如何规划成功的校园网迁移

使用 OSI 模型作为提醒检查表，避免各种问题

白皮书

执行摘要

为大学校园寻找新的 WiFi 供应商可能有很多原因。但不幸的是，供应商迁移也会产生很多问题：关键应用程序的中断、网络中断、愤怒的用户以及 IT 人员面临的堆积如山的客服请求，这只是列出了几个例子而已。

WiFi 迁移过程中伴随出现的各种问题是非常真实的，但这些问题也不是不可避免的。退一步讲，我们不妨考虑下传统的 OSI 网络模型，仔细考虑新供应商的基础设施对各网络层产生的影响以及当用户和流量从一个供应商的区域跨越到另一个供应商时的边界条件，就可以在实现各种 WiFi 目标时面临最小的风险和更少的困难。

本白皮书将为如何将新 WiFi 供应商的网络引入到各种情况，各种规模的大学现有校园基础设施中提供深入的指导。这些知识有助于让你了解制定合理策略需要关注的问题，使用 OSI 模型对每个网络层的变化进行考量，避免常见的陷阱，并了解基于证书的设备接入门户如何为基于位置的策略控制带来新的机遇。

校园 WIFI 迁移检查表

- 定义边界线 — 首先清晰界定哪个供应商负责哪个区域。在可能的情况下，确保供应商覆盖区域与物理环境的自然边界一致，例如：
  - 室内 — 通过具体的教学楼、宿舍楼或侧楼划分覆盖范围的边界。
  - 室外 — 确定覆盖范围是庭院、运动场，还是整个校园。
  - 在建筑物内 — 对于较大的建筑物，如有必要，定义内部覆盖范围的边界，例如在建筑物东西侧楼之间。

  想一想这些边界随着时间的推移将产生怎样的变化。如果可能的话，按区域制定网络开通时间表。
- 第 4 层到第 7 层 — 应用程序和用户体验
  - 仔细考虑每个覆盖区域内的应用程序和用户需求。
  - 确定所支持的应用程序是教学目的、娱乐目的还是混合目的。
  - 确定是否允许流媒体服务。
  - 仔细考虑网络流量的策略影响。
- 第 3 层 — 路由包
  - 确定将通过集中隧道式 WLAN 还是本地数据分流来对流量进行路由。
  - 仔细考虑 DHCP、DNS 和其他第 3 层服务跨界的影响。
- 第 2 层 — VLAN 和广播域
  - 仔细考虑对宿舍的影响，包括如何保证用户隐私以及是否将实施个人 VLAN。
  - 仔细考虑报告厅共享资源的影响，包括系统将如何处理 Bonjour 和其他广播协议。
  - 仔细考虑“热点”区域（图书馆、学生会）的影响，以及如何使用带有互联网接入功能的客户端隔离。
  - 评估交换机是否需要更新换代，考虑新接入点需要的以太网供电（PoE）预算。
- 第 1 层 — 信道选择和无线资源
  - 确定实际接入点安装位置。仔细对场地进行规划，确保它们不会相互干扰。
  - 指定覆盖基站，并尽可能确保它们与自然物理边界一致。
- 回到开始的位置
  - 回顾为解决每个网络层面临的问题而采取的步骤，并确保您理解在一个层上做出的选择对其他层的影响。

校园 WIFI 迁移深入剖析

在现代的大学校园里，WiFi 是一项非常重要的基础设施。WiFi 出现掉线、下载速度过慢、反复提示重新输入登录凭据等奇怪的问题，每个人都会痛苦无比。这种情况会导致学生在社交媒体上疯狂“吐槽”，让学校校园在潜在生源中的声誉受损。在这个过程中，IT 人员也会因各种投诉和客服任务而忙得不可开交。

如果你的校园也是这样，那么现在就是时候改变了。但做出引入新无线网络供应商的决定并非易事。在不影响用户、IT 人员或现有服务的情况下弄清楚如何在校园中部署新的基础设施要困难得多。但这并非不可逾越的鸿沟。

