

实验室测试 概述 报告

2011 年 4 月
报告 110411

产品类别:

无线控制器

受测供应商:



受测产品:

思科 Flex 7500
摩托罗拉 WiNG
Aruba VBN



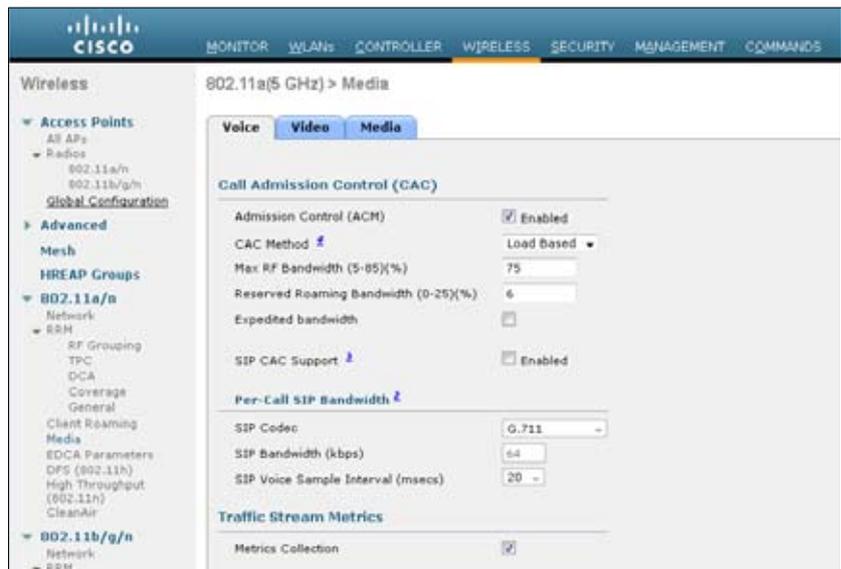
重要发现和结论:

- 思科 FlexConnect 架构允许分支办事处在广域网链路中断或无线控制器不可用时继续工作
- 基于端口的 802.1x 身份验证可以防止安装欺诈无线接入点
- CCKM 的快速漫游不需要交换密钥, 即使在无线控制器故障的情况下也允许漫游
- 提供无线语音动态“呼叫许可控制”(Call Admission Control, CAC) 支持, 可以管理有限带宽和延迟问题, 并保护现有的语音呼叫
- FlexConnect 架构支持灵活的身份验证 — 无线接入点 可以执行对无线客户端的802.1x 身份验证

思 科委托 Miercom 对其以 Flex 7500 无线控制器为代表的 FlexConnect 架构进行了一次独立的验证, 重点在于其应用于分支办事处时部署的弹性。为了进行比较, 我们还评估了摩托罗拉和 Aruba 的解决方案, 具体产品为摩托罗拉 WiNG v5.0 和 Aruba Virtual Branch Networking 2.0。

由于无线在分支的部署已经扩展到了较大的应用规模, 因此还会考虑几个相关因素: 到数据中心的广域网连接中断时分支办事处的业务运营连续性以及部署成本。Miercom 选择了多个指标来评估每个厂商的解决方案在解决这些问题方

图 1: 思科语音 CAC



资料来源: Miercom, 2011 年 4 月

思科语音 CAC 可在无线链路堵塞时管理带宽的使用, 以保护现有的语音通话。管理员可以选择“基于负载”或“基于带宽”的限制模式。

面的效果。我们检查了无线控制器故障和/或广域网链路故障时对新客户端的身份验证能力，以及如何避免高延迟广域网链接上的无线接入点身份验证会话超时的解决方案。最后测试了各个厂商的解决方案如何在 Radius 服务器故障时处理身份验证？

广域网故障期间的分支存活能力包括继续进行移动语音呼叫的能力。为此，我们观察了广域网故障时分支内部继续进行语音呼叫漫游的能力。为了评估带宽有限或者存在延迟问题的情况，我们检查了每个产品提供的“呼叫许可控制” (CAC) 支持。此外，我们还观察了每个厂商解决方案如何防御安装在分支中的欺诈无线接入点的威胁。

