实验室测试报告
DR100409C

Cisco CleanAir 竞争测试

2010 年 4 月

Miercom
www.miercom.com

目录

执行摘要

我们的独立第三方评估发现，Cisco CleanAir 技术是一种全面而有价值的解决方案，可解决无线网络中非 Wi-Fi 干扰源所造成的干扰问题。

常见的非 Wi-Fi 设备运行的无线电频谱与无线局域网络相同，因此可能会导致用户体验的质量显著下降，往往表现在延迟偏高，在某些情况下，还会完全破坏无线网络通信。这是因为 802.11 协议的设计基于先听后说的算法礼仪。这种设计可使信道完全被干扰阻塞，从而导致客户端中断。能够识别和避免这类干扰对网络管理员来说是非常重要的能力。

Cisco CleanAir 技术利用在无线接入点定制的无线电 ASIC，提供一流的频谱分析和干扰缓解工具，而这是标准 Wi-Fi 芯片集所不能提供的。这些工具增强了扫描分辨率精细度，并可快速避免信道较差情况，以保护最终用户体验。

我们对 CleanAir 检测各种常见非 Wi-Fi 干扰源的速度和精确度感到满意，尤其对其所提供的用于协助缓解干扰活动的可操作信息级别感到满意。Cisco CleanAir 为每个干扰源提供唯一标识符，显示严重性和空气介质质量级别，正确对设备类型进行分类，并映射来源的物理位置。其识别和定位多个同时干扰源的能力令人惊叹。

CleanAir 还展示了自行恢复能力，在不到 1 分钟内即能够可靠地更改到干净信道，避免远达 100 英尺干扰源的干扰，这是其他竞争产品所不具备的独特优势。它的另一个优点是能够检测到隐藏在非标准频率中的欺诈无线接入点，这些无线接入点可能会对网络安全形成威胁。

竞争产品的供应商并没有积极参与本报告所涉及的测试。但所有供应商如果对我们提供的任何发现结果存在异议，都有机会在我们的实验室中展示他们的产品测试。

能够为 Cisco CleanAir 技术所展示的性能和干扰缓解功能集成提供“性能验证认证”，Miercom 对此感到十分自豪。

Rob Smithers
执行总裁
Miercom

主要发现结果

- 非 Wi-Fi 干扰会影响 2.4GHz 和 5GHz 频谱上无线接入点与客户端之间的吞吐量
- Cisco CleanAir 技术能够对干扰位置进行检测、分类和映射，以快速完成补救
- Cisco Aironet 3500 系列无线接入点 (AP) 中的定制 CleanAir ASIC 提供其他 Wi-Fi 芯片集所不具备的扫描和检测优势
- CleanAir 提供先进的外频率欺诈设备检测，防止后门安全威胁
- 能够避免干扰的快速自行恢复能力改善了最终用户体验，并可从信道干扰中快速恢复
- Motorola AirDefense 产品的竞争分析表明，在不到 25% 的测试案例中的确如此。（错误识别 15%；间歇性检测 23%；遗漏或不完整分类 38%）。

概述

Miercom 对 Cisco CleanAir 技术在干扰分类、缓解和避免方面进行了验证，并将其与其他供应商的产品进行比较。此次评估对思科、Aruba、Motorola、Trapeze、HP 和 Meru 的最新版本无线控制器和无线接入点就其各自的性能进行了比较。

我们测试了各种非 Wi-Fi 设备干扰对吞吐量的影响，包括来自视频监视摄像头的连续波类型信号、跳频 2.4GHz 和 5GHz 电话和蓝牙设备，以及来自微波炉的循环型干扰。评估包括对单一源的每类干扰进行检测和分类的能力，以及对多个干扰源进行准确分类的能力。我们还研究了自行恢复特性，即能够识别主要干扰源并切换到另一个信道的避免干扰能力。我们还针对隐藏在标准 Wi-Fi 信道间的外频率欺诈无线接入点的检测能力进行了测试，这些无线接入点可提供后门接入到有线网络。

Cisco CleanAir 技术能够检测干扰源并确定和映射位置，以便采取补救措施。

使用的无线局域网设备：

Cisco 无线局域网控制器 5508 (7.0.93.110)
- Cisco 3500 序列 802.11n 无线接入点

Cisco 无线控制系统 (7.0.130)

思科移动服务引擎 (7.0.99)

Aruba 6000 控制器 (3.4.2.2)
- Aruba AP125 802.11n 无线接入点
- Aruba AP105 802.11n 无线接入点

HP MSM760 控制器（软件版本 5.3.3）
- HP MSM422 802.11n 无线接入点

Motorola RFS7000 控制器（软件版本 4.2.1）

装有最新版软件的 Motorola AP-7131N 802.11n 无线接入点 (4.0.3)

装有最新版软件的 Motorola AirDefense 1250 服务控制台 (8.0.0.15)

装有最新固件的 Motorola AirDefense M520 传感器 (5.2.0.11)

Trapeze MX-200R 控制器 (7.0.13.3)
- Trapeze MP-432 802.11n 无线接入点

Meru MC4100 控制器（软件版本 3.6.1）
- Meru AP320 802.11n 无线接入点

802.11n 客户端（Intel 5300AGN – 驱动程序 13.1.1.1）

干扰源：

微波炉

Plantronics 蓝牙无线耳机

2.4GHz DECT 无绳电话

5.8GHz DECT 无绳电话

2.4GHz Q-See 无线视频监视摄像头

5.8GHz 无线视频监视摄像头（型号：W5803W1）

试验台图

如何操作

分类测试：

对于思科，我们利用三个 Aironet3500 系列无线接入点、5508 无线控制器、Cisco 无线控制系统 (WCS) 和思科移动服务引擎 (MSE) 创建测试环境。对于 Motorola，我们使用两个 M520 传感器、一个 AP7131N 无线接入点、一个 Motorola AirDefense 1250 服务器和 Motorola RFS7000 无线局域网控制器。这两个供应商的传感器位置相同。两个传感器之间相距 50 英尺，到干扰源的距离相等。第三个传感器放在距离大约 70 英尺的位置。我们使用标准台式微波炉作为干扰源，在测试期间将微波炉设置为 HIGH 并工作 2 分钟。我们还使用了 2.4GHz 和 5GHz 无绳电话听筒和基站、2.4GHZ 和 5GHz 无线视频监视摄像头、一个蓝牙耳机和充电基站，以及射频干扰器设备。