开始着手规划方案时，要注意 4 个关键的领域，包括各项迁移工作的优先顺序，如何管理用户和 IT 人员的体验，建立基于证书的设备接入机制，简化安全和策略控制机制的优势，以及最重要的一点，如何清晰定义新的和现有的供应商之间的边界条件，包括在 OSI 网络模型每一层进行边界跨越所产生的影响。我们将在以下章节中详细讨论这一过程中涉及的每个方面。

主要关注最优先的工作任务

要想在任何迁移中取得成功，最重要的因素就是要对你希望实现的目标有一个清晰的了解。在与数以百计的高校客户进行的讨论中，各大院校往往会优先考虑这四大基本目标：

- **在对用户影响最小的前提下进行迁移：**在这种方案中，目标就是在无人察觉的情况下开始使用新的供应商。这意味着要避免在人们工作或学习的地方进行计划外施工或电缆铺设。在新建筑或正在改造的建筑物中部署新的供应商设备是评估室内项目新供应商的理想选择。开始，也可以先进行新供应商室外部署，因此不会对任何课程或室内空间产生影响。
- **以最短的 IT 工作时间、最低的成本和最小的精力进行部署：**在这种方案中，IT 预算和资源可能比较有限，或者只想简单地引入第二个供应商，以便与当前的基础设施进行对比。这种方案中，户外部署是一个很好的选择 — 因为户外接入点的每个接入点可以覆盖更大的空间区域，可以减少新接入点的需求量，进而减少部署和管理的工作量。对于室外空间而言，一般情况下，不需要进行过多现场调查，也可最大限度地对新设备加以利用。作为一种低成本/低工作量的替代部署方案，也可以选择在 IT 大楼内部署新设备。在这种方案中，可能需要提前在现场进行调研，但可以自己体验变化。
- **实现最大的使用者效益：**这种方案在某种程度上与第一种方案相反，因为你希望用户注意到所发生的变化。比如说，如果试图通过新的供应商进行投资较大的改造项目，这种方案可能会是比较明智的选择。通过在学生会、图书馆或自助餐厅等学生、教师和管理人员经常使用的热门区域进行部署，可以展示新的供应商设备的成功并产生需求。因此，如果用户问为什么新地点的 WiFi 比宿舍/报告厅快这么多，可以解释说，这是新供应商提供的新技术，以及将这样的性能水平扩展到其他区域所需要的预算。
- **实现最大的 IT 人员效益：**在这种方案中，需要努力减少 IT 人员需要着力解决的 WiFi 相关问题，包括用户投诉和客户支持请求。一般情况下，这些问题来自设备连接、接入点过载和空域问题。具体来说，可以先在宿舍或报告厅进行部署，这些地方是最容易产生问题，用户最密集、最复杂的地方。或者，也可以在客服帮助请求最多的区域开始部署，以便验证自己制定的部署优先顺序。

这些方案都不是“放之四海而皆准”的 — 最理想的方法就是做到面面俱到。但如果想要正确评估通过新供应商进行的项目投资，就必须决定这些方案中的哪个方案符合自己的工作优先顺序。

对体验进行管理

无论如何对实施目标进行优先排序，都需要仔细考虑为用户和 IT 人员提供的经验。记住，无论这只是整个校园改造的第一步，还是针对目标领域的长期解决方案，校园里都将建立起一个多供应商参与的 WiFi 环境。这可能意味着，你也在创建一个“多种体验”的环境，所以要进行相应的规划。需要考虑的问题：

- **学生的需求：**当学生通过新供应商的基础设施接入网络时，他们会希望使用相同的设备并访问相同的应用程序，而且要有相同或更好的性能。他们不希望他们使用的网络掉线，或者必须不断输入密码才能重新连接网络。对于计划内的迁移过程，应该坚持的原则是“不会引起新的问题”。
- **IT 人员的体验：**一般来说，IT 人员都希望所有工作都能尽量简单。一个例子就是，在任何供应商的基础设施中，所有设备（有线或无线）的安全策略、访问权限和特有权限都有一个一致的框架，没有安全隐患。

