应用说明：管理 BYOD 和 IT 消费化

OneTouch AT 网络助手应用程序手册

目录

简介

IT 消费化正在许多公司的 IT 部门迅速成为现实。近年来，平板电脑和其他智能设备的推广大幅增长，这些“消费类”产品在企业网络中几乎无处不在。最近的研究显示，90 % 参加投票的组织允许一定程度地在办公室使用某些个人设备，这一现象被称为 BYOD（自带移动设备）。除了作为客户端的大量手机和平板电脑之外，随处可以买到的低成本住宅网关、路由器、AP 和交换机也将进入企业。员工们对他们新发现的民宅网络技能充满自信，将会比以往更加大胆地创建网络熵。

移动客户端和网络设备的大量涌入使得 IT 部门需要寻求最好的方式来检测、盘点、审计、定位和管理大量新设备。在最近的一项调查中，百分之 62 的公司报告他们缺乏必要的工具来支持员工的个人设备，无论政策是否到位。恐惧和担忧比比皆是。管理个人设备造成的影响、保护公司数据和知识产权及进行审核以确保合规成为大多数 IT 部门一方的棘手难题。

Fluke Networks 的 OneTouch™ AT 网络助手拥有各种提供可见性和控制的功能，可抑制 BYOD 激增、降低风险和操作成本，从而提供一个安全的、高性能的、无处不在的、可靠的有线和无线基础设施。OneTouch 坚固耐用，拥有独特的有线与无线分析功能的组合，这使它能够如同自己所管理的设备一样可以移动。此应用文章探究了为应对 IT 常见的多种 BYOD 问题 Fluke Networks OneTouch AT 网络助手的实际应用，例如：

- 如何盘点当前 Wi-Fi 网络的状态
- 如何调查用户关于性能和连接性的投诉
- 如何识别恶意客户端、AP 和其他网络设备
- 如何审计网络权限
- 如何测量 Wi-Fi 性能
- 如何测试移动电话切换的覆盖范围

如何了解 **Wi-Fi** 设备的清单？

大多数企业中的 Wi-Fi 使用率正在激增，而网络以前仅支持公司笔记本电脑处理大量不同的手机和平板电脑。除了设备总数的增长，对带宽的需求还可能破坏企业关键任务应用程序的性能。应对 BYOD 现象的关键是理解其普遍性。您必须盘点设备，查看其所连接的网络和接入点，并确认环境的健康性。

OneTouch 可以自动发现并将 Wi-Fi 分为四类：网络、AP、客户端和信道。按属性排序可从不同角度认识无线网络。例如，根据信号强度排序可解决 Wi-Fi 覆盖范围问题。按利用率排序，以识别 AP、客户端或信道利用问题。根据授权状态排序可以找出潜在的安全违规行为。根据 MAC 制造商排序可以发现 Wi-Fi 设备的类型，以及其相对于 SSID、AP 和信道的连接方式。

“客户端”选项卡显示所有无线设备，可在所有信道上看到 OneTouch。这可能审计 IT 在支持 BYOD 时所采用的正式政策的合规性。Android 设备的代表通常为三星、HTC 和摩托罗拉制造商代码以及代表 RIM 的黑莓。图 1 为示例。我们能够快速识别异常值，如信道 161 上的 Apple 设备、5 GHz 信道和其他 Apple 设备，以探测已知但未连接到网络的 SSID 。

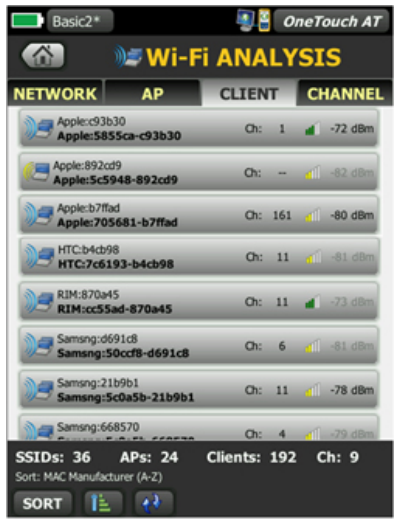


图 *1*

轻触任何设备可展开视图，以显示设备所使用的网络、SSID、信道和安全性的详细信息，并开始显示关键设备指标的详细趋势信息。参见图 2。过滤器按钮可为与每个客户端相关的网络、接入点和信道提供更深入的分析。

当您获取最相关领域（SSID、AP、客户端或信道）的 Wi-Fi 分析时，排序和过滤是了解设备清单最常用的方法。轻触右上角的 OneTouch AT 按钮可捕获一个屏幕（获取屏幕截图）或创建详细的 PDF 报告以便将 BYOD 设备清单存档。

OneTouch 与 Wi-Fi 提供商无关，可在办公、走路或进行远程操作时使用。

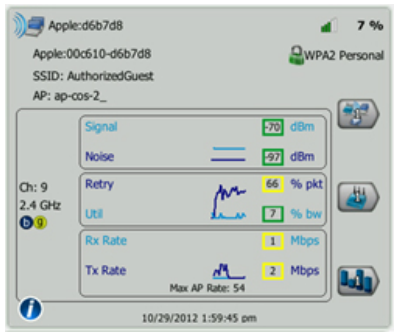


图 *2*

如何识别干扰网络？

低成本的接入点和移动热点可能会造成公司网络在性能和安全性方面的风险。手机热点可不使用公司 LAN/WAN 与互联网连接。便携式热点通过移动电话网络回程，并继续共享企业 Wi-Fi 网络环境。这可能导致信道阻塞或同信道干扰。

比便携式 3G 热点问题更严重的是，员工通过将网关接入公司网络来引进住宅 AP 或网关，为他们的平板电脑和手机创建个人 Wi-Fi 网络。这不仅会导致环境阻塞，而且会使未经授权的 Wi-Fi 访问公司 LAN。

