IEEE P802.22  
Wireless RANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Remaining Security Issues | | | | |
| Date: 2014-09-30 | | | | |
| Author(s): | | | | |
| Name | Company | Address | Phone | email |
| Ranga Reddy | Self |  |  | [Ranga.reddy@me.com](mailto:Ranga.reddy@me.com) |
|  |  |  |  |  |

Abstract

This document addresses remaining security issues not addressed in other contributions.

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](mailto: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**](mailto:patcom@ieee.org)**>**.

# Introduction

During LB2 comment resolution, security issues brought up by DCN 22-14/82r0 have been resolved. This document seeks to provided the resolutions to the remaining issues (from DCN 22-14/82r0) listed below:

* Section 1.C: 1.C.2, 1.C.3, 1.C.4
* Section 1.D: 1.D.2
* Section 1.E: 1.E.1
* Section 1.F: 1.F.1, 1.F.2, 1.F.3
* Section 2: 2.1, 2.2, 2.3
* Section 3: 3.1 – 3.6
* Section 4: 4.1, 4.2, 4.3

The remainder of this document is organized into sections that provide resolutions to the aforementioned issues.

# Section 1.C & 1.D Issues

Modifications in this section address 1.C.2, 1.C.3, 1.C.4, and 1.D.2 from DCN 22-14/82r0.

***Add the following text at the end of section 8, pg 250 as follows***

***<Start of Modification>***

The security concepts that are enabled by security sublayers 1 and 2 are also extended to the relay network, for both A-CPEs and S-CPEs. The security model in the relay network is end-to-end. Authentication of MAC management and user data sent between the A-BS and S-CPE is handled at each end of the connection, i.e. by the A-BS and S-CPE. Centralized and Distributed A-CPEs are only responsible for authentication of MAC management messages exchanged between itself and the A-BS. Centralized/Distributed A-CPEs shall not be involved in initial- or re-authentication or keying of attached S-CPEs, other than to forward SCM-REQ/RSP messages between any attached S-CPEs and the A-BS. Centralized/Distributed S-CPEs do not maintain or store any of the authentication information (e.g. AK Context) related to any attached S-CPEs.

***<End of Modification>***

***Modify the text in section 8.1.2, pg 252 as follows***

***<Start of Modification>***

The SCM protocol allows for mutual authentication where both the network and CPEs authenticate each other. It also supports periodic reauthentication and key refresh. It uses strong encryption algorithms to perform key exchanges between a CPE and BS.

The SCM’s authentication protocol establishes a shared secret (i.e., the AK) between the CPE and the BS. The shared secret is then used to secure subsequent SCM exchanges of TEKs. This two-tiered mechanismfor key distribution permits refreshing of TEKs without incurring the overhead of computation-intensive operations.

EAP-based authentication uses Extensible Authentication Protocol framework (IETF RFC 3748 [B30]). EAP offers the operator to select an EAP Method (e.g., EAP-TLS; IETF RFC 2716 [B25]) to execute the authentication. Each EAP Method specifies a credential that is used to perform authentication and verify the device’s /user’ s identity. For example, EAP-TLS uses a X.509 certificate, while EAP-SIM uses a Subscriber Identity Module.

EAP-TLS or EAP-TTLS shall be used; 1045H 8.5 defines the profile for the X.509 credential. In order to avoid security vulnerabilities, the EAP Method implemented in an IEEE 802.22 network shall comply with the mandatory requirements stated in Section 2.2 of IETF RFC 4017 [B33]. During initial authentication EAP transfer messages are not protected. For reauthentication, the EAP transfer messages are protected (encrypted and authenticated) using the MMP\_Key (8.2.4.6.2). If EAP reauthentication messages fail their authentication verification (8.3.2) or are not protected, they shall be ignored by the BS and CPE.

The AAA server and a client CPE authenticate each other during the initial authentication exchange. The AAA and CPE present their credentials to each other. Since the AAA and CPE mutually authenticate each other, there is protection against an attacker employing a cloned CPE that masquerades as a legitimate subscriber’s CPE. Once authentication is completed, the BS and CPE have keying that is used to protect management messages (e.g., MMP\_Key) and keying used in transportation of keys for protection of user data (e.g., KEK).

