在统一无线网络的恶意管理

目录

简介

无线网络是对有线网络的延伸，它提高了工作人员的工作效率，便于工作人员访问信息。然而，一个未授权的无线网络提交安全性问题一块另外的层。对有线网络上的端口安全问题关注较少，并且无线网络相对于有线网络来说，更易于推广。所以，带领他们自己的接入点的员工(思科或非思科)进入一受到良好保护的无线或有线基础架构并且否则提供对此的未经授权的用户用户访问安全网络，能容易地减弱安全网络。

恶意程序检测允许网络管理员监控和排除此类安全问题。Cisco Unified网络架构为恶意检测提供启用一完整恶意识别和遏制解决方案，不用对昂贵和难以证明覆盖网络和工具的需要的方法。

先决条件

要求

本文假设您熟悉基本控制器配置。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息基于以下软件和硬件版本：

- 运行版本7.0的Cisco Unified控制器(2100， 5500， 4400,WiSM和NM-WLC系列)
- 控制和供应无线接入点协议(CAPWAP) -基于膝部- 1130AG， 1140， 3500， 1200， 1230AG， 1240AG， 1250和1260系列膝部

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

恶意概述

共享您的光谱和没有由您管理的所有设备可以假定有歹徒。歹徒在这些情况下变得危险：

- 当设置使用SSID和您的网络(蜂蜜)一样。
- 当它在有线网络也检测。
- 临时歹徒也是一个大威胁。
- 由局外人设置，多数次，与恶意目的。

有三个主要阶段在Cisco Unified无线网络(UWN)解决方案的恶意设备管理：

- 检测–高级无线电资源管理(RRM)扫描用于检测恶意设备出现。
- 分类–恶意位置发现协议(RLDP)，恶意探测器和交换机端口跟踪用于识别，如果恶意设备连接对有线网络。恶意分类规则也协助解决过滤歹徒到根据他们的特性的特定类别。
- 缓解–交换机端口关闭，恶意位置和恶意遏制用于搜寻其物理位置和使恶意设备的威胁无效。

恶意管理运行原理

入侵检测

歹徒根本是共享您的光谱的所有设备，但是不在您的控制中。这包括非法接入点(AP)，无线路由器、恶意客户端和恶意临时网络。思科UWN使用一定数量的方法检测基于WI-FI的恶意设备包括脱离信道扫描和专用的监控模式功能。Cisco Spectrum Expert可能也使用识别根据802.11协议没的恶意设备，例如蓝牙网桥。

脱离信道扫描

此操作由本地传送方式和H-REAP (在已连接模式) AP执行并且使用允许客户端服务和信道扫描使用同样无线电的时间分割技术。默认情况下，通过去信道期限50ms每16秒， AP只度过不为其的时间的小百分比客户端服务。并且，请注释那里是将发生的10ms信道更改间隔。在默认scan interval 180秒，每个2.4Ghz FCC信道(1-11)至少一次被扫描。对于其他管理域，例如ETSI， AP时间的一个轻微高百分比的信道。信道列表和scan interval可以在RRM配置里调节。这对最多1.5%限制性能影响，并且智能被建立到算法暂停扫描，当高优先权QoS帧，例如语音，需要传送时。

此图形是脱离信道扫描算法的描述本地传送方式AP的在2.4GHz频率波段。如果AP有一存在，一相似的操作在5GHz无线电平行被执行。每红场代表在AP家庭信道的中花费的时间，而每蓝色square代表在邻接信道的中花费的时间扫描的目的。

监控模式扫描

此操作由监控模式和使用100%扫描所有信道的无线电的时期在每各自频率波段的可适应wIPS监控模式AP执行。这准许一更加了不起的速度检测并且启用更多时刻在每单个信道上度过。因为他们有发生的活动的更多综合视图在每个信道，监控模式AP也是更主管在检测恶意客户端。

此图形是脱离信道扫描算法的描述监控模式AP的在2.4GHz频率波段。如果AP有一存在，一相似的操作在5GHz无线电平行被执行。

本地传送方式和监控模式比较

本地传送方式AP拆分其在服务WLAN客户端和扫描信道之间的周期威胁的。结果，它采取更加长本地传送方式的AP通过所有信道循环，并且在所有特定信道上花费收集数据的较少时间，以便没有打乱客户端操作。结果，歹徒和攻击检测检测时间更加长(3到60分钟)，并且一个更加小的范围通过空气攻击可以检测比与监控模式AP。此外，突发数据流的检测，例如恶意客户端，较不确定的，因为AP必须在流量的信道流量同时传送或接收。这变为在可能性的一练习。监控模式AP花费扫描信道的所有其周期寻找歹徒和通过空气攻击。监控模式AP可能同时用于可适应wIPS、位置(上下文意识)服务和其他监控模式服务。当监控模式AP部署时，好处是更低定期对检测。当监控模式AP另外配置与可适应wIPS时，各种各样的通过空气威胁和攻击可以检测。

恶意识别

如果探测响应或信标从恶意设备由本地传送方式听到， H-REAP模式或者监控模式AP，则此信息通过CAPWAP被传达对无线局域网控制器(WLC)处理的。为了防止错误肯定，一定数量的方法用于保证其他管理的基于Cisco的AP没有识别作为恶意设备。这些方法通过无线控制系统(WCS)包括移动组更新、RF邻接数据包和白色列表自治AP。

