Hewlett Packard Enterprise

技术说明

HPE Aruba Networking WPA3 和 Enhanced Open 101

修订历史

文档状态：已发布

更改 请求号 （可选）	文档 版本	日期	准备 / 修改者	审核者	批准者	章节和文本修订
	1.0	10/10/2023	Josh Schmelzle			
	1.1	10/13/2023	Josh Schmelzle			参考文献 WPA3-Personal WPA3-Enterprise CCM 128
	1.2	11/13/2023	Josh Schmelzle			在8.10和10.4上使用 WPA2 -AES +MFP-R 的 WPA3 解 决方法
	1.3	11/14/2023	Josh Schmelzle			1.2 版中添加了针对 WPA3 解决方法的更新。
	1.4	11/21/2023	Josh Schmelzle			1.2 版中添加了针对 WPA3 解决方法的更新。

目录

术语

本技术说明中使用以下术语。 有关更多信息，请参考附录中提到的来源。

AKM – 认证和密钥管理

BSS – 基本服务集

CNSA – 商业国家安全算法

DH – Diffie-Hellman

Enhanced Open(增强开放)- 基于OWE的Wi-Fi联盟认证

IEEE – 电气和电子工程师学会

OWE – 机会性无线加密

MFP – 管理帧保护（见PMF）

MFPC – 管理帧保护能力

MFPR – 管理帧保护要求

PMF – 受保护的管理帧（见MFP）

PMK – 对等主密钥

RSNE – 强大的安全网络元素

SAE – 相等的同时认证

WFA – Wi-Fi联盟

Wi-Fi 6 – 基于IEEE 802.11ax (HE)

Wi-Fi 6E – Wi-Fi 6扩展到包括6 GHz频段

Wi-Fi 7 – 基于IEEE 802.11be (EHT)

WPA2 – Wi-Fi保护访问版本2

WPA3 – Wi-Fi保护访问版本3

介绍

在一个日益互联的世界中，安全可靠的Wi-Fi通信是必不可少的。 从家庭办公室到工业环境再到企业网络，Wi-Fi已成为移动连接的重要组成部分。 随着对Wi-Fi网络的依赖程度增加，保护和确保敏感数据的隐私的安全性也在增强。

增强开放和Wi-Fi保护访问版本3（WPA3）是Wi-Fi联盟（WFA）的当前Wi-Fi安全标准的进步，旨在解决其前身WPA2和开放网络的弱点。 本技术说明旨在提供关于使用ArubaOS部署的增强开放和WPA3网络的见解，探讨关键组件、实际影响和最佳实践。 我们还将讨论部署考虑因素和兼容性方面。

认证和密钥管理（AKM）

在Wi-Fi网络中使用的安全解决方案由IEEE 802.11标准和Wi-Fi联盟定义。每个安全协议都有特定的身份验证和密钥管理（AKM）套件类型（编号）。

该标准使用OUI:N的格式定义了AKM套件选择器，其中N表示套件类型。 基于标准的AKM由00-0F-AC的OUI表示。 例如，WPA3-Personal的套件选择器（`wpa3-sae-aes`）为00-0F-AC:8。 本技术说明可能将00-0F-AC:N称为AKM:N。

Wi-Fi联盟通过AKM、密码套件和受保护的管理帧（PMF）组合来定义安全认证。 以下用于指示标准中定义的不同身份验证类型及其对应的Wi-Fi联盟认证计划：

- AKM:1 = IEEE 802.1X with SHA-1
  - WPA2-Enterprise
- AKM:2 = 预共享密钥 (PSK)
  - WPA2-个人
- AKM:5 = IEEE 802.1X with SHA-256
  - WPA3-企业级
- AKM:8 = 相等的同时认证 (SAE)
  - WPA3-个人（with SHA-256)
- AKM:12 = 使用符合CNSA套件标准的密码和EAP方法的IEEE 802.1X与SHA-384
  - WPA3-企业级192位
- AKM:18 = 机会式无线加密（OWE）
  - 增强开放式
- AKM:24 = 根据Diffie-Hellman（DH）组的变量哈希算法进行的等式同时认证（SAE）
  - WPA3-个人级（使用SHA-256、SHA-384或SHA-512）

Wi-Fi联盟认证

本节详细介绍了Wi-Fi联盟安全认证计划定义的规范。 下一节将把它们映射到HPE Aruba Networking在ArubaOS中实现的安全模式。

增强开放式规范

Wi-Fi联盟增强开放式规范定义了以下内容：

- 基于RFC 8110中定义的机会式无线加密（OWE）的增强开放式（AKM:18）

WPA3 规范

Wi-Fi联盟WPA3规范定义如下：

- WPA3-Personal（AKM:8或AKM:24）
- WPA3-Personal过渡（AKM:2 + AKM:8）
- WPA3-Enterprise Only (AKM:5)
- WPA3-Enterprise过渡模式（AKM:1 + AKM:5）
- WPA3-Enterprise 192位模式（AKM:12）

对应的 Aruba 安全模式

Wi-Fi联盟认证	Aruba密钥管理	Aruba安全模式（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位	WPA3-Enterprise (CNSA)	`wpa3-cnsa`

6 GHz 运行

Wi-Fi 6E是Wi-Fi 6的'扩展'，包括6 GHz频段。 将操作扩展到6 GHz频段是一个机会，可以摆脱在2.4 GHz和5 GHz频段中存在的一些传统要求。

Wi-Fi联盟（WFA）决定要求在6 GHz频段中使用WPA3或增强开放作为最低安全模式。

以下传统安全模式在6 GHz操作中不允许使用：

- WPA2-企业版或相应的过渡模式
- WPA2-个人版或相应的过渡模式
- 开放、WPA版本1、TKIP或WEP

受保护的管理帧

IEEE 802.11w-2009修正案（现已成为IEEE 802.11-2020的一部分）引入了受保护的管理帧（PMF），用于保护强大的管理帧。 在WPA3和增强开放之前，大多数管理帧都没有加密。 由于Wi-Fi是广播介质，任何设备都可以窃听或作为合法或恶意客户端参与。 保护管理帧与保护数据帧同样重要。 没有PMF，所有管理帧都是明文发送的。 PMF保护一组强大的管理帧，并增强了已经存在的数据帧（802.11i）的隐私保护。WPA3和增强开放要求使用PMF。PMF也被称为管理帧保护（MFP）。 在讨论受保护的管理帧是可选还是必需时，将使用MFPC（可用）和MFPR（必需）这些术语。 下面讨论了它们的配置选项。 在本技术说明中，PMF和MFP这两个术语可能会互换使用。

保护管理帧有三种可能的配置：

配置	参数	支持PMF的客户端	不支持PMF的客户端
禁用	MFPC=0和MFPR=0	没有PMF的好处	没有PMF的好处
可选（可选项）	MFPC=1和MFPR=0	PMF的好处	没有PMF的好处
强制（必需）	MFPC=1和MFPR=1	PMF的好处	无法连接

PMF有助于保护强大的管理帧免受各种攻击。 关键的安全组件是防止被动窃听，防止单播和组播动作帧的伪造，允许重放检测，并防止站点冒充另一个站点。 PMF在关联后保护免受伪造的解除关联和去认证帧的攻击。

受保护的强大动作帧的示例包括：

- 信道切换通告
- QoS
- ADDBA协商
- 块ACK
- 无线电测量
- 安全关联（QA）查询
- 无线网络管理

PMF支持在RSN能力的RSNE中进行广告宣传，可以在信标、探测响应和关联响应中找到。

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

图 1 –RSN功能示例，显示MFPC=1和MFPR=1

ArubaOS具体细节：

- WPA3或Enhanced Open安全模式下，PMF不可由用户配置，MFPC（可行）和MFPR（必需）配置是自动的。

Enhanced Open

开放式Wi-Fi网络以明文传输和传递数据。 Enhanced Open提供未经身份验证的数据加密，并保护数据免受开放式Wi-Fi网络中的嗅探器的侵害。

加密由RFC 8110中定义的机会式无线加密（OWE）提供。 使用OWE，客户端和AP执行未经身份验证的Diffie-Hellman密钥交换，从而生成唯一的一对一密钥（PMK）。 生成的密钥在关联后的4路握手中用于生成流量加密密钥。