自行恢复测试：

五个客户端被放置在距离无线接入点从 10 到 100 英尺的位置。每个客户端都不断接收循环播放的低带宽视频流。因为视频播放器应用程序对流执行缓冲，我们设置了一个命令提示窗口不断 ping 无线接入点，以确定通信是在何时中断的。用秒表计时。我们为干扰源选择了三个位置：距离无线接入点 10 英尺的位置 A、距离无线接入点 50 英尺的位置 B 和距离无线接入点 100 英尺的位置 C。我们预计每个客户端根据距离干扰源的远近以及干扰源距离无线接入点的远近会受到不同程度的影响。在位置 C 处，我们预计距离无线接入点 100 英尺但距离干扰源最近的客户端将中断，而其他客户端则会不受影响地继续通信。我们选择的干扰源是 2.4GHz 视频监视摄像头，因为该设备的负面影响最大，测试的第一个无线接入点是 Cisco 3500 系列。

测试结果

干扰影响

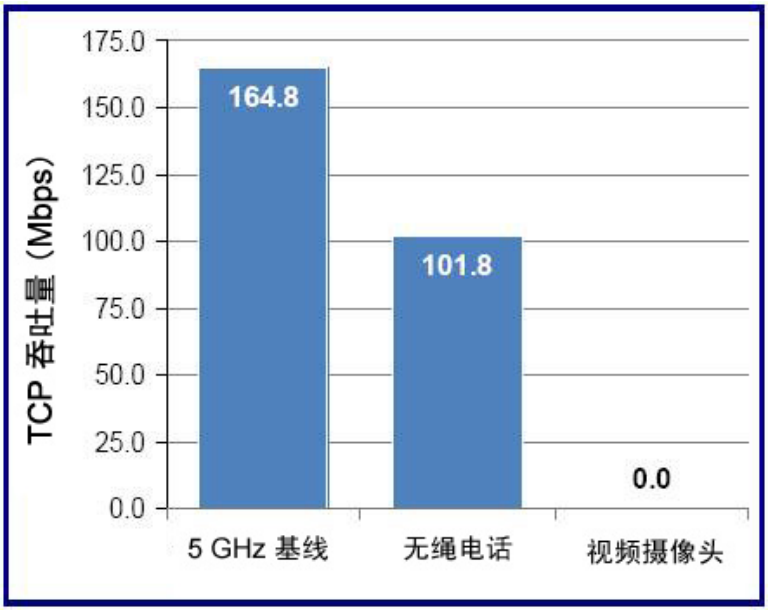
我们执行测试以确定不同类型的非 Wi-Fi 信号对性能的影响。客户端为 802.11n 手提电脑，Cisco 3500 用作无线接入点。基准吞吐量在 5 GHz 波段 40 MHz 信道的原始频谱中进行测量。打开单个干扰信号，并对吞吐量进行测量。多次运行以获得平均值。原始频谱中基准吞吐量为 164.8 Mbps。

激活 5GHz 无线视频监视摄像头时，信道 153 因连续波干扰而阻塞，客户端失去通信。视频摄像头运作时网络吞吐量为 0%。

我们使用 5GHz DECT 来记录跳频的信号影响。我们使用了三部电话：两部进行会议通话，一部为连接到座机的基站。使用三部电话时，网络吞吐量下降到 102 Mbps，无线接入点测量的空气介质质量为 86%。

