统一无线网络的恶意检测

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，未授权的无线网络却存在其他的安全层问题。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，若员工将自己的 Cisco 接入点 (AP) 带入受到良好保护的无线或有线基础架构，并且允许未经授权的用户访问此安全网络，这样很容易对安全网络造成危害。

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 统一网络体系结构提供两种恶意程序检测方法，可实现全面的恶意程序识别和遏制解决方案，无需高额成本和难以证明的覆盖网络和工具。

功能概述

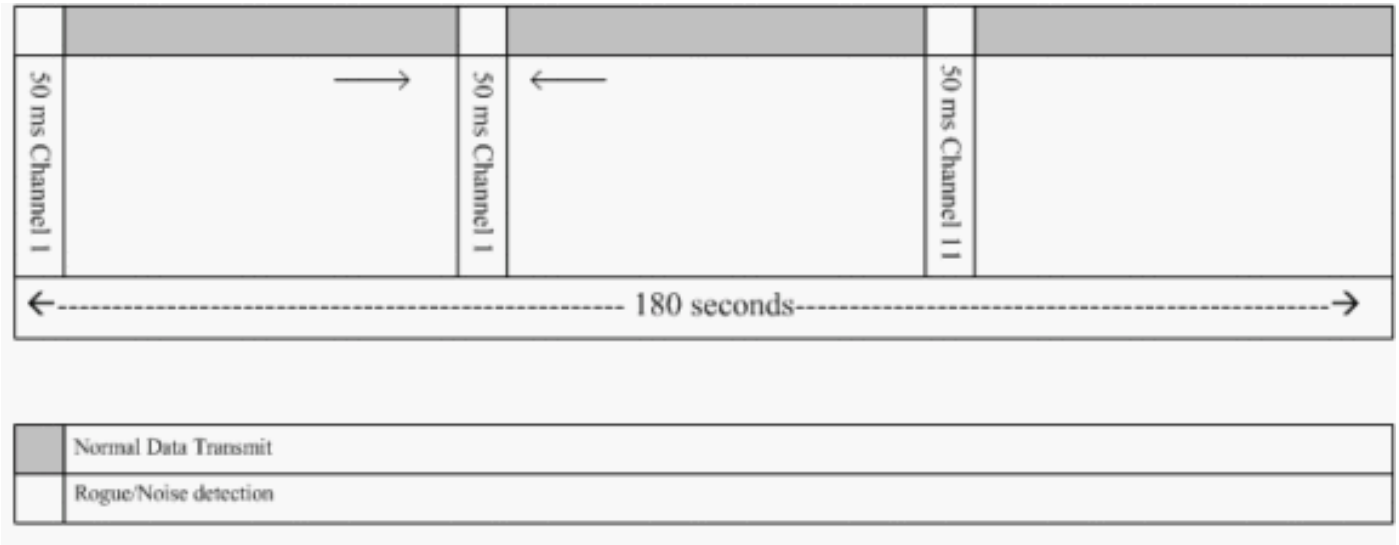
恶意程序检测不受任何法规限制，操作时也无需遵守任何法律要求。然而，恶意程序遏制通常会带来法律问题，如果让其自动操作，则使基础架构提供商处于比较尴尬的境地。Cisco 对此类问题非常敏感，所以提供了以下解决方案。轻量AP注册到控制器后，会在其所有信标/探测响应帧中嵌入**特定于控制器上**配置的RF组的身份验证信息元素(IE)。当轻量 AP 侦听到来自另一 AP 的没有此 **IE 或具有错误 IE** 的信标/信号响应帧时，轻量 AP 会将此 AP 作为恶意程序报告，将 BSSID 记录在一个恶意程序表中，然后把此表发送到控制器。下文详细介绍了两个方法，即恶意程序位置发现协议 (RLDP) 和被动操作；请参阅[确定活动的恶意程序部分。](#)

基础架构恶意程序发现

在活动的无线环境中发现恶意程序的代价可能十分昂贵。此进程请求服务中（或本地模式）的 AP 停止服务，监听噪声然后进行恶意程序检测。网络管理员配置扫描信道，并配置对所有站点进行扫描的时间段。AP 监听 50 毫秒以检测恶意客户端信标，然后回到已配置的信道以再次为客户端提供服务。这种活动扫描，与邻接消息相结合，可识别恶意 AP 和有效且从属于网络的 AP。为配置扫描

