Hewlett Packard Enterprise

Technical Note

HPE Aruba Networking WPA3 and Enhanced Open 101

Revision History

Document status: Released

Change Request# (Optional)	Document Version	Date	Prepared / Modified by	Reviewed by	Approved by	Section and Text Revised
	1.0	10/10/2023	Josh Schmelzle			
	1.1	10/13/2023	Josh Schmelzle			References WPA3-Personal WPA3-Enterprise CCM 128
	1.2	11/13/2023	Josh Schmelzle			WPA3 workaround on 8.10 and 10.4 with WPA2-AES + MFP-R
	1.3	11/14/2023	Josh Schmelzle			Updates for WPA3 workaround added in 1.2.
	1.4	11/21/2023	Josh Schmelzle			Updates for WPA3 workaround added in 1.2.

Contents

Terminology

The following terminology is used throughout this technical note. For additional information, refer to sources mentioned in the appendix.

AKM – Authentication and Key Management

BSS – Basic Service Set

CNSA – Commercial National Security Algorithm

DH – Diffie-Hellman

Enhanced Open – Wi-Fi Alliance certification based on OWE

IEEE – Institute of Electrical and Electronics Engineers

OWE – Opportunistic Wireless Encryption

MFP – Management Frame Protection (see PMF)

MFPC – Management Frame Protection Capable

MFPR – Management Frame Protection Required

PMF – Protected Management Frame (see MFP)

PMK – Pairwise Master Key

RSNE – Robust Security Network Element

SAE – Simultaneous Authentication of Equals

WFA – Wi-Fi Alliance

Wi-Fi 6 – Based on IEEE 802.11ax (HE)

Wi-Fi 6E – Wi-Fi 6 extended to include the 6 GHz band

Wi-Fi 7 – Based on IEEE 802.11be (EHT)

WPA2 – Wi-Fi Protected Access version 2

WPA3 – Wi-Fi Protected Access version 3

Introduction

In an increasingly interconnected world, secure and reliable Wi-Fi communication is a must-have. Across home offices to industrial environments to enterprise networks, Wi-Fi has become a crucial part of mobile connectivity. As the reliance on Wi-Fi networks has grown, so has the security to protect and ensure privacy for sensitive data.

Enhanced Open and Wi-Fi Protected Access version 3 (WPA3) are the current advancements in Wi-Fi security standards from the Wi-Fi Alliance (WFA), designed to address weaknesses of their predecessors WPA2 and Open networks. This technical note aims to provide insights into Enhanced Open and WPA3 networks with ArubaOS deployments, exploring key components, practical implications, and best practices. We will also discuss deployment considerations and compatibility aspects.

Authentication and Key Management (AKM)

The security solutions used in Wi-Fi networks are defined by the IEEE 802.11 standards and Wi-Fi Alliance. Each security protocol has a specific authentication and key management (AKM) suite type (number).

The standard defines AKM suite selectors with a format of OUI:N where N represents the suite type. The standards based AKMs are denoted by an OUI of 00-0F-AC. For example, the suite selector for WPA3-Personal (`wpa3-sae-aes`) is 00-0F-AC:8. This technical note may refer to 00-0F-AC:N as AKM:N.

The Wi-Fi Alliance defines security certifications by AKM, cipher suites, and Protected Management Frame (PMF) combinations. The following is used to indicate the different authentication types defined in the standard and their corresponding Wi-Fi Alliance certification program:

- AKM:1 = IEEE 802.1X with SHA-1
  - WPA2-Enterprise
- AKM:2 = Pre-Shared Key (PSK)
  - WPA2-Personal
- AKM:5 = IEEE 802.1X with SHA-256
  - WPA3-Enterprise
- AKM:8 = Simultaneous Authentication of Equals (SAE)
  - WPA3-Personal (with SHA-256)
- AKM:12 = IEEE 802.1X with SHA-384 using CNSA Suite compliant ciphers and EAP method
  - WPA3-Enterprise 192-bit
- AKM:18 = Opportunistic Wireless Encryption (OWE)
  - Enhanced Open
- AKM:24 = Simultaneous Authentication of Equals (SAE) with a variable hash algorithm depending on Diffie-Hellman (DH) group
  - WPA3-Personal (with SHA-256, SHA-384, or SHA-512)

Wi-Fi Alliance Certifications

This section details the specifications defined by the Wi-Fi Alliance security certification programs. A following section will map them to the security modes implemented by HPE Aruba Networking in ArubaOS.

Enhanced Open Specification

The Wi-Fi Alliance Enhanced Open specification defines the following:

- Enhanced Open based on Opportunistic Wireless Encryption (OWE) defined in RFC 8110 (AKM:18)

WPA3 Specification

The Wi-Fi Alliance WPA3 specification defines the following:

- WPA3-Personal (AKM:8 or AKM:24)
- WPA3-Personal Transition (AKM:2 + AKM:8)
- WPA3-Enterprise Only (AKM:5)
- WPA3-Enterprise Transition Mode (AKM:1 + AKM:5)
- WPA3-Enterprise 192-bit mode (AKM:12)

Corresponding Aruba Security Modes

Wi-Fi Alliance Certification	Aruba Key Management	Aruba Security Mode (opmode)
Enhanced Open	Enhanced Open	`enhanced-open`
WPA3-Personal	WPA3-Personal	`wpa3-sae-aes`
WPA3-Enterprise	WPA3-Enterprise (CCM 128)	`wpa3-aes-ccm-128`
	WPA3-Enterprise (GCM 256)	`wpa3-aes-gcm-256`
WPA3-Enterprise 192-bit	WPA3-Enterprise (CNSA)	`wpa3-cnsa`

6 GHz Operation

Wi-Fi 6E is Wi-Fi 6 ‘extended’ to include the 6 GHz band. Extending operation into the 6 GHz band was an opportunity to leave behind some of the legacy requirements which exist for operation in the 2.4 GHz and 5 GHz bands.

The Wi-Fi Alliance (WFA) made the decision to require WPA3 or Enhanced Open as the minimum security modes in the 6 GHz band.

The following legacy security modes not allowed in 6 GHz operation include:

- WPA2-Enterprise or the corresponding transition mode
- WPA2-Personal or the corresponding transition mode
- Open, WPA version 1, TKIP, or WEP

Protected Management Frames

The IEEE 802.11w-2009 amendment (now part of IEEE 802.11-2020) introduced Protected Management Frames (PMF) which addresses the protection of robust management frames. Prior to WPA3 and Enhanced Open, most management frames are not encrypted. Since Wi-Fi is a broadcast medium, any device can eavesdrop or participate as a legitimate or rogue client. Securing management frames also is equally important as data frames. Without PMF, all management frames are sent unprotected in the open. PMF protects a set of robust management frames and augments privacy protections already in place for data frames (802.11i). WPA3 and Enhanced Open require use of PMF.

PMF is also referred to as Management Frame Protection (MFP). When discussing whether Protected Management Frames are optional or required, the terms MFPC (capable) and MFPR (required) will be used. Their configuration options are discussed below. Throughout this technical note the terms PMF and MFP may be used interchangeably.

Three possible configurations exist for Protected Management Frames:

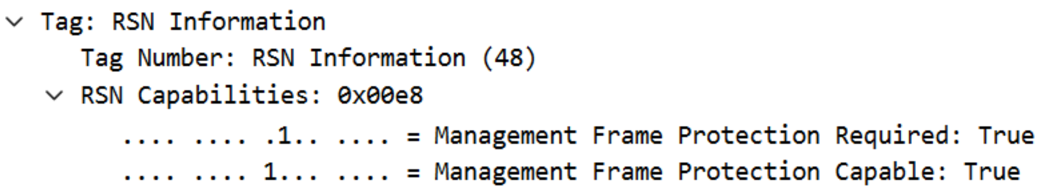
Configuration	Parameters	PMF Capable Client	Non-PMF Client
Disabled	MFPC=0 and MFPR=0	No PMF benefit	No PMF benefit
Capable (Optional)	MFPC=1 and MFPR=0	PMF benefit	No PMF benefit
Mandatory (Required)	MFPC=1 and MFPR=1	PMF benefit	Cannot connect

PMF helps secure robust management frames against various attacks. The key security component is to protect against passive eavesdropping, prevent forgery of unicast and multicast action frames, allow replay detection, and prevent stations from masquerading as another station. PMF protects against forged disassociation and de-authentication frames post association.

Examples of protected robust action frames include:

- Channel Switch Announcements
- QoS
- ADDBA Negotiation
- Block ACK
- Radio Measurement
- Security Association (QA) Query
- Wireless Network Management

PMF support is advertised in the RSN Capabilities of the RSNE which can be found in beacons, probe responses, and association responses.



```
⌄ Tag: RSN Information
    Tag Number: RSN Information (48)
  ⌄ RSN Capabilities: 0x00e8
      .... .... .1.. .... = Management Frame Protection Required: True
      .... .... 1... .... = Management Frame Protection Capable: True
```

Figure 1 – RSN Capabilities example showing MFPC=1 and MFPR=1

ArubaOS specifics:

- PMF is not user configurable for WPA3 or Enhanced Open security modes and MFPC (Capable) and MFPR (Required) configuration is automatic.

Enhanced Open

Open Wi-Fi networks transport and pass data in the clear. Enhanced Open provides unauthenticated data encryption and protects data from sniffers in open Wi-Fi networks.

Encryption is provided by Opportunistic Wireless Encryption (OWE) defined in RFC 8110. With OWE, the client and AP performs an unauthenticated Diffie-Hellman key exchange which results in a unique pairwise secret key (PMK). The resulting key is used in a 4-way handshake post association to generate the traffic encryption keys.

