通过RADIUS服务器和无线控制器动态分配VLAN

介绍

本文介绍一种新的叫做管理帧保护（MFP）的安全功能，该文件还介绍了如何在 LAP 和 WLC 上配置 MFP 的功能。

配置条件

必要条件

在配置前，请先确定掌握以下知识点：

（1） WLC 和 LAP 的基本知识

（2） 802.11 的管理帧的相关知识

使用说明

本文涉及的信息基于以下软件及硬件版本：

（1） 运行 4.1 版固件的思科 2000 系列 WLC

（2） 思科 1131AG LAP

（3） 使用固件 3.6 的思科８０２．１１ａ／ｂ／ｇ的无线客户端

（4） 软件版本 3.6 的思科无线客户软件（ＡＤＵ）

【译者注】在 WLC 版本 4.0.155.5 及以后就支持 MFP，版本 4.0.206.0 提供可选的执行 MFP，客户端的 MFP 在版本 4.1.171.0 及后续支持。

文档中描述的是在实验环境，所有设备都是初始配置，请先确定各命令的意义，再做配置。

规定

请参考以下网址，获得更多信息
http://www.cisco.com/en/US/tech/tk801/tk36/technologies_tech_note09186a0080121ac5.shtml

知识点

在 802.11 中，认证过程，连接过程和探查过程中使用的管理帧都是没有经过认证和加密的，换句话说，802.11 的管理帧经常被以不安全的形式发送，而不像被 WPA，WPA2 或者 WEP 加密的数据。

这样的话，一个攻击者就会模仿管理帧，对连接到 AP 上的客户端发起攻击。攻击者的行为可以是

(1) 对无线网络进行 DOS 攻击
(2) 中间人的攻击
(3) 非在线的字典攻击

当在无线网络中对管理帧进行认证后，可以杜绝上述攻击

【译者注】本文档描述构造以及客户端 MFP
【译者注】当无线设备开启了 MFP 的功能时，对于某些无线客户端，有某种限制。MFP 会为每个探针和 SSID 添加一段信息。像 PDA，智能手机，条码扫描器等无线设备，不能处理这些请求，不能完全的看到 SSID，和接入无线设备，取决于识别 SSID 的能力。这个问题并不是因为 MFP 产生的，而是因为某些 SSID 具有多个信息结构（IEs）。可以通过在部署前，检测打开的 MFP 的 SSID 的无线设备的接入功能，避免更多的客户无线接入。

【译者注】MFP 的构成
（1） 管理帧保护，当打开管理帧的保护功能，AP 会为传输的管理帧添加信息完整性检查（MIC IE），任何试图复制，修改或者替换，都会使 MIC 无效，被配置检测 MFP 的 AP 会检查 MIC 属性，并通告给 WLC
（2） 管理帧确认，当管理帧确认功能被打开后，AP 会检测从其他 AP 接受到的所有的管理帧，它将检测 MIC 的完整性，如果接受到的 MIC 的信息不完整，将会报告。
（3） 信息报告，当 AP 发现有不规则的信息，会通知 WLC，会通过 SNMP 告知管理员

MFP 功能的构造

使用 MFP 后，所有的管理帧都会被加密，并建立完整性检查（MIC），MIC 会被添加到帧的后面以及帧校验序列（FCS）之前。
（1） 在集中架构中，MFP 在 WLC 中开启，可以基于每个 WLAN 中打开保护，及检测功能。
（2） 当设备不能处理帧保护时，可以基于 WLAN 关闭保护功能。
（3） 当负荷超载时，要在 AP 上关闭确认功能。

当在 WLC 中，为某些 WLAN 配置 MFP 的功能时，WLC 会给每个注册到上面的 AP 发送唯一的密钥，AP 在每个打开 MFP 功能上的 WLAN 中发送管理帧，这些 AP 会被标识为帧的完整性保护功能，任何对信息的改变，都会使其无效，AP 会发现帧的改变，并通知到 WLC。