信道和扫描时间段，请浏览 **Wireless > 802.11b/g Network (“b/g”或“a”，根据网络要求），然后在浏览器窗口右上角选择 Auto RF 按钮。**

您可以向下滚动到 **Noise/Interference/Rogue Monitoring Channels 以配置要进行恶意程序和噪音扫描的信道。**可用的选择是：所有信道（1 至 14），国家/地区信道（1 至 11）或动态信道关联 (DCA) 信道（默认为 1、6 和 11）。 可在同一窗口中配置扫描这些信道的时间段，先是**监控间隔（60 到 3600 秒），然后是噪音测量间隔。**默认情况下，信道外的噪声和恶意程序的监听间隔是 180 秒。这意味着每个信道每 180 秒扫描一次。以下示例对每 180 秒扫描一次的 DCA 信道进行说明：



如图所示，配置的要扫描的信道数量巨大，但扫描间隔却很短，这样使得 AP 实际服务于数据客户端的时间就极少。

轻量 AP 等待以将客户端和 AP 标记为恶意程序，因为在另一个周期完成之前，这些恶意程序可能不会被另一个 AP 报告。相同的 AP 再次移动到同一个信道以监控恶意 AP、客户端以及噪声和干扰。如果检测出同样的客户端和/或 AP，它们将再次作为控制器上的恶意程序列出。控制器开始确定这些恶意程序是连接到本地网络，还是仅仅连接到相邻 AP。在任何情况下，不属于受管本地无线网络的 AP 都被认定为恶意程序。

恶意程序详细信息

轻量 AP 脱离信道 50 毫秒以监听恶意客户端，监控噪声和信道干扰。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 MAC 地址
- 恶意 AP 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)

恶意探测器接入点

您可以将 AP 当做恶意探测器使用，这样就可以将其放置于中继端口以便侦听所有有线端连接的 VLAN。它继续查找所有 VLAN 上的有线子网上的客户端。恶意探测器 AP 监听地址解析协议

(ARP) 数据包以确定由控制器发送的已标识的恶意客户端或恶意 AP 的第 2 层地址。如果找到匹配的第 2 层地址，控制器会发出将恶意 AP 或客户端认定为威胁的警报。此警报表明在有线网络上发现了恶意程序。

确定活动的恶意程序

控制器将恶意 AP 添加为恶意程序之前必须“发现”恶意 AP 两次。如果恶意 AP 没有连接到公司网络的有线网段，则不认为构成威胁。可使用多种方法确定恶意程序是否为活动状态。那些方法包括 RLDP。

恶意位置发现协议 (RLDP)

RLDP 是一种活动方法，在恶意 AP 没有配置认证（开放式认证）时使用。此模式（在默认情况下禁用）指示活动的 AP 向恶意信道移动并作为客户端连接到恶意程序。在此期间，活动的 AP 向所有连接的客户端发送解除认证消息，然后关闭无线接口。然后，它将作为客户端与恶意 AP 关联。

然后，AP 尝试从恶意 AP 获取 IP 地址并且通过恶意 AP 将包含本地 AP 和恶意连接信息的 User Datagram Protocol (UDP) 数据包（端口 6352）转发到控制器。如果控制器接收此数据包，则使用 RLDP 功能，将警报设置为通知网络管理员在有线网络上发现恶意 AP。

注意：使用**debug dot11 rldp enable命令**检查轻量AP是否关联并从欺诈AP接收DHCP地址。此命令还会显示轻量 AP 向控制器发送的 UDP 数据包。