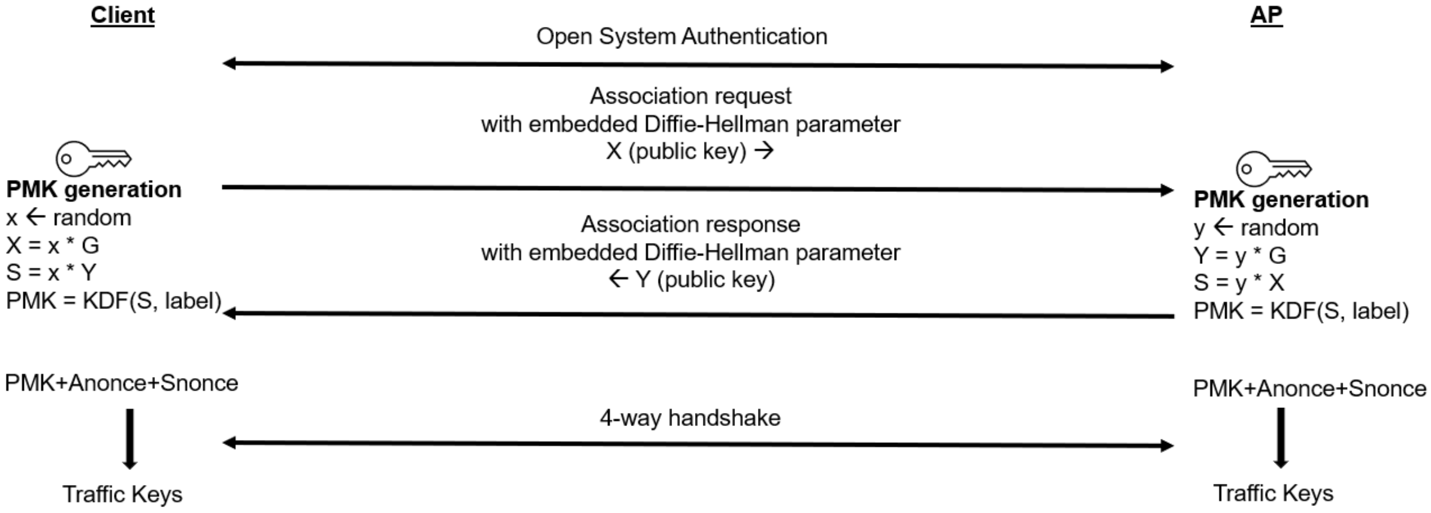
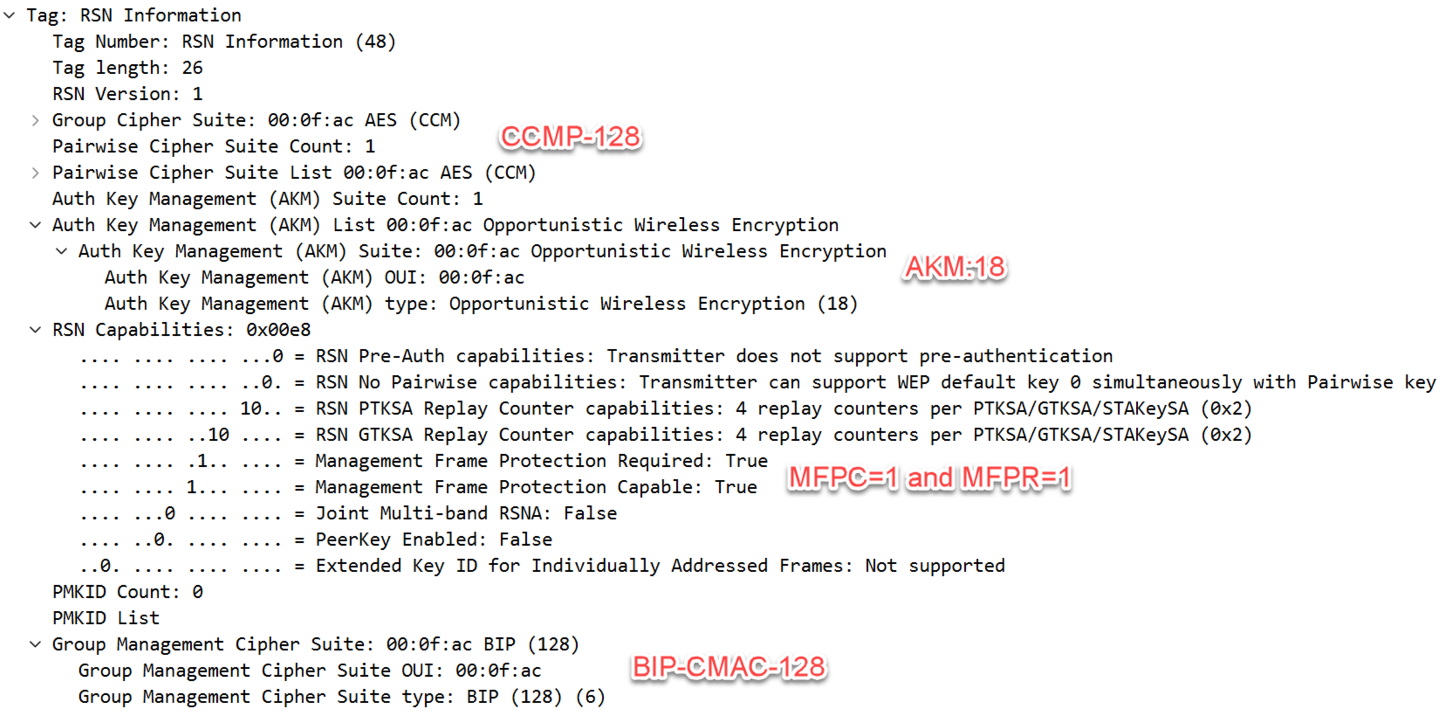


Figure 2 – Enhanced Open (OWE) illustration of operations

The resulting benefit is a Wi-Fi network more secure than a shared and public PSK because it is not susceptible to a passive attack which results in an attacker being able to eavesdrop, forge, and replay frames on the network. Enhanced Open is also easier to deploy because there is nothing to provision. There is no password.

Enhanced Open advertises or negotiates the following capabilities in beacons, probe response, or association (figure 3 on the next page):

- AKM suite selector as 00-0F-AC:18 (OWE).
- Pairwise cipher suite selector as 00-0F-AC:4 (CCMP-128), 00-0F-AC:8 (GCMP-128), 00-0F-AC:9 (GCMP-256), or 00-0F-AC:10 (CCMP-256) could be negotiated.
- Group data cipher suite selector as 00-0F-AC:4 (CCMP-128).
- Group management cipher suite selector as 00-0F-AC:6 (BIP-CMAC-128).
- Protected Management Frames are mandatory (MFPC=1 and MFPR=1).



```
⌄ Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 26
    RSN Version: 1
  › Group Cipher Suite: 00:0f:ac AES (CCM)
    Pairwise Cipher Suite Count: 1
  › Pairwise Cipher Suite List 00:0f:ac AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
  ⌄ Auth Key Management (AKM) List 00:0f:ac Opportunistic Wireless Encryption
    ⌄ Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption
        Auth Key Management (AKM) OUI: 00:0f:ac
        Auth Key Management (AKM) type: Opportunistic Wireless Encryption (18)
  ⌄ RSN Capabilities: 0x00e8
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... .1.. .... = Management Frame Protection Required: True
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
    PMKID Count: 0
    PMKID List
  ⌄ Group Management Cipher Suite: 00:0f:ac BIP (128)
      Group Management Cipher Suite OUI: 00:0f:ac
      Group Management Cipher Suite type: BIP (128) (6)
```

Figure 3 – Enhanced Open (OWE) RSNE

Best Practices

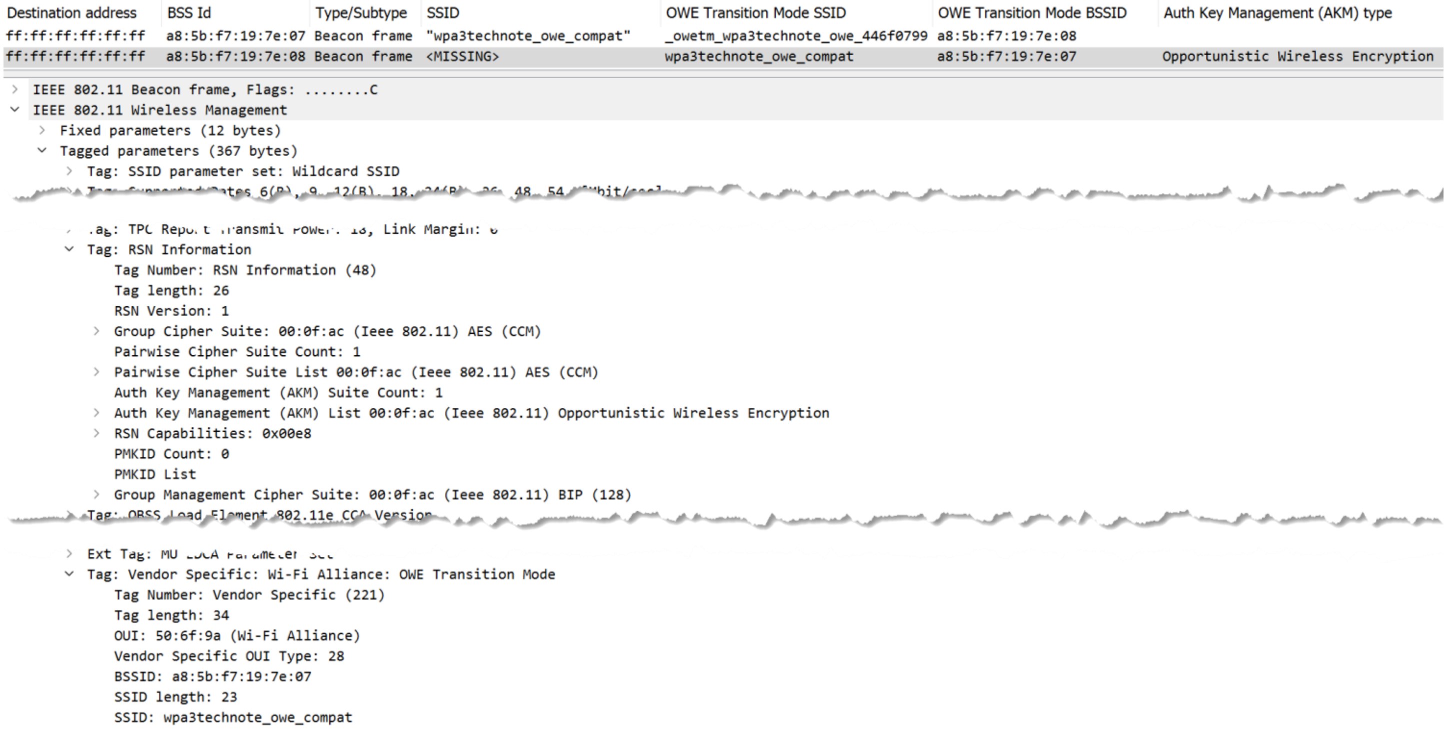
Enhanced Open is suitable for use-cases such as captive portals, coffee shops, cafés, schools, enterprises, public venues like airports, stadiums, etc., anywhere that encryption is needed but identity and authentication is not.

Enhanced Open Transition Mode

Enhanced Open Transition Mode (OWETM) offers a backwards compatible transition from unencrypted Open Wi-Fi networks. OWETM provides the ability for non-OWE clients (Open) and OWE capable clients to connect to the same Wi-Fi network.

This is accomplished by creating and broadcasting two Basic Service Sets (BSSes) with separate beacons for each Virtual AP. Both BSSes point at the other through the OWE Transition Mode IE (figure 4).