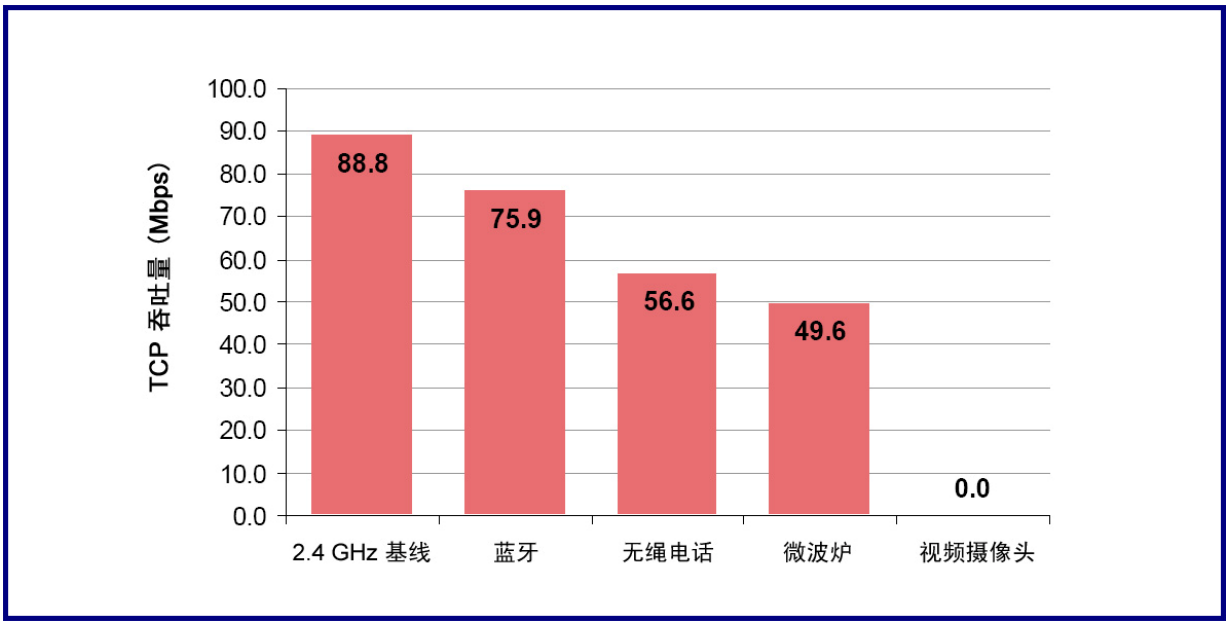
有关 5.0GHz 基准值的信息，请参见*图 1*。

图 1：5.0GHz 基准测量值与干扰对吞吐量的影响



基准测量值与无绳电话和视频摄像头的比较

图 2：2.4GHz 基准测量值与干扰对吞吐量的影响



比较基准值与来自蓝牙、无绳电话、微波炉和视频摄像头的干扰。每个非 Wi-Fi 干扰源都具有不同的影响，分别测试并与基准值进行对比。

然后测试对 2.4GHz Wi-Fi 波段的干扰。该波段由信道 1、6 和 11 组成。原始频谱中的基准值为 88.849 Mbps。使用蓝牙耳机传输语音时，吞吐量下降到 76 Mbps。蓝牙也是跳频类干扰。

我们使用 2.4GHz 无绳电话来记录跳频的信号影响。我们使用了三部电话：两部进行会议通话，一部为连接到座机的基站。使用三部电话时，网络吞吐量下降到 57 Mbps。

循环型干扰由微波炉产生，影响 2.4GHz 的上半部分，包括 6 到 11（取决于型号）的信道。将微波炉设置为以高功率运行两分钟，网络吞吐量下降到 50 Mbps。有关 2.4GHz 基准值的信息，请参见*图 2*。

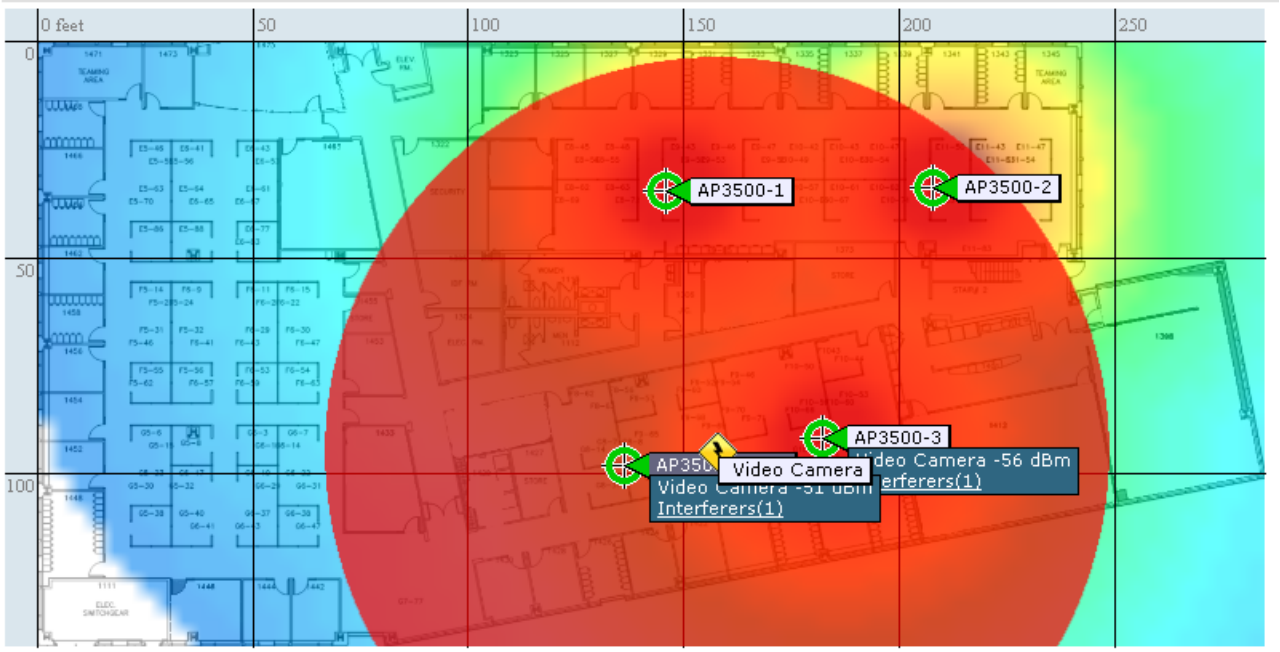
使用 2.4GHz 波段无线视频监视摄像头时，记录的吞吐量为 0 Mbps。

干扰分类

除了了解其他信号设备对网络的影响之外，我们还需要确定这些设备的地点和来源，以补救问题。我们对使用 Cisco CleanAir 技术的 Aironet 3500 系列无线接入点以及使用 AP-7131N 无线接入点和 M520 传感器的 Motorola AirDefense 解决方案进行了评估。这两种解决方案都可以对干扰源进行分类，而测试的其他供应商则不具有干扰分类功能。

Cisco Aironet 3500 系列无线接入点内置定制的 CleanAir ASIC 芯片，有频谱分析功能，可实时监控网络，并为客户端提供无线局域网服务。Motorola AP-7131N 也提供频谱分析。无线接入点可以提供无线局域网服务，也可以监控频谱，但二者不能同时进行。通过禁用无线接入点来提供干扰监控会增加其他无线接入点上的负载，并降低网络容量。由于这是标准 Wi-Fi 芯片集，因此该分析的分辨率受到限制。我们观察到 Cisco CleanAir 提供 78 KHz 的扫描分辨率而 Motorola 只提供 5 MHz 的扫描分辨率。前者可提供多于 Motorola 64 倍的扫描分辨率。