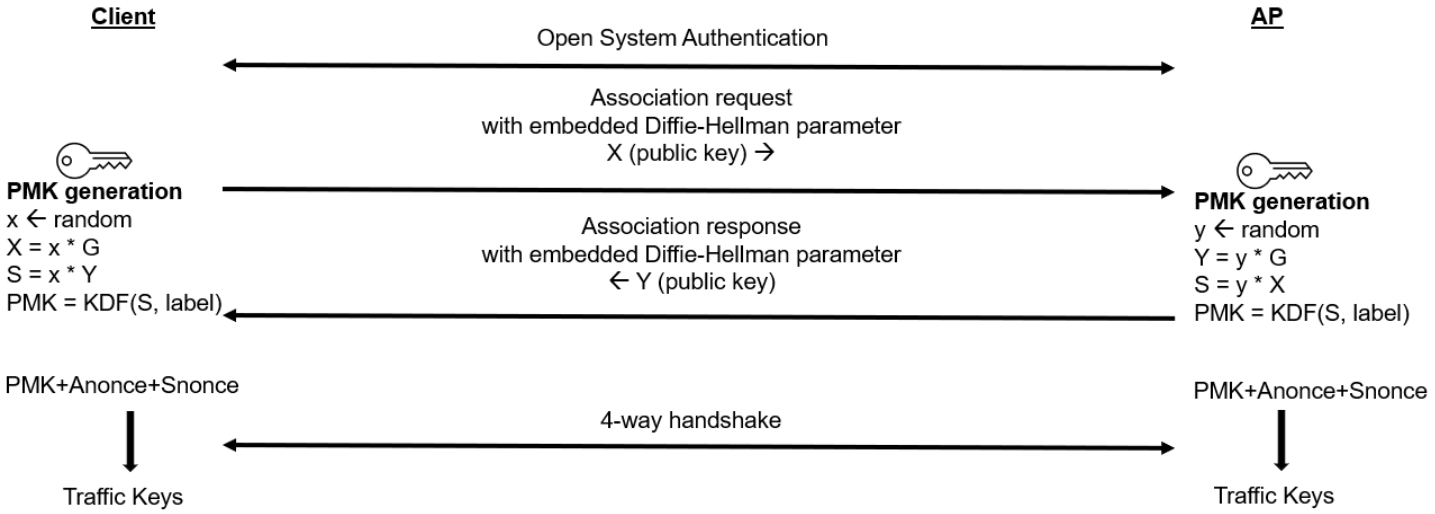

图 2 –Enhanced Open （OWE）操作示意图

由此带来的好处是，Wi-Fi网络比共享和公共PSK更安全，因为它不容易受到被动攻击，攻击者可以窃听、伪造和重放网络上的帧。 Enhanced Open的部署也更加简单，因为无需进行任何配置。没有密码。

