Cisco CleanAir 技术：实际应用中的智能

本白皮书讲述广泛使用共享频谱所引起的射频干扰难题。它探究了标准 Wi-Fi 芯片设计的限制，以及该限制如何影响 IT 组织收集有关无线频谱的关键可操作数据，以便有效进行故障排除的能力。最后，它介绍了 Cisco® CleanAir 技术并说明用户如何通过将射频智能集成到网络，来充分了解无线频谱的实际使用。这很有必要，可以帮助主动管理 Wi-Fi 网络，以支持当今医院、分布式企业、制造工厂、零售商店和办公室所需的关键且对延迟敏感的应用。

Wi-Fi 变得至关重要

企业 Wi-Fi 网络设施的最初目的是为了在前厅或会议室上网提供方便。对于这些应用，“尽力而为”级别的性能即可接受。

如今，Wi-Fi 已发展成熟，部署到了许多关键应用中。医院使用 Wi-Fi 对患者病例进行移动访问，以及远程监控辅助床边系统。在零售业和制造业，Wi-Fi 用于物流和业务交易。小型分支机构开始将 Wi-Fi 用作网络访问专用方法，从而取代有线连接。而且，Wi-Fi 越来越多地用于对干扰影响很敏感的语音和视频应用。

在所有上述示例中，人们都希望 Wi-Fi 网络的运行具有极高的可靠性。人们无法再接受 Wi-Fi 网络由于干扰而意外停机。

定义解决方案

频谱智能 (SI) 是有关射频频谱活动的数据，该数据衍生自高级干扰识别算法，该算法与与军事中所使用的算法类似。频谱智能让您了解共享频谱的所有使用情况——Wi-Fi 设备和非 Wi-Fi 干扰源。对于在无需授权波段中工作的每个设备，频谱智能将显示：它是什么？它在哪里？它如何影响 Wi-Fi 网络？

频谱管理是指主动使用频谱智能数据，来提高 Wi-Fi 网络的性能，并降低其运营成本。可以利用有关干扰严重程度和持续时间的信息，来计算干扰对网络的影响，并对问题进行故障排除。另外，还可以将此信息存储起来，以便用于回溯分析和趋势预测。频谱管理是一个强大的主动式工具，它与物理位置和系统范围关联等环境数据相结合，提高了无线局域网的可靠性、性能和安全性。

外部或独立频谱智能工具已经存在了一段时间，思科则迈出了大胆的一步，将其直接集成到新的无线接入点的芯片集中。Cisco CleanAir 是一种革命性的技术，在业界尚属首例。使用该技术，IT 经理可以访问自动收集的关于每个非 802.11 干扰源的丰富频谱信息。CleanAir 技术提供的频谱智能支持全新级别的频谱管理。与以前的频谱管理工具相比，新的集成式频谱管理是无线网络结构的一部分，而以前的频谱管理工具则仅适应于其他 Wi-Fi 设备，并且通常与无线网络分离。第二代频谱管理可充分感知所有无线频谱用户，而且能够采取行动来缓解或避免干扰，从而优化网络性能。

性能和可靠性

除了了解干扰问题外，IT 还希望网络尽可能自动处理干扰问题，以便节省运营成本 (OpEx) 和最大限度地减少网络停机。这种类型的自动调整涉及到无线电资源管理 (RRM)，其属于基础架构中的软件层，可自动调整网络参数，以维护射频性能。较早几代的 RRM 除了能大致感知到“噪声”以外，大部分都感知不到干扰问题。而有了集成式 SI 之后，新一代 RRM 能够使用干扰源的详细信息，来进行真正智能的决策并实现全新级别的可靠性。

除自动 RRM 外，还可以在系统范围内使用集成式频谱智能，以完成更广泛的频谱管理任务。这对于 Wi-Fi 来说，可能是全新功能，但有线网络的管理者应该不会感到陌生：