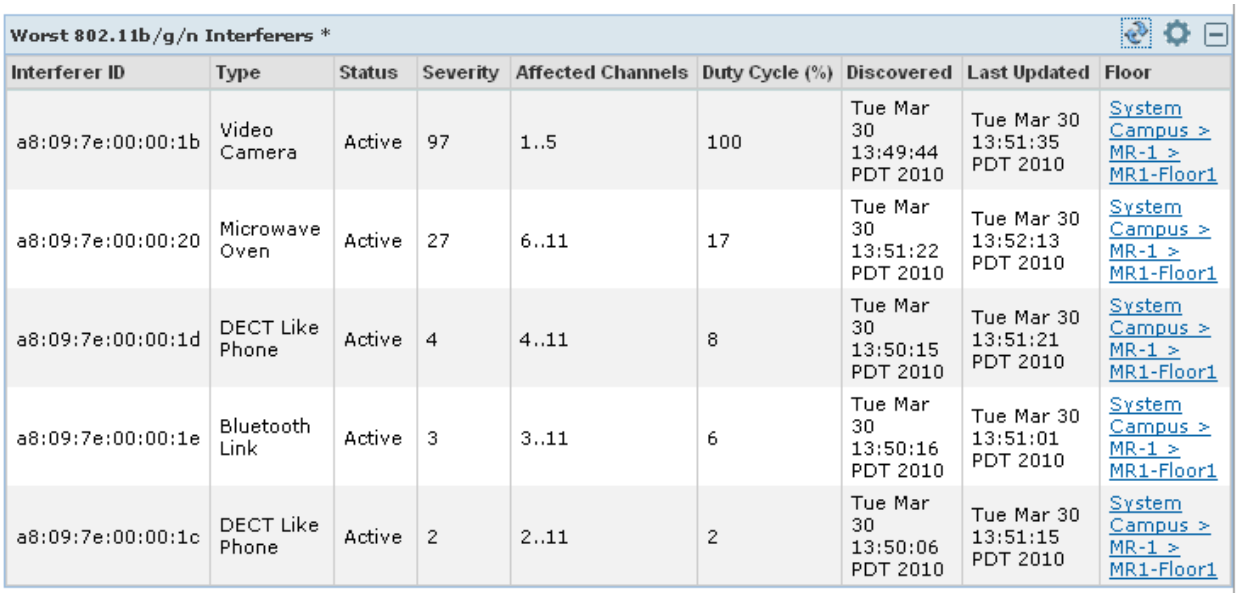
Cisco CleanAir 还通过 WCS 的图形化接口提供映射功能，可定位干扰信号的物理位置。



这是 Cisco WCS 显示视频摄像头干扰源物理位置的屏幕抓图。设备周围的红色圆圈代表干扰源的影响区。

我们在 2.4GHz 波段下使用单一干扰源和多个干扰源，在 5GHz 波段下使用单一干扰源进行测试。

来自思科的屏幕抓图



Worst 802.11b/g/n Interferers *

Interferer ID	Type	Status	Severity	Affected Channels	Duty Cycle (%)	Discovered	Last Updated	Floor
a8:09:7e:00:00:1b	Video Camera	Active	97	1..5	100	Tue Mar 30 13:49:44 PDT 2010	Tue Mar 30 13:51:35 PDT 2010	System Campus > MR-1 > MR1-Floor1
a8:09:7e:00:00:20	Microwave Oven	Active	27	6..11	17	Tue Mar 30 13:51:22 PDT 2010	Tue Mar 30 13:52:13 PDT 2010	System Campus > MR-1 > MR1-Floor1
a8:09:7e:00:00:1d	DECT Like Phone	Active	4	4..11	8	Tue Mar 30 13:50:15 PDT 2010	Tue Mar 30 13:51:21 PDT 2010	System Campus > MR-1 > MR1-Floor1
a8:09:7e:00:00:1e	Bluetooth Link	Active	3	3..11	6	Tue Mar 30 13:50:16 PDT 2010	Tue Mar 30 13:51:01 PDT 2010	System Campus > MR-1 > MR1-Floor1
a8:09:7e:00:00:1c	DECT Like Phone	Active	2	2..11	2	Tue Mar 30 13:50:06 PDT 2010	Tue Mar 30 13:51:15 PDT 2010	System Campus > MR-1 > MR1-Floor1

该图显示了成功地将多个同时存在的干扰源进行分类。

我们以单个 2.4GHz 视频监视摄像头作为干扰源开始测试。Motorola 对“连续波”触发了警报，但是未能识别该设备。Cisco WCS 则识别出该设备为视频摄像头、确定了它的位置并指出其干扰严重性为 98。思科无线控制器用户接口还显示了 Wi-Fi 信道利用率较低，空气介质质量较差。

使用微波炉的测试中，Motorola 提供了两个警报，一个位于无线接入点，另一个位于传感器，并正确识别出了干扰源。无线接入点检测到 2437MHz 的干扰，而传感器检测到 2462MHz 的干扰源。Motorola 未提供任何关联，因此同一个设备在 AirDefense 系统中显示了两个警报。

思科从三个无线接入点检测到干扰并确定干扰源为微波炉，并报告了一个事件。另外还检测到受影响的信道，并确定了微波炉的位置。干扰过后该信息会保留，以对定期干扰进行补救。

环境中放置了 DECT 无绳电话基站。当基站尝试与电话进行通信时会产生干扰，但是比真正进行语音呼叫时的占空比要小。Motorola 在频谱分析界面中显示了干扰，但是未能识别来源。因为占空比太小而无法识别。思科则将该来源分类为“DECT 类电话”，并确定了物理位置。

将使用中的电话添加到基站时，占空比增加。这次 Motorola 在无线接入点和两个传感器都检测到干扰，并确定来源为“跳频”。检测时断时续。思科检测到电话和基站并将其分类为“DECT 类电话”，并再次映射了物理位置。