OneTouch 通过逐信道不断扫描环境，描述 SSID、AP、客户端和信道使用特征来执行 Wi-Fi 分析。分析分别以四个选项卡显示，具有运用多种方法对分析进行排序的能力。例如：要检测潜在的恶意 Wi-Fi 网络，选择“网络”选项卡并按最少接入点排序。参见图 3。这为识别含有受单个 AP 支持的单个 SSID 的一次性网络提供了快捷的方法。其他干扰网络表现为开放网络，以红色开放锁图标指示。

选择任何 SSID 来展开网络详情。参见图 4。正常企业 Wi-Fi 网络使用多个被精心安排和分配给非重叠信道的 AP 提供覆盖范围和容量。支持 SSID 的 AP、信道和客户数量显示于显示屏右侧的过滤器按钮上，轻触按钮即可显示那些设备。

SSID “cody-dlink”只有一个 AP，与一个主机连接，使用一个信道。参见图 5。这不是正常公司网络的代表，可能显示的是一个恶意 AP。分类是识别异常值网络、接入点、客户端和信道的一种功能强大的工具。

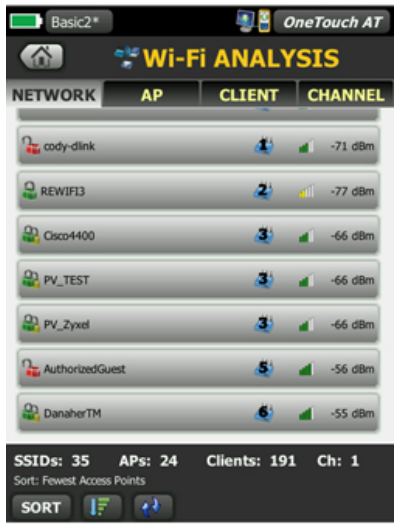


图 3

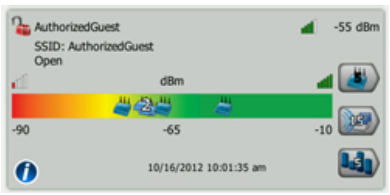


图 4

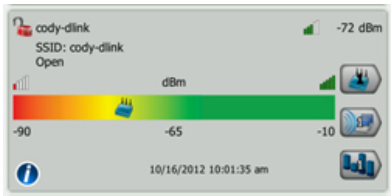


图 5

使用企业 **SSID** 时出现恶意 **AP** 怎么办？

如果工作人员将其设备 SSID 设置为与企业 SSID 相匹配，以试图掩盖其私人网络怎么办？在“网络”选项卡上展开认可的公司 SSID（如授权客户），我们可以立即看到它由 4 个 AP 所支持。参见图 6。选择 AP 按钮释放功能强大的过滤视图。通过选项卡您可以以 SSID、AP、客户端或信道为基础选择一个起点进行分析，三个过滤器按钮可使您轻松缩小调查范围。

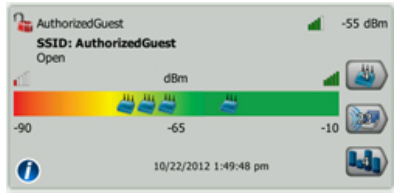


图 *6*

过滤时，标题栏从 Wi-Fi 分析变为源过滤器标准，本例中为授权客户。参见图 7。我们立即可以看到，该 SSID 受三个 Cisco AP 和 Linksys 设备支持，这意味着它可能不是公司网络的一部分。

您可以使用 OneTouch 主动识别网络中新的恶意设备和其他设备。您可以在前提条件中标记已知的 AP 和附近的 AP。已知的和预期的公司 AP 可标记为“授权”。参见图 8。前提条件以外的已知 AP 可标记为“相邻”。OneTouch 会记忆已标记的 AP。预期 AP 标记后将迅速按照“授权状态”进行排序以识别未知接入点，如“授权客户”屏幕中显示的 Linksys，如图 8中所示。

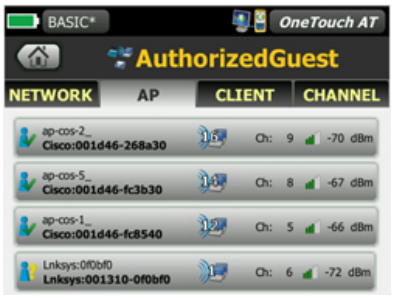


图 *7*

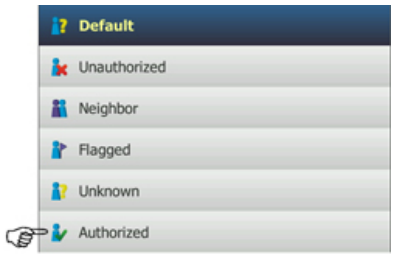


图 *8*

我可以定位问题 AP、热点或特定设备吗？

识别恶意 AP 或移动热点后，OneTouch 提供了几种方法来定位设备。使用外部定向天线（参见图 9）和定位功能（参见图 10），任何无线设备、AP 或客户端的物理位置都能被迅速发现。