增强开放在信标、探测响应或关联中宣传或协商以下功能（见下一页的图3）：

- AKM套件选择器为00-0F-AC:18（OWE）。
- 一对一密码套件选择器为00-0F-AC:4（CCMP-128）、00-0F-AC:8（GCMP-128）、00-0F-AC:9（GCMP-256）或00-0F-AC:10（CCMP-256）可进行协商。
- 组数据密码套件选择器为00-0F-AC:4（CCMP-128）。
- 组管理密码套件选择器为00-0F-AC:6（BIP-CMAC-128）。
- 保护管理帧是强制的（MFPC=1和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                    CCMP-128
  > Pairwise Cipher Suite List 00:0f:ac AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
  v Auth Key Management (AKM) List 00:0f:ac Opportunistic Wireless Encryption
    v Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption
          Auth Key Management (AKM) OUI: 00:0f:ac                          AKM:18
          Auth Key Management (AKM) type: Opportunistic Wireless Encryption (18)
  v 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    MFPC=1 and MFPR=1
      .... ...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          BIP-CMAC-128
      Group Management Cipher Suite type: BIP (128) (6)
```

图 3 – 增强开放（OWE）RSNE

最佳实践

增强开放适用于诸如捕获门户、咖啡店、咖啡馆、学校、企业、公共场所（如机场、体育场等）等场景，需要加密但不需要身份验证和认证。

Enhanced Open 过渡模式

增强开放过渡模式（OWETM）提供了从未加密的开放Wi-Fi网络向后兼容的过渡。 OWETM提供了非OWE客户端（开放）和支持OWE的客户端连接到同一个Wi-Fi网络的能力。

这是通过创建和广播两个基本服务集（BSS），为每个虚拟AP分别发送信标来实现的。两个BSS通过OWE过渡模式IE（图4）相互指向。

- BSS-1用于非OWE客户端的开放，IE指示BSS-2。
- BSS-2用于“隐藏”的OWE，具有零长度的SSID（隐藏），IE指示BSS-1。

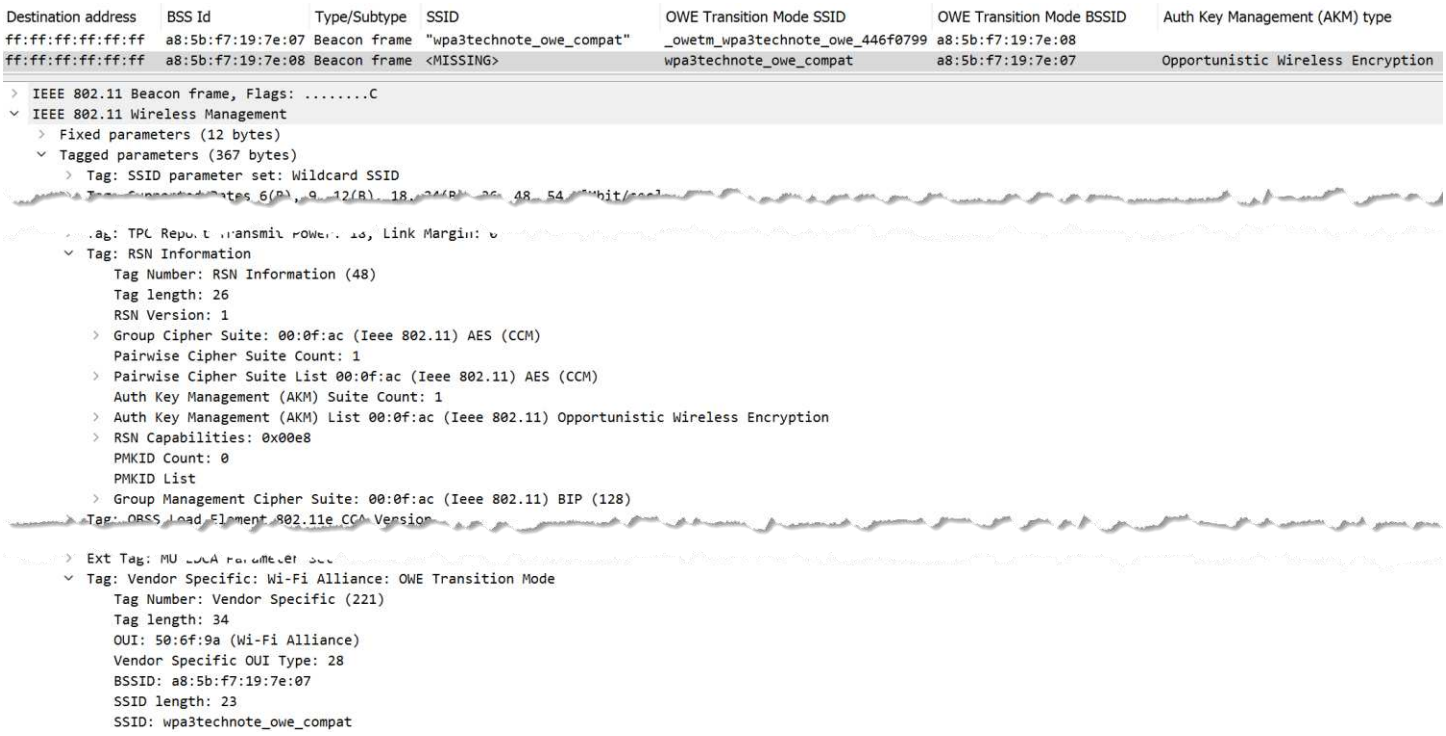

图 4 –增强开放式（OWE）过渡模式RSNE示例

开放式BSS的信标和探测响应帧包括一个OWE过渡模式IE，用于封装OWE BSS的BSSID和SSID。

- 开放式BSS和关联的客户端无法从受保护的管理帧或数据加密中受益。

OWE BSS的信标和探测响应帧包括一个OWE过渡模式IE，用于封装开放式BSS的BSSID和SSID。

- OWE BSS的信标帧将是零长度的，并包括RSNE中AKM:18的OWE身份验证和密钥管理（AKM）选择器（00-0F-AC）。
- OWE BSS需要PMF（MFPC=1和MFPR=1）。
- OWE客户端同时受益于加密和PMF。

OWE客户端通过主动或被动扫描来发现OWE AP。

注意

增强开放模式的一个缺点是每个OWE BSS都需要广告一个额外的BSS，需要进行计算。另一个缺点是未加密的开放BSS。

WPA3-Personal

针对WPA2-Personal的离线字典攻击已经广为人知超过二十年。 最初在IEEE 802.11-2016中引入用于网状安全的Simultaneous Authentication of Equals (SAE)用基于密码的身份验证方法取代了WPA2-Personal中的预共享密钥(PSK)，以抵抗字典攻击。 SAE和PSK都是基于密码的，但实现上有所不同。