- BSS-1 for Open for non-OWE clients with the IE to indicate BSS-2.
- BSS-2 for “hidden” OWE with a zero length SSID (hidden) and the IE to indicate BSS-1.



```
Destination address  BSS Id             Type/Subtype  SSID                       OWE Transition Mode SSID          OWE Transition Mode BSSID  Auth Key Management (AKM) type
ff:ff:ff:ff:ff:ff    a8:5b:f7:19:7e:07  Beacon frame  "wpa3technote_owe_compat"  _owetm_wpa3technote_owe_446f0799  a8:5b:f7:19:7e:08
ff:ff:ff:ff:ff:ff    a8:5b:f7:19:7e:08  Beacon frame  <MISSING>                  wpa3technote_owe_compat           a8:5b:f7:19:7e:07          Opportunistic Wireless Encryption

> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (367 bytes)
    > Tag: SSID parameter set: Wildcard SSID
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

    > Tag: TPC Report Transmit Power: 18, Link Margin: 0
    v Tag: RSN Information
        Tag Number: RSN Information (48)
        Tag length: 26
        RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
        Pairwise Cipher Suite Count: 1
      > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
        Auth Key Management (AKM) Suite Count: 1
      > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption
      > RSN Capabilities: 0x00e8
        PMKID Count: 0
        PMKID List
      > Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
    > Tag: QBSS Load Element 802.11e CCA Version

    > Ext Tag: MU EDCA Parameter Set
    v Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode
        Tag Number: Vendor Specific (221)
        Tag length: 34
        OUI: 50:6f:9a (Wi-Fi Alliance)
        Vendor Specific OUI Type: 28
        BSSID: a8:5b:f7:19:7e:07
        SSID length: 23
        SSID: wpa3technote_owe_compat
```

Figure 4 – Enhanced Open (OWE) Transition Mode RSNE example

The beacon and probe response frames of the Open BSS includes an OWE Transition Mode IE to encapsulate the BSSID and SSID of the OWE BSS.

- The Open BSS and associated clients do not benefit from Protected Management Frames or data encryption.

The beacon and probe response frames from the OWE BSS include an OWE Transition Mode IE to encapsulate the BSSID and SSID of the Open BSS.

- The Beacon frame from the OWE BSS will be zero length and includes the OWE Authentication and Key Management (AKM) selector (00-0F-AC) of AKM:18 in the RSNE.
- PMF is required (MFPC=1 and MFPR=1) for the OWE BSS.
- The OWE client benefits from both encryption and PMF.

The OWE client discovers the OWE AP by using active or passive scanning.

Note

A drawback of Enhanced Open in transition mode is one additional BSS is advertised for every OWE BSS which needs to be accounted for. Another drawback is the unencrypted Open BSS.

WPA3-Personal

Offline dictionary attacks against WPA2-Personal have been widely known for well over two decades. Originally introduced for mesh security in IEEE 802.11-2016, Simultaneous Authentication of Equals (SAE) replaces the Pre-Shared Key (PSK) found in WPA2-Personal with a password-based authentication method resistant to dictionary attacks. Both SAE and PSK are password provisioned but with differences in implementation.

Certain venues offer free Wi-Fi networks using a shared and public PSK. Some incorrectly believe their Wi-Fi traffic is secured with a PSK. For these venues that intend to offer better data protection for their users, SAE offers a more secure password-based option than a shared and public PSK. This is because the master key (PMK) resulting from SAE is not solely based on the password. With PSK, the password directly derives the master key and knowledge of the password enables decryption, replay, and forgery of data frames.

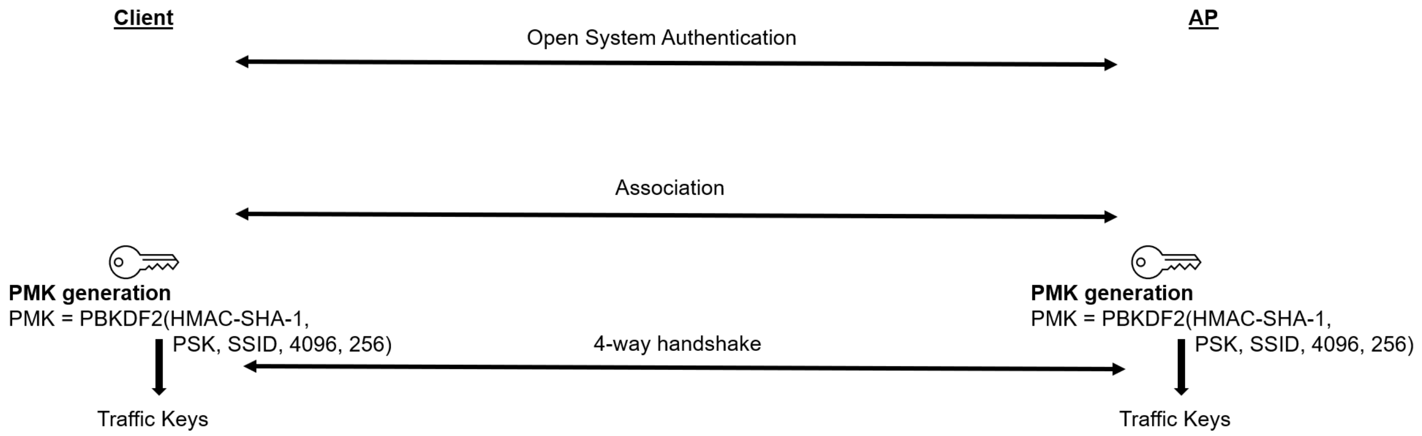

Client
AP
Open System Authentication
Association
PMK generation
PMK = PBKDF2(HMAC-SHA-1, PSK, SSID, 4096, 256)
4-way handshake
PMK generation
PMK = PBKDF2(HMAC-SHA-1, PSK, SSID, 4096, 256)
Traffic Keys
Traffic Keys

Figure 5 – WPA2-Personal (PSK) illustration of operations

With SAE, the password is used in a zero-knowledge proof cryptographic function to derive a unique pairwise master key (PMK) per client. The password is used to index a secret point on an elliptic curve. The point on the curve becomes the generator for use in a cryptographic exchange. This means the password or password-derived data is never sent over the air. Knowledge of the password cannot decrypt SAE encrypted data frames. The PMK is needed to decrypt SAE encrypted data frames and the only parties that know the PMK are the client and AP which performed SAE. This means the SAE protocol is resistant to active, passive, and dictionary attacks.

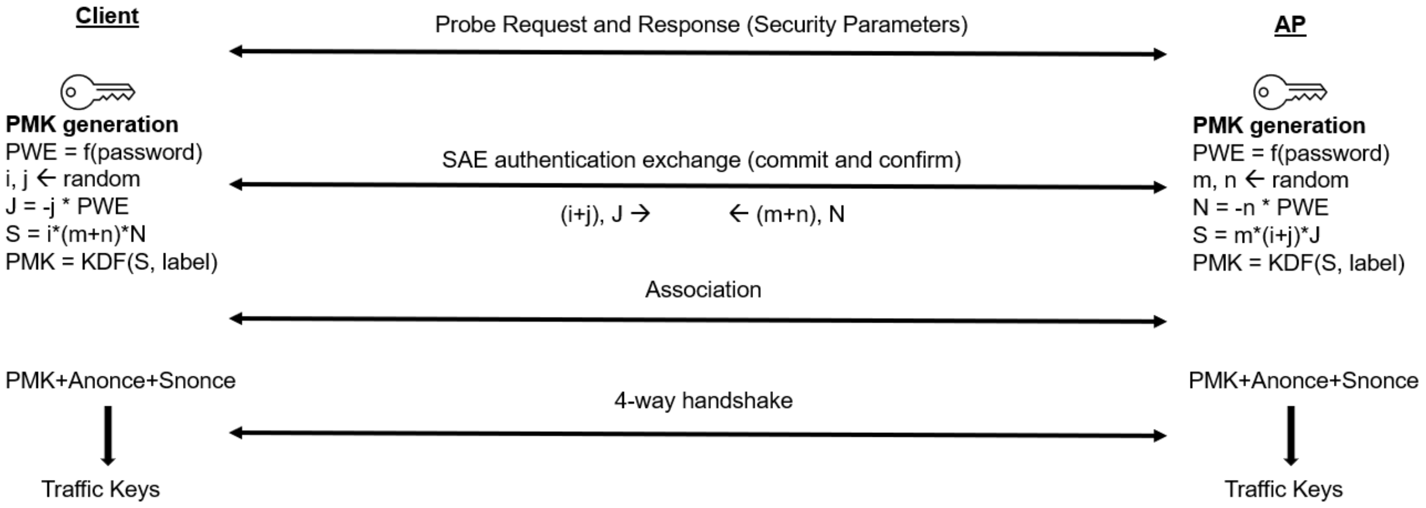


Figure 6 – WPA3-Personal (SAE) illustration of operations

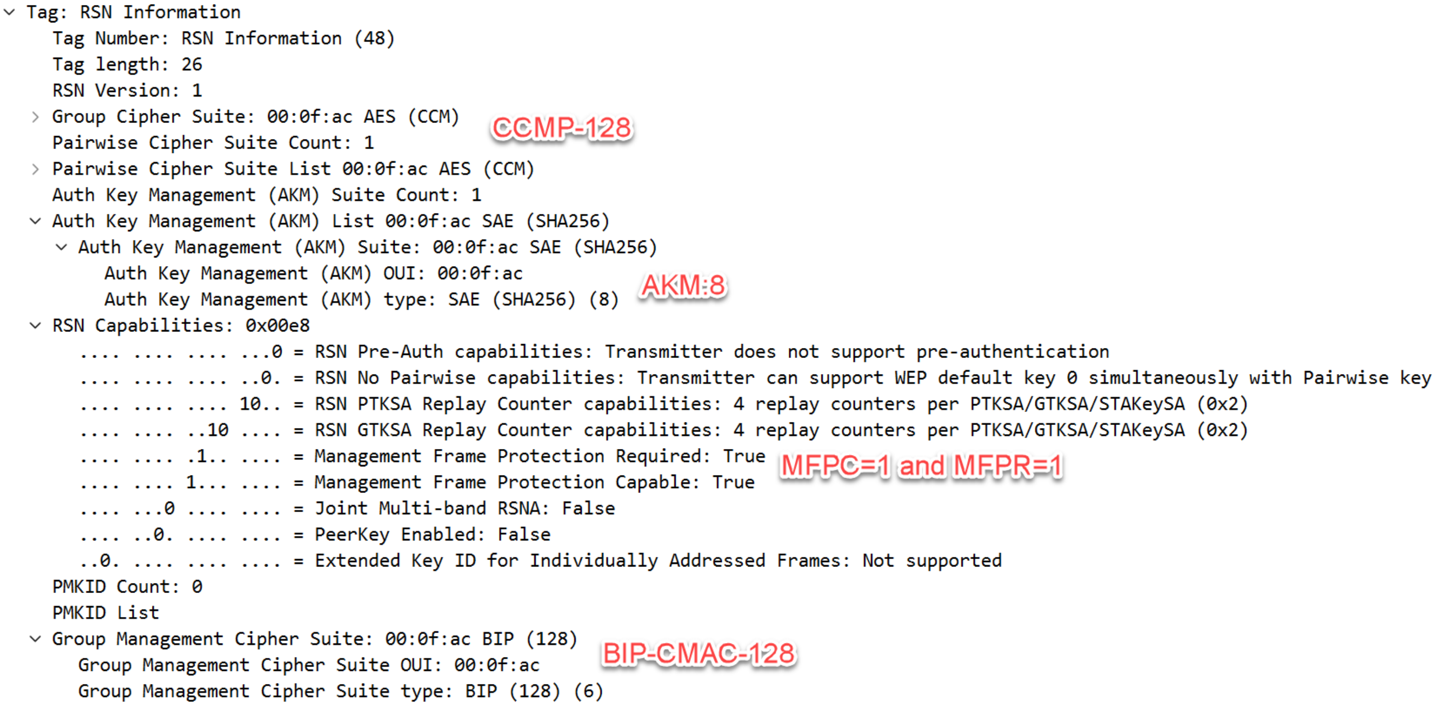
WPA3-Personal advertises or negotiates the following capabilities in beacons, probe response, or association:

- AKM suite selector as AKM:8 (SAE) or AKM:24 (SAE)*

Note

When AKM:24 (SAE) is negotiated, Hash-to-Element (H2E) is enforced. With AKM:24, the hash algorithm is based on the Diffie-Hellman (DH) group used with SAE. For example, a prime with a length of 384 (p384) will use SHA-384 instead of SHA-256. Wi-Fi 7 devices must use AKM:24 for WPA3-Personal. GCMP-256 for cipher suites and BIP-GMAC-256 for group management may be advertised with AKM:24.

- Pairwise cipher suite selector as 00-0F-AC:4 (CCMP-128).
- Group data cipher suite selector as 00-0F-AC:4 (CCMP-128).
- Group management cipher suite selector as 00-0F-AC:6 (BIP-CMAC-128).
- Protected Management Frames are mandatory (MFPC=1 and MFPR=1).



```
⌄ Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 26
    RSN Version: 1
  > Group Cipher Suite: 00:0f:ac AES (CCM)
    Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List 00:0f:ac AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
  ⌄ Auth Key Management (AKM) List 00:0f:ac SAE (SHA256)
    ⌄ Auth Key Management (AKM) Suite: 00:0f:ac SAE (SHA256)
        Auth Key Management (AKM) OUI: 00:0f:ac
        Auth Key Management (AKM) type: SAE (SHA256) (8)
  ⌄ RSN Capabilities: 0x00e8
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... .1.. .... = Management Frame Protection Required: True
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
    PMKID Count: 0
    PMKID List
  ⌄ Group Management Cipher Suite: 00:0f:ac BIP (128)
      Group Management Cipher Suite OUI: 00:0f:ac
      Group Management Cipher Suite type: BIP (128) (6)
```

Figure 7 – WPA3-Personal RSNE example

Best Practices

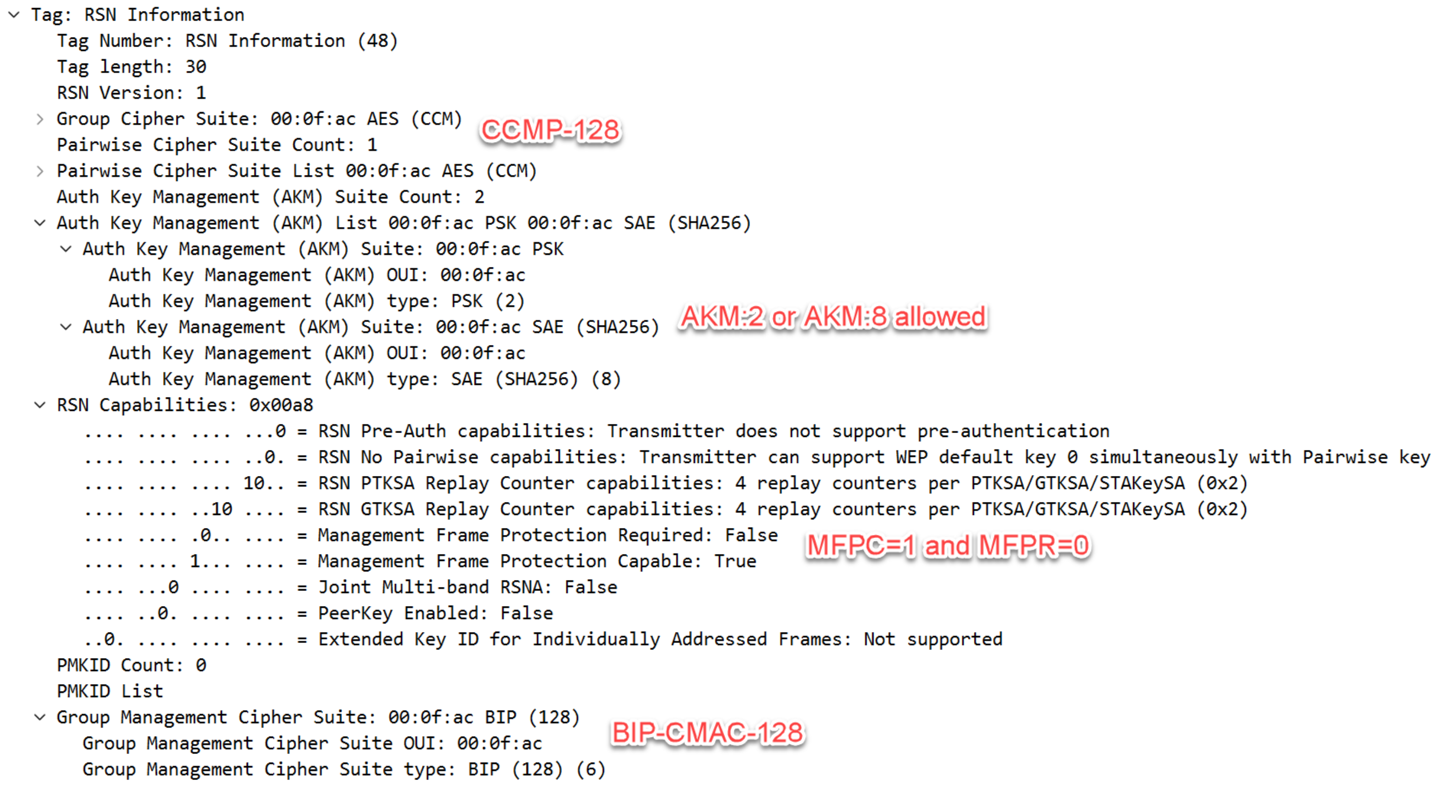
WPA3-Personal is suitable for use-cases where WPA2-Personal was used before as it provides better security, even when a non-complex password is used. WPA3-Personal provides encryption and authentication.

WPA3-Personal Transition Mode

WPA3-Personal may be deployed in transition mode that allows both SAE clients and PSK clients to connect to the same Basic Service Set (BSS), which is a mixed mode of operation. The beacon or probe response contains an AKM list in the RSNE which will contain both PSK (AKM:2) and SAE (AKM:8).

This means the password is shared between WPA2-Personal and WPA3-Personal. The WPA2-Personal network is still vulnerable to all the classic issues. If an attacker gains knowledge of the password by attacking WPA2-Personal, they will get access to the network, but will not be able to decrypt WPA3-Personal sessions.

Due to the same BSS servicing both WPA2-Personal (PSK) and WPA3-Personal (SAE) clients, Protected Management Frames are optional (MFPC=1 and MFPR=0) for WPA3-Personal Transition networks.



```
v Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 30
    RSN Version: 1
  > Group Cipher Suite: 00:0f:ac AES (CCM)
    Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List 00:0f:ac AES (CCM)
    Auth Key Management (AKM) Suite Count: 2
  v Auth Key Management (AKM) List 00:0f:ac PSK 00:0f:ac SAE (SHA256)
    v Auth Key Management (AKM) Suite: 00:0f:ac PSK
        Auth Key Management (AKM) OUI: 00:0f:ac
        Auth Key Management (AKM) type: PSK (2)
    v Auth Key Management (AKM) Suite: 00:0f:ac SAE (SHA256)
        Auth Key Management (AKM) OUI: 00:0f:ac
        Auth Key Management (AKM) type: SAE (SHA256) (8)
  v RSN Capabilities: 0x00a8
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... .0.. .... = Management Frame Protection Required: False
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
    PMKID Count: 0
    PMKID List
  v Group Management Cipher Suite: 00:0f:ac BIP (128)
      Group Management Cipher Suite OUI: 00:0f:ac
      Group Management Cipher Suite type: BIP (128) (6)
```

CCMP-128

AKM:2 or AKM:8 allowed

MFPC=1 and MFPR=0

BIP-CMAC-128

Figure 8 – WPA3-Personal Transition Mode RSNE example

Note

A drawback of WPA3-Personal in transition mode includes downgrade attacks where attackers target PSK rather than SAE to gain network access or force clients that support SAE into connecting to a rogue PSK network.

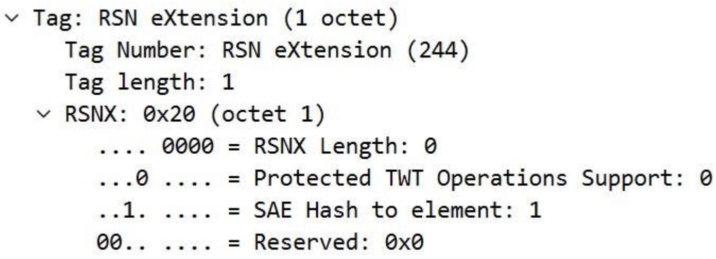
Consider disabling transition mode to limit attack vectors. Consider deploying WPA3-Personal and WPA2-Personal on different individual VAPs and logically separated and isolated network segments, and if you do so make sure to use different credentials on the WPA3-Personal and WPA2-Personal networks.

For more details on these vulnerabilities, which was published under the name of Dragonblood, see https://blogs.arubanetworks.com/solutions/dragonblood-an-analysis-of-the-wpa3-sae-handshake.