（1） 当在 WLC 上全局打开 MFP 时，WLC 会为每个配置 MFP 的 AP 产生一个唯一的密钥，WLC 会在移动的环境中，知道每个 AP。

【译者注】所有在移动组内的 WLC 都要配置为 MFP

（2） 当一个 AP 不能识别收到的被保护的 MFP 时，会存储它，并向 WLC 请求密钥

（3） 如果 WLC 中也没有关于此的标识，它会返回一个不能标识的 BSSID 给 AP，AP 会丢弃相应的 MFP

（4） 如果 WLC 知道相应的 BSSID，但是 MFP 是在相应的 BSSID 中关闭，WLC 会返回“关闭 BSSID”的命令，AP 会认为收到的 MFP 都是没有完整性（MIC）检查。

（5） 如果 WLC 知道相应的 BSSID，并且也在相应的 WLAN 中开启，WLC 会告知 AP 相应的密钥。

（6） AP 保存相应的密钥，为 MFP 做完整性检查

客户端 MFP 的功能

客户端 MFP 保护那些在无线网络中的客户不会被攻击。

特别的，客户端 MFP 会在无线接入点和 CCXV5 的客户端之间，加密管理帧，以便拒绝网络攻击行为，客户端 MFP 是 IEEE802.11i 中定义保护以下三种类型的单播管理帧，分离，重认证，和 QOS（WMM）。它可以保护接入无线网络的客户避免 DOS 攻击，它为三种管理帧提供同样的加密方式。如果无线接入点或者客户收到未加密的数据，丢弃数据并报告给 WLC。

如果客户端要使用客户端 MFP，必须支持 CCXv5 的 MFP 以及使用 TKIP 或者 AES-CCMP 加密的 WPA2 认证方式，EAP 或者 PSK 的认证方式可以获得 PMK，在二层或者三层漫游中，CCKM 和 WLC 的移动管理，用来在 AP 和客户端之间分布密钥。

为了阻止广播帧的危害，支持 CCXv5 的 AP 不会传输任何以上三种帧的广播，CCXv5 的客户端以及 AP 会拒绝三种管理帧的广播形式。

客户端 MFP 的组成

由以下部件组成：

（1） 密钥的产生和分发

（2） 保护以及确认管理帧

（3） 错误报告

密钥的产生和分发

客户端 MFP 并不使用 MFP 结构的密钥产生和分发过程，取而代之的是，客户端 MFP 是 IEEE802.11i 中定义保护以下三种类型的单播管理帧，分离，重认证，和 QOS（WMM）。

AES-CCMP 和 TKIP 会在 IV 的地方包含序列号，以便防止被替代的发生，通过杜比序列号的大小，察看是否有替代发生。

错误报告

MFP-1 的报告格式，是用来 AP 报告发现的重封装的管理帧，WLC 通过收集错误报告以便发送给 WCS。

广播管理帧的保护

为了阻止使用广播帧的攻击，支持 CCXv5 的 AP 不会转发三种管理帧的广播形式，具备 CCXv5 的客户端会丢弃收到的广播帧。

支持的平台

（1） WLC：

2006

2106

4400

WISM

带 WLC 的 3750

26/28/37/38xx Routers

（2） LWAPP

1000 系列

1100，1130

1200，1240，1250

1310

（3） 客户端软件

ADU 3.6.4 或者以上版本

（4） 网络管理

WCS

1500 系列的 LAP 不支持

支持方式

Supported Access Point Modes	
Mode	Client MFP Support
Local	Yes
Monitor	No
Sniffer	No
Rogue Detector	No
Hybrid REAP	Yes
REAP	No
Bridge Root	Yes

