XXX(深圳)有限公司

无线局域网解决方案

2008 年 12 月

目　　录

一、 深圳 XXX 工厂无线局域网系统建设需求

1．项目背景

XXX（深圳）有限公司母厂于 1973 年在台湾省创立，1991 年在深圳某镇设立主要生产基地，1997 年 XXX 品牌正式在中国市场推广。XXX 公司投资总额 4750 万美元，厂房建筑面积 12.5 万平方米，员工 6000 余人，30 条成品生产线，年产量高达 1500 万台，是世界最大的家用电风扇生产厂家之一，凭着高度一体化的生产综合实力，XXX 已成为一家自制率高达 95%的全球知名小家电企业，产品远销美国、日本、韩国、加拿大、德国、法国等 60 多个国家和地区，并与东芝、三洋、三星等 10 大国际著名品牌保持长久合作关系。

2001-2006 年 XXX 电风扇市场综合占有率连续六年稳居国内企业前三名。2005 年，XXX 一举成为全国家用通风电器具制造行业的领头羊，2006 年被世界品牌实验室评为全国前 500 强最具品牌价值的企业，XXX 品牌价值高达 12. 08 亿，同年产品销售总额近 14 亿元人民币。2007 年，XXX 荣获国家商务部认定的“2006 年度最具市场竞争力品牌”。

公司在信息化领域不甘后人，继续加强信息化建设，为实现移动办公的需要，现计划在全厂区范围或部分办公区域内实现无线 WiFi 覆盖，对内部员工或外来宾客提供无线接入服务。

二、 深圳 XXX 工厂无线局域网设计原则和技术需求

2．1 遵循标准

无线局域网采用的技术支持应为国际标准或业界标准，不使用某个厂商的专用技术和协议，以保证网络设备的互通性，有利于网络的投资保护。

根据深圳 XXX 工厂的需求和无线网建设与设计原则，建议采用美国 Ruckus Networks 公司的第三代无线交换局域网系统（以下简称 Ruckus 无线系统），完成无线局域网覆盖项目。

2．2 技术潮流

第一代无线局域网主要是采用胖 AP 架构，每台 AP 都是一个独立的个体，AP 与 AP 之间不会进行任何沟通，需要逐台逐台进行配置和管理，费时、费力、维护成本高，安全低，融合性差；第二代无线局域网融入了认证网关设备，仍然不能集中对 AP 进行管理和配置，只是对认证管理方面有所提高而已。现今大型无线网络要求其与传统有线网络平滑融合，要求管理性和安全性都必须有一个质的提高，而第一代和第二代无线技术必定不能满足，因此，在这样的环境下，基于无线交换机集中式管理的第三代无线架构延生了。第三代无线局域网架构采用无线交换机加瘦 AP 的结构，使得无线局域网的网络性能、网络管理和安全管理能力得以大幅提高，使建设大型无线网成为可能。但是网络的发展日新月异，随着人们对无线局域网技术要求的不断提高，以及对无线局域网认识的深入，瘦 AP 的概念已经过时。 可胖可瘦成了 AP 发展的趋势，尤其是随着 802.11n 的普及，简单的瘦 AP 给后台的无线交换机带来极大的负担。为了解决这个问题，用户付出的代价也是巨大而不划算的。第四代可胖可瘦 AP 成为无线局域网发展的必然。

2．3 安全可靠

在网络安全性方面，无线局域网系统要具有与有线局域网同样要求的安全防护措施，无线网的安全性主要从以下几个方面考虑：

（1）接入认证：具有支持多种用户认证方式；

（2）数据链路的全程加密；

（3）具有无线电波监控能力，能提供无线入侵侦测功能。

具有提供智能化的无线电波自动调控与切换能力，以确保单个 AP 接入点在发生故障时自动切换到邻近 AP，不会影响无线的接入服务；具有支持热备份的无线交换机的冗余备份机制。

2．4 可扩展可升级

通过一个集中的无线局域网网管平台实现对所有的 AP 功能的配置和管理，AP 在

提供无线接入的同时，也可进行无线入侵监控、无线电波传输分析。同时整个系统可以根据用户的需要进行规模上的扩展，扩展后所有功能和管理的模式保持不变。

2．5 易管理易维护

在网络管理方面，必须具有集中控管、智能调控、自动恢复、系统冗余等实用功能，使所建的无线网络可以适应多种环境的变化，可动态地保证良好的应用效果。同时，还应支持多 SSID，可以方便的把语音、视频以及其他类型的数据的应用进行分开管理。

2．6 技术需求

根据深圳 XXX 工厂无线局域网系统建设要求，无线局域网系统建设原则如下：

1、充分利用现有网络结构与资源，不单独组网，AP 就近接入有线网络（最近的交换机），并且不改变原有网络结构以及交换机配置。

2、采用集中控管的组网方式，集中控制管理所有的 AP。

3、AP 的供电可以不单独拉线，采用 POE 供电的方式。

4、采用先进的 WLAN 网管系统管理局域网。

5、充分考虑 WLAN 的安全性，采用先进的 WLAN 安全技术保障。

6、无线局域网系统要支持故障热备冗余能力。

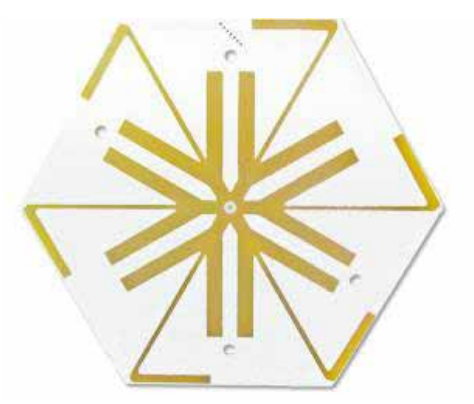
7、无线局域网系统要能方便和灵活地调整与扩充。

三、 Ruckus 无线交换局域网系统技术特点

3．1 Ruckus 先进的天线和射频控制

3．1．1 智能天线技术

智能天线技术



智能天线通过一组带有可编程电子相位关系的固定天线单元获取方向性，并可以同时获取基站和移动台之间各个链路的方向特性。智能天线的原理是将无线电的信号导向具体的方向，产生空间定向波束，使天线主波束对准用户信号到达方向 DOA(Direction of Arrinal)，旁瓣或零陷对准干扰信号到达方向，达到充分高效利用移动用户信号并删除或抑制干扰信号的目的。同时，智能天线技术利用各个移动用户间信号空间特征的差异，通过阵列天线技术在同一信道上接收和发射多个移动用户信号而不发生相互干扰，使无线电频谱的利用和信号的传输更为有效。在不增加系统复杂度的情况下，使用智能天线可满足服务质量和扩展网络容量的需要。

智能天线的发展里程

９０年代以来，阵列处理技术引入移动通信领域，很快形成了一个新的研究热点－智能天线。智能天线应用广泛，它在提高系统通信质量、缓解无线通信日益发展与频谱资源不足的矛盾、以及降低系统整体造价和改善系统管理等方面，都具有独特的优点。

最初的智能天线技术主要用于雷达、声纳、军事抗干扰通信，用来完成空间滤波和定位等。近年来，随着移动通信的发展及对移动通信电波传播、组网技术、天线理论等方面的研究逐渐深入，现代数字信号处理技术发展迅速，数字信号处理芯片处理能力不断提高，利用数字技术在基带形成天线波束成为可能，提高了天线系统的可靠性与灵活程度。智能天线技术因此用于具有复杂电波传播环境的移动通信。此外，随着移动通信用户数迅速增长和人们对通话质量和数据质量要求的不断提高，要求数据通信网在较大用户承载下仍具有较高的话音和数据质量。

技术分类

智能天线技术有两个主要分支。波束转换技术（switched beam technology）和自适应空间数字处理技术（adaptive spatial digital processing technology），或简称波束转换天线和自适应天线阵。天线以多个高增益的动态窄波束分别跟踪多个期望信号，来自窄波束以外

的信号被抑制。但智能天线的波束跟踪并不意味着一定要将高增益的窄波束指向期望用户的物理方向，事实上，在随机多径信道上，移动用户的物理方向是难以确定的，特别是在发射台至接收机的直射路径上存在阻挡物时,用户的物理方向并不一定是理想的波束方向。智能天线波束跟踪的真正含义是在最佳路径方向形成高增益窄波束并跟踪最佳路径的变化，充分利用信号的有效的发送功率以减小电磁干扰。

１．波束转换天线

波束转换天线具有有限数目的、固定的、预定义的方向图，通过阵列天线技术在同一信道中利用多个波束同时给多个用户发送不同的信号，它从几个预定义的、固定波束中选择其一，检测信号强度，当移动台越过扇区时，从一个波束切换到另一个波束。在特定的方向上提高灵敏度，从而提高通信容量和质量。

为保证波束转换天线共享同一信道的各移动用户只接收到发给自己的信号而不发生串话，要求基站天线阵产生多个波束来分别照射不同用户，特别地，在每个波束中发送的信息不同而且要互不干扰。

每个波束的方向是固定的，并且其宽度随着天线阵元数而变化。对于移动用户，基站选择不同的对应波束，使接收的信号强度最大。但用户信号未必在固定波束中心，当使用者是在波束边缘，干扰信号在波束的中央，接收效果最差。因此，与自适应天线阵比较，波束转换天线不能实现最佳的信号接收。由于扇形失真，波束转换天线增益在方位角上不均匀分布。但波束转换天线有结构简单和不需要判断用户信号方向（ ＤＯＡ） 的优势。主要用于模拟通信系统。

２．自适应天线阵

融入自适应数字处理技术的智能天线是利用数字信号处理的算法去测量不同波束的信号强度，因而能动态地改变波束使天线的传输功率集中。应用空间处理技术（spatial processing technology）可以增强信号能力，使多个用户共同使用一个信道。

自适应天线阵是一个由天线阵和实时自适应信号接收处理器所组成的一个闭环反馈控制系统，它用反馈控制方法自动调准天线阵的方向图，使它在干扰方向形成零陷，将干扰信号抵消，而且可以使有用信号得到加强，从而达到抗干扰的目的。

天线阵元配置方式包含直线的型，环型和平面的型，自适应天线是智能天线的主要的

型式 。自适应天线完成用户信号接收和发送可认为是全向天线。它采用数字信号处理技术识别用户信号的 DOA ，或者是主波束方向。根据不同空间用户信号传播方向，提供不同空间通道，有效克服对系统干扰。自适应天线主要用于数字通信系统。

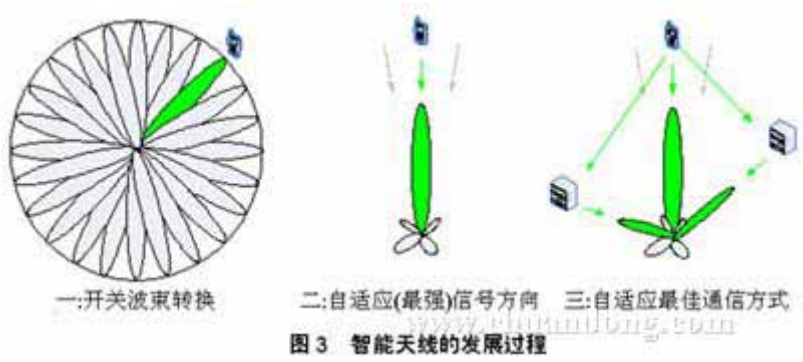
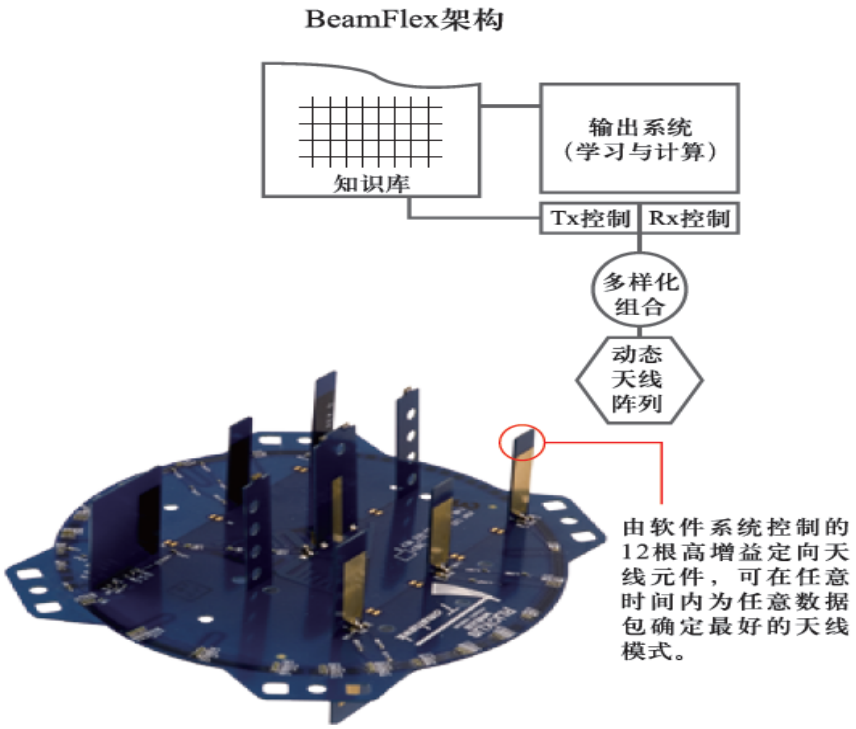


图 3 智能天线的发展过程

3．1．2 Ruckus 的智能天线系统

Ruckus BeamFlex 采用的就是自适应天线阵形式的智能天线系统。它由 12 个天线单元

组成可以形成 2^N-1 种不同的波束特征，也就是 4095 种的组合。BeamFlex 系统软件实时了解工作环境，包括射频情况，通讯设备，网络性能已经应用流，并为每一台通讯设备选择最合适的天线阵列。传输控制模块能够选择高质量的信号路径，并为接收设备选择最佳的数据传输速率。



3．1．3 绿色的的电磁环境

电磁辐射和健康

随着人们生活节奏的加快和生活质量的提高，人们正被越来越多的电子设备所笼罩。科技带给人们便捷的同时，也带来更多的伤害。电子产品产生的电磁污染问题已经成为人们关注的热点。正所谓关心则乱，关于电磁辐射的相关报道和言论很多时候让人谈虎色变。电子产品的电磁辐射真就那么可怕吗？究竟什么样的电磁辐射才构成污染？消费者又该如何正确认识电磁辐射，将电磁辐射的负面影响降低到最小？

电磁辐射是由空间共同移送的电能量和磁能量所组成，而该能量是由电荷移动所产生；举例说，正在发射讯号的射频天线所发出的移动电荷，便会产生电磁能量。电磁“频谱”包括形形色色的电磁辐射，从极低频的电磁辐射至极高频的电磁辐射。两者之间还有无线电波、微波、红外线、可见光和紫外光等。电磁频谱中射频部分的一般定义，是指频

率约由 3 千赫至 300 吉赫的辐射。 电磁辐射所衍生的能量，取决于频率的高低-频率愈高，能量愈大。频率极高的 X 光和伽玛射线可产生较大的能量，能够破坏合成人体组织的分子。事实上，X 光和伽玛射线的能量之巨，足以令原子和分子电离化，故被列为“电离”辐射。这两种射线虽具医学用途，但照射过量将会损害健康。X 光和伽玛射线所产生的电磁能量，有别于射频发射装置所产生的电磁能量。射频装置的电磁能量属于频谱中频率较低的那一端，不能破解把分子紧扣一起的化学键，故被列为“非电离”辐射。哪里会有电磁辐射？ 电磁辐射的来源有多种。人体内外均布满由天然和人造辐射源所发出的电能量和磁能量；闪电便是天然辐射源的例子之一。至于人造辐射源，则包括微波炉、收音机、电视广播发射机和卫星通讯装置等。

