在WLC上配置802.11w管理帧保护

目录

简介

本文档介绍有关IEEE 802.11w管理帧保护及其在Cisco无线LAN控制器(WLC)上配置的详细信息。

先决条件

要求

Cisco建议您了解运行代码7.6或更高版本的Cisco WLC。

使用的组件

本文档中的信息基于运行代码7.6的WLC 5508。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

802.11w标准旨在保护控制和管理帧以及一组强大的管理帧，防止伪造和重播攻击。受保护的帧类型包括Disassociation、Deauthentication和Robust Action帧，例如：

- 频谱管理
- 服务质量 (QoS)

- 块确认
- 无线电测量
- 快速基本服务集(BSS)过渡

802.11w不会加密帧，但它会保护管理帧。它确保消息来自合法来源。为此，必须添加消息完整性检查(MIC)元素。802.11w引入了一个称为Integrity Group Temporal Key(IGTK)的新密钥，用于保护广播/组播鲁棒管理帧。这是与无线保护访问(WPA)一起使用的四向密钥握手过程的一部分衍生的。因此，当您需要使用802.11w时，需要dot1x/预共享密钥(PSK)。它不能与open/webauth服务集标识符(SSID)一起使用。

当协商管理帧保护时，接入点(AP)加密EAPOL-Key帧中的GTK和IGTK值，该EAPOL-Key帧在4次握手的消息3中传送。如果AP稍后更改GTK，它会使用组密钥握手将新的GTK和IGTK发送到客户端。它添加使用IGTK密钥计算的MIC。

管理MIC信息元素(MMIE)

802.11w引入了一个新的信息元素，称为管理MIC信息元素。它具有如图所示的报头格式。

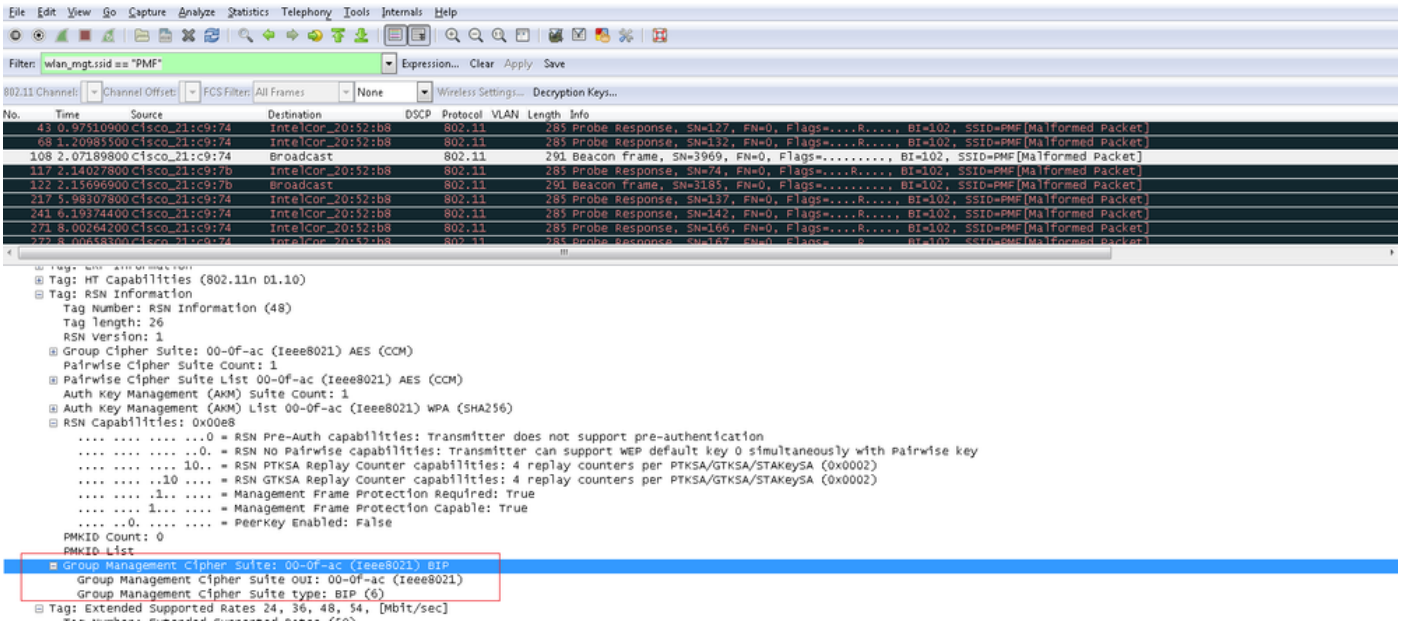
1	1	2	6	8
Element ID	Length	KeyID	IPN	MIC