恶意记录

当恶意设备控制器的数据库包含仅当前设置检测的歹徒时， WCS也包括事件历史记录和不再看到的日志歹徒。

[恶意程序详细信息]

CAPWAP AP去50ms的脱离信道为了细听恶意客户端，为噪声和信道干扰监控。所有检测到的恶意客户端或 AP 被发送到用于收集此信息的控制器：

- 恶意AP的MAC地址
- AP检测的歹徒的名称
- 恶意程序连接的客户端 MAC 地址
- 是否用 WPA 或 WEP 保护帧
- 报头
- 信噪比 (SNR)
- 接收信号强度指示符 (RSSI)
- 恶意检测信道
- 歹徒检测的无线电
- 恶意SSID (如果恶意SSID广播)
- 恶意IP地址
- 歹徒报告的首先和上次
- 信道宽度

导出恶意事件

为了导出恶意事件到归档的一个第三方网络管理系统(NMS)，将被添加的WLC许可证另外的

SNMP陷阱接收器。当检测或控制器时清除歹徒，包含此信息的陷阱被传达到所有SNMP陷阱接收器。与导出事件的一个警告通过SNMP是，如果广泛控制器检测同样恶意，重复的事件由NMS看到，相关性只完成在WCS。

恶意记录超时

一旦非法AP被添加了到WLC's记录，将保持那里，直到不再被看到。在用户可配置超时(1200秒默认)以后，_unclassified_类别的一个歹徒老化。歹徒在其他状态例如_Contained_和_Friendly_将仍然存在，以便适当的分类应用对他们，如果他们再现。

有在控制器平台间是可变恶意记录的一个最大数据库大小：

- 21XX和WLCM - 125个歹徒
- 44XX - 625个歹徒
- WiSM - 1250个歹徒
- 5508个- 2000个歹徒

恶意分类

默认情况下，由思科UWN检测的所有歹徒被认为未保密。如此图形所示，歹徒在一定数量的标准可以分类包括RSSI、SSID、安全类型、开/关客户端网络和编号：

恶意探测器AP

歹徒探测器关联恶意信息的AP目标听到在空气与从有线网络得到的ARP信息。如果MAC地址在空气在有线网络听到作为非法AP或客户端和也听到，则确定歹徒是在有线网络。如果歹徒检测是在有线网络，则该非法AP的告警严重性被上升到_critical_。值得注意的是，歹徒探测器AP不是成功的在识别恶意客户端在设备背后使用NAT。

可扩展性考虑事项

歹徒探测器AP能检测500个歹徒和500个恶意客户端。如果恶意探测器在一中继被放置用许多恶意设备，则这些限额也许超过，导致问题。为了防止其发生，请保持恶意探测器AP在您的网络分配或接入层。

RLDP

如果一特定非法AP连接对有线基础架构， RLDP的AIM将识别。此功能根本使用最接近的Unified AP连接到恶意设备作为无线客户端。在连接作为客户端以后，数据包用WLC的目的地址传送估计，如果AP连接对有线网络。如果歹徒检测是在有线网络，则该非法AP的告警严重性被上升到关键。

列出得RLDP算法此处：

1. 识别最接近的Unified AP给使用信号强度值的歹徒。
2. AP然后连接给歹徒作为WLAN客户端，尝试三个关联在定时前。
3. 如果关联是成功的，然后AP使用DHCP获取IP地址。
4. 如果IP地址获取， AP (作为WLAN客户端)发送UDP数据包对其中每一个控制器的IP地址。
5. 如果控制器收到均等一个从客户端的RLDP数据包，该歹徒被标记作为在电线用严重性关键。

注意： RLDP数据包无法到达控制器，如果过滤规则是到位在控制器的网络和恶意设备查找的网络之间。

RLDP警告

- RLDP只运作与广播他们的与验证的SSID和加密的开放歹徒AP禁用。
- RLDP要求作为客户端的托管型AP能通过在恶意网络的DHCP获取IP地址
- 手工的RLDP可以用于多次尝试和在歹徒的RLDP trace。
- 在RLDP进程中， AP无法服务客户端。这将负面影响性能和连接本地传送方式AP的。
- RLDP不尝试连接到操作在5GHz DFS信道的非法AP。

交换机端口跟踪

交换机端口跟踪是在5.1版本首先实现的非法AP缓和技术。虽然交换机端口跟踪启动在WCS，使用CDP和SNMP信息搜寻歹徒到网络的一个特定端口。为了交换机端口跟踪能运行，必须添加在网络的所有交换机到与SNMP凭证的WCS。虽然只读凭证为识别端口工作歹徒继续下去，读写凭证允许WCS也关闭端口，因而包含威胁。此时，此功能用运行IOS以启用的CDP的Cisco交换机仅运作，并且在托管型AP必须也启用CDP。

列出得交换机端口跟踪的算法此处：

- WCS查找最接近的AP，检测通过空气的非法AP，并且获取其CDP邻居。
- WCS然后使用SNMP检查在相邻交换机内的CAM表，寻找一正匹配识别歹徒位置。
- 一正匹配根据确切的恶意MAC地址、+1/−1恶意MAC地址，所有恶意客户端MAC地址或者根据供应商信息的OUI匹配内在MAC地址。
- 如果一正匹配在最接近的交换机没有被找到， WCS持续搜索相邻交换机至离开两的跳(默认情况下)。