电磁辐射不等于电磁污染

从理论上来讲，电场和磁场的交互变化产生电磁波，电磁波向空中发射或汇汛的现象，叫电磁辐射。过量的电磁辐射造成了电磁污染。在这个电子产品充斥的时代，环境中的电磁辐射几乎无处不在，尤其是摆满各种电器设备的房间，电磁辐射源更多。

通常情况下，电磁辐射能干扰电视的收看，使图像不清或变形，并发出噪声；会干扰收音机和通信系统工作，使自动控制装置发生故障，使飞机导航仪表发生错误和偏差，影响地面站对人造卫星、宇宙飞船的控制。

专家指出，并非所有的电磁辐射都会伤害人体，电磁辐射和电磁污染其实是两个概念。电磁污染是电磁辐射超过一定强度（即安全卫生标准限值）后的结果，电磁污染会对人体产生负面效应，如头疼、失眠、记忆衰退、血压升高或下降、心脏出现界限性异常等。

据职业病研究的专业人士介绍，电磁辐射对人体危害程度则随波长而异，波长愈短对人体作用愈强，微波作用最为突出。有资料显示，处于中、短波频段电磁场（高频电磁场）的操作人员，经受一定强度与时间的暴露，将产生身体不适感，严重者引起神经衰弱，如心血管系统的植物神经失调，但这种作用是可逆的，脱离作用区，经过一定时间的恢复，症状可以消失，并不成为永久性损伤; 处于超短波与微波电磁场中的人员，其受伤害程度要比中、短波严重。尤其是微波的危害更甚。在其作用下，人体除将部分能量反射外，部分被吸收后产生热效应。这种热效应是由于人体组织的分子反复地极向和非极向的运动摩擦而产生的。热效应引起体内温度升高，如果过热会引起损伤，一般以微波辐射最为有害。这种危害主要的病理表现为：引起严重神经衰弱症状，最突出的是造成植物神经机能紊乱。

在高强度与长时间作用下，对视觉器官造成严重损伤，同时对生育机能也有显著不良影响。

电磁辐射衰减很快

电磁场在介质中传播时，其场量的振幅随距离的增加而按指数规律衰减。从能量的观点看，电磁波在介质中传播时有能量损耗。所以人工设备产生的电磁辐射值随距离的增加，而显现衰减。普通纯平电视机的磁场在屏幕前 5 厘米处可高达 5 微特斯拉，而屏前 40 厘米外就是安全范围。日常所用功效的微波炉前 5 厘米处，磁场强度达 8 微特斯拉，离微波炉开关 95 厘米才是安全范围。

以下的表格是日常家电产品电磁波强度及衰减距离，供您日常摆放参考。

	3 厘米	30 厘米	1 米
吸尘器	200－800	2－20	0.13－2
搅拌机	60－70	0.6－60	0.02－0.25
微波炉	75－200	4－8	0.25－0.6
电视机	2.5－50	0.04－2	0.1－0.15
洗衣机	0.8－50	0.15－3	0.01－0.15
电熨斗	8－30	0.12－0.3	0.01－0.025
咖啡壶	1.8－25	0.08－0.15	>0.01
电冰箱	0.5－1.7	0.01－0.25	>0.01

从上表可以看出电磁波的强度随着距离的增加，电磁波衰减的非常快。除了微波炉，其他电器距离超过 1 米以外的辐射都非常的低。

电磁辐射不是恶魔

在世界卫生组织 296 号“实况报道”中，描述了电磁辐射超敏反应的系列症状：“这些常见的症状包括皮肤症状（发红、刺痛感和烧灼感）以及神经衰弱和植物性症状（疲乏、劳累、不专心、眩晕、恶心、心悸和消化障碍）。大量症状聚集并不是任何公认综合症的一部分。”http://www.who.int/mediacentre/factsheets/fs296/zh/index.html

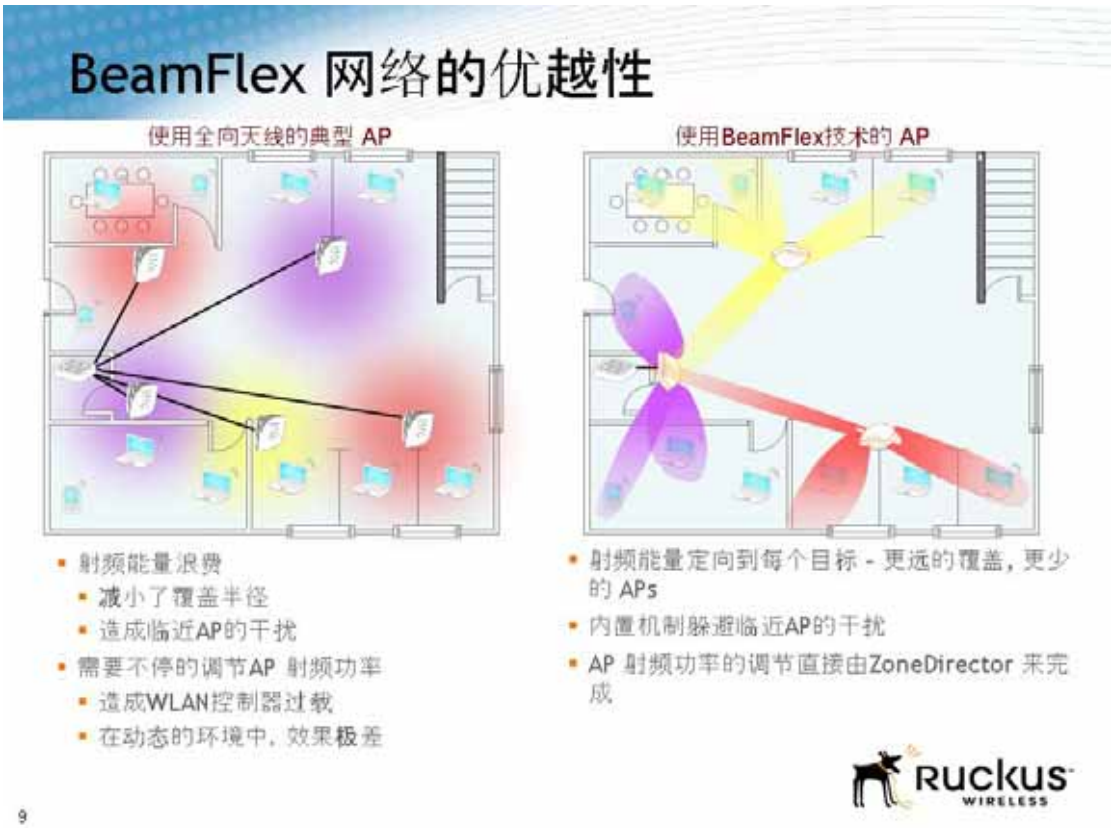
对比这些症状，人们会怀疑自己处在电磁辐射超敏反应中。不过在同一篇文献中，医学界承认电磁辐射超敏反应没有明确的诊断标准，甚至没有科学依据将电磁辐射超敏反应与电磁场暴露联系在一起。

这是世界卫生组织在 2005 年公开发布的实况报道。不过最近的医学实践似乎对电磁辐射尤其是持续的 WiFi 辐射提出了更多的怀疑和批评。

尤其是对于家庭用户而言，整天 24 小时使用 WiFi 是不可能的，甚至在某些公共场所的热点也并非时时刻刻有人使用 WiFi。就像手机一样，WiFi 完全有必要智能调节发射接受功率，在潜在的辐射危害和使用便捷中达成平衡。

平衡的选择－BeamFlex

纵然电磁辐射不能被证明对健康有伤害；电磁辐射随着距离的增加，辐射强度衰减非常明显；Wi-Fi 设备的辐射强度与手机相比较要更安全的，但是电磁辐射小一些，少一些，电磁环境就会更环保一些。



Ruckus 基于 BeamFlex 技术的智能无线网解决方案可以使得有限的无线信号能量更有目的性的指向正在通讯的客户端；而在没有无线客户端工作的区域，没有电磁辐射。与现有的无线网相比较，工作环境更绿色环保，电磁辐射的目的性更强，更有效率。最大程度的避免了电磁污染现象。

还要强调的是，人体对于电磁波有很强的衰减。如果人体处于 Ruckus 的 AP 和客户端之间时，Ruckus 的 AP 会主动选择其他信号路径，主动避免对人体的照射。（上图中指示灯的指示方向就是信号的发送方向）

3．1．4 BeamFlex 和 802.11n

802.11n 基础

802.11n 是一个美国电气电子工程师协会（IEEE）无线标准，和较老的 802.11 标准相比，在吞吐量和传输距离上有了显著的提升。802.11n 开发了很多高级技术和新技术，如空间复用、频道复合以及帧集成等，在物理层面上，其理论数据传输率最高可达 IEEE 802.11a/g 系统最大速度 54Mbps 的 11 倍。

802.11n 主要使用了七种技术来提升整体带宽与性能：

多路空间数据流： 1 路，2 路，3 路或 4 路

这让其可以在某些环境中，提升 2 到 4 倍的数据传输率。

频道带宽： 20MHz 组合成 40MHz

在某些环境下，这让其可以大体提升一倍的物理数据传输率。

时空块识别选项

未来的某些芯片组将支持此功能，某些环境下能提升可靠性。

波束形成（Beamforming）选项

未来某些芯片组会支持。

可变保护间隔

某些环境下可以提升大约 11%的吞吐量。

帧集成

更高的物理速率，可以极大的改善有效吞吐量。

块应答

更高的物理速率，可以极大的改善有效吞吐量。

在目前生产的芯片组中，这些最重要技术已经实现的有：空间复用，频道复合，帧集成，以及块应答。

期待的 802.11n 数据传输率

期望的802.11n数据传输速率

	1路空间数据流			2路空间数据流		
802.11a 802.11g Rates	11n 指标速率	频道复合（40MHz）	短守护间隔	2路空间数据流	频道复合（40MHz）	短守护间隔
6	6.5	13.5	15	13	27	30
9	13	27	30	26	54	60
12	19.5	40.5	45	39	81	90
18	26	54	60	52	108	120
24	39	81	90	78	162	180
36	52	108	120	104	216	240
48	58.5	121.5	135	117	243	270
54	65	135	150	130	270	300

虽然生产商们在不断宣传 802.11n 的理论数据传输率是 300Mbps 或者更高，但实际用户们的吞吐量却要低了不止一个数量级。这是因为当前的 802.11n 产品并未能最有效的使

用这些新技术。因为拥有对 Wi-Fi 信号构成以及信号方向的完全控制能力,Smart Wi-Fi 通过使用这些技术，无论在时间上还是距离上，都确保了更高的 TCP 吞吐量。

物理速率的提升

802.11n 标准的核心之一，是一种叫做“空间复用”的技术。空间复用是基于多个传输天线的不同编码数据信号或数据流的并发传输。这样，同一空间就被重复利用了多次，或者是被多路复用了多次。

空间复用的工作原理是将一个数据帧分割为多个数据片，然后通过多个天线的多路无线信号，并发传输这些数据片。而接受者则使用不同的天线，接受不同的信号，并执行还原过程，将其恢复为原始数据流。空间复用通过提升发射者与接受者之间并发数据流的数量，从而提升吞吐量。

空间复用实际上是利用了一个常见的无线现象，叫做“多路径”（后文会对此进行详细讨论）。 就是一个无线信号会因为反射，经由不同的路径达到最终客户端，导致客户端因此难以确定正确的信号。

而在 802.11n 里，多路径却是被希望发生的现象，这样就可以向接收端传输更多的数据。因此，确保信号会经由不同的射频路径传输，对获取更高性能而言就很重要了。

空间复用的挑战

虽然 802.11n 规范允许高达 4 路的空间数据流，但是目前绝大多数可用的芯片组和系统只能支持 2 路。或许在几年后，芯片制造商们推出新一代 802.11n 芯片组时，会改变这一点。

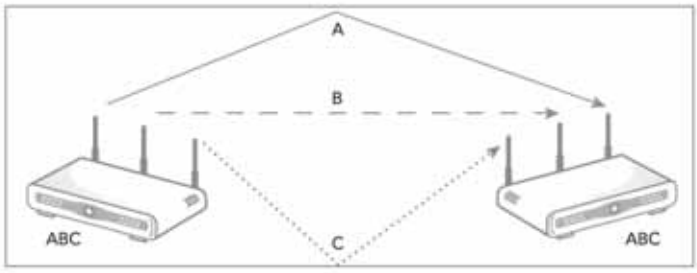
802.11n 数据流速率:

802.11n Data Rates by Stream

空间数据流数量	最大物理数据传输率
1	150 Mbps
2	300 Mbps
3	450 Mbps
4	600 Mbps

空间复用和物理数据传输率一样，对干扰和数据包丢失高度的敏感。在一个充满干扰的环境以及（或者）不佳的位置下，AP 和客户端可能会倾向于选择更少的空间数据流。这会导致物理数据传输率和实际吞吐量的急剧降低。

正如前文所提及的那样，空间复用依赖于多路径传输（无线信号通过 2 条或者多条路径到达接受者天线）和相关延迟（每个信号自发射到被接收到之间的时间间隔）。 接收端就是依据这些路径差异来重组或者重建原始数据流的。如果在发送端和接收端之间的空间穿越路径太过近似（或者“相互关联”），空间复用就会失败，发送端就必须削减空间数据流的数量，从而降低传输速率。因此，确保多路径运作对于获取 802.11n 所承诺的高性能来说，也是必不可少的



空间复用同时也提升了空间数据流出错的概率。因为此时穿越无线介质的数据更多了，所以出现数据损伤或者数据包丢失的概率也就更大了。在这种情况下，对一个 AP 或者一个客户端来说，最典型的反应就是使用较少的空间数据流，并降低数据传输率，以确保平稳运行以及最小化丢包率。

认识空间复用的潜力

智能天线技术才是最适合空间复用的。因为通过控制信号路径的方向和时间，智能天线阵列最小化了阵列之间的关联性。而正是不同的天线配置之间的非关联性，才能保证实现使用这些系统所获取的大部分统计增益。

通过独立掌控或者路由每一个空间数据流通过最适宜的射频路径，智能天线提升了空间复用通讯可用的时间百分比，拓展了空间复用的实用性。

如今，几乎所有的 802.11n AP 都使用了多根全方位天线，以发射不同的数据流。这些全方位天线几乎是同等极化的，因此导致了多路径的可能性被降到最低，特别是在很短的距离上。

相反，智能天线阵列允许使用水平或者垂直极化的天线部件，以用于不同的空间数据流。这增加了（几乎是确保了）正确多路径传输的可能性。

除了最大化路径的非相关性之外，智能天线阵列技术还可以排除干扰。这点对于 2.4GHz 的频谱来说特别重要，因为它只有 3 个非重复的频道，要不是那些全方位天线的 Wi-Fi 系统几乎不可能做到这一点，频道复合也不会变得如此困难。

要减轻外来干扰，并防止空间数据流间彼此相互干扰，使用自适应智能天线是最适合的，因为每一个 Wi-Fi 传输都可以被相应的特定天线独立控制，包括对方向的控制，以及对每个数据包穿越射频介质的路径控制。

此外，在 5GHz 的无线频谱中（和 2.4Ghz 频谱一样），智能天线阵列为 802.11n 提供了相当高的信号增益（在许多个案中高达 9dBi）。其结果就是可以在更大的覆盖范围内使用更多的空间数据流。

40MHz 频道（频道复合）

802.11n 另一个重要的技术就是 40MHz 频道（也就是常说的“频道复合”）。频道复合通过将两个临近的 20MHz 频道复合成一个单独的 40MHz 频道，来提升带宽。就吞吐量的提高来说，实际上比两倍还略高一点点，因为两个整合频道之间的保护带也能被去掉。