在每个指标上，思科 FlexConnect 解决方案都在提供移动分支存活能力上展示了明显的优势，由于无需在每个分支中部署无线控制器，无线分支部署成本方面也有明显的优势。

本地身份验证/分布式客户端身份验证

在无线控制器发生故障或广域网链路发生故障时，思科 FlexConnect 是否会产生任何停止运营时间？我们通过成功将笔记本电脑和 VoIP 客户端与每个供应商的无线接入点关联，并确认通过每个供应商的无线控制器成功的与 ACS 服务器进行身份验证，以此为基准进行测试。然后关闭与数据中心无线控制器的链路来模拟广域网中断。之后我们监测笔记本电脑上运行的 VoIP 呼叫和 FTP 下载会话，以观察是否有任何数据丢失。

思科 FlexConnect 解决方案在无线控制器不可用的这段时间内没有经历任何服务中断。FTP 下载继续进行，VoIP 呼叫保持正常。思科无线接入点可以跳过无线控制器直接使用 ACS 服务器进行身份验证。不仅现有用户可以保持连接，而且新用户也可以使用 ACS 服务器进行身份验证，成功地转发通信流量。用户在无线控制器中断期间没有经历任何停机时间。通过 ACS 上的身份验证日志报告，我们确认了无线

接入点能够直接使用 ACS 进行身份验证。这表明无线接入点正以“独立”模式运行。当与无线控制器恢复联机后，我们观察到无线接入点返回了“连接”模式，这表明现在将使用无线控制器进行身份验证。

摩托罗拉 WiNG v5.0 的情况有所不同。摩托罗拉无线接入点完全依赖无线控制器。在模拟无线控制器中断的过程中，整个分支都失去了无线功能。所有无线接入点都停止了工作，没有广播 SSID。现有客户端失去了连接，新客户无法加入。在网络管理方面增加的问题是：无线控制器恢复时，分支处的每个无线接入点都必须重新启动后才能恢复最终用户的无线连接。

对于 Aruba VBN 2.0，当无线控制器停机时，现有的用户仍保持了其连接。VoIP 呼叫仍然正常，FTP 会话继续下载。但是，新用户无法使用 802.1x 进行身份验证，因为无线接入点无法代替无线控制器进行身份验证，不管 ACS 是否可用。

本地 EAP（无线网络的弹性）

如果数据中心的主要和备份 ACS Radius 服务器都停机时，会发生什么？我们在无线客户端和服务器之间建立 FTP 会话以访问服务器资源。接着，在提供广域网接入（Radius 服务器处于远端）的交换机上关闭连接广域网的端口。我们尝试向 SSID 为 Branch 的无线接入点上添加一个新客户端，并监测该无线接入点的控制台端口以观察是否成功对客户端进行了身份验证。

在思科 Flex 7500 无线控制器以及主要和备份 Radius 服务器都不可用的情况下，现有无线客户端保持正常状态，FTP 传输没有中断。新客户通过直接使用无线接入点进行身份验证成功加入。FlexConnect 解决方案允许无线接入点承担分支备份 Radius 服务器的功能。身份验证过程所花费的时间比基准略多，因为系统需要依次采用备用身份验证方法。分支中数据平面的通信保持正常，分支可以在没

有无线控制器和 Radius 服务器的情况下自主运行。和预期的一样，无线接入点与无线控制器之间没有可见性，因为管理和控制平面已停止运行。摩托罗拉的系统需要具有无线控制器才能让无线接入点保持正常运行。一旦它们之间的链路中断后，就无法进行测试，即仅使用 Radius 服务器在整个分支通信中断的情况下无法进行身份验证。Aruba VBN 在 ACS 不可用的情况下成功保持了到现有客户端的 FTP 下载。但是，新客户无法与无线接入点关联，因为 Aruba 无线接入点无法在没有无线控制器的情况下进行身份验证。此外，只要无线控制器不可用，现有客户端的身份验证计时器过期后也将无法重新进行身份验证。

语音快速漫游和无线网络的弹性

无线弹性方面的一个关键因素是无线客户端在广域网故障期间可以在分支内部进行漫游。一个客户端与第一个分支无线接入点 AP-1 关联。从无线电话向有线电话机发起了一个语音呼叫。然后，使广域网链路停止运行。接着，我们从分支 AP-1 走到分支 AP-2 以强制进行漫游。对语音呼叫进行了监测以观察是否有数据丢失。

