无线干扰的20种错误说法：纠正错误说法以实现稳定高效的无线网络

随着无线设备的普及以及对于移动应用要求的提高，企业必须勤于管理规划整个部署。而有些已投入使用的或者新兴的无线技术和常用电子设备却影响了无线网络的运行性能。

其中RF干扰是最主要的影响无线网络运作的原因，它会影响安全性和无线网络的稳定性。

本文罗列了关于无线干扰问题的20种最普遍的错误说法。

错误说法 #1: “唯一的干扰来自于其他的802.11网络。”

802.11设备数不胜数，其他的802.11网络肯定会对你的网络产生干扰。这种干扰众所周知就是同频或临近频率的干扰，但是由于802.11设备都遵循同一个协议，所以他们是可以相互合作的——也就是说，同一个频率上的2个无线接入点分享频道容量。

但是实际上，在一个没有许可证限制的频段里，其他型号的设备数量远远超过802.11设备的数量。其他设备包括微波炉，无绳电话，蓝牙设备，无线摄像机，户外微波链路，无线游戏控制器，Zigbee设备，荧光灯，WiMAX等等，甚至一个坏的电气连接都可以产生非常宽的RF频谱。这些非802.11类型的干扰不能与802.11设备很好地相互合作，它们会大大降低吞吐量。此外，它们还会产生二次影响，比如降低速率，干扰导致的数据重传会误导802.11设备使用低数据速率而不是合适的速率。

总结： 无许可证的频段是FCC在共享不规则频谱内的一个实验。该实验到目前为止是一大成功，但是RF干扰还是构成了很大的挑战，仍需适当关注。

错误说法 #2: “我的网络似乎在工作，所以干扰不是一个问题。”

802.11协议被设计成在某种程度上可以抵抗干扰。802.11设备在数据传输前发现有干扰，它会暂停传输直到干扰消失为止。如果在传输过程中发生干扰（并且该干扰导致数据包不能正常接收），那么确认包收不到会使数据重新传输。最终数据包会全部通过。但是，暂停或者重新传输数据会严重影响你的无线网络容量和性能。

例如，微波炉会产生占空比是50%的干扰（由于它们根据60-Hz的交流电循环）。这意味着微波炉和你的802.11无线接入点频率一致，会降低50%的网络容量和性能。所以如果你的无线接入点速率设计是24Mbps，在正使用的微波炉周围可能只有12Mbps。如果你的无线网络上的应用只是接收数据（比如上网浏览），那么吞吐量的损失可能不会感觉很明显。但是如果你使用容量和延时敏感的应用，比如无线语音，那么控制干扰会变成一个重要问题。

总结： 干扰无处不在，它目前只是一个无声的杀手罢了。

错误说法 #3: “在部署前我做了一次RF清理，所以我发现了所有的干扰源。”

一个最头疼的干扰问题就是干扰总是间歇性的。可能干扰只在一天或一周的某个时间发生——比如某人使用诸如无线耳机的时候。所以，除非持续清理，否则很容易遗漏一些干扰源。即使持续清理（比如在每个地方进行24小时测试），周围的事物还是会随着时间而变化。一些工作在无需许可证频段的设备很容易会进入到你的网络环境中。周期性清理次数再多也不能保证你有一个完全没有干扰的环境。

总结：清除干扰问题是不可能的。微波炉，无绳电话，蓝牙设备，无线摄像机，户外微波链路，无线游戏控制器，Zigbee设备，荧光灯，WiMAX等等，甚至是坏的电气连接——所有这些都可以产生RF频谱。这些非802.11设备都不能和802.11设备一起相互协作。

错误说法 #4: “我的基础架构设备自动检测干扰。”

一些新型的，基于交换机的无线基础架构产品能够在一定程度上管理RF干扰。802.11芯片可以检测到非802.11信号，然后改变干扰区域内无线接入点的802.11频道。但是这个功能有一个问题，就是他不能解决区域外的问题。一些干扰设备——例如蓝牙设备，无绳电话，802.11 FH设备，人为干扰信号等，都是宽频的，而且他们无处不在，所以改变频道并不能避开这些设备。即使对于一个运行在固定频率的设备，要在一个基于蜂窝的大网络里管理频率也是很困难的。所以，分析干扰源，确定设备性质，所处位置然后确定如何解决干扰才是最关键的。在很多情况下，最好的解决方法就是将设备拿走。有的时候，将设备移动或者屏蔽它，避免干扰信号影响到网络也是一个不错的选择。