- 实时排查性能问题
- 对间歇性或过去问题进行调查分析
- 报告使用情况和干扰趋势
- 跨多个无线接入点将干扰问题相关联，以集中处理产生的影响并减少过多的警告

无线安全性

最后，Wi-Fi 所面临的不单纯只是性能方面的挑战，也有安全方面的挑战。业界已经致力于了解欺诈无线接入点如何在企业网络中打开安全漏洞，且已经达到了很好的水平。目前，已经设计了无线入侵检测系统和入侵防御系统 (wIDS/wIPS) 来解决这一问题。但是，当前 IDS 和 IPS 解决方案还有一些重大盲点，如果不增加频谱智能就无法解决。

当前 IDS/IPS 系统无法检测以专有扩展模式（如 Super G，来自 Atheros）运行的无线接入点。这些随时可用的设备是检测不到的。此外，黑客还可能采用标准 Wi-Fi 设备（例如，运行 Linux）并对其进行修改，以使其在非标准信道上运行或以其他非标准调制方案运行。只有在您分析射频物理层以后，才能检测到这些扩展或修改的设备。

除 Wi-Fi 设备外，许多其他类型的非 Wi-Fi 设备（包括蓝牙无线接入点、运行较早标准（如 802.11FH）的无线接入点，以及专用无线网桥）也可以用于打开网络中的漏洞。对于网桥，这些设备可以将数据发送给距离您的大厦数公里远的攻击者。再重复一次，只有在您分析频谱上出现的所有设备后，才能检测到这些类型的设备。

除欺诈设备的威胁外，怀有恶意的人的威胁也始终存在，他们尝试利用射频拒绝服务 (DoS) 攻击，使您的 Wi-Fi 网络失效。虽然 IDS/IPS 系统能够监控许多“协议层”DoS 攻击，但它们检测不到可能通过干扰设备或 Wi-Fi 设备（这些设备在诊断干扰模式下设置）实施的射频层 DoS 攻击。

除有目的的攻击外，还有一些简单设备（如无线视频摄像头或模拟无绳电话）可能会意外导致网络陷于干扰之中。集成式频谱智能和频谱管理对确定射频级别 DoS 安全威胁的类型非常有效。

集成式频谱管理是如何实施的？

标准 Wi-Fi 硬件中的限制

在基础级别，标准 Wi-Fi 芯片集实施 SI 的能力有限。这是因为 Wi-Fi 芯片集的设计目的仅用于接收 Wi-Fi 信号——它们不能识别其他类型的信号（Dynamic Frequency Selection [DFS] 雷达除外）。标准芯片集的设计甚至不包括提供更多的信息，以便在更高级别的软件上进行频谱智能分析。

具体来说，当标准 Wi-Fi 芯片集看到无法理解的突发传输时，它一般仅能够报告几件事情：1) 发生了不可理解的突发传输；2) 突发的功率级别；3) 突发的开始和结束时间。请注意，突发可能实际上来自另一个信道上或同一个信道上的 Wi-Fi 设备，但由于太远而无法正确接收。或者突发可能来自非 Wi-Fi 设备。通常，我们无法获得有关突发的调制类型，以及它在信道内的发生位置等详细信息。而且，软件无法访问从突发接收的实际数据，以进行进一步的分析。

虽然存在这些限制，但可以使用 Wi-Fi 芯片来添加未经识别的突发，并计算干扰总量以及平均干扰强度。不幸的是，此方法不提供实际解决问题所需要的信息。例如，“总干扰”方法不能告诉您干扰的具体类型（例如，它不过是同频 Wi-Fi 干扰还是其他干扰？）、干扰是来自一个源还是多个源、干扰位于何处，等等。如列表所示，可以使用标准 Wi-Fi 芯片集收集到的 SI 级别非常有限。