思科 FlexConnect 解决方案同时使用 802.1x 和分布式密钥，使得密钥都缓存在无线接入点处。在无线控制器不可用时，这些密钥仍然有效，无线客户端仍可进行身份验证。快速漫游不要求客户端重新进行身份验证。无线语音客户端成功地在分支无线接入点间进行了漫游，没有对呼叫造成任何中断。而竞争友商的解决方案则基本上没有分支通信方面的弹性。摩托罗拉 WiNG v5.0 要求无线控制器可用时才能让无线接入点正常运行。一旦广域网链路中断，无线客户端就无法在分支内部漫游。Aruba VBN 2.0 保持了语音呼叫，前提是客户端保持与最初的无线接入点关联。如果客户端漫游到其他无线接入点，呼叫将丢失，客户端无法与新的无线接入点关联。客户端也无法与原来的无线接入点重新关联，从而使分支内的通信完全丢失。发生漫游时，Aruba 要求无线接入点重新对客户

端进行身份验证，并且在无线控制器不可用的情况下无法在本地验证客户端身份。

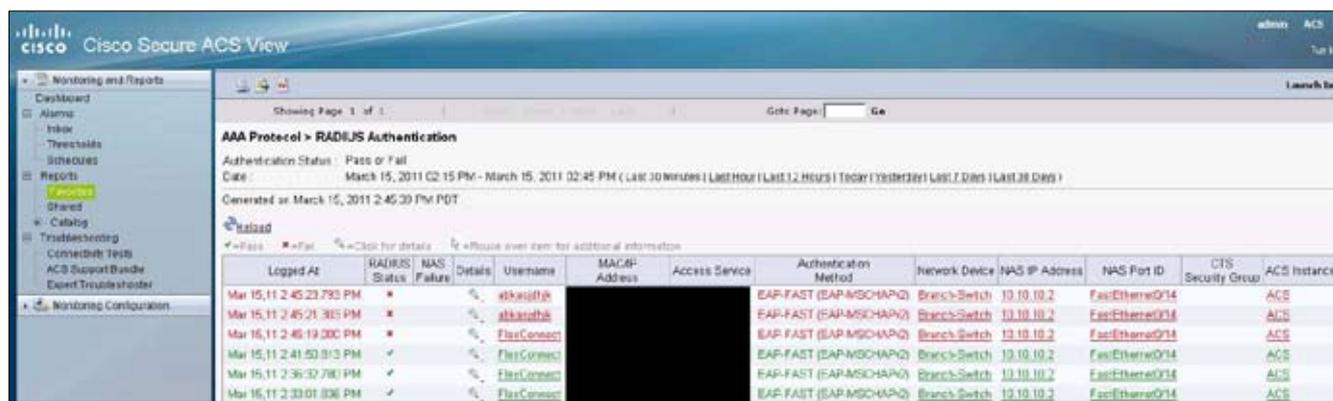
语音呼叫许可控制 (CAC)

我们确认了每个厂商的解决方案支持呼叫许可控制的方式，以及可用于基于负载和静态 CAC 的选项。分支处的呼叫许可控制对在有限的广域网带宽或存在延迟问题的情况下保持现有呼叫的质量至关重要，它可以限制增加新的客户端语音呼叫。

在思科 Flex 7500 无线控制器上，CAC 被设置成一个静态值 (5% 的带宽)。语音呼叫发生在一对无线话机之间。当我们试图发起另一个语音呼叫时，客户端收到了“网络忙”消息，指示 CAC 正在限制网络上的客户端数量。我们观察到在可用的 6,250 kbps 带宽中，使用的带宽为 1,072 kbps。接着，我们将 CAC 更改为 20% 带宽。这次，增加的无线客户端可以成功地进行呼叫。报告的正在使用的是 6,250 kbps 可用带宽中的 3,184 kbps 带宽。仅当无线接入点连接到无线控制器时，才支持 CAC 功能。请参见第 1 页上的图 1。