以下示例显示轻量 AP 发送的 UDP（目标端口 6352）数据包：

```
0020 0a 01 010d 0a 01 .......(.*..... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00
00......x......... 0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

数据的前 5 个字节包含由恶意 AP 提供给本地模式 AP 的 DHCP 地址。后面的 5 个字节是控制器的 IP 地址，接下来的 6 个字节表示恶意 AP MAC 地址。然后，有 18 个字节为零。

被动操作：

当恶意 AP 有某种形式的认证（WEP 或 WPA）时使用此方法。当恶意 AP 配置了某种形式的认证时，轻量 AP 无法关联，因为其不知道恶意 AP 配置的密钥。当控制器开始向作为恶意探测器的 AP 传送恶意客户端 MAC 地址列表时，开始此进程。恶意探测器按 ARP 请求扫描所有已连接和已配置的子网，ARP 搜索匹配的第 2 层地址。如果发现匹配，控制器通知网络管理员在有线子网上发现恶意程序。

活动恶意程序遏制

一旦在有线网络上检测到恶意客户端，网络管理员可以将恶意 AP 和恶意客户端都包含在内。此方法之所以能实现是因为 802.11 解除认证数据包被发送给与恶意 AP 关联的客户端，从而使此类漏洞造成的威胁得以缓解。每次尝试将恶意 AP 包含在内的时候，将近 15% 的轻量 AP 资源被占用。所以，如果 AP 也包含在内，建议物理定位到恶意 AP，然后将其删除。

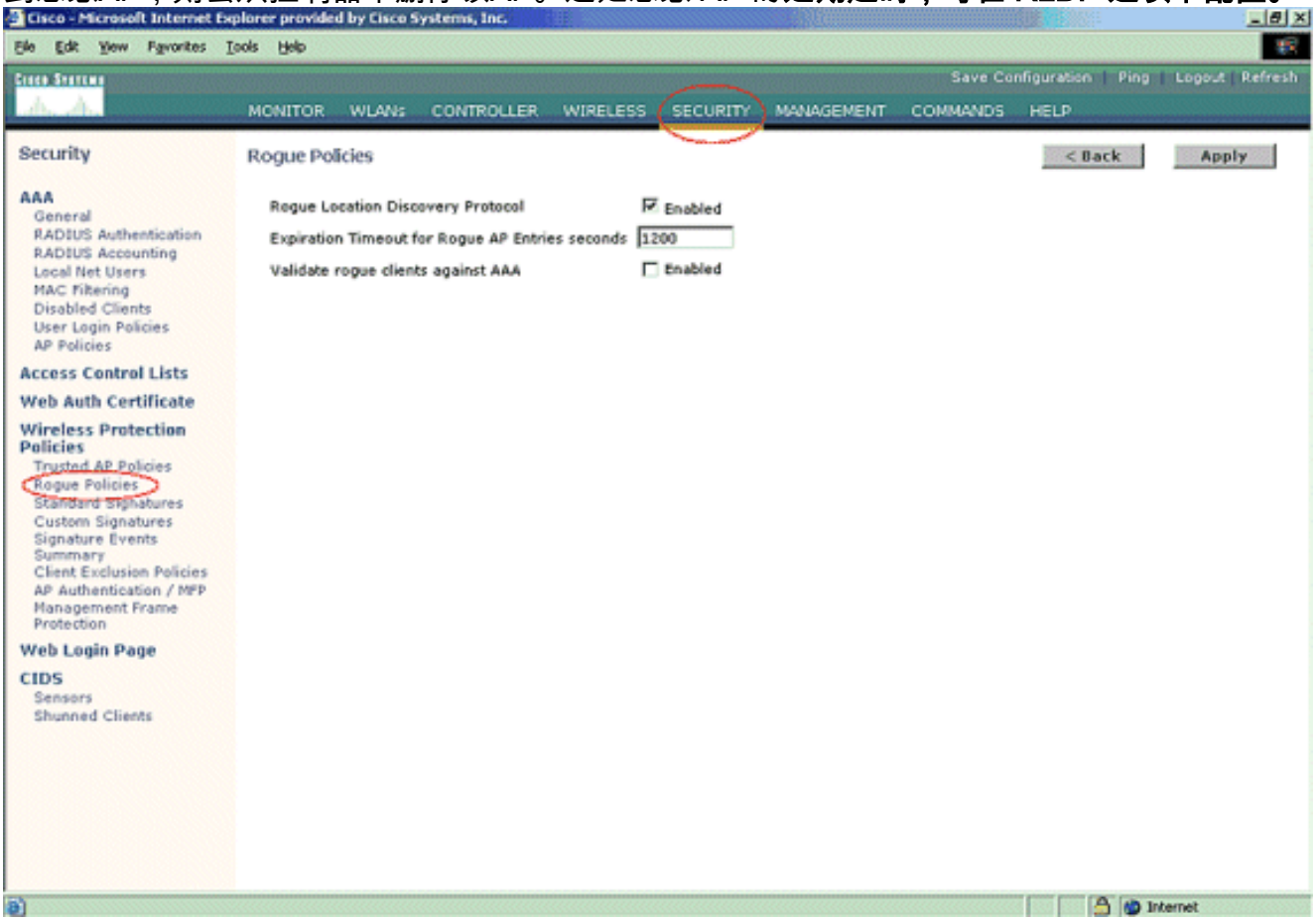
注意： 自 WLC 5.2.157.0 版起，一旦检测到恶意程序，您可以选择手动或自动包含被检测到的恶意程序。在 5.2.157.0 之前的控制器软件版本中，只能手动遏制。

恶意程序检测 – 配置步骤

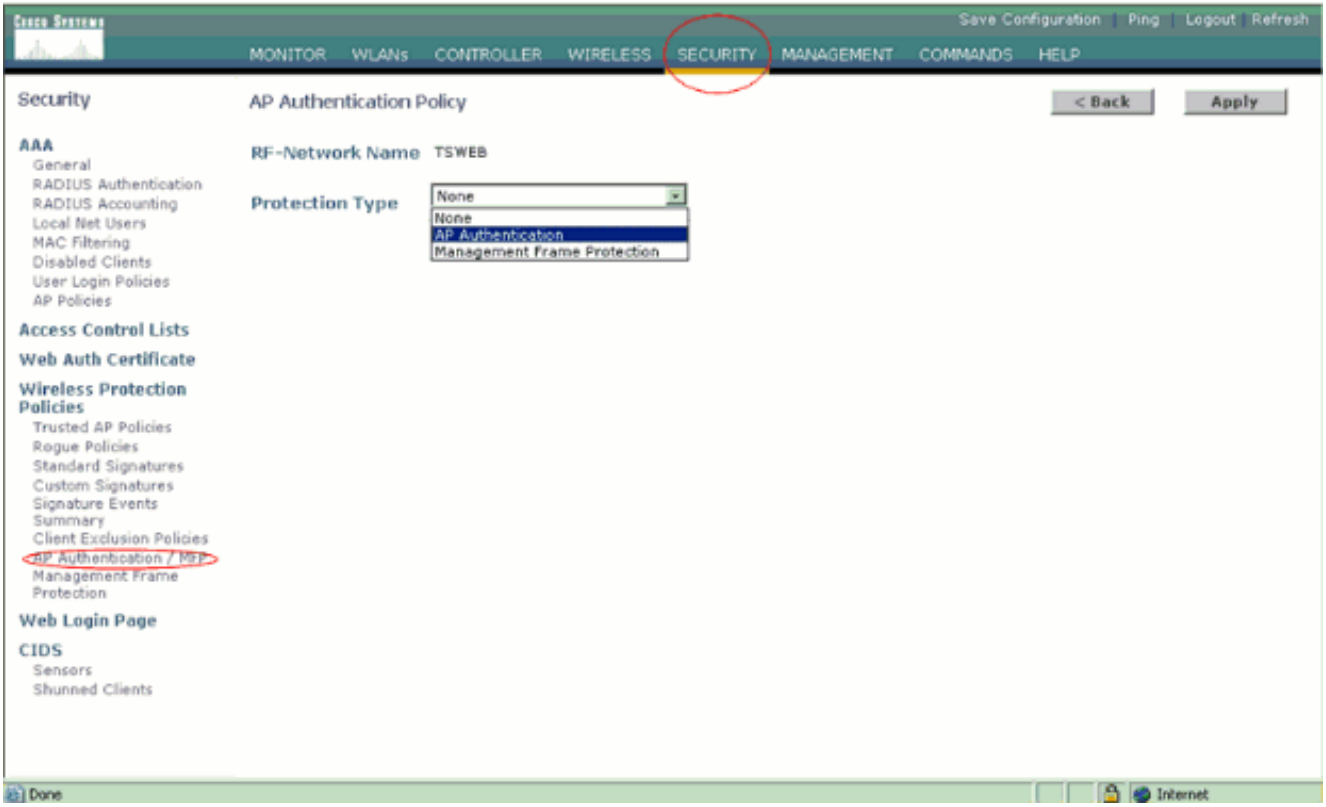
默认情况下几乎已启用所有的恶意程序检测配置，以实现最大程度的、开箱即用的网络安全。这些配置步骤假设控制器上未设置任何恶意程序检测以阐明重要的恶意程序检测信息。

为设置恶意程序检测，请完成以下步骤：

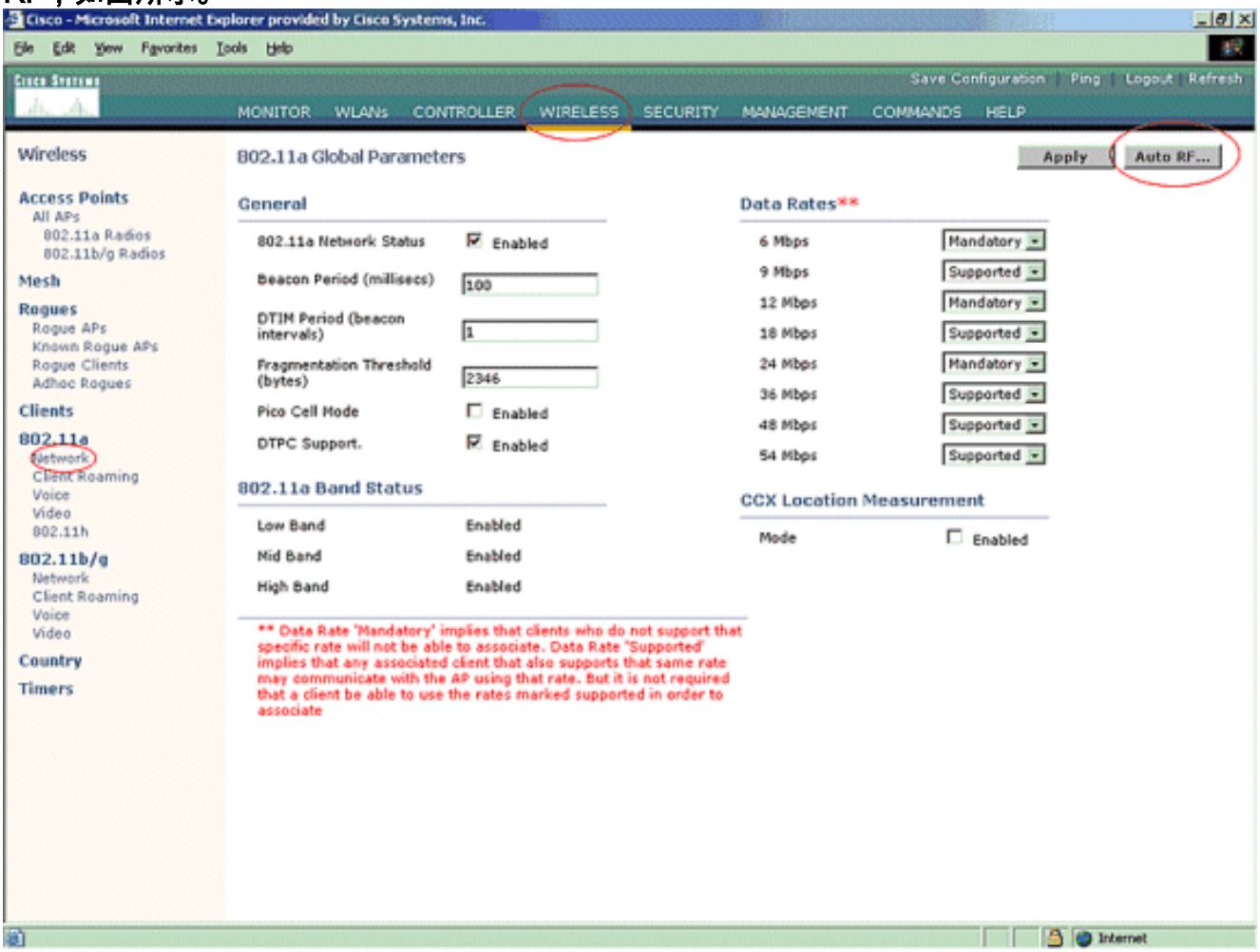