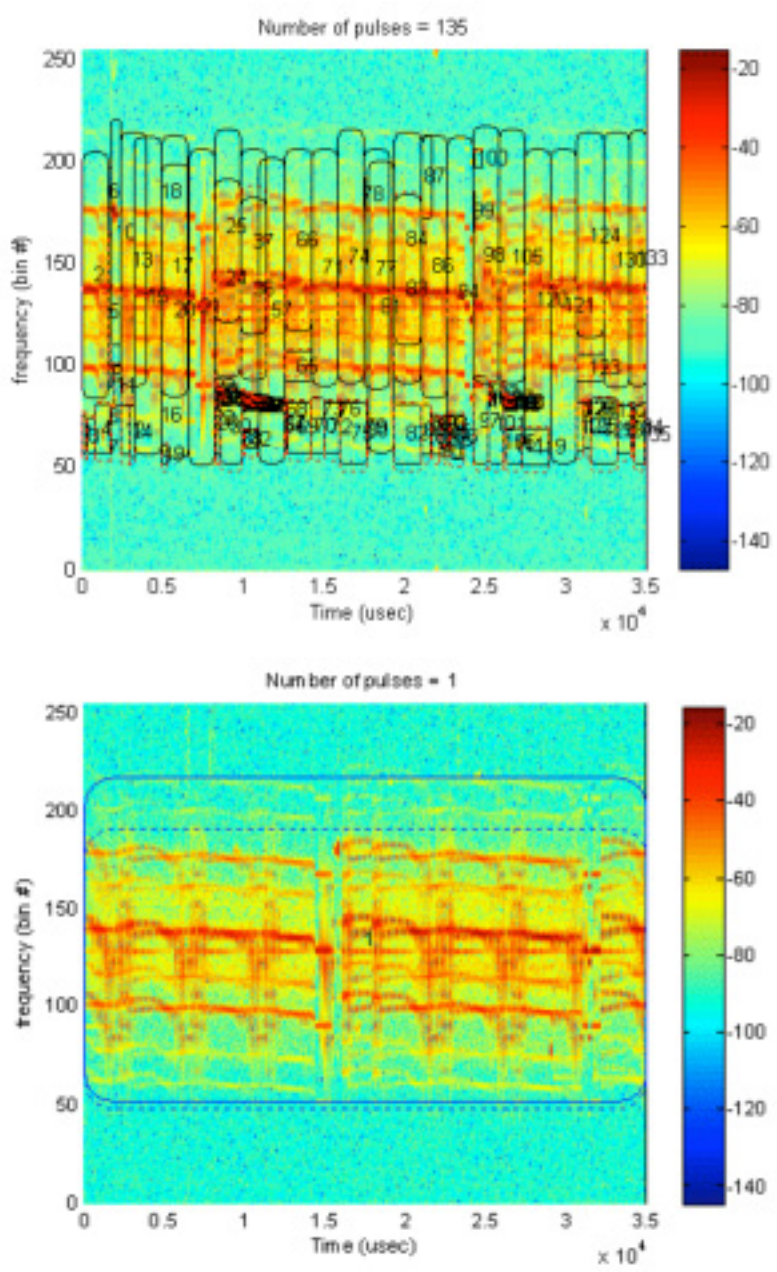
Cisco CleanAir 技术：定制化硬件/软件解决方案

为克服标准 Wi-Fi 芯片集固有的可见性限制，思科创建了含有专利芯片的集成式解决方案，以及专用于分析和分类所有射频活动的软件。（针对此项技术至今已签发了超过 25 个专利） 特别是，思科采用了 Cisco 智能频谱分析仪分析工具背后的技术，而且将其直接集成到基础架构中，包括在 Wi-Fi 芯片集内的深度集成。这是一项重要的发展，它表明无线网络已经在企业中从可有可无变成了至关重要。消费者等级的 Wi-Fi 硅片已不够好。

该定制化解决方案以 Cisco 频谱分析引擎 (SAgE) 硬件核心开始，该核心已直接集成到新 Cisco Aironet® 3500 系列无线接入点的 Wi-Fi 芯片集中。SAgE 核心处理是一项极为计算密集型的操作，如执行高分辨率快速傅立叶变换 (FFT) 和脉冲检测操作。（脉冲是频率和时间中的射频能量的突发）基本来说，SAgE 核心处理基本级别的频谱分析操作，这些操作是极为处理密集型的，因此在实时软件中可能会禁止处理它们。

