统一无线网络中Rogue接入点的侦测

文档 **ID: 70987**

介绍

无线网络扩展了有线网络，增加了员工的生产力和访问信息的能力。然而，未授权的无线网络产生了另一层面的安全问题。有线网络的端口安全性通常不需要考虑，而无线网络能方便地扩展有线网络。因此，一个员工把自己的思科无线接入点带到安全性很高的无线或有线网络中，允许未授权的用户接入网络，威胁到了这个安全性很高的网络。

Rogue侦测可以让网络管理员监控并去除这样的安全隐患。思科统一无线架构提供了2种Rogue侦测的方法，可以完全辨认并且限制Rogue接入点，而不需要昂贵并且难以确定的网络覆盖图和工具。

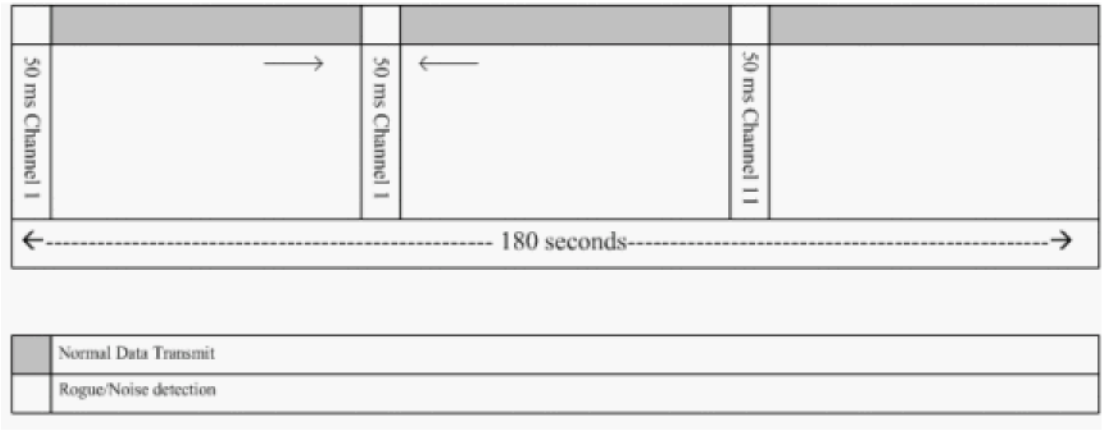
特性概述

Rogue侦测没有受到任何规章的限制，也不需要法律的认可。然而，如果Rogue侦测完全是自动操作的话，通常会给基础架构网络的提供商带来法律上的事务而处于不利状态。思科对于这些事务非常敏感，并且提供了解决方案。每个控制器都配置了RF Group名，一旦轻量级无线接入点注册上控制器，它会在所有的beacons/probe的响应帧中嵌入控制器上配置的特有的RF Group的**authentication Information Element (IE)** 。当轻量级无线接入点接收到没有**IE**或是有错误的**IE**的beacons/ probe的响应帧时，它就会把这个无线接入点报告为Rogue无线接入点，BSSID列入Rogue表，传送给控制器。有2种方法，就是Rogue位置发现协议 (RLDP) 和被动操作，这些会在“确定活动的Rogue接入点”一节中详细介绍。

基础架构网络中**Rogue**的发现

在活动的无线环境中Rogue发现的代价是很大的。这个过程需要工作中的接入点（或者本地模式）中断服务，监听噪音，执行Rogue侦测。网络管理员配置要扫描的频道，所有的终端都扫描一遍的时间周期。接入点用50ms的时间来监听Rogue客户端的包，然后再次回到配置好的频道来为客户端提供服务。这样的主动扫描，与相邻设备的信息结合后，可以辨认出哪个接入点是Rogue的，哪个接入点是自己网络的一部分。配置扫描的频道和扫描时间周期，访问**Wireless > 802.11b/g Network** (是 **b/g** 或 **a** 根据实际的网络设备) 并且点击右上角的 **Auto RF** 按钮。