摩托罗拉 WiNG v5.0 也支持 CAC，可以根据空口时间和无线客户端数量进行限制。但设置有些容易让人混淆，例如，“最大空口时间” (Maximum Airtime) 指定的范围是 0-150，但不清楚采用的是什么测量单位。我们开始时将“最大空口时间”设置为 5。在无线电话与有线电话之间成功建立了呼叫。接着，我们将第二部无线电话与无线接入点关联起来，并尝试进行呼叫。该电话收到“网络忙”消息，不能进行任何呼叫。然后，我们将“最大空口时间”增加到 20。此设置更改需要在无线接入点进行无线电重启后才能生效。在无线客户端与有线电话之间成功建立了呼叫。另外两个无线客户端之间成功建立了另一个呼叫。这证明了摩托罗拉有效地根据可用带宽数量限制了客户端的数量。和思科一样，仅在到无线控制器的广域网链接可用时才支持 CAC。

图 2：失败的端口身份验证



The screenshot shows the Cisco Secure ACS View interface. The main content area displays 'AAA Protocol > RADIUS Authentication' with a table of logs. The table has columns for 'Logged At', 'RADIUS Status', 'NAS', 'Details', 'Username', 'MAC#-Address', 'Access Service', 'Authentication Method', 'Network Device', 'NAS IP Address', 'NAS Port ID', 'CTS Security Group', and 'ACS Instance'. Several rows show 'Failure' in the RADIUS Status column, with the 'Details' column containing 'FlexConnect'. These failed entries are highlighted in red. The table also shows successful entries with 'Success' in the RADIUS Status column.

Logged At	RADIUS Status	NAS	Details	Username	MAC#-Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Instance
Mar 15, 11 2:45:23.793 PM	Failure			akhsjdfh			EAP-FAST (EAPMSCHAPv)	Branch-Switch	10.10.10.2	FastEthernet0/14		ACS
Mar 15, 11 2:45:21.305 PM	Failure			akhsjdfh			EAP-FAST (EAPMSCHAPv)	Branch-Switch	10.10.10.2	FastEthernet0/14		ACS
Mar 15, 11 2:45:19.000 PM	Failure			FlexConnect			EAP-FAST (EAPMSCHAPv)	Branch-Switch	10.10.10.2	FastEthernet0/14		ACS
Mar 15, 11 2:41:50.013 PM	Success			FlexConnect			EAP-FAST (EAPMSCHAPv)	Branch-Switch	10.10.10.2	FastEthernet0/14		ACS
Mar 15, 11 2:36:32.780 PM	Success			FlexConnect			EAP-FAST (EAPMSCHAPv)	Branch-Switch	10.10.10.2	FastEthernet0/14		ACS
Mar 15, 11 2:33:01.036 PM	Success			FlexConnect			EAP-FAST (EAPMSCHAPv)	Branch-Switch	10.10.10.2	FastEthernet0/14		ACS

资料来源：Miercom，2011年4月

当 802.1x 身份验证时提供了不正确的用户凭证，设备将无法使用 ACS 5.2 服务器进行身份验证。失败的身份验证用红色显示在上面。这将阻止安装欺诈设备。

基于端口的无线接入点802.1x 身份验证

在分支无线部署中，存在安装欺诈设备的威胁，这可能会破坏网络的安全性。有线网络上基于端口的 802.1x 身份验证要求输入正确的用户身份凭证，从而提高了安全性。在无线接入点加入网络之前，要向 ACS/Radius 服务器提供身份凭证以便检查其是否为合法设备。我们评估了每个厂商的解决方案提供这种级别的网络安全性的能力。

思科 FlexConnect 解决方案使用分支交换机作为身份验证的代理。分支交换机上启用了端口安全设置。无线接入点配置了正确的 802.1x 身份凭证连接到交换机端口，确认它能够成功地加入无线控制器。ACS 使用 Radius 和共享密钥，无线接入点支持作为 802.1x 客户端，对连接到边缘交换机的无线接入点进行身份验证。欺诈无线接入点无法进行身份验证，因此不会获得 IP 地址。请参见图 2。