2.4GHz 对 5GHz 以及频道复合

没有频道复合的话，802.11n 将是残缺不全的。限制客户端仅能使用 20MHz 是一种实质上的误导，并且会从整体上损害 802.11n。由于绝大多数 Wi-Fi 系统中对于射频传输控制的缺乏，传统经验告诉我们，40MHz 频道仅在 5GHz 波段有效，因为在那个频谱中，有大量的非重复频道可用。而在 2.4GHz 波段，仅仅只有 3 个非重复的 20MHz 频道（频道 1，6 和 11）。将 3 个非重复频道中的 2 个组合成一个更宽的 40MHz 频道，将限制你只能使用一个单独的非重复 40MHz 频道。

在 5GHz 波段，有 23 个非重复的 20MHz 频道（实际数目视不同的国家规定而不同），因此使用 40MHz 频道没有任何的风险。

另一个常见的误解是认为使用 40MHz 频道的话，将造成更多的干扰。虽然 40MHz 的运作会消耗 2 倍的带宽，但是数据包却只有一半（相对于时间），所以在干扰方面其实并无实际增加。

要最大化 802.11n 的运作，AP 和客户端方面是否都有足够的智能以确认运作的正确模式，就显得非常重要了。Smart Wi-Fi 通过其独有的方式解决了干扰问题，因而在 2.4GHz 频谱内解决了频道复合的问题。

Smart Wi-Fi 提升了频道复合的几率

无论是使用 2.4GHz 还是 5GHz 的波段，40MHz 的频道都对干扰和数据包丢失极其敏感。对指定客户端而言，绝大多数的 AP 都会在发现出现干扰或者数据包丢失时作出反应，降回 20MHz 频道。这会导致潜在吞吐量损失一半以上。

Smart Wi-Fi 提供了更大程度上的更多自由，允许 AP 在数千种可能天线模式以及路径之间进行选择。在绝大多数情况下，它都可以找到一种特定的天线组合，可以保证在干扰依旧的情况下，继续使用 40MHz 频道。

虽然实际操作还要依赖于具体的不同环境，但实际情况就是，使用了 Smart Wi-Fi 的频道复合，即使在 2.4GHz 的波段里也是非常有效的。

有效吞吐量的提高

除了物理速率提升，802.11n 还增加了 MAC-层技术，来提升有效吞吐量。

802.11n 帧集成

帧集成

帧集成将多个小数据包组合成一个大帧——系统开销（Overhead）更少，有效地提高数据包效率。

块应答

块应答让接受者可以对一组帧进行应答，而不是以前那样对单个帧进行应答。因为延迟的响应时间，应答降低了发射时间的效率。而通过一次应答多个帧，802.11n 现在可以更加有效的使用无线介质。

802.11n 块应答

802.11n 块应答

物理数据传输率	1	2	4	8	16	32
30 Mbps	21.72	24.72	26.55	27.57	28.11	28.39
60 Mbps	34.96	43.44	49.44	53.10	55.14	56.23
120 Mbps	50.29	69.92	86.88	98.87	106.20	110.29
180 Mbps	58.90	87.75	116.23	138.73	153.61	162.31
240 Mbps	64.41	100.58	139.84	173.76	197.74	212.40
300 Mbps	68.24	110.24	159.26	204.79	238.93	260.67

帧集成及块应答的潜在益处和挑战

这两个技术在约定的物理数据传输率上，一起引人注目的提升了实际吞吐量。这种在时间和距离上的实际吞吐量才对绝大多数用户有意义，因为环境的改变并不总能被事先考虑到。

802.11g 的最大物理传输速率是 54Mbps，但是实际的 UDP 性能不超过大约 35Mbps，而最大的 TCP 吞吐量则要更低得多。而使用 802.11n，在物理数据传输率方面的问题就更加戏剧化了。

在一个没有块应答的 300Mbps 物理传输速率上，有效的最大 UDP 吞吐量不超过

68Mbps。 一次应答 2 帧可以将潜在吞吐量提升到 110Mbps；一次应答 4 帧可以将吞吐量提升到 200Mbps，以此类推。很显然，帧集成和块应答技术，对于 802.11n 所承诺的性能而言，有多么的关键。

毋庸置疑，帧集成和块应答同样也对数据包丢失和干扰极其的敏感。在一个嘈杂的环境里，绝大多数 AP 和客户端都会回归到一个侵略性较少的集成上，其结果就是较低的吞吐量。

通过优化到达每个客户端的路径，减轻干扰，提升距离，以及提供优异的接受灵敏度，Smart Wi-Fi 技术可以通过提升 AP 和客户端之间协商达成更具侵略性的帧集成以及块应答方案的可能性，从而帮助实现并最大化 MAC 层增强技术的潜力。其结果就是，在距离方面获得可靠的性能提升。

向下兼容性——802.11a/b/g 客户端

802.11n 向下兼容于 802.11a，802.11b，以及 802.11g，所以老客户们也可以使用 802.11n 的 AP。许多人担心，面对这些老客户端，802.11n 将失效。这种想法是错误的。

一些专家推荐对新式 802.11n 客户端使用 5GHz 波段（假定很少会有拖慢网络的 802.11a 客户端），而对老客户（802.11b/g）则使用 2.4GHz 波段。嗯，很合理，但这远不是最理想的。

使用双波段 AP 或者覆盖式 802.11n 网络将更加的昂贵，而 5GHz 波段的空气传播性更低，传输距离也更短。这会导致需要更多的 AP，整体方案的成本也会更贵。

相对于可供选择的更多可用频道，802.11n 的 5GHz 波段提供了更多的弹性，但在使用此频谱解决和低物理速率 802.11a/802.11n 客户端相关的问题方面，并没有任何与生俱来的优势。

这一点，和 802.11b 在一个 802.11g 网络中如何运作很相似。Smart Wi-Fi 引入了相关技术，以解决这些潜在的问题。

某些情况下，最佳方案是给予每一个客户端（无论其属于何种类型）同等的介质访问份额。 比方说，10 个同时进行的客户端，每一个都消耗十分之一的传输时间。对于有 300Mbps 物理速率的一个客户端来说，这意味着最高 30Mbps 的吞吐量（忽略系统开销）。而对于只有 1Mbps 物理速率的客户端而言（可能是一个老客户端，或者是一个远程 802.11n 客户端），则意味着不超过 100kbps。

在其他情况下，一个最佳方案可能是惩罚慢速客户端，而给予更快的客户端以更多的无线网络访问权。其结果就是更高的整体性能和整体应用水平。问题是，绝大多数 Wi-Fi AP 都使用集成在无线芯片组中的非弹性硬件队列，只能提供 4 路标准队列，分别是语音，视频，数据，以及其他应用。其结果就是，一个慢速的语音客户端将消极影响网络中的所有其他客户端。

Smart Wi-Fi 结合了智能天线阵列以及 QoS（服务质量控制）技术来解决这个问题。智能天线阵列允许对每一个数据包及每一个客户端使用不同的天线阵列。与此同时，一个复杂的服务质量控制引擎为每一个客户端都保持 4 条软件队列。不同的客户端之间应用一个加权的循环法则。这些技术结合在一起，可以形成不同的特定策略，保证对不同客户端之间的传输时间分配可以达到最优化效果。

BeamFlex 和 802.11n

802.11 允诺会重新定义无线网络，最终让企业无线化触手可及。但是伴随 802.11n 而来的，却是复杂性、成本的增加以及混乱性。

在生产商宣扬高达 300Mbps 的数据传输率时，用户的体验却完全不同。获取 802.11n 系统所承诺高性能的关键，在于利用全新的 802.11n 基本技术，例如空间复用、频道复合、帧集成以及块应答。要做到这一点，在射频领域方面拥有可见性以及控制力就势在必行，与此同时，还需要对那些能对性能造成负面影响的实时环境变化拥有自适应能力。

当今的 802.11n 系统，绝大多数都未提供能满足需求的射频区域控制——其结果就是不合理的系统性能。这些系统必须不断进行一次又一次的人工调整——需要你熟知信号传播特征以及环境条件方面的相关知识。

而智能天线技术的进步，却的的确确解决了环绕在 802.11n 周围的难题，比如复杂性、可靠性，以及性能方面的问题。通过自动控制 Wi-Fi 信号的路径选择，Smart Wi-Fi 系统能够确保进行空间复用，频道复合，帧集成以及块应答的最大可能性。

此外，通过任何时候都对 Wi-Fi 信号进行最佳路径的路由，这些 Smart Wi-Fi 系统能够避免和减轻所受到的干扰。其结果就是，在任何指定范围内，都能为用户提供性能更好，更加可靠的无线连接。

3．2 Ruckus 无线局域网的管理

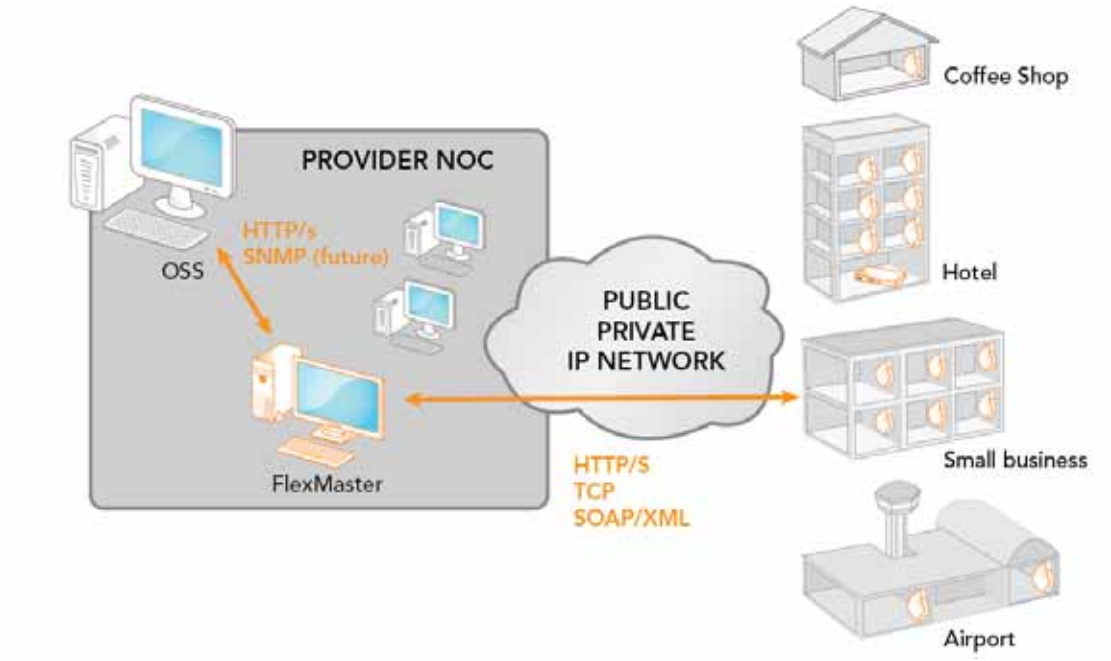
XXX 的无线局域网是一个数量较多的无线网络，包括数以十计的无线 AP，如何管理这些数量庞大的无线 AP 和复杂的无线应用业务，是 XXXIT 管理者面临的一大难题。

传统无线局域网的所有网络配置都必须在 AP 上设定。采用无线交换机管理控制的 AP 解决了上述问题，但由于所有 AP 的业务流量都要汇聚到无线控制器，使得无线交换机成为单点故障和性能瓶颈，而且随着最新的 802.11n 技术的逐步采用，每个 AP 无线传输速率高达 300Mbps，如果遍布在各处的 802.11n AP 的数据都汇聚到中心的无线交换机进行处理，那么集中式无线交换机的单点故障和瓶颈效应彰显的尤为明显，而且将遍布各处的无线用户的数据都汇聚到中心的无线交换机进行处理，无论是用户的使用性能还是可扩展性都是需要慎重考虑的。

对 XXX 来讲，兼容现有的网络和运营模式是建设任何网络的优先考虑。所以集中管理就是一个必须要支持的功能，比如部署在用户场所的 AP 要求获取当地的 IP，而部署在管理中心机房的集中网管系统可以跨网段对部署在各用户场所的 AP 进行远程管理。

新一代的无线网络管理方案既要能够满足当前 XXX 业务的集中管理需求，又能够满足 XXX 网络规模和新业务不断发展的需要。

Ruckus 无线公司基于 TR-069 标准的网管系统 FlexMaster 是目前最适合的网管系统，它使得人们能够方便的管理分布于不同区域、数量庞大的 AP，可以在很大程度上减少的配置/管理工作，提高设备的易用性和可管理性，便于设备的快速部署和业务的迅速开展。



3．2．1 集中管理 – FlexMaster 和 ZD1000/3000

FlexMaster 集中网管服务器安装在网管中心，直接管理分布在各处的 2942 AP 和无线控制器 ZoneDirector 1000/3000。有些地方如运营商管理的连锁咖啡厅、连锁零售商店、无线热点等，由于这些场所一般安装的 2942 AP 数目比较少，建议这些地点安装的 2942 AP 直接归 FlexMaster 集中网管系统管理，供电可采用 220 伏 AC/DC 转换器直接供电，也可以通过支持 802.3af 标准的 PoE 以太网交换机对其供电。

对于连锁酒店、学区、中大型企业以及无线管理业务，由于这些客户一般拥有多个场所，每个场所需要部署几十个到成百上千个 AP 不等，建议在这些场所的设备间部署 Ruckus 无线公司的无线控制器 ZoneDirector 1000/3000，统一管理部署在本场所的 2942 AP，分布在各个场所的无线控制器 ZoneDirector 1000/3000 由部署在网管中心的 FlexMaster 集中管理。这样每个场所可以通过部署在本地的 ZoneDirector 1000/3000 进行一些本地化的配置，如只服务于该场所的特定的 SSID，ZoneDirector 1000/3000 可以对部署在本场所的 AP 做灵活的射频管理，如无线信道的选择，发射功率的调整、负载均衡等，也有利于 VoWLAN 等语音业务的无缝漫游。

FlexMaster 集中网管系统提供以下基本功能：

(1) AP“零”配置、即插即用

在任何地点的 AP 加电后，能够自动找到 FlexMaster 网管服务器，主动请求管理，从 FlexMaster 网管服务器下载配置，自动进行初始化配置。AP 只需要配置 IP 地址和指定 FlexMaster 网管服务器的 IP/URL 地址，其它的配置都由 AP 自动完成。基本做到 AP 设备的“零”配置或即插即用。AP 也可以通过 DHCP 服务器或 DNS 服务器自动获得 FlexMaster 网管服务器的 IP/URL 地址。

（2）集中配置管理

配置管理由 FlexMaster 网管服务器控制发起，通过在 FlexMaster 网管服务器上按组或设备类型设置配置模板。批量对指定设备和指定设备组配置更新，也可以对单台设备进行个性化配置和管理。

（3）软件升级管理

AP 可以主动请求版本更新，也可由以 FlexMaster 网管服务器强制进行版本的升级。无论是哪种方式，版本的决策都由 FlexMaster 网管服务器来控制。FlexMaster 网管服务器可以定制升级任务，为了不影响用户的正常上网，FlexMaster 网管服务器一般可以指定软件升级或配置更新安排在凌晨用户比较少的时间段进行。

（4）性能监控和系统日志文件

FlexMaster 网管服务器可以实时查询设备状态，显示设备信息，包括：型号, 设备名称, MAC 地址, 序列号，Firmware 版本, 上次通信事件，组名称等。AP 可主动发送事件报告实现设备的实时告警，设备告警、事件、设备日志能够通过 Email 发送到指定管理员帐号。FlexMaster 网管服务器能够查看设备 log 信息和存储 log 文件。