The process related to setting up and maintaining keying to protect user data is known as the “TEK Exchange” (see Section 8.2.3) process. During authentication exchange, protection of user data is configured for the CPE. ~~, if a CPE indicates that it does not support protection of user data,~~ ~~no key exchange and state machines used to maintain keying to protect user data will be executed~~The TEK Exchange process shall only be engaged by a CPE, if protection of user data has been configured during the authentication exchange.

If an A-CPE is configured to support operation as Distributed or Centralized A-CPE, shall not initiate TEK Exchange process. Distributed and Centralized A-CPEs shall also not be capable of maintaining/stroing the keying material related to S-CPEs that are attached to the A-BS through them.

The traffic key management portion of the SCM protocol adheres to a client/server model, where the CPE (a SCM “client”) requests keying material and the AAA server (a SCM “server”) responds to those requests. This model provides for an individual CPE to receive keying material for security associations (SAs), for which they are configured.

The SCM protocol uses MAC management messaging, i.e., SCM-REQ and SCM-RSP messages defined in 7.7.21. The SCM protocol is defined in detail in 8.2.

***<End of Modification>***

***Modify the text in section 8.2.2, pg 254 as follows***

***<Start of Modification>***

The Authentication state machine (ASM) adopts an authentication framework similar to the model specified in IEEE Std 802.16-2009. The ASM incorporates EAP authentication and is made up of four states and thirteen events and messages that are used to communicate with other aspects of the SCM framework. The ASM has to interoperate with the TEK state machine (TSM, see 8.2.3) and the EAP Process. In the following sections (see 8.2.2.1 – 8.2.2.7), the term “CPE” refers to S-CPEs as well as A-CPEs.

***<End of Modification>***

***Modify the text in the first paragraph of section 8.2.3.1, pg 260 of base standard as follows***

***<Start of Modification>***

~~If the CPE and BS decide “No authentication” as their authentication policy, t~~The CPE and BS shall not perform the Key Request/Key Reply handshake in either of the following cases:

* The CPE and BS decide “No authentication” as their authentication policy
* The A-CPE is configured to operate as either a Distributed/Centralized A-CPE

In ~~this~~the first case, target SAID value, which may be included in DSA-REQ/RSP messages, shall be Null SAID.

***<End of Modification>***

***Add the following text to the end of sect 8.2.3.2, pg 262 of base standard as follows***

***<Start of Modification>***

In sections 8.2.3.2.1 through 8.2.3.2.5, the term “CPE” refers to both legacy CPEs, S-CPEs, and A-CPEs that are not configured to operate as Distributed/Centralized A-CPEs.

***<End of Modification>***

***Add the following text to the end of sect 8.3.1.2 but prior to Figure 118, on pg 276 of base standard as follows***

***<Start of Modification>***

In Figure 118, “CPE” refers to legacy CPEs, S-CPEs, and Distributed/Centralized A-CPEs.

***<End of Modification>***

***Add the following text to the end of sect 8.3.1.4 but prior to Figure 119, on pg 279 of base standard as follows***

***<Start of Modification>***

In Figure 119, “CPE” refers to legacy CPEs, S-CPEs, and A-CPEs that are not configured to operate as Distributed or Centralized mode.

***<End of Modification>***

# Section 1.E Issues

As of the current revision of this document, no resolution has been agreed upon to handle recommendation 1.E.1 from DCN 22-14/82r0.

# Section 1.F Issues

As of the current revision of this document, no resolution has been agreed upon to handle recommendation 1.F.1, 1.F.2, and 1.F.3 from DCN 22-14/82r0.

# Section 2 Issues

Modifications in this section address 2.1, 2.2, and 2.3 from DCN 22-14/82r0.

***To address issue 2.1, 2.2, and 2.3; modify the 2nd to last paragraph in section 8.2.2.7, pg 260***

***<Start of Modification>***

If the SA defines use of ~~authentication only or~~ “no protection” method (e.g. = 0x00, see Table 193), all MAC PDUs sent with FIDs linked to this SA must have EC bit set to ‘0’ in the generic MAC header. If the SA defines use of any other cryptographic methods (e.g. >= 0x01, see Table 193), ~~Otherwise, if only “authentication+encryption” or “encryption only” is supported~~ the EC bit must be set to ‘1’ in the generic MAC header. Other combinations are not allowed; MAC PDUs presenting other combinations should be discarded.

