无线协议学习指南

无线协议学习指南

无线协议和技术总是在变化——越来越影响我们的通信方式。目前无线网络部署仍然只是企业网络的许多部分之一。随着协议和技术的改变，如果预言成真，无线网络可能最终完全替代有线网络。然而，为了应对这些变化，管理员应该考虑无线网络需要做什么样的计划和部署。通过解释无线协议和技术——包括 802.11 及其部署、无线接入端、安全性和故障修复问题，本文鼓励 IT 专家考虑无线技术带来的正在快速靠近的变化。了解无线技术，包括它们工作的方式以及领域的发展方向，这些重要基础知识是最适合你开始理解无线技术的。

无线协议定义与规范

无线是一个描述电子通信的词汇，它是由电磁波 ——而不是某种导线的形式——将信号传输到部分或所有通信路径上。随着电视、传真、数据通信和更大范围波谱的有效使用，“无线”这个词汇开始流行了。

- ❖ 无线协议定义与规范

802.11n 协议

当谈到无线网络时，很多人都会想到 802.11 协议——以及特定方式工作的频道，理解这些协议的信号进出和它们是如何影响无线网络是非常重要的。本节将会对当前使用和企业正在考虑的主要的 802.11 协议进行概括说明。

- ❖ 802.11 协议

无线接入端配置

安装无线接入端是建设无线网络中的一个棘手的工作。因为其中需要考虑的方面很多，如决定哪些无线协议能在企业中发挥最佳性能、安装合适的 AP 和保证 AP 不会互相干扰或者干扰其它设备。本节将提供关于 WAP 的采购、安装和配置的专业建议。

- ❖ 无线接入端安装
- ❖ 无线接入端配置

无线网络部署与管理

部署无线网络可能是一个困难的任务，而且在部署完成后，它还需要进行管理以维持高效的运作。本节将讨论无线网络部署的准备工作，包括网络和协议分析以及无线网络的管理和监控。

- 无线网络部署
- 无线网络管理

无线安全

保证无线安全可能对于实际的部署或延续企业无线网络使用而言仍然是一个阻碍。本节将讨论无线网络的监控和安全策略，以及讨论一些可以增强无线网络安全的工具和配置。

- 无线安全监控和策略
  - 无线安全工具和配置

无线故障修复

修复无线问题可能需要大量持续且未知的支持——特别是在了解了所有这方面专家的建议以及花费大量时间准备和规划网络之后。本节将探讨如何处理无线连接问题、调试和无线容量规划。

- 无线故障修复

无线协议定义与规范

无线技术定义

无线是一个描述电子通信的词汇，它是由电磁波——而不是某种导线的形式——将信号传输到部分或所有通信路径上。第一台无线电发射器出现在 20 世纪早期，它使 用的是无线电报（摩尔斯电码）。后来，调制技术使得通过无线传输声音和音乐成为可能，这种无线媒体被称为无线电广播。随着电视、传真、数据通信和更大范围 波谱的有效使用，“无线”这个词汇开始流行了。

无线技术正在快速发展，并且在全世界人们的生活中扮演越来越重要的角色。无线使用的增长催生出了各种技术和设备。另外，许多人都直接或间接地依赖这个技术。

无线接入技术通常基于速度和距离分成以下几类：

•**无线个人网（WPAN）**技术有效范围仅仅有 10 米左右。红外线（IrDA）和蓝牙（Bluetooth）是两个常见的技术。这个领域的新兴技术还有 802.15.4a (Zigbee) 和 802.15.3c (UWB)。

•**无线局域网（WLAN）**技术最高支持 100 米范围的 200 Mbps速度。其中 802.11a/b/g (Wi-Fi)是最广泛使用的技术。这类技术的新兴技术包括特许的MIMO产品和新的 802.11n高速WLAN标准。

•**无线城域网（WMAN）**技 术支持跨越几公里的无线“第一哩”链路并最高达到 75 Mbps速度。在WiMAX商标认证下的 802.16 Broadband Wireless Access WMAN标准已经有了几个迭代。目前稳定的WiMAX已经有了新的补充，它就是新兴的 802.20 Mobile WiMAX标准。

•**无线广域网（WWAN）**技 术目前可以跨越大型服务区域，如城市、地区，甚至国家并支持高达几百Kbps速度。通常部署的WWAN技术包括GSM/GPRS/EDGE和 CDMA2000 1xRTT。这些服务逐渐补充了一些新的第三代技术，如UMTS/HSDPA和 CDMA EV-DO Rev.0/A。其中，在不久的将来还将包括HSUPA和EV-DO Rec.C等技术。