你可以向下到 **Noise/Interference/Rogue Monitoring Channels** ，配置要扫描Rogue和噪音的频道。可选的选项有：All Channels (1 through 14)， Country Channels (1 through 11) 或 Dynamic Channel Association (DCA) Channels (默认是1，6和11)。扫描的时间周期也在同一窗口下配置，与噪音测量周期一起都在 **Monitor Intervals (60到3600秒)** 下面。默认情况下，对于噪音和Rogue的监听周期为180秒，也就是说，每个频道隔180秒扫描一次。这是每隔180秒扫描DCA频道的例子：



如图所示，如果很多频道都要在很短的时间周期内作扫描，那么接入点真正用于服务客户端的时间就很少了。

轻量级无线接入点会为了把客户端和接入点定义为Rogue而等待，因为这些Rogue可能在另一个周期完成之前不会被另一个接入点汇报。同一个接入点会再次到同一个频道上去监听Rogue接入点，客户端，噪音及干扰。如果同一个客户端和/或接入点被侦测到，它们会被再次列入控制器的Rogue表中。控制器开始确定这些Rogue设备是连接到了本地网络或只是邻居的接入点。在任一种情况下，不是本地无线网络的接入点会被认为是Rogue设备。

Rogue详细信息

轻量级无线接入点用50ms的时间到工作频道之外的频道去监听Rogue客户端，噪音和频道干扰。任何侦测到的客户端或接入点都传送到控制器，控制器会收集如下的信息：

- Rogue接入点的MAC地址
- Rogue接入点的名字
- 连接的Rogue客户端的MAC地址
- 帧是否有WPA或WEP的保护
- Preamble相关信息
- 信噪比(SNR)
- 信号强度(RSSI)

Rogue侦测器接入点

你可以让接入点工作于Rogue侦测器的模式，连接到Trunk口，这样它就可以监听到所有有线网络的VLAN上的信息。它会发现有线网络所有VLAN的客户端信息。Rogue侦测器接入点监听ARP包，确定控制器上的Rogue客户端或接入点的2层地址信息。如果发现了2层地址的匹配，控制器会发出Rogue接入点或客户端有威胁的告警，这表示Rogue设备在有线网络上。

确定活动的Rogue接入点

控制器将接入点确定为Rogue设备前必定要看到Rogue接入点2次。如果Rogue接入点没有连接到公司的有线网络，则不会被认为是安全威胁。为了确定Rogue设备是否活动，可以用多种方法。这些方法中包括RLDP。

Rogue位置发现协议 (RLDP)

RLDP是一个主动的方法，当Rogue接入点不需要认证（开放认证）的时候可以使用。这种模式在默认情况下是禁用的，它使活动的接入点转移到Rogue接入点的频道，作为客户端连接到Rogue接入点。在这段时间内，活动接入点会向所有连接着的客户端发送认证不过的消息，然后关闭Radio端口，作为客户端连接上Rogue接入点。

然后接入点会尝试着从Rogue接入点获得IP地址，通过Rogue接入点向控制器发送包含本地接入点和Rogue接入点信息的UDP（port 6352）包。如果控制器收到了这个包，就会向网络管理员发警告，通过RLDP在有线网络上发现了Rogue接入点。

注意： 使用 **debug dot11 rldp enable** 的命令来检查轻量级无线接入点是否连上了Rogue接入点，是否通过DHCP拿到了地址。这个命令同样会显示轻量级无线接入点发送到控制器的UDP包。

轻量级无线接入点发送的UDP (目标端口6352)包举例如下：

```
0020 0a 01 01 0d 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
```

前5个字节包含了本地模式接入点通过Rogue接入点获得的DHCP地址的信息。之后的5个字节是控制器的IP地址，紧接着的6个字节是Rogue接入点的MAC地址。然后是18个字节的0。

被动操作：

这种方法是当Rogue接入点有某种形式的认证时使用，WEP或WPA。当Rogue接入点上使用了认证，轻量级无线接入点就没法连接，因为它不知道Rogue接入点上的密钥。控制器把Rogue客户端的MAC地址列表发送到工作于Rogue侦测器模式的接入点，Rogue侦测器会扫描所有连接的子网的ARP请求，搜索ARP信息来找2层地址的匹配。如果发现了匹配信息，控制器会向网络管理员发出有线网络上发现Rogue接入点的告警。