There are some rules that should be considered for selecting which Cryptopgraphic Suites listed in Table 193 are applicable to CPE:

* Legacy CPEs shall not be capable of being cryptographic Suites that use a 4byte PN value, e.g. suite 0x0C-0x14
* Distributed/Centralized A-CPE may make use of crytopgrahic suites related to DS multicast Group SA (e.g. 0x03, 0x04, 0x0A, 0x0B, 0x0E, 0x0F, 0x13, and 0x14) for MAC management messages sent on the Mulitcast Management FID
* A distributed/centralized A-CPE, S-CPE, or legacy S-CPE shall not be simultaneously configured to use cryptographic suites with 3byte and 4byte PNs on the static Null and Primary SAs, as well as dynamically allocated Group SAs
* A distributed/centralized A-CPE, S-CPE, or legacy S-CPE shall not be simultaneously configured to use cryptographic suites with 4byte and 8byte ICVs on the static Null and Primary SAs, as well as dynamically allocated Group SAs

***<End of Modification>***

***To address issue 2.1 & 2.2, modify Table 193, Section 8.4.1 as follows***

***<Start of Modification>***

|  |  |  |  |
| --- | --- | --- | --- |
| **Cryptographic Suite Value** | **~~Cryptographic Suite~~Key Type** | **PN Size (bytes)** | **ICV Size (bytes)** |
| 0x00 | No Protection (No Authentication, No Encryption) | 0 | 0 |
| 0x01 | Authentication only for Unicast, AES-128 key wrap of TEK using KEK, 3byte PN, 4byte ICV | 3 | 4 |
| 0x02 | Authentication and Encryption for Unicast, AES-128 key wrap of TEK using KEK, 3byte PN, 4byte ICV | 3 | 4 |
| 0x03 | Authentication only for Multicast, AES-128 key wrap of GTEK with GKEK, 3byte PN, 4byte ICV | 3 | 4 |
| 0x04 | Authentication and Encryption for Multicast, AES-128 key wrap of GTEK with GKEK, 3byte PN, 4byte ICV | 3 | 4 |
| 0x05 | Encryption only for Unicast, AES-128 key wrap of TEK using KEK, 3byte PN | 3 | 0 |
| 0x06 | BS random generation of GKEK and GTEK | N/A | N/A |
| 0x07 | Operator-specific function for GKEK and GTEK generation | N/A | N/A |
| 0x08 | Authentication only for Unicast, AES-128 key wrap of TEK using KEK, 3byte PN, 8byte ICV | 3 | 8 |
| 0x09 | Authentication and Encryption for Unicast, AES-128 key wrap of TEK using KEK, 3byte PN, 8byte ICV | 3 | 8 |
| 0x0A | Authentication only for Multicast, AES-128 key wrap of GTEK with GKEK, 3byte PN, 8byte ICV | 3 | 8 |
| 0x0B | Authentication and Encryption for Multicast, AES-128 key wrap of GTEK with GKEK, 3byte PN, 8byte ICV | 3 | 8 |
| 0x0C | Authentication only for Unicast, AES-128 key wrap of TEK using KEK, 4byte PN, 4byte ICV | 4 | 4 |
| 0x0D | Authentication and Encryption for Unicast, AES-128 key wrap of TEK using KEK, 4byte PN, 4byte ICV | 4 | 4 |
| 0x0E | Authentication only for Multicast, AES-128 key wrap of GTEK with GKEK, 4byte PN, 4byte ICV | 4 | 4 |
| 0x0F | Authentication and Encryption for Multicast, AES-128 key wrap of GTEK with GKEK, 4byte PN, 4byte ICV | 4 | 4 |
| 0x10 | Encryption only for Unicast, AES-128 key wrap of TEK using KEK, 4byte PN | 4 | 0 |
| 0x11 | Authentication only for Unicast, AES-128 key wrap of TEK using KEK, 4byte PN, 8byte ICV | 4 | 8 |
| 0x12 | Authentication and Encryption for Unicast, AES-128 key wrap of TEK using KEK, 4byte PN, 8byte ICV | 4 | 8 |
| 0x13 | Authentication only for Multicast, AES-128 key wrap of GTEK with GKEK, 4byte PN, 8byte ICV | 4 | 8 |
| 0x14 | Authentication and Encryption for Multicast, AES-128 key wrap of GTEK with GKEK, 4byte PN, 8byte ICV | 4 | 8 |
| 0x15~~0x08~~-0xFF | Reserved | N/A | N/A |

***<End of Modification>***

***To address issue 2.1, modify Section 8.4.2.1.1 as follows***

***<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, the PN and MMP\_PN shall be incremented by 1.

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 not be used more than once for the purposes of transmitting data. This measure 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, the PN and MMP\_PN shall be incremented by 1.