在无线局域网（WLAN）中，一个移动用户能够以无线方式连接一个局域网。无线个人网（WPAN）则是一个个人区域网络，它用于以个人工作区域为中心实现无线方式的设备互连。虽然目前的 IrDA and Bluetooth 已经很先进，但 WPAN 技术仍然在快速发展中。

协议和规范

Wi-Fi 是一个描述使用 802.11 族规范的特定类型的 WLAN 的词汇。Wi-Fi 是由 Wi-Fi 联盟创造的，这个联盟负责监督验证产品互操作性的测试。通过 特定位置的 Wi-Fi 来提供公共 Internet 连接的一个无线 LAN 节点被称为一个热点。许多机场、酒店和快餐店提供了 Wi-Fi 网络的公共访问。

无线工业联盟 WiMAX (Worldwide Interoperability for Microwave Access)负责改进用于无线宽带接入的 IEEE 802.16 标准，有时它也称为 BWA、网络。WiMax 支持最大 30 英里的范围，实现了提供商网络可靠的最后一哩无线方案。

蓝牙是一个电信工业规范，它描述了移动电话、计算机和 PDA 是如何能够简单地通过一个短距离无线连接实现互相连接。超宽带无线技术（也称为 UWB 或数据脉冲 无线）是一个将大量数字数据传输到一个宽频段的无线技术，它在短距离中（最远 230 英尺）消耗非常少的功率，它在传递信号时能穿越门和其它障碍物，而这些 障碍物能够反射更大带宽范围和更大功率的信息。

WAP (无线应用协议，Wireless Application Protocol)是一组通信协议规范，它能标准化用于 Internet 访问的无线设备。Wired Equivalent Privacy (WEP)是一个安全协议，包含在 IEEE Wi-Fi 标准：802.11，它是设计用来提供带有与有线网络类似的安生和隐私机制的 WLAN。另一个配备 Wi-Fi 无线连接的计算机用户安全标准是 Wi-Fi Protected Access (WPA)。它对原始 Wi-Fi 安全标准 WEP 作了改进，并预计会替代 WEP。

802.11 是 WLAN 规范的一个改进协议族，它是由 Institute of Electrical and Electronics Engineers (IEEE)的一个工作组所开发的。这个协议族中有几个规范，并且有时候会有新的规范加入。

由于这些规范还没有被正式认可或部署，802.11x 指的是一组进化中的 WLAN 标准，它作为 IEEE 802.11 协议族的元素目前仍然在开发中。802.11 规范总结在 802.11 Fast Reference 中，其中包括了每一个规范的定义的链接。

(作者：SearchNetworking.com 来源：TechTarget 中国 译者：陈柳，曾少宁)

802.11n 协议

当谈到无线网络时，很多人都会想到 802.11 协议——以及特定方式工作的频道，理解这些协议的信号进出和它们是如何影响无线网络是非常重要的。本节将会对当前使用和企业正在考虑的主要的 802.11 协议进行概括说明。

802.11 协议

如果询问熟悉无线网络的人：802.11a、802.11b 和 802.11g 之间的区别是什么？他们将会提到数据传输率，当然具体会是关于最大为 11 Mbps（a）到 54 Mbps（a 或 g）。

但是不同的 802.11 标准在不同的频道有不同的工作方式，因此理解不同的协议影响网络的方式是很重要的。

802.11a 是 802.11 协议族中的几个 WLAN 协议之一。802.11a 是用于无线 ATM 系统标准，并用在接入集线器上。

802.11b 也是一个 WLAN 标准——通常称为 Wi-Fi，它也是 IEEE 的 802.11 WLAN 系列标准的一部分。802.11b 向下兼容 802.11。它也定义了相差 5 MHz 的频道，并且它的频率位于 22MHz 频道的中间。

802.11g 是一个 WLAN 的标准，它支持相对较短的传输距离，并且最高传输速度为 54 Mbps，比更早的 802.11b 标准的理论最大值 11 Mbps 高很多。与 802.11b 相似，802.11g 规范也定义了相差 5MHz 的频道，并且每个定义的频率都位于 22MHz 的频道中间。