恶意分类规则

指示一个歹徒如有恶意或友好的恶意分类规则，介绍在5.0版本，允许您定义一组条件。这些规则配置在WCS或WLC，但是他们在控制器总是执行如新建的歹徒已发现。

读在无线局域网控制器(WLC)和无线控制系统(WCS)的本文基于规则的恶意分类关于在WLCs的恶意规则的更多信息。

欺诈缓解

欺诈遏制

遏制是使用通过空气数据包方法临时地中断在恶意设备的服务，直到可能物理的删除。遏制工作在伪装解除验证数据包旁边和非法AP的被伪装的源地址一起，以便所有客户端关联开始。

恶意遏制详细信息

在非法AP启动的遏制没有客户端只将使用解除验证帧发送对广播地址：

在与客户端的一非法AP启动的遏制将使用解除验证帧发送对广播地址和对客户端地址：

遏制数据包被发送在管理的AP的功率电平和以最低的已启用数据速率。

遏制发送至少2数据包每个100ms ：

注意： 从6.0版本，非箴言报模式执行的遏制AP发送在间隔500ms而不是监控模式使用的100ms间隔AP。

- 一个单个恶意设备可以由1到4包含在联合工作临时地缓和威胁的管理的AP。
- 使用本地传送方式，监控模式和H-REAP (已连接)模式AP，遏制可以执行。对于本地传送方式H-REAP AP，最多每无线电三个恶意设备可以包含。对于监控模式AP，最多每无线电六个恶意设备可以包含。

自动遏制

除手工启动在一个恶意设备的遏制之外通过WCS或WLC GUI，也有能力自动地启动遏制在某些方案下。此配置被找到在WCS或控制器接口的**恶意**策略部分的**常规下**。这些功能默认情况下中的每一个禁用并且应该只启用使最残损的威胁无效。

- 电线的歹徒-如果恶意设备识别附加到有线网络，则自动地被放置在遏制下。
- 使用我们的SSID -如果恶意设备使用是相同的象在控制器配置的那的一SSID，自动地包含。在造成损伤前，此功能打算寻址蜂蜜攻击。
- 非法AP的有效客户端-如果发现在ACS列出的客户端用恶意设备关联，遏制启动只有该客户端，防止它关联到所有非托管型AP。
- 临时非法AP -如果临时网络是已发现，自动地包含。

恶意遏制警告

- 由于遏制花管理的AP无线电时间的部分发送解除验证帧，对数据和语音客户端的性能负面影响20%。对于数据客户端，影响是减少的吞吐量。对于语音客户端，遏制能导致中断进入会话和减少的语音质量。
- 遏制能有法定含意，当启动相邻的网络。保证恶意设备在您的网络内并且形成安全风险，在您启动遏制前。

交换机端口关闭

使用SPT，一旦交换机端口跟踪，有选项使WCS的该端口无效。管理员必须手工执行此练习。如果歹徒从网络，物理的删除选项是可用通过WCS启用交换机端口。

配置恶意管理

配置恶意检测

默认情况下恶意检测在控制器启用。

要查找在使用图形界面的控制器的恶意详细信息，请去**监视器>歹徒**。

在此页，歹徒的另外分类是可用的：

- **友好AP** –被标记作为友好由管理员的Aps。
- **有恶意的AP** –识别如有恶意使用RLDP或恶意探测器AP的Aps。
- **未保密的AP** –默认情况下恶意AP将显示作为在控制器的未保密的列表。
- **恶意客户端**–客户端连接欺诈AP。
- **临时歹徒**–临时恶意客户端。
- **非法AP忽略列表**–通过WCS列出的Aps。

注意： 如果WLC和自治AP由同样WCS管理， WLC自动地列出在非法AP忽略列表的此自治AP。没有在WLC要求的更多的配置启用此功能。

从CLI：

```
(Cisco Controller) >show rogue ap summary

Rogue on wire Auto-Contain....................... Disabled
Rogue using our SSID Auto-Contain................ Disabled
Valid client on rogue AP Auto-Contain............ Disabled
Rogue AP timeout................................. 1200

MAC Address        Classification     # APs # Clients Last Heard
-----------------  ------------------ ----- --------- ----------------------
00:14:1b:5b:1f:90  Unclassified       1     0         Thu Jun 10 19:04:51 2010
00:14:1b:5b:1f:91  Unclassified       1     0         Thu Jun 10 18:58:51 2010
00:14:1b:5b:1f:92  Unclassified       1     0         Thu Jun 10 18:49:50 2010
00:14:1b:5b:1f:93  Unclassified       1     0         Thu Jun 10 18:55:51 2010
00:14:1b:5b:1f:96  Unclassified       1     0         Thu Jun 10 18:58:51 2010
00:17:df:a9:08:00  Unclassified       1     0         Thu Jun 10 18:49:50 2010
00:17:df:a9:08:10  Unclassified       1     0         Thu Jun 10 18:55:51 2010
00:17:df:a9:08:11  Unclassified       1     0         Thu Jun 10 19:04:51 2010
00:17:df:a9:08:12  Unclassified       1     0         Thu Jun 10 18:49:50 2010
00:17:df:a9:08:16  Unclassified       1     0         Thu Jun 10 19:04:51 2010
```