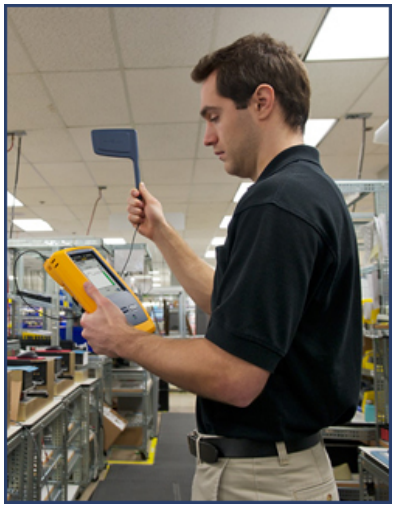


图 *9*

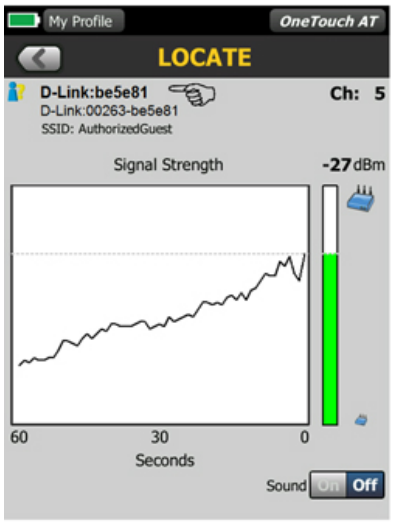


图 *10*

当恶意 AP 接入有线网络时，可使用 OneTouch 有线分析定位与其连接的交换机插槽和端口。设备和用户可拔掉接线板电源插头或禁用交换机端口断开网络连接。

要在“有线分析”中查找 Wi-Fi 分析设备，可通过 MAC 地址排序有线分析并寻找无线 MAC 地址。参见图 11。注意，在某些情况下相邻的 MAC 地址可用于多接口设备。在这种情况下，相邻 MAC 地址的 D-Link 设备可连接到 COS_DEV_SW1 的插槽 2 /端口 44，使用 VLAN 500 的 IP 地址 10.250.1.176。

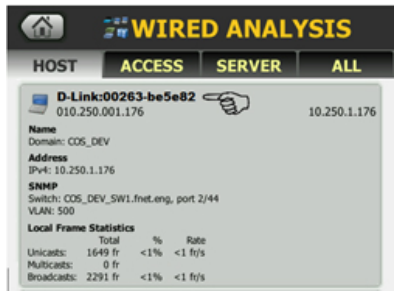


图 *11*

如果恶意 **AP** 不广播 **SSID** 怎么办？

如果工作人员将其 AP 配置为不广播 SSID，从而使其在公司网络中无法被检测到，怎么办？通过识别非广播网络，OneTouch 可管理网络使用并减少安全问题。

OneTouch 积极侦听非广播网络并将 SSID 作为[隐藏]报告到发现的网络列表中。参见图 12。选择 AP 过滤器按钮识别使用非广播网络的 AP。使用为主动识别标记未授权 AP 或定位问题 AP 的工具。

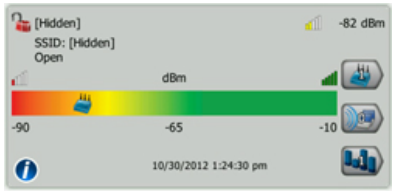


图 *12*

若已知隐藏网络的 SSID，OneTouch 将发送一个主动探测请求，包括一个 AP 的特定 SSID，来处理非广播 SSID。OneTouch 探测设备上所有配置文件中配置的 SSID 并通过 802.11 个数据包被动地了解网络使用的非广播 SSID。这些被解决的非广播 SSID 将以括号的形式写入报告，如[黑洞]。参见图 13。

已有人建立了特定网络吗？

如果少数工作人员已将其笔记本电脑配置为在特定模式中操作游戏怎么办？尽管特定网络在企业环境中占据一席之地，但如果配置为无担保的开放网络，他们经常违反 IT 政策并造成安全风险，从而危及公司数据。如果公司 AP 使用相同信道，特定网络还会影响网络性能。

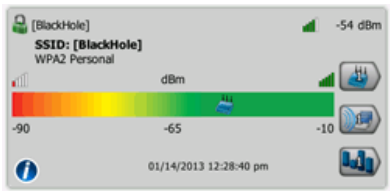


图 *13*

排序网络类型可使发现的特定网络在列表顶部显示。参见图 14。可立即看到正在使用的特定网络名称（蒙大拿州）及网络是否安全。展开网络以获得有关网络的详细信息。使用客户端过滤器识别和定位构成网络的设备。

图 *14*

公司 **SSID** 上有任何意外客户端吗？

IT 人员用来保持对移动设备扩散的控制的唯一方法是将移动计算设备分为三个完全不同的设备类别：由公司提供的可信任的标准设备、可接受的设备和不支持的设备。最好的做法是确保公司 SSID 仅可完全访问预期的 AP 和客户端。从“网络”选项卡选择公司 SSID。参见图 15。AP 强度指示条上的 AP 图标通过 4 个不同信道上的 4 个 AP 显示 SSID 有良好的覆盖范围，并管理企业的安全性。要审计所选 SSID 上的客户端，只需点击“客户端”过滤器按钮，以查看客户端。

标题栏显示过滤的 SSID。参见图 16。要使 37 客户端列表更易于理解，可根据制造商 MAC 排序列表。这将对普通设备进行分组。列表显示公司有 36 台使用 Intel MAC 地址的笔记本电脑与该 SSID 连接，但不知何故，一台 Apple 设备已成功地关联到公司网络。根据公司政策的不同，此设备可以被允许或不被允许。如果不被允许，可以使用无线定向天线或可能通过寻找有线分析中的设备 MAC（如前所述）对该设备进行定位。