Hash-to-Element (H2E)

Hash-to-element (also referred to as hash-to-curve or direct hashing) is a cryptographic method for generation of the password element (PWE) which replaces the weaker and original hunting-and-pecking (also referred to as looping) method for SAE. With hash-to-element, SAE (WPA3-Personal) is further resistant to side-channel attacks and timing attacks.

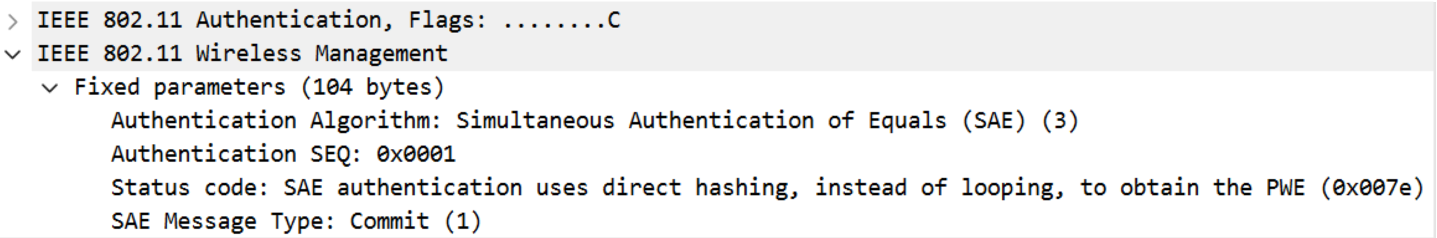
SAE H2E capability can be found in beacon and probe response frames in the extended RSN capabilities field of the RSN eXtension element (RSNXE).



```
˅ Tag: RSN eXtension (1 octet)
    Tag Number: RSN eXtension (244)
    Tag length: 1
  ˅ RSNX: 0x20 (octet 1)
      .... 0000 = RSNX Length: 0
      ...0 .... = Protected TWT Operations Support: 0
      ..1. .... = SAE Hash to element: 1
      00.. .... = Reserved: 0x0
```

Figure 9 – RSNXE example

Status code 126 found in the authentication frame from the client indicates which method is used.



```
› IEEE 802.11 Authentication, Flags: ........C
˅ IEEE 802.11 Wireless Management
  ˅ Fixed parameters (104 bytes)
      Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
      Authentication SEQ: 0x0001
      Status code: SAE authentication uses direct hashing, instead of looping, to obtain the PWE (0x007e)
      SAE Message Type: Commit (1)
```

Figure 10 – SAE authentication frame example

ArubaOS behavior starting in ArubaOS 8.10 and 10.4:

- Operation in the 2.4 GHz and 5 GHz bands:
  - Hash-to-element (H2E) is preferred but allows hunting-and-pecking if the client does not support H2E.
- Operation in the 6 GHz band:
  - Enforces use of H2E and does not allow hunting-and-pecking.

Support for hash-to-element (H2E) is mandatory for WPA3 certified devices. Clients started supporting H2E in 2021:

- Android 12+
- Linux wpa_supplicant v2.10+ (see `sae_pwe` parameter for configuration)
- macOS Catalina+
- Windows 10 21H2+

WPA3-Enterprise

Aruba offers three different modes of operation for WPA3-Enterprise: 128 CCM, 256 GCM, and CNSA.

- 128 CCM offers the widest compatibility, including WPA2-certified clients when deployed in transition mode.
- 256 GCM restricts to WPA3-certified clients that support GCMP-256 ciphers.
- CNSA constrains the available options used with WPA3-Enterprise with the intent to raise the bar of attack sophistication making CNSA suitable for some of the highest levels of data protection.

WPA3-Enterprise 128 CCM

WPA3-Enterprise 128 CCM meets the requirements for two modes of operation for WPA3-Enterprise as specified by the Wi-Fi Alliance.

- "WPA3-Enterprise transition mode" which advertises key management for both WPA2-Enterprise and WPA3-Enterprise clients and sets PMF to optional (when operating in the 2.4 GHz and 5 GHz bands).
- "WPA3-Enterprise only mode" which advertises key management for only WPA3-Enterprise configured clients and requires PMF (across all bands of operation). This is the behavior when transition mode configuration is explicitly disabled.

WPA3-Enterprise 128 CCM in transition mode (default behavior) advertises or negotiates the following capabilities in beacons, probe response, or association in the 2.4 GHz and 5 GHz bands of operation:

- AKM suite selectors include 00-0F-AC:1 (802.1X with SHA-1) and 00-0F-AC:5 (802.1X with SHA-256).
- Protected Management Frames are capable and automatically set as optional (MFPC=1 and MFPR=0).
- This mode supports both WPA2-Enterprise only clients to connect with WPA2 (AKM:1) and WPA3-Enterprise capable clients to connect with WPA3 (AKM:5).

WPA3-Enterprise 128 CCM with transition mode disabled (WPA3-Enterprise only mode) advertises or negotiates the following capabilities in beacons, probe response, or association in the 2.4 GHz and 5 GHz bands of operation:

- AKM suite selector as 00-0F-AC:5 (802.1X with SHA-256).
- Protected Management Frames are required and automatically set as mandatory (MFPC=1 and MFPR=1).
- This mode only supports WPA3-Enterprise capable client connection with WPA3 (AKM:5).

When operating in the 6 GHz band, WPA3-Enterprise 128 CCM is automatically set as "WPA3-Enterprise only mode", and advertises or negotiates the following capabilities in beacons, probe response, or association:

- AKM suite selector as 00-0F-AC:5 (802.1X with SHA-256).
- Protected Management Frames are required and automatically set as mandatory (MFPC=1 and MFPR=1).
- This mode only supports WPA3-Enterprise capable client connection with WPA3 (AKM:5).

WPA3-Enterprise 128 CCM advertises or negotiates the following ciphers in all modes of operation in beacons, probe response, or association:

- Pairwise cipher suite selector as 00-0F-AC:4 (CCMP-128).
- Group data cipher suite selector as 00-0F-AC:4 (CCMP-128).
- Group management cipher suite selector as 00-0F-AC:6 (BIP-CMAC-128).

Note

Key management and Protected Management Frames configuration for WPA3-Enterprise 128 CCM varies depending on band of operation and ArubaOS version deployed. Transition mode is supported starting in ArubaOS 8.11 and 10.5. ArubaOS 8.10 and 10.4 behavior is different where WPA3-Enterprise clients will negotiate connectivity using WPA2 in 2.4 and 5 GHz operation. Please review following pages for specifics.

ArubaOS 8.10 and 10.4 specific behavior for WPA3 Enterprise CCM 128

- Transition mode configuration has no effect on operation.
- **2.4 GHz and 5 GHz operation:**
  - 00-0F-AC:1 (802.1X with SHA-1) is advertised in the RSNE.

Note

00-0F-AC:5 (802.1X with SHA-256) is not advertised with CCM 128 in ArubaOS 8.10 or 10.4. This means WPA3 capable clients will negotiate connectivity as WPA2 because only AKM:1 is advertised by the AP.

  - PMF is optional (MFPC=1 and MFPR=0).
- 6 GHz operation:
  - 00-0F-AC:5 (802.1X with SHA-256) is advertised in the RSNE.
  - PMF is required (MFPC=1 and MFPR=1).

WPA3 only CCM 128 workaround

If there is a requirement to restrict connectivity to “WPA3-Enterprise Only Mode” while using CCMP-128 ciphers on 8.10 or 10.4 deployments, consider the following workaround and caveats:

- The WPA2-Enterpise security mode (`wpa2-aes`) with PMF configured as mandatory (MFPC=1 and MFPR=1) effectively uses WPA3-Enterprise (AKM:5) for key management instead of WPA2-Enterprise (AKM:1).
- Use cases for this workaround:
  - “WPA3-Enterprise Only Mode” with no support for legacy WPA2-Enterprise clients.
  - ArubaOS 8.10 or 10.4 deployments.
- To deploy this workaround two configurations are required.
  - 1) Security mode set as WPA2-Enterprise (`wpa2-aes`)
  - 2) PMF set as mandatory (MFPC=1 and MFPR=1)
    - Instant 8 configuration for MFP via CLI (`mfp-capable` and `mfp-required` parameters), Central template group, or Central REST API.
    - AOS 8 configuration for MFP via WebUI, CLI, or local REST API.
    - AOS 10 configuration for MFP via Central REST API.
- Caveats:
  - This workaround does not support 6 GHz operation.
  - AOS 8 forwarding mode caveats:
    - PMF operation for Wi-Fi 5 APs requires use of decrypt-tunnel mode.
    - PMF operation in tunnel mode is supported starting with Wi-Fi 6 APs.
  - When this workaround is deployed and a capable deployment is being upgraded to an 8.11 release, upgrade to at least 8.11.2.1 or later due to a multicast encryption mismatch bug present in earlier 8.11 releases.

WPA3 only CCM 128 workaround (continued)

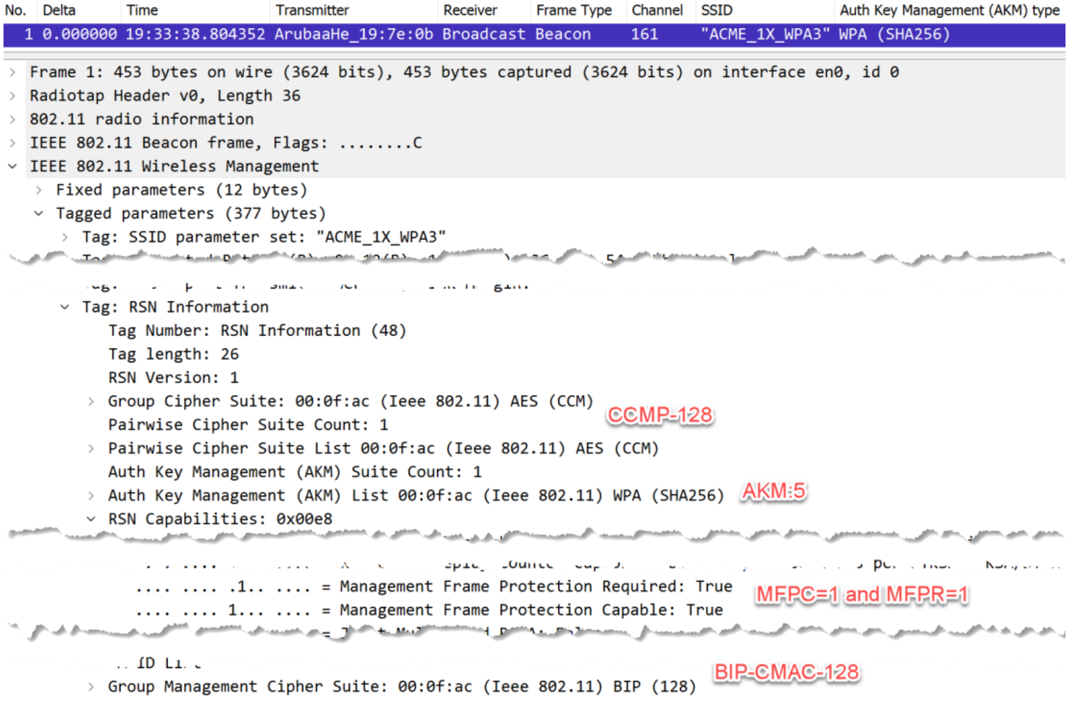
Example ArubaOS 8.10 configuration:

```
# WPA3 only key management for 2.4 GHz & 5 GHz using wpa2-aes + mfp-capable + mfp-required configuration
wlan ssid-profile "ACME_1X_WPA3"
    essid "ACME_1X_WPA3"
    opmode wpa2-aes
    mfp-capable
    mfp-required
!
```