摩托罗拉和 Aruba 都不支持无线接入点作为 802.1x 客户端。摩托罗拉 RFS 4000 无线控制器有一个 802.1x 身份验证区域，但“启用” (Enable) 复选框已变灰，不能选择该选项。

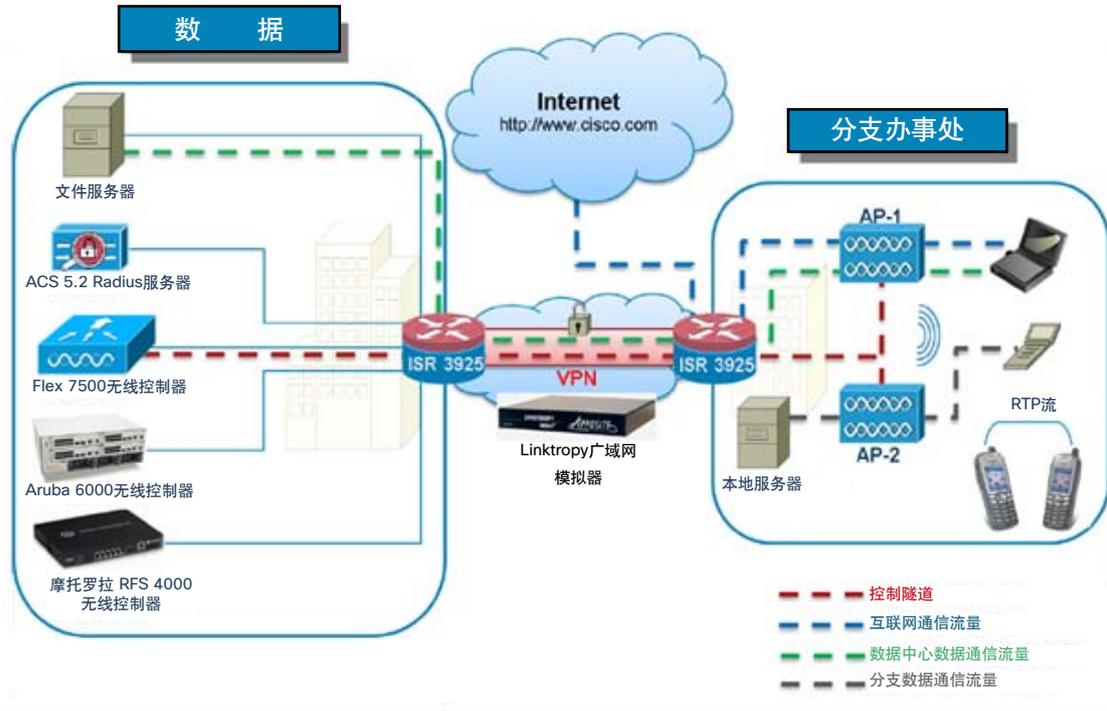
结论

对于使用无线策略进行分支部署的大客户，分支架构的弹性和部署的成本控制是关键性的考虑事项。思科 Flex 7500 无线控制器中采用的 FlexConnect 架构是这次测试中完全达到这些指标的唯一解决方案。

如果中心身份验证由于无线控制器或广域网链路故障而不可用时，FlexConnect 架构可以使用无线接入点在本地对无线客户端进行身份验证。广域网链路失效时 FlexConnect 架构可使无线客户端在分支内部漫游。要提供同样级别的弹性，则需要每个分支配备主要和备份无线控制器，这会大大增加分支部署的成本。思科 FlexConnect 架构使用 802.1x 身份验证来防止在分支中安装欺诈无线接入点，提高了网络安全性。