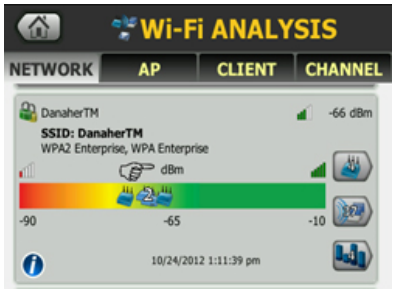


图 *15*

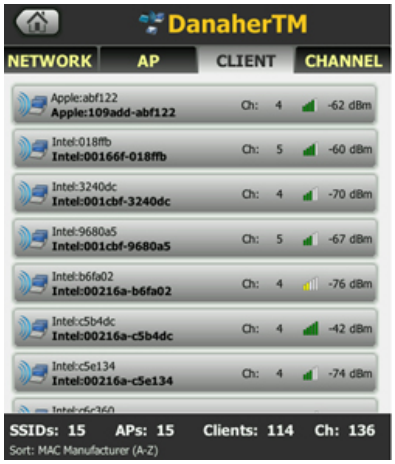


图 *16*

为什么这个区域内的性能不好？

支持 BYOD 的缺陷之一是在使用个人设备的情况下，很难保证关键任务对公司 Wi-Fi 的访问。阻塞的环境和高带宽使用模式（如流媒体视频）可能会阻碍关键任务通信。当经理在会议室抱怨 VoIP 电话的性能问题时会发生什么？

在这种情况下，与 Wi-Fi 分析配合使用的 OneTouch 的便携性功能是无可比拟的。走向问题区域，使用“Wi-Fi 分析客户端”选项卡识别抱怨的客户端。此外，也可使用网络选项卡和客户端过滤器缩小搜索范围。在图 17 中，可看到信号电平很强。同时注意稳定的信号电平可表示这是一个不移动的客户端。噪声电平低表明总体环境健康且没有非 802.11 干扰。然而，黄色分级表明重试率高。还有，Rx 和 Tx 率十分易变。

图 *17*

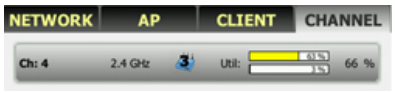


图 *18*

选择信道过滤器按钮可进入信道 4，（参见图 18），可看到黄色栏显示的高 802.11 利用率。要确定利用率的来源，过滤 AP。

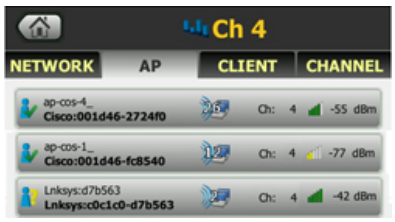


图 *19*

过滤信道 4 AP（参见图 19），可看到三个 AP。两个为企业 AP，有 38 个客户端。还可看到附近有一个较强的 LinkSys AP，有 2 个客户端。它意外地与我们共享信道。使用之前描述的定位技术定位 AP。

如何验证 **Wi-Fi QoS** 是否在工作？

图 *20*

随着个人用户设备的涌入，关键是验证 Wi-Fi 在最佳状态用户数据流量时的性能与工作流量的优先级。服务质量 (QoS) 支持 Wi-Fi 接入点和交换机优先考虑流量。没有QoS，运行在不同设备上的所有应用程序有均等的机会传输数据帧。行业标准如 802.11e 和 WME（无线多媒体扩展）优先考虑来自不同设备和应用程序的流量，以扩展对关键任务流量的高质量最终用户体验，如各种环境和流量条件下的声音。QoS 流量控制可通过多种机制如 SSID、端口或 DSCP 进行实现。

OneTouch Veri-Fi™ 功能允许通过流化 OneTouch 有线和无线接口间的数据，快速、有效地验证有线/Wi-Fi 性能。参见图 20。可使用多种方法进行验证：

- 测量 Wi-Fi 上行和下行性能
- 生成大量后台流量以验证加载 AP 时关键 QoS 未受影响。
- 验证未受最佳状态流量影响的 QoS。

在本示例中，我们将使用正确配置的 46 DSCP 加速转发 (EF) 值测试 VoWi-Fi 流量。参见图 21。此外，我们将验证 QoS 在 IPv4 和 IPv6 上的工作。我们选择一个帧大小为 128 字节的 VoIP RTP 代表，并指定 1 Mbps 的上行（Wi-Fi →有线）和下行（有线→Wi-Fi）对称数据传输速率来模拟 10 同步呼叫。测试结果（显示为丢帧率）低于 1% 的通过/失败限制，因此测试通过。参见图 22。使用个人设备或第二个 OneTouch 可生成后台流量。

