy and Procedures

<[**http://standards.ieee.org/guides/bylaws/sb-bylaws.pdf**](http://standards.ieee.org/guides/bylaws/sb-bylaws.pdf)>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair Apurva Mody <apurva.mody@ieee.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.22 Working Group. **If you have questions, contact the IEEE Patent Committee Administrator at <****patcom@ieee.org****>**.

This document provides resolutions for comment CID7 in the LB2 re-circulation comment database (DCN 22-14/130r1).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 7 | 7.6.1.2 | 1 | 45 | 1 | TR | In 7.6.1.2, we only briefly mentioned the Extended type subheader. This subheader has a Channel Aggregation subtype. No where in 7.6.1.2 or 7.24 is this subheader and its options discussed, nor is there any distinction between how MAC PDUs are transmitted using this subheader when multi-channel operation is enabled. | Add text in section 7.24 to define how channel aggregation modes are configured when CA is enabled. Add/modify text in section 7.24 to clarify the difference between trasnsmitting in “Transmit Diversity” or “Bulk Transmission Mode” when CA is enable. Add/modify text in section 8.4.2.1.1/8.4.2.3 to clarify how the PN values of MPDUs are to be treated given whether “Transmit Diversity” or “Bulk Transmission Mode” is enabled for multi-channel operation. Refer to section 3 of 22-14/82r0 and section 7 of 22-14/128r0 |

In this document we provide a slight modification to the text in section 8.4.2.3 and 8.4.2.1.1 to address how the PN counter and PN\_WINDOW should be handled when multi-channel operations are engaged for “Bulk Transmission” or “Transmit Diversity” methods of transmitting PDUs in the DS/US on each CHU that is enabled.

***Modify the text in section 8.4.2.3 of base standard as follows***

***<Start of Modification>***

On receipt of a PDU the receiving CPE or BS shall decrypt and authenticate the PDU consistent with the NIST GCM specification configured as specified in 8.4.2.2.

Packets that are found to be not authentic shall be discarded.

Receiving BS or CPEs shall maintain a record of the highest value PN and MMP\_PN received for each SA. The receiver shall maintain a PN window whose size is specified by the PN\_WINDOW\_SIZE parameter for SAs and management connections as defined in Table 272. The setting of PN\_WINDOW\_SIZE shall take into account the number of active CPE-CHUs when the network is configured to work in multi-channel operation with “Bulk Tranmsission” mode.

When single or multi-channel operation is engaged, a~~A~~ny received PDU with a PN lower than the beginning of the PN window shall be discarded as a replay attempt. The receiver shall track PNs within the PN window. ~~Any PN that is received more than once shall be discarded as a replay attempt. Upon reception of a PN, which is greater than the end of the PN window, the PN window shall be advanced to cover this PN.~~

When the network is configured for single-channel operation, any PN that is received more than once shall be discarded as a replay attempt. When the network is configured for multi-channel operation in “Transmit Diversity” mode, any PN that is received more than once on all active CHUs shall be discarded as a replay attempt. When the network is configured for multi-channel operation in “Bulk Transmission” mode, any PN that is received more than once on one or more of the active CHUs shall be discarded as a replay attempt. Upon reception of a PN, which is greater than the end of the PN window, the PN window shall be advanced to cover this PN.

***<End of Modification>***

***Modify the text in section 8.4.2.1.1 of draft as follows (existing modifications are in black underline, modifications on top of exisiting D3 draft are in blue)***

***<Start of Modification>***

**8.4.2.1.1 Packet number**

A PN (Packet Number) is prepended to a MAC PDU payload when a CPE is configured for a cryptographic suite other than x00. The PN value associated with a cryptographic suite selected for an SA can be 3bytes or 4bytes. A CPE cannot be configured for a multiple cryptographic suites that support both 3byte and 4byte PNs simultaneously across the SAs its configured for. Section 8.4.2.1.1.1 describes how a CPE and BS handle the operation of a 3byte PN, and Section 8.4.2.1.1.2 describes how a CPE and BS handle the operation of 4byte PN.

**8.4.2.1.1.1 3byte PN Procedure**

The MAC PDU payload shall be prefixed with a 3-byte PN ~~(Packet Number)~~, when the cryptographic suite selected for the SA is 0x01-0x05, and 0x08-0x0A. The PN shall be encoded in the MAC PDU least significant byte first. The PN shall not be encrypted.