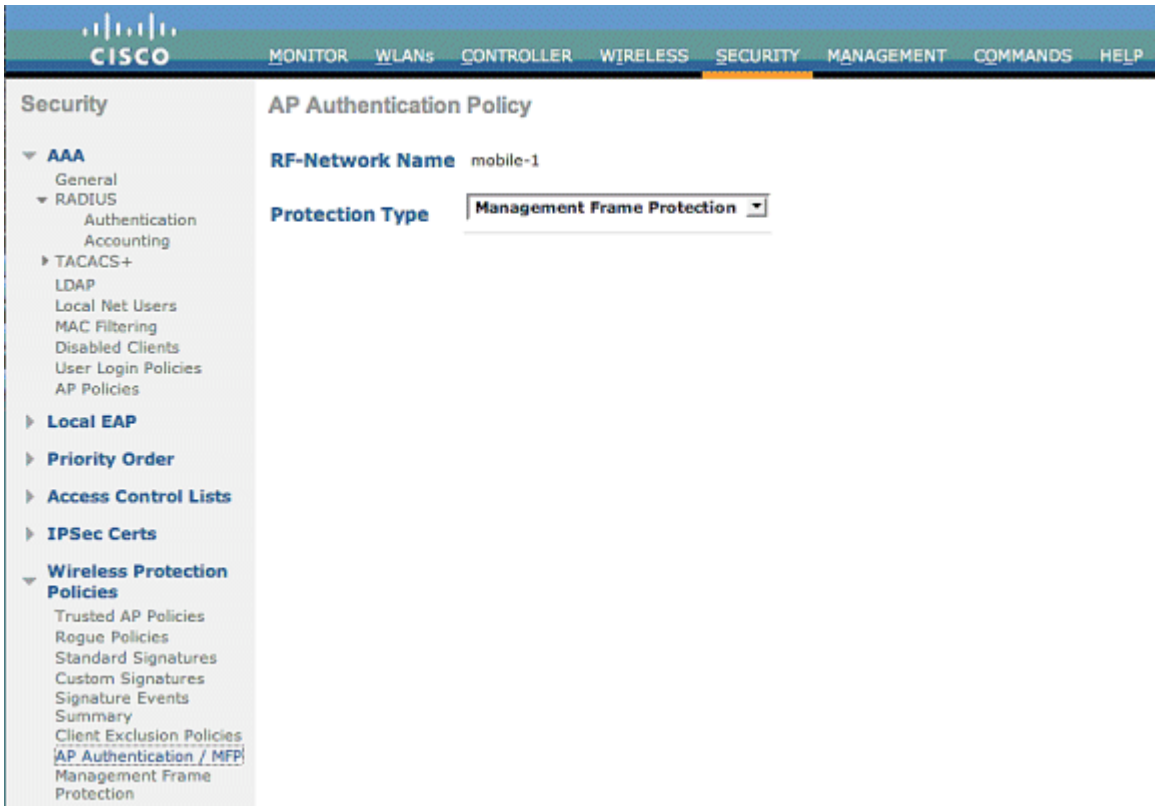
WGB	No

混合单元的支持

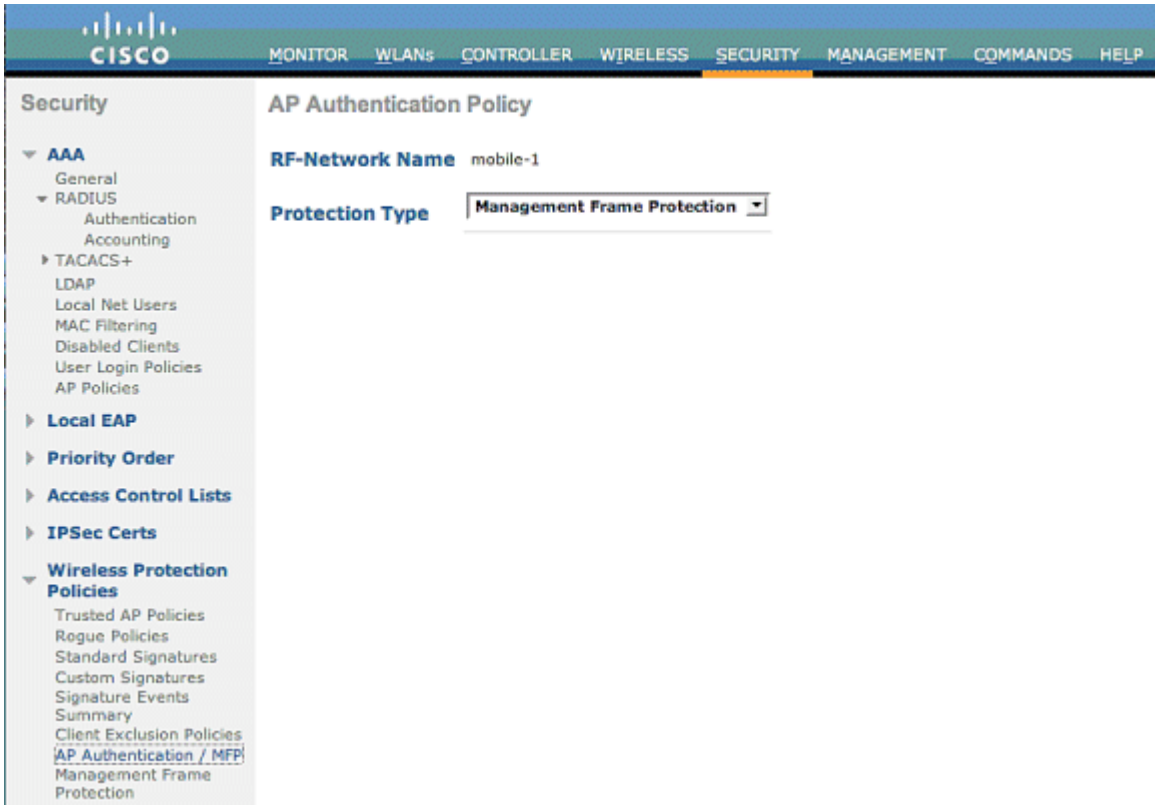
不支持 CCXv5 的客户端可以接入 MFP-2 的无线网络，AP 会跟踪这些客户端，并检测是否具有网络安全威胁。