使用基于证书的接入方式进行统一管理

在理想的情况下，我们都会有安全和策略管理平台，这类平台与基础设施和供应商无关，可以简化策略管理和接入安全性，还可以为用户提供简便的接入。幸运的是，有一种很常见的方法可以满足这些要求。自助式接入方法可以使用数字证书来简化安全和策略控制。许多院校已经使用类似的平台来为用户提供简便的接入，或者已经对“自带设备”（BYOD）的安全和策略管理进行了简化。但这种方法对多厂商迁移过程的导航也非常有用。

因为平台与供应商和设备无关，所以它可以避免同时运行两个不同供应商的基础设施所产生的诸多问题。平台支持所有主流的客户端操作系统，可以签发用来访问供应商基础设施需要的证书。用户只需进行一次设备注册过程，此后无论如何连接，在何处连接，都无需再次输入访问凭据。他们将保持连接状态，直到证书过期或被撤销，而且从一个供应商的区域移动到另一个供应商区域时不会发现任何变化，因为他们的设备已经有了正确的证书。同时，IT 人员可以保有一套接入和安全策略，并且可以让证书平台对将策略应用到通过不同基础设施进行网络连接的设备所产生的复杂性。

可以通过想象将使用接入和策略平台与实施教育漫游的方式进行对比，除了在自己的校园内。使用教育漫游的方案，访客用户可以使用本校的接入和身份验证基础设施安全地通过身份验证并连接至所在院校的校园网络。如果院校同时使用基于证书的接入和策略平台和教育漫游方案，他们可以有效地运行两种身份验证模式，一种方式用于通过 802.1x RADIUS 身份验证方式进行身份验证的本地用户，另一种方式则用于通过远程方式进行身份验证的访客用户。接入平台可以处理这两种身份验证方法的复杂性，这样访客用户不需要进行任何额外的操作步骤。他们打开他们的笔记本电脑，通过身份验证并接入网络，整个过程一气呵成。

在校园网供应商迁移过程中，从概念上讲，就是在做同样的工作，管理两种不同的身份验证过程，一种是通过供应商 A 的基础设施，另一种则通过供应商 B 的基础设施。对于用户而言，在体验上没有任何区别，他们的设备会自动连接，从一个供应商覆盖的区域移动另一个供应商覆盖的区域，他们无需进行任何操作。

仔细考虑边界和 OSI 层

作为网络工程师，我们大多数人都学会了如何使用 OSI 模型来构建我们的思维，在 WiFi 供应商迁移这样复杂的情况下，我们也可以通过回归这一常用的方式来避免出错。

WiFi 的独特之处在于它是一种基于位置的移动设备接入技术。当然，以太网端口也有特定的位置，但通常情况下，通过以太网接入网络的设备移动性比较有限或者根本无法移动。但 WiFi 设备的设计目的就是实现频繁的位置更改。因此，从 WiFi 迁移规划的角度来看，可以将其抽象地定义为“边界”。WiFi 用户会不断跨越边界，移动到新的位置。每个位置对应用情况（第 4-7层）、不同 IP 地址和路径（第 3 层）、不同 VLAN 和漫游需求（第 2 层）以及不同 WiFi 供应商的接入点（第 1 层）的需求可能都不尽相同。鉴于此，定义边界并仔细考虑跨越既定边界会对哪个 OSI 层产生影响将有助于定义给定位置的策略和每个位置的边界变更策略。

例如，学生在报告厅和宿舍时就会有不同的需求。在宿舍里，学生们会使用许多他们在课堂上不能使用的应用程序（在线游戏、IPTV 视频流等），而且还希望他们的个人设备与其他用户隔离开来。而报告厅需要允许所有设备同时访问教室或报告应用程序，但可能会阻止或控制 Netflix。在这些位置接入网络的用户和设备的目的是非常不同的，各种网络层的政策和技术影响也会有所不同，尤其是从一个覆盖区域移动到另一个覆盖区域时。从规划的角度来看，当每个 OSI 层的 WiFi 考虑因素与所在位置的物理边界匹配时，就可以更加顺利地进行迁移并提供更好的体验。