某些场所提供使用共享和公共PSK的免费Wi-Fi网络。一些人错误地认为他们的Wi-Fi流量是通过PSK进行安全保护的。对于那些希望为用户提供更好数据保护的场所，SAE提供了比共享和公共PSK更安全的基于密码的选项。这是因为SAE产生的主密钥(PMK)不仅仅基于密码。 使用PSK，密码直接派生主密钥，知道密码可以解密、重放和伪造数据帧。

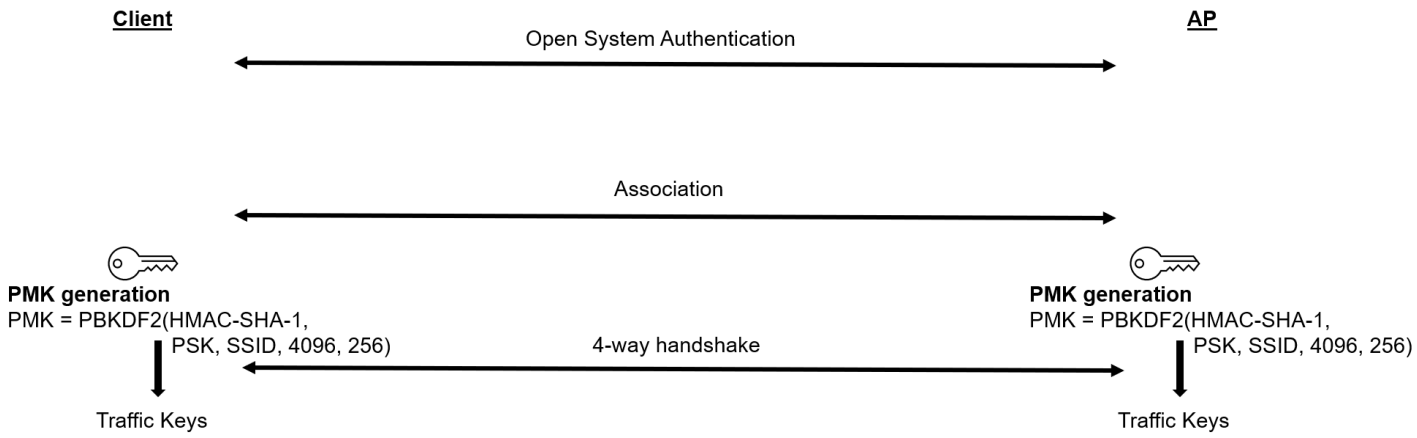

图 5 – WPA2-Personal (PSK) 操作示意图

使用SAE时，密码用于在零知识证明加密函数中派生出每个客户端的唯一对等主密钥（PMK）。 密码用于在椭圆曲线上索引一个秘密点。 曲线上的点成为密码交换中的生成器。 这意味着密码或密码派生数据永远不会通过无线传输。知道密码也无法解密SAE加密的数据帧。 解密SAE加密的数据帧需要PMK，而唯一知道PMK的方是执行SAE的客户端和AP。这意味着SAE协议对主动、被动和字典攻击具有抵抗力。

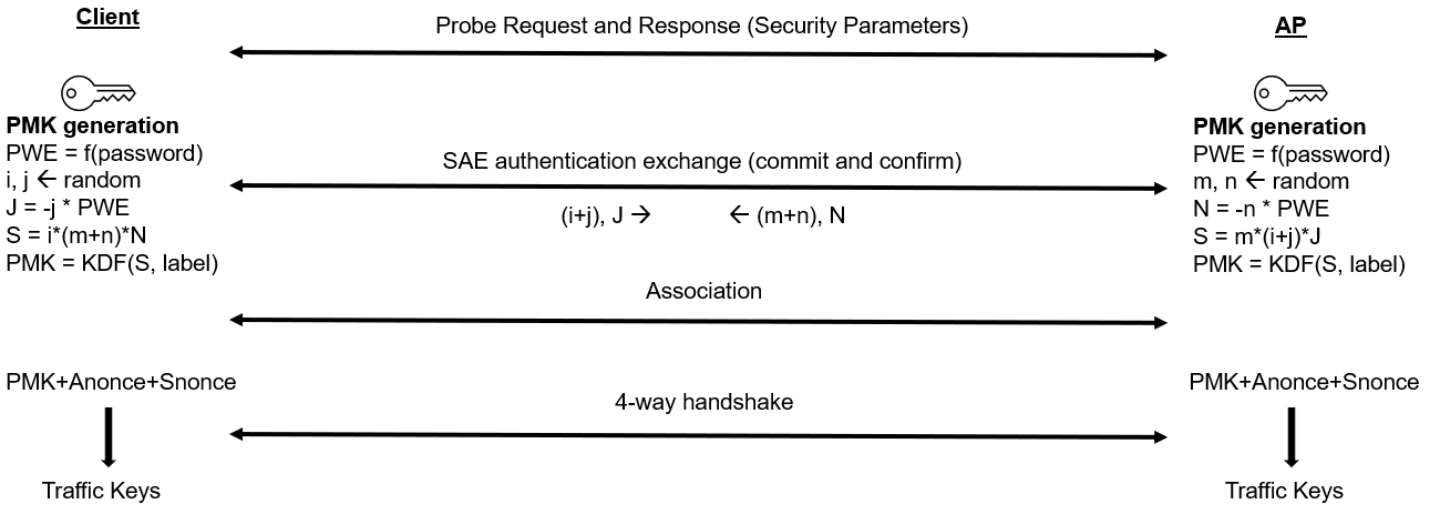

图 6 – WPA3-Personal (SAE) 操作示意图

WPA3-Personal在信标、探测响应或关联中广告或协商以下功能：

- AKM套件选择器作为AKM:8（SAE）或AKM:24（SAE）*

注意

当协商AKM:24（SAE）时，强制执行Hash-to-Element（H2E）。 使用AKM:24时，哈希算法基于与SAE一起使用的Diffie-Hellman（DH）组。例如，长度为384的素数（p384）将使用SHA-384而不是SHA-256。 Wi-Fi 7设备必须使用AKM:24进行WPA3-Personal。可以使用GCMP-256作为密码套件和BIP-GMAC-256作为组管理来进行广告宣传。

- 对等密码套件选择器为00-0F-AC:4（CCMP-128）。
- 组数据密码套件选择器为00-0F-AC:4（CCMP-128）。
- 组管理密码套件选择器为00-0F-AC:6（BIP-CMAC-128）。
- 保护管理帧是强制的（MFPC=1和MFPR=1）。

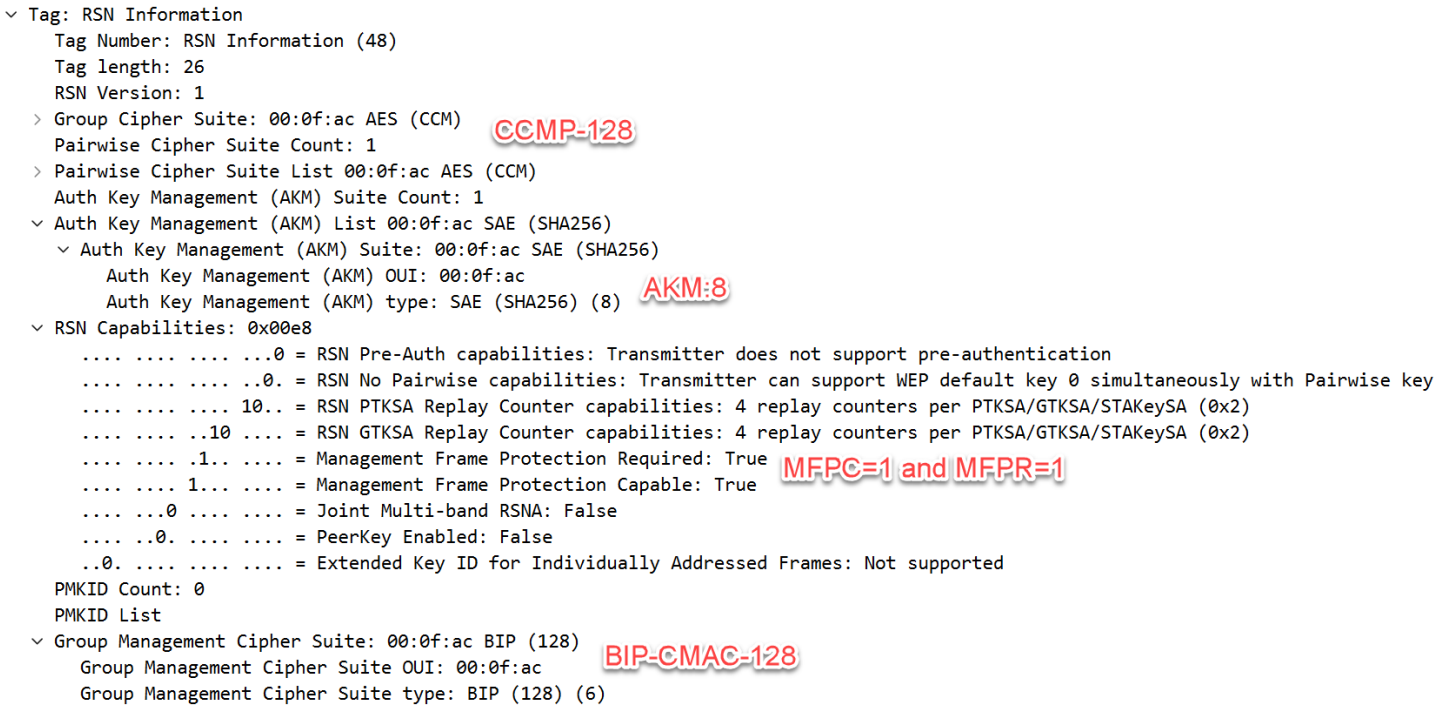

图 7 – WPA3-Personal RSNE示例

最佳实践

WPA3-Personal适用于以前使用WPA2-Personal的用例，因为它提供更好的安全性，即使使用非复杂密码。 WPA3-Personal提供加密和身份验证。

WPA3个人过渡模式

WPA3-Personal可以在过渡模式下部署，允许SAE客户端和PSK客户端连接到同一个基本服务集（BSS），这是一种混合模式的操作。 信标或探测响应在RSNE中包含一个AKM列表，其中包含PSK（AKM:2）和SAE（AKM:8）。

这意味着密码在WPA2-Personal和WPA3-Personal之间共享。WPA2-Personal网络仍然容易受到所有经典问题的攻击。 如果攻击者通过攻击WPA2-Personal获得密码，他们将可以访问网络，但无法解密WPA3-Personal会话。

由于同一个BSS为WPA2-Personal（PSK）和WPA3-Personal（SAE）客户端提供服务，对于WPA3-Personal过渡网络，保护管理帧是可选的（MFPC=1和MFPR=0）。

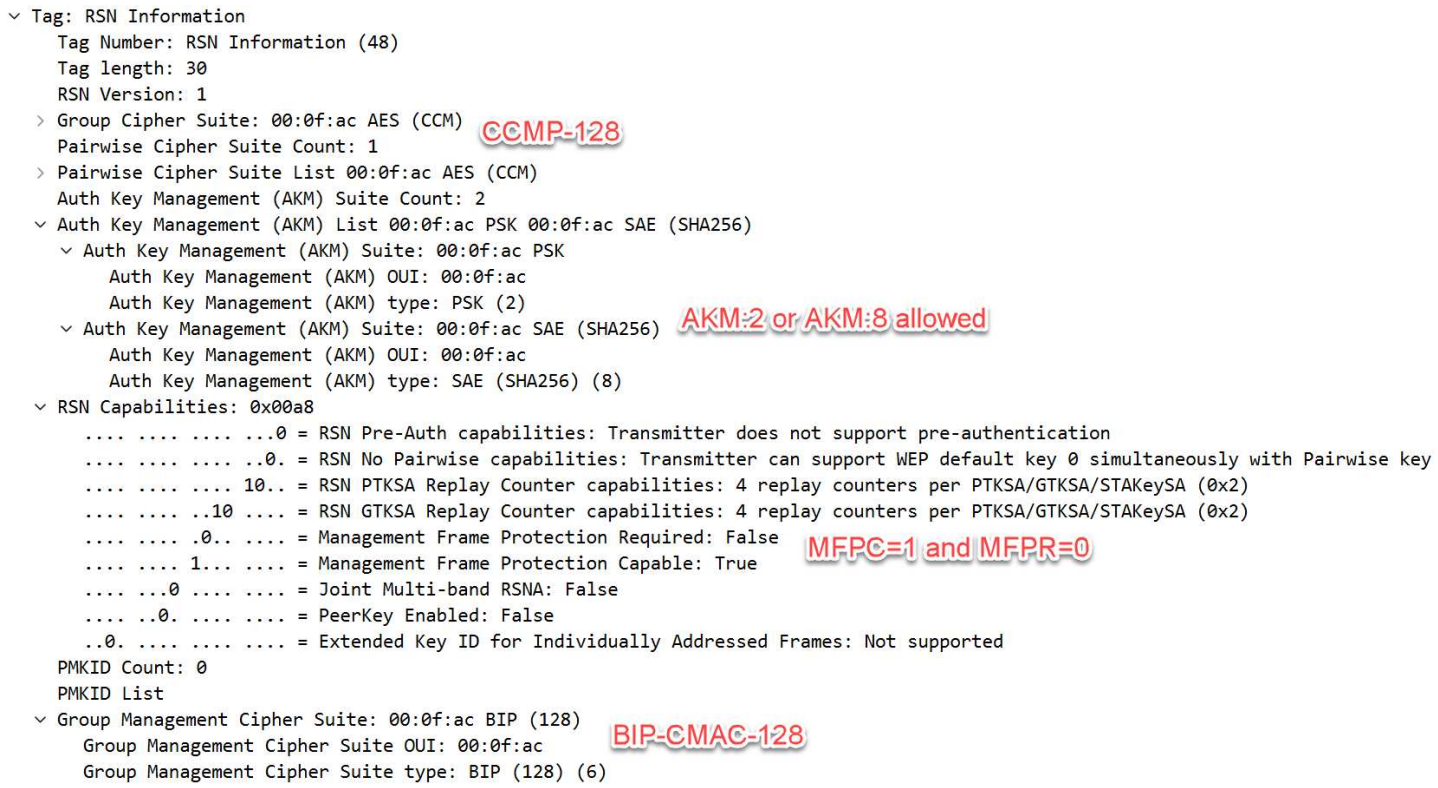

图 8 – WPA3-Personal过渡模式RSNE示例

注意

WPA3-Personal过渡模式的一个缺点是降级攻击，攻击者会针对PSK而不是SAE来获取网络访问权限，或者迫使支持SAE的客户端连接到一个恶意的PSK网络。

考虑禁用过渡模式以限制攻击向量。 考虑在不同的独立VAP和逻辑上分离和隔离的网络段上部署WPA3-Personal和WPA2-Personal，并确保在WPA3-Personal和WPA2-Personal网络上使用不同的凭据。

有关这些漏洞的更多详细信息，请参阅以Dragonblood为名发布的博客：https://blogs.arubanetworks.com/solutions/dragonblood-an-analysis-of-the-wpa3-sae-handshake。

哈希到元素（H2E）

哈希到元素（也称为哈希到曲线或直接哈希）是一种用于生成密码元素（PWE）的加密方法，取代了SAE的较弱和原始的寻找和敲击（也称为循环）方法。通过哈希到元素，SAE（WPA3-Personal）对侧信道攻击和时序攻击更具抵抗力。

SAE H2E功能可以在RSN扩展元素（RSNXE）的RSN扩展能力字段中的信标和探测响应帧中找到。