The PN associated with an SA shall be set to 1 when the SA is established and when a new TEK is installed. Upon completion of initial authentication or reauthentication and after the MMP\_KEY has been derived has been derived, the MMP\_PN is set to 1. After each PDU transmission made during single channel operation or each PDU transmission that is to be copied across all active BS/CPE-CHUs during multi-channel operation in “Transmit Diversity” mode, the PN and MMP\_PN shall be incremented by 1. After each unique PDU transmission made on each active BS/CPE-CHU during multi-channe operation in “Bulk Transmission”, the PN and MMP\_PN shall be incremented by 1 on each active CHU in succession.

When admitting a CPE to an existing multicast/broadcast group, the BS will take the current value of the PN related to the newest generation of material for that GSA, and increment by 1 when establishing. The maximum number of CPEs that can be admitted to a multicast/broadcast group simultaneously is one half the PN\_WINDOW\_SIZE (see 8.4.2.3).

On DS connections, the PN shall be XORed with 0x800000 prior to encryption and transmission. This effectively splits the PN space into two ranges for DS (0x000000–0x7FFFFF) and DU (0x800001–0xFFFFFF); thereby avoiding collision of PN values when using a single PN for DS and DU. On DS connections, the PN shall be used without such modification.

Any tuple value of {PN, KEY} shall be handled as per the receive processing rules for treating the PN value as described in 8.4.2.3~~not be used more than once for the purposes of transmitting data~~. ~~This~~ These measures is known a protection against replay attacks. A new TEK shall be requested and transferred before the PN on either the CPE or BS reaches 0x7FFFFF~~FF~~. If the PN in either the CPE or BS reaches 0x7FFFFF~~FF~~ without new keys being installed, transport communications on that SA shall be halted until new TEKs are installed. In the case of the MMP\_KEY, if MMP\_PN expires, then current AK is invalidated and shall start Reauthentication.

**8.4.2.1.1.2 4byte PN Procedure**

The MAC PDU payload shall be prefixed with a 4-byte PN, when the cryptographic suite selected for the SA is 0x0C-0x14. The PN shall be encoded in the MAC PDU least significant byte first. The PN shall not be encrypted.

The PN associated with an SA shall be set to 1 when the SA is established and when a new TEK is installed. Upon completion of initial authentication or reauthentication and after the MMP\_KEY has been derived has been derived, the MMP\_PN is set to 1. After each PDU transmission made during single channel operation or each PDU transmission that is to be copied across all active BS/CPE-CHUs during multi-channel oepratio in “Transmit Diversity” mode, , the PN and MMP\_PN shall be incremented by 1. After each unique PDU transmission made on each active BS/CPE-CHU during multi-channe operation in “Bulk Transmission”, the PN and MMP\_PN shall be incremented by 1 on each active CHU in succession.

When admitting a CPE to an existing multicast/broadcast group, the BS will take the current value of the PN related to the newest generation of material for that GSA, and increment by 1 when establishing. The maximum number of CPEs that can be admitted to a multicast/broadcast group simultaneously is one half the PN\_WINDOW\_SIZE (see 8.4.2.3).

On DS connections, the PN shall be XORed with 0x80000000 prior to encryption and transmission. This effectively splits the PN space into two ranges for DS (0x00000000–0x7FFFFFFF) and DU (0x80000001–0xFFFFFFFF); thereby avoiding collision of PN values when using a single PN for DS and DU. On DS connections, the PN shall be used without such modification.

Any tuple value of {PN, KEY} shall be handled as per the receive processing rules for treating the PN value as described in 8.4.2.3~~not be used more than once for the purposes of transmitting data~~. ~~This~~ These measures is known a protection against replay attacks. A new TEK shall be requested and transferred before the PN on either the CPE or BS reaches 0x7FFFFFFF. If the PN in either the CPE or BS reaches 0x7FFFFFFF without new keys being installed, transport communications on that SA shall be halted until new TEKs are installed. In the case of the MMP\_KEY, if MMP\_PN expires, then current AK is invalidated and shall start Reauthentication.

***<End of Modification>***