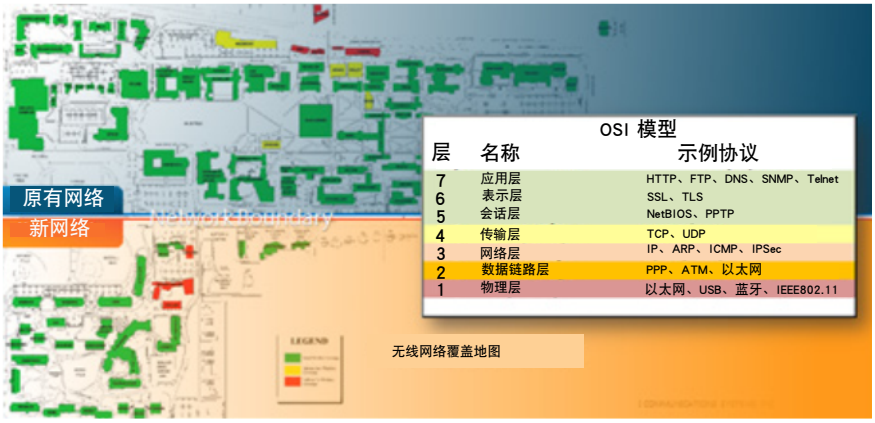

图 1：将“OSI 模型”视为一种框架。

从根本上讲，良好的 WiFi 漫游体验可以确保用户从一个区域跨越到另一个区域时可以实现正常的网络连接。之后，针对每一个层，应该仔细考虑当用户越过边界，从一个供应商的覆盖区域跨越到另一个供应商的覆盖区域时，OSI 层的服务将会面临什么情况。归根结底，边界跨越是最有可能出现问题的地方，而且，这些问题可能跨越多个 OSI 层。这意味着，不同的层不能相互隔离，一个层的需求会对其他层产生影响。例如，第 3 层的需求可能对第 1 层中做出的选择有直接影响。但是，如果要实现积极的用户和 IT 人员经验，就应该在部署之前仔细考虑这些影响。

一般来说，要不断问自己，这些边界对 OSI 模型的每一个层都意味着什么，以及部署方案的地理边界在哪里。在可能的情况下，要确保这些边界的一致。

以下章节将对 OSI 模型的每一个层进行介绍。我们将对应该考虑的事项进行探讨，并为每个方面的问题提供一个检查表，以确保做到万无一失。

边界线：定义覆盖区域

深入研究信道复用、信号传播等特定的 WiFi 问题前，请打开一张校园地图并定义覆盖区域。几乎可以肯定的是，这将与建筑物对齐，但也不排除按照室外区域进行划分，或在适当时将较大的建筑物分割成若干部分。为了尽可能简单地划分新旧供应商的覆盖区域，需要按照校园的自然地理情况进行划分。这也是制定网络开通时间表的关键步骤，因为定义覆盖区域后，就可以确定这些区域的迁移顺序。在许多情况下，可以使用此过程将工作量划分为更小、更易于管理的部分。

覆盖区域检查表

- ❑ 将校园划分为与自然边界一致的覆盖区域（如建筑物的墙壁算作室内区域，庭院的自然事物算作室外区域）。
- ❑ 确定每个区域是否已经有 WiFi，以及新供应商的基础设施将取代现有的基础设施，还是会构成一个新的网络开通位置。
- ❑ 确定位置是否需要进一步细分划分。一栋有两个大型侧翼建筑或多个楼层的建筑物可能需要使用一个以上的覆盖区域。
- ❑ 定义该空间中 WiFi 使用区域的大致轮廓。
  - ❍ 确定预计的用户密度。
  - ❍ 定义不同地点/使用情况下的大致 WiFi 使用需求：
    - ▪ 宿舍
    - ▪ 热点
    - ▪ 一般教室/办公室
    - ▪ 报告厅
- ❑ 如果可能的话，在规划过程的早期对位置列表进行优先排序。但是，要知道此检查表需要重复使用。对迁移计划进行充实时，应该不断地重新审视每一个 OSI 网络层，以确定一个层的变化和决策将对其他层产生何种影响。