（5）基于加密通道的远程管理

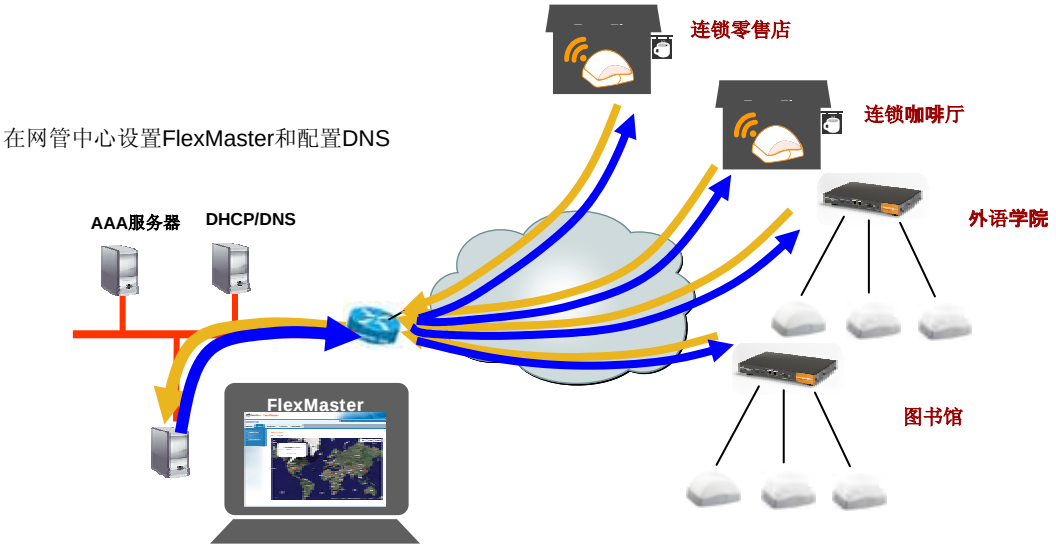
采用加密通道对 AP 进行远程管理，管理更安全。采用基于 TCP 的网管，管理更可靠（SNMP 是基于 UDP 的网管）。

（6）提供审计 log

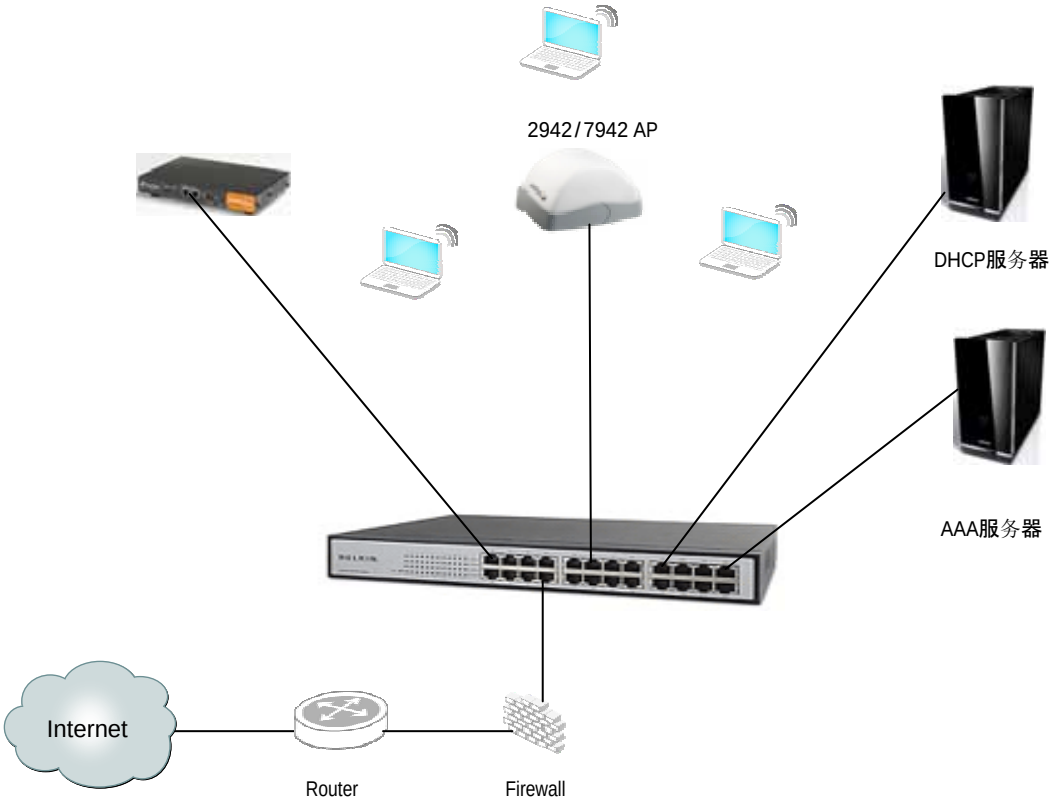
保存管理员操作日志，内容包括时间、审计类型、重要程度、用户帐号和日志具体信息。可以 Email 审计日志到指定管理员账号。

（7）实时监视无线 RF 环境

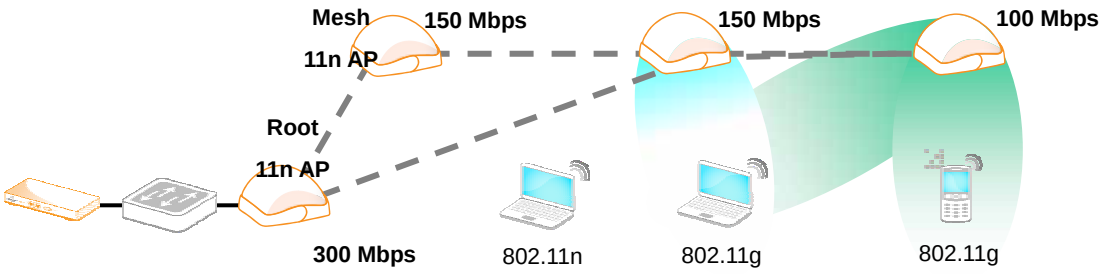
提供无线信号的热敏图，能够实时看到无线频谱分布、无线信号强度。



当某个区域 AP 相对集中，如酒店、学校的图使馆、教学楼等，可以在这些大楼的设备管理间部署 Ruckus 无线公司的无线控制器 ZoneDirector 1000/3000，统一管理部署在本楼内的 2942 室内型 11g AP。这样无论 2942 AP 安装本楼的在什么地方，都集中到安装在本楼设备管理间的无线控制器 ZoneDirector 1000/3000 进行管理。ZoneDirector 1000/3000 可以对部署在本楼内的 AP 做灵活的射频管理，如无线信道的选择，发射功率的调整、负载均衡等，也有利于 VoWLAN 等语音业务的无缝漫游。ZoneDirector 1000/3000 则可以由部署在网管中心的 FlexMaster 网管系统集中远程管理。

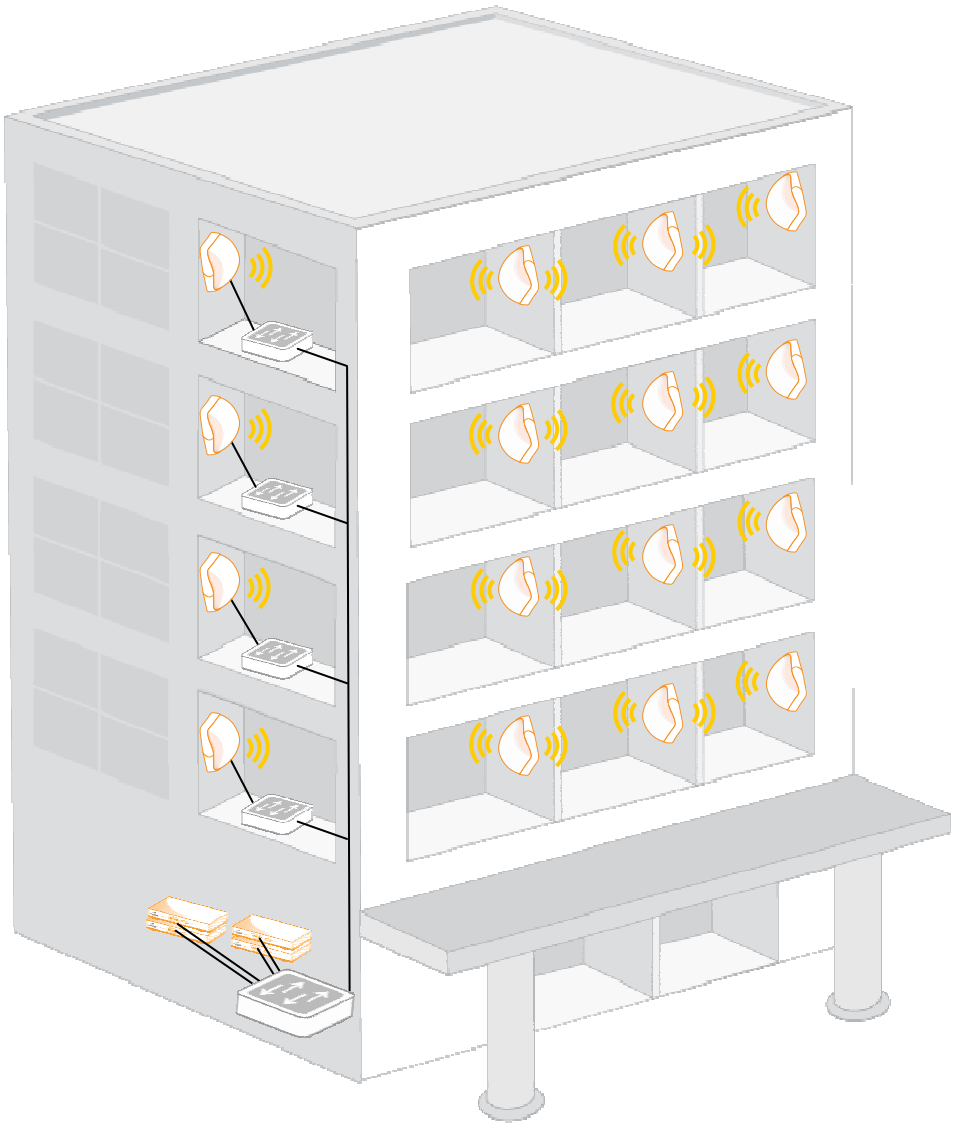


部署在大楼内的 2942 AP，通过以太网线连接到楼层以太网交换机或通过大楼的综合布线系统直接连接到大楼设备管理间的以太网交换机。如果楼层有些地方难以实施综合布线，则可以考虑采用 Ruckus 无线公司的智能 MESH 技术，2942 AP 只需部署到所需的位置，通过 220V AC/DC 电源适配器对其进行供电，2942 AP 会自动发现周围邻居，并自动发现一条最佳的路径连接到有线网。

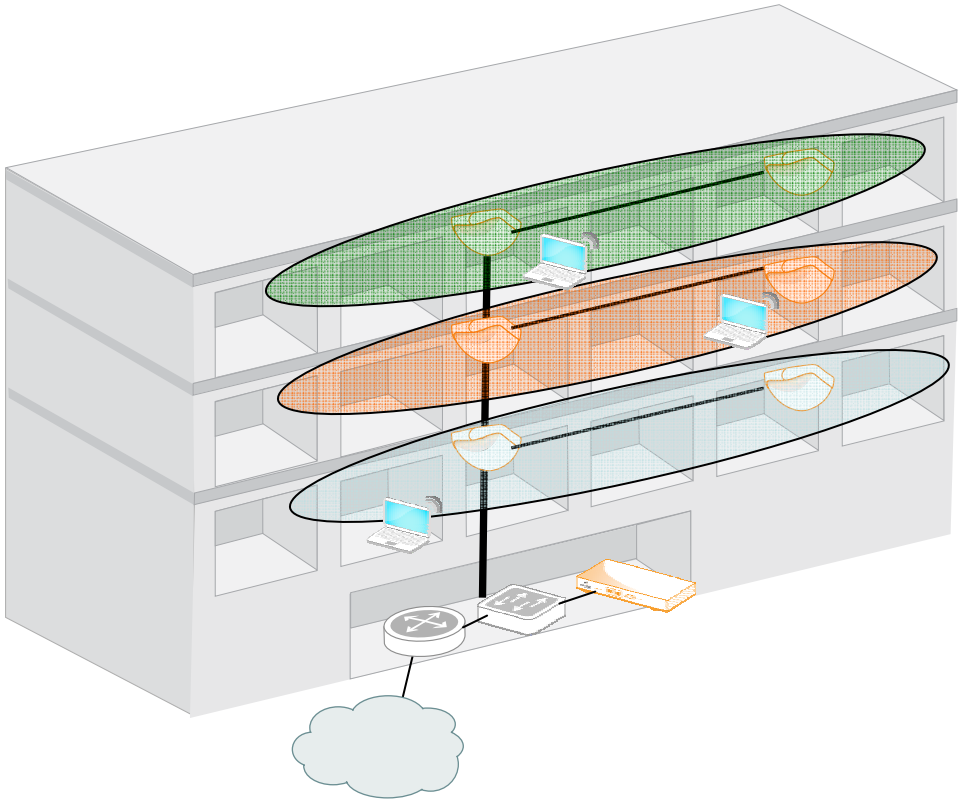


如果采用 Ruckus 无线公司智能 MESH 技术，则可以大大降低施工的难度，降低工程成本，加快工程建设进度。这项技术对于已装修的大楼或临时增加无线覆盖的应用场景尤为重要。由于无线 MESH 网经过多跳后，性能会下降。如采用 Ruckus 无线公司 2942 11g AP，经过

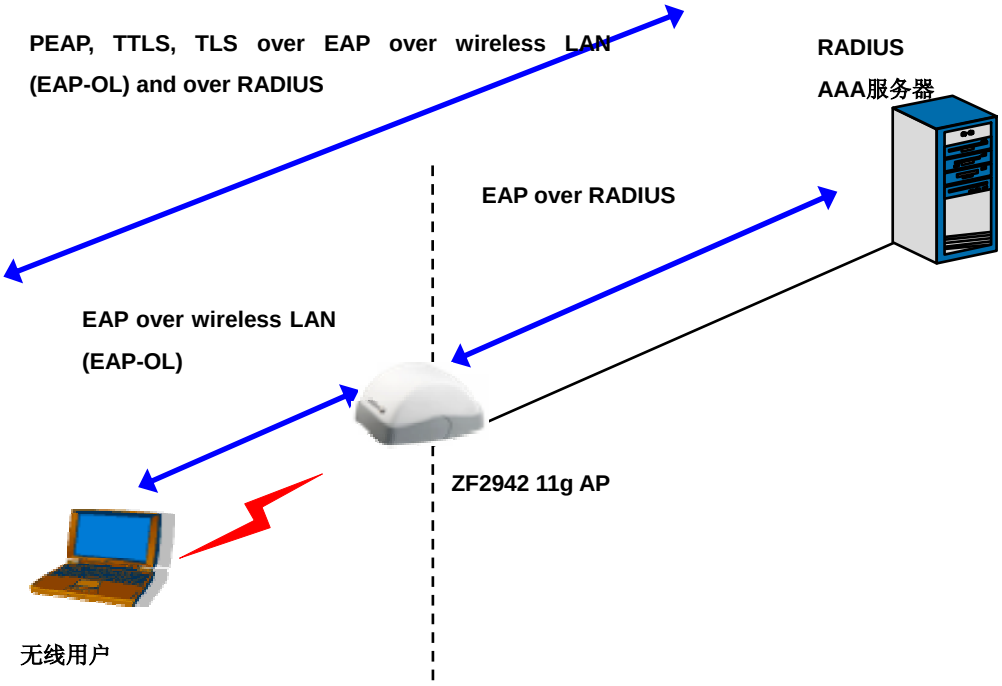
3 跳 MESH 连接后，带宽约为 7Mbps。如果用户应用需要很大的带宽，则建议采用 Ruckus 无线公司最新的 7942 11n AP，如上图所示，经过 3 跳 MESH 连接后，带宽仍高达 100Mbps。