```
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
```

图 9 – RSNXE示例

从客户端的认证帧中找到的状态码126表示使用的方法。

```
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)
```

图 10 –SAE认证帧示例

ArubaOS行为从ArubaOS 8.10和10.4开始：

- 在2.4 GHz和5 GHz频段的操作：
  - 首选哈希到元素（ H2E），但如果客户端不支持 H2E，则允许逐个尝试。
- 在6 GHz频段的操作：
  - 强制使用 H2E，不允许逐个尝试。

对于WPA3认证设备，哈希到元素（H2E）的支持是强制性的。 从2021年开始，客户端开始支持H2E：

- Android 12+
- Linux wpa_supplicant v2.10+（参见 `sae_pwe`参数进行配置）
- macOS Catalina+
- Windows 10 21H2+

WPA3-Enterprise

Aruba为WPA3-Enterprise提供了三种不同的操作模式：128 CCM、256 GCM和CNSA。

- 128 CCM提供了最广泛的兼容性，包括在过渡模式下部署时支持WPA2认证的客户端。
- 256 GCM限制为支持GCMP-256密码的WPA3认证客户端。
- CNSA限制了与WPA3-Enterprise一起使用的可用选项，旨在提高攻击复杂性的门槛，使CNSA适用于最高级别的数据保护。

WPA3-企业级 128 CCM

WPA3-Enterprise 128 CCM满足Wi-Fi联盟指定的WPA3-Enterprise的两种操作模式的要求。

- “WPA3-Enterprise过渡模式”同时为WPA2-Enterprise和WPA3-Enterprise客户端提供密钥管理，并将PMF设置为可选（在2.4 GHz和5 GHz频段操作时）。
- “仅支持WPA3企业模式”仅为配置了WPA3企业模式的客户端提供密钥管理功能，并要求在所有操作频段上使用PMF。 当显式禁用过渡模式配置时，将出现此行为。

过渡模式下的WPA3企业128 CCM（默认行为）在2.4 GHz和5 GHz操作频段的信标、探测响应或关联中广告或协商以下功能：

- AKM套件选择器包括00-0F-AC:1（使用SHA-1的802.1X）和00-0F-AC:5（使用SHA-256的802.1X）。
- 受保护的管理帧是可选的（MFPC=1和MFPR=0）并且自动设置。
- 此模式支持仅支持WPA2企业模式的客户端连接到WPA2（AKM:1），以及支持WPA3企业模式的客户端连接到WPA3（AKM:5）。

WPA3-企业级128 CCM（禁用过渡模式的WPA3-企业级专用模式）在操作的2.4 GHz和5 GHz频段的信标、探针响应或关联中广告或协商以下功能：

- AKM套件选择器为00-0F-AC:5（802.1X with SHA-256）。
- 保护管理帧是必需的，并自动设置为强制性（MFPC=1和MFPR=1）。
- 此模式仅支持具备WPA3-企业级能力的客户端连接，使用WPA3（AKM:5）。

在6 GHz频段操作时，WPA3-企业级128 CCM会自动设置为“仅WPA3-企业级模式”，并在信标、探针响应或关联中广告或协商以下功能：

- AKM套件选择器为00-0F-AC:5（802.1X with SHA-256）。
- 保护管理帧是必需的，并自动设置为强制性（MFPC=1和MFPR=1）。
- 此模式仅支持具备WPA3-企业级能力的客户端连接，使用WPA3（AKM:5）。

WPA3-企业级128 CCM在所有操作模式中的信标、探针响应或关联中广告或协商以下密码：

- 对等密码套件选择器为00-0F-AC:4（CCMP-128）。
- 组数据密码套件选择器为00-0F-AC:4（CCMP-128）。
- 组管理密码套件选择器为00-0F-AC:6（BIP-CMAC-128）。

注意

WPA3-Enterprise 128 CCM的密钥管理和受保护的管理帧配置取决于操作频段和部署的ArubaOS版本。 过渡模式支持从ArubaOS 8.11和10.5开始。ArubaOS 8.10和10.4的行为不同，WPA3-Enterprise客户端将使用2.4GHz和5GHz操作中的WPA2进行连接协商。 请查看以下页面以了解具体信息。

WPA3 Enterprise CCM 128的ArubaOS 8.10和10.4特定行为

- 过渡模式配置对操作没有影响。
- **2.4GHz和5GHz操作：**
    - 00-0F-AC:1（802.1X with SHA-1）在RSNE中进行广告宣传。

注意

00-0F-AC:5（802.1X with SHA-256）在ArubaOS 8.10或10.4中不使用CCM 128进行广告宣传。这意味着只有AP广告了AKM:1，因此支持WPA3的客户端将以WPA2进行连接协商。

    - PMF是可选的（ MFPC=1和 MFPR=0）.
- 6 GHz操作:
    - 00-0F-AC:5（802.1X with SHA-256）在RSNE中广告。
    - PMF是必需的（MFPC=1和MFPR=1）。

WPA3只有CCM 128的解决方法

如果有限制连接性的要求到“仅限WPA3企业模式”在8.10或10.4部署中使用CCMP-128密码时，请考虑以下解决方法和注意事项:

- WPA2-企业安全模式（`wpa2-aes`）与 PMF配置为强制（ MFPC=1和 MFPR=1）
  实际上使用WPA3-企业（AKM:5）进行密钥管理，而不是WPA2-企业（AKM:1）.
- 此解决方法的使用情况:
    - “WPA3-仅限企业模式”不支持传统的WPA2-企业客户端.
    - ArubaOS 8.10或10.4部署。
- 为了部署这个解决方法，需要两个配置。
    - 1) 安全模式设置为WPA2-Enterprise (`wpa2-aes`)
    - 2) PMF设置为强制性 (MFPC=1和MFPR=1)
        - 通过CLI (`mfp-capable`和 `mfp-required`参数)、Central template group或Central REST API，对MFP进行即时8配置。
        - 通过WebUI、CLI或本地REST API对AOS 8进行MFP配置。
        - 通过Central REST API对AOS 10进行MFP配置。
- 注意事项:
    - 此解决方法不支持6 GHz操作。
    - AOS 8转发模式注意事项:
        - Wi-Fi 5 AP的PMF操作需要使用解密隧道模式。
        - 从Wi-Fi 6 AP开始支持隧道模式的PMF操作。
    - 当部署此解决方法并将可行部署升级到8.11版本时，由于早期8.11版本中存在多播加密不匹配的错误，请至少升级到8.11.2.1或更高版本。

WPA3仅CCM 128解决方案（续）

示例ArubaOS 8.10配置：