总结： 简单的，对干扰能够自动反应的产品是十分有用的，但是你也需要对潜在的问题有一定的了解。

错误说法 #5: “只要我使用高密度的无线接入点我就可以克服干扰。”

由于802.11无线接入点并不昂贵，所以很多人倾向于将其部署得非常密集。例如，一些网络中每个房间里面都设置了一个无线接入点。这种部署方式通过频谱的空间复用大大提高了网络的容量和性能。似乎周围无线接入点覆盖越多，即使有干扰，设备运行也可以非常正常地运行。

事实上，你将无线接入点部署得太过密集的话，你就必须降低信号传输的功率。如果不降低功率，各个无线接入点之间就会相互影响，这个情况就是我们大家熟悉的同频干扰。降低无线接入点的功率确实会抵消潜在的干扰免疫的优点。所以高密度的无线接入点的网络并不一定比低密度的部署好。

总结： 为了容量而特别设计你的网络是合理的，但是高密度的无线接入点并不是解决干扰问题的万能药。

错误说法 #6: “我可以使用数据包探测器分析干扰问题。”

802.11数据包探测器与无线网络的基础架构设备面临的问题是一样的：他们只能看到802.11芯片告诉它们的东西。他们可以告诉你干扰的次级问题，比如增加的重新传输的次数，较低的数据速率等，但是它们不能分析干扰的问题，确定干扰的原因，也不可以帮你找到干扰设备的位置。

802.11芯片的第二个问题就是功率测量通常都不够精确。这意味着根据802.11芯片上接收到的以dBm为单位的数据不能准确可靠地判断出无线接入点（或其他设备）的信号强度。所以仅凭数据包探测器的数字很难判断到底情况如何。

总结： 你需要正确的工具来分析干扰问题。最终，能够分析干扰源从而确定最好的解决干扰的方法是非常重要的。很多时候，最好的方法就是将干扰设备移去。

错误说法 #7: “我有一个无线策略，可以不允许干扰设备进入。”

定义无线策略是解决干扰问题的良好的第一步。但是如果没有实施，有策略也是徒劳的。无许可证频段的最大特点之一就是它不贵并且应用广泛。所以，员工很容易买这些设备并且把他们带到工作场所。很多情况下，员工根本没有意识到他们带了可能产生干扰的设备到无线网络里。有的设备，比如无绳耳机，微波炉，是办公室的必需品，也不可能被完全禁止。

总结： 不要奢望干扰设备会在你的环境中销声匿迹。

错误说法 #8: “5GHz的频段内没有干扰。”

与2.4-GHz设备相比，会造成干扰的5GHz的设备的确比较少，但是这个情况也是会改变的。就像每个人都从900 MHz 转到2.4 GHz 来避免干扰一样，5 GHz也会遇到同样的情况。无绳电话，雷达，周边感应器，数字卫星等一些设备已经使用5GHz频段了。

总结： 你可以逃，但是你躲不掉。

错误说法 #9: “我可以找一个顾问来解决所有我遇到的干扰问题。”

如果你使用无线网络一段时间，你会发现你的网络时不时地会运行不够好。没有亲眼看见，你只能猜测是不是干扰的问题。IT人员面临的一个问题就是不能亲眼所见，特别是当CEO问道为什么昨天会议室的网络连接有问题的时候。除了不能控制以外，找一个顾问来诊断这些问题也费时费钱。一次上门服务，出差汇报要花费大约5000到10000美元。

总结： 找第三方来解决网络问题费用太高。

错误说法 #10: “我放弃了，RF根本不能理解。”

不要绝望。现在有一些工具可以让RF变得更加容易理解，即使那些自认为是有线网络专家但却不是无线专家的人也可以理解。例如，思科Spectrum Expert Wi-Fi能将干扰分类，所以你不需要读懂那些曲线。当我们确定了干扰种类，我们会帮助你找到并且清除它们。