点击一个特定的恶意条目为了获得那的详细信息歹徒。

从CLI：

```
(Cisco Controller) >show rogue ap detailed 00:14:1b:5b:1f:90

Rogue BSSID..................................... 00:14:1b:5b:1f:90
Is Rogue on Wired Network....................... No
Classification.................................. Unclassified
Manual Contained................................ No
State........................................... Alert
First Time Rogue was Reported................... Thu Jun 10 18:37:50 2010
Last Time Rogue was Reported.................... Thu Jun 10 19:04:51 2010
Reported By
    AP 1
        MAC Address............................. 00:24:97:8a:09:30
        Name.................................... AP_5500
        Radio Type.............................. 802.11g
        SSID.................................... doob
        Channel................................. 6
        RSSI.................................... -51 dBm
        SNR..................................... 27 dB
        Encryption.............................. Disabled
        ShortPreamble........................... Enabled
        WPA Support............................. Disabled
        Last reported by this AP................ Thu Jun 10 19:04:51 2010
```

配置恶意检测的信道扫描

对于本地/Hreap模式/监控模式AP有选项在允许用户选择信道为歹徒被扫描的RRM配置下。根据设置，AP扫描所有信道/国家channel/DCA信道歹徒的。

从GUI要配置此，请去**无线> 802.11a/802.11b > RRM >**General。

从CLI：

```
(Cisco Controller) >config  advanced 802.11a monitor channel-list ?

all             Monitor all channels
country         Monitor channels used in configured country code
```

```
dca             Monitor channels used by automatic channel assignment
```
要配置这些选项，请去**安全>无线保护策略>歹徒策略>**General。

1. 更改恶意AP的超时。
2. 启动临时恶意网络的检测。

从CLI ：

```
(Cisco Controller) >config rogue ap timeout ?

<seconds>      The number of seconds<240 - 3600> before rogue entries are flushed

(Cisco Controller) >config rogue adhoc enable/disable
```

配置恶意分类

请手工分类非法AP

分类非法AP如友好，有恶意或者未保密，去**监视器>歹徒>未保密的AP**和点击特定的非法AP名称。从下拉列表选择选项。

从CLI ：

```
(Cisco Controller) >config rogue ap ?

classify       Configures rogue access points classification.
friendly       Configures friendly AP devices.
rldp           Configures Rogue Location Discovery Protocol.
ssid           Configures policy for rogue APs advertsing our SSID.
timeout        Configures the expiration time for rogue entries, in seconds.
valid-client   Configures policy for valid clients using rogue APs.
```
从恶意列表要手工删除一个恶意条目，去**监视器>歹徒>未保密的AP**，和点击**删除**。

要配置非法AP作为友好AP，请去**安全>无线保护策略>歹徒策略>友好歹徒**并且添加恶意MAC地址。

已添加友好恶意条目可以从**监视器>**验证**欺诈>友好恶意**页。

配置歹徒探测器AP

使用GUI，要配置AP作为一台恶意探测器，请去**无线>所有AP**。选择AP名称并且更改AP模式。

从CLI ：

```
(Cisco Controller) >config ap mode rogue AP_Managed

Changing the AP's mode will cause the AP to reboot.
Are you sure you want to continue? (y/n) y
```
配置歹徒探测器AP的Switchport

```
(Cisco Controller) >config ap mode rogue AP_Managed

Changing the AP's mode will cause the AP to reboot.
Are you sure you want to continue? (y/n) y
```
注意： 本地VLAN在此配置方面是有IP连通性对WLC的一个。

配置RLDP

要配置在控制器的GUI的RLDP，请去**安全>无线保护策略>歹徒策略>**General。

监控模式AP –允许在监控模式的仅AP参加RLDP。

所有AP –本地/Hreap/监控模式AP参加RLDP进程。

已禁用– RLDP没有自动地被触发。然而，用户能为特定MAC地址手工触发RLDP通过CLI。

注意： 如果他们两个检测在-85dbm RSSI上的一个特定歹徒监控模式AP将获得在本地/Hreap AP的首选执行的RLDP的。

从CLI：

```
(Cisco Controller) >config rogue ap rldp enable ?

alarm-only     Enables RLDP and alarm if rogue is detected
auto-contain   Enables RLDP, alarm and auto-contain if rogue is detected.

(Cisco Controller) >config rogue ap rldp enable alarm-only ?

monitor-ap-only Perform RLDP only on monitor AP

RLDP scheduling and triggering manually is configurable only through Command
    prompt

To Initiate RLDP manually:

(Cisco Controller) >config rogue ap rldp initiate ?

<MAC addr>     Enter the MAC address of the rogue AP (e.g. 01:01:01:01:01:01).
For Scheduling RLDP

Note: RLDP scheduling and option to configure RLDP retries are two options
    introduced in 7.0 through CLI

RLDP Scheduling :

(Cisco Controller) >config rogue ap rldp schedule ?

add            Enter the days when RLDP scheduling to be done.
delete         Enter the days when RLDP scheduling needs to be deleted.
enable         Configure to enable RLDP scheduling.
disable        Configure to disable RLDP scheduling.


(Cisco Controller) >config rogue ap rldp schedule add ?

mon            Configure Monday for RLDP scheduling.
tue            Configure Tuesday for RLDP scheduling.
wed            Configure Wednesday for RLDP scheduling.
thu            Configure Thursday for RLDP scheduling.
fri            Configure Friday for RLDP scheduling.
sat            Configure Saturday for RLDP scheduling.
sun            Configure Sunday for RLDP scheduling.



RLDP retries can be configured using the command

(Cisco Controller) >config rogue ap rldp retries ?
```

```
<count>        Enter the no.of times(1 - 5) RLDP to be tried per Rogue AP.
```