草拟版 802.11n 标准定义了 2.4 和 5 GHz 频带的 20MHz 频道，以及一个把两个 20MHz 频道整合为一个 40MHz（控制+扩展）频道来增加吞吐量的选项。

对于网络设计人员，还有另外一个重要方面要考虑——不重叠频道。802.11b 和 g 只有三个不重叠频道，这意味着你只能在同一个区域放三个 WAP 才不会互相干扰，而 802.11a 有不重叠频道。（注意这数字是在美国的，其它国家可能不一样。）

802.11 无线部署

在考虑现有的无线部署时——这几乎总是对现有 LAN 交换部署的补充，我们还需要考虑当前运行的协议。许多单位已经部署了 802.11b 硬件，并且现在想要转 为 802.11g。众所周知，许多硬件模块都可以升级到 802.11a 或 g，鉴于它也是一个相当新的规则，所以我们可能会尝试直接升级到最新版本 g，并保 留 WAP。这里建议避免这样升级，因为

没有必要为所有环境做最好的升级。相反，我们应该考虑先做新位置测试，并考虑在较高用户密度位置上使用 802.11a。

通过更多的不重叠频道，我们将可能发现更高效管理频率与覆盖面积，特别是可以在之前因为重叠问题无法安装 WAP 的地方重新安装 WAP。而且我猜想用户注意到的网络性能改进更多是由于抢占减少（特定 WAP 上的用户减少）带来的，而不只是数据传输速率引起的。

随着 802.11n 逐渐得到认可，更多企业也正在考虑新协议对于他们的 Ethernet 和 WLAN 的好处。急于发布 802.11n 产品的供应商已经测试了他 们的兼容草拟版 802.11n 标准的硬件。随着时间的推移，802.11n 是必然出现的，企业也应该仔细考虑什么样的无线方案能继续给他们带来好处。

考虑 802.11n

即将出现的 IEEE 802.11n 无线标准将支持高带宽应用，如流媒体与 VoIP。而该协议的最终完成和认可可能需要到 2008 年年初，IT 管理人员现在可以开始考虑新标准将对新标准发挥最大作用的现有网络和环境的影响。

当前版本的标准承诺的数据传输速率高达 540 Mbits/秒。典型的吞吐量应该在 100 到 200 Mbits/秒的范围之间，随着技术的成熟这个速率还可能有进一步的提升。IEEE 802.11n 的吞吐量增加将会影响到整个网络的性能，而不仅仅是无线部分。100 MB 的 Ethernet 足够承载来自于 802.11g 接入端（AP）的流量，但 802.11n 会要求 GB 级连接。为了处理更高数据传输速率而对网络进行升 级将会影响到整个网络，即使大多数 802.11n 产品能够通过降低速率到 802.11g 级别来兼容运行在相同频道的 802.11g 设备。但是，速度的降低 将影响整个无线网络，而非只是 802.11g 设备。

802.11n 的速度增加是通过使用 MIMO 技术实现的，这是一个更宽的无线电频率的频道，也是减少传输时间的方法。每个天线发出的信号从发送端到达接收端的传输路径是不相同的。它们会受到路径上的障碍物影响从而到达次数会有些差别，这使得接收端可以使用多个信号重建原始数据流。事实上，路径上的障碍物帮助了接收端的信 号重建，这意味着 802.11n 设备可以支持更远的距离，并且相比目前的技术死点更少。

IEEE 802.11n 也将支持帧聚集。当一个站点获取了权限进行信号传输时，它可以连续发送一系列的帧而不需要释放和重新获取每一个帧的发送权限。 802.11n 也支持将目前仅限于有线网络的高带宽应用移植到无线网络。这将改进无线 VoIP 应用范围。更高速度和更大范围的好处是保证 IEEE 802.11n 能被广泛地被采用，但 IEEE 802.11n 部署前的准备也很重要。

无线网络和笔记本供应商很早以前就已经计划了 802.11n 的支持，并宣布——已经开始交付——基于草拟版标准的设备。而且，Wi-Fi Alliance 计划基于草拟版标准认证这些

产品之间的互操作性。在为 802.11n 准备企业网络时，很有必要先仔细地研究新标准选项。

(作者：SearchNetworking.com 来源：TechTarget 中国 译者：陈柳，曾少宁)

无线接入端安装

安装无线接入端是建设无线网络中的一个棘手的工作。因为其中需要考虑的方面很多，如决定哪些无线协议能在企业中发挥最佳性能、安装合适的 AP 和保证 AP 不会互相干扰或者干扰其它设备。本节将提供关于 WAP 的采购、安装和配置的专业建议。