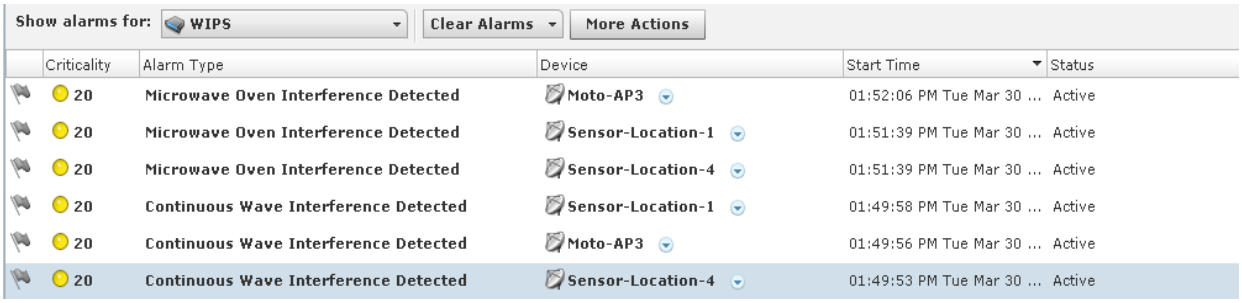
我们又添加了两个听筒并使其均处于使用状态。Motorola 将干扰来源分类为跳频。检测仍然时断时续。我们对 Motorola 使用完整扫描模式和干扰扫描模式都进行了测试。两种模式下的检测都时断时续；在干扰模式下，距离来源最近的无线接入点未检测到干扰，而两个传感器则将来源错误分类为蓝牙。

思科对关联无线接入点的每部电话都进行了正确分类，并正确映射了它们的物理位置。

在发现模式下，蓝牙占空比较小（1% 干扰）。在测试环境中放置了蓝牙耳机，以确定思科或 Motorola 是否能检测到。思科和 Motorola 都未能检测到该设备，因为蓝牙发现模式仅发生在很短的时间内。使用蓝牙耳机时，占空比为 15%。Motorola 的一个传感器时断时续地检测到干扰，但是距离干扰源最近的无线接入点未检测到。由于 Motorola 没有为每个干扰源指定唯一的 ID，因此在之前的无绳电话测试中无绳电话被错误的分类为蓝牙。警报显示了先前测试的开始时间，但是未显示结束时间。另外还为蓝牙警报分配了与连续波相同的严重性级别，而事实上这两类干扰的影响并不相同。

思科检测到该蓝牙设备为唯一干扰源并对其进行了正确分类，显示了其在环境平面图的位置，并显示了严重性。

来自 Motorola 屏幕抓图



在使用多个同时干扰源的测试案例下，Motorola 检测到了微波炉和视频摄像头，但是未检测到 DECT 电话和蓝牙干扰源，这两者都是跳频。请注意，即使只打开一个微波炉，也会触发多个警报。

多个干扰源——2.4GHz 波段

我们想要确定如果多个干扰源同时运作，CleanAir 和 AirDefense 是否能正确进行分类。

我们使用了两个视频监视摄像头，一个使用信道 1，另一个使用信道 11。思科将两个干扰源正确分类为视频摄像头，并报告一个影响信道 1-4，第二个影响信道 9-11。还显示了在平面图中的物理位置。

而 Motorola 在传感器和无线接入点都触发了警报，但是未能确定是一个设备还是多个设备导致发出警报。每个传感器和无线接入点都显示单个干扰警报。

之后我们又添加了其他干扰源。多个干扰源由 2.4GHz DECT 电话、2.4GHz 视频摄像头、蓝牙耳机和微波炉组成。

思科准确检测到所有设备，对其进行分类并确定了它们的位置。微波炉位置图标最初被视频摄像头位置图标隐藏。

Motorola 检测到 2462MHz 连续波设备（视频摄像头）并发出警报，也正确分类了微波炉，但是未能检测出 DECT 电话或蓝牙耳机为跳频设备。

单一干扰源——5GHz 波段

我们还测试了每个产品在 5GHz 波段分类干扰源的能力。

从 DECT 无绳电话开始，思科能够检测到设备，将其正确分类为“DECT 类电话”，并确定其位置。

如先前 2.4GHz 测试中所显示，占空比较小使 Motorola 无法检测到干扰，因此未触发任何警报。

为增加干扰的占空比，我们又添加了听筒并使其处于使用状态。思科再次正确分类并映射了电话位置。Motorola 的一个传感器时断时续地检测到跳频并发出警报，而无线接入点却未检测到干扰。

三部电话都处于使用状态时，Motorola 无线接入点和两个传感器都检测到跳频并发出警报。思科对这三部电话都进行了正确分类并确定了它们的位置。

之后我们又在环境中放置了 5GHz 视频摄像头。Motorola 能够检测并确定干扰，可能因为干扰的占空比足够大超过了触发警报的阈值。思科能够准确分类并确定视频摄像头的位置。

有关干扰源以及如何对其进行检测和分类的摘要，请参见第 13 页的*图 3*。

图 3：Cisco CleanAir 和 Motorola AirDefense 对干扰源的分类和相关信息

干扰源		是否分类？		Motorola AirDefense 备注
频率波段	类型	Cisco Clean Air	Motorola AirDefense	
2.4GHz	视频摄像头	是	是	笼统分类为“连续波”
	微波炉	是	是	显示了两个警报：每个传感器显示一个，二者无关联。
	仅 DECT 基站	是	否	Motorola 需要较高的占空比才能进行分类。
	DECT 基站 + 一部电话	是	间歇	Motorola 会分类，但时断时续。
	DECT 基站 + 三部电话	是	分类错误	一个传感器未检测到。其他传感器触发了蓝牙和跳频警报
	蓝牙	是	间歇	时断时续且只有一个传感器检测到
	干扰发射台	是	分类错误	Motorola 在 1 秒钟内错误分类为微波炉
多个 2.4GHz	视频摄像头 (Ch1) 视频摄像头 (Ch11)	是	否	Motorola 的所有传感器都提供了“连续波”警告，但是未列出导致干扰的两个设备。
	DECT 电话、视频摄像头、蓝牙、微波炉	是	否	仅识别出微波炉和视频摄像头
5GHz	DECT 基站	是	否	Motorola 需要高的占空比才能进行分类。
	DECT 基站 + 一部电话	是	间歇	时断时续且只有一个传感器检测到
	DECT 基站 + 三部电话	是	是	
	视频摄像头	是	否	