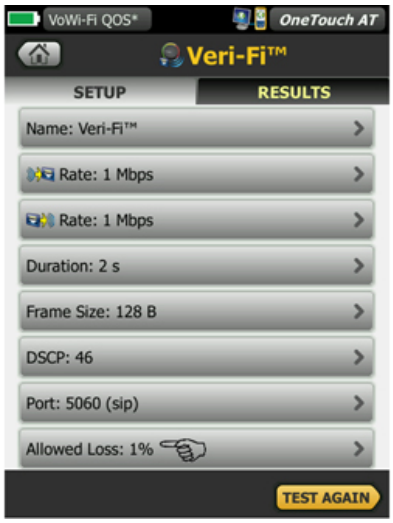


图 *21*

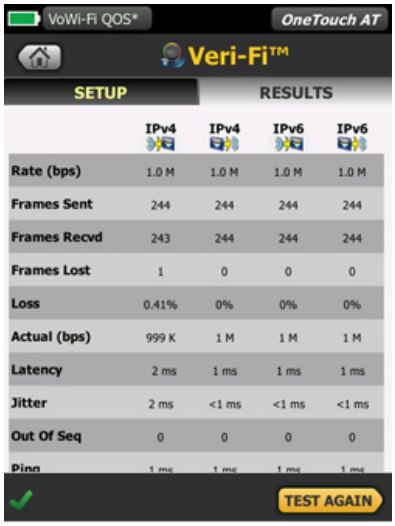


图 *22*

如何更多地了解 **Wi-Fi** 设备？

Wi-Fi 分析提供了前所未有的无线网络、接入点、客户端和信道视图。关于客户端（图 23），可看到以下信息：

- MAC 地址
- SSID（网络）
- AP
- 安全性
- 射频类型 (a/b/g/n)
- 信道和频段
- 最后一次看到时
- 一分钟内的关键指标趋势

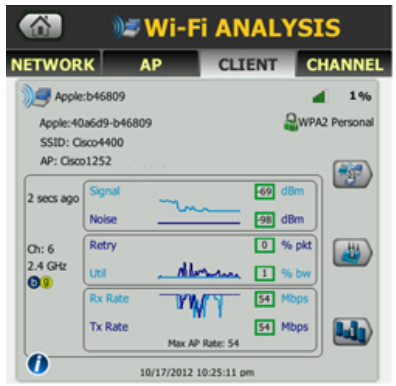


图 *23*

也可轻松过滤相关网络、AP和信道。然而，因为包括层 3 IP 地址在内的来源和目标 MAC 的所有内容都是加密的，经常需要通过有线分析了解关于设备的更多信息。

在许多情况下，OneTouch 有线分析可通过发现和询问无线 LAN 控制器，从而发现 IP 地址、VLAN 甚至指定设备的名称。无线设备可根据 MAC 地址排序有线分析并匹配 Wi-Fi MAC 地址而被找到。在图 24 中可看到 MAC 地址为 40a6d9-b46809 的 Apple 设备出现在有线网络上，其在 VLAN 500 上的 IP 地址为 10.250.0.135。VLAN 信息可根据其授权级别或用户组验证是否是在相应的 VLAN 上运行设备。您可以使用 OneTouch 有线分析扫描有线设备开放端口，以了解有关设备的更多信息；在这种情况下，iphone 同步 TCP 端口 62078 是开放的。

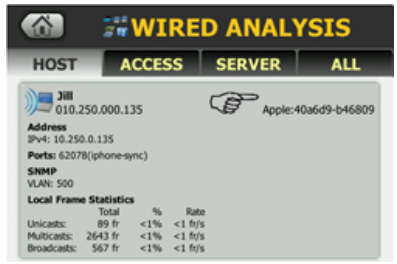


图 *24*

如何验证对各种 **SSID** 的访问是否适当？

企业通常通过实施访问网络区域来限制个人移动设备的连接，使用多个 SSID 进而控制网络访问。

许可	访问	SSID
完全访问	互联网 & 全部公司资源	AcmeCorp
部分访问	互联网 & 部分公司资源	AcmeContractor
仅互联网	仅互联网	AcmeGuest

BYOD 需要政策和配置来控制客户端允许访问的公司资源。SSID 经常使用唯一 IP 地址和有线 VLAN 分段控制访问。

OneTouch 配置文件为指定配置，可用于各种方法来简化操作。使用配置文件可让组织创建标准测试程序，包含任何 SSID 预期的网络操作。

在图25 中可看到名为“承包商访问”的配置文件，可测试到允许和禁止的服务的连通性。重命名各层以分组允许和禁止的测试。

使用配置文件在组织内创建标准审计，可实现一致而彻底的测试过程，实现更少的技术人员在企业的任何地方执行复杂的网络测试和审计。

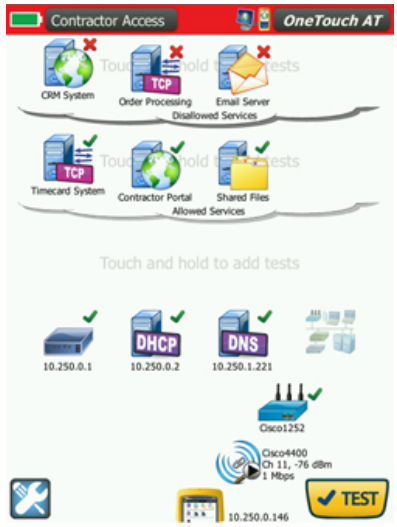


图 *25*

我的 **Wi-Fi** 分流在起作用吗？

当今的 BYOD 用户可享受在企业内无缝漫游的基本功能。从移动电话转到 Wi-Fi 有许多好处，包括：

- 更低的数据费用
- 更快速的连接
- 更低的电池消耗
- 提升的最终用户体验

但是如何确保 Wi-Fi 信号覆盖范围足以防止射频间的颠簸（持续的信道跳跃）呢？

连接到 SSID 时，OneTouch 可追踪从一个 AP 区域到另一个的覆盖范围。OneTouch 可记录每次漫游时设备的详情。您可以使用漫游结果导航控件查看每个相关 AP 的详细信息。参见图 26。对于每个 AP，通过信号、噪声、重试和利用的最小值和最大值可深入观察 AP 区域的操作范围。

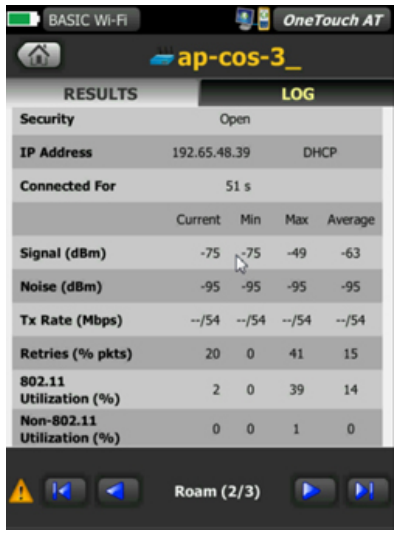


图 *26*

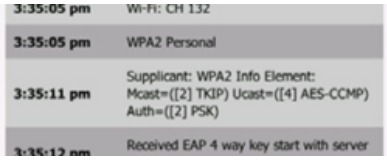


图 *27*

点击“日志”选项卡查看每个连接、认证和关联标有时间戳记的详情。参见图 27。

漫游时使用 Ping (ICMP) 工具可找到覆盖范围内会导致 3G 加载的死角。通过设定无法通过移动电话访问的内部 ping 响应器目标，可保证在未连接 Wi-Fi 时丢失数据。连续 ping 模式中有一秒钟的时间限制；丢失的 ping 数据包数量与未连接 Wi-Fi 的秒数相等。参见图 28。在这种情况下，在 228 秒的漫游中 Wi-Fi 失去了6秒。此测试也可通过使用“连接 (TCP)”测试得以执行，使 TCP 端口面向所选目标开放，以测试应用程序端口的可达性。使用 AirMagnet Survey 和 AirMapper™ 可进行更广泛的覆盖范围测试。