总结： 解决问题的方案在思科这里呢！

错误说法 #11: “Wi-Fi干扰不经常发生。”

越来越多证据显示，Wi-Fi干扰其实很常见，并且很难解决。这里有一些最近的例子：

- 来自Wi-Fi基础设备厂商的技术工程师们向思科汇报说，最近他们对一个大客户进行电话回访时发现该客户找到有大约20种干扰源，其中50%来自客户自己的Wi-Fi网络中。
- 一个大型无线服务外包商经理向思科反映，他的技术员接到的电话中，每3个Wi-Fi问题里面就有一个是关于干扰的。
- 一个大型Wi-Fi工具供应商在最近一次针对300位他们的客户的调查报告显示，诊断干扰问题是他们管理Wi-Fi网络面临的最大挑战。
- Jupiter Research报告说有67%的居民的Wi-Fi问题和干扰设备有关，这些干扰设备包括无绳电话，婴儿监视器，微波炉。

总结： 请不要逃避：Wi-Fi干扰确实存在。

错误说法 #12: “在排除了其他问题可能性的情况下，我才需要检查干扰问题。”

任何网络系统的物理层都是固定的。如果物理层工作不正常，高协议层就会工作效率低下或者工作不正常。由于这个原因，我们通常是先确认物理层的情况，然后再去检查更高层面的问题。

以此类推，当你的电脑插入了以太网线，可是网络却不能够运作，你检查的第一步就是查看以太网适配器上的灯是否亮起。如果灯不亮，那就没有必要去进一步检查网络配置问题，因为你的物理层的连接出问题了。

Wi-Fi方面潜在的物理层问题比以太网更加严重。物理层是否连接上这个问题只要在第一次插入以太网线时考虑。如果第一天可以正常工作，那么以后都应该可以正常运作。但是在RF环境下，物理层连接的质量每个小时都在变化，因为会有人为地带入其他设备影响这个网络环境。

总结： 为避免浪费时间，首先要检查RF物理层。

错误说法 #13: “即使我找到了干扰，我也不能做什么。”

最常见的解决干扰的方法就是更换或移去干扰源。比如，你可以更换旧的有微波泄漏的微波炉或者把2.4-GHz无绳耳机换成并非工作于Wi-Fi频段的其他型号产品。很多时候干扰是由好心的员工无意间造成的。某个Wi-Fi管理员发现一个背对门坐的员工带了一个无线摄像机，这样他就可以看到他背后的东西。可是这个摄像机是工作在2.4GHz的。在这个情况下，需要制定禁止这类设备出现在园区内的策略。

还有一个办法就是移动在干扰设备周围的无线接入点，或者将无线接入点的工作频率改到不受设备影响的频率上。一旦你知道了干扰设备的位置和频率参数，这个解决方法很容易做到。必须注意，有的设备（如蓝牙设备）是跳频的，所以要改变工作频率来减少干扰是不可能的。

最后一种解决方法是移去或者屏蔽干扰源。例如，在医院里，产生RF干扰的设备可以被隔离在一个没有Wi-Fi网络需求的特定房间。如果不能隔离，那么用电磁干扰（EMI）屏蔽设备可以将干扰限定在一个小区域里。你可以使用接地的屏蔽网或者在墙内加金属箔（本质上就是Faraday cages）或者绝缘涂料来达到屏蔽的目的。

总结： 只要你知道了干扰的源头，总会找到解决的方法。

错误说法 #14: “只有一些很容易发现的设备会干扰我的Wi-Fi网络。”

无许可证频段中的无线设备数不胜数，什么设备会是干扰源已经不再明显——无线连接现在存在于手表，鞋子，MP3播放器和许多小的消费品内。

有些情况下，一些设备升级到了采用RF技术。动作检测器就是一个很好的例子，它作为声控电灯的一部分被用于很多办公室内。一种新型的混合动作检测器使用被动红外传感器（PIR）和2.4-GHz雷达来探测动作情况。这些设备安装时初始的目的是好的，但是现在对于Wi-Fi网络却有较大的干扰。