Example ArubaOS 8.10 verification:

```
(MCR) [mynode] #show wlan ssid-profile ACME_WPA3_Enterprise

SSID Profile "ACME_1X_WPA3"
-------------------------------------
Parameter                                                Value
---------                                                -----
SSID enable                                              Enabled
ESSID                                                    ACME_1X_WPA3
Encryption                                               wpa2-aes
Enable Management Frame Protection (for WPA2 opmodes)    Enabled
Require Management Frame Protection (for WPA2 opmodes)  Enabled
```



```
No. Delta    Time            Transmitter          Receiver  Frame Type Channel SSID           Auth Key Management (AKM) type
  1 0.000000 19:33:38.804352 ArubaaHe_19:7e:0b    Broadcast Beacon     161     "ACME_1X_WPA3" WPA (SHA256)

> Frame 1: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface en0, id 0
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (377 bytes)
    > Tag: SSID parameter set: "ACME_1X_WPA3"

    v Tag: RSN Information
        Tag Number: RSN Information (48)
        Tag length: 26
        RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
        Pairwise Cipher Suite Count: 1
      > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
        Auth Key Management (AKM) Suite Count: 1
      > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA (SHA256)
      v RSN Capabilities: 0x00e8

          .... .... .1.. .... = Management Frame Protection Required: True
          .... .... 1... .... = Management Frame Protection Capable: True

      > Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
```

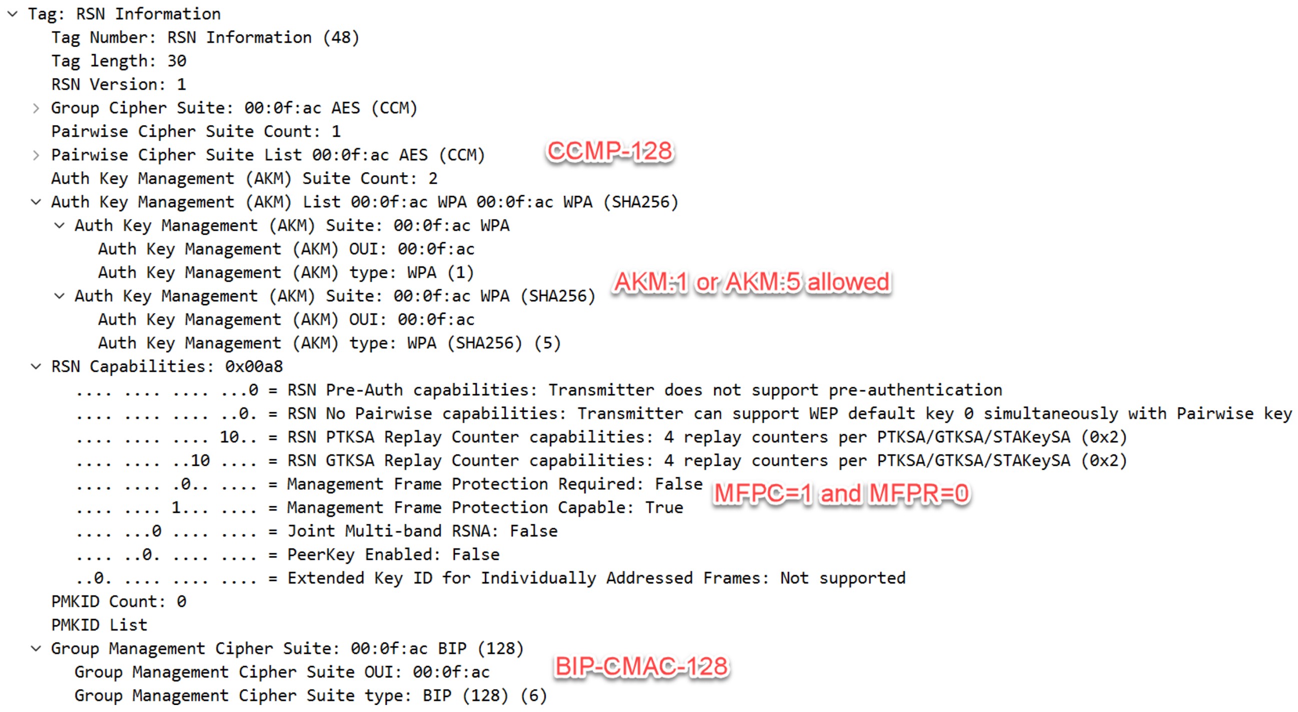
Figure 11 – WPA3 only CCM 128 workaround example beacon frame.

WPA3 only CCM 128 workaround (continued)

- When configured and supported, the following capabilities are advertised or negotiated in beacons, probe response, or association in the 2.4 GHz or 5 GHz bands:
    - AKM suite selector as 00-0F-AC:5 (802.1X with SHA-256).
    - Pairwise cipher suite selector as 00-0F-AC:4 (CCMP-128).
    - Group data cipher suite selector as 00-0F-AC:4 (CCMP-128).
    - Group management cipher suite selector as 00-0F-AC:6 (BIP-CMAC-128).
    - Protected Management Frames are mandatory (MFPC=1 and MFPR=1).
- When configured and not supported, such as by Wi-Fi 5 APs in tunnel mode on AOS 8, the following capabilities are advertised or negotiated in beacons, probe response, or association in the 2.4 GHz or 5 GHz bands:
    - AKM suite selector as 00-0F-AC:1 (802.1X with SHA-1).
    - Pairwise cipher suite selector as 00-0F-AC:4 (CCMP-128).
    - Group data cipher suite selector as 00-0F-AC:4 (CCMP-128).
    - Protected Management Frames are disabled (MFPC=0 and MFPR=0).
- After some period of implementation and a new deployment requirement arises for 6 GHz operation, for example when 6 GHz capable hardware is added, consider the following upgrade and configuration migration to maintain consistency in advertised key management:
    - 1)
        - AOS 8: Upgrade to 8.11.2.1 or later.
        - AOS 10: Upgrade to 10.5 or later.
    - 2)
        - Change the security mode from WPA2-Enterprise (`wpa2-aes`) to WPA3-Enterprise CCM 128 (`wpa3-aes-ccm-128`).
        - Disable transition mode to disable support for WPA2 clients using AKM:1.
            - Transition mode configuration for WPA3-Enterprise CCM 128 is supported starting in 8.11 and 10.5 and is enabled by default advertising both AKM:1 and AKM:5.
    - 3)
        - AOS 8: Configure “Allow 6GHz band” on respective VAP.
        - AOS 10: Enable 6 GHz band in respective WLAN configuration.

ArubaOS 8.11 and 10.5 specific behavior for WPA3-Enterprise CCM 128

- Support for transition mode is introduced for WPA3-Enterprise CCM 128.
- When transition mode is enabled (default), the behavior is as follows:
  - 2.4 GHz and 5 GHz operation:
    - Both 00-0F-AC:1 (802.1X with SHA-1) and 00-0F-AC:5 (802.1X with SHA-256) are advertised in the RSNE.
    - Capable clients can negotiate using WPA2 or WPA3.
    - PMF is optional (MFPC=1 and MFPR=0).
  - 6 GHz operation:
    - 00-0F-AC:5 (802.1X with SHA-256) is advertised in the RSNE.
    - PMF is required (MFPC=1 and MFPR=1).

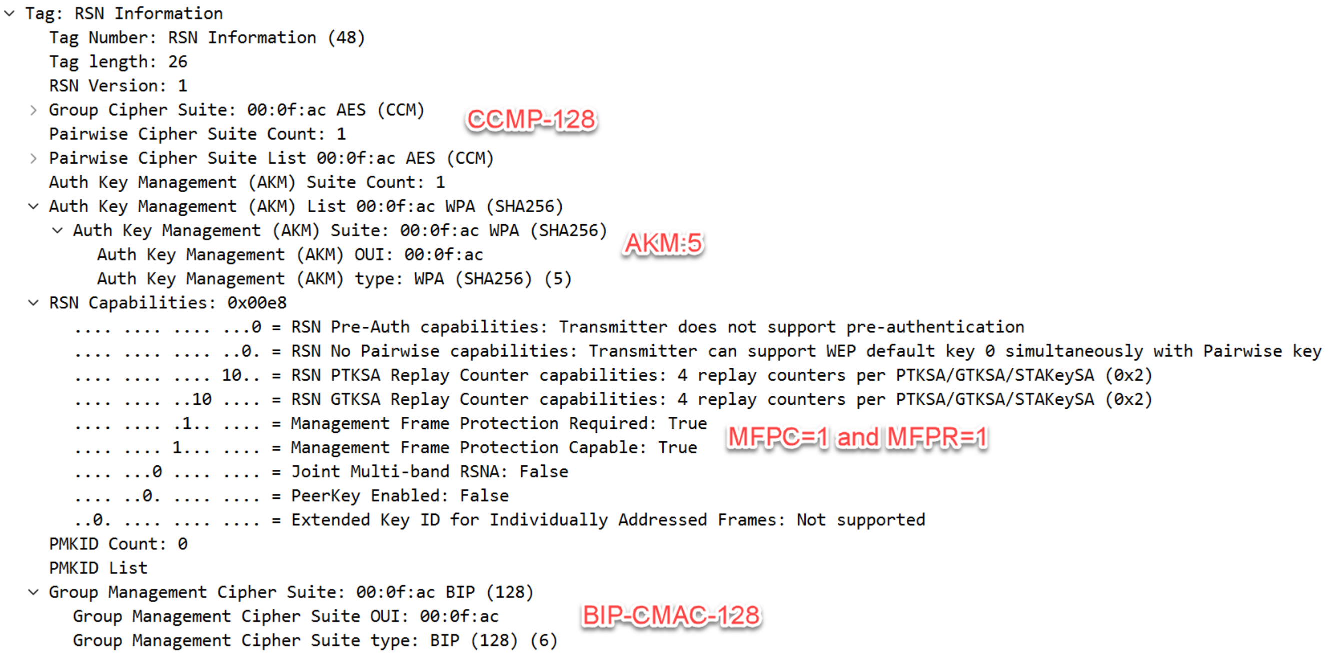


```
v Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 30
    RSN Version: 1
  > Group Cipher Suite: 00:0f:ac AES (CCM)
    Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List 00:0f:ac AES (CCM)
    Auth Key Management (AKM) Suite Count: 2
  v Auth Key Management (AKM) List 00:0f:ac WPA 00:0f:ac WPA (SHA256)
    v Auth Key Management (AKM) Suite: 00:0f:ac WPA
        Auth Key Management (AKM) OUI: 00:0f:ac
        Auth Key Management (AKM) type: WPA (1)
    v Auth Key Management (AKM) Suite: 00:0f:ac WPA (SHA256)
        Auth Key Management (AKM) OUI: 00:0f:ac
        Auth Key Management (AKM) type: WPA (SHA256) (5)
  v RSN Capabilities: 0x00a8
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... .0.. .... = Management Frame Protection Required: False
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
    PMKID Count: 0
    PMKID List
  v Group Management Cipher Suite: 00:0f:ac BIP (128)
      Group Management Cipher Suite OUI: 00:0f:ac
      Group Management Cipher Suite type: BIP (128) (6)
```