2942 AP 如果和 ZoneDirector 1000/3000 处于同一个二层子网内，那么 AP 通过二层子网内广播自动发现 ZoneDirector 1000/3000，进行软件和配置的更新和管理。2942 AP 如果和 ZoneDirector 1000/3000 处于不同二层网络内，那么 AP 可通过 DHCP 服务器的选项 Option 43 或手动设置 ZoneDirector 1000/3000 的 IP 地址来发现 ZoneDirector 1000/3000，进行软件和配置的更新和管理。



ZoneDirector 1000/3000 安装在 XX 大楼的管理设备间，一台 ZoneDirector 1000/3000 最多可以管理 50/250 个部署大楼内的 AP。2942 11g AP 的配置管理、日志管理、RF 管理、Rouge AP 检测和故障诊断管理均由 ZoneDirector 1000/3000 负责。



用户的认证和计费可以通过 ZoneDirector 1000/3000 与大楼现有的 AAA 认证计费服务器联系完成。ZoneDirector 1000/3000 负责将用户的用户名和密码认证信息以及计费信息传送到大楼现有的 AAA 认证计费服务器。

实现的功能如下：

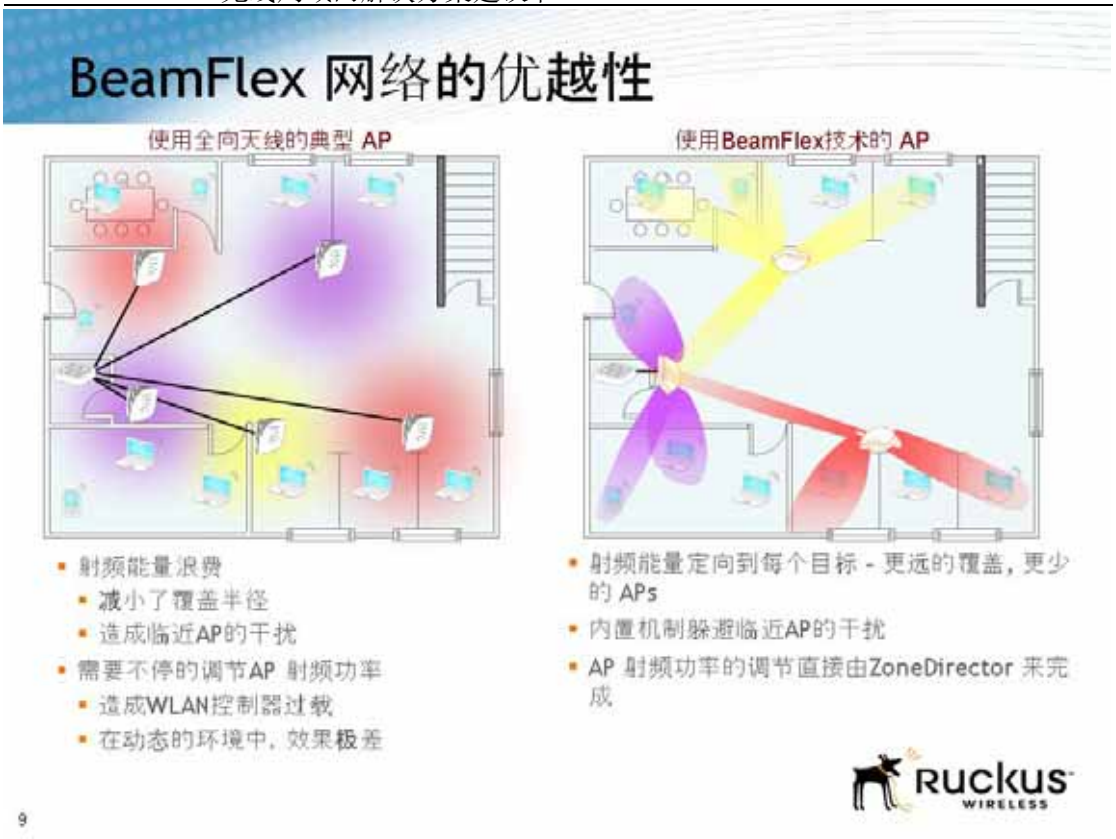
1. 与现有网络结构兼容，无需对现有网络进行任何调整和改变。
2. 集中管理和计费。
3. 支持 8 个 SSID，支持 PoE。
4. 认证加密机制是基于每个 SSID 来设定，针对不同的目标用户可以采用不同的认证加密机制，例如对于访客可以采用 Web portal 认证方式，而且可以设定访客限制，一旦认证成功，访客一般只能接入访问互联网。
5. 和大楼现有的 AAA 认证计费服务器相配合，支持基于 802.1x 的 EAP-PEAP、EAP-TTLS 等无线用户认证加密机制，合法用户必须输入正确的用户名和密码，通过 AAA 系统认证后，才能接入访问互联网。
6. 用户数据库可以采用 ZoneDirector 1000/3000 内置的用户数据库，也可以采用外置的 RADIUS 服务器或 ActiveDirectory 服务器。
7. 支持合法用户在在大楼内无线网覆盖范围内的漫游识别，认证和计费。
8. 支持无线用户在大楼内不同 2942 AP 间的无缝切换而不中断用户数据连接。具有

提供智能化的无线电波自动调控与切换能力，以确保单个 AP 接入点在发生故障时无线用户自动切换到邻近 AP，不会影响到用户的无线接入服务。

9. 支持无线用户的二层隔离，保证用户数据的安全。
10. 支持数据在无线信道上传输的 VPN 机制，以实现某些特殊的用户数据集中管理；
11. 支持无线电波监控能力，能自动调整信道和发射功率，以减少干扰。
12. 支持多业务区分，可以根据用户分类与分布情况，设置多 SSID 技术来实现多业务区分。
13. 支持基于每个 SSID 的用户上行、下行数据输率限制，防止使用 PtP 下载应用的用户大量占用宝贵的网络带宽。
14. 支持防 DoS 恶意攻击，一旦 ZoneDirector 1000/3000 检测到某台机器连续多次认证失败，ZoneDirector 1000/3000 可以根据预先的设定，一段时间内拒绝该机器发出的所有无线数据，缺省时间一般为 30 秒钟。
15. 无线用户数据流量缺省不经过 ZoneDirector 1000/3000 进行交换，没有瓶颈，性能好，扩展灵活。如果有些应用确实需要汇聚到 ZoneDirector 1000/3000 进行处理，则可以通过建立 VPN 隧道的方式来实现。
16. 支持零配置安装，全自动配置更新、软件升级。
17. 除了支持硬件 QoS 队列以外，还支持分别针对每个无线用户的软件 QoS 队列，以确保对时延和抖动敏感的应用如语音、视频等的良好支持。
18. 支持智能 WiFi MESH 功能，有些难以布线的地方或临时需要部署 AP 的地方，则可以采用无线 MESH 的方法，通过其它有以太网连接的 2942 AP 接入到大楼的有线以太网内。

3．2．2 RF 的智能管控

Ruckus 基于 BeamFlex 技术的智能无线网解决方案可以使得有限的无线信号能量更有目的性的指向正在通讯的客户端；而在没有无线客户端工作的区域，没有电磁辐射。与现有的无线网相比较，工作环境更绿色环保，电磁辐射的目的性更强，更有效率。最大程度的避免了电磁污染现象。

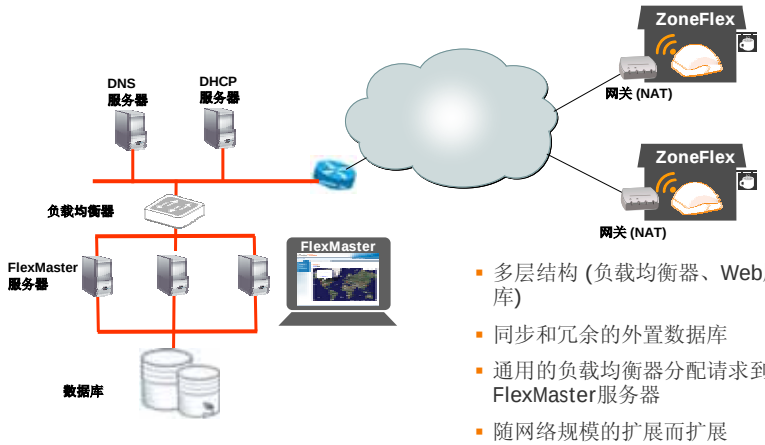


Ruckus 无线控制器 ZoneDirector 1000/3000 自动设定 AP 的工作信道，当检测到 AP 工作信道有射频干扰时，ZoneDirector 1000/3000 会自动调整 AP 的工作信道来避免干扰。当 AP 的部署密度很高，一旦 AP 内置的 BeamFlex 技术无法有效避免邻近 AP 的相互干扰，ZoneDirector 1000/3000 会自动调整 AP 的发射功率来有效避免相互之间的射频干扰。由于 Ruckus 无线公司的 2942 AP 采用专利的 BeamFlex 智能天线技术，AP 只往有无线用户的方向定向发送无线信号，而不象其它厂商的 AP 采用 360 度全向发送无线信号，因此大大减少了邻近 AP 之间的相互干扰，ZoneDirector 1000/3000 无需像其它厂商的无线交换机频繁地调整 AP 的发射功率，这一点在动态环境下尤为重要。

3．2．3 系统的冗余备份

当无线网络规模越来越大，作为集中网管系统 FlexMaster 就需要系统冗余备份。最简单、最初步的系统冗余备份是增加冗余的外置数据库和 FlexMaster 服务器，增加一个负载均衡器来平衡每个 FlexMaster 服务器的负载，所有的 FlexMaster 服务器共用一个虚拟的 IP 地址。

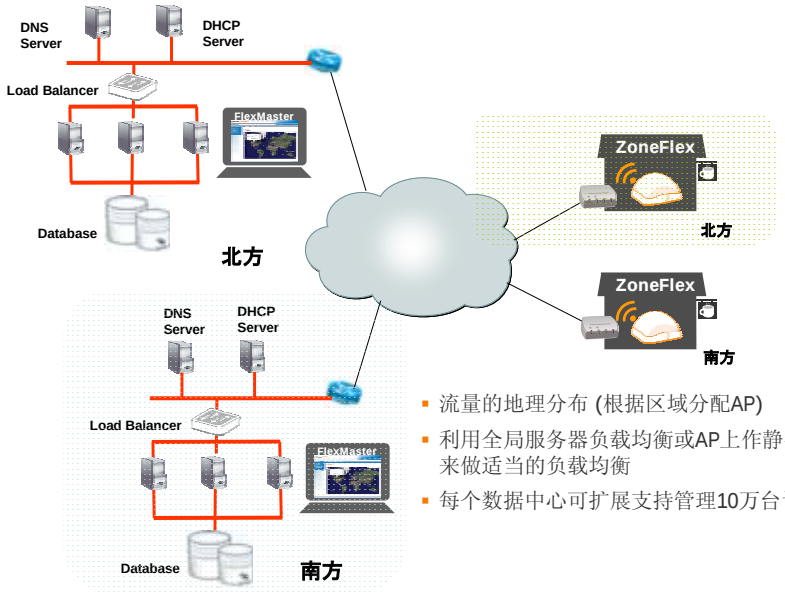
冗余数据库多个服务器



- 多层结构 (负载均衡器、Web服务器、数据库)
- 同步和冗余的外置数据库
- 通用的负载均衡器分配请求到负载最轻的FlexMaster服务器
- 随网络规模的扩展而扩展
- 一个数据中心可扩展支持管理10万台设备

进一步的网络扩展和系统冗余备份则是分布式数据中心冗余，分别部署 FlexMaster 集中网管系统在地理冗余的不同数据中心，北部地区的 AP 则配置网管 URL 到部署在北部数据中心 FlexMaster 的 URL，同样南部地区的 AP 则配置网管 URL 到部署在南部数据中心 FlexMaster 的 URL，利用 AP 上配置不同 FlexMaster 服务器 URL 来做适当的负载均衡。

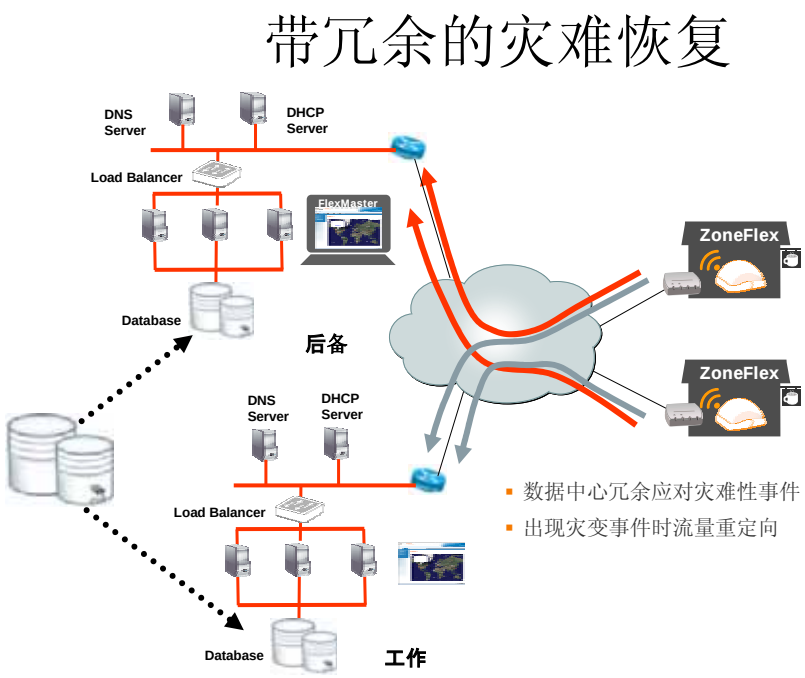
分布式数据中心冗余



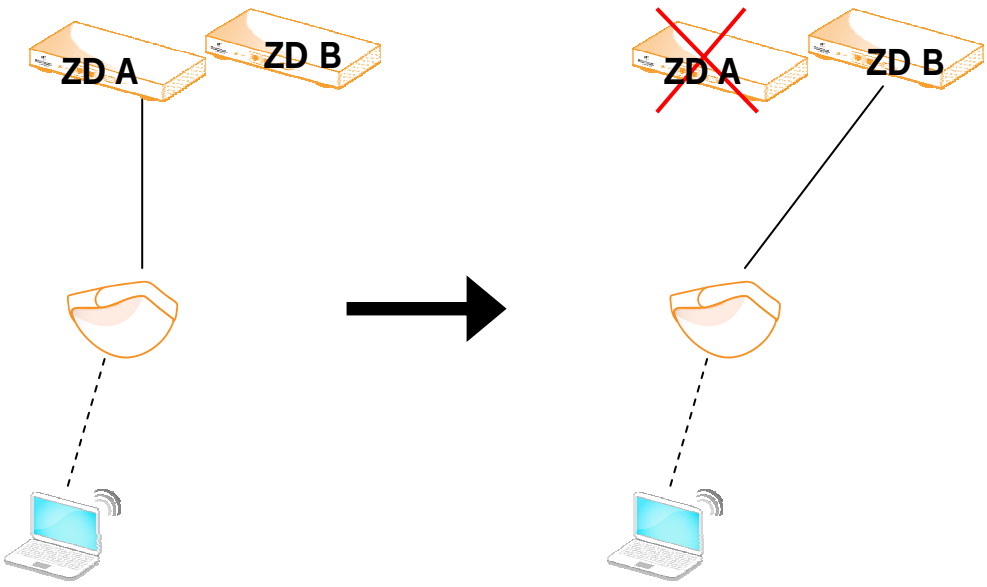
- 流量的地理分布 (根据区域分配AP)
- 利用全局服务器负载均衡或AP上作静态配置来做适当的负载均衡
- 每个数据中心可扩展支持管理10万台设备

