# WPA3 技术白皮书

# 目 录

# 1 概述

WPA3（Wi-Fi Protected Access 3，Wi-Fi 受保护访问 3）是 Wi-Fi 联盟发布的下一代无线网络安全性方案，在已有的 WPA2 基础上进行了进一步的更新和规范，对无线网络的安全性提供了更强的保护。WPA3 主要分为 WPA3-Personal 和 WPA3-Enterprise 两部分，WPA3-Personal 一般适用于个人、家庭等小型网络，WPA3-Enterprise 则可用于对网络管理、接入控制和安全性等有更高需求的政府、企业等大中型组织。

## 1.1 产生背景

Wi-Fi 联盟于 2003 年推出了 WPA 来取代有致命缺陷的 WEP（Wired Equivalent Privacy，有线等效隐私），在 WPA 中引入了 TKIP（Temporal Key Integrity Protocol，临时密钥完整性协议）作为加密套件来保护无线流量。在随后的 2006 年，Wi-Fi 联盟推出了 WPA2，WPA2 引入了基于 AES（Advanced Encryption Standard，高级加密标准）的 CCMP（Counter mode with CBC-MAC Protocol，[计数器模式]搭配[区块密码锁链一信息真实性检查码]协议）作为加密套件，CCMP 的安全性比 TKIP 有较大的提升。近年来，由于 WPA2 不断暴露出新的安全漏洞，Wi-Fi 联盟于 2018 年发布了最新的 WPA3。与 WPA2 相比，WPA3 有以下优点：

- 禁止使用过时的加密套件 TKIP，必须使用基于 AES 的认证加密算法
- 必须使用管理帧保护

为了在 WPA3 的推广应用时期兼容较老的无线设备，Wi-Fi 联盟针对 WPA3-Personal 制定了 WPA3 的过渡模式，在过渡模式中，不支持 WPA3 的无线客户端可以以 WPA2-Personal 的方式接入。

## 1.2 技术优点

在 WPA3-Personal 中，使用 SAE（Simultaneous Authentication of Equals，对等实体同时认证）取代了单纯基于 PSK（Pre-Shared Key，预共享密钥）保护无线流量的方式。无线客户端必须通过在 Authentication 阶段与 AP 之间的 4 次 SAE 报文交互，才可以与 AP 关联。SAE 具有抵抗离线字典攻击的特性，攻击者无法通过嗅探无线报文并结合常用的密码组合推测出无线网络的密钥，因此，网络管理者可以为个人网络配置更简单易记的密码。即使攻击者已获取到无线网络的密钥，由于每个无线客户端通过 SAE 交互和后续 4 次握手过程得到的会话密钥均不同，也无法破解无线流量的内容。

在 WPA3-Enterprise 中，提供了可选的 192-bit 强度模式。在企业级的无线网络中，除了 AC 和 AP 之外，一般还需要额外部署 AAA（Authentication、Authorization、Accounting，认证、授权、计费）服务器用于处理无线客户端的各类接入控制需求，WPA3-Enterprise 192-bit 模式对整个网络中使用的密码学算法做了强制规定，所使用的各种算法符合 CNSA（Commercial National Security Algorithms，商业国家安全算法）Suite 中的要求，在终端的上线过程中的各个阶段及上线后的无线流量提供最低 192-bit 强度的安全性。