限制活动Rogue设备

一旦在有线网络上发现Rogue客户端，网络管理员可以限制Rogue接入点和客户端。通过发送802.11认证不过的数据包到连接在Rogue接入点的客户端使其掉线，减轻安全漏洞的威胁性。每次要限制Rogue接入点，轻量级无线接入点上就会有将近15%的资源被用掉。因此，一旦限制了Rogue接入点，最好是找到其位置并且移除。

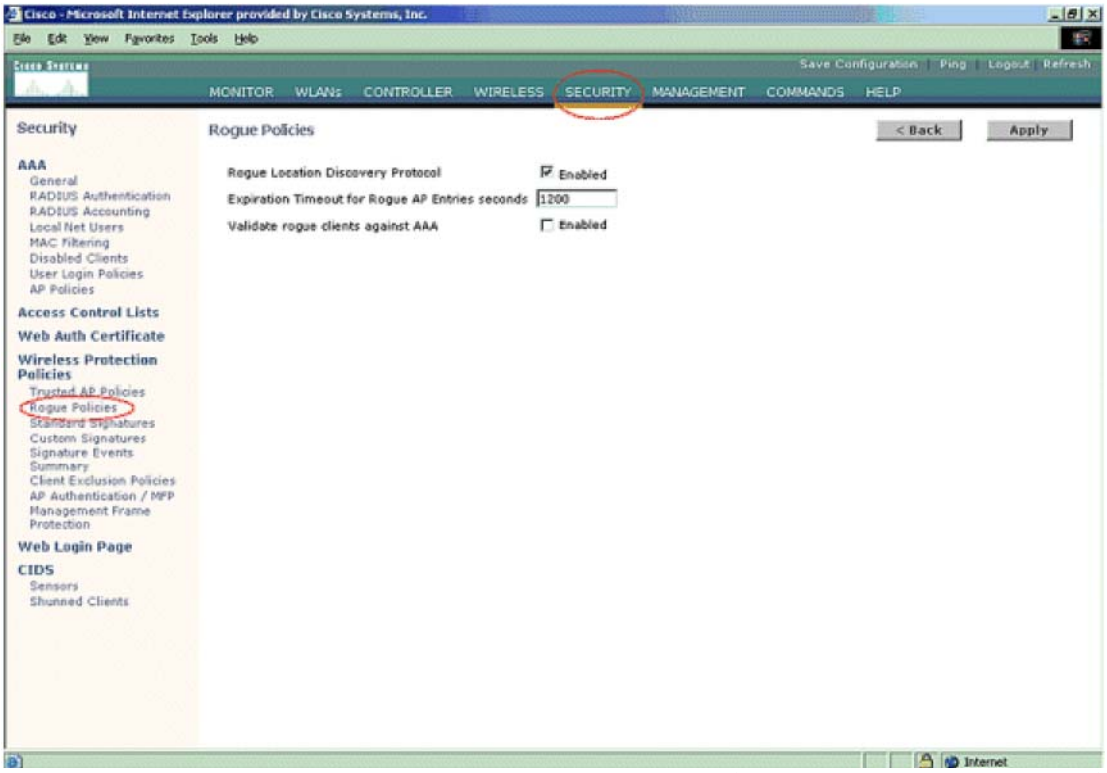
Rogue侦测配置步骤

几乎所有的Rogue侦测配置都是默认打开的，以允许最佳的初始即有的网络安全。这里的配置步骤是假定控制器上没有配置过Rogue侦测，以阐明重要的Rogue侦测相关的信息。