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 not be used more than once for the purposes of transmitting data. This measure 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>***

***To address issues 2.1, 2.2, and 2.3, Modify the text in Section 8.4.2.1.2 as follows***

***<Start of Modification>***

The ciphersuites allow for authentication and/or encryption of MAC PDUs. If suites 0x01, ~~or~~ 0x03, 0x08, 0x0A, 0x0C, 0x0E, 0x11, or 0x13 is assigned to the SA, then only authentication is provided for any MAC PDUs transmitted on service flows that are mapped to these SAs.

The AES in GCM protocol is applied in the following manner:

1) The Plaintext Payload is processed, generating an Integrity Check Value (ICV) that is 8 bytes long (i.e. for suites 0x08, 0x0A, 0x11, and 0x13) or 4 bytes long (i.e. for suite 0x01, 0x03, 0x0C, 0x0E).

2) The PN value is either 4 bytes (i.e. for suites 0x0C, 0x0E, 0x11 0x13) or 3 bytes (i.e. for suites 0x01, 0x03, 0x08, 0x0A). PN Maintence is described in Seciton 8.4.2.1.1

~~2~~3) Only the ICV is encrypted using the active TEK/GTEK, generating the Ciphertext ICV.

~~3~~4) The Authenticated PDU is formed by prepending the proper PN value to the Plaintext Payload and appending the Ciphertext ICV to the Plaintext Payload form the authenticated PDU (see Figure 120).

This requires the EC bit in the GMH to be set to ~~0~~1. If EC bit is not set to ~~0~~1, the PDU shall be discarded, as this would indicate a conflict between the configured cryptographic suite and how it is being applied.

Figure ~~119~~120 illustrates how MAC PDUs are processed and formatted when suite 0x01, ~~or~~ 0x03, 0x08, 0x0A, 0x0C, 0x0E, 0x11, or 0x13 is configured and the EC bit in GMH is set to ~~0~~1. The Ciphertext ICV is transmitted so that byte index 0 (as enumerated in NIST Special Publication 800-38D) is transmitted first and byte index 7 is transmitted last (i.e., LSB first) for suites 0x08, 0x0A, 0x11, and 0x13. The Ciphertext ICV is transmitted so that byte index 0 (as enumerated in NIST Special Publication 800-38D) is transmitted first and byte index 3 is transmitted last (i.e., LSB first) for suites 0x01, 0x03, 0x0C, 0x0E.

***<End of Modification>***

***To address issues 2.1, 2.2, and 2.3, replace Figure 120 with the following***

***<Start of Modification>***



***<End of Modification>***

***To address issues 2.1, 2.2, and 2.3, Modify the text in Section 8.4.2.1.3 as follows***

***<Start of Modification>***

The ciphersuites allow for authentication and/or encryption of MAC PDUs. If the suites 0x02, ~~or~~ 0x04, 0x09, 0x0B, 0x0D, 0x0F, 0x12, or 0x14 is assigned to the SA, then authentication and encryption is provided for any MAC PDUs transmitted on service flows that are mapped to these SAs.

The AES in GCM protocol is applied in the following manner:

1) The Plaintext Payload is processed, generating an Integrity Check Value (ICV) that is 8 bytes long (i.e. for 0x09, 0x0B, 0x12, 0x14) or 4 bytes long (i.e. for 0x02, 0x04, 0x0D, 0x0F).

2) The PN value is either 4 bytes (i.e. for suites 0x0D, 0x0F, 0x12, 0x14) or 3 bytes (i.e. for suites 0x02, 0x04, 0x09, 0x0B). PN Maintence is described in Seciton 8.4.2.1.1

~~2~~3) Then the ICV is encrypted using the active TEK/GTEK, generating the Ciphertext ICV.

~~3~~4) Then the Plaintext Payload is then encrypted with AES using the active TEK/GTEK, generating a Ciphertext Payload.

4) The encrypted PDU is formed by prepending the proper PN value to the Ciphertext Payload and appending the Ciphertext ICV to the Ciphertext Payload (see Figure 121).