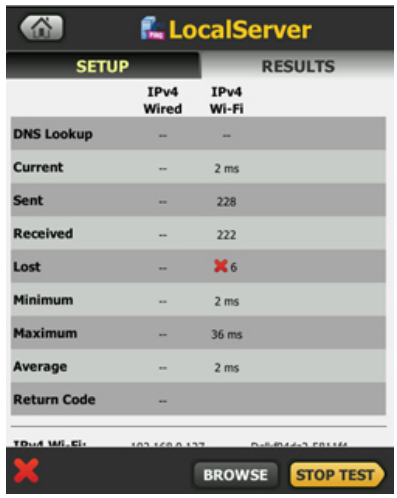


图 *28*

如何通过访客 **SSID** 进行验证？

连接到访客网络和酒店 Wi-Fi 网络时，通常需要验证或接受强制网络门户的条款。强制网络门户强制网络上的 HTTP 客户端在使用网络前查看特定网页。

OneTouch 的集成 web 浏览器可通过管理、有线或 Wi-Fi 测试端口进行操作。在图 29中，OneTouch 分析仪使用其 Wi-Fi 端口访问网页，浏览器被重新定向到可能需要身份验证和/或付款的网页，或仅显示可接受政策并要求用户同意。验证身份后，OneTouch Wi-Fi 测试端口的 MAC 地址通常会被缓存，允许在 24 小时内访问。在酒店使用有线网络的房间内，如果有线测试接口正在使用强制网络门户，同样的技术可用于验证有线接口。

除浏览强制网络门户外，OneTouch 的集成 web 浏览器可用于配置网元，如交换机和无线 LAN 控制器。参见图 30。

OneTouch 分析仪还包括集成 SSH/终端，进行命令行配置和诊断。参见图 31。

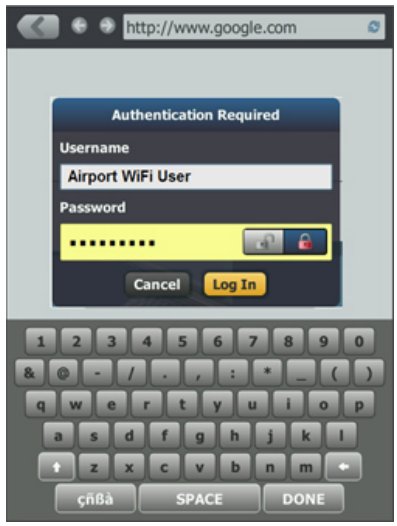


图 *29*

图 *30*

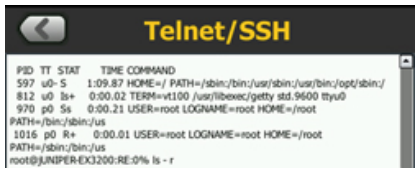


图 *31*

我在这里，但我的问题没有解决。我应该怎么做？

Wi-Fi 是非常具有挑战性的媒体。除动态带宽要求外，客户端及干扰源变化不断。例如 BYOD OS 升级、更新流行的应用程序、云备份甚至病毒视频会给网络带来压力。当你走遍校园想要诊断出客户端问题时，却发现此时并不存在问题，会怎样？

通过其管理端口将 OneTouch 分析仪连接到网络可将设备留下并进行远程操作。这样您可以继续其他工作，在办公桌前定期或当客户端再次呼叫时检查 Wi-Fi。

只需在 web 浏览器或 VNC 客户端键入管理端口 IP 地址即可开始。可从运行的桌面、笔记本电脑、平板电脑或手机操作 OneTouch。参见图 32。OneTouch 分析仪的用户界面有大尺寸的可触图标，甚至用手机也能很方便的操作。如果看到可疑的内容，可点击屏幕顶部的 OneTouch AT 按钮保存报告或捕获屏幕，以将间歇性问题存档。

图 *32*

图 *33*

OneTouch 分析仪的功能如此之多，甚至可将普通网络摄像头插入 USB 端口进行远程监控。例如，可以查看会议室内参会者的数量、观察屏幕或显示屏，或者监控网络设备上的 LED。这不仅可监控网络，还可监控实际空间。参见图 33。

是无线或有线问题吗？

通过使用 RF，Wi-Fi 可提供不同的方法访问第 1 层和 802.11 第 2 层网络。然而，当您通过接入点后，将依赖相同的有线基础设施。除目前拥有的 Wi-Fi 分析技术外，OneTouch 分析仪还拥有大量可在 BYOD 管理中发挥作用的功能。OneTouch 分析仪的有线分析类别与 Wi-Fi 分析中的操作相似。按问题排序可将任何已发现的有线问题迅速推至列表的顶端。参见图 34。点击任何设备，获取更多详情。

图 *34*

例如在图 35 中，无线 LAN 控制器 (WLC) 在 12 分钟前重新启动并负责当前的故障单。使用 SNMP，OneTouch 分析仪还可报告设备和所有者的位置。其他类别包括 IPv4 地址、IPv6 地址、MAC 地址、制造商名称、首要广播设备、域名及更多。