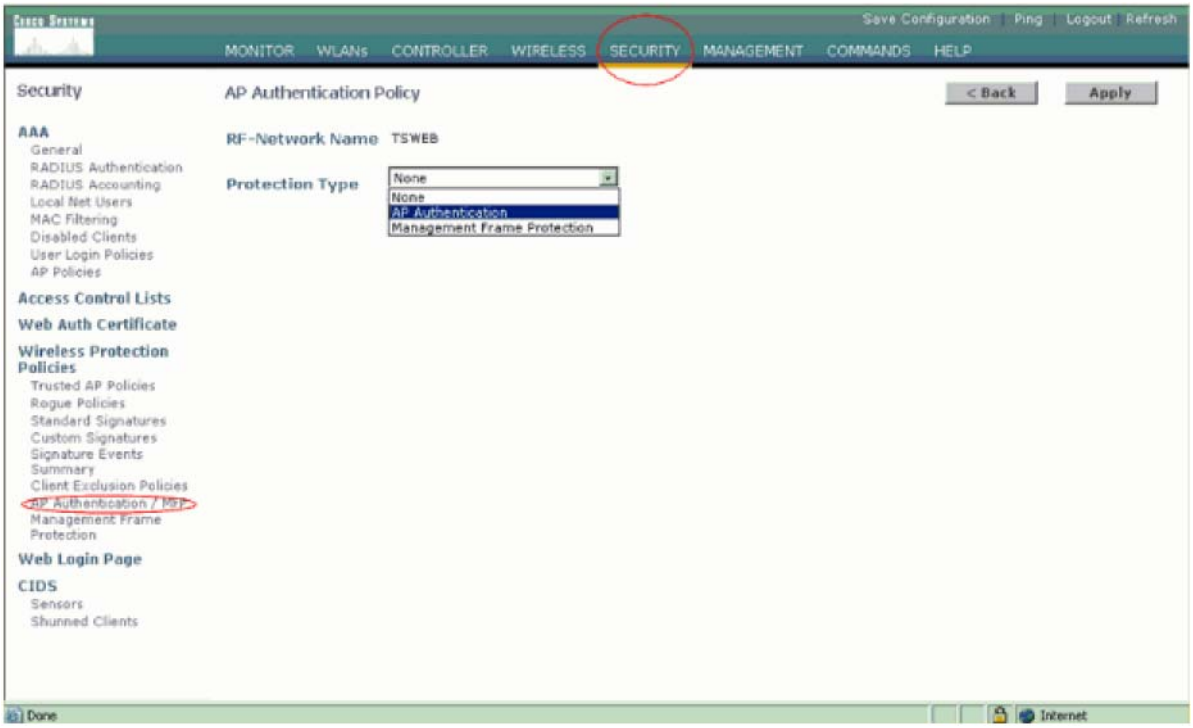
根据如下步骤，配置Rogue侦测：

1. 确保Rogue位置发现协议已经打开。为了打开它，选择 **Security > Rogue Policies** ，在**Rogue Location Discovery Protocol**上点击 **Enabled** ，如图所示。

   注意： 如果一个Rogue接入点在一定时间内都没有监听到，就会从控制器上移除。这就是Rogue接入点的 **Expiration Timeout** ，在RLDP选项的下面可以配置。