This requires the EC bit in the GMH to be set to 1. If EC bit is not set to 1, the PDU shall be discarded, as this would indicate a conflict between the configured cryptographic suite and how it is being applied.

Figure ~~120~~121 illustrates how MAC PDUs are processed and formatted when suite 0x02, ~~or~~ 0x04, 0x09, 0x0B, 0x0D, 0x0F, 0x12, or 0x14 is configured and the EC bit in GMH is set to 1. The Ciphertext ICV is transmitted so that byte index 0 (as enumerated in NIST Special Publication 800-38D) is transmitted first and byte index 7 is transmitted last (i.e., LSB first) for suites 0x09, 0x0B, 0x12, 0x14. The Ciphertext ICV is transmitted so that byte index 0 (as enumerated in NIST Special Publication 800-38D) is transmitted first and byte index 3 is transmitted last (i.e., LSB first) for suites 0x02, 0x04, 0x0D, 0x0F.

***<End of Modification>***

***To address issues 2.1, 2.2, and 2.3, replace Figure 121 with the following***

***<Start of Modification>***



***<End of Modification>***

***To address issues 2.1, 2.2, and 2.3, Modify the text in Section 8.4.2.1.4 as follows***

***<Start of Modification>***

If ~~the~~ suite 0x05 or 0x10 ~~ciphersuite~~ is assigned to an SA, then MAC PDUs associated with service flows mapped to this SA shall only be protected by encryption and no other cipher suites can be mapped to this SA.

The AES in GCM protocol is applied in the following manner:

1) Processing of the Plaintext Payload is processed, generating the Integrity Check Value (ICV), and encrypting the ICV to generate the Ciphertext ICV is skipped.

2) The PN value is either 4 bytes (i.e. for suite 0x10) or 3 bytes (i.e. for suite 0x05). PN Maintence is described in Seciton 8.4.2.1.1

~~2~~3) Then the Plaintext Payload is then encrypted with AES using the active TEK/GTEK, generating a Ciphertext Payload.

~~3~~4) The encrypted PDU is formed ~~from~~ by prepending the proper PN valu to the Ciphertext Payload.

This requires the EC bit in the GMH to be set to 1. If the EC bit is not set to 1, the PDU shall be discarded, as this would indicate a conflict between the configured cryptographic suite and how it is being applied.

Figure 122 illustrates how MAC PDUs are processed and formatted when suite 0x05 0x10 is configured and the EC bit in GMH is set to 1.

***<End of Modification>***

***To address issues 2.1, 2.2, and 2.3, replace Figure 122 with the following***

***<Start of Modification>***



***<End of Modification>***

***To address issues 2.1 and 2.2, modify the text in Section 8.4.2.2 as follows***

***<Start of Modification>***

The GCM specification (NIST SP 800-38D) defines specific values for several parameters.

The additional authenticated data (AAD) to be used in the GCM process shall be the GMH.

*T* represents the ICV (otherwise known as Message Authentication Code, MAC). This value, as stated in 8.4.2.1, shall be 64 bits (8 octets) long for suites 0x08, 0x09, 0x0A, 0x0B, 0x11, 0x12, 0x13, or 0x14. This value, as stated in 8.4.2.1, shall be 32 bits (4 octets) long for suites 0x01, 0x02, 0x03, 0x04, 0x0C, 0x0D, 0x0E, or 0x0F.

Consistent with the GCM specification, the IV or Initialization Vector is used to initialize the Authenticated Encryption function of GCM. The IV shall be 128 bits (16 octets) long for suites that use a 3byte PN or 136 bits (17 octets) for suites that use a 4byte PN. The IV ~~and~~ shall be constructed according to the procedure defined Section 8.2.1 of NIST Special Publication 800-38D. The IV for suites using the 3byte PN is described in Figure 123. The IV for suites using the 4byte PN is described in Figure 123a.

IV construction for suites using the 3byte PN is ordered as follows:

* The IV shall be 16 bytes long
* Bytes 0 through 3 shall be set to the first 4 bytes of the generic MAC header (thus excluding the HCS). The HCS of the generic MAC header is not included in the IV since it is redundant.
* Bytes 4 through 12 are reserved and shall be set to 0x000000000000.
* Bytes 13 through 15 shall be set to the value of the PN. The PN bytes shall be ordered so that byte 13 shall take the least significant byte and byte 15 shall take the most significant byte.