在 WLC 上配置 MFP

（1） 点击 **Security**，单击 **AP Authentication/MFP** under **Wireless Protection Policies**

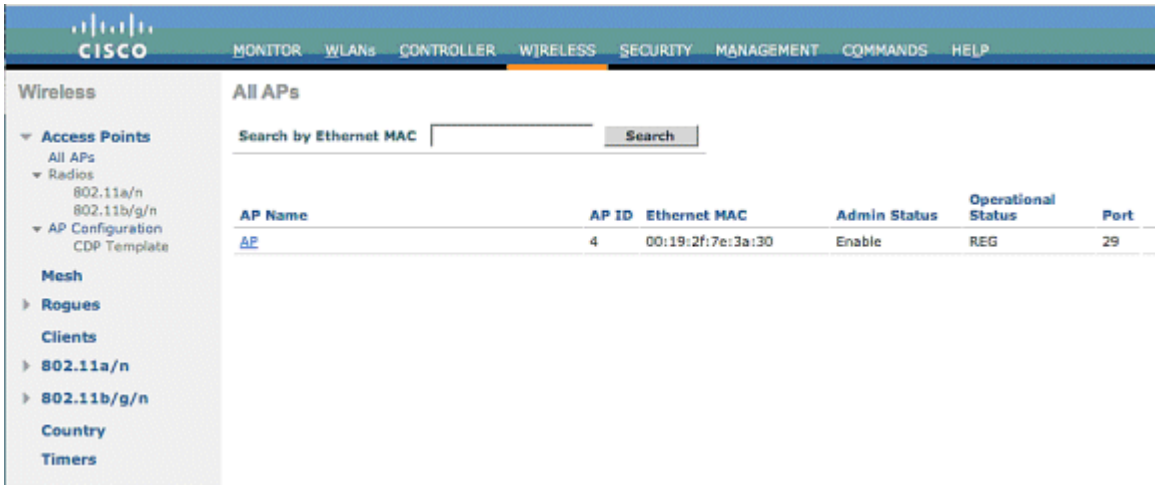


（2） 选择 **Management Frame Protection**



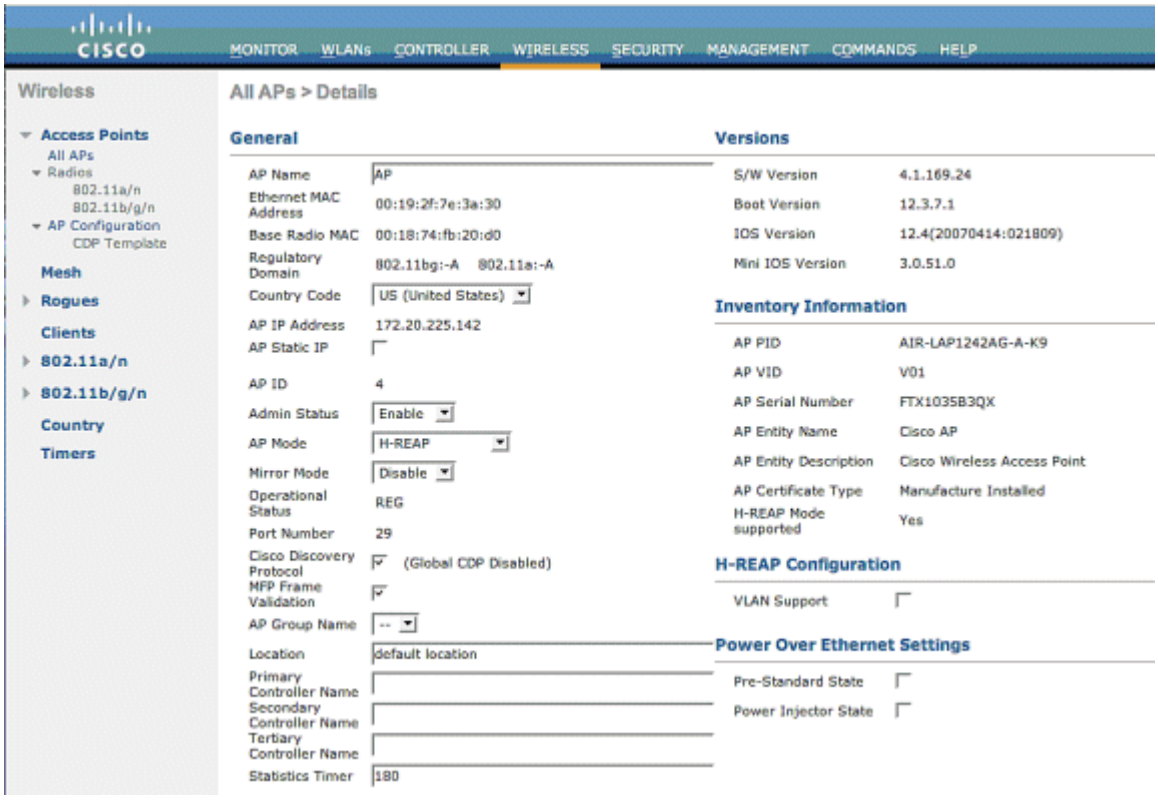
在 LAP 上配置 MFP 的检查

（1） 在 Wireless 下点击 **Access Points**，单击 Detail



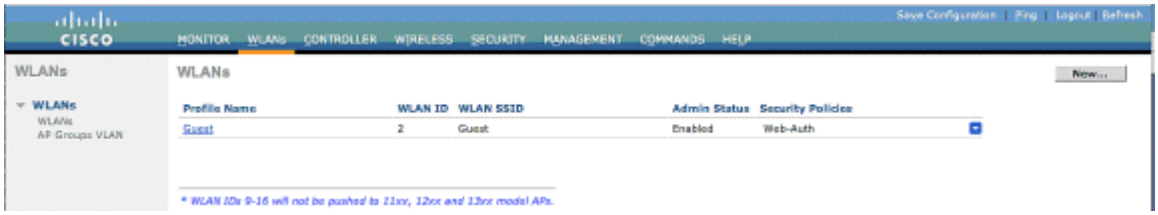
（2） 在 Detail 下，点击 **MFP Frame Validation**