要配置恶意客户端的AAA验证，请去**安全>无线保护策略>歹徒策略>**General。

启用此选项确保恶意client/AP地址验证与在分类它前的AAA服务器如有恶意。

从CLI：

```
(Cisco Controller) >config rogue client aaa ?

disable        Disables use of AAA/local database to detect valid mac addresses.
enable         Enables use of AAA/local database to detect valid mac addresses.
```

要验证一个特定的恶意客户端是一个有线的歹徒，有选项检查该特定歹徒的可接通性从控制器的(如果控制器能检测恶意客户端IP地址)。此选项在恶意客户端的详细信息页可以访问并且通过图形界面是仅可用的。

要配置交换机端口跟踪，参考本文歹徒管理白皮书(仅限注册用户)。

配置恶意缓解

配置手工的遏制：

为了手工包含非法AP，请去**监视器>欺诈>未保密。**

从CLI：

```
(Cisco Controller) >config rogue client ?

aaa            Configures to validate if a rogue client is a valid client using
                   AAA/local database.
alert          Configure the rogue client to the alarm state.
contain        Start containing a rogue client.

(Cisco Controller) >config rogue client contain 01:22:33:44:55:66 ?

<num of APs>   Enter the maximum number of Cisco APs to actively contain the
                   rogue client [1-4].
```

注意： 使用1-4 AP，一个特定的歹徒可以包含。默认情况下，控制器使用一个AP包含客户端。如果两AP能检测一个特定的歹徒，不管AP模式，与最高的RSSI的AP包含客户端。

要配置自动遏制，请去**安全>无线保护策略>歹徒策略>**General，并且启用您的网络的所有可适用的选项。

从CLI：

```
(Cisco Controller) >config rogue adhoc ?

alert          Stop Auto-Containment, generate a trap upon detection of the
                   adhoc rogue.
auto-contain   Automatically containing adhoc rogue.
contain        Start containing adhoc rogue.
disable        Disable detection and reporting of Ad-Hoc rogues.
enable         Enable detection and reporting of Ad-Hoc rogues.
external       Acknowledge presence of a adhoc rogue.

(Cisco Controller) >config rogue adhoc auto-contain ?
```

```
(Cisco Controller) >config rogue adhoc auto-contain
 Warning! Using this feature may have legal consequences
        Do you want to continue(y/n) :y
```

故障排除

如果歹徒没有检测：

- 验证使用此命令，歹徒检测在AP启用。默认情况下，恶意检测在AP启用。(Cisco_Controller) >show ap config general Managed_AP

```
Cisco AP Identifier.............................. 2
Cisco AP Name.................................... Managed_AP
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 2
MAC Address...................................... 00:1d:a1:cc:0e:9e
IP Address Configuration......................... DHCP
IP Address....................................... 10.8.99.104
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.8.99.1
CAPWAP Path MTU.................................. 1485
Telnet State..................................... Enabled
Ssh State........................................ Disabled
Cisco AP Location................................ india-banaglore
Cisco AP Group Name.............................. default-group
Primary Cisco Switch Name........................ Cisco_e9:d9:23
Primary Cisco Switch IP Address.................. 10.44.81.20
Secondary Cisco Switch Name.....................
Secondary Cisco Switch IP Address................ Not Configured
Tertiary Cisco Switch Name.....................
Tertiary Cisco Switch IP Address................. Not Configured
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Local
Public Safety ................................... Disabled
AP SubMode ...................................... Not Configured
Remote AP Debug ................................. Disabled
Logging trap severity level ..................... informational
Logging syslog facility ......................... kern
S/W  Version .................................... 7.0.98.0
Boot  Version ................................... 12.3.7.1
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 209
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Enabled
PoE Power Injector MAC Addr...................... Override
Power Type/Mode.................................. Power injector / Normal mode
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1242AG-A-K9
AP Image......................................... C1240-K9W8-M
IOS Version...................................... 12.4(23c)JA
Reset Button..................................... Enabled
AP Serial Number................................. FTX1137B22V
AP Certificate Type.............................. Manufacture Installed
AP User Mode..................................... AUTOMATIC
AP User Name..................................... Not Configured
AP Dot1x User Mode............................... GLOBAL
AP Dot1x User Name............................... Cisco12
```

```
    Cisco AP system logging host..................... 255.255.255.255
    AP Up Time....................................... 13 days, 15 h 01 m 33 s
    AP LWAPP Up Time................................. 13 days, 15 h 00 m 40 s
    Join Date and Time............................... Tue Jun  1 10:36:38 2010

    Join Taken Time.................................. 0 days, 00 h 00 m 52 s
    Ethernet Port Duplex............................. Auto
    Ethernet Port Speed.............................. Auto
    AP Link Latency.................................. Enabled
     Current Delay................................... 0 ms
     Maximum Delay................................... 56 ms
     Minimum Delay................................... 2 ms
     Last updated (based on AP Up Time).............. 13 days, 15 h 00 m 44 s
    Rogue Detection.................................. Enabled
    AP TCP MSS Adjust................................ Disabled
```