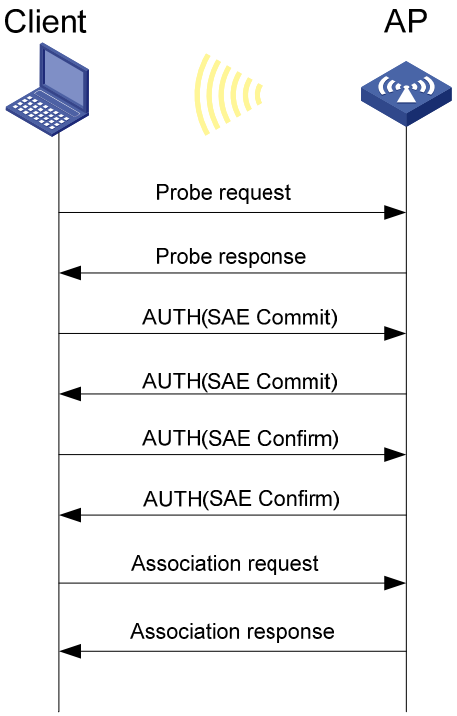
# 2 技术实现

## 2.1 WPA3-Personal

WPA3-Personal 中，在无线客户端上线完成主动扫描/被动扫描阶段的交互后，在链路层认证过程中，使用 SAE 交互。SAE 不区分“发起者”与“认证者”，通信双方均可首先发起认证。

SAE 协议分为“Commit”和“Confirm”两个阶段，在 Commit 阶段，通信双方发出 Commit 帧来推测 PSK，在 Confirm 阶段，通信双方发出 Confirm 帧确认推测的结果。通信双方的 Confirm 帧校验成功后，进行后续的关联过程。SAE 最主要的作用是产生 PMK（Pairwise Master Key，成对主密钥），PMK 用于后续的 4 次握手协商会话使用的临时密钥。Commit 帧与 Confirm 帧使用 Authentication 封装。

图1 SAE 认证过程




### 2.1.1 Commit交互

SAE 使用基于离散对数算法的密码学进行密钥的协商，使用 FFC（Finite Field Cryptography，有限域密码）或 ECC（Elliptic Curve Cryptography，椭圆曲线密码）上的运算完成相关参数的计算。目前 Wi-Fi 联盟要求 SAE 中的椭圆曲线密码学计算在由 IANA（Internet Assigned Numbers Authority，互联网编号分配机构）编号的第 19 号 ECC Group 上完成。

说明

本文档中如无特殊说明，均以在 ECC Group 19 上的运算为例介绍 SAE 工作机制。

在发送 Commit 帧前，发送方根据 PSK、收发双方的 MAC 地址，通过“Hunting and Pecking”算法计算出 PWE（Password Element，密码元素），PWE 为椭圆曲线上一点。

Commit帧的格式如 表 1 所示，前 3 个字段为Authentication帧中的固定内容。Group ID字段表示使用的Group编号，一般为 19；当使用Group 19 时，Scalar为一个大整数，Element为计算出的椭圆曲线上一点的坐标。

表1 Commit 帧的格式

| Authentication Algorithm(2 bytes) |
| --- |
| Squence Number(2 bytes) |
| Status Code(2 bytes) |
| Group ID(2 bytes) |
| Scalar(variable) |
| Element(variable) |

发送方根据内部生成的随机数、PWE，通过椭圆曲线运算，计算出 Scalar 和 Element。

接收方对收到的 Commit 帧进行校验，当校验通过后，使用本端和对端的 Scalar 等内容，通过密钥衍生算法计算出 KCK（Key Confirmation Key，密钥确认密钥）和 PMK，其中的 KCK 用于在 Confirm 阶段生成并校验帧中的内容。

### 2.1.2 Confirm交互

Confirm帧的格式如 表 2 所示。前 3 个字段为Authentication帧中的固定内容，Send-Confirm为发送Confirm帧的计数器，Confirm字段为使用KCK、Send-Confirm、本端和对端的Scalar、本端和对端的Elemen通过基于哈希的消息认证码算法计算得到。

接收方收到 Confirm 帧后，使用在 Commit 阶段产生的 KCK 和同样的参数及算法，计算一个校验码，当校验码与收到帧中的 Confirm 字段一致时，验证通过，继续进行后续的关联及 4 次握手协商临时会话密钥过程。

表2 Confirm 帧的格式

| Authentication Algorithm(2 bytes) |
| --- |
| Squence Number(2 bytes) |
| Status Code(2 bytes) |
| Send-Confirm(2 bytes) |
| Confirm(32 bytes) |