```
# 2.4 GHz和5 GHz的WPA3仅密钥管理，使用wpa2-aes + mfp-capable + mfp-required配置
wlan ssid-profile "ACME_1X_WPA3"
    essid "ACME_1X_WPA3"
    opmode wpa2-aes
    mfp-capable
    mfp-required
!
```

示例ArubaOS 8.10验证：

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


SSID配置文件"ACME_1X_WPA3"
-----------------------------------
参数                                        值
---------                                   -----
启用SSID                                    已启用
ESSID                                       ACME_1X_WPA3
加密                                        wpa2-aes
启用管理帧保护（适用于WPA2操作模式）          已启用
要求启用管理帧保护（适用于WPA2操作模式）
```

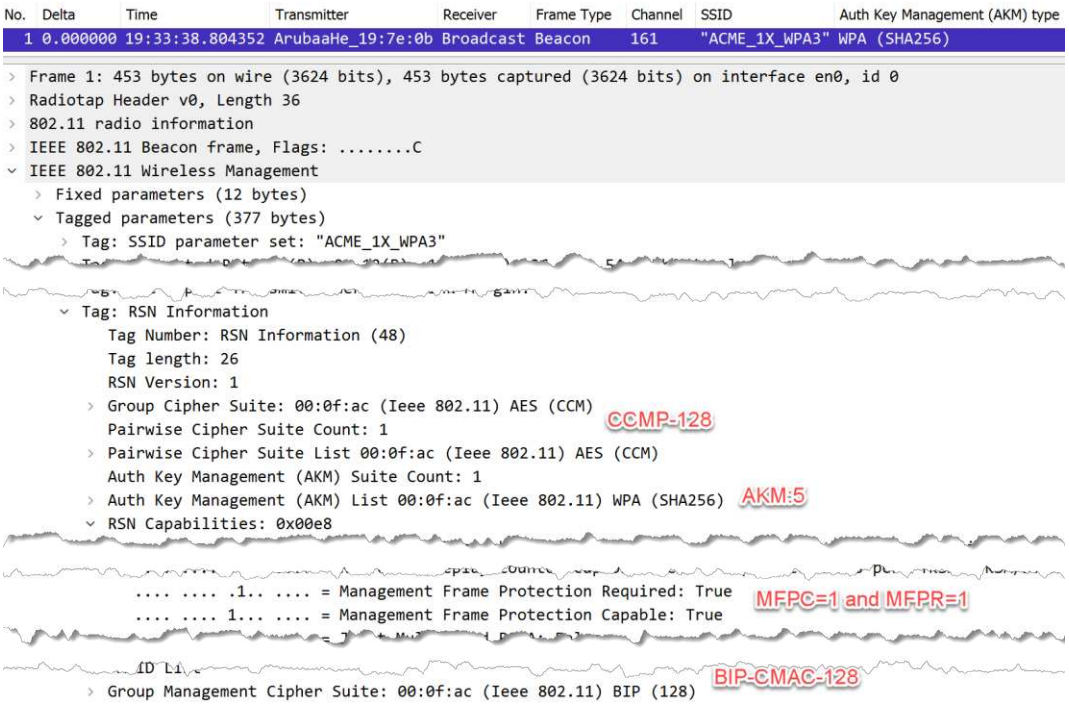

图 11 –WPA3仅CCM 128解决方案示例信标帧。

WPA3仅CCM 128解决方法（续）

- 当配置和支持时，在2.4 GHz或5 GHz频段的信标、探针响应或关联中广告或协商以下功能：○ AKM套件选择器为00-0F-AC:5（802.1X with SHA-256）。○ 对等密码套件选择器为00-0F-AC:4（CCMP-128）。

  ○ 组数据密码套件选择器为00-0F-AC:4（CCMP-128）。

  ○ 组管理密码套件选择器为00-0F-AC:6（BIP-CMAC-128）。

  ○ 保护管理帧是强制的（MFPC=1和MFPR=1）。

- 当配置但不支持时，例如在AOS 8上的Wi-Fi 5 APs的隧道模式中，在2.4 GHz或5 GHz频段的信标、探针响应或关联中广告或协商以下功能：○ AKM套件选择器为00-0F-AC:1（802.1X with SHA-1）。○ 对等密码套件选择器为

  00-0F-AC:4（CCMP-128）。

  ○ 组数据密码套件选择器为00-0F-AC:4（CCMP-128）。

  ○ 保护管理帧被禁用（MFPC=0和MFPR=0）。

- 在一段时间的实施后，如果出现了对 6 GHz操作的新部署要求，例如当添加了6 GHz兼容硬件时，请考虑以下升级和配置迁移以保持广告密钥管理的一致性：

  ○ 1)

  - AOS 8：升级到8.11.2.1或更高版本。
  - AOS 10：升级到10.5或更高版本。

  ○ 2)

  - 将安全模式从 WPA2-Enterprise（`wpa2-aes`）更改为WPA3-Enterprise CCM 128（`wpa3-aes-ccm-128`）。
  - 禁用过渡模式以禁用对使用AKM:1的WPA2客户端的支持。

  - 从8.11和10.5开始支持WPA3-Enterprise CCM 128的过渡模式配置，默认情况下广告了AKM:1和AKM:5。○ 3)

  - AOS 8：在相应的VAP上配置“允许6GHz频段”。
  - AOS 10：在相应的WLAN配置中启用6 GHz频段。

ArubaOS 8.11和10.5针对WPA3-Enterprise CCM 128的特定行为

- 支持 WPA3-Enterprise CCM 128的过渡模式。
- 启用过渡模式（默认情况下），行为如下：
    - 2.4 GHz和5 GHz操作：
        - RSNE中广告了00-0F-AC:1（802.1X with SHA-1）和00-0F-AC:5（802.1X with SHA-256）。
        - 兼容的客户端可以使用WPA2或WPA3进行协商。
        - PMF是可选的（MFPC=1和MFPR=0）。
    - 6 GHz操作：
        - RSNE中广告了00-0F-AC:5（802.1X with SHA-256）。
        - 需要PMF（MFPC=1和MFPR=1）。

```
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)        CCMP-128
    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)   AKM:1 or AKM:5 allowed
        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   MFPC=1 and MFPR=0
      .... .... 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        BIP-CMAC-128
      Group Management Cipher Suite type: BIP (128) (6)
```

图 12 – WPA3-企业过渡模式（CCM 128） RSNE示例

ArubaOS 8.11和10.5针对WPA3-Enterprise CCM 128的特定行为

- 当禁用过渡模式时，WPA3-企业CCM 128的行为如下：
  - 2.4 GHz和5 GHz操作：
    - RSNE中广告了00-0F-AC:5（802.1X with SHA-256）。
    - 仅支持WPA2-企业客户端将无法连接。 禁用过渡模式会强制WPA3连接。
    - 需要PMF（MFPC=1和MFPR=1）。
  - 6 GHz操作：
    - RSNE中广告了00-0F-AC:5（802.1X with SHA-256）。
    - 需要PMF（MFPC=1和MFPR=1）。