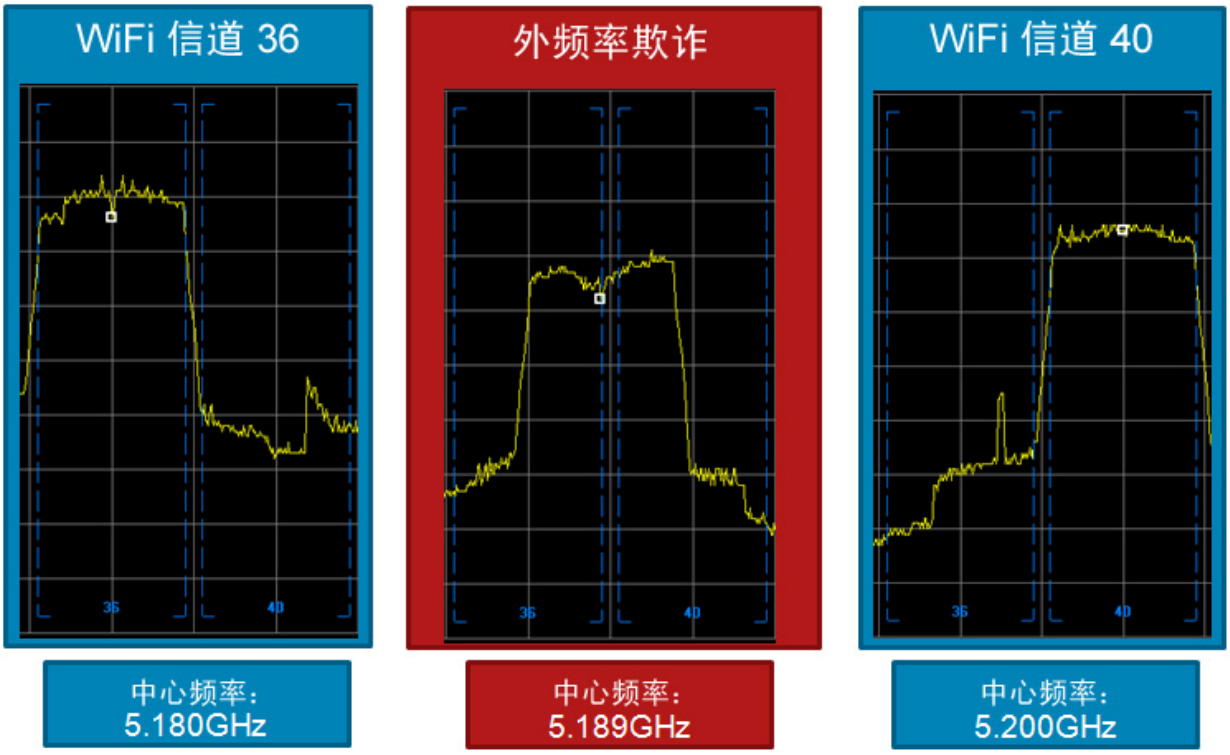
非标准信道中的欺诈设备

由于欺诈设备会通过允许“后门”访问，对有线网络造成威胁，因此我们对无线接入点进行了测试，以查看这些访问点是否能发现此类威胁。

我们将思科无线接入点配置为一个工作组网桥，并将其置于信道 36。我们为该桥提供“隐藏”的 SSID，然后检查它是否会被检测到。

思科正确识别了该网桥为一个欺诈无线接入点。Trapeze 也正确识别了该欺诈设备。Motorola 检测为一个“未经批准的 BSS”。HP 也检测出欺诈，Aruba 检测为“窃取”SSID。Meru 则未检测到该欺诈。

几乎所有的无线接入点都能够探测到置于网络中的欺诈设备。然后我们想要测试如果欺诈设备配置为外频段会发生什么情况。有些产品能让用户改变用于大多数 Wi-Fi 无线接入点上基于 Atheros 的芯片集的中心频率，从而使它们在网络中隐藏起来。为确定是否能检测到此类外频率欺诈，我们将欺诈设备的中心频率改为 5.189GHz。我们将其置于信道 36 到 40 之间，重新进行测试。



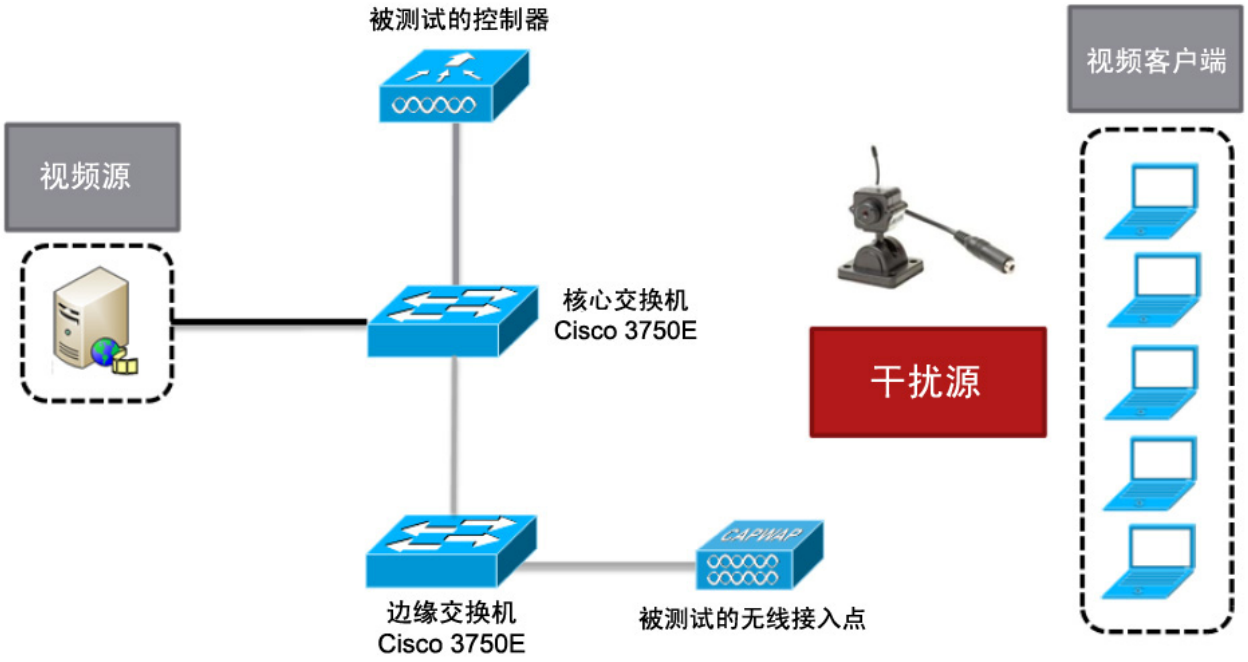
思科能正确识别欺诈设备为“Wi-Fi 无效信道”，并映射其位置。所有其他供应商都针对外频段，而不是外频率进行了扫描。Aruba 不能在新频率检测到欺诈设备，Trapeze、Motorola、HP 和 Meru 同样不能检测到欺诈设备。