一些不经意的发射器也很难被发现。荧光灯上有问题的镇流器也会产生宽频的RF干扰从而影响Wi-Fi网络。仅简单地检查设备是发现不了问题的。“隐藏的设备”现在也越来越常见了。我们看到很多例子，比如安全部门安装隐藏摄像头——网络部门不知道——这些设备就在不知不觉中影响Wi-Fi。

总结： 你需要正确的工具快速找到干扰，而不是一面放大镜。

错误说法 #15: “当干扰发生时，对于数据的影响通常是非常轻微的。”

一个干扰源对Wi-Fi网络的数据吞吐量（或数据容量）的干扰可能是非常惊人的。

主要有3个要素来确定干扰设备的影响大小：

- **输出功率。** 输出功率越大，干扰设备产生的物理“干扰区域”越大。
- **信号行为的时间特性。** 模拟设备，比如摄像机和旧的无绳电话，有一个恒定的表示在线的信号。数码产品，比如数字无绳电话，趋向于开启和关闭信号。不同的设备在线和下线信号间隔都不同。总的来说，在线信号的时间百分比越大，发送越频繁，对于吞吐量的影响就越大。
- **信号行为的频率特性。** 有的设备以固定频率运行，影响特定的Wi-Fi频率。有的设备跳跃于多个频率，影响每个频道但是影响程度相对比较小。有的设备比如微波炉，干扰发射机，快速地扫过整个频谱，对于很多频率造成简短但是严重的中断。

Farpoint Research最新的一个研究中，测量不同干扰设备对Wi-Fi数据吞吐量的影响。离无线接入点或者客户端25英尺的微波炉会降低64%的数据吞吐量，同样位置如果放置一个跳频电话，数据吞吐量降低19%，模拟电话和摄像机会导致降低100%（也就是说，不能连接）。

总结： 干扰的确会影响Wi-Fi网络的数据吞吐量。

错误说法 #16: “语音传输的速率很低，所以干扰对Wi-Fi语音的影响应该是最小的。”

使用现代语音编码，个人的语音电话使用的数据速率为8Kbps。和Wi-Fi网络的最大吞吐量相比，这个是小巫见大巫了。所以似乎一个Wi-Fi无线接入点可以很容易同时承载多个VoIP电话。

然而，很多因素会影响无线接入点承载电话的数量。第一，有大量VoIP协议层的包头，会增加数据流达到100Kbps的流量。此外还有Wi-Fi额外的协议包头。第二，语音流量对抖动和延迟非常敏感，需要网络上预留大量带宽以减少网络拥塞情况。一个Wi-Fi无线接入点上推荐的语音电话使用数量为15个。如果有干扰的话，可使用的电话数量会相应减少。

此外，有少量的干扰会严重影响无线语音电话的质量。Farpoint Research最新的一项研究中，测试不同的干扰设备对于无线语音电话通话质量的MOS值的影响，发现当有微波炉，无绳电话，摄像机或者同频Wi-Fi设备在无线接入点或者无线话机的25英尺内时，话音质量几乎不可以接受。更重要的是，干扰会产生信号覆盖的空洞，语音会中断掉。一个室内研究显示，在无线接入点75英尺范围内有干扰源（无绳电话或摄像机）时，会使无线语音的有效范围降低50%。无线语音的范围降低50%相当于整个楼层的75%以上的空间产生了信号覆盖空洞。

总结： 你能听到我吗？无线语音与干扰不能共存。

错误说法 #17: “干扰会影响性能，而不是安全问题。”

如果一个网络蠕虫病毒突破了你的防火墙，占用了50%的网络带宽，在一台台电脑之间传播，那么你认为这是个安全问题还是性能问题？重点就是任何影响核心IT网络系统的问题就是安全问题。公司Wi-Fi网络变得越来越关键的情况下，任何干扰的设备——不管是恶意的，如干扰发射器，或者是偶然的——都应被视为潜在的安全问题。除了RF拒绝服务外，还有其他一些非Wi-Fi RF设备相关的威胁，包括：