图 1 以图形方式显示识别能量脉冲的 SAgE。第一个图像显示来自硬件脉冲检测器块的数据，第二个图像显示软件组合了多个脉冲之后的数据，这些脉冲极为匹配，以致可认为是单个脉冲

图 1. 在过滤之前和之后检测到的射频能量脉冲



完成 SAgE 处理后，有意义脉冲的无线电样本会传送到软件级别，以进行详细的指纹分析。在主无线电 CPU 上执行此处理会对 Wi-Fi 性能产生不利的影响。为消除这种影响，思科硬件解决方案包括一个自定义处理核心，称为 DSP 向量加速器 (DAvE)，它直接集成到无线接入点的 Wi-Fi 芯片集中。DAvE 核心能够执行密集型信号处理操作，这叫做“Davelet”（如过滤、多项消除、旋转、同步字检测和调制检测），而不会增加主 CPU 的负担。DAvE 处理 CPU 密集型信号处理操作，分担主 CPU 的负担。

最后的处理级别发生在软件模块中，该模块在主 CPU 上运行，称为“Sensord”。请注意，由于 SAgE 和 DAvE 硬件块完成了繁重的工作，因此 CPU 开销现在已非常低。Sensord 软件查看干扰突发的时间和频率，以及已发现的突发属性，如调制类型和已识别同步字等。然后，这种高级别信息被用来执行设备之间的最终识别和分隔。这个最终分类步骤提供强大的 SI 功能：告诉您干扰的具体来源、位置以及如何进行缓解。

SI 实施的性能方面

分类器的数量

CleanAir 技术包括 20 个强大的非 Wi-Fi 分类器。由于分析发生在软件中，因此，随着新的干扰源在市场中的利害关系日渐重要，分类器列表可能会扩展。换言之，只要更新软件，基础硬件解决方案即能够检测未来可能引入的任何种类干扰。

同时检测

CleanAir 技术分类能够区分多种同时运行的不同干扰源（相同类型或不同类型）。实际上，CleanAir 技术能够在每个无线电模块上报告 10 个同时产生干扰的设备。这很重要，因为实际的同时射频活动量可能会很高。与之竞争的解决方案无法提供这些高级功能，无法区分多个同时产生干扰的设备，就会很快在此领域败下阵来，只能供演示和实验室测试。

检测时间

干扰设备可能是瞬变的，因为它们可能快速打开或关闭，或者因为用户在不断走动。鉴于以上原因，必须在干扰转瞬即逝之际，快速对其进行分类。通过 CleanAir 技术，无线接入点可以在 30 秒内即对设备进行分类，而且往往不到 5 秒即可完成。（请注意，当跨多个无线接入点整合数据时，报告可能会略有延迟）