此处关注的主要字段是元素ID和MIC。MMIE的元素ID为 0x4c 当您分析无线捕获时，它可作为一个有用的标识。

注意:MIC — 它包含在管理帧上计算的消息完整性代码。请务必注意，这是在AP上添加的。然后，目的客户端重新计算帧的MIC，并将其与AP发送的内容进行比较。如果值不同，则作为无效帧将其拒绝。

对RSN IE的更改

强大的安全网络信息元素(RSN IE)指定AP支持的安全参数。802.11w向RSN IE引入了组管理密码套件选择器，其中包含由AP用于保护广播/组播可靠管理帧的密码套件选择器。这是了解AP是否支持802.11w的最佳方法。也可以如图所示进行验证。

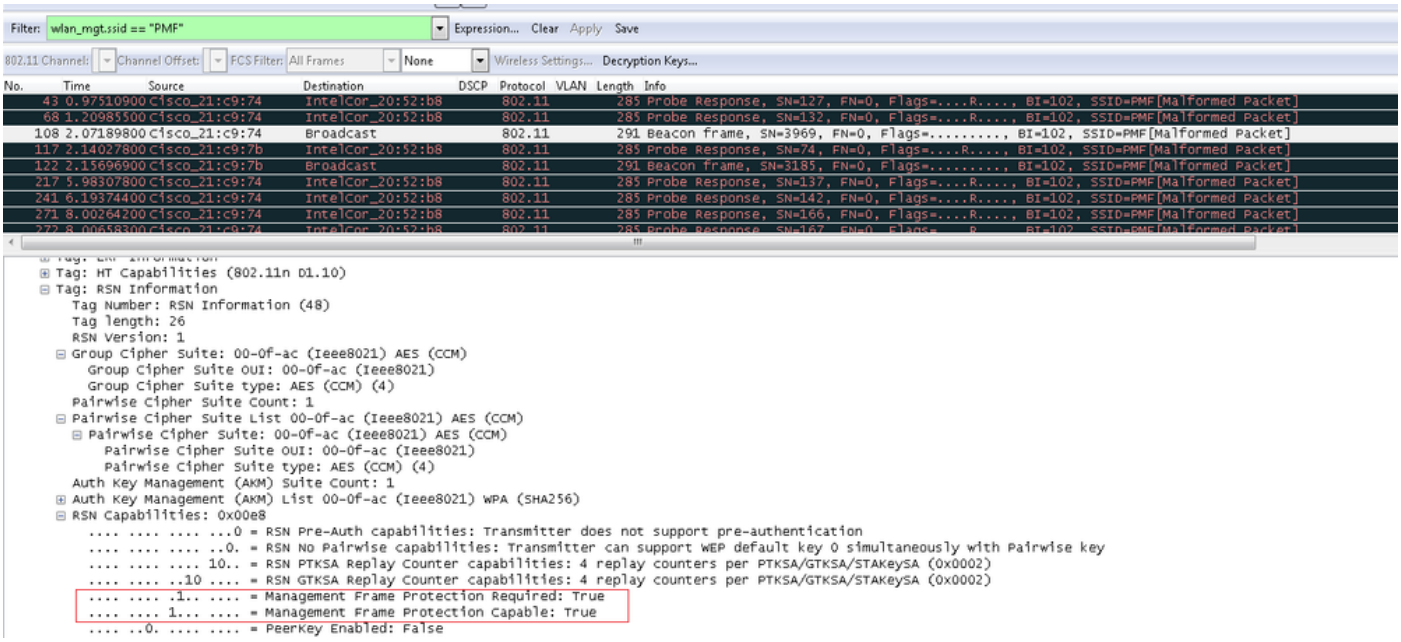


此处，您会找到group management cipher suite字段，该字段显示已使用802.11w。

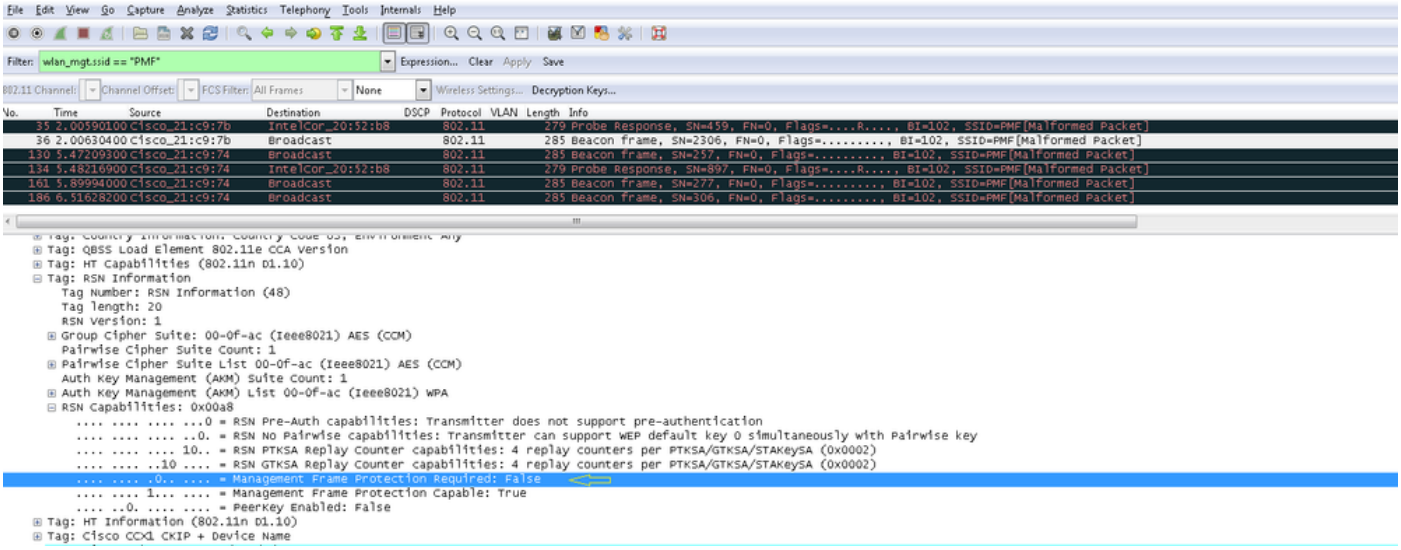
在RSN功能下也进行了更改。第6位和第7位现在用于表示802.11w的不同参数。

- 位6：需要管理帧保护(MFPR)- STA将此位设置为1以通告强健管理帧保护是必需的。
- 第7位：支持管理帧保护(MFPC)- STA将此位设置为1以通告已启用强健管理帧保护。当AP设置时，它会通知它支持管理帧保护。

如果在配置选项下根据需要设置管理帧保护，则同时设置第6位和第7位。如这里的数据包捕获映像所示。



但是，如果将其设置为可选，则仅设置第7位，如图所示。



