思科辅导:如何利用现有设施部署安全的无线网络思科认证
 由于业务需要，企业对移动化的要求也越来越高，同时安全风险也随之而来。虽然已经制订了解决具体安全问题的解决方案，我们还需要采取综合办法来利用企业网络中的有线网络基础设施来加强对WLAN(无线局域网，Wireless Local Area Network)，的安全保护。 企业WLAN的发展 企业WLAN已经飞速发展，再也不是过去的只需要简单便宜的接入点就能覆盖家庭或者小型办公室的无线网络。在WLAN部署的发展后面主要有两个推动力，第一个就是为增强生产效率，需要为客户或者使用笔记本的员工提供无线接入。 第二个推动力就是使用无线取代有线基础设施，并且受到先进技术(如802.1n标准等)的推动。无线速度提高到170Mbps以及建立企业范围内的无线网络的能力等优点，都让无线技术性能已经足以成为有线的更好替代品。此外，已经开发出很多有效攻击能够帮助确定最佳网络覆盖范围、避免重叠以及更好的利用扩频以减少碰撞和最大限度地提高性能。虽然，重点都是在性能，但无线真正的好处在于为生产力带来更好的移动性。 日益增长的移动化安全风险 然而，移动性也招致很多安全风险和问题。因为无线端点并非固定不变的，相比于无线网络，企业对于有线网络的安全性更加放心，因为有线网络受到企业建筑实体墙和门的保护，并且还有门禁卡和用户身份验证基础设施。由于无线网络能够轻易地被建筑外的人访问，因此无线网络更容易受到盗窃、攻击和各种匿名攻击形式。 当然也已经开发了很多技

术来试图解决这些问题，包括从WEP转移到LEAP、WPA、802.1x，以及在客户端和接入基础设施嵌入IPSec VPN等各种措施。所有这些方法都有一定的限制。 客户访问也是企业WLAN的一大问题，因为可能造成严重的后果。如果客户使用企业的无线网络接入并进行非法操作，提供网络接口的企业就必须承担一定的法律责任。如果无线网络被攻破，或者重要数据库被攻击，给企业带来的负面影响将更加严重。这些结果可能包括罚款、诉讼和名誉损失等。 IT部门需要清楚地知道是企业员工笔记本还是客户笔记本在访问无线网络，当笔记本通过无线网络访问企业网络时必须进行严格的加密。IT部门还应该使用现有的基础设施(如Active Directory)对员工进行身份验证，并希望客户也能进行同样的验证。 目前解决方案的局限性 现在有很多企业级WLAN解决方案已经可以解决上述问题，但是很多解决方案价格昂贵并且功能也不是很完善，与常用的有线基础设施的加密验证功能还是差很多。 在无线世界里，不能解决WLAN安全的所有问题，问题都需要单独解决。不足为怪的是，很多解决方案都是很独立的，只有从同个供应商获取整体解决方案才能获得最好效果。不断变化的市场也让这些移动产品需要对基础设施不断的更新和升级，以充分利用必要的改进的技术。 利用现有的有线基础设施 鉴于这种情况，是应该问问是否有不同的方法。在有线世界里，Layer 2交换机以神奇的速度进行着大量交换数据包的工作，Layer3交换器和路由器则进行连接网络的工作，还有验证基础设施(如Active Directory、LDAP和 RADIUS)进行直接验证。此外，验证基础设施(如防火墙和访问控制列表)也能加强保护，接入技术(如IPSec和SSL VPN)能够提供外

部网络到内部网络的连接，当然也有NAC基础设施、端点安全、IDS/IPS等，这些有线设施不胜枚举。 鉴于对所有这些基础设施技术的现有投资，以及这些现有基础设施后面的各种有线和远程用户的部署，如果将WLAN基础设施放在Layer 2并让现有技术提供其他功能，不就能节省很多开支吗?如果我们这样做，就可以拥有便宜的接入点，而控制器也不需要比Layer2/3交换器更好，这将很大程度降低企业无线部署的成本，并能让企业混合搭配使用不同供应商的何时技术，而避免大规模锁定升级。 还有比较便宜的替代方法可以帮助企业实现这一点。NAC技术已经成熟到它可以自动接入端点并分辨企业接入还是客户接入。NAC与SSL的整合确保了传输路径在所有时候都能进行加密，与验证基础设施(如IPSec和SSL VPN)的整合又能提供对员工的验证。内置的虚拟化技术和客户自动重新定向至不同的虚拟端口，能够消除为客户和员工使用单独SSID或者单独客户接入设备的需要。某些SSL VPN上的默认路由和VLAN技术能够确保客户端流量完全区分与企业流量，并能确保只有通过这个框架才能接入其他位置。身份验证问题 广泛的身份验证框架允许客户登记接入，并拥有作为用户真实身份的永久令牌，这能够通过客户登记程序(如接待处的功能一样)来实现。甚至可以区分不同类型的客人，为其登录不同的网络。 部署身份验证应该是自动化的，日志和问责制能够提供通过接入媒介的用户极其行为相关联的线索，当法律规定或者上级主管有要求时，就能提供这种线索。 