使用此命令，恶意检测在AP可以启用：`(Cisco Controller) >`**`config rogue detection enable ?`**

```
all                   Applies the configuration to all connected APs.
<Cisco AP>     Enter the name of the Cisco AP.
```

- 本地传送方式AP根据配置扫描仅国家channels/DCA信道。如果歹徒是在其他信道，控制器不能识别歹徒，如果没有在网络的监控模式AP。发出此命令以进行验证：`(Cisco Controller) >`**`show advanced 802.11a monitor`**

```
    Default 802.11a AP monitoring
      802.11a Monitor Mode........................... enable
      802.11a Monitor Mode for Mesh AP Backhaul...... disable
      802.11a Monitor Channels....................... Country channels
      802.11a AP Coverage Interval................... 180 seconds
      802.11a AP Load Interval....................... 60 seconds
      802.11a AP Noise Interval...................... 180 seconds
      802.11a AP Signal Strength Interval............ 60 seconds
```

- 非法AP可能不广播SSID。
- 确保恶意AP的MAC地址没有被添加在友好恶意列表或白色列出的通过WCS。
- 从非法AP的信标可能不是可及的对检测歹徒的AP。使用接近AP检测的歹徒的一个嗅探器这可以通过捕获数据包验证。
- 本地传送方式AP可能花费9分钟检测歹徒(3个周期180x3)。
- 思科AP不能检测频率的歹徒类似公共安全信道(4.9千兆赫)。
- 思科AP不能检测工作在FHSS (跳频扩频)的歹徒。

有用的调试

```
(Cisco Controller) >show advanced 802.11a monitor

Default 802.11a AP monitoring
  802.11a Monitor Mode........................... enable
  802.11a Monitor Mode for Mesh AP Backhaul...... disable
  802.11a Monitor Channels....................... Country channels
  802.11a AP Coverage Interval................... 180 seconds
  802.11a AP Load Interval....................... 60 seconds
  802.11a AP Noise Interval...................... 180 seconds
  802.11a AP Signal Strength Interval............ 60 seconds
```

`debug dot11 rogue enable`

```
(Cisco_Controller) >*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12
    Looking for Rogue 00:27:0d:8d:14:12 in known AP table
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Rogue AP 00:27:0d:8d:14:12
    is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Change state from 0 to 1
    for rogue AP 00:27:0d:8d:14:12
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 rg change state Rogue AP:
    00:27:0d:8d:14:12
```

```
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 New RSSI report from AP
    00:1b:0d:d4:54:20  rssi -74, snr -9 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg send new rssi -74
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Updated AP report
    00:1b:0d:d4:54:20  rssi -74, snr -9
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg new Rogue AP:
    00:27:0d:8d:14:12

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Found Rogue AP:
    00:24:97:2d:bf:90 on slot 0

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Added Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Looking for Rogue
    00:24:97:2d:bf:90 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Rogue AP 00:24:97:2d:bf:90
    is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Change state from 0 to 1
    for rogue AP 00:24:97:2d:bf:90
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg change state Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 New RSSI report from AP
    00:1b:0d:d4:54:20  rssi -56, snr 34 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg send new rssi -56
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Updated AP report
    00:1b:0d:d4:54:20  rssi -56, snr 34
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg new Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Found Rogue AP:
    9c:af:ca:0f:bd:40 on slot 0

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Added Rogue AP:
    9c:af:ca:0f:bd:40

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Looking for Rogue
    9c:af:ca:0f:bd:40 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Rogue AP 9c:af:ca:0f:bd:40
    is not found eithe*apfRogueTask: Jun 15 01:45:09.011: 00:25:45:a2:e1:62
    Updated AP report 00:1b:0d:d4:54:20  rssi -73, snr 24
*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 rg new Rogue AP:
    00:25:45:a2:e1:62

*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Found Rogue AP:
    00:24:c4:ad:c0:40 on slot 0

*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Added Rogue AP:
    00:24:c4:ad:c0:40
```

预计陷阱日志

一旦歹徒检测

debug dot11 rogue enable

```
(Cisco_Controller) >*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12
    Looking for Rogue 00:27:0d:8d:14:12 in known AP table
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Rogue AP 00:27:0d:8d:14:12
    is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Change state from 0 to 1
    for rogue AP 00:27:0d:8d:14:12
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 rg change state Rogue AP:
    00:27:0d:8d:14:12

*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 New RSSI report from AP
    00:1b:0d:d4:54:20  rssi -74, snr -9 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg send new rssi -74
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Updated AP report
    00:1b:0d:d4:54:20  rssi -74, snr -9
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg new Rogue AP:
    00:27:0d:8d:14:12

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Found Rogue AP:
    00:24:97:2d:bf:90 on slot 0

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Added Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Looking for Rogue
    00:24:97:2d:bf:90 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Rogue AP 00:24:97:2d:bf:90
    is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Change state from 0 to 1
    for rogue AP 00:24:97:2d:bf:90
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg change state Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 New RSSI report from AP
    00:1b:0d:d4:54:20  rssi -56, snr 34 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg send new rssi -56
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Updated AP report
    00:1b:0d:d4:54:20  rssi -56, snr 34
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg new Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Found Rogue AP:
    9c:af:ca:0f:bd:40 on slot 0

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Added Rogue AP:
    9c:af:ca:0f:bd:40

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Looking for Rogue
    9c:af:ca:0f:bd:40 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Rogue AP 9c:af:ca:0f:bd:40
    is not found eithe*apfRogueTask: Jun 15 01:45:09.011: 00:25:45:a2:e1:62
    Updated AP report 00:1b:0d:d4:54:20  rssi -73, snr 24
*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 rg new Rogue AP:
    00:25:45:a2:e1:62

*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Found Rogue AP:
    00:24:c4:ad:c0:40 on slot 0
```

```
*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Added Rogue AP:
    00:24:c4:ad:c0:40
```

