

目录

第 1 章 管理帧保护	1-1
1.1 标准制定和应用.....	1-1
1.1.1 802.11w协议介绍	1-1
1.1.2 PMF服务介绍	1-1
1.1.3 健壮管理帧保护介绍	1-2
1.1.4 PMF下发介绍	1-3
1.2 PMF基本配置.....	1-3
1.3 PMF配置举例.....	1-4
1.3.1 WPA2-PSK配置举例	1-4
1.3.2 WPA2-EAP配置举例	1-4
1.3.3 配置注意事项	1-5
1.4 PMF排错帮助.....	1-5

第1章 管理帧保护

1.1 标准制定和应用

1.1.1 802.11w协议介绍

IEEE 802.11w 无线加密标准是建立在 IEEE 802.11i（数据帧保护协议）框架上的，它可以对抗针对无线 LAN（WLAN）管理帧的攻击，用来保护客户端与 AP 之间的关联帧，从而防止无线网络攻击，保障客户端网络的安全性。IEEE Task Group 正在改进 IEEE 802.11 的介质保护层，目的是通过提供数据完整性，数据来源的真实性和重放保护。

IEEE 802.11w 主要可以提供三种类型帧的保护。第一种是用于“单播管理封包”（unicast management frames），即一个 AP 与一个 STA 之间的封包。IEEE 802.11w 延伸了 IEEE 802.11i 的临时密钥完整性协议（Temporal Key Integrity Protocol, TKIP）与 RC4 加密算法，将现有的数据加密演算扩展到单播管理帧中。如此一来，可以防止攻击者伪造的管理封包，使其被解密引擎所阻挡，进而增加保密性。第二种是用于“广播管理封包”（broadcast management frames）中，这类信息通常用于调整无线电波频率或者启动测量，并不像单点封包般需要保密，而且广播封包的加密动作比单播封包更为复杂。因此，IEEE 802.11w 只针对这类广播封包提供伪造、放窃听的保护，并不提供加密性的保护，仅依赖一组信息完整性代码附加在无加密的管理包上。最后一种方法则是用于“解除认证与解除关联封包”（deauthentication and disassociation frames）上，通过在 AP 和 STA 上的一对一次密钥（a pair of one-time keys），使用端能确定解除帧是否凑效。

1.1.2 PMF服务介绍

WIFI 是合法和非法设备都能参与的一个广播媒介，管理帧（比如认证帧、去认证帧、关联帧、去关联帧、probe 帧、beacon 帧）被客户端用于发起或者关闭网络会话服务。数据帧可以通过加密（TKIP 或者 CCMP）来保护数据的安全性，但是管理帧为了被所有客户端所理解，必须进行透明传输。由于是透明传输，关联帧必须被保护防止无线网络攻击。802.11w 协议通过 PMF（Protected Management Frames）服务定义了一组强大的管理框架来防止无线攻击，包括以下管理帧：

- Disassociation
- De-authentication
- Spectrum Management
- QoS
- DLS
- Block Ack
- Radio Measurement
- Fast BSS Transition

- SA Query
 - Protected Dual of Public Action
 - Vendor-specific Protected
1. 哪些无线帧不支持 PMF:
 - 1) Beacon and Probe Request/Response
 - 2) Announcement traffic indication message(AITM)
 - 3) Authentication
 - 4) Association request/response
 - 5) Spectrum Management Action
 2. 哪些无线帧支持 PMF
能管理的保护帧是发送密钥建立后，可以使用现有 802.11 的保护密钥层，802.11w 的 RFC 修正案描述说，只有 TKIP/AES 帧受保护而 WEP/OPEN 帧不受保护。
 - 1) Disassociation and Deauthentication
 - 2) Radio Measurement Action for infrastructure BSS(802.11k frames)
 - 3) Qos Action Frame(802.11e frames)
 - 4) Future 11v management frames(802.11v frames)