IV construction for suites using the 4byte PN is ordered as follows:

* The IV shall be 17 bytes long
* Bytes 0 through 3 shall be set to the first 4 bytes of the generic MAC header (thus excluding the HCS). The HCS of the generic MAC header is not included in the IV since it is redundant.
* Bytes 4 through 12 are reserved and shall be set to 0x000000000000.
* Bytes 13 through 16 shall be set to the value of the PN. The PN bytes shall be ordered so that byte 13 shall take the least significant byte and byte 16 shall take the most significant byte.

~~The IV shall be 15 bytes long as shown in8H Figure 123. Bytes 0 through 3 shall be set to the first 4 bytes of the generic MAC header (thus excluding the HCS). The HCS of the generic MAC header is not included in the IV since it is redundant. Bytes 4 through 12 are reserved and shall be set to 0x000000000000. Bytes 13 through 15 shall be set to the value of the PN. The PN bytes shall be ordered so that byte 13 shall take the least significant byte and byte 15 shall take the most significant byte.~~

|  |  |  |  |
| --- | --- | --- | --- |
| Field | Fixed Field | | Invocation Field |
| Byte | 0 3 | 4 12 | 13 15 |
| Data | GMH | *Reserved* | PN |
| Contents | GMH (without HCS) | 0x000000000000000000 | 3byte PN field from Payload |

**Figure 123 – *IV* construction for suites with 3byte PN**

|  |  |  |  |
| --- | --- | --- | --- |
| Field | Fixed Field | | Invocation Field |
| Byte | 0 3 | 4 12 | 13 16 |
| Data | GMH | *Reserved* | PN |
| Contents | GMH (without HCS) | 0x000000000000000000 | 4byte PN field from Payload |

**Figure 123a – *IV* construction for suites with 4byte PN**

Consistent with the GCM specification, pre-counter block J0 is generated using the equations defined in Section 7 of NIST Special Publication 800-38D.

***<End of Modification>***

# Section 3 Issues

As of the current revision of this document, no resolution has been agreed upon to handle recommendation 3.1 - 3.6 from DCN 22-14/82r0.

# Section 4 Issues

Modifications in this section address 4.1, 4.2, and 4.3 from DCN 22-14/82r0.

***Modify the second paragraph in section 7.20.4, pg 178 of the LB2 draft as follows***

***<Start of Modification>***

For self-coexistence in 802.22b networks, the SCW shall be synchronized at all CPEs within a 802.22b network. For synchronizing SCW, an ~~MR-BSA-BS shall transmit~~ either one of the following can be transmitted:

1. BS/A-BS transmits SCH in PHY Mode 1
2. A-BS transmits~~, or~~ Frame Control Header in PHY Mode 2
3. A-BS transmits Frame Control Header + Extended Frame Control Header in PHY Mode 2.

When CPEs receives either one of these transmission the forward it to ~~SCH or Extended Frame Control Header from~~ the ~~MRBS~~A-BS, which~~they~~ synchronizes the SCW within a 802.22b network.

When a distributed scheduling ~~R-CPE~~A-CPE receives the SCW schedule information from the ~~MR-BS~~A-BS, it shall arrange the SCW schedule within a local cell by sending the same information from within either transmission (1), (2), or (3) listed above, which it has ~~of SCH or Extended Frame Control Header~~ received from the its’ serving ~~MRBS~~A-BS to the CPEs in a local cell.

***<End of Modification>***

***Modify text in section 7.20.4.1, pg 179, lines 34-36 of the LB2 draft as follows***

***<Start of Modification>***

6) The ~~MR-BS~~A-BS performs the DS/US Split adjustment mechanism. This can only be done if~~using the relevant parameter exchange carried by the SCH or Extended Frame Control Header (see Table B1) and/or by~~ the CBP burst received directly from the other ~~MR-BS~~A-BSs or received by a CPE and forwarded to A-BS, contains information related to transmission (1), (3), and/or (4) listed in Section 7.20.4. Once it has acquired information on the

***<End of Modification>***

***Modify text in section 7.20.4.2, pg 180 of the LB2 draft as follows***

***<Start of Modification>***

During network entry and initialization and before any data transmission takes place, the ~~MR-BS~~A-BS and CPE shall perform a network discovery procedure by scanning the wireless medium for CBP packets that contain either of the four transmissions listed in Section 7.20.4~~, SCH, FCH , or DRZ-FCH~~. This discovery procedure is part of the ~~MR-BS~~A-BS and CPE initialization procedures described in 7.14.