失误检测的可能性

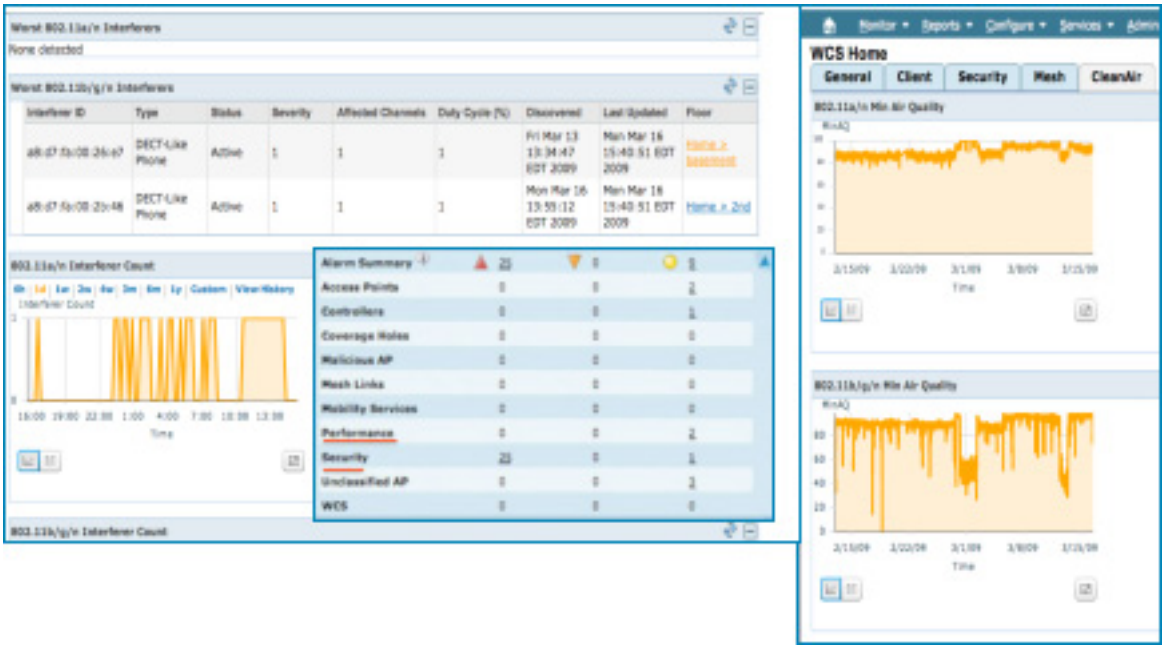
一定不要错过干扰源，这和在没有干扰或误标干扰时不报告“仿真”干扰一样重要，因为二者都会导致 IT 寻找错误的设备类型。CleanAir 技术专用于降低误检测率，即使在极为繁忙的射频环境中，有成百上千个 Wi-Fi 和非 Wi-Fi 设备在同时运行，也能做到这一点。通过降低误检测率，CleanAir 技术可节省 IT 时间。

CleanAir 技术：集成式频谱智能和频谱管理的重要性

虽然在部署网络之前，基于智能频谱分析仪产品和工具的解决方案扮演非常重要的角色，但将 SI 技术集成到 Wi-Fi 基础架构中则可提供更多竞争优势。在 CleanAir 集成式解决方案中，SI 引擎直接内置到无线接入点中，SI 信息完全集成到网络架构和管理系统中，从而实现智能频谱管理。

CleanAir 技术的优势是它能够全天候运行，不间断地监控有无干扰和空气介质质量问题（参见图 2）。这能让 IT 采用更为主动方法来管理频谱。IT 不用再等待最终用户报告干扰（以故障通知单的形式），然后调用工具来分析问题，而是在干扰发生时即刻找到它并立即采取措施。另外，全天候的历史记录可以进行回溯分析。使用历史数据，可以很方便地分析随时间的变化趋势。

图 2. 在思科无线控制系统中监控干扰设备、空气介质质量趋势和警报



能够跨无线接入点匹配检测到的设备

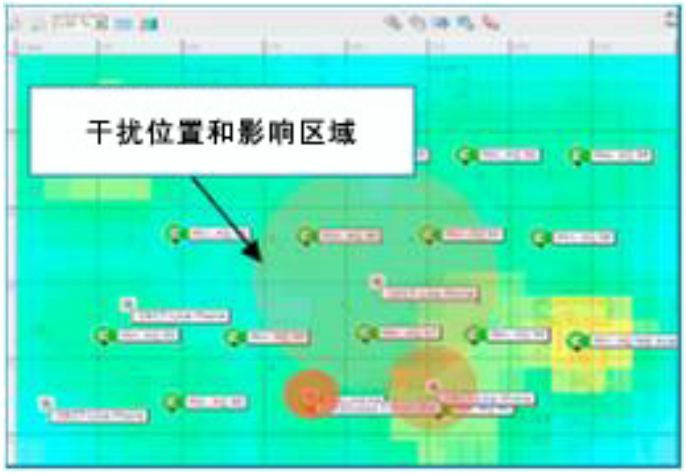
在采用集成式频谱管理的无线局域网中，很可能会在多个无线接入点中检测到同一个干扰设备。如果这些设备都分别进行报告，则会对管理员生成过多警报。有了 CleanAir 技术，就会根据设备属性为每个由无线接入点检测到的设备分配一个伪 MAC (PMAC) 地址。然后，跨无线接入点比较 PMAC。当两个设备的 PMAC 匹配（而且无线接入点彼此足够接近）时，来自这两个无线接入点的报告会“群集”到一起。现在，可以将群集作为单个设备报告给管理员。