无线接入端

如何购置无线接入端（AP）是一件棘手的事。这时需要紧跟 IEEE 的最新标准。草拟版 802.11n 正在改进，但还不算成熟。

目前草拟版 802.11n 产品正尽可能地遵循 IEEE 的最新标准，并努力投入市场以便当标准最终发布时转化成具体产品。但是，严格地说现在还没有兼容草拟版 标准的产品。生产支持草拟版标准产品的供应商也在承担一定的风险，因为在标准完全发布后还会有重大问题出现的。特别地，其中很可能会有一些互操作性问题出 现。Farpoint Group 在 2006 年 5 月对早期的草拟版 802.11n 产品进行了基准测试，测试发现了许多互操作性问题。

如 果我们可以将升级延迟到标准发布后，我们就可以购置到更可信的基于 802.11n 的产品。如果我们不得不马上购置新的硬件，我们可以寻找带有能够支持从 802.11g 升级到 802.11n 的域可替代组件的企业 AP。同时不要忘记当 Wi-Fi 认证的 802.11n 产品最终出现时，我们还需要对客户端进行升 级。

为了维持小信号覆盖无线设备的电池寿命，802.11 标准定义了一个省电（Power Save）模式。AP 会缓冲为休眠基站接收的帧。在临时关闭除了计时功能之外的所有功能之前，进入省电模式的基站会宣布它将要休眠。计时功能会在一段时间 间隔后唤醒基站以监听 AP 信号发射台。通过发送包含 Traffic Indication Map (TIM)信号的方式，AP 让所有基站知道单播帧是否暂停传输。当一个休眠的基站监听到这些信号，它会离开省电模式，并打开它的无线电来准备接收缓冲的 帧。另一个有些不同的机制是在特定时间间隔将缓冲的广播/多播帧发送到所有基站，这个时间就是所谓的 DTIM（Delivery Traffic Indication Message）时间间隔。

价值$50 的家用级 AP 和价值$500 的企业级 AP 是非常不一样的。入门级家用 AP 只有一个 802.11b/g 无线电。像 1130 的企业级 AP 则有双重无线 电，可以同时支持 802.11a 和 802.11g。企业级 AP 专门设计用于高密度应用的，支持更多的并发客户端，有更高的吞吐量。企业级 AP 也更可能支持 外部天线，这样可以优化覆盖率，这与家用 AP 的橡胶天线很不一样。

从性能上看，商业级 AP 的功能远不止于双重无线电。企业 AP 提供了更多的电源控制，支持高密度的 WLAN。它们的无线电可能有更好的信号接收灵敏度和范围。 它们可

能有硬件支持的数据加密，激活安全性时有更高的吞吐量。并且越来越多的企业 AP 支持 Wi-Fi Multi-Media (WMM)，它可以根据 Quality of Service (QoS)来对流量进行优先级划分。

无线接入端安置

不管是部署无线网络或调整现有部署，常规的做法是需要先进行“现场勘测”。大多数供应商现在都提供了非常智能的工具来完成勘测工作，但如果手动地找到无线接入端（AP）的最佳安置点，我们需要记住下面三个主要的关系。

无线接入端安置检查单：

与用户的关系：

•根据你的需求，这里有两个方法可以实现：给最多用户或最大覆盖区域设计最好的信号；设置一个最小值，使每一个用户或区域都至少能达到这个值。

•显然，距离是关键，因为数据速率随着距离的增加而下降，要根据上面的设计目标最小化距离。

•记住信号是共享的，所以每一个 WAP 的用户越多，每一个用户共享的带宽会越少。

•对于安全性，WAP 应该尽可能不让人碰到——最好是在天花板上（随建筑物结构而定）。

与工具的关系：

•显然，离金属物、档案橱柜、管道或混凝土墙，以及其它的干扰源（如机器）越远越好。

•为特定区域使用恰当的天线。

•设备必须有电缆和/或 Ethernet 网线，所以安装位置应该尽可能最小化布线距离和成本。

与其它WAP的关系：

•某些供应商推荐 20%的重叠以覆盖准确的语音漫游设备。这是条很好的经验，但还需仔细参考文档说明。

•当 WAP 在各自的频道范围内时，请考虑频道使用。这在多人共用区域特别重要，因为我们可能没有该位置的其它无线电的管理控制权限。

•要通过调整电源来增加或减少信号以优化信号的重叠，而不是通过直接物理地移近或移远 WAP 来实现。

(作者：SearchNetworking.com 来源：TechTarget 中国 译者：陈柳，曾少宁)