1. 确保恶意程序位置发现协议打开。为打开协议，请选择 **Security > Rogue Policies，然后单击 Rogue Location Discovery Protocol 上的 Enabled，如图所示。注意：**如果某个时间段内未听到恶意AP，则会从控制器中删除该AP。这是恶意 AP 的**过期超时，可在 RLDP 选项下配置。**



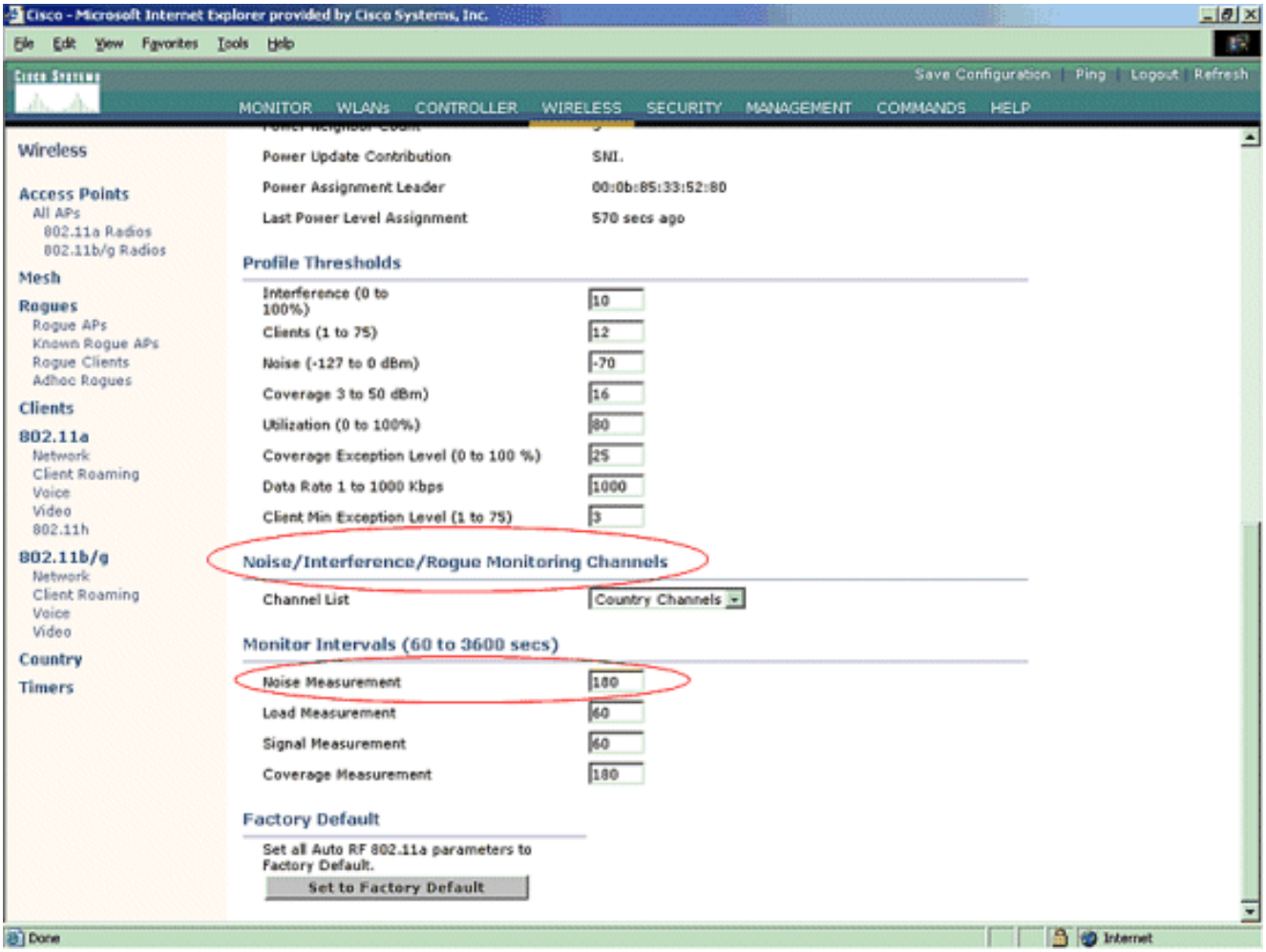
2. 这是可选步骤。此功能启用时，发送具有不同 **RF 组名的 RRM 邻接数据包的 AP 将被当做恶意程序报告。**这将有助于您学习 RF 环境。为启用此功能，请依次选择 **Security-> AP Authentication**。然后，请选择 **AP Authentication 作为保护类型，如图所示。**



3. 执行以下步骤确认信道已扫描：选择 **Wireless > 802.11a Network**，然后选择右边的 **Auto RF**，如图所示。



中在 **Auto RF** 页中，向下滚动然后选择 **Noise/Interference/Rogue Monitoring Channels**。