## 2.2 WPA3-Enterprise

WPA3-Enterprise 192-bit 模式与 WPA2-Enterprise 相比，主要改进在于增加了密钥的长度、使用了新的加密套件和对网络的各个组件的安全性提出了一致性的要求。此模式只能用在 802.1X 认证场景下，在 802.1X 认证阶段，使用基于 384-bit 的椭圆曲线算法或者模数大于 3072-bit 的 RSA 算法，TLS（Transport Layer Security，传输层安全）加密套件需使用 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384、TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 或 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384；在 4 次握手阶段使用 HMAC-SHA-384 导出密钥；在终端上线后，使用 GCMP-256（Galois Counter Mode Protocol，伽罗瓦计数器模式协议）来保护用户的无线流量，使用 GMAC-256 保护组播管理帧。尽管 GCMP-192 已可以满足 192-bit 强度的需求，由于 GCMP-256 使用更为广泛，因此选择了 GCMP-256。

说明

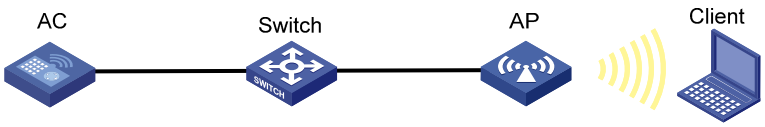
WPA3-Enterprise 192-bit 模式需要 AAA 服务器、无线客户端均支持 192-bit 的安全性，用户可能需要对 AAA 服务器和无线客户端进行相关的升级后来满足这一要求。

# 3 典型组网应用

## 3.1 WPA3-Personal组网

WPA3-Personal 模式的组网方式与使用 PSK 身份认证和密钥管理模式的组网方式一致。当配置为 WPA3-Personal 强制模式时，仅支持 WPA3-Personal 的无线客户端可以接入；当配置为 WPA3-Personal 可选模式时，WPA2-Personal 与 WPA3-Personal 的客户端均可接入。由于可选模式时 WPA2 的无线客户端也可以上线，该模式下依然有 WPA2 中存在的安全漏洞，如易遭受离线字典攻击，因此推荐使用 WPA3-Personal 强制模式。

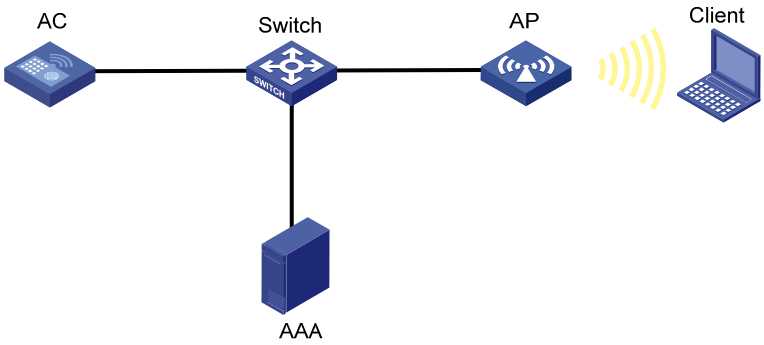
图2 WPA3-Personal 组网示意图




## 3.2 WPA3-Enterprise组网

WPA3-Enterprise 模式的组网方式与传统的使用 802.1X 认证模式的组网方式一致，需要使用 AAA 服务器。AAA 服务器上需安装 ECC P-384 或 RSA > 3072bit 的证书，当使用的 EAP 方法为 EAP-TLS 时，无线客户端也要安装对应的证书。

图3 WPA3-Enterprise 组网示意图




# 4 参考文献


- IEEE Std 802.11-2016
- Wi-Fi CERTIFIED WPA3™Technology overview
- WPA3™-SAE Test Plan
- WPA3™-Enterprise 192-bit Security Test Plan