无线接入端配置

理解无线 LAN（WLAN）客户端和 WLAN 接入端（AP）的通信机制对于任何想要尝试初始化连接、配置或修复一个 WLAN 连接的人来说都是非常重要的。

WLAN 客户端的几个特性要求配置才能连接到一个无线 AP 和传输数据。这其中包括 SSID、IP 地址、安全和频道配置参数。基本上，WLAN 客户端配置必须与 AP 上的配置相匹配。在大多数情况下，为办公室用户配置 WLAN 的管理员或在家庭办公室创建 WLAN 的用户会配置接入端，因此客户端配置与 AP 配置很容易做到 相匹配。

为了连接到一个 AP，客户端和 AP 的配置必须能够互相匹配。其中第一件事就是保证客户端的正确配置。下面是必须配置的基本参数：

1.服务集标识（SSID）设置：这是区分每个 WLN 的唯一标识符。它过去是 WLAN 的唯一安全性机制，因此只有客户端配置了合适的 SSID 才能连接到 WLAN。在大多数情况下，SSID 是广播出去的，所以 WLAN 网卡可以自动地识别。

2.频道设置：AP 有多个传播信号的频道。如果一个地方有多个 AP。它们需要用不同的频道传输数据，以避免互相干扰。这意味着你可能在家里使用频道 1 而在 Wi-Fi 热点或酒店里使用频道 6 或 11。频道 1、6 和 11 是适用于 802.11b WLAN 网络。同样，大多数情况下这个信息是广播的，并且 WLAN 网卡也能自动地检测到它。

3.安全设置：与 SSID 和频道设置不同，这个信息必须是已有的。安全性设置是现成的，这样可以阻止未授权的访问。

4.IP 地址：一个 IP 地址、子网掩码和默认网关是通过 WLAN 连接传输数据所必须的。上面这三个设置与实现笔记本/PC 与 AP 的物理连接相关。IP 地址必须通过 该连接进行通信。当连接建立后，AP 就能够自动地将这些信息传给 WLAN 客户端，但如果 AP 没有设置进行这样的操作，客户端就需要手动地使用这些信息进行 配置。另外，你必须先得到这些信息。

为了找到最佳的使用加密和认证的连接，我们要记住这些配置 WAP 的技巧：

•如果启用了加密，我们必须在所有的无线客户端启用加密，这样才能建立无线连接。同时要保证接入端和客户端的加密位数是相同的。

•保证接入端和客户端的 SSID 是完全相同的。如果不同，就无法建立无线连接。

•将路由器、接入端和无线适配器设置为不同的频道，以避免互相干扰。同时将无线产品安装到远离产生 RF 噪音的电子设备（至少 3-6 英尺）位置——微波炉、显示器、电动机等。

•当部署多个接入端和无线设备时，要保证附近的接入端没有相重叠的频道。附近的接入端使用的接入端应该至少与本接入端的频道相差 4 个频道。

(作者：SearchNetworking.com 来源：TechTarget 中国 译者：陈柳，曾少宁)

无线网络部署

部署无线网络可能是一个困难的任务，而且在部署完成后，它还需要进行管理以维持高效的运作。本节将讨论无线网络部署的准备工作，包括网络和协议分析以及无线网络的管理和监控。

无线网络部署

特殊的 WLAN 测试工具和经验丰富、知识渊博的 IT 人员，这两者都是部署和维护满足用户需求的 IEEE 802.11 无线网络所需要的。

当准备设计和部署一个无线网络时，我们需要一个协议分析工具来协助诊断预期性能和连接性问题、检测非授权用户的网络访问，以及检测“非法”AP——由员工或其他人连接到网络的未授权 AP。

如果无线网络中部署了语音应用，我们还需要增加了一个专门报告 VoIP 呼叫质量的协议分析工具。

无线技术是复杂的。工具本身并不足以实现一个成功的部署。“一个工具能够告诉我们信号不够强，但它不能为我们分析和选择出特定环境和条件下的理想天线 ”，Sue Galpchian，Celergy Networks 的执行主管这样说道。Celergy Networks 主要关注于无线网络规划。