During normal operation, the ~~MR-BS~~A-BS and CPEs can discover other nearby ~~IEEE 802.22b~~A-WRAN cells by listening to the medium on the look out for CBP packets that contain either one of the four transmissions listed in 7.20.4. These transmissions can be received from other cells on the same channel ~~and, possibly, SCH, FCH or DRZ-FCH~~ or from cells on different channels. This can be accomplished through the scheduling of the Coexistence UIUC = 1 for passive mode SCW. If a CBP packet, containing either one of the transmissions listed in section 7.20.4~~SCH, or FCH is~~ received by the CPE, which is managed by the ~~MR-BS~~A-BS , it shall package that information and transport it to its ~~MR-BS~~A-BS (see Table 172). ~~If a CBP packet or DRZ-FCH is received by the CPE, which is managed by the distributed scheduling R-CPEACPE , it shall package that information and transport it to its distributed scheduling R-CPEA-CPE .~~

***<End of Modification>***

***NOTE: The last sentence was removed because it deviates from the current operation for CBP handling defined in the base standard. In the base standard, the CPEs only forward CBPs captured in passive SCW to BS or forward a CBP generated by BS in an active SCW. This was done to put all the complexity of CBP scheduling, CBP MAC PDU generation, CBP MAC PDU authentication (see 8.6.2 of base standard), SCW scheduling, etc in the BS. Putting any of this complexity into the distributed A-CPE, warrants further discussion. However, there is utility in sending a CBP MAC PDU with information identifying the local cell of the distributed A-CPE. For example, the receiver of the CBP MAC PDU will most likely pick up on the characteristics of the local cell managed by the distributed A-CPE, and not the serving A-BS. Therefore, identification of the local cell and its parameters is useful. Towards this end, we introduce an additional CBP IE that can be added to CBP MAC PDU, that contains the MAC address of the distributed A-CPE that is forwarding a CBP MAC PDU (that would still be generated by the A-BS). This way, the DRZ-FCH is not neededed as an option to be transmitted in CBP MAC PDU.***

***Modify the text in Section 7.6.1.3.1, pg 39 of base standard as follows***

***<Start of Modification>***

CBP packets shall carry at least one information element (IE) in their payload among the set described in Table 9 since it provides the basic information required to enable self-coexistence. CBP packets shall at least carry a Backup/Candidate Channel information element (IE) in their payload. This is to allow WRANs to execute the spectrum etiquette mechanism before deciding to execute the other spectrum sharing mechanisms described in 7.20.3.

If an A-BS is generating a CBP packet to be forwarded by a distributed A-CPE or an S-CPE attached to a distributed S-CPE, it may optionally add “CBP Local Cell ID IE” to the CBP MAC PDU. The purpose of the “CBP Local Cell ID IE” is to provided an identity of the local cell maintained by a distributed A-CPE, the CBP MAC PDU header (which would contain contents of transmission types indicated in 7.20.4) would contain the MAC Address of the A-BS that serves the distributed A-CPE. When the “CBP Local Cell ID IE” is added to a CBP MAC PDU, the transmissions indicated in 7.20.4 would contain the MAC Address of the A-BS in the CBP MAC PDU header.

**Table 9 – CBP IEs**

|  |  |
| --- | --- |
| **Element ID** | **Name** |
| 0x00 | Backup\_and\_Candidate\_Channel\_List\_IE |
| 0x01 | FC\_REQ\_IE |
| 0x02 | FC\_RSP\_IE |
| 0x03 | FC\_ACK\_IE |
| 0x04 | FC\_REL\_IE |
| 0x05 | CBP\_Identificate\_IE |
| 0x06 | Signature\_IE |
| 0x07 | CERT-REQ\_IE |
| 0x08 | CERT-RSP\_IE |
| 0x09 | CBP\_Local\_Cell\_ID\_IE |

***<End of Modification>***

***After Section 7.6.1.3.1.7.3, add a new subsection 7.6.1.3.1.8 titled “CBP Local Cell ID IE” with the following text***

***<Start of Modification>***

**7.6.1.3.1.8 CBP Local Cell ID IE**

The CBP Local Cell ID IE may be added to CBP MAC PDUs that are to be forwarded by a Distributed A-CPE or S-CPEs attached to the Distributed A-CPE. This IE allows the recipient of the CBP MAC PDU containing this IE to distinguish the presence of a local cell from that of CBP MAC PDUs emitted by the A-BS and S-CPEs operating within the serving cell.