注意:WLC在关联/重新关联响应中添加此修改的RSN IE，AP在信标和探测响应中添加此修改的RSN IE。

802.11w管理帧保护的优势

- 客户端保护

这通过向Deauthentication和Disassociation帧添加加密保护来实现。这可以防止未经授权的用户通过欺骗合法用户的MAC地址并发送deauth/disassociation帧来发起Denial of Service(DOS)攻击。

- AP保护

通过增加由关联恢复时间和SA-Query过程组成的安全关联(SA)断开保护机制来增加基础设施侧保护。在802.11w之前，如果AP从已关联的客户端收到关联或身份验证请求，则AP将终止当前连接，然后启动新连接。当您使用802.11w MFP时，如果STA已关联并已协商管理帧保护，则AP会拒绝返回状态代码为30的关联请求 Association request rejected temporarily; Try again later 到客户端。

关联响应中包含关联回退时间信息元素，该元素指定当AP准备接受与此STA的关联时的回退时间。这样，您可以确保合法客户端不会因为虚假关联请求而取消关联。

注意：如果客户端不使用802.11w PMF，WLC（AireOS或9800）将忽略客户端发送的取消关联或取消身份验证帧。如果客户端使用PMF，则客户端条目只有在收到此类帧后才会立即被删除。这是为了避免恶意设备拒绝服务，因为这些没有PMF的帧没有安全性。