为了更多了解关于设计满足需求的无线网络的知识，文章“WLAN 测试工具、知识，将理论网络变成现实”包含了设计、分析和开发一个健壮的无线网络的丰富知识以及按部就班的指导。

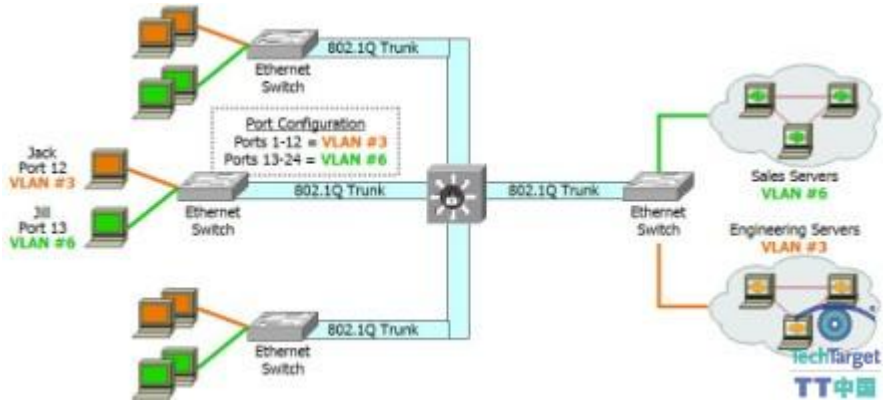
如果没有一流的容量规划技巧，要在无线网络上避免拥塞是非常困难的。

许多公司很注重购置 Wi-Fi 接入端、路由器和交换机，但却很少考虑 Wi-Fi 客户端的选择。但实际上这两方面都很重要：客户端设备对 WLAN 的运作有很大 的影响。支持混杂的 Wi-Fi 客户端会增加维护、修复和性能/安全规划的复杂性。通过标准化而选择少数适当的 Wi-Fi 客户端会使情况很不一样。要知道如 何确认内置的还是外置的无线设备更满足需求，如何比较客户端选项，以及如何制定最佳选择的标准。

(作者：David Jacobs 来源：TechTarget 中国 译者：陈柳，曾少宁)

无线网络管理

在所有工作日，当用户会在 Ethernet 和 Wi-Fi 之间转换时，明智的做法是将 VLAN 同时应用到有线和无线网络访问中。学习更多关于将 Wi-Fi 基站映射到企业 VLAN 和一 个现有 VLAN 如何能够经过扩展而包含无线基站——这样可以给予员工与之前 Ethernet 完全相同的网络访问权限和限制。



将 SSID 映射到 VLAN

由于 VLAN 越来越受欢迎并且不断扩大和逐步替代 Ethernet，因此 IT 经理们将被要求监控 802.11 网络使用，以满足计费、容量规划和报表等需求。但是怎么样才能追踪看不见的东西呢？通过整合传统的网络和会话监控技术以及无线特有的方法和工具，就可以做到。

许多用于收集和分析 IP 流量、网络设备统计信息和应用服务使用状况的常规方法也可以应用到包含无线链路的网络中。无线特有的管理工具还提供了传统网络流量监控和 AAA 服务器所没有的细节。

每一个 802.11 基站有一样的共享媒介（频道）访问权限。优先级和管理服务质量(QoS)功能需要对 802.11 标准进行扩展，目前这个扩展还在开发中。

在办公楼、公寓和购物区的无线网络的广泛部署会带来一些问题，因为这些地方会有多个无线网络在共享电波。在提供无线服务的咖啡厅里情况可能会更坏。有两个新的 IEEE 标准可用于改进无线 LAN 可管理性：

802.11k 将指定周围的 AP 和笔记本创建的无线电频率的测量方法，并提供方法实现这些组件交换测量结果。802.11v 将指定使用 802.11k 测量方法来协助管理无线环境，以及改进 WLAN 可靠性、吞吐量和 QoS 的方法。

(*作者：David Jacobs 来源：TechTarget 中国 译者：陈柳，曾少宁*)

无线安全监控和策略

保证无线安全可能对于实际的部署或延续企业无线网络使用而言仍然是一个阻碍。本节将讨论无线网络的监控和安全策略，以及讨论一些可以增强无线网络安全的工具和配置。

无线安全监控和策略

WLAN 技术部署越来越多，而且与安全相关的联邦法规（如 HIPAA、Sarbanes Oxley 和 Gramm-Leach-Bliley）促使单位必须应对 WLAN 的管理。在联邦法规允许范围内的 WLAN 的基本管理方法是非常重要的。联邦 法规要求每一个单位都要提供网络访问的控制机制，要能够控制访问网络的用户，并且保证在网络中传输的数据安全。