Figure 12 – WPA3-Enterprise Transition Mode (CCM 128) RSNE example

ArubaOS 8.11 and 10.5 specific behavior for WPA3-Enterprise CCM 128

- When transition mode is disabled, the behavior for WPA3-Enterprise CCM 128 is as follows:
  - 2.4 GHz and 5 GHz operation:
    - 00-0F-AC:5 (802.1X with SHA-256) is advertised in the RSNE.
    - WPA2-Enterprise only clients will not connect. Transition mode disabled forces WPA3 connections.
    - PMF is required (MFPC=1 and MFPR=1).
  - 6 GHz operation:
    - 00-0F-AC:5 (802.1X with SHA-256) is advertised in the RSNE.
    - PMF is required (MFPC=1 and MFPR=1).



```
⌄ Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 26
    RSN Version: 1
  › Group Cipher Suite: 00:0f:ac AES (CCM)
    Pairwise Cipher Suite Count: 1
  › Pairwise Cipher Suite List 00:0f:ac AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
  ⌄ Auth Key Management (AKM) List 00:0f:ac WPA (SHA256)
    ⌄ Auth Key Management (AKM) Suite: 00:0f:ac WPA (SHA256)
        Auth Key Management (AKM) OUI: 00:0f:ac
        Auth Key Management (AKM) type: WPA (SHA256) (5)
  ⌄ RSN Capabilities: 0x00e8
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... .1.. .... = Management Frame Protection Required: True
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
    PMKID Count: 0
    PMKID List
  ⌄ Group Management Cipher Suite: 00:0f:ac BIP (128)
      Group Management Cipher Suite OUI: 00:0f:ac
      Group Management Cipher Suite type: BIP (128) (6)
```

Figure 13 – WPA3-Enterprise Only (CCM 128) RSNE example

Best Practices

WPA3-Enterprise is suitable for use cases where WPA2-Enterprise was used prior because of Protected Management Frames and when AKM:5 (SHA-256) is negotiated the key length is increased. It is encouraged to disable weak EAP methods such as PEAP-MSCHAPv2, CHAPv1, PAP, etc., and consider using a stronger EAP method such as EAP-TLS.

Consider disabling transition mode to limit attack vectors. When PMF is disabled or not used by a client, attackers can spoof management frames from an AP to attack an associated client through Denial of Service (DoS) or attacker-in-the-middle techniques.

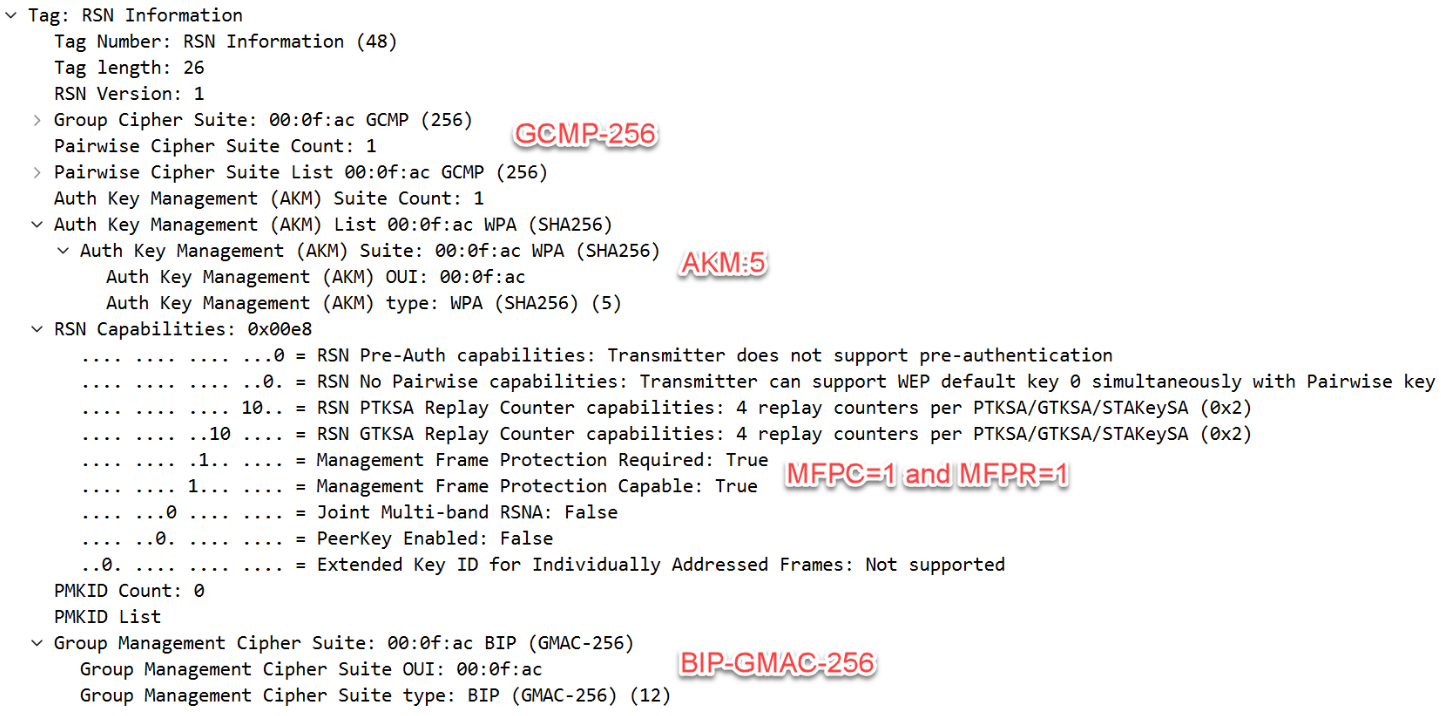
Consider deploying WPA3-Enterprise and WPA2-Enterprise on different individual VAPs.

WPA3-Enterprise 256 GCM

Introduced in ArubaOS 8.5, WPA3-Enterprise with 256 bits enables GCMP-256 cipher suites without requiring CNSA compatible EAP. This mode is also referred to as WPA3-Enterprise Non-CNSA.

The following is advertised and negotiated in beacons, probe response, and association:

- AKM suite selector as 00-0F-AC:5 (802.1X with SHA-256).
- Pairwise cipher suite selector as 00-0F-AC:9 (GCMP-256).
- Group data cipher suite selector as 00-0F-AC:9 (GCMP-256).
- Group management cipher suite selector as 00-0F-AC:12 (BIP-GMAC-256).
- Protected Management Frames are mandatory (MFPC=1 and MFPR=1).



```
⌄ Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 26
    RSN Version: 1
  › Group Cipher Suite: 00:0f:ac GCMP (256)
    Pairwise Cipher Suite Count: 1
  › Pairwise Cipher Suite List 00:0f:ac GCMP (256)
    Auth Key Management (AKM) Suite Count: 1
  ⌄ Auth Key Management (AKM) List 00:0f:ac WPA (SHA256)
    ⌄ Auth Key Management (AKM) Suite: 00:0f:ac WPA (SHA256)
        Auth Key Management (AKM) OUI: 00:0f:ac
        Auth Key Management (AKM) type: WPA (SHA256) (5)
  ⌄ RSN Capabilities: 0x00e8
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... .1.. .... = Management Frame Protection Required: True
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
    PMKID Count: 0
    PMKID List
  ⌄ Group Management Cipher Suite: 00:0f:ac BIP (GMAC-256)
      Group Management Cipher Suite OUI: 00:0f:ac
      Group Management Cipher Suite type: BIP (GMAC-256) (12)
```

Figure 14 – WPA3-Enterprise 256 GCM RSNE example

Note

As of writing, client support for GCMP-256 ciphers remains fragmented. Some new clients are starting to be produced with support for GCMP-256 and support of GCMP-256 will be a requirement for Wi-Fi 7 certified clients.