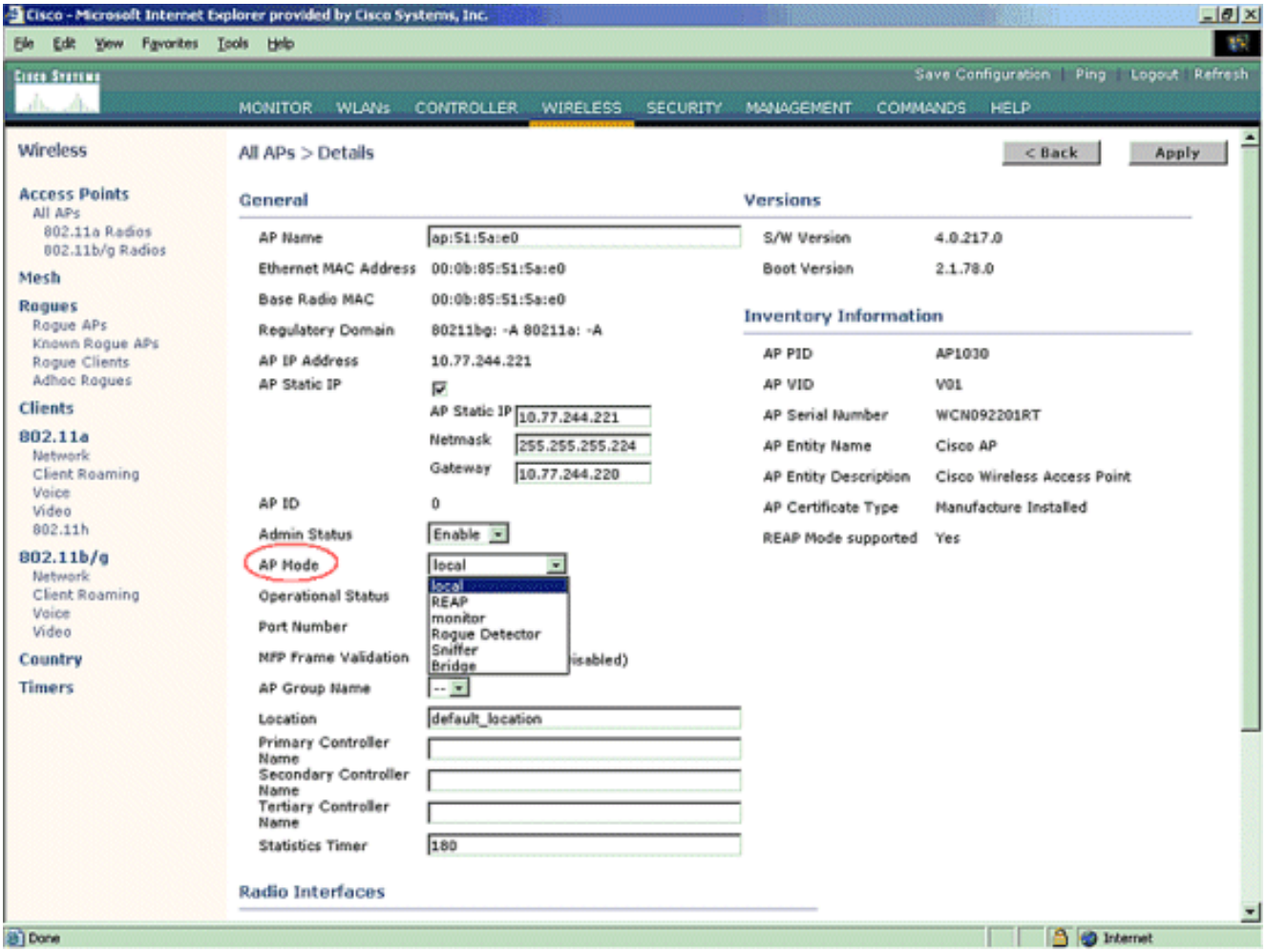


除其他控制器和 AP 功能之外，信道列表还详细说明了进行恶意程序监控扫描的信道。请参阅[轻量接入点常见问题解答了解有关轻量 AP 的更多信息，请参阅无线 LAN 控制器 (WLC) 故障排除常见问题解答了解有关无线控制器的更多信息。](#)

Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

4. 设置扫描选定信道的时间段：定义信道组的扫描持续时间在 **Monitor Intervals > Noise Measurement** 下配置，允许范围是 60 到 3600 秒。如果保留默认的 180 秒，则每 180 秒 AP 对信道组中的每个信道进行一次扫描，每次扫描持续时间是 50 毫秒。在此期间，AP 无线电从其服务信道更改到指定的信道，监听 50 毫秒并记录数值，然后返回到原始信道。跃点时间加上 50 毫秒的停留时间，AP 每次脱离信道的时间约为 60 毫秒。