第 4-7 层 — 应用程序

在上层网络层，尽量不要迷失在“管道”中，相反，首先要确定网络存在的目的是什么。用户到底用它来做什么？对于一个报告厅而言，可能需要支持 Mediasite、Blackboard 和 Lync 等应用程序，或者可能需要保证大厅里的每个人都接入到一个特定的 VLAN，以便更好地管理广播应用程序和共享，但需要对其他流量进行更加严格的控制。如果在宿舍，就要用到媒体应用程序（Netflix、Skype、IPTV），这些应用可能不会被当作一个教育机构的“任务关键型”应用，但对于住校生来说却非常重要。

当用户移动时，需要保证哪些应用程序可以正常工作？当用户到达目的地时，哪个应用程序可以停止并重新启动？一般来说，简单的数据应用比流式视频或 IP 语音（VoIP）应用要稳定得多（且跨越边界的能力更好）。如果要应用服务类型、服务分类或服务质量（QoS）策略，或在某些特定区域启用或限制应用程序，则需要在供应商 A 和供应商 B 的区域之间保持一致。

应用程序检查表

- ❑ 确定每个位置中哪个应用程序最重要并定义服务区域。
- ❑ 报告厅
  - ❍ 定义将会允许的多媒体应用程序（如 Mediasite、Blackboard、Lync 等）。
  - ❍ 确定对流媒体和游戏等“娱乐性”应用程序将会采取允许、禁止，还是阻止操作。
  - ❍ 确定是否应用严格的内容过滤。
- ❑ 宿舍
  - ❍ 根据提供“家一般”体验的原则定义策略，很有可能允许所有类型的流媒体、社交媒体、游戏等。
  - ❍ 确定将使用多少内容过滤（如有）。
- ❑ 热点
  - ❍ 确定 WiFi 将在哪些空间用作公共热点，比如在图书馆、室外、学生中心和餐厅等位置。
  - ❍ 检查公共接入区域的策略，例如是否应用了轻微内容过滤。
- ❑ 检查前面定义的覆盖区域，并评估某个给定区域中的应用程序需求是否需要更改映射的位置边界。

第 3 层 — 网络架构

在第 3 层，接入点允许用户设备接入网络。因为已经有了一个网络架构，现在，了解新的基础架构将如何适应这一架构很重要。考虑网络边界的 IP 寻址方案和 VLAN。在基本层面上，它用于跟踪数据包的去向，以及当用户越过边界，数据包是否将到达它们应该到达的目标位置？

这一层的决定会反过来与其他层相关联，尤其是上层应用程序需要注意的事项。如果用户在跨越地理边界时需要流媒体或 VoIP 呼叫，那么网络不强制他们获得新的 IP 地址非常重要。相反，如果用户越过边界时不需要新的 IP 地址，那么从对第 3 层对部署方案的影响进行规划的目的出发，它就不算是一个真正的边界。仔细考虑这些决定；你可能被迫根据供应商 A 或 B 的地理起点部署某种方法。

在我们亲身经历的一个案例中，WiFi 被添加到自助餐厅，而咖啡厅对面的接入点则被插入到完全不同的子网中。当用户走到房间的对面去喝苏打水时，他们的手机会从一个网络转移到另一个网络。尽管用户仍然在同一个房间，但网络会不断地停止和重新启动用户会话。每个人都可以接入 WiFi，每个人都可以上网，但每个人都要跨越第 3 层边界，但这种情况下其实本应有一个统一的网络。不要让这种事发生在你身上！幸运的是，解决方案比较直观–将接入点插入相应的交换机即可，网络边界和建筑边界（在这一案例中，即用于界定自助餐厅空间的墙体/窗户/楼梯间）通过该设备实现一致。