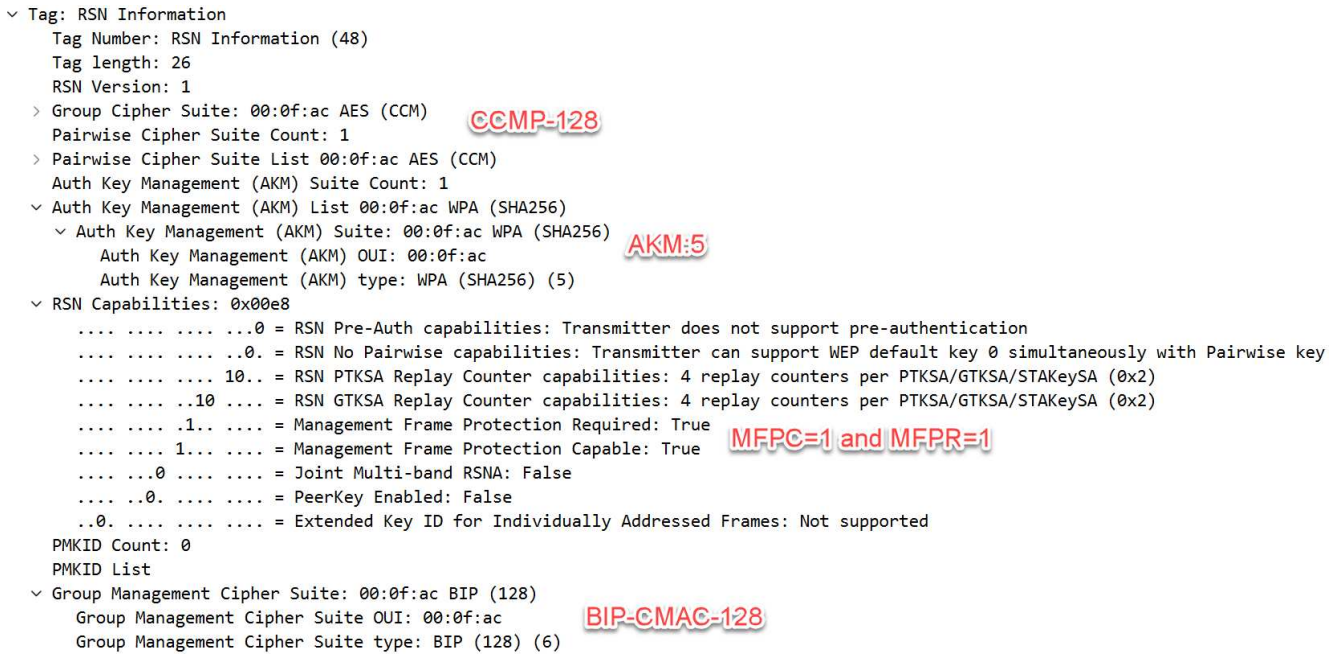

图 13 – WPA3-企业仅限（CCM 128）RSNE示例

最佳实践

WPA3-企业适用于之前使用WPA2-企业的用例，因为受保护的管理帧以及当协商AKM:5（SHA-256）时，密钥长度增加。 鼓励禁用弱EAP方法，如PEAP-MSCHAPv2，CHAPv1，PAP等，并考虑使用更强大的EAP方法，如EAP-TLS。考虑禁用过渡模式以限制攻击向量。 当禁用PMF或客户端不使用PMF时，攻击者可以通过拒绝服务（DoS）或中间人技术，伪造来自AP的管理帧来攻击关联的客户端。

考虑在不同的个别VAP上部署WPA3-Enterprise和WPA2-Enterprise。

WPA3-企业级 256 GCM

在ArubaOS 8.5中引入的WPA3-Enterprise具有256位，可以在不需要CNSA兼容EAP的情况下使用GCMP-256密码套件。这种模式也被称为WPA3-Enterprise Non-CNSA。以下内容在信标、探测响应和关联中进行广告和协商：

- AKM套件选择器为00-0F-AC:5（802.1X with SHA-256）。
- 一对一密码套件选择器为00-0F-AC:9（GCMP-256）。
- 组数据密码套件选择器为00-0F-AC:9（GCMP-256）。
- 组管理密码套件选择器为00-0F-AC:12（BIP-GMAC-256）。
- 保护管理帧是强制的（MFPC=1和MFPR=1）。

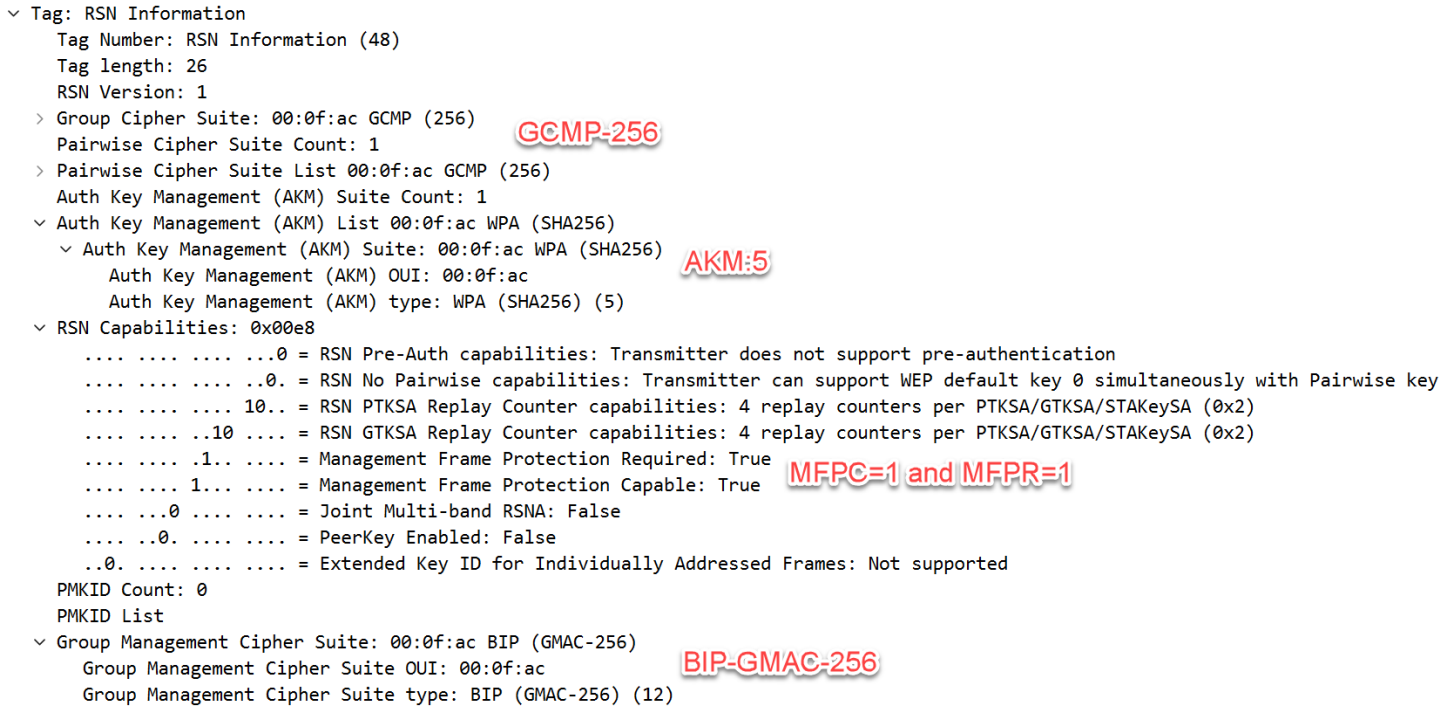

图 14 – WPA3-Enterprise 256 GCM RSNE示例

注意

截至目前，对GCMP-256密码的客户端支持仍然不完整。 一些新的客户端开始生产，支持GCMP-256并且支持GCMP-256将成为Wi-Fi 7认证客户端的要求。