【译者注】在 Sniffer 模式下的 AP 不能配置 MFP

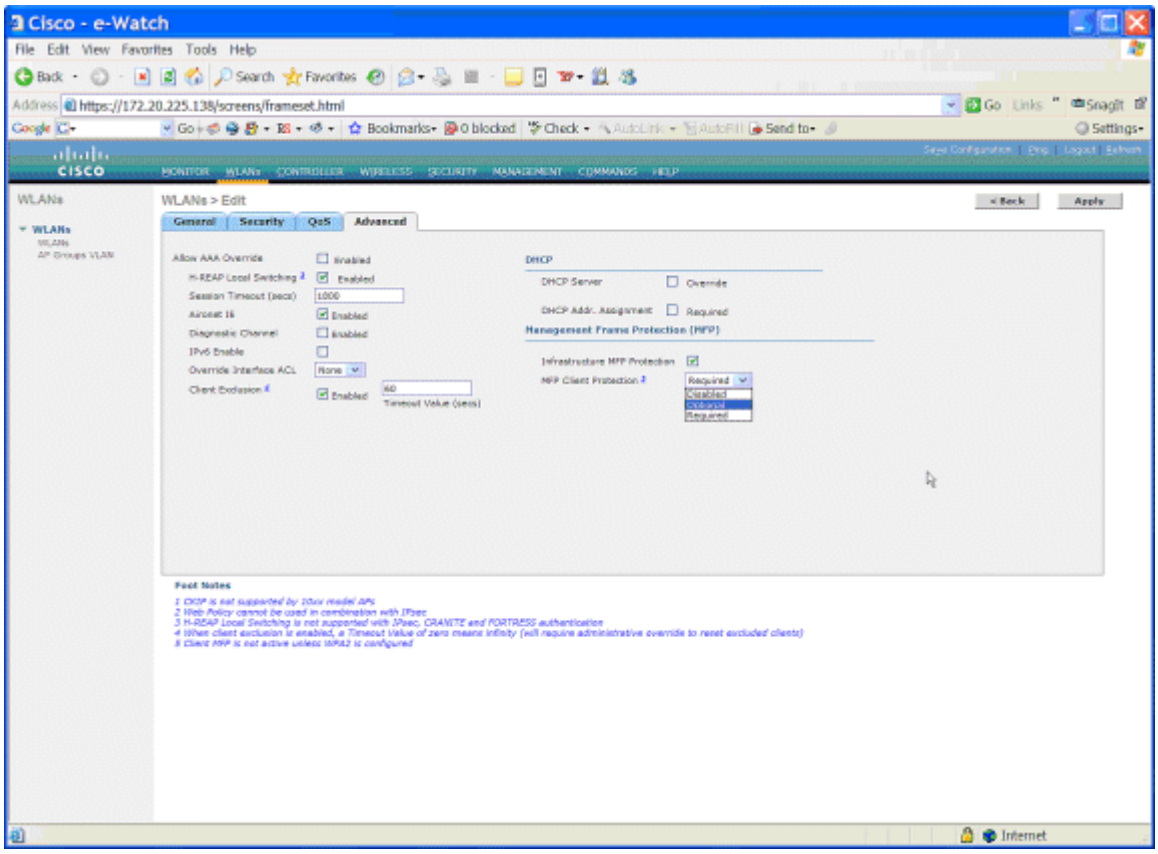


在 WLAN 上配置 MFP

（1） 点击 **WLANs** 单击 New

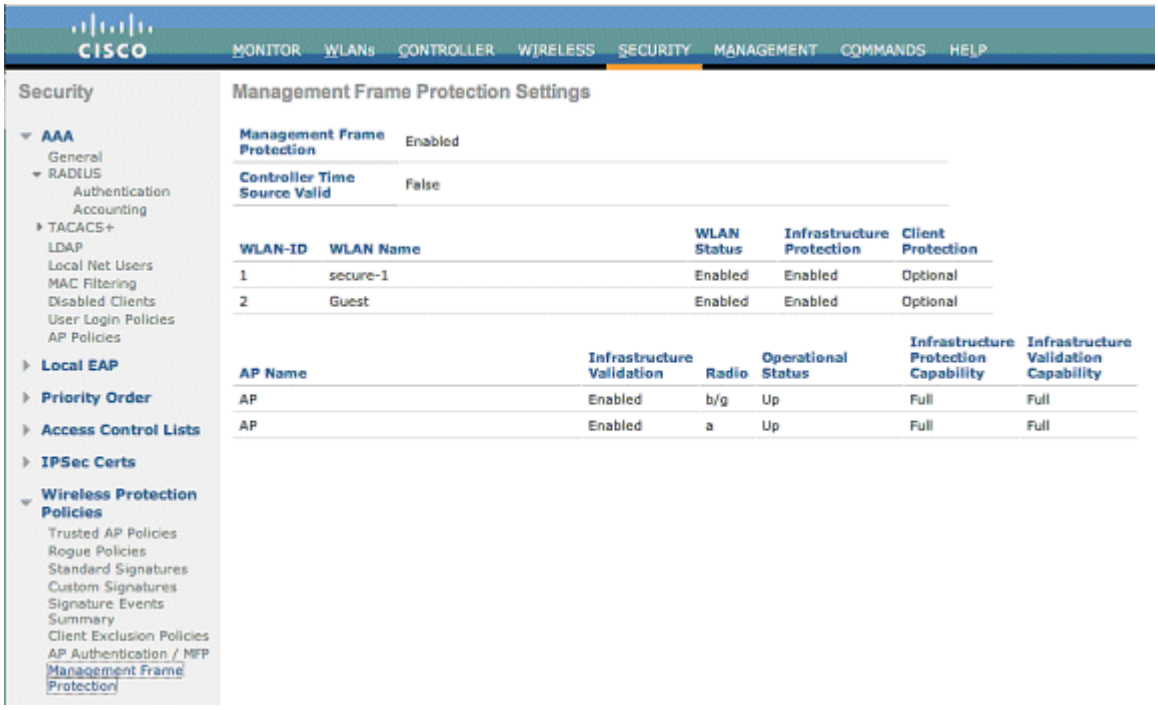


（2） 点击 **Infrastructure MFP Protection**



检测

单击 **Management Frame Protection**



在 MFP 配置界面，你可以看到配置情况

（1） 在 WLC 上是否开启 MFP

（2） 在 WLC 上配置相应的时间属性

【译者注】如果开启了 MFP，建议配置 NTP 服务器

（3） **MFP Protection** 显示为独立的 WLAN 开启 MFP

（4） **MFP Validation** 显示 MFP 的检测

以下命令很有用处

show wps summary 显示 MFP 的总结

show wps mfp summary 显示在 WLC 配置 MFP 的情况

show ap config general *AP_name* 显示某个 AP 关于 MFP 的配置情况

```
(Cisco Controller) >show ap config general AP

Cisco AP Identifier..............................4
Cisco AP Name....................................AP
Country code.....................................US    - United States
Regulatory Domain allowed by Country.............802.11bg:-AB        802.11a:-AB
AP Country code..................................US    - United States
AP Regulatory Domain.............................802.11bg:-A        802.11a:-A
Switch Port Number ..............................29
MAC Address......................................00:19:2f:7e:3a:30
IP Address Configuration.........................DHCP
IP Address.......................................172.20.225.142
IP NetMask.......................................255.255.255.248
Gateway IP Addr..................................172.20.225.137
Cisco AP Location................................default location
Cisco AP Group Name..............................default-group
Primary Cisco Switch.............................
Secondary Cisco Switch...........................
Tertiary Cisco Switch............................
Administrative State ............................ADMIN_ENABLED
Operation State .................................REGISTERED
Mirroring Mode ..................................Disabled
AP Mode .........................................H-Reap
Public Safety ...................................Global: Disabled, Local: Disabled
Remote AP Debug .................................Disabled
S/W    Version ..................................4.1.169.24