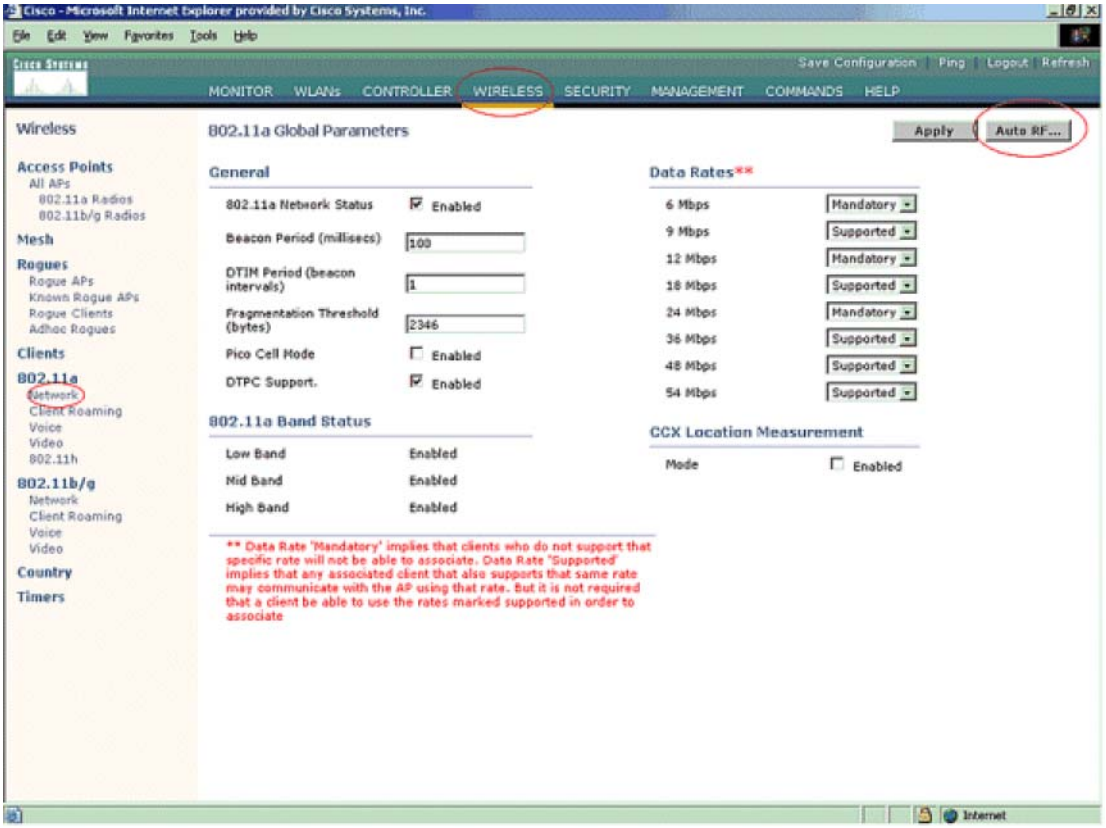


2. 这是一个可选的步骤。当这个特性被打开，发送包含不一致的 **RF Group** 名字的RRM邻居包的接入点会被认为是Rogue设备。这对你在了解RF环境时是非常有用的。选择 **Security-> AP Authentication** 以打开这一特性。然后，选择 **AP Authentication** 作为保护类型，如图所示。