1.1.3 健壮管理帧保护介绍

•CCMP

- 单播健壮管理帧保护
- 在密钥协商（四次握手）完成之后启动
- 为单播健壮管理帧提供了数据机密性、数据来源验证、完整性保护、重放保护
- 与 CCMP 保护单播数据帧使用的临时密钥一样
- AAD 的计算一样，Nonce 计算有所改动

•BIP

- Broadcast/Multicast Integrity Protocol
- 组播健壮管理帧保护
- 基于 CMAC 模式的 AES-128 算法（Cipher-based Message Authentication Code，基于密码的信息认证码，128bits 数据块、128bits 完整性密钥）
- 使用密钥 IGTK，在 IGTK 协商成功之后可以启用 BIP
- 在帧主体之后添加一个 MIMIE
- 当一个 STA 发送一个受保护的组播健壮管理帧，应该：
 - A、选择 IGTK，构建 MIMIE，即将 MIC 字段设置为 0，KeyID 字段设置为 IGTK 的 KeyID，IPN 字段写入一个单调递增的非负整数；
 - B、计算 ADD；
 - C、计算 AES-128-CMAC，并将 64bits 的输出插入到 MIMIE 的 MIC 字段；
 - D、组合帧，包括 IEEE 802.11 头部、管理帧主体（包括 MIMIE）、FCS，MIMIE 应

该出现在帧主体的最后；

F、发送帧。

•SA Query Procedure

- Security Association Query
- 验证当前安全关联的有效性
- 防止关联封锁问题（Association Lockout problem）
- 通过 SA Query 类型的 Action 帧实现
- AP 和 STA 都有可能发起 SA Query 过程
- 两种帧：SA Query Request、SA Query Response

1.1.4 PMF下发介绍

当用户需要修改开启 PMF 功能时，AC 下发 profile，设置 PMF 使能开关。AP 上线后根据接收到的 profile 配置，进行开启/关闭 PMF 功能。AP 把 PMF 使能开关存储到配置文件中，在创建 vap 的时候使用。

用户根据需要配置 PMF 功能模式，有 2 种模式可以选择，兼容模式或强制模式。

兼容模式包含两种情况，一种是不携带数字签名算法 sha256 打开管理帧保护，一种是携带数字签名算法 sha256 打开管理帧保护。AP 配置兼容模式时，不管终端支持或不支持 802.11w 协议，都可以与 AP 交互。如果终端支持 802.11w，则 AP 与终端基于 802.11w 协议进行交互，若终端不支持 802.11w，则 AP 可以与终端不基于 802.11w 协议进行交互。

强制模式要求终端必须支持 802.11w 协议，才能与 AP 进行交互，否则终端无法成功关联。

1.2 PMF基本配置

1. 开启或关闭兼容模式下不带 sha256 数字签名的 pmf 配置开关

命令	解释
network 配置模式	
pmf enable	开启管理帧保护功能，兼容模式，但是不开启 sha256，no 命令用于关闭 pmf 开关。
no pmf	

2. 开启或关闭兼容模式下带 sha256 数字签名的 pmf 配置开关

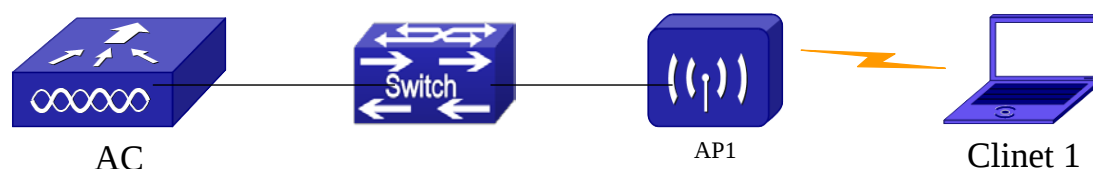
命令	解释
network 配置模式	
pmf enable-sha256	开启管理帧保护功能，兼容模式，并且开启 sha256，no 命令用于关闭 pmf 开关。
no pmf	