信道和本地数据分流

在迁移规划中的这一时间点，应该回过头来，仔细考虑一下基本的 WiFi 架构。许多供应商通过信道将 WLAN 接入中央控制器，尤其是在较陈旧的实施项目中。而另一些人则喜欢对网络流量进行本地数据分流，而且速度较快，目前业内更倾向于这一方式。不过，只有你可以确定是否需要从一个模型迁移到另一个模型，以及当前是否是进行供应商迁移的好时机。你需要仔细考虑现有的架构，并决定这种选择将对用户体验产生什么影响，以及对于 IT 人员，它将意味着什么。

网络层检查表

- ❑ 检查每个位置当前的网络架构。
  - ❍ 对于现有 WiFi 覆盖的区域而言，确定它们是使用隧道式架构，还是本地数据分流，以及你会继续使用当前的模型，还是要进行更改。
  - ❍ 评估架构将对 IP 寻址方案产生怎样的影响。
  - ❍ 确定有线和无线客户端将在同一个子网上，还是将在不同的子网上。
- ❑ 检查 DHCP 方案，并评估它是否会改变。
- ❑ 检查 DHCP/DNS 服务器的位置。
- ❑ 检查路由器的位置和当前第 3 层的边界，并确定它们是否与新基础设施一致。
- ❑ 检查第 3 层边界加入整体网络的方式，以及目前的模式是否仍然科学。
- ❑ 检查 VLAN 和 VLAN 边界。
- ❑ 满足不同位置类型的特定网络层要求。例如，在报告厅，就要确定是否：
  - ❍ 使用一个广播域
  - ❍ 在第 3 层使用客户端隔离
  - ❍ 保留特定的可访问系统“白名单”。

第 2 层 — 漫游和 SSID

从根本上说，接入点可以充当具有虚拟端口的交换机。从本质上讲，SSID 是最终用户端口，因此管理 SSID，尤其漫游方面的管理，是防止多供应商部署项目失败的核心因素。考虑为不同供应商的基础设施使用相同，还是不同的 SSID，以及供应商之间的数据链路边界会对用户和身份验证产生怎样的影响。

在过去的十年里，尽可能使用一个 SSID 的做法已经成为一种最佳实践。要知道，多个 SSID 会强制执行多次接入活动，自然产生麻烦的可能也越大（更不用说，没有人原意看到可以连接到 20 个不同匿名 WiFi 网络的选项）。但自助式接入端口的引入为这种惯常的做法赋予了新的含义。接入门户可以毫不费力地加载十几个或更多的 SSID 配置文件，用户同样也无需进行繁琐操作。过去，数学楼、化学楼、学生活动中心和宿舍内的不同 SSID 每次发生变化时都需要用户交互（和随后发生的大量客服电话）。今天，每个 SSID 配置文件可以在其只需进行一次的注册操作时预加载到每台设备上。

但多个 SSID 实际上可以有助于故障排除和策略分配，尤其是在多供应商环境。如果需要向特定的地理区域部署新的供应商，从策略角度讲，在 SSID 之间划清界线可以让网络设计师和 IT 支持人员的工作更加简单。如果根据 SSID 对供应商进行细分，这样就可以更加容易地识别拨打客服电话的客户使用的是哪种系统，这样就无需费力地同时对两个不同的系统进行处理。如果需要对跨越特定边界的过程进行调整，就可以快速识别这种状况，并对这一位置的 BSS 初始最低率或 Tx 功率进行调整。

交换机更换和 POE 预算

新的接入点技术耗电量往往更大。改造方案的供电需要交换机升级，外加 PoE 供电模块，还是midspan？如果要改造为四串流 11ac 接入点，就可能需要 802.3at 供电。交换机可以支持大功率 PoE，但支持的端口比当前 802.3 af 供电接入点的端口更少。同时也有两种方法可以对这一功能进行分析，从接入点侧，或者从交换机侧。所有接入点供应商都会有低功率模型（如二串流和四串流），或者很可能，他们的高端，高功率模型也有低功率选项。在迁移计划中，这些方案都可以接受吗？从另一个角度看，仍然需要对交换机进行升级吗？现有交换机有接入点计划的 PoE 预算吗？一定要保证交换机计划与接入点计划一致。