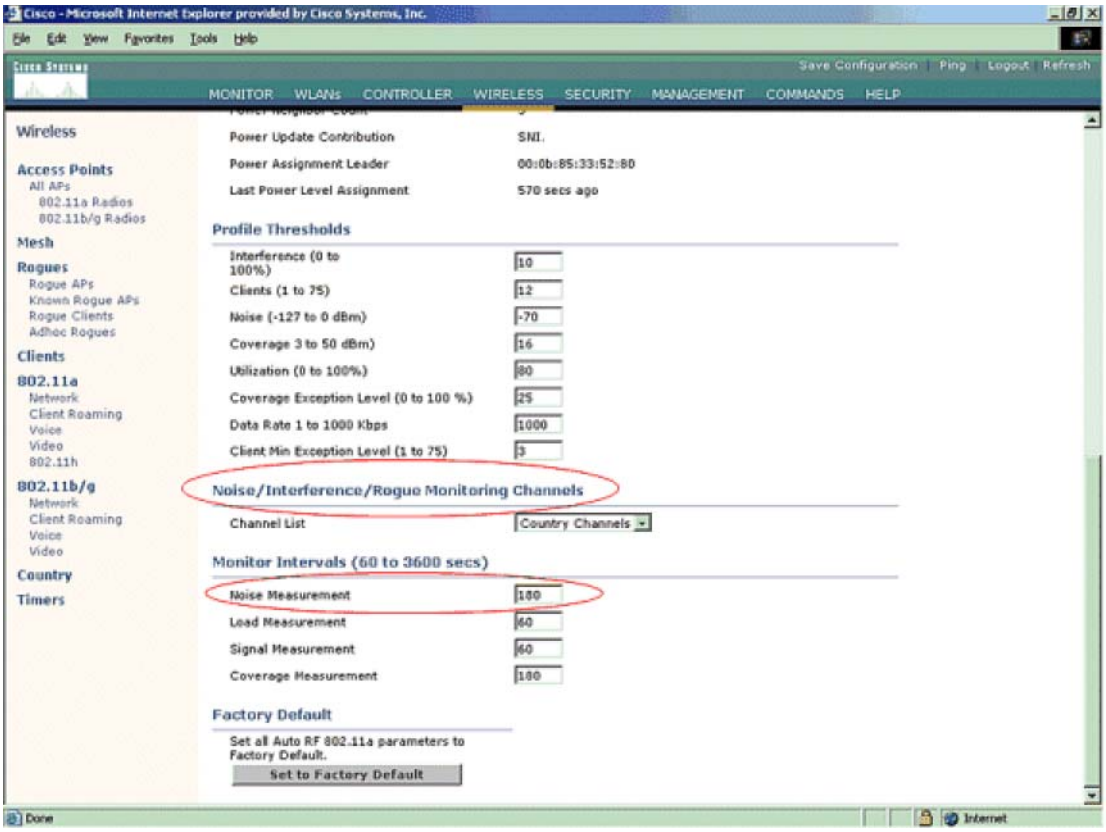


3. 根据如下步骤，确认扫描的频道：

a. 选择 **Wireless > 802.1 1a Network,** 然后在右边选择 **Auto RF** ， 如图所示。



b. 在 **Auto RF** 页面上，往下翻并选择 **Noise/Interference/Rogue Monitoring Channels.**



c. 除了其他的控制器和接入点的功能之外，频道列表详细列出了Rogue监测扫描的频道信息。更多关于轻量级无线接入点的信息参见Lightweight Access Point FAQ，更多关于无线控制器的信息参见Wireless LAN Controller (WLC) Troubleshoot FAQ。

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. 为扫描选定的频道设置时间周期：

扫描频道的周期在 **Noise Measurement** > **Monitor Intervals** 中配置，允许的范围是60到3600秒。在默认180秒的情况下，接入点会每隔180秒扫描每个频道，用时50ms。在这50ms的时间内，接入点会从服务的频道转到特定的频道，监听并记录信息，然后再回到原来的服务频道。接入点每次改变频道加上扫描的50ms一共用去60ms时间。这就意味着，每个接入点在整个180秒内会花去大约840ms的时间来监听Rogue设备。

监听的时间不可能在Noise Measurement的参数中设置，如果Noise Measurement的时间值降低了，Rogue发现过程就会发现更多的Rogue设备，并且发现得更快。然而，这样的提升是以牺牲数据传输和客户端服务为代价的。另一方面，如果时间值升高，数据传输就会更顺利，但是快速发现Rogue设备的能力降低了。