群集在定位设备时也扮演重要角色。匹配的 PMAC 群集为系统提供同一设备的多个功率测量值，因此可以对设备的位置进行三角测量。设备群集的重要特征是网络能够正确地对设备进行群集处理，既不会过度集群化（将不应合并的设备合并到一起），也不会集群化不足（在仅有一个设备时报告多个设备）。

CleanAir 技术的第二个优势是它可以远程操作。对于许多 Wi-Fi 部署，一个位置的 IT 人员管理园区中多个建筑物内的设备或多个地理位置的设备，而且可能很难以物理方式使用一种工具来远程管理这些站点。如果部署涉及到许多分支办公室，或者干扰在本质上是瞬变的，这种情况尤为明显。通过将频谱管理集成到基础架构中，IT 能够在网络中的任何位置远程查看干扰条件。

Cisco CleanAir 技术还能够以物理方式定位干扰设备（图 3）。大多数情况下，多个无线接入点将会观察到同一个引发干扰的设备。思科已经开发了高级技术，对从多个无线接入点报告的设备进行比较，并确定哪些报告实际上是由同一个设备导致的。对设备进行比照后，可以使用三角测量法查明设备的准确位置，此方法和基础架构系统当前定位 Wi-Fi 客户端与标签所使用的方法类似。

图 3. 定位干扰设备及其影响区域



CleanAir 技术集成到无线局域网中的最大优势可能是：无线接入点 RRM 系统可以使用 SI 数据来实施全天候自动干扰缓解。这确实是下一代 RRM，与以前的版本相比，可以提供更大的可靠性，而以前的版本感知不到干扰。有了 CleanAir 技术，就可以将网络调整为自动规避许多类型的干扰。

思科统一无线网络与 CleanAir 技术结合所提供的功能

空气介质质量和性能警报

Cisco CleanAir 技术提供大量有关干扰的详细信息。但为了便于“大致”了解干扰问题在哪里影响网络，它会将详细信息累积成易于理解的高级别指标，称为空气介质质量 (AQ)。AQ 在信道、地面和系统级别进行报告，而且支持 AQ 警报，因此，当 AQ 低于预期阈值时，您会自动收到通知。

基于地图的可视化

在支持 CleanAir 技术的无线局域网中，已经过分析和检测的设备也会集成到思科无线控制系统 (WCS) 和移动服务引擎 (MSE) 管理系统所提供的直观映射显示中。除在地图上查看无线接入点和客户端外，您还可以在同一地图上跟踪干扰设备的位置。在性能方面，由于能够在地图上查看干扰设备（及其影响区域），因此您可以确定受影响的无线接入点、客户端和楼层空间。

从安全角度看，在地图上跟踪设备能让您立即知道应将安保人员派遣到哪里。

安全警报

除在地图上显示影响安全的设备外，您还可以按位置（例如，建筑物的特定某层）自定义警报。这是一种强大的功能，因为某些设备可能在建筑物的一些区域（例如，交易翼）内被认为是威胁，但在其他区域（如建筑物大厅）则不被认为是威胁。

缓解功能

除灵活的部署外，CleanAir 技术还提供高级的自动干扰响应。这些自动响应包括永久设备避免和事件驱动的 RRM。

永久设备避免可感知某些设备在位置和频率上倾向于静态，例如，微波炉和无线视频摄像头。鉴于此，即使当前未在特定位置的特定信道上检测到这些设备，也可以知道它们有可能返回到以前检测到它们的位置。系统会跟踪这类设备，在进行信道选择时，会尝试不选择已经观察到永久设备位置上的信道。