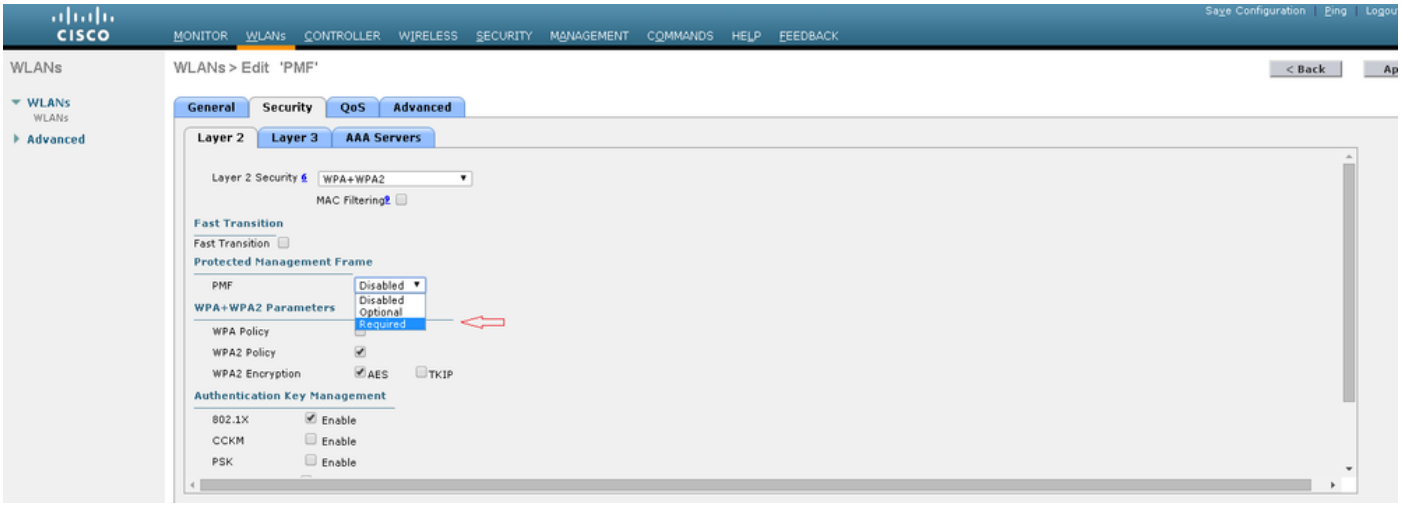
启用802.11w的要求

- 802.11w要求使用dot1x或PSK配置SSID。
- 所有支持802.11n的AP都支持802.11w。这意味着AP 1130和1240不支持802.11w。
- 7.4版本中的flexconnect AP和7510 WLC不支持802.11w。自7.5版本以来已添加支持。