一旦一个恶意条目从恶意删除请列出

debug dot11 rogue enable

```
(Cisco_Controller) >*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12
    Looking for Rogue 00:27:0d:8d:14:12 in known AP table
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Rogue AP 00:27:0d:8d:14:12
    is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Change state from 0 to 1
    for rogue AP 00:27:0d:8d:14:12
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 rg change state Rogue AP:
    00:27:0d:8d:14:12

*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 New RSSI report from AP
    00:1b:0d:d4:54:20  rssi -74, snr -9 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg send new rssi -74
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Updated AP report
    00:1b:0d:d4:54:20  rssi -74, snr -9
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg new Rogue AP:
    00:27:0d:8d:14:12

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Found Rogue AP:
    00:24:97:2d:bf:90 on slot 0

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Added Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Looking for Rogue
    00:24:97:2d:bf:90 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Rogue AP 00:24:97:2d:bf:90
    is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Change state from 0 to 1
    for rogue AP 00:24:97:2d:bf:90
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg change state Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 New RSSI report from AP
    00:1b:0d:d4:54:20  rssi -56, snr 34 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg send new rssi -56
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Updated AP report
    00:1b:0d:d4:54:20  rssi -56, snr 34
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg new Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Found Rogue AP:
    9c:af:ca:0f:bd:40 on slot 0

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Added Rogue AP:
    9c:af:ca:0f:bd:40

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Looking for Rogue
    9c:af:ca:0f:bd:40 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Rogue AP 9c:af:ca:0f:bd:40
    is not found eithe*apfRogueTask: Jun 15 01:45:09.011: 00:25:45:a2:e1:62
```

```
    Updated AP report 00:1b:0d:d4:54:20  rssi -73, snr 24
*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 rg new Rogue AP:
    00:25:45:a2:e1:62

*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Found Rogue AP:
    00:24:c4:ad:c0:40 on slot 0

*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Added Rogue AP:
    00:24:c4:ad:c0:40
```

建议

1. 如果怀疑您的网络的，潜在的歹徒请配置扫描对所有信道的信道
2. 根据有线网络的布局，恶意探测器AP的编号和位置能从一个变化每个楼层到一个每建立。有在建立的每个楼层的至少一个恶意探测器AP是可行的。由于歹徒探测器AP要求中继对应该是受监视的所有第2层网络广播域，放置依靠网络的逻辑布局。

如果歹徒没获得分类

- 验证恶意规则适当地配置。
- 如果歹徒是在DFS信道， RLDP不工作。
- RLDP工作，只有当歹徒的WLAN是开放的，并且DHCP是可用的。
- 如果本地传送方式AP服务DFS信道的客户端，不会参加RLDP进程。

有用的调试

```
(Cisco Controller) > debug dot11 rogue rule enable
(Cisco Controller) > debug dot11 rldp enable

Received Request to detect rogue: 00:1A:1E:85:21:B0
00:1a:1e:85:21:b0 found closest monitor AP 00:17:df:a7:20:d0slot =1 channel = 44
Found RAD: 0x158f1ea0, slotId = 1
rldp started association, attempt 1
Successfully associated with rogue: 00:1A:1E:85:21:B0

!--- ASSOCIATING TO ROGUE AP Starting dhcp 00:1a:1e:85:21:b0 RLDP DHCP SELECTING for rogue
00:1a:1e:85:21:b0 00:1a:1e:85:21:b0 Initializing RLDP DHCP for rogue 00:1a:1e:85:21:b0
.00:1a:1e:85:21:b0 RLDP DHCPSTATE_INIT for rogue 00:1a:1e:85:21:b0 00:1a:1e:85:21:b0 RLDP
DHCPSTATE_REQUESTING sending for rogue 00:1a:1e:85:21:b0 00:1a:1e:85:21:b0 Sending DHCP packet
through rogue AP 00:1a:1e:85:21:b0 00:1a:1e:85:21:b0 RLDP DHCP REQUEST RECV for rogue
00:1a:1e:85:21:b0 00:1a:1e:85:21:b0 RLDP DHCP REQUEST received for rogue 00:1a:1e:85:21:b0
00:1a:1e:85:21:b0 RLDP DHCP BOUND state for rogue 00:1a:1e:85:21:b0 Returning IP 172.20.226.246,
netmask 255.255.255.192, gw 172.20.226.193 !--- GETTING IP FROM ROGUE Found Gateway MacAddr:
00:1D:70:F0:D4:C1 Send ARLDP to 172.20.226.198 (00:1D:70:F0:D4:C1) (gateway) Sending ARLDP
packet to 00:1d:70:f0:d4:c1 from 00:17:df:a7:20:de Send ARLDP to 172.20.226.197
(00:1F:9E:9B:29:80) Sending ARLDP packet to 00:1f:9e:9b:29:80 from 00:17:df:a7:20:de Send ARLDP
to 0.0.0.0 (00:1D:70:F0:D4:C1) (gateway) Sending ARLDP packet to 00:1d:70:f0:d4:c1 from
00:17:df:a7:20:de !--- SENDING ARLDP PACKET Received 32 byte ARLDP message from:
172.20.226.24642 Packet Dump: sourceIp: 172.20.226.246 destIp: 172.20.226.197 Rogue Mac:
00:1A:1E:85:21:B0 !--- RECEIVING ARLDP PACKET security: 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00
```