第 2 层检查表

- ❑ 无线侧
  - ❍ 确定每个位置将运行的 SSID，以及它们将如何与策略进行映射。
  - ❍ 检查当前在某一位置运营的供应商，以及在该位置进行迁移的优先顺序。
  - ❍ 确定将来需要的接入点数量。（见下一章节。）
  - ❍ 确定将使用哪一个 VLAN。
  - ❍ 确定有线层 2 广播域是否将与无线层 2 的广播域一致。
- ❑ 有线侧
  - ❍ 确定接入点将回程至哪些交换机，它们是否支持 PoE。
  - ❍ 检查当前 PoE 预算，确定是否可以支持所有接入点。这对运行 11n 或 11ac 以及很快就可以运行 11ax 的新接入点尤为重要。
  - ❍ 检查路由器的位置并确定在这个覆盖位置执行您需要的策略所需要的条件。确定上游网络设备是否可以满足策略要求，或者是否需要新的防火墙。
- ❑ PoE 基础设施
  - ❍ 盘点可用高功率 PoE 端口数量
  - ❍ 确定需要交换机升级，外加 PoE 供电模块，还是需要midspan
  - ❍ 确定低功率模式下接入点的功能权衡问题
  - ❍ 保证交换机计划与接入点计划相一致（例如，确保四串流 11ac 接入点与 802.3at 供电一致）

第 1 层 — 物理环境

在这一层，应该考虑覆盖基站和接入点放置的分组。事实上，即使是最先进的无线系统，无线信道管理仍然会非常复杂。要尽量详细地按照供应商划分覆盖区域。不应该对供应商进行混乱的分组，而且要避免两个系统在空域和信道方面相互冲突。

当然，网络边界不是直的。但应尽可能清晰地对边界进行划分。如果可能的话，根据用户导航的实际地理环境划定边界，为建筑物、大型建筑侧翼、室内和室外服务设施之间的过渡区域等定义网络边界。

开始实施时，考虑使用预测性现场调查计划工具。如果新供应商的基础设施是现有网络的扩展设施，就无需过分担心第 1 层的边界。但如果是在现有位置更换基础设施，就需要考虑以下几个问题。是否要一次性对整个建筑/场馆/地点进行改造？如果是大型建筑物，是否需要分阶段进行迁移？接入点的位置会改变吗？如果会，相应区域有电缆吗？是否可以在不产生任何影响的情况下将接入点布置在同一个地方吗？如果不能，铺设新的线路将产生何种程度的中断？

第 1 层检查表

- ❑ 检查现有的现场调查，如有必要，进行新的调查。
- ❑ 确定待部署的接入点位置是否存在以太网线，是否可以重用现有的电缆，还是要铺设更多电缆。
  - ❍ 如果在不做现场调查的情况下重用当前接入点位置，升级技术和更换供应商时要谨慎操作。
- ❑ 确定何时可以完成物理切换，以及可接受的中断程度。如果可能的话，短暂中断或周末可能是最好的选择。
- ❑ 仔细考虑户外部署的影响。
  - ❍ 检查具体在哪里可以接入网络和/或连接电源。
  - ❍ 注意树木和其他障碍物。可以在冬季（树上没有树叶时）进行现场调查，不可在春天（树上长满树叶时）进行调查。
  - ❍ 确定是否需要全向（扇区）接入点。
- ❑ 仔细考虑整个学年将发生哪些情况变化。
  - ❍ 这不仅仅只是室外考虑。例如，学生可能会移动可能阻碍接入点的家具。

重新检查区域边界

现在，你已经了解了每个 OSI 网络层上要注意的 WiFi 问题，现在让我们回到项目开始时定义的边界。鉴于对第 1-7 层进行的分析，原边界地图还可以继续使用吗？需要对任何区域进行修改吗？