自行恢复

鉴于非 Wi-Fi 干扰对无线网络的负面影响，无线接入点需要避免此干扰，以保护最终用户的用户体验质量 (QoE)。我们使用 2.4GHz 波段进行此测试。

思科设备：

在位置 A 启用摄像头，所有五个客户端的 ping 测试立即中断。无线接入点从信道 1 切换到信道 6，客户端在 49 秒内恢复 ping。在位置 B 使用摄像头时，无线接入点用时 39 秒更改信道，且客户端恢复 ping。在位置 C 使用摄像头，无线接入点用时 1 分零 4 秒更改信道并恢复 ping。由于思科无线接入点具有持续避免能力，因此我们在两次测试之间会重置无线接入点以清除持续避免设置，这样备用信道就不会被功能锁定。在正常运作中，持续的设备避免功能自动使干扰源过期，以便系统可再次使用该信道。针对每个位置的第二次运行在位置 A 花了 30 秒，在位置 B 花了 41 秒，在位置 C 花了 48 秒。按照预期，在 100 英尺位置，仅最远的客户端 ping 失败。虽然视频质量在所有客户端上都受影响，无线接入点还是检测到干扰并更改了信道。



Aruba 设备：

在 Aruba AP125 上运行相同测试。在位置 A 使用摄像头，Aruba 报告噪音级别为 -87dBm，频谱分析仪报告噪音级别为 -52dBm。虽然信道完全被干扰，但是未报告任何错误。由于没有达到噪音级别和错误阈值，因此无线接入点并没有更改信道，所有客户端都断开连接。

在位置 B 使用摄像头，远离无线接入点的客户端受影响，较近的客户端未受影响，原因在于信号噪音比。触发了噪音级别阈值，无线接入点在 2 分零 1 秒更改了信道。

在 100 英尺，噪音级别读取值为 -75 到 -77dBm，不够高而没有触发。远离无线接入点的客户端所受影响最大，整个蜂窝遭遇了高延迟和带宽下降。执行第二次测试噪音级别 -70dBm 触发了阈值时，在 10 英尺处未更改信道，在 50 英尺处花 2 分 10 秒更改信道，在 100 英尺处花 2 分 22 秒更改信道。

我们还对 Aruba AP105 的自行恢复能力进行了评估。基准噪音级别读取值为 -105dBm。该读取值太小，与同一环境中 AP125 的读取值 -87dBm 不符。在同时包括 AP105 和 AP125 设备的网络环境中，由于底噪音读取值互相不匹配，因此很难调节更改信道所需的噪音阈值。噪音级别必须超过阈值 120 秒才能触发信道更改。由于 10 英尺位置处视频摄像头干扰而导致客户端断开通信 30 分钟后，我们观察到这一不准确现象证明，噪音级别保持在阈值以上的时间长度不够而无法设置触发。我们还通过 CLI 接口发现无线接入点一直在重置无线电。

在 50 英尺位置处，所有客户端在摄像头打开后均无法 ping。AP105 报告噪音级别为 -74 到 -80dBm，但是在测试的 30 分钟时段内未更改信道。

在 100 英尺处，所有客户端在视频摄像头使用后均无法 ping。无线接入点上的噪音读取值为 -100dBm，客户端断开 30 分钟后，没有发现更改信道。我们试着将“非 802.11 抗干扰”设置从默认级别 2 提高到级别 5，但是所有五个客户端仍然无法 ping 无线接入点。

HP 设备：

HP 无线接入点的最短信道更改间隔为一小时。在 10 英尺处打开视频摄像头时，无线接入点失去与所有客户端的通信。一个多小时后，无线接入点还未更改信道，也未在事件日志中记录任何内容。在 50 英尺处，仅最靠近无线接入点的一个客户端在打开摄像头后还保持通信。一个多小时后，HP 还未更改信道或记录任何事件。按照预期，在 100 英尺处，四个客户端保持连接，仅最远的客户端受到干扰。一个多小时后，无线接入点还未更改信道。

Trapeze 设备：

Trapeze 默认扫描间隔为 3600 秒，最小扫描时间可设为 900 秒。距离视频摄像头 10 英尺处，所有客户端都断开连接，Trapeze 在 47 分钟后更改了信道。在 50 英尺处，一个客户端保持连接状态。一个多小时后，Trapeze 还未更改信道。我们注意到，噪音级别始终报告 -96dBm，不管阻塞干扰处于哪个位置以及距离视频摄像头有多远都是如此。在 100 英尺处，仅最远的客户端受到影响。一个多小时后，Trapeze 还未更改信道。

Motorola 设备：

Motorola AP-7131N 提供传统自行恢复以及 Smart-RF 功能。我们在无线接入点上启用了“自动信道选择”并修改了数据速率设置，以增加可用带宽并降低信道利用率，从而支持测试中所用的视频流。

使用传统自行恢复，无线接入点使用平均重试次数作为更改信道的触发阈值。在 10 英尺位置处使用视频摄像头，Motorola 报告 0 次重试。无法检测到任何干扰。客户端吞吐量太低，因此以科学记数法表示。一个小时后，无线接入点还未更改信道。启用并重新测试了 Smart-RF 功能，但是看到的结果相同。没有看到重试，并且未报告噪音级别。所有统计数字都归零。网络完全受到干扰，但是无线接入点未检测到这一点也未更改信道。