事件驱动的 RRM 可感知某些干扰事件在本质上是严重的和灾难性的。例如，具有连续 FM 信号的无绳电话可能会引发数分钟的故障（只要电话处于活动状态）。鉴于此，空气介质质量的急剧下降会使系统立即评估是否更改受影响无线接入点的信道。请注意，如果信道发生更改，则只是针对受影响无线接入点，从而避免对相邻无线接入点的信道计划造成关联影响。

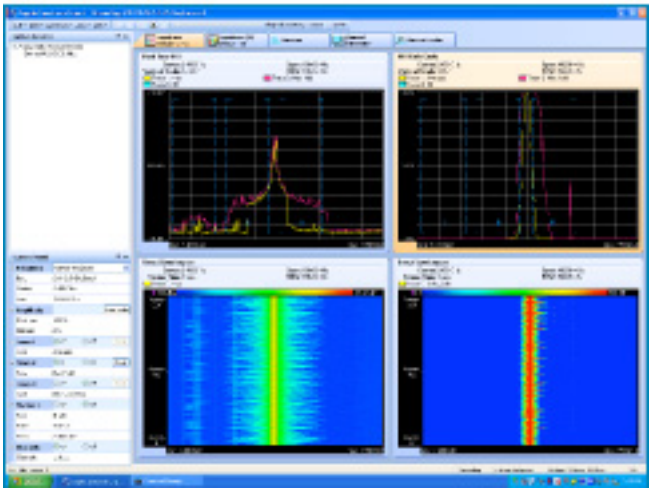
虽然在许多情况下，最佳干扰响应是管理员手动移动、移除、更换或屏蔽干扰设备，但更令人欣喜的是拥有自动缓解，它可以在采取其他措施之前，维护短期的性能。在某些情况下，可能无法移除干扰源，例如，如果它来自建筑物之外。

无线接入点充当分析仪

最后，CleanAir 技术继续从专家视角，提供可与智能频谱分析仪工具所提供的频谱图相媲美的低层物理级别频谱图。任何 CleanAir 无线接入点都可以配置为联网传感器，以便在无线接入点上的无线电接收到频谱图时可直接查看。

虽然系统确实可以提供大量的更高级别已分析数据（包括已分类设备和空气质量），但有时仍会需要实时查看原始频谱数据。即使对于没有内部射频专家的企业，也可以聘请外部专家，使用图 4 所示的频谱专家连接功能，来帮助解决极难诊断的问题。

图 4. 使用频谱专家连接功能诊断无线接入点的问题



结论

由于 Wi-Fi 在共享无需授权的波段工作，因此，要在 Wi-Fi 网络中支持高级别性能、安全性和可靠性，必须拥有集成式频谱智能和频谱管理。频谱管理对于在关键无线应用中为最终用户提供丰富、可靠的移动性体验至关重要。

由于商用 Wi-Fi 芯片集的有限射频可见性功能不能满足需要，因此思科集成了获得专利的频谱处理硬件和软件，专用于分析干扰，而且还创建了真正的企业级 Wi-Fi 芯片集。由于具有这种底层硅片功能，Cisco CleanAir 技术可对各个干扰源进行分类，并找出干扰源，告诉您它们如何影响网络性能或安全性。

虽然可以采用在部署前阶段很有用的工具（如智能频谱分析仪）来获取 SI，但最佳选择是将 SI 技术直接集成到基础架构中。Cisco CleanAir 技术提供强大的频谱管理功能，如全天候主动监控干扰、频谱安全与性能警报、远程管理和干扰设备位置。最重要的是，集成式 SI 支持全新级别的自动频谱管理，因此能够了解干扰影响，并以智能方式对其进行缓解。

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

美国印刷 C11-599260-00 04/10