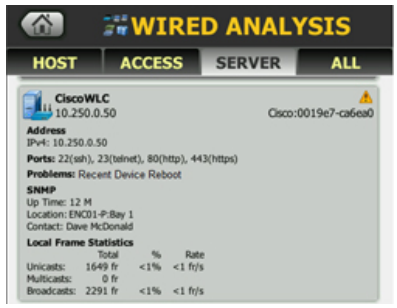


图 *35*

按 VLAN （图 36）排序可验证 BYOD 设备是否与指定的与其 SSID 相关的指定 VLAN 正确隔离。

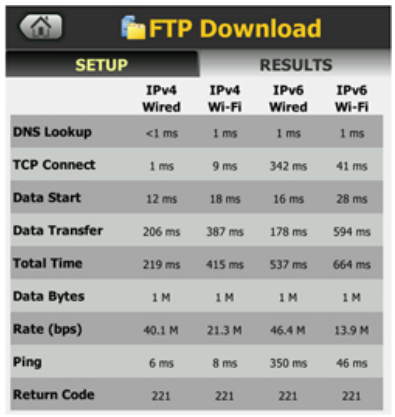
图 *36*

可使用内置端口扫描仪对任何已发现的设备进行进一步探测。此外，有线分析可用于识别关键 Wi-Fi 设备。您可以建立 AutoTest 配置文件以创建标准化测试，从而快速确定关键网络设备的可用性并诊断其状况。

我的 **Wi-Fi** 事务处理性能与有线相比如何？

有时很难确定瓶颈是在 Wi-Fi 还是网络其余部分。OneTouch 分析仪可同时测试有线 Ethernet 和 Wi-Fi 网络，并可以很方便地将性能与并列式测试结果进行比较。这种比较可扩展到 OneTouch 分析仪的有线设置中所启用的 IPv6。

在图 37 中，我们使用 FTP 用户测试来测量下载 1 兆字节文件的最终用户响应时间 (EURT)。FTP 的使用取决于测试结果中显示的基础 TCP 性能。FTP 工具允许文件下载（获得）或上传（放置）。



	IPv4 Wired	IPv4 Wi-Fi	IPv6 Wired	IPv6 Wi-Fi
DNS Lookup	<1 ms	1 ms	1 ms	1 ms
TCP Connect	1 ms	9 ms	342 ms	41 ms
Data Start	12 ms	18 ms	16 ms	28 ms
Data Transfer	206 ms	387 ms	178 ms	594 ms
Total Time	219 ms	415 ms	537 ms	664 ms
Data Bytes	1 M	1 M	1 M	1 M
Rate (bps)	40.1 M	21.3 M	46.4 M	13.9 M
Ping	6 ms	8 ms	350 ms	46 ms
Return Code	221	221	221	221

图 *37*

总时间 (EURT) 是构成事务处理的个别时间的合计：

- *DNS* 环路是用于将 URL 解析为 IP 地址所用的时间长度。
- *TCP* 连接是在服务器上打开端口所用的时间长度。
- 数据开始是从服务器接收 FTP 文件数据帧所用的时间。
- 数据传送是传送文件数据所用的时间。

精确定时地并排对比有线和无线性能以及事务处理组件故障，对确定您的 Wi-Fi 是否是瓶颈非常重要。

如果总时间超过选择的时间限制，测试将失败。因此，可创建 AutoTest 配置文件以测试最终用户体验。注意，根据 FTP 服务器的位置，瓶颈可能是 WAN 容量，在这种情况下，有线和 Wi-Fi 数据传输时间可能近似。其他有用的对比用户测试包括网络、多播和用于视频订阅的 RTSP。

我如何识别 **BYO** 集线器、交换机和路由器？

员工受到新发现的家庭网络技能和商业网络设备的鼓舞，这意味着他们可能给 IT 带来自带威胁。如果员工决定要在自己的办公间中设置另一个有线端口，他们可能会使用一个从任何大卖场都能买到的不受控的低成本交换机。这样他们将会在办公室里插入多台以太网设备。

使用有线分析和根据交换机名称/插槽/端口排序主机，根据设备到受管的企业交换机的连接来安排设备。通常每个交换机端口连接一台主机设备，并且每个插槽/端口只使用一次。如果交换机端口被多台设备使用，则表明可能有一个小集线器或交换机连接到企业交换机。在图 38 中，交换机 cos_dev_sw3 有多台设备连接到端口 20。进一步检查表明，此员工不仅将一台交换机插入他们墙上的插座，还使用其他端口插入一台使用 MAC 地址 Rspbry:9977393 的个人 Raspberry Pi linux 系统计算机，只有信用卡大小。尽管该员工可能仅仅是在午餐时玩一些游戏，但此设备可能在不知不觉中损害企业网络。

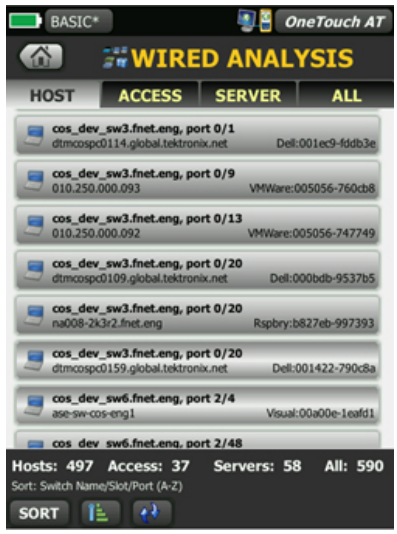


图 *38*

如果某个员工将一个常驻网关插入网络，并不知道它将作为一台 DHCP 服务器，则会发生更加不利的情况。在这种情况下，DHCP 恶意服务器以及企业 DHCP 都将响应每台新设备在网络上启动时发送的初始 DHCP Discover 广播消息。在许多情况下，恶意网关距离交换机不远并将首先响应，在 192.168.0.x 地址空间中授权一个典型的专用网络地址。一切看起来正常，但新设备无法在企业子网上通信。