Best Practices

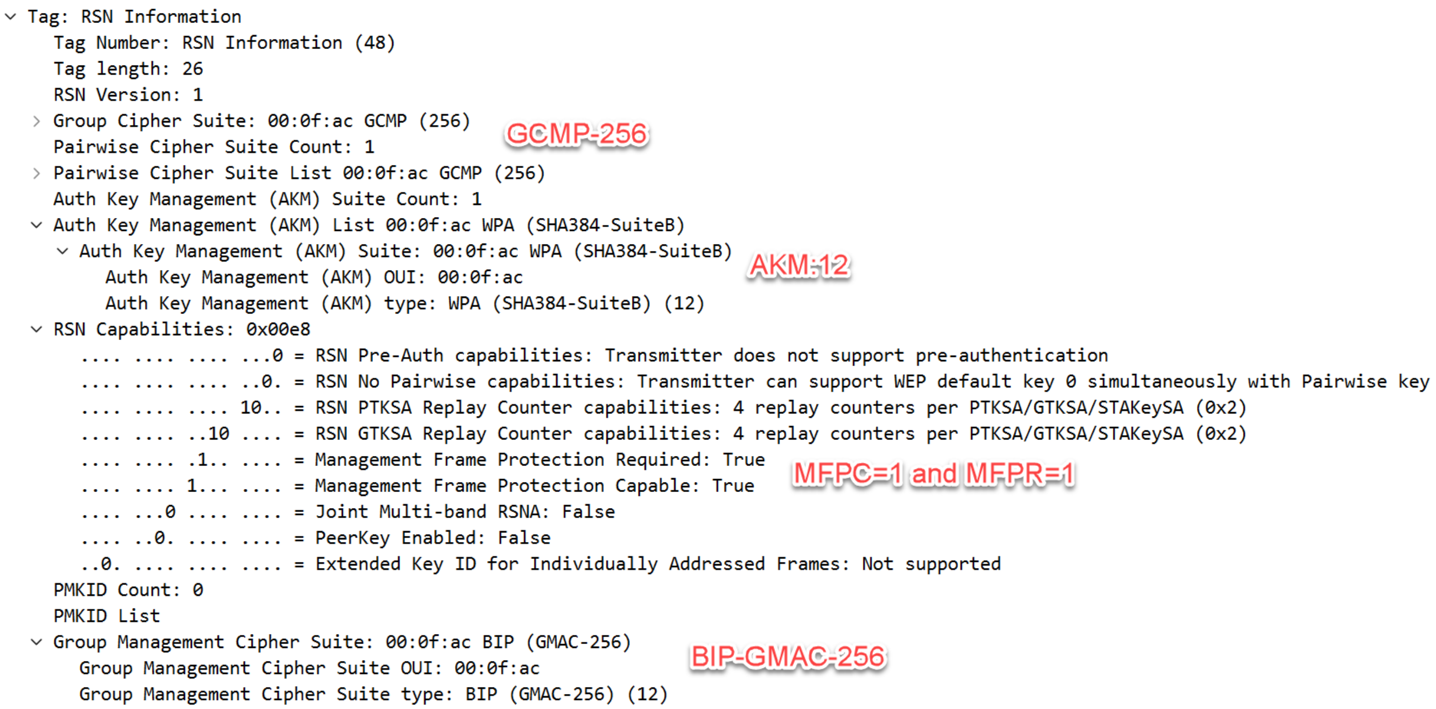
This security mode is suitable for use-cases where WPA2-Enterprise was used prior because of Protected Management Frames and stronger ciphers than CCM 128. Use this security mode if the client population is under administrative control and knowledge of support for GCMP-256 is known. Weak EAP methods such as PEAP-MSCHAPv2, CHAPv1, PAP, etc., should be disabled and client connections moved to using a stronger EAP method such as EAP-TLS. The client population must support the defined security parameters as transition mode is not allowed for WPA3-Enterprise GCM 256.

WPA3-Enterprise CNSA (192-bit)

WPA3-Enterprise CNSA (192-bit) enforces CNSA Suite security standards for enterprise Wi-Fi networks.

The following is advertised and negotiated in beacons, probe response, and association:

- AKM suite selector as 00-0F-AC:12 (802.1X with SHA-384).
- Pairwise cipher suite selector as 00-0F-AC:9 (GCMP-256).
- Group data cipher suite selector as 00-0F-AC:9 (GCMP-256).
- Group management cipher suite selector as 00-0F-AC:12 (BIP-GMAC-256).
- Protected Management Frames are mandatory (MFPC=1 and MFPR=1).



```
⌄ Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 26
    RSN Version: 1
  › Group Cipher Suite: 00:0f:ac GCMP (256)
    Pairwise Cipher Suite Count: 1
  › Pairwise Cipher Suite List 00:0f:ac GCMP (256)
    Auth Key Management (AKM) Suite Count: 1
  ⌄ Auth Key Management (AKM) List 00:0f:ac WPA (SHA384-SuiteB)
    ⌄ Auth Key Management (AKM) Suite: 00:0f:ac WPA (SHA384-SuiteB)
        Auth Key Management (AKM) OUI: 00:0f:ac
        Auth Key Management (AKM) type: WPA (SHA384-SuiteB) (12)
  ⌄ RSN Capabilities: 0x00e8
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
      .... .... .1.. .... = Management Frame Protection Required: True
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
    PMKID Count: 0
    PMKID List
  ⌄ Group Management Cipher Suite: 00:0f:ac BIP (GMAC-256)
      Group Management Cipher Suite OUI: 00:0f:ac
      Group Management Cipher Suite type: BIP (GMAC-256) (12)
```

Figure 15 – WPA3-Enterprise CNSA (192-bit) RSNE example

Other notes of importance:

- Requires a CNSA Suite compatible EAP-TLS cipher suite (RFC 6460):
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 using p384
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 using p384 and RSA > 3k bits
    - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 using RSA > 3k bits
- TLS v1.2 or later is required.
- Key length must be greater than 3000 bits.
- Certificate chain validation is mandatory.
- EAP termination is not supported. EAP termination is when EAP tunnel termination is moved upstream from the RADIUS server to the controller or AP. WPA3-Enterprise 192-bit (CNSA) expects that a RADIUS server is used, and policy is enforced by the RADIUS server. This means CNSA Suite compatible 802.1X happens between client and RADIUS server based on the authenticator indicating which AKM is negotiated between client and AP.

WPA3-Enterprise CNSA (192-bit) is supported by Aruba ClearPass (CPPM) starting in version 6.8 and supports the following RADIUS attributes from RFC 7268:

- WLAN-Reason-Code (185)
- WLAN-Pairwise-Cipher (186)
- WLAN-Group-Cipher (187)
- WLAN-AKM-Suite (188)
- WLAN-Group-Mgmt-Cipher (189)

Best Practices

This security mode is suitable for use-cases where WPA2-Enterprise was used prior because of Protected Management Frames, increased key length, stronger ciphers, and requirement of CNSA Suite compatible EAP-TLS methods. This is primarily focused on customers such as government, finance, and other industries who require a high level of security. The client population must support the defined security parameters as transition mode is not allowed for WPA3-Enterprise CNSA (192-bit).

Appendix

Decoder Ring

SECURITY MODE (`opmode`)	AKM	KEY DERIVATION HASH ALGORITHM	FT AKM	CIPHER SUITE	GROUP MANAGEMENT SUITE	PMF
WPA3 Personal (1) Transition Mode Enabled (`wpa3-sae-aes`)	2.4 / 5 GHz: AKM:2 AKM:8	2.4 / 5 GHz: SHA-1 SHA-256	2.4 / 5 GHz: AKM:4 AKM:9	CCM-128	BIP-CMAC-128	2.4 / 5 GHz: MFPC=1 MFPR=0
	6 GHz: AKM:8	6 GHz: SHA-256	6 GHz: AKM:9			6 GHz: MFPC=1 MFPR=1
WPA3 Personal (1) Transition Mode Disabled (`wpa3-sae-aes`)	2.4 / 5 / 6 GHz: AKM:8	2.4 / 5 / 6 GHz: SHA-256	2.4 / 5 / 6 GHz: AKM:9	CCM-128	BIP-CMAC-128	2.4 / 5 / 6 GHz: MFPC=1 MFPR=1
WPA2 Enterprise (2) (`wpa2-aes`)	2.4 / 5 GHz: AKM:1	2.4 / 5 GHz: SHA-1	2.4 / 5 GHz: AKM:3	CCM-128		2.4 / 5 GHz: MFPC=0 MFPR=0
WPA3 Enterprise (3) (`wpa2-aes + MFP-R`)	2.4 / 5 GHz: AKM:5	2.4 / 5 GHz: SHA-5	2.4 / 5 GHz: AKM:3	CCM-128	BIP-CMAC-128	2.4 / 5 GHz: MFPC=1 MFPR=1
WPA3 Enterprise 128 CCM Transition Mode Enabled (4) (`wpa3-aes-ccm-128`)	2.4 / 5 GHz: AKM:1 AKM:5 (5)	2.4 / 5 GHz: SHA-1 SHA-256 (5)	2.4 / 5 / 6 GHz: AKM:3	CCM-128	BIP-CMAC-128	2.4 / 5 GHz: MFPC=1 MFPR=0
	6 GHz: AKM:5	6 GHz: SHA-256				6 GHz: MFPC=1 MFPR=1
WPA3 Enterprise 128 CCM Transition Mode Disabled (4) (`wpa3-aes-ccm-128`)	2.4 / 5 / 6 GHz: AKM:5	2.4 / 5 / 6 GHz: SHA-256	2.4 / 5 / 6 GHz: AKM:3	CCM-128	BIP-CMAC-128	2.4 / 5 / 6 GHz: MFPC=1 MFPR=1
WPA3 Enterprise 256 GCM (`wpa3-aes-gcm-256`)	2.4 / 5 / 6 GHz: AKM:5	2.4 / 5 / 6 GHz: SHA-256	2.4 / 5 / 6 GHz: AKM:3	GCMP-256	BIP-GMAC-256	2.4 / 5 / 6 GHz: MFPC=1 MFPR=1
WPA3-Enterprise CNSA (192-bit) (`wpa3-cnsa`)	2.4 / 5 / 6 GHz: AKM:12	2.4 / 5 / 6 GHz: SHA-384	2.4 / 5 / 6 GHz: AKM:13	GCMP-256	BIP-GMAC-256	2.4 / 5 / 6 GHz: MFPC=1 MFPR=1

(1) wpa3-sae-aes with AKM:24 is not yet supported in ArubaOS.

(2) wpa2-aes is not typically deployed with PMF due to lack of support by WPA2 clients.

(3) wpa2-aes with PMF set to required will remove AKM:1 and add AKM:5 forcing WPA3 only.

(4) Transition mode for WPA3-Enterprise 128 CCM is supported starting in ArubaOS 8.11 and 10.5.

(5) WPA3-Enterprise 128 CCM adds transition mode and AKM:5 (802.1X with SHA-256) in the 2.4 GHz and 5 GHz bands starting in ArubaOS 8.11 and 10.5. When transition mode is disabled, AKM:1 (802.1X with SHA-1) is removed.

Useful CLI Commands

AOS 8

```
(MD) # show ap association
(MD) # show ap bss-table
(MD) # show ap essid
(MD) # show ap owe-tm-info
(MD) # show auth-tracebuf mac <client-mac>
(MD) # show dot1x supplicant-info <client-mac> <bssid>
(MD) # show dot1x supplicant-info pmkid
(MD) # show log security
(MD) # show wlan ssid-profile <profile-name>
```

AOS 10

```
(AP) # show ap association
(AP) # show ap bss-table
(AP) # show ap debug client-table
(AP) # show ap debug mgmt-frames mac <client-mac>
(AP) # show clients debug advanced
(AP) # show log security
(AP) # show network
(AP) # show network <profile-name>
```

References

- IEEE 802.11-2016
- IEEE 802.11-2020
- RFC 6460 – Suite B Profile for Transport Layer Security (TLS)
- RFC 6379 – Suite B Cryptographic Suites for IPsec
- RFC 7268 – RADIUS Attributes for IEEE 802 Networks
- RFC 8110 – Opportunistic Wireless Encryption
- WPA3 Specification version 3.0
- WPA3 Specification version 3.1