建议

1. 手工启动RLDP在可疑恶意条目。
2. 周期地日程RLDP。
3. 如果认识恶意条目，请添加他们在友好列表或启用与AAA的验证并且确保条目在那里在AAA数据库的已知客户端。

4. RLDP在本地或监控模式AP可以部署。对于多数可扩展部署和消除在客户端服务的所有影响，在监控模式AP应该部署RLDP，当可能。然而，此建议要求监控模式AP覆盖配置有一个典型的比率作为每5的本地传送方式AP 1个监控模式AP。在可适应wIPS监控模式的AP可以也是杠杆作用的为此任务。

恶意探测器AP

在一台恶意探测器的恶意条目能被看到使用此in命令AP控制台。对于有线的歹徒，标志将设置。

```
Rogue_Detector_5500#show capwap rm rogue detector
 CAPWAP Rogue Detector Mode
  Current Rogue Table:
  Rogue hindex = 0: MAC 0023.ebdc.1ac6, flag = 0, unusedCount = 1
  Rogue hindex = 2: MAC 0023.04c9.72b9, flag = 1, unusedCount = 1

!--- once the flag is set, rogue is detected on wire Rogue hindex = 2: MAC 0023.ebdc.1ac4, flag
= 0, unusedCount = 1 Rogue hindex = 3: MAC 0026.cb4d.6e20, flag = 0, unusedCount = 1 Rogue
hindex = 4: MAC 0026.cb9f.841f, flag = 0, unusedCount = 1 Rogue hindex = 4: MAC 0023.04c9.72bf,
flag = 0, unusedCount = 1 Rogue hindex = 4: MAC 0023.ebdc.1ac2, flag = 0, unusedCount = 1 Rogue
hindex = 4: MAC 001c.0f80.d450, flag = 0, unusedCount = 1 Rogue hindex = 6: MAC 0023.04c9.72bd,
flag = 0, unusedCount = 1
```

有用的调试In命令AP控制台

```
Rogue_Detector#debug capwap rm rogue detector

*Jun 18 08:37:59.747: ROGUE_DET: Received a rogue table update of length 170
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac4
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac5
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1aca
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acb
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acc
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acd
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acf
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0024.1431.e9ef
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0024.148a.ca2b
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2d
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2f
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3570
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3574
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357b
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357c
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357d
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357f
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3dcd
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff0
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff2
*Jun 18 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4aec
*Jun 18 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4b77
*Jun 18 08:37:59.774: ROGUE_DET: Flushing rogue entry 0040.96b9.4794
*Jun 18 08:37:59.774: ROGUE_DET: Flushing rogue entry 0022.0c97.af80
*Jun 18 08:37:59.775: ROGUE_DET: Flushing rogue entry 0024.9789.5710
*Jun 18 08:38:19.325: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 18 08:38:19.325: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
*Jun 18 08:39:19.323: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 18 08:39:19.324: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
```

如果恶意遏制不发生：

1. 本地/Hreap模式AP能每次包含3个设备每无线电，并且监控模式AP能包含每无线电6个设备。结果，请确保AP已经包含允许的设备最大。在此方案中，客户端在遏制待定状态。

2. 验证自动遏制规则。

预计陷阱日志

```
Rogue_Detector#debug capwap rm rogue detector

*Jun 18 08:37:59.747: ROGUE_DET: Received a rogue table update of length 170
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac4
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac5
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1aca
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acb
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acc
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acd
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acf
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0024.1431.e9ef
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0024.148a.ca2b
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2d
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2f
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3570
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3574
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357b
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357c
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357d
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357f
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3dcd
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff0
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff2
*Jun 18 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4aec
*Jun 18 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4b77
*Jun 18 08:37:59.774: ROGUE_DET: Flushing rogue entry 0040.96b9.4794
*Jun 18 08:37:59.774: ROGUE_DET: Flushing rogue entry 0022.0c97.af80
*Jun 18 08:37:59.775: ROGUE_DET: Flushing rogue entry 0024.9789.5710
*Jun 18 08:38:19.325: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 18 08:38:19.325: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
*Jun 18 08:39:19.323: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 18 08:39:19.324: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
```

结论

Cisco 集中式控制器解决方案中的恶意检测和遏制是业内最有效和干扰度最低的方法。网络管理员可以灵活调整方案，以适应任何网络要求。

相关信息

- 在无线局域网控制器(WLC)和无线控制系统(WCS)的基于规则的恶意分类
- 统一无线网络的恶意检测
- 恶意管理白皮书(仅限注册用户)
- Cisco无线LAN控制器配置指南，版本7.0
- 技术支持和文档 - Cisco Systems