最高级别的系统冗余则是带冗余的灾难恢复，多个地理冗余的数据中心共享同步的数

据库，数据中心可以是工作-工作状态，也可以是工作-备份状态，这样可以从容应对灾难性事件。

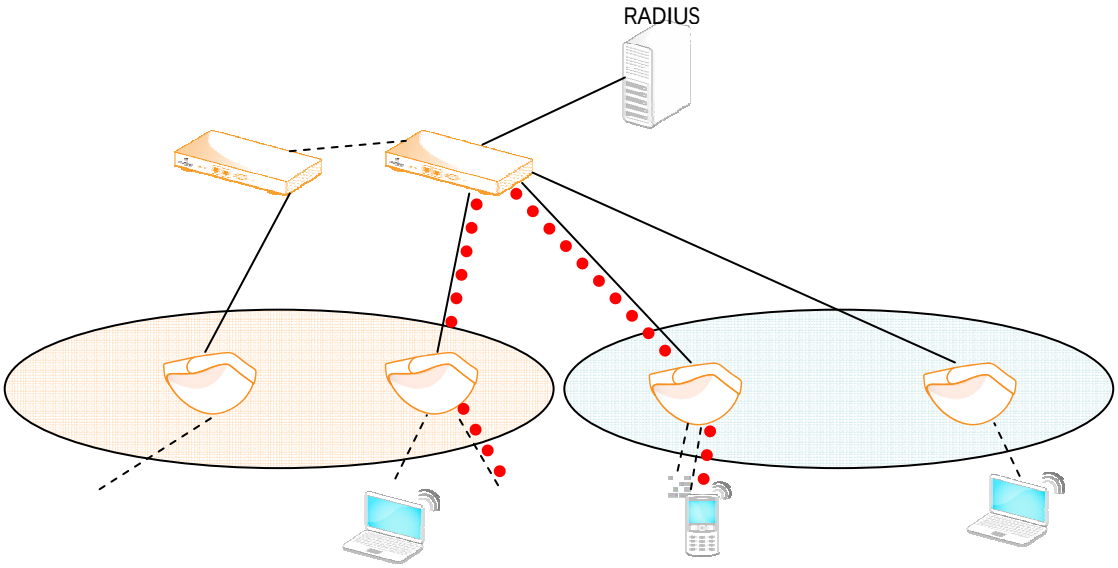


在某些重要的场所，可以在一个 IP 子网内部署冗余的 Ruckus 无线公司的无线控制器 ZoneDirector 1000/3000，当某一个工作的 ZoneDirector 1000/3000 出现故障，AP 会自动注册到备用的 ZoneDirector 1000/3000，无线用户能够维持会话，不需要重新手工登录。其效果和无线用户在同一个 ZoneDirector 1000/3000 管理下的不同 AP 之间漫游的效果是一样的。



3．2．4 客户端的漫游

无线用户在在同一个 ZoneDirector 1000/3000 管理下的不同 AP 之间可以无缝漫游，维持会话的连续性。



对于基于 802.1x 认证的漫游，ZoneDirector 1000/3000 和无线客户端在完成 802.1x/EAP 认证后，ZoneDirector 1000/3000 和无线客户端保存 PMK，ZoneDirector 1000/3000 把保存的 PMK 通知邻近的 AP，当无线客户端漫游到邻近 AP，搜索到同样的 SSID，无线客户端会使用存储的 PMK 和新的 AP 做 4 次握手，完成快速漫游切换。当无线客户端再漫游回到原先的 AP 时，无线客户端仍然会使用存储的 PMK 和原先的 AP 做 4 次握手，完成快速漫游切换，每个 PMK 一般保存 8 个小时。

3．2．5 SNMP 和 TR-069

SNMP 简单网管协议比较适合在企业网内使用，当用于管理大规模网络的时候，SNMP 会遇到不能穿透防火墙或 NAT 设备的难题。而基于 TR-069 的集中网管系统能够穿透 NAT 设备，方便的管理分布于不同区域、数量庞大的 CPE(客户端网络设备)，集中管理服务器具有如下功能：自动设备发现、批量并发配置更新、安全远程无线监视、告警、日志和报告、单个设备的细节管理、无需上门进行故障诊断、可远程自动升级。AP 的部署简单，只需要配置好 IP 地址和 TR-069 的集中网管服务器的 URL，设备就会自动完成 AP 的复杂

配置。基本做到 AP 设备的“零”配置或即插即用。

Ruckus 无线公司的 AP 既支持传统的 SNMP 网管，也支持新型的 TR-069 网管。如果用户已部署 SNMP 网管系统，Ruckus 公司可以提供 AP 详细的 MIB 库，经 SNMP 网管软件编译后，Ruckus 公司的 AP 就可以纳入用户的 SNMP 网管系统来管理。

如果用户新建网管系统，则建议采用新的 TR-069 网管系统，如 Ruckus 公司的基于 TR-069 协议的 FlexMaster 网管系统，安装在一台通用的 Linux 服务器上，就可以管理多达 20000 台 Ruckus 公司的 AP。

Ruckus 公司的 AP 可以人为配置由基于 SNMP 的网管系统管理还是由基于 TR-069 的网管系统管理，也可以让 AP 自动选择。如果 AP 找到基于 TR-069 的网管系统，则选择 TR-069 管理系统，否则选择 SNMP 的网管系统，但同时 AP 仍然会继续寻找基于 TR-069 的网管系统。随着网络规模的不断发展，基于 TR-069 的网管系统会越来越普遍。

3．3 Ruckus 无线局域网系统的安全管理

3．3．1 网络安全的体系架构

网络安全的任何一项工作，都必须在网络安全组织、网络安全策略、网络安全技术、网络安全运行体系的综合作用下才能取得成效。首先必须有具体的人和组织来承担安全工作，并且赋予组织相应的责权；其次必须有相应的安全策略来指导和规范安全工作的开展，明确应该做什么，不应该做什么，按什么流程和方法来做；再次若有了安全组织、安全目标和安全策略后，需要选择合适的安全技术方案来满足安全目标；最后在确定了安全组织、安全策略、安全技术后，必须通过规范的运作过程来实施安全工作，将安全组织、安全策略和安全技术有机地结合起来，形成一个相互推动、相互联系地整体，通过实际的工程运作和动态的运营维护，最终实现安全工作的目标。

完善的网络安全体系应包括安全策略体系、安全组织体系、安全技术体系、安全运作体系.

安全策略体系应包括网络安全的目标、方针、策略、规范、标准及流程等，并通过在组织内对安全策略的发布和落实来保证对网络安全的承诺与支持。安全组织体系包括安全组织结构建立、安全角色和职责划分、人员安全管理、安全培训和教育、第三方安全管理等。安全技术体系主要包括鉴别和认证、访问控制、内容安全、冗余和恢复、审计和响应。安全运作体系包括安全管理和技术实施的操作规程，实施手段和考核办法。安全运作体系提供安全管理和安全操作人员具体的实施指导，是整个安全体系的操作基础。

从管理和技术两个维度推进网络安全工作不仅是现阶段解决好网络安全问题的需要，也是今后网络安全发展的必然趋势。

从技术角度而言

1．逻辑隔离技术。以防火墙为代表的逻辑隔离技术将逐步向大容量，高效率，基于内容的过滤技术以及与入侵监测和主动防卫设备、防病毒网关设备联动的方向发展，形成具有统计分析功能的综合性网络安全产品。

2．防病毒技术。防病毒技术将逐步实现由单机防病毒向网络防病毒方式过渡，而防病毒网关产品的病毒库更新效率和服务水平,将成为今后防病毒产品竞争的核心要素。

3．身份认证技术。80%的攻击发生在内部，而不是外部。内部网的管理和访问控制相对外部的隔离来讲要复杂得多。在一般人的心目中，基于 Radius 的鉴别、授权和管理（AAA）系统是一个非常庞大的安全体系，主要用于大的网络运营商，企业内部不需要这么复杂的东西。这种看法越来越过时，实际上组织内部网同样需要一套强大的 AAA 系统。

4．入侵监测和主动防卫技术。入侵检测和主动防卫（IDS、IPS）作为一种实时交互的监测和主动防卫手段，正越来越多的被政府和企业应用，但如何解决监测效率和错报、漏报率的矛盾，需要继续进行研究。

5．加密和虚拟专用网技术。组织的员工外出、移动办公、单位和合作伙伴之间、分支机构之间通过公用的互联网通信是必需的，因此加密通信和虚拟专用网（VPN）有很大的市场需求。IPSec 已经成为市场的主流和标准。

6．网管。网络安全越完善，体系架构就越复杂。管理网络的多台安全设备需要集中网管。集中网管是目前安全市场的一大趋势。

从管理角度讲应遵循以下原则

1．整体考虑，统一规划。网络安全取决于系统中最薄弱的环节。“一点突破，全网突破”，单个系统考虑安全问题并不能真正有效的保证安全，需要从整体 IT 体系层次建立网络安全架构，整体考虑，全面防护。

2．战略优先，合理保护。网络安全工作应服从组织信息化建设总体战略，滚动式实现系统安全体系的统一。在此前提之下，追求适度安全，合理保护组织信息资产，安全投入与资产的价值应相匹配。

3．集中管理，重点防护。统筹设计安全总体架构，建立规范、有序的安全管理流程，集中管理各系统的安全问题，避免安全“孤岛”和安全“短板”。

4．七分管理，三分技术。管理是企业网络安全的核心，技术是安全管理的保证。只有制定完整的规章制度、行为准则并和安全技术手段合理结合，网络系统的安全才会有最大的保障。

3．3．2 基础型无线网安全机制

（1）更改无线 AP 的管理员登录初始口令和初始 SSID

（2）SSID 设置成隐藏，不广播 SSID

大多数破解无线网的初始步骤都是先嗅探出无线 AP 所使用的频道和 SSID，再进行下一个步抓包、破解。隐藏 SSID 广播功能可能对某些嗅探工具有用。

（3）WEP 加密

尽管 WEP 已经被证明是比较脆弱的，但是采用加密方式比明文传播还是要安全一些。现在可以从互联网上下载到很多破解 WEP 加密的工具软件，象 Airsnort 这种工具可以对无线网信号进行抓包，进行破解 WEP 密钥，避免这种工具破解最有效的方法就是给 WEP 设置较为健壮的 128 位密钥，而不是 40 位的密钥，这样可以让破解的难度加大，而需要更长的时间。

（4）采用比 WEP 更安全的 WPA，甚至 WPA2

要破解 WPA 加密并非易事，需要监听到的数据包是合法客户端正在开始与无线 AP 进行“握手”的有关验证操作过程，而且还要提供一个正好包含有这个密钥的“字典文件”。除非为 WPA 设置了比如：ADMIN123，111222333444 这样的“大众式”密钥，容易被猜中而收录在“字典”中，那么设置了复杂的密码组合

还是比较安全的。而 WPA2 是 WPA 的第二代，它支持更高级的 AES 加密，因此能够更好地解决无线网络的安全问题。

（5）MAC 地址访问控制列表

对于小型的无线网，可以采用 MAC 访问列表功能的精确限制哪些无线工作站可以连接到无线网中，而那些不在访问列表中的工作站，是无权进入无线网络中的。每一块无线网卡都有自己的 MAC 地址，我们可以在无线网络节点设备中创建一张“MAC 访问控制表”，然后将合法的无线网卡 MAC 地址逐一录入到这个列表中，允许只有“MAC 访问控制表”中显示的 MAC 地址，才能进入到无线网络中。当然 MAC 地址是有可能被非法访问者克隆，这要求我们妥善保管相关网卡的 MAC 信息，防止遗失。

（6）关闭 SNMP 功能

要是无线网络访问节点支持“简单网络管理”（SNMP）功能的话，笔者建议你尽量将该功能关闭，以防止非法攻击者轻易地通过无线网络节点，来获取整个无线局域网中的隐私信息。

以上安全机制主要针对分布式胖的部署方式。实现比较简单有效，主要解决无线覆盖的问题。

3．3．3 增强型无线网安全机制

若无线网传输的数据较为重要，或者连接到一个保密级别较高但又不能进物理隔离的有线网络的情况下，可以考虑采用增强的无线网安全防范措施。

（1）Web Portal 和 802.1x 认证

Web Portal 认证的基本过程是：客户机首先通过 DHCP 协议获取到 IP 地址（也可以使用静态 IP 地址），但是客户使用获取到的 IP 地址并不能登上 Internet，在认证通过前只能访问特定的 IP 地址，这个地址通常是 PORTAL 服务器的 IP 地址。采用 Portal 认证的接入设备必须具备这个能力。用户登录到 Portal Server 后，可以浏览上面的内容，比如广告、新闻等免费信息，同时用户还可以在网页上输入用户名和密码，它们会被 WEB 客户端应用程序传给 Portal Server，再由 Portal Server 与 NAS

之间交互来实现用户的认证。Portal Server 在获得用户的用户名和密码外，还会得到用户的 IP 地址，以它为索引来标识用户。然后 Portal Server 与 NAS 之间用 Portal 协议直接通信，而 NAS 又与 RADIUS 服务器直接通信完成用户的认证和上线过程。因为安全问题，通常支持安全性较强的 CHAP 式认证。它的优点是不需要特殊的客户端软件，降低网络维护工作量。

802.1X 是一个 IEEE 标准，用于对有线以太网和无线 802.11 网络进行经过身份验证的网络访问。IEEE 802.1X 支持集中化用户标识、身份验证、动态密钥管理以及记帐。802.1X 标准通过允许计算机和网络彼此验证身份、生成通过无线连接加密数据的每用户/每会话密钥以及提供动态更改密钥的能力来提高安全性。

（2）VPN 虚拟专网系统

除了 802.1x 认证，在无线网之上采用 VPN 技术，可以进一步增强关键数据的安全性。VPN 技术不属于 802.11 标准定义，因此它是一种增强性无线网络安全解决方案。

VPN 协议包括第二层 PPTP/L2TP 协议以及第三层的 IPsec 协议。VPN 只涉及发起端，终结端，因此对无线访问点 AP 来讲是透明的，并不需要在无线访问点支持 VPN。IPsec 是标准的第三层安全协议，用于保护 IP 数据包或上层数据，它可以定义哪些数据流需要保护，怎样保护以及应该将这些受保护的数据流转发给谁。由于它工作在网络层，因此可以用于两台主机之间，网络安全网关之间，或主机与网关之间。

当对数据的安全性要求非常之高时，可以考虑增加 VPN 虚拟网关，尤其是以 IPsec 协议建立的 VPN。这是目前可以实现的较高数据安全等级的技术。

（3）防火墙系统

防火墙是建立在被保护网络与不可信网络之间的一道安全屏障，用于保护企业内部网络和资源。它在内部和外部两个网络之间建立一个安全控制点，对进、出内部网络的服务和访问进行控制和审计。