Boot    Version .................................12.3.7.1
Mini IOS Version ................................3.0.51.0
Stats Reporting Period ..........................180
LED State........................................Enabled
PoE Pre-Standard Switch..........................Disabled
PoE Power Injector MAC Addr......................Disabled
Number Of Slots..................................2
AP Model.........................................AIR-LAP1242AG-A-K9
IOS Version......................................12.4(20070414:021809)
```

```
Reset Button..................................... Enabled
AP Serial Number................................ FTX1035B3QX
AP Certificate Type............................. Manufacture Installed
H-REAP Vlan mode :............................... Disabled
Management Frame Protection Validation........... Enabled
Console Login Name..............................
Console Login State............................. Unknown
Ethernet Port Duplex............................ Auto
Ethernet Port Speed............................. Auto



Cisco Controller) >show wps mfp summary

Global MFP state................................ enabled
Controller Time Source Valid..................... false


                                                WLAN          Infra.        Client
WLAN ID    WLAN Name                            Status        Protection    Protection
-------    ------------------------    ---------    ----------    ----------
1          secure-1                             Enabled       Enabled       Optional
2          Guest                                Enabled       Enabled       Optional  but  inactive
(WPA2 not configured)

                                   Infra.                   Operational        --Infra. Capability--
AP Name                            Validation    Radio      State              Protection    Validation
--------------------    ----------    -----    --------------    ----------    ----------
AP                                 Enabled       b/g        Up                 Full          Full
```