最佳实践

此安全模式适用于之前使用WPA2-Enterprise的用例，因为它具有受保护的管理帧和比CCM 128更强的密码。 如果客户端数量在管理控制下，并且已知支持GCMP-256，则使用此安全模式。 应禁用弱EAP方法，如PEAP-MSCHAPv2、CHAPv1、PAP等，并将客户端连接转移到使用更强的EAP方法，如EAP-TLS。客户端群体必须支持定义的安全参数，因为不允许过渡模式用于WPA3-Enterprise GCM 256。

WPA3-企业级 CNSA (192位)

WPA3-Enterprise CNSA（192位）强制执行企业Wi-Fi网络的CNSA Suite安全标准。

以下内容在信标、探测响应和关联中进行广告和协商：

- AKM套件选择器为00-0F-AC:12（802.1X with SHA-384）。
- 一对一密码套件选择器为00-0F-AC:9（GCMP-256）。
- 组数据密码套件选择器为00-0F-AC:9（GCMP-256）。
- 组管理密码套件选择器为00-0F-AC:12（BIP-GMAC-256）。
- 保护管理帧是强制的（MFPC=1和MFPR=1）。

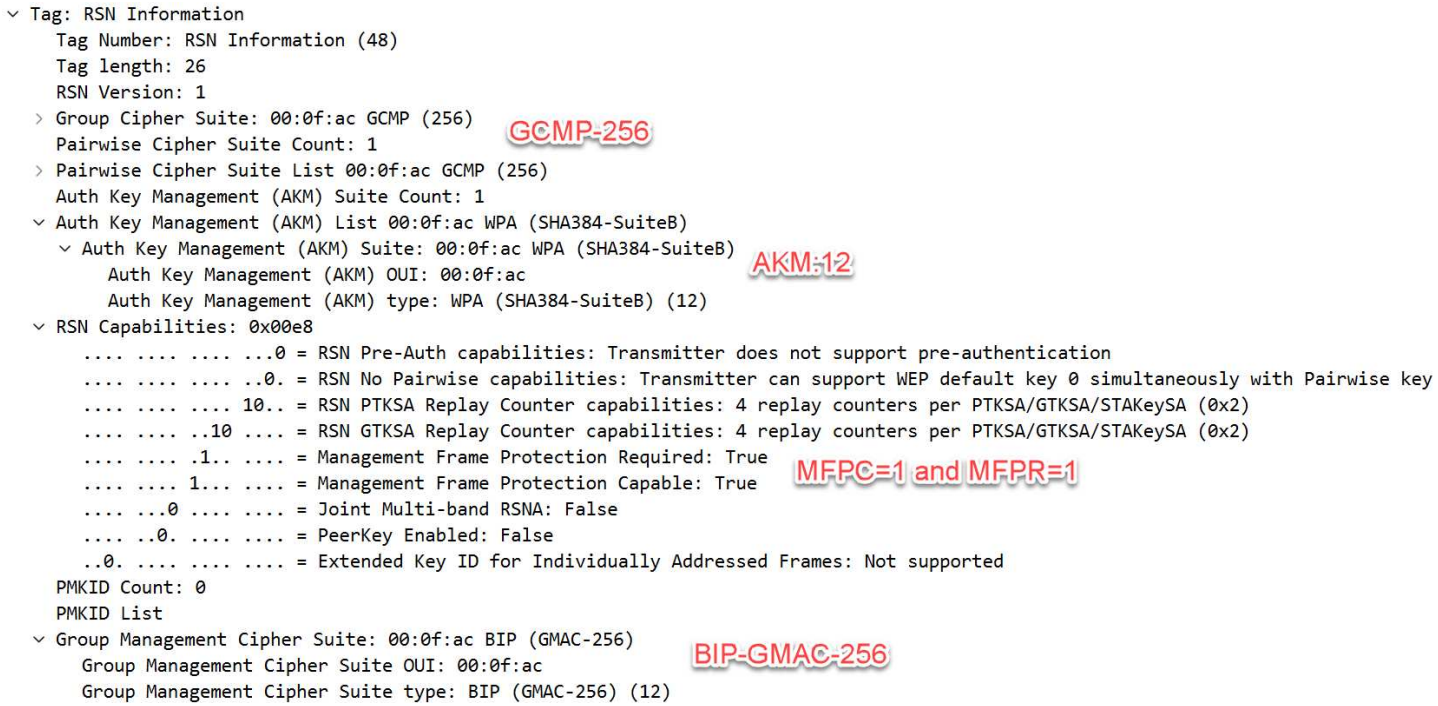

图 15 – WPA3-Enterprise CNSA（192位） RSNE示例

其他重要说明:

- 需要CNSA套件兼容的EAP-TLS密码套件（RFC 6460）：
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384使用p384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384使用p384和RSA > 3k位
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384使用RSA > 3k位
- 需要TLS v1.2或更高版本。
- 密钥长度必须大于3000位。
- 证书链验证是强制性的。
- 不支持EAP终止。 EAP终止是指将EAP隧道终止点从RADIUS服务器移至控制器或AP。WPA3-Enterprise 192位（CNSA）期望使用RADIUS服务器，并且策略由RADIUS服务器强制执行。 这意味着基于认证器指示客户端和AP之间发生的CNSA套件兼容的802.1X是在客户端和RADIUS服务器之间进行的，指示了客户端和AP之间协商的AKM。

WPA3-企业CNSA（192位）由Aruba ClearPass（CPPM）从版本6.8开始支持，并支持RFC 7268中的以下RADIUS属性：

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

最佳实践

此安全模式适用于以前使用WPA2-企业的用例，因为它具有受保护的管理帧、增加的密钥长度、更强的密码和对CNSA套件兼容的EAP-TLS方法的要求。 这主要针对需要高级安全性的政府、金融和其他行业的客户。

客户端群体必须支持定义的安全参数，因为WPA3-企业CNSA（192位）不允许过渡模式。

附录

解码器环

安全模式 (op模式)	AKM	密钥派生 哈希 算法	FT AKM	密码 套件	组 管理 套件	PMF
WPA3个人 (1) 过渡模式已启用 (wpa3-sae-aes)	2.4 / 5 GHz: AKM:2 AKM:8 6 GHz: AKM:8	2.4 / 5 GHz: SHA-1 SHA-256 6 GHz: SHA-256	2.4 / 5 GHz: AKM:4 AKM:9 6 GHz: AKM:9	CCM-128	BIP-CMAC-128	2.4 / 5 GHz: MFPC=1 MFPR=0 6 GHz: MFPC=1 MFPR=1
WPA3个人 (1) 过渡模式已禁用 (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企业级 (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企业级 (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企业级 128 CCM 过渡模式启用 (4) (wpa3-aes-ccm-128)	2.4 / 5 GHz: AKM:1 AKM:5 (5) 6 GHz: AKM:5	2.4 / 5 GHz: SHA-1 SHA-256 (5) 6 GHz: SHA-256	2.4 / 5 / 6 GHz: AKM:3	CCM-128	BIP-CMAC-128	2.4 / 5 GHz: MFPC=1 MFPR=0 6 GHz: MFPC=1 MFPR=1
WPA3企业级 128 CCM 过渡模式已禁用 (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企业级 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企业级 CNSA (192位) (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与AKM:24的组合在ArubaOS中尚不支持。

(2) 由于WPA2客户端的支持不足，通常不会使用wpa2-aes与PMF一起部署。

(3) 将PMF设置为必需的wpa2-aes将删除AKM:1并添加AKM:5，强制使用WPA3。

(4) 从ArubaOS 8.11和10.5开始支持WPA3-Enterprise 128 CCM的过渡模式。

(5) 在ArubaOS 8.11和10.5中，WPA3-Enterprise 128 CCM在2.4 GHz和5 GHz频段中添加了过渡模式和AKM:5 (802.1X with SHA-256)。当禁用过渡模式时，将删除AKM:1 (802.1X with SHA-1)。

有用的CLI命令

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>
```

参考资料

- 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 –IEEE 802网络的RADIUS属性
- RFC 8110 –机会式无线加密
- WPA3规范版本3.0
- WPA3规范版本3.1