防火墙产品主要分为两大类：

包过滤防火墙（网络层）在网络层提供较低级别的安全防护和控制。

应用级防火墙（应用代理）在最高的应用层提供高级别的安全防护和控制。

应将无线局域网的流量接入有线网的非信任区，由整个网络的安全控制机制统一

的进行安全控制。

如果专门为无线配置防火墙，会造成不必要的设备成本的增加；分散的安全机制造成安全策略的不一致等。

（4）专用无线网入侵检测系统

采用第三方专业公司生产的无线网专用入侵检测系统对网络进行监控，及时发现非法接入的 AP 以及假冒的客户端，并且对无线网的安全状况进行实时的分析和监控。

WLAN 入侵检测系统主要是针对采用 802.11 协议的 WLAN 进行网络安全状态的判断和分析，WLAN 入侵检测系统采用了分布式的结构，将进行数据采集的 Sensor 分布在 WLAN 的边缘和关键地点，并且通过有线的方式将收集到的信息统一传输到一个集中的信息处理平台。

信息处理平台通过对 802.11 协议的解码和分析，判断有无异常现象，比如非法接入的 AP 和终端设备、中间人攻击、有无违反规定传输数据的情况，以及通过对无线网络进行的性能和状态分析，识别拒绝服务攻击现象。它能够自动发现网络中存在的 Ad Hoc 网络，并且通过通知管理员来及时阻止可能造成的进一步损害。基于 Web 界面的安全管理界面让管理员可以进行策略的集中配置和分发，以及观察网络状况、产生报表。

WLAN 入侵检测系统通过结合协议分析、特征比对以及异常状况检测三种技术，对 WLAN 网络流量进行深入分析，并且能够实时阻断非法连接。

（5）动态秘钥技术

Ruckus 无线系统可以为每个用户分配唯一的加密密钥，对 MAC 地址一一对应，这样就不用一条 KEY 由 N 个人共用，并且可以定义密钥的使用时间。这种方法在使用上相对麻烦一些。

3．3．4 Ruckus 支持的认证方式

AP 支持认证方式

用户可以通过设置 AP 自身对无线用户进行认证。认证方式有以下几种：

1. 开放

2. WEP
3. WPA/WPA2
4. WPA-PSK/WPA2-PSK
5. 802.1X 认证

Zone Director 无线控制器支持的认证方式

用户可以通过 Ruckus ZoneDirector 对无线用户进行认证。认证方式有以下几种：

1. 本地认证
2. 与现有的 Windows 服务器的 AD 认证
3. 与现有的 RADIUS 服务器整合进行认证
4. 802.1X 认证

3．3．5 安全的 AP 技术

由于 Ruckus 的 AP 是不储存任何网络配置（IP 地址除外）和安全设置，因此 Ruckus 管理的 AP 是不能单独工作的，因此获得和接入进 Ruckus AP，黑客也不会拿到无线网的网络和安全配置参数。

3．3．6 无线接入点安全侦测和保护

采用 Ruckus 无线系统的 RF 侦测功能和保护机制可以实时监测厂区无线网覆盖区域内的所有 AP 接入情况,如相邻的 AP、设置错误的 AP 以及未经认可而连接到网络中的 AP。通过 Ruckus 的网络安全管理系统，网络安全管理人员可以及时发现是否有非法的 AP 接入，发现后可以开启自动保护机制，阻止无线终端通过非法 AP 联接到无线网中。

3．3．7 无线网络入侵侦测

网络监控与入侵检测系统将网络上传输的数据实时捕获下来，检查是否有黑客入侵和可疑活动的发生，一旦发现有黑客入侵，系统将做出实时响应和报警。

入侵检测模型可以分为两大类：基于网络的入侵检测：通过实时监视网络上的数据流，来寻找具有网络攻击特征的活动；基于主机的入侵检测：通过分析系统的审记数据，检查系统资源的使用情况以及启动的服务等来检测本机是否受到了攻击。

对已知攻击的检测:通过分析攻击的原理提取攻击特征，建立攻击特征库，使用模式匹配的方法，来识别攻击； 对未知攻击和可疑活动的检测:通过建立统计模型和智能分析模块，来发现新的攻击和可疑活动。

Ruckus 向用户推荐使用第三方的入侵侦测产品。入侵侦测是专业性非常强的技术，需要对网络攻击有深入的认识。入侵侦测做的不专业，只能是花钱买心理安慰，不能发挥作用。入侵侦测只是报警并不能防范，所以还要与网络安全服务商签订服务合同，通过人为的方式改变网络的参数配置实现网络的防入侵，防攻击。Ruckus 的专长在天线的技术，射频的技术，以及网络接入技术。我们认为在无线产品中加入入侵侦测功能，并不能对用户的网络安全做到全方位的保护，同时还增加了用户不必要的成本。

3．3．8 无线接入的病毒防护

病毒的防护要从客户端的防护做起。客户端中毒会造成性能下降，不能正常工作，丢失文件，丢失密码，形成僵尸被控制机所控制。对网络有影响主要是蠕虫类病毒。通过计算机网络传播，不改变文件和资料信息，利用网络从一台机器的内存传播到其他机器的内存，计算网络地址，将自身的病毒通过网络发送。像蠕虫病毒尼坶达，它不但会感染 EXE 文件，还会通过局域网，电子邮件网页等途径进行传播。对网络形成压力，造成网络系统的不稳定。

所以病毒的防护，一定要从源头抓起，要采取各种手段，减少客户端不中毒的可能性。同时 Ruckus AP 还可以进行限速，对于每一个客户端的速率进行严格限定，纵然客户端中毒，病毒在网络上泛滥也不会造成网络的瘫痪，减缓病毒在网络上传播的速度。同时 Ruckus 还有较强的访问控制机制，可以采取阻断中毒客户端流量的措施。但所有这些网络手段只能是辅助性的，是防护性的。

3．3．9 通过 VPN 再次加固无线接入

对于数据安全性要求非常高的用户可以考虑 VPN 的方式，尤其是 IPSec 的 VPN 解决方案。IPSec 协议是网络层协议，是为保障 IP 通信而提供的一系列协议族。IPSec 针对数据在通过公共网络时的数据完整性、安全性和合法性等问题设计了一整套隧道、加密和认证方案。IPSec 能为 IPv4/IPv6 网络提供能共同操作/使用的、高品质的、基于加密的安全机制。提供包括存取控制、无连接数据的完整性、数据源认证、防止重发攻击、基于加密的数据机密性和受限数据流的机密性服务。

IPSec 的基本目的是把密码学的安全机制引入 IP 协议，通过使用现代密码学方法支持保密和认证服务，使用户能有选择地使用，并得到所期望的安全服务。IPSec 将几种安全技术结合形成一个完整的安全体系，它包括安全协议部分和密钥协商部分。

（1）安全关联和安全策略：安全关联（Security Association，SA）是构成 IPSec 的基础，是两个通信实体经协商建立起来的一种协定，它们决定了用来保护数据包安全的安全协议（AH 协议或者 ESP 协议）、转码方式、密钥及密钥的有效存在时间等。

（2）IPSec 协议的运行模式：IPSec 协议的运行模式有两种，IPSec 隧道模式及 IPSec 传输模式。隧道模式的特点是数据包最终目的地不是安全终点。通常情况下，只要 IPSec 双方有一方是安全网关或路由器，就必须使用隧道模式。传输模式下，IPSec 主要对上层协议即 IP 包的载荷进行封装保护，通常情况下，传输模式只用于两台主机之间的安全通信。

（3）AH（Authentication Header，认证头）协议：设计 AH 认证协议的目的是用来增加 IP 数据报的安全性。AH 协议提供无连接的完整性、数据源认证和抗重放保护服务，但是 AH 不提供任何保密性服务。IPSec 验证报头 AH 是个用于提供 IP 数据报完整性、身份认证和可选的抗重传攻击的机制，但是不提供数据机密性保护。 验证报头的认证算法有两种：一种是基于对称加密算法（如 DES），另一种是基于单向哈希算法（如 MD5 或 SHA-1）。验证报头的工作方式有传输模式和隧道模式。传输模式只对上层协议数据（传输层数据）和 IP 头中的固定字段提供认证保护，把 AH 插在 IP 报头的后面，主要适合于主机实现。隧道模式把需要保护的 IP 包封装在新的 IP 包中，作为新报文的载荷， 然后把 AH 插在新的 IP 报头的后面。隧道模式对整个 IP 数据报提供认证保护。

（4）ESP（Encapsulate Security Payload，封装安全载荷）协议：封装安全载荷（ESP）用于提高 Internet 协议（IP）协议的安全性。它可为 IP 提供机密性、数据源验证、抗重放

以及数据完整性等安全服务。ESP 属于 IPSec 的机密性服务。其中，数据机密性是 ESP 的基本功能，而数据源身份认证、数据完整性检验以及抗重传保护都是可选的。ESP 主要支持 IP 数据包的机密性，它将需要保护的用户数据进行加密后再重新封装到新的 IP 数据包中。

（5）Internet 密钥交换协议（IKE）：Internet 密钥交换协议（IKE）是 IPSec 默认的安全密钥协商方法。IKE 通过一系列报文交换为两个实体（如网络终端或网关）进行安全通信派生会话密钥。IKE 建立在 Internet 安全关联和密钥管理协议（ISAKMP）定义的一个框架之上。IKE 是 IPSec 目前正式确定的密钥交换协议，IKE 为 IPSec 的 AH 和 ESP 协议提供密钥交换管理和 SA 管理，同时也为 ISAKMP 提供密钥管理和安全管理。IKE 具有两种密钥管理协议（Oakley 和 SKEME 安全密钥交换机制）的一部分功能，并综合了 Oakley 和 SKEME 的密钥交换方案，形成了自己独一无二的受鉴别保护的加密材料生成技术。

在数据链路的加密选项中尽量选择 3DES 和 AES 的加密算法。以目前的技术水平，即使破解了截获的数据，并且破解了有效内容，其破解消耗的时间非常长，以至于信息已经失效。

对称加密算法用来对敏感数据等信息进行加密，常用的算法包括：

DES（Data Encryption Standard）：数据加密标准，速度较快，适用于加密大量数据的场合。

3DES（Triple DES）：是基于 DES，对一块数据用三个不同的密钥进行三次加密，强度更高。

AES（Advanced Encryption Standard）：高级加密标准，是下一代的加密算法标准，速度快，安全级别高；

AES 算法基于排列和置换运算。排列是对数据重新进行安排，置换是将一个数据单元替换为另一个。AES 使用几种不同的方法来执行排列和置换运算。AES 是一个迭代的、对称密钥分组的密码，它可以使用 128、192 和 256 位密钥，并且用 128 位（16 字节）分组加密和解密数据。与公共密钥密码使用密钥对不同，对称密钥密码使用相同的密钥加密和解密数据。通过分组密码返回的加密数据的位数与输入数据相同。迭代加密使用一个循环结构，在该循环中重复置换和替换输入数据。

AES 与 3DES 的比较

算法名称	算法类型	密钥长度	速	解密时间（建设机器	资源消耗

			度	每秒尝试255个密钥）	
AES	对称 block 密码	128、192、256 位	高	1490000 亿年	低
3DES	对称 feistel 密码	112 位或 168 位	低	46 亿年	中

通过以上的介绍可以看出 VPN 尤其是基于 IPSec 的 VPN 是非常安全的技术。只要终端设备是正常的，整个通讯过程都是非常安全的，尤其是利用证书方式的加密。当然，由此也产生了一个新的问题，从哪里得到证书。所以说，安全是一个系统，包括方方面面的组成部分。为取得理论上尽可能的安全，付出的代价也是不小的。用户应该在成本和安全系统强度之间取得一定的平衡。

3．4 无线移动音视频应用－Ruckus SmartCast

3．4．1 带宽控制与服务质量保证 QOS

WiFi 最初的设计是用于数据应用（尽最大努力传送）。所有 802.11 用户都使用同一频道，先到先服务。当某个需要发送数据的用户发现信道是忙碌的，它必须避免相撞等待一个随机时期。这是被称为 CSMA / CA （载波侦听/冲突避免）的技术。

在一个不繁忙的 Wi - Fi 网络，一个用户可以轻松地拥有整个频道。由于负荷增加，所有用户都需要遭受同样的等待更长的时间才能传送的情况。这种设计适用于多数数据应用,但创造一个适合于对时延和抖动敏感的多媒体业务的网络则需要一个完全不同的方法。SIP ， H.323 协议 VoIP 协议不同，语音、视频对带宽的要求不同，但对性能的要求要求是一致的。

具体来说，在传送实时同步的业务流时，必须尽量减少抖动，延迟和数据包的丢失。数据包到达时间的标号产生抖动，表现为声音和图象的不连贯。延迟或丢失的音频或视频数据包可以通过缓冲进行平滑。但 VoIP 数据包延迟，可使电话无法拨通和使用。

因此， IEEE 定义了 802.11 e （ MAC 层上的增强服务质量） ，以改善音频，视频和语音在 WiFi 网络上的传输 。许多企业级 AP 产品(但不包括消费性 AP 产品)支持 802.11

e 的子集：所谓 Wi - Fi 多媒体（ WMM ）给不同的 Wi - Fi 业务流分配不同的优先级，使需要不同的延迟和吞吐量的应用，可以得到更适当的处理。WMM 的定义 4 类业务：语音，视频，尽最好的努力（一般为数据），和背景业务流支持 WMM 的 AP 通常具有不同的传输队列，可以比其他的业务流更频繁，更长时间地传输语音（VoWLAN）业务。不过，WMM 仍不能区分具有相同的优先级的应用。如果由于干扰或衰减，一个语音终端的连接已经断开，AP 仍将尝试将语音重新发送到该语音终端，而不是向其他语音终端发送队列中的语音业务包。

在 VoWLAN 终端从一个 AP 漫游到另外一个 AP 时，WMM 也不能减少延迟。（ Wi - Fi 设备会不断评估的信号强度，并会自动重新连接到“最佳的”AP”） 。在短期内，WMM 的优先级技术可以给 VoWLAN 一个尝试的机会，但仍然没有解决语音质量下降的本质问题。较新的 11n AP 可使数据的传输速度更快，更远，但对解决语音和视频质量或链路的不稳定毫无裨益。

Ruckus Wirelss 专利的 SmartCast 技术，包括创新的组播流量处理技术、智能 QoS 和基于“识别应用”的流量分类能力。这些技术可确保无线数据传输能够实现最高的可靠性。

SmartCast 能够从所有流量中自动区分和管理语音、视频流以及数据和背景管理数据流，还能够提供从宽带网关到用户多媒体终端的强大稳定无线传输。当 SmartCast 检测出用户为多媒体终端时，就会将相关的语音或视频，包括组播视频包使用优化的数据传输速率和信号传输路径传递到接收端。这样即可为语音和视频包的可靠传输保证最佳的性能。为多媒体优化的流量管理算法，能够确保语音和多个广播级质量视频流性能，同时还能确保针对数据应用足够的带宽。SmartCast 可智能地根据不同应用的流量特性、UDP/TCP 端口和其他应用属性对所有流量分类，并且根据分类的优先级和特点管理每一种流量类型（视频、语音和数据）。

自动的打服务类型（ToS）标签功能能够避免复杂的 QoS 配置，而自动管理低速 802.11b 设备的功能可为优先的视频应用保证有效的带宽。每个客户端拥有 4 个优先级队列，从而在同时传送语音、多个视频流时还能够保证传输优先级和精确性。将由一个专门调度器对所有包根据相应的流量类型来排入/排出队列。每个调度器都会考虑语音、视频和数据流量对延迟/抖动容忍度、带宽需求以及不断变化的无线客户端性能特点需求，从而保证最佳的用户体验。