- **多协议设备。** Wi-Fi网络通常都设置安全接入控制，但是运行在非Wi-Fi网络的设备（如蓝牙设备）就没有安全接入保护。一个带有Wi-Fi及蓝牙连接的笔记本会像桥一样，会让入侵设备进入到局域网或无线局域网。要防止不安全的网络与公司网络意外连接，需要：1）基于客户端的工具，控制无线网络接口的配置。2）RF检测器，用于检查可疑的可能造成桥接的非Wi-Fi活动。
- **非Wi-Fi的rogue设备。** 大多数企业都会采用Wi-Fi的rogue无线接入点探测设备来发现公司网络中未授权的（和不安全的）无线接入点。但是非Wi-Fi设备（如蓝牙接入点）会造成类似的安全漏洞。像Wi-Fi的rogue设备一样，这些设备也必须被检测出来并清除掉。

- **敏感数据泄漏。** 某些非Wi-Fi设备如照相机，无线电话在旁路了公司的安全策略后会可以将敏感的数据带出限制区域。如果涉及到这样的问题，就必须在区域内限制无线网络的运行，该区域必须进行频谱监控，找出未授权的设备。

总结： RF的安全性问题不会因为Wi-Fi网络的停止而停止，你知道谁正在使用你的频谱吗？

错误说法 #18: “802.11n及其天线系统能在任何干扰情况下运行。”

使用多根天线或智能天线的系统可以通过加强接收器上的有用信号来提高干扰免疫能力。如果有用信号强了，那么信噪比（SNR）也会增加，这样能有效地缩小干扰设备干扰的区域范围。不过智能天线系统所获得的增益通常只是增加了10 dB的信号强度。这就意味着相对于传统的天线系统，干扰的范围会缩小2倍，但是这离解决干扰问题还是很遥远。比如，如果一个干扰设备以前会在离接收器80英尺的位置上有影响，现在就是在40英尺范围内有影响。那么在楼层空间内，5000平方英尺的范围还是有干扰的问题。

总结： 天线可以缓解问题，但不是解决问题的方法。

错误说法 #19: “我的现场勘测工具可以用来找到干扰问题。”

标准的Wi-Fi现场勘测工具是用于测量Wi-Fi信号的覆盖情况的。当你在大楼里走动时，Wi-Fi芯片能测量出无线接入点信号的强度。但是Wi-Fi芯片只能用于看Wi-Fi信号，不能告诉你来自非Wi-Fi设备的干扰信号。（Wi-Fi数据包分析器也有同样问题）。Wi-Fi现场勘测工具能够监测到非Wi-Fi信号的大致位置，但是不能帮你确定干扰源的特性，设备类型或者位置。所以你的问题还是解决不了。你确实需要一个RF层的工具来诊断干扰的问题。有一个好消息就是很多下一代Wi-Fi现场勘测工具会更完善地集成RF层的工具，以提供一个完整的解决方案。

总结： 现场勘测工具测量的是信号覆盖，但是并不能满足你的RF层面的需求。

错误说法 #20: “RF分析工具都太庞大并且太昂贵了。”

许多RF分析工具 （如庞大而昂贵的频谱分析仪）都不适合企业应用。

但是思科的RF频谱分析工具，设计得既满足你期望的外形 （插入笔记本电脑的小型卡片），又满足你的IT预算。更棒的是，思科的智能频谱解决方案使你不需要成为RF专家就能解决干扰问题。

总结： 更多关于思科智能频谱解决方案的信息请访问：
http://www.cisco.com/en/US/products/ps9393/index.html

结论

关于阻碍高性能及可靠的无线网络服务的障碍物有很多错误的说法。对于Wi-Fi干扰问题的误解成为许多错误说法的基础，就如人们相信要看清RF频谱的问题很困难并且成本很高。实际上，要看清RF频谱问题非常困难且昂贵这一说法是所有错误的说法中最为严重的一条。

思科的统一无线网络支持实时的无线网络智能频谱分析。行业领先的解决方案，能够在无许可证的2.4-GHz 和 5-GHz的频段内，检测，分类并且定位产生RF干扰的设备。

更多关于管理无线干扰方法的信息，请访问思科RF解决方案的网页：
http://www.cisco.com/en/US/netsol/ns736/networking_solutions_package.html

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.**

Printed in USA **C11-449271-00 12/07**