要快速确定恶意 DHCP 服务器，OneTouch 分析器提供专用的第二 DHCP Offer 检测功能。如果在获取其 DHCP 地址期间通过有线或无线接口收到第二个 DHCP 地址，OneTouch 在主页屏幕上显示一个警告图标。

接入 DHCP 服务器以显示服务器的 IP 地址及其提供的地址。参见图 39。如果恶意 DHCP 服务器首先响应，第二个 DHCP Offer 可能是企业 IP 地址。

图 *39*

我的接入点是否能获得足够的电源？

如今的接入点消耗功率和以前完全不同，因为它们包括两个或三个无线电。OneTouch AT 分析器及其 TruePower™ 测量功能可测量并使 PoE 负载达到 25.5 瓦的 IEEE 802.3at 限值。这样，即使是对最耗电的 AP，你也可以在安装时验证其固有功率。PoE 还隐蔽在从中间馈电器到交换机衍生产品和配置的各种硬件选择中。

在图 40 中，可以看到只能在距交换机 90 米的 AP 位置消耗 23.7 瓦特。回到交换机端口，我们可再次测试功率负载，以便在交换机端口容量和接线板以及水平布线之间进行优选。使用 OneTouch 分析器的捕获功能时，也可测量一个在线 AP 的 PoE 功耗。

部署通过光纤连接的外部 AP？使用 OneTouch 分析器测量通过光纤链路收到的光功率。

因为无线中仍有许多有线，OneTouch 分析器提供一套完整电缆测试。使用 OneTouch AT 分析器的短路/开路/串扰双股电缆测试和 TDR 长度测量了解双绞线电缆。参见图 41。使用电缆识别器和 IntelliTone™ 音频来定位和识别电缆以及闪存端口。

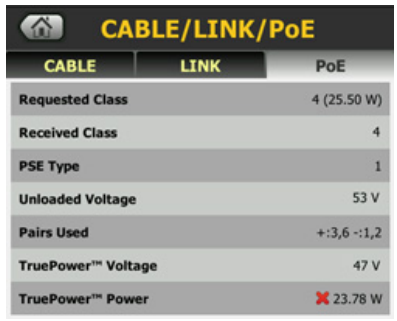


图 *40*

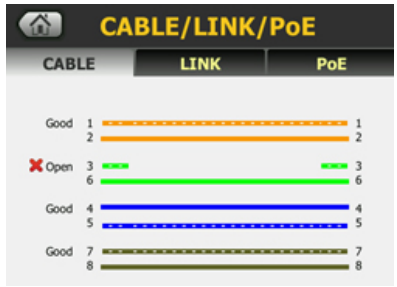


图 *41*

怎样捕获流量？

在需要详细的逐帧视图以解决网络或应用程序问题时，数据包捕获是最终的解决办法。Wi-Fi 捕获的困难之一是通过 MAC 地址的有效负载加密需要通过协议分析器解密。但只有在可以在协议分析器中输入简单密码短语或预共享密钥 (PSK) 的位置使用薄弱的非企业级加密时，这才会起作用。

使用 OneTouch 分析器的内置铜/光纤过滤分路器访问在接入点与交换机或 WLC 之间运行的流量时，可不受阻碍地捕获 Wi-Fi 流量。参见图 42。OneTouch 分析器避免了配置交换机镜像端口或安装独立 TAP 的复杂性，节省了所需的时间和成本。线速硬件过滤器允许您根据 MAC 或 IP 地址挑出一个站，根据端口挑出一个应用程序，如 HTTP，或根据 VLAN 挑出一个用户组。通过管理端口或 SD 卡将捕获文件导出至您偏好的协议分析器（例如 Fluke Networks ClearSight™ Analyzer）中进行解码和分析。

在 AP 在线安装时，OneTouch 分析器提供以太网功率 (PoE) 电压、电流和功率的实时测量，因此您可以量化各种 AP 配置的功耗。

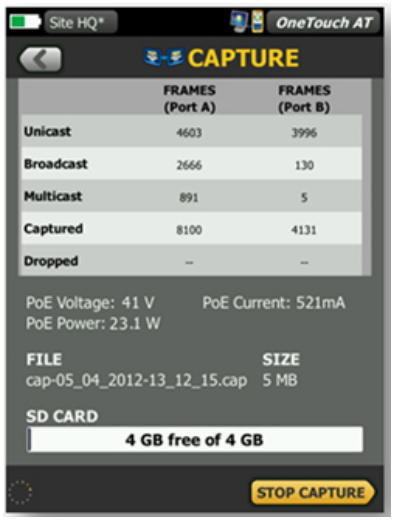


图 *42*

结论

BYOD 已经普遍存在。大部分机构现在允许那些为消费者设计而被他们购买的智能手机、平板电脑和其他智能设备接入企业网络，供个人和企业使用。随着设备的成倍增加，有关无线的争论越多，网络压力、复杂的政策和配置、恶意设备和用户抱怨也越多。Fluke Networks OneTouch AT 网络分析器是用于 BYOD 管理的一个独特的工具。其与您使用的桌面、移动或远程方面的有线和 Wi-Fi 功能的组合，让您能快速记录、量化和故障排除有关 BYOD 和 IT 消费化的问题。

有关 **Fluke Networks** 的 **BYOD** 解决方案的详细信息，请访问 **www.flukenetworks.com/BYOD**