配备有 Flex 7500 无线控制器的思科 FlexConnect 解决方案在提供无线分支存活能力上表现非常出色。

测试台示意图



测试条件和方法

数据中心的网络架构组件包括思科 Flex 7500 无线控制器、Aruba 6000 无线控制器（软件版本v6.0.0.1）、摩托罗拉 RFS 4000（软件版本v5.0.3.0-001 R）、思科 ISR 3925 路由器提供了站点到站点的 VPN 连接、文件服务器（Windows Server 2008 R2）和思科 ACS 5.2 身份验证服务器运行在 VMware ESX 下。在分支办事处，我们部署了配置为 FlexConnect 模式的思科 Aironet 3500 系列和 1040 系列无线接入点（也称为 HREAP 无线接入点—混合远程边缘无线接入点）、配置为远程无线接入点模式的 Aruba 105 无线接入点、以及摩托罗拉 650 无线接入点、思科 ISR 3925 路由器（提供 VPN 和呼叫管理器功能）和无线客户端（笔记本电脑和思科 7921G IP 电话）。数据中心通过 VPN 使用广域网连接到分支办事处，使用 Apposite 广域网模拟器来模拟 T1 线路。分支办事处中有来自每个供应商的两个无线接入点，一个无线 PC 客户端，两个思科无线 VoIP 客户端，以及一个思科有线 VoIP 电话。

每个厂商的无线控制器都专门针对分支站点进行了配置。这将允许分支站点的无线用户直接访问互联网，而不是返回到数据中心后再访问互联网。内部通信流量保持在本地，互联网和数据中心的流量被向外转至不同的路径（基于路由器中的访问规则）。此分支部署可以节省广域网的带宽，提高分支用户的速度。两个无线接入点相距大约 30 英尺，配置了最低的信号强度。无线接入点上的低信号强度可确保无线信号不会重叠，使其更易于进行漫游测试。

Apposite Linktropy (www.apposite-tech.com) 广域网模拟器用于模拟数据中心与分支站点之间的 T1 广域网链路。两个站点之间的带宽限制在一个 1.44 Mbps 链路上，广域网延迟设置为 40 毫秒，数据包丢失率设置为 0.1000%。

每个供应商的无线控制器采用相同的配置以保证测试的公平性。测试环境在每个供应商产品的测试过程中保持不变。

对于希望采用相应的测试和测量设备重复测试的客户，可以重复本报告中的测试。如果当前或潜在的客户希望重复这些结果，可以与 reviews@miercom.com 联系，获取有关应用于“测试系统”的配置以及在此次评估中所用测试工具的其他详细信息。Miercom 建议客户进行需求分析研究，在做出选择之前专门针对预期产品部署环境进行测试。

Miercom 性能认证结果

根据我们的测试和观察，在与类似产品比较的情况下，思科 Flex 7500 无线控制器获得了存活能力和分支办事处网络弹性方面的性能认证。

Miercom 测试了无线控制器或广域网链路故障时的身份验证流程，观察了广域网故障期间的漫游语音呼叫，检查了带宽有限的情况下的 CAC 支持，并分析了 FlexConnect 架构如何防御欺诈无线接入点。

在所有的测试中，思科 FlexConnect 解决方案在提供移动分支存活能力上展示了明显的优势，同时由于不需要在每个分支中安装无线控制器，在控制无线分支部署成本方面也有显著优势。



思科 Flex 7500



思科系统公司
170 West Tasman Drive
San Jose, CA 95134
1-800-553-6387
www.cisco.com

关于 Miercom 的产品测试服务

Miercom 多年来已经在多种领先的网络商业期刊上发表了几百份产品比较分析文章，其中包括《Network World》、《Business Communications Review - NoJitter》、《Communications News》、《Exchange》、《Internet Telephony》以及其他优秀出版物。Miercom 作为领先的独立产品测试中心，享有毋庸置疑的可靠声誉。

Miercom 的专门测试服务包括竞争产品分析以及个别产品评估。Miercom 提供综合的认证和测试方案，其中包括：互操作性认证 (Certified Interoperable)、可靠性认证 (Certified Reliable)、安全性认证 (Certified Secure) 和环保认证 (Certified Green)。我们还在“广告网络” (NetWORKS As Advertised) 方案下进行产品评估，这是行业中最全面可靠的产品可用性和性能评估。



报告 110411

reviews@miercom.com

www.miercom.com

 在打印之前，请考虑分发电子版

本报告中提及的产品名称或服务是其各自所有者的注册商标。Miercom 竭尽全力确保我们报告中所包含的信息精确完整，但不为任何错误、不精确或遗漏负责。Miercom 不为本报告中包含的信息引起的或与该信息有关的损害负责。如需特定的客户需求分析，请向专业服务机构（如 Miercom Consulting）咨询。