重新检查区域边界检查表

- ❑ 检查为不同供应商定义的边界线。
- ❑ 检查 SSID 之间的边界线。
- ❑ 再次仔细考虑接入点布置，将在供应商、SSID 和服务区域之间的漫游问题降至最低水平。

RUCKUS CLOUDPATH ENROLLMENT 认证系统

校园网供应商的迁移可以很快就变得非常复杂。但使用自助式、基于证书的接入和策略平台可以大大降低在供应商基础设施之间进行移动产生的复杂性，使迁移过程对用户和 IT 人员而言可以更加顺利。

Ruckus Cloudpath Enrollment 认证系统 (ES) 被世界各地的各大院校广泛使用，可提供安全的自助式接入和策略控制方法。系统采用 WiFi 安全领域的黄金标准，带有 EAP-TLS 的 WPA2 企业，可提供全面的证书服务，避免用户可能遇到的各种密码和接入问题，同时为 IT 人员简化设备和策略管理工作。与供应商完全无关的平台 Cloudpath 平台可以提供功能强大，成本效益较高的工具，有助于网络迁移和多供应商基础设施的管理。Cloudpath 可提供：

- **自动接入：**用户可随时接入自助式门户，该门户可为所有适用校园网络自动对设备进行配置，包括来自多个供应商的有线和无线基础设施。
- **证书基础设施：**支持策略的证书可在校园各处将用户、设备和策略联系在一起，无需密码。
- **设备完全可见：**IT 团队可以跟踪网络上每台设备，了解“用户身份、设备类型和使用目的”。
- **强大的安全性：**Cloudpath 使用从未被黑客破解过的网络安全黄金标准，带有 EAP-TLS 的 WPA2企业版。
- **丰富的策略控制方式：**可以定义 VLAN、ACL 和基于用户、群组、设备和更多条件的策略。这样，就可以更加容易地创建基于学生或基于房间的 VLAN，并应用细粒度设备控制方法。
- **支持多种设备：**Cloudpath 基本上支持所有用户设备，iOS、Android、ChromeOS、Mac OS X、Windows、Linux 等等。
- **WiFi 可靠性：**通过从密码方式转换为证书形式，可以避免与密码相关的断开和重新登录的情况，还可避免因这些问题产生的客服支持电话。
- **经过简化的策略：**Cloudpath 可一次性将用户设备注册到多个 SSID，从而可以更加容易地应用基于位置的策略。

Cloudpath 平台的核心是一个自助式接入门户，该门户允许管理员通过高度灵活，但容易理解的方式对策略进行定义。用户可以在校内，甚至是到校前在家访问接入门户，以便接入他们的设备。你可以在上课前向学生发送门户链接，这样他们就可以注册他们所有的设备，并在他们进入校园的那一刻实现自动网络连接。

一次性设备注册过程之后，学生就可以“一劳永逸”地使用 WiFi 了。他们的设备（包括无外设设备）可以自动连接网络。没有初始网页，无需重复登录，不用记住密码。在证书到期之前，设备已经过完整的身份验证。针对定义的所有策略自动配置，IT 人员无需触摸设备。用户拥有无缝的体验，无论他们身在何处，也无论他们正在使用哪个供应商的基础设施。

迈出成功迁移的第一步

校园网是复杂的，供应商迁移更是如此。但通过清晰定义策略和目标，并有条不紊地仔细考虑网络支持的所有服务的影响，可以在不为用户和工作人员增加负担的情况下充分利用全新 WiFi 基础设施的优势。

如需申请免费试用版 Ruckus Cloudpath 或其他 Ruckus 产品，请访问：https://www.ruckuswireless.com/zh-hans/request-a-demo

如需联系专家级 Ruckus 系统工程师或申请现场调查，请发送电子邮件至 info@ruckuswireless.com。

如需了解校园网供应商迁移的更多信息：请观看我们的网络研讨会。

美国优科无线 | 中国北京市朝阳区光华路 1 号 嘉里中心写字楼南楼 27 层 2718 室 | 电话：010-6539-3083
电邮：ChinaSales@ruckuswireless.com | http://cn.ruckuswireless.com