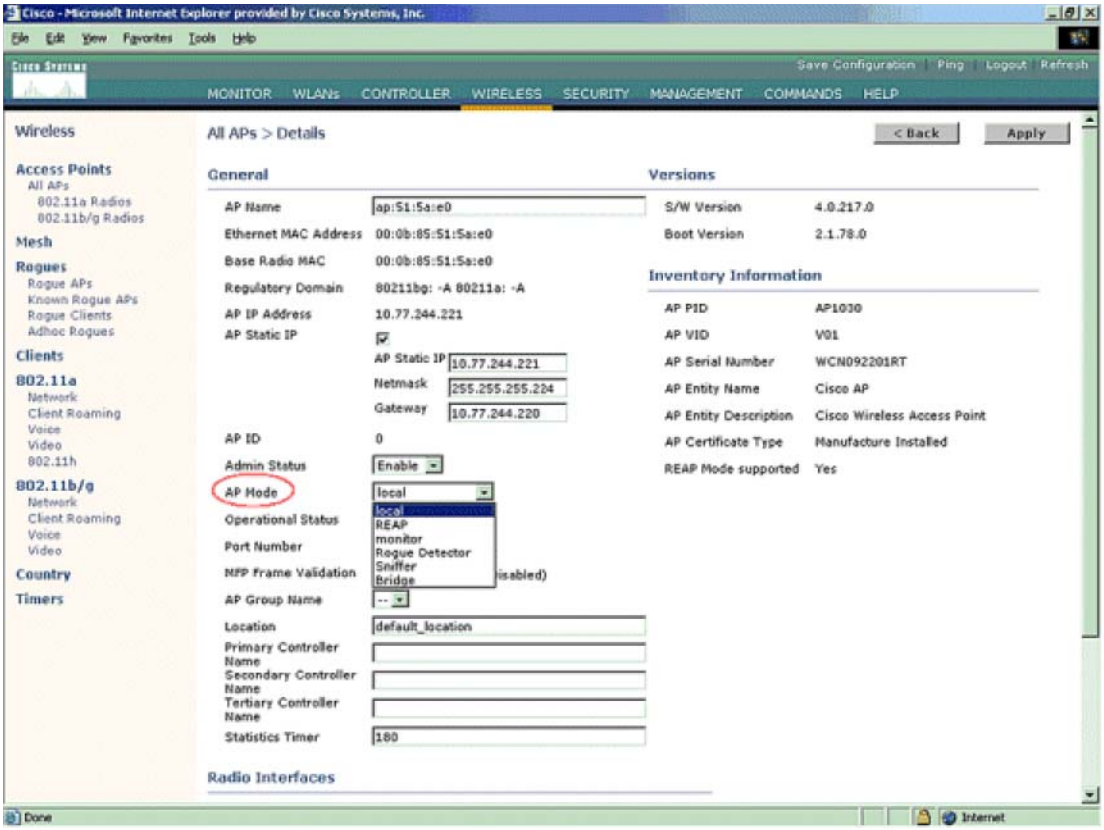
5. 配置接入点的工作模式：

轻量级无线接入点的模式决定接入点工作的角色。与本文档相关的模式信息如下：

- **Local** 这是接入点常规工作的模式。这个模式允许接入点服务数据客户端，并在配置的频道上扫描噪音和Rogue设备。在这个工作模式下，接入点去用50ms跳到其他频道上去监听Rogue设备。它在每个频道都以Auto RF中配置的时间周期循环。
- **Monitor** 这是只接收电波信号的模式，允许接入点每隔12秒扫描配置的频道。这个模式的接入点只会发送无法认证的包。监控模式的接入点可以侦测Rogue设备，但是它不能作为客户端连接到可疑的Rogue设备上去发送RLDP数据包。

  注意： DCA指的是在默认模式下可配置的不重叠的频道。
- **Rogue Detector** 在这个模式下，接入点的radio端口是关闭的，接入点只监听有线的流量。控制器把可疑的Rogue客户端和接入点的MAC地址发送到Rogue侦测器模式的接入点，Rogue侦测器只监听ARP数据包，并且可以通过Trunk口连接到所有的广播域中。

一旦轻量级无线接入点连接到控制器上，你就可以配置接入点的工作模式了。要改变接入点的模式，访问控制器的WEB界面，进入 **Wireless.** 点击要设置的接入点的 **Details** ，出现如下的界面：



使用AP Mode的下拉菜单，选择需要的接入点工作模式。

故障诊断命令

你也可以用如下的命令来故障诊断接入点上的配置：

- **show rogue ap summary** 这个命令显示轻量级无线接入点上侦测到的Rogue接入点。
- **show rogue ap detailed** <*Rogue接入的MAC地址*> 使用这个命令来查看特定的Rogue接入点的详细信息。这个命令用于确定Rogue接入点是否连接到了有线网络。

结论

思科集中控制器解决方案中的Rogue设备的侦测与限制是行业中最有效最少干扰的方法，其强大的适应性使网络管理员在任何的网络需求下都可以特别定制并适应。

NetPro论坛 – 特殊的会话

Networking Professionals Connection是一个让网络专家们分享网络解决方案、产品和技术相关的问题、建议及信息的论坛。这些特殊的链接是一些在这个技术领域内最新的会话。

NetPro论坛 - 无线的特殊的会话

Wireless - Mobility: WLAN Radio Standards

Wireless - Mobility: Security and Network Management

Wireless - Mobility: Getting Started with Wireless

Wireless - Mobility: General

相关信息

- **Overview of RF Groups**
- **Technical Support & Documentation - Cisco Systems**

更新： Sep 25, 2007 文档 ID: 70987