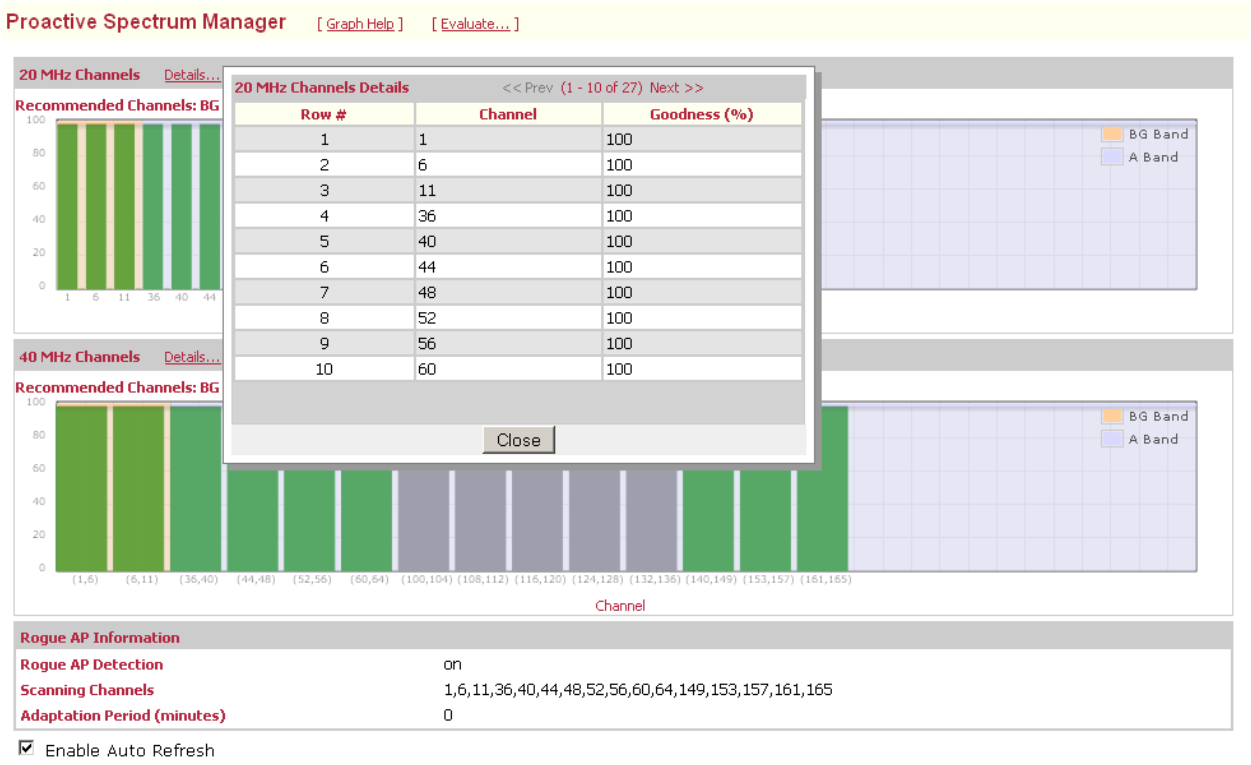
在 50 英尺处，重试平均数在 1 到 2 之间徘徊，未触发阈值。20 分钟后，信道还未更改，我们尝试强制 ACS 执行信道更改，但是什么也没有发生。

视频摄像头距离无线接入点 100 英尺时，仅最远的客户端受影响。噪音级别读取值为 -66dBm。一个小时后，无线接入点还未更改信道。我们尝试强制 ACS 手动切换信道，但是未成功。

Meru 设备：

Meru 的 AP320 使用主动频谱管理器 (PSM) 功能。它显示每个信道的“良性”级别。通过干净信道发送视频流时，由于利用率较高，PSM 报告信道为“欠佳”，但是当信道受到视频摄像机干扰导致利用率为零时，PSM 报告信道为 100%“良性”分数。

该 802.11n 无线接入点基本不支持 802.11 a/b/g 型号所支持的自动信道，也不支持自行恢复。PSM 按照用户定义的秒数每隔一段时间对信道进行评估，然后将工作站移动到干净信道。用于触发此更改的唯一阈值是出现欺诈设备。



视频摄像头完全干扰信道时所捕获的屏幕抓图。Meru 报告信道 100%“良性”分数，因为阻塞干扰表示 Wi-Fi 信道利用率实际上为 0%（来自 Meru 的信道质量评分）。Meru 不会改变信道，即使信道完全受到干扰且 Wi-Fi 无法使用时也是如此。

我们测量了 Meru 无线接入点上的相对噪音级别，以确定其准确性。Meru 测量了噪音级别 -82dBm 作为干净信道中的基准值。距离视频摄像头 50 英尺时，本底噪音读取值为 -85dBm。距离视频摄像头 100 英尺时，本底噪音读取值为 -71dBm。有关结果摘要，请参见第 18 页的*图 4*。

图 4：Cisco CleanAir 与其他竞争者之间的自行恢复测试摘要

	自行恢复时间						
无线接入点到干扰源距离	**思科**	**Aruba AP 125**	**Aruba AP105**	**Motorola**	**HP**	**Trapeze**	**Meru**
较近（10 英尺）	30 秒	从不	从不	从不	从不	47 分钟	从不
中等（50 英尺）	41 秒	2 分 10 秒	从不	从不	从不	从不	从不
较远（100 英尺）	48 秒	2 分 22 秒	从不	从不	从不	从不	从不
注意：		在较近位置，噪音保持在 -87dBm	噪音在每个位置不同，但始终不会保持超过更改阈值。	重试次数没有超过触发更改的阈值。	距离摄像头 50 英尺时，HP 发现噪音级别为 -70dBm。	噪音级别保持在 -96dBm。	信道“良性”始终保持在 100%。