配置

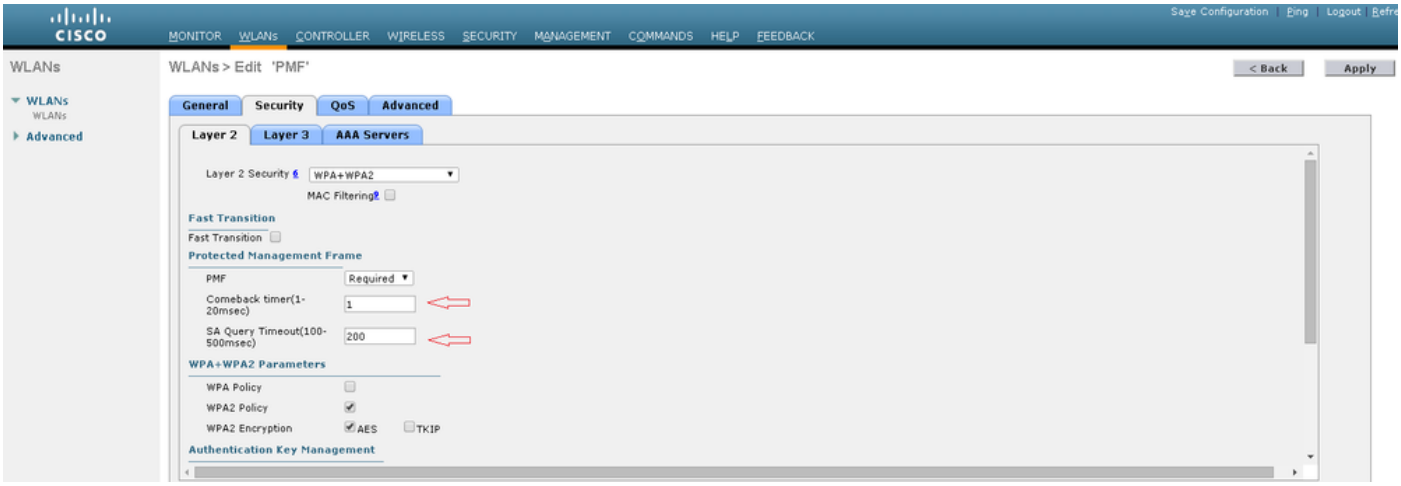
GUI

步骤1:您需要在配置了802.1x/PSK的SSID下启用受保护的管理帧。您有三个选项，如图所示。

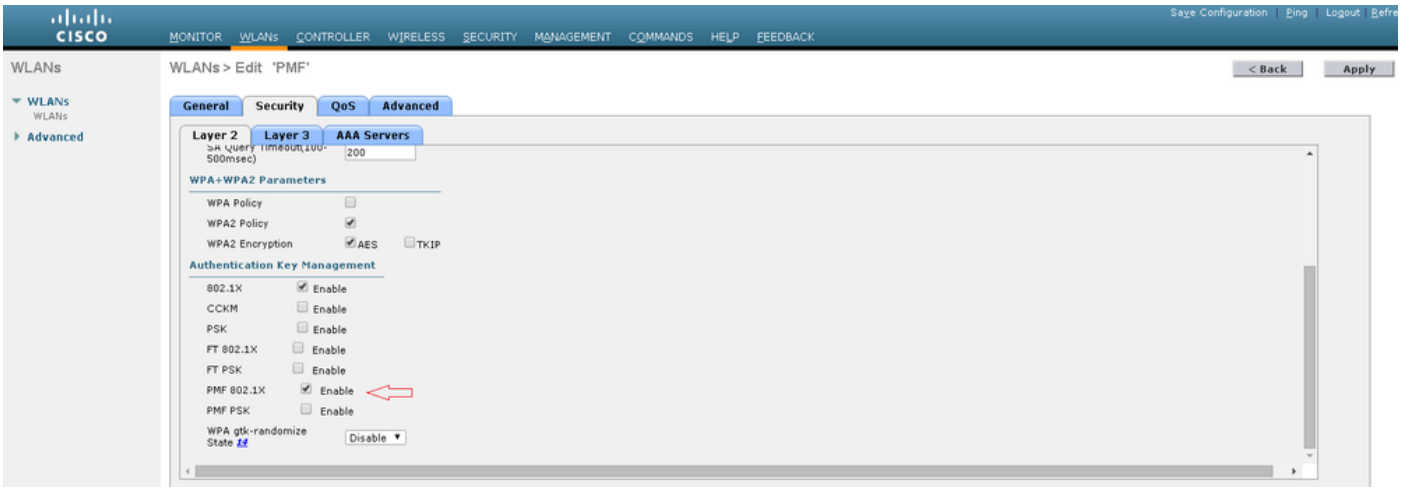


“Required”指定不允许不支持802.11w的客户端进行连接。“可选”指定甚至允许不支持802.11w的客户端进行连接。

第二步：然后，您需要指定恢复计时器和SA查询超时。Comeback timer指定关联客户端在首次被拒绝时再次尝试关联之前必须等待的时间，状态代码为30。SA查询超时指定WLC等待来自客户端的查询进程的响应的时间。如果没有来自客户端的响应，其关联将从控制器中删除。如图所示。



第三步：如果将802.1x用作身份验证密钥管理方法，则必须启用“PMF 802.1x”。如果使用PSK，则必须选择PMF PSK复选框，如图所示。



CLI

- 要启用或禁用11w功能，请运行命令：

config wlan security wpa akm pmf 802.1x enable/disable

config wlan security wpa akm pmf psk enable/disable

- 要启用或禁用受保护管理帧，请运行命令：

config wlan security pmf optional/required/disable

- 关联回显时间设置：

config wlan security pmf 11w-association-comeback

- SA查询重试超时设置：

config wlan security pmf saquery-retry-time

验证

使用本部分可确认配置能否正常运行。

802.11w配置可以验证。检查WLAN配置：

```
(wlc)>show wlan 1
Wi-Fi Protected Access (WPA/WPA2)............. Enabled
<snip>
802.1x................................ Enabled
PSK................................... Disabled
CCKM.................................. Disabled
FT-1X(802.11r)........................ Disabled
FT-PSK(802.11r)....................... Disabled
PMF-1X(802.11w)....................... Enabled
PMF-PSK(802.11w)...................... Disabled
FT Reassociation Timeout.................. 20
FT Over-The-DS mode....................... Enabled
GTK Randomization......................... Disabled
<snip>
PMF....................................... Required
PMF Association Comeback Time................. 1
PMF SA Query RetryTimeout..................... 200
```

故障排除

本节提供可用于对配置进行故障排除的信息。

以下debug命令可用于排除WLC上的802.11w问题：

- **debug 11w-pmf events enable/disable**
- debug 11w-pmf keys enable/disable
- debug 11w-pmf all enable

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。