这意味着每个 AP 在 180 秒的总时间里有约 840 毫秒在监听恶意程序。“监听”或者“停留”时间不可以修改，并且不会因噪音测量值调整而变动。如果噪音测量计时器降低，恶意程序发现过程可能找到更多恶意程序并且更加迅速。然而，此改进以牺牲数据完整性和客户端服务为代价。另一方面，值越高，数据完整性越好，但会降低找到恶意程序的速度。
5. 配置 AP 运行模式：轻量 AP 操作模式定义了 AP 的角色。与本文提供的信息相关的模式是

：**Local — 这是 AP 的常规运行模式。**如果已配置了信道进行噪声和恶意程序扫描，在此模式下允许数据客户端接受服务。在此运行模式中，AP 脱离信道 50 毫秒以监听恶意程序。它循环通过每个信道，一次只对一个信道监听 Auto RF 配置下指定的秒数。**Monitor — 这是无线电只接收模式，允许 AP 每 12 秒扫描所有已配置信道。**配置为此模式的 AP 仅发送解除认证的数据包。监控模式 AP 能检测出恶意程序，但是不能作为客户端连接到可疑恶意程序以发送 RLDP 数据包。**注意：**DCA是指可配置为默认模式的非重叠信道。**Rogue Detector — 在此模式中，AP 无线电关闭，并且 AP 仅监听有线数据流。**控制器传递配置为恶意探测器的 AP 和可疑恶意客户端列表及 AP MAC 地址。恶意探测器仅监听 ARP 数据包，并且如有需要可通过中继链路连接到所有广播域。只要轻量 AP 连接到控制器，您就可以轻松配置单个 AP 模式。为了更改 AP 模式，连接到控制器 Web 界面然后导航到 **Wireless**。单击目标 AP 旁边的 **Details，此时显示的屏幕与下图类似**：



使用 AP Mode 下拉菜单以选择所需的 AP 运行模式。

故障排除命令

还可以使用以下这些命令排除 AP 上的配置故障：

- **show rogue ap summary — 此命令显示轻量 AP 检测出的恶意 AP 列表。**
- **show rogue ap detailed *<恶意 ap 的 MAC 地址>*** — 使用此命令查看单个恶意 AP 的详细信息。此命令帮助确定恶意 AP 是否插入到有线网络上。

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

- RF 组概述
- 技术支持和文档 - Cisco Systems