许多单位只是将这些作为一时的安全策略，但是 WLAN 环境是需要持续管理的，以便它能够抵抗和阻止侵入以及检测侵入。监控 WLAN 环境和维护安全规范是多方面的。

802.1X 可以用来将无线流量转到反映用户或组权限的 Virtual LAN 上。理解如何建立认证和授权之间的这个重要链路是很有用的。其中数据包会被打上标记，表明它们进入了一个 LAN，这样上游设备（如网关、路由器和防 火墙）就可以应用安全性和 QoS 过滤器。AP 也可以标记无线流量，这样它就可以在通过网络时保持与有线流量的隔离，包括从 AP 到边界交换机、再到核心交换 机、最后是 Internet 路由器。

在最近发布的文章中，安全供应商 Network Chemistry 分析了从 RFprotect Endpoint 用户收集的事件，得到以下数据：

•用户会同时连接无线和有线网络。

（37%分析的终端启用了网桥。）

•使用 VPN 的用户并不总是使用它来保护流量。

（68%的用户曾经违反了 VPN 策略。）

•端对端网络经常被使用。

（63%的用户启用了端对端或者尝试连接一个端对端节点。）

•无线连接经常会用于连接未知网络。

（87%的终端已经连接到未知的 AP。）

公司可以通过教育员工关于 Wi-Fi 威胁以及强化阻止不安全连接的 Wi-Fi 安全策略来阻止这些有风险的行为。

同时连接到内部和外部可能会带来安全风险——这早就是一个已知的VPN风险，并且也是为什么很多公司不使用称为**“分隔通道（split tunnels）”**技术的原因。当连接到一个公司Ethernet的用户初始化来自隔壁AP的Wi-Fi连接或城市网络时，他们会将公司网络暴露给外部威胁。但阻止这种行为的发生并不像想象中那么容易。

(作者：SearchNetworking.com 来源：TechTarget 中国 译者：陈柳，曾少宁)

无线安全工具和配置

小型或中型企业（SMB）的 WLAN 安全已经变得越来越像大型公司一样危急了。无线 LAN 不像有线，它对于入侵是特别脆弱的，因为这在物理线路中是没有的。无线波能够将流量传递到公司外面，这使得入侵者不需要进入公司就可以访问网络。

而且，WLAN 流量不会总是流向一个中央节点，因此无法使用这样一个中央节点来监控和控制访问的用户。SMB 可能需要 WLAN 安全来遵守政府的规定，如 Health Insurance Portability 和 Accountability Act。了解可用的技术可以帮助 SMB 购置相应的 WLAN 安全工具。

802.11 Wired Equivalent Privacy's (WEP)的许多缺点之一就是它依赖于手动配置的静态密钥，一般是 16 位的。许多用户不知道如何配置 WEP，而且供应商并没有采取措施将 WEP 细节隐藏在 用户友好的 GUI 下。WLAN 管理员很快发现手动配置 WEP 密钥是很乏味的工作，这很容易出错并且导致失败，因为一个密钥丢失或被盗后，他们就必须在上百 个设备上进行更新。Wi-Fi Protected Access (WPA)已经对此作了一定的改进。并且有许多方法可以简化 WLAN 安全配置。

WPA2 是针对实现 IEEE 802.11i 安全扩展产品的 Wi-Fi Alliance 认证程序。WPA2 认证的产品从 2004 年 9 月开始就有了。现在，大多数企业和许多新的家用 Wi-Fi 产品都支持 WPA2。而且从 2006 年 3 月起，WPA2 已经是强制使用了。我们现在已经进入了 WPA2 的时代了。

WPA2 有两种形式：WPA2 个人版是用于家庭和小型办公室的，而 WPA2 企业版是用于商业应用的。创建一个大型的物理分布式兼容 WPA2 网络可能是一个很大的挑战，并且这要求在开始前进行预先规划。首先理解各种相关元素可以保证开发过程顺利进行。