**Table xxx – CBP Local Cell ID IE**

|  |  |  |
| --- | --- | --- |
| **Syntax** | **Size** | **Description** |
| CBP\_Local\_Cell\_ID\_IE\_format(){ |  |  |
| Element ID | 8bits | 0x09 |
| Local Cell MAC ID | 48 bits | IEEE 48bit MAC address of distributed A-CPE that manages the local cell |
| } |  |  |

***<End of Modification>***

***Modify text in section 7.20.4.2.1, pg 180 of the LB2 draft as follows***

***<Start of Modification>***

The ~~MR-BS~~A-BS can discover other ~~MR-WRAN~~A-WRAN cells by scheduling SCWs in passive mode, during which, it may request one or more of its CPEs to listen to the current operating channel to look for CBP packets from other ~~MR-WRAN~~A-WRAN s or to listen to other channels for CBP packets. These CBP packets can contain either one of the four transmissions listed in 7.20.4, that originate ~~SCH, FCH or DRZ-FCH transmissions~~ from other ~~MR-BS~~A-BSs or CPEs associated with other ~~MR-BS~~A-BSs.

***<End of Modification>***

***At the bottom of pg 295, Section 8.6.2 of base standard, insert the following text before the sentence “The organization of this subclause is as follows:”***

***<Start of Modification>***

In this section “MAC Address” refers to the IEEE 48-bit MAC address that identifies the BS or A-BS that the CBP MAC PDU is being forwarded on behalf of by a CPE.

***<End of Modification>***

***On pg 301, Section 8.6.2.4.1 of base standard, modify the text for as follows***

***<Start of Modification>***

1) Infrastructure as described in Figure 125 for certificate generation and distribution

2) Recommended EC domain parameters to be used shall be for binary fields on either 223-bit random or Koblitz curves. Example domain parameters can be found in:

i) K-233 or B-233 elliptic curves defined in [FIPS 186-3],

ii) sect233k1 and sect233r1 curves defined in SEC2 [B64]

iii) In the EC domain parameters, elliptic curve points shall be represented in compressed form

3) BS/A-BS/Distributed A-CPE shall be identified by its 48bit MAC Address

4) ‘to -be-signed certificate data’, IU construction is as follows:

- For BSIC: BSIC = IU || BEU , where IU = KeyID || ~~BS~~ MAC Address || CA ID || Key Validity Date (Not Before) ||

Key Validity Date (Not After) || Version, and BEU = BS or A-BS Public Key Reconstruction

Data;

- For CARC: CARC = IU || BEU , where IU = KeyID || ~~BS~~ MAC Address || CA ID || Key Validity Date (Not Before)

|| Key Validity Date (Not After) || Version || EC Domain Parameters, and BEU = CA Public

Key Reconstruction Data

- NOTE — BS MAC Address comes from the BS, the operator NCMS, or the SCH data in the CBP burst

respectively. In addition the A-BS MAC address comes form the FCH PHY Mode 2. The Key ID, Key Validity

Date (Not Before) and Key Validity Time Period are assigned by the CA and are contained in the Implicit

Certificate.

~~3~~4) The CA shall have a public-key pair that selected from the EC domain parameters in Requirement 2 and bound to the CA ID. Entities shall have access to the CA implicit certificate (with the CA’s public key reconstruction data), but no the private key associated with the implicit certificate.

5~~4~~) SHA-256 shall be used as a Hash function.

6~~5~~) If each operator is allowed to maintain its own BS implicit certificates (i.e., act as its own Certificate Authority)

- Operator will register its Certificate Authority ID when registering its Operator ID. Mechanism by registration is

executed is outside the scope of the standard.

- Operators may share their own CA Root certificate with other operators that have BSs/A-BSs that border or

overlap with BSs/A-BSs in their own network. The mechanism for CA Root Certificate sharing is outside the scope

of the standard.

***<End of Modification>***

***In Section 8.6.2.4.2, 8.6.2.4.3, 8.6.2.4.4, 8.6.2.5.1, 8.6.2.5.2, 8.6.2.5.3, and 8.6.2.6 of base standard, replace all references to “BS” with “BS/A-BS”***