3. 开启或关闭 pmf 强制模式配置开关

命令	解释
----	----

network 配置模式	
pmf required	开启管理帧保护功能，强制模式，no 命令用于关闭 pmf 开关。
no pmf	

1.3 PMF配置举例



搭建环境，AC 通过 switch 或 poe 和 ap 相连，ap 被成功管理，client1 关联 ap1。

1.3.1 WPA2-PSK配置举例

1. AC 基本配置：network 模式下配置 pmf 开关、无线认证方式、ssid、无线加密方式、wpa 版本等信息：

```

AC#config
AC(config)#wireless
AC(config-wireless)#network 1
AC(config-network)# pmf enable
AC(config-network)#security mode wpa-personal
AC(config-network)#ssid vlan116
AC(config-network)#wpa ciphers ccmp
AC(config-network)#wpa versions wpa2
  
```

2. 配置 network 并应用：

```

AC(config-wireless)#ap profile 1
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)#vap 0
AC(config-ap-profile-vap)#network 1
AC#wirelessap profile apply 1
  
```

3. 用终端去关联 ssid vlan116，可以关联成功。

1.3.2 WPA2-EAP配置举例

1. AC 基本配置：network 模式下配置 pmf 开关、认证服务器名称、计费服务器名称、无线认证方式、ssid、无线加密方式、wpa 版本等信息：

```

AC#config
AC(config)#wireless
AC(config-wireless)#network 1
  
```

```
AC(config-network)# pmf required
AC(config-network)#radius server-name auth abcd1234
AC(config-network)# radius server-name acct abcd5678
AC(config-network)#security mode wpa-enterprise
AC(config-network)#ssid vlan116
AC(config-network)#wpa ciphers ccmp
AC(config-network)#wpa versions wpa2
```

2. 配置 network 并应用:

```
AC(config-wireless)#ap profile 1
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)#vap 0
AC(config-ap-profile-vap)#network 1
AC(config-ap-profile-vap)#end
AC#wirelessap profile apply 1
```

3. 用终端去关联 ssid vlan116, 可以关联成功。

1.3.3 配置注意事项

需要注意的是, WPA-PSK 和 WPA-EAP 都需要同时配置 CCMP 加密并且配置密钥, AP 和 STA 的无线连接才支持管理帧保护。如果只配置认证方式和 wpa 的版本, 而不配置 wpa 的认证密钥, 无线链路的管理帧将不受 PMF 保护。

单播 deauthentication 帧、单播 disassociation 帧、单播 action 帧、AP 发送的 SA Query 帧、AP 发送的 SA query 回应帧、BIP 保护的广播帧, 这些报文都在 PMF 保护范围内。

当部署的网络范围内的 STA 部分支持 11w, 部分不支持 802.11w, 为了保证兼容性, 我们可以配置 pmf enable、pmf enable-sha256, 当然, no pmf 也可以。当部署的网络对安全性要求比较高, 并且网络设备都支持 802.11w 时, 我们可以选在配置 pmf required 方式, 同时还可以防止无关的终端接入。pc 终端可以在 cmd 窗口中用命令 netsh.exe wlan show driver 查看网卡是否支持 802.11w 管理帧保护。

1.4 PMF排错帮助

在使用中, 如果发现 PMF 配置没有生效或者配置了 PMF 后, STA 无法关联成功, 可以采用下面的检查步骤:

- ☞ 查看当前 AC 和 AP 硬件和版本是否支持管理帧保护。
- ☞ show wireless network 1 | include PMF 查看 client 关联的 ssid 所对应的 network 是否配置了 PMF, 配置的是哪一种模式的 PMF。
- ☞ 检查 AC 的 network 配置的认证方式是否是 WPA2-PSK 或者 WPA2-EAP 中的一种
- ☞ 检查 AC 的 network 配置的加密方式是否是 CCMP, TKIP 或者 CCMP+TKIP 的混合加密是不支持 PMF 的
- ☞ 检查 AC 的 network 配置的 WPA 版本是否是 WPA2

- ☞ 查看终端网卡是否支持 802.11w 协议，目前已知的是部分 intel 无线网卡配合 win8.1 及以上操作系统完美支持 802.11w。