为了决定设备是否支持 WPA2，我们可以查询 Wi-Fi Alliance 认证产品列表。如果设备太旧或者它不是 WPA（版本 1）认证的，就不要它——如果不是马上，那也要尽快。为了将其它设备更新到 WPA2， 在供应商的支持网站上检查新的 AP 硬件或者网卡驱动。我们需要不超过 2 年出产的硬件，WPA2 要求实现 Advanced Encryption Standard (AES)的芯片。如果你正在购买新的 AP，要确保它们是 WPA2 认证的。

(作者：SearchNetworking.com 来源：TechTarget 中国 译者：陈柳，曾少宁)

无线故障修复

修复无线问题可能需要大量持续且未知的支持——特别是在了解了所有这方面专家的建议以及花费大量时间准备和规划网络之后。本节将探讨如何处理无线连接问题、调试和无线容量规划。

无线故障修复

使用无线也许可以节省布线和有线 LAN 的开支，但是无线网络仍然需要有效的技术支持和故障修复。

平稳操作始于一个设计良好的无线 LAN（WLAN）。现场勘测、RF 建模和自动 RF 管理系统，这些都能够减少服务台求助从而产生收益的投资。

但没有 WLAN 能够离开故障修复。环境的条件和网络使用正在改变。设备故障和软件错误总会有。最终，无线用户会求助。好的无线网络故障修复工具和系统方法可以协助更快地隔离和解决这些问题。

当无线 LAN（WLAN）用户遇到连接问题时，问题可能发生在客户端或网络端。学习如何修复由于网络问题引起的无线连接问题可以确保员工保持连接并继续工作。

无线用户所遇到问题到处都有，从无线干扰和客户端错误配置到接入端 LAN 布线问题和不稳定的应用。类似于有线故障修复，系统方法可用于追踪问题而不会忽略常 见起因或重复检查。跟踪客户端到服务器的连接，验证每一个中间组件的操作，也可以用到无线网络上。这需要先理解无线设备、协议和 WLAN 体系结构。

当遇到连接办公网无线主机（台式机、笔记本、PDA）的问题时，下面的调试步骤可能会有帮助：

1.从重新检查物理连接开始。

2.验证无线适配器已经安装并正确工作。

3.验证无线路由器的 LAN 设置是正确的。

4.验证客户端的 TCP/IP 设置。

5.当客户端的 IP 地址出错时，使用“ping”来验证网络的连接性。

6.如果修改成一个有效的 IP 地址或者 ping 路由器后，无线客户端仍然不能连接上，就必须考虑无线相关的问题了。

7.如果匹配的客户端和路由器连接上后，仍然不能连接或发送流量，就要检查安全性问题。

8.确保 RADIUS 正常工作。

9.如果 RADIUS 正常工作了，但客户端访问仍然被拒绝，尝试查找 802.1X Extensible Authentication Protocol (EAP)或用户登录问题。

10.最后，如果无线客户端连接和 ping 成功后，但仍遇到网络连接间断问题（如，一些 ping 成功，一些失败），可能就是信号强度太弱、RF 干扰或 AP 漫游引起的问题。

大多数企业 WLAN 交换和接入端供应商都有自己的网络管理软件，这些软件有规划、约束和/或监控功能。其中包括 Aruba Networks Mobility Management System，Bluesocket BlueView Management System， Cisco Wireless Control System and Wireless LAN Solution Engine (WLSE)， Colubris Networks NMS and RF Planner，Trapeze Networks RingMaster 和 Siemens HiPath Wireless Convergence Software。

随着许多单位在关键任务和实时应用中越来越依赖于无线通信，无线局域网的使用报告变得越来越重要。

想象一下：有一个医院使用 WLAN 实现客户 Internet 访问、员工邮件以及其它诸如病人监控和急救/家庭医疗应用等。管理员最不希望看到的是客户或员工 网络占用所有可用的带宽，而急救系统没有带宽传输数据。在 802.11e (WLAN QoS)出现之前，通过 WLAN 使用报告的容量规划仍然是必需的。

在狭小空间的办公室实现 802.11g 也可能带来特定的问题——想象一个带有狭窄过道的办公室，处在分隔的封闭房间和同一层内多个相同设计的区的情形。员工 肯定会发现他们在楼里和设备交换 AP 之间移动时网络总会断开和重连。但即使按标准在每 3，000 平方英尺面积安装一个 AP 也无法解决这个问题。有几个选项 可考虑用以改进这种状况和阻止连接掉线。

(作者：SearchNetworking.com 来源：TechTarget 中国 译者：陈柳，曾少宁)