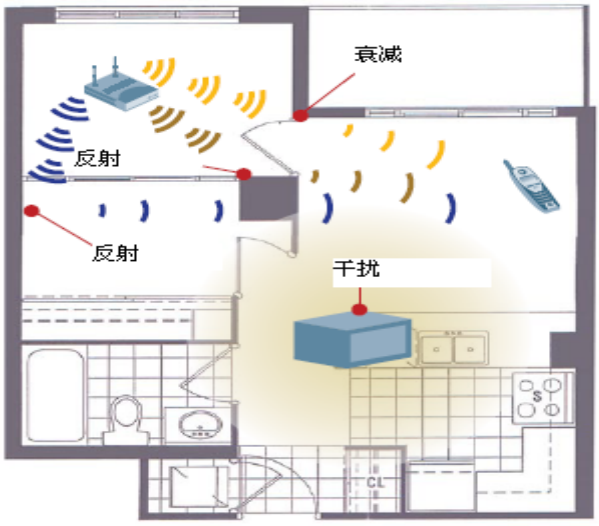
Ruckus 无线系统的带宽管理能力使得在移动音视频应用方面表现出很强的优势。还可

以限制用户无线连接的最高带宽，以及分别设置语音、视频和数据的应用带宽。

3．4．2 BeamFlex 和 服务品质保证

因为 802.11 业务流是使用公用频段进行传输的，无需购买频段和授权， Wi – Fi 网络可以被任何人很容易和方便地部署在家里，办公室，或其他公众地点。今天，许多消费者将 Wi – Fi 技术和宽带连接结合，以便于在室内各个房间进行网页浏览和电子邮件。但是，当消费者尝试利用 Wi – Fi 技术做更多的事情时，结果却往往是失望，尤其是当试图实现实时多媒体应用－语音时。

开始， Wi – Fi 频段干扰非常严重。 802.11 无线使用的 2.4 和 5 GHz 频带也被其他设备包括无绳电话，蓝牙设备，卫星服务以及与周边 Wi - Fi 网络使用。这些干扰源使室内 WiFi 设备难以区分合法的传输和背景噪音。调整 AP 的发射频率（频道），可以减少噪音。但只有三个不重叠的频道供 802.11 b / g 设备使用，大多数 Wi - Fi 网络，最终将与若干个干扰设备共存。Wi - Fi 信号变弱，不仅因为噪音，还有距离和障碍物。一台笔记本电脑和 AP 在同一房间内，如果它们之间只有空气，可以体验较高的数据传输速率达 54 Mbps 。但把笔记型电脑放在隔壁房间，部分无线电波将被墙吸收（衰减）（见图） 。



Wi - Fi 网络还受隐藏节点和多路径传输的影响。多路径传输的发生是因为无线电波在发送端和接收端传送时，会以一定的角度反射，特别是液体或金属表面（例如，百叶窗，电器，门） 。多次反射的相同的信号可能都会达到接收端，在那里的增强，减弱，无效或破坏的主信号。这种常见的现象，造成信号严重退化和覆盖漏洞。即使传输的条件保

持不变，避免多径衰落也是困难的。不过，射频环境的变化不断，从微波炉产生噪音，到人移动时产生的突发噪声，都会改变无线电波在室内的传播。即使是很小的环境变化可能对性能产生巨大影响。

新的 Wi - Fi 技术已了解多路径传输的问题。新兴的 IEEE 802.11n 标准对多个使用不同的路径达到接收器的 Wi - Fi 信号进行重组以提高吞吐量。2007 年批准的 802.11n 标准通过所谓的“空间复用”和使用更高容量的信道，可望实现的数据传输速率高达 200 Mbps 的性能。但是，

802.11n 标准在 2.4GHz 和 5GHz 频段通过将 20MHz 通道组合为 40MHz 通道以增加数据速率。更宽的通道主要用于高带宽的数据应用，但减少了非重叠的信道数量和增加了受干扰的可能。

802.11n 标准利用多径传输以改善覆盖范围和吞吐量。多输入多输出（ MIMO ）技术在某一距离提供了更高的数据传输速率。不过， 802.11n 标准不利于需要稳定时延一致的数据帧传输的应用，如 I P 语音、视频等。声音，与其他实时多媒体应用，更多的带宽不是一个问题；稳定，可预见的连接才是问题。

因此，在 WiFi 网络上提供可靠的语音服务需要一个与现有和未来的 802.11 技术兼容的新的解决办法。

虽然 802.11n 标准只使用不同的传播路径，以增加吞吐量，但可以使用不同的传播路径的优化到用户终端的传输。这既需要硬件/也需要软件的改进，具体来说，需要一种自适应的高增益天线阵列，采用智能算法为每个终端设备及应用动态地选择和配置天线，选择最佳传播途径，以达到最优化的性能。

多数室内 APs (包括支持 MIMO APs) 使用偶极子天线，能量在所有的方向输出。浪费了发射能量，并产生了干扰。自适应天线可以将发射能量集中在一个特定的方向，让无线电波的传播更远，减少与其他设备的干扰，并避免障碍物引起的信号衰减和反射。

智能阵列天线增加了可能的传播途径，当用户终端移动或环境条件变化时可以有更多的路径选择以达到特定的用户终端。当消费者手持一个 Wi - Fi 手机从一个 AP 漫游到另一个 AP，最佳传播路径也相应地变化 。当附近的一个微波炉或蓝牙启动时，信号传播路径再次改变以得到最佳的传输性能。事实上，最优传输路径会非常频繁并迅速地改变，能及时适应这些改变是非常关键的。

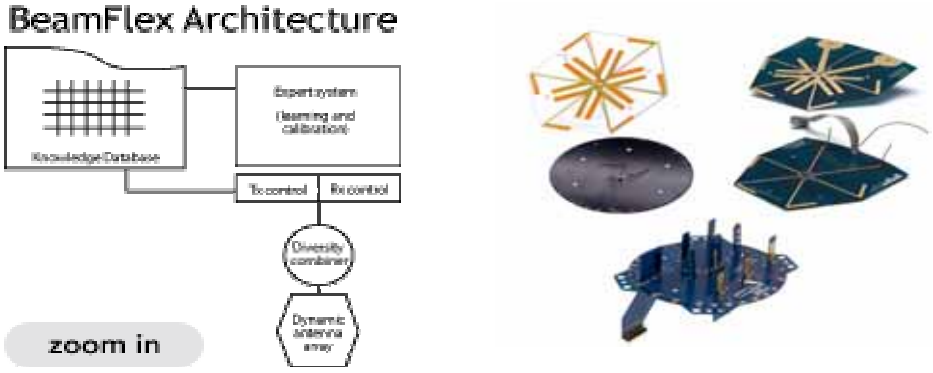
数据应用的传输比较弹性，保证正确地送达就基本可以了。视频流可以忍受的时延，

为数百或数千毫秒。但声音的延迟要求小得多。要保持 100 ms 以内的延迟，Wi- Fi 设备必须实时适应环境的变化，包括连续运动的语音终端实时调整最佳传输路径。

这些机制，使 AP 可以就往哪里和如何传送，处理什么输入，忽视什么干扰等问题作出明智选择。理想的情况是，这些物理层的算法应与链路层的算法，像 WMM 一样，能了解应用需求。这种 AP 可以不只是基于优先级作出如何传输的决定，而且还要基于目前每个用户端的表现来决定。

BeamFlex 智能天线阵列

每一个 Ruckus 的 AP 都内置了一个紧凑的、6 到 12 根天线组成的专利的 BeamFlex 天线阵列，这个阵列能够为分集形成 63 个到 4095 唯一的定向天线模式。基于专家系统的控制软件利用构建在 802.1MAC 层协议中的反馈机制不间断地为每一个接受设备调整天线模式。



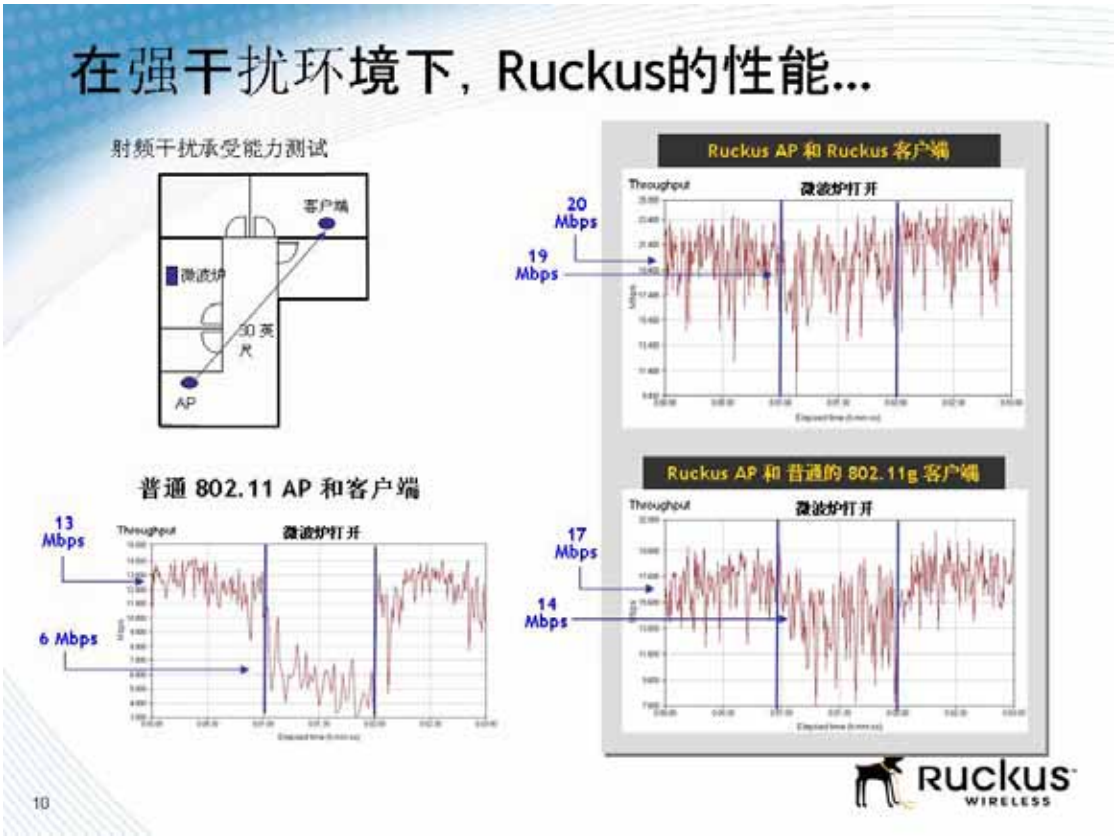
支持 BeamFlex 的 Ruckus AP 通过检测射频和多径问题以及邻居网络噪声带来的干扰，能够实时重新自行配置和调整。通过为每一个接收设备选择一个优化的天线阵列，BeamFlex 能够扩展无线覆盖范围并提供更高的通讯速度。利用 BeamFlex 天线系统的大量分集功能，可使 Ruckus AP 在一个不断变化的环境中从多种不同质量的信号传输路径中实时选择一个最优的传输路径。这一能力为语音和视频应用提供了稳定一致的性能基础。

除了提供大量的多级路径选择，天线结构和传输策略可以实现实时同步优化，BeamFlex 所具有的多边智能允许其实现最大程度的信号覆盖、吞吐量、网络容量，以确保对实时应用，如视频和在线游戏一致和瞬时流量传输。

动态防干扰，不像全方位天线，信号向四面八方辐射，BeamFlex 指挥能量向最佳路径传播。此外，不像固定位置的定向天线，BeamFlex 为每一个位置，每个包动态配置其"beam"，实现室内全方位的覆盖。BeamFlex 提供两种天线技术最好的技术以最大化功率效率，同时

减少对邻近网络和设备的噪音。

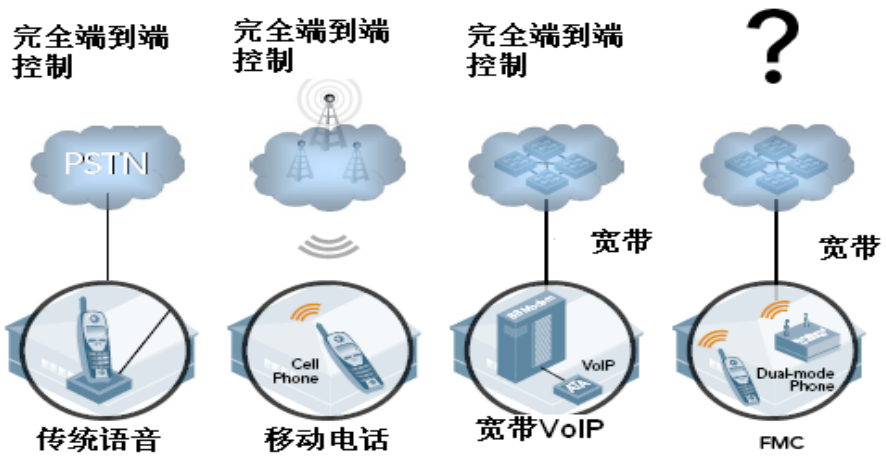
此外，避干扰算法使 BeamFlex 能侦查干扰来源的方向，例如相邻的网络、微波炉或附近的蓝牙装置。作为回应，BeamFlex 能选择天线模式，引导能量远离干涉方向;从而减轻噪声对接收站的影响。下面的性能报告证实了 BeamFlex 避干扰算法的性能。



3．4．3 VoIP 与 Wi-Fi 手机

对于消费者来说，固定/移动融合（ FMC ）是指集成语音和数据服务，到处都可以通过一个单一的手机，取代移动电话和固定电话。对电信运营商， FMC 的一个有利可图的机会，利用经济的技术从花费巨资的网络基础设施中卸载日益增加的多媒体业务流。

FMC 对运营商可管理语音业务的影响



不过，FMC 也对过去对语音连接具有完全端到端控制的运营商提出了一些新的挑战（见前图）。新的双模手机同时支持 Wi - Fi 和蜂窝技术，由于干扰和 QoS 问题，完全的端到端控制已经不可能。

此外，宽带运营商还面临如何管理最后 100 米接入的挑战。现有的语音服务，无论是蜂窝，宽带网络电话（VoIP）还是传统的 POTS，都是建立在端到端管理控制的基础上。由于目前还没有好的办法去深入了解或控制使用消费级 Wi – Fi 设备用户端的 Wi - Fi 连接，因此，服务质量不能得到保证。

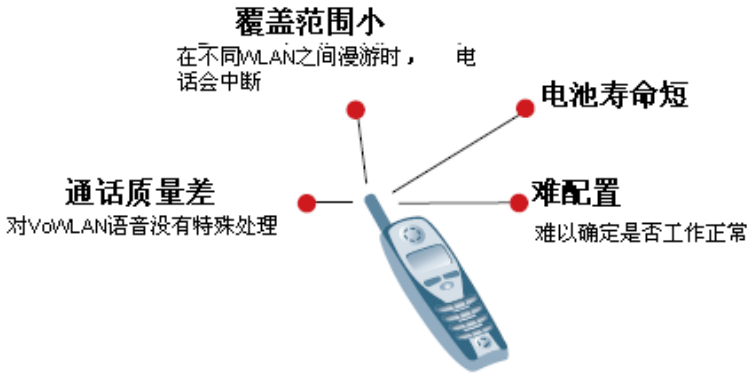
世界各地宽带运营商都忙于提供新的多媒体服务----即在宽带接入链路商提供所谓的三重或四重播放业务。尽管数据是宽带的最初驱动力，IPTV 和语音却是新的重点和亮点。这就需要建设一个可靠的基础设施，以同时支持所有的业务类型。但在室内，Wi - Fi 技术已成为用户室内数据传送事实上的标准，因为蜂窝技术覆盖是众所周知的弱，而且改善的代价太高。如果 W i- F i 可以变得足够稳定和可靠支持可支付的语音服务。 Wi - Fi 技术有着巨大的潜力，以较低的成本实现用户室内的融合服务的普及。

但是，双向、互动式语音业务极易受时延和干扰的影响。具体来说，在传送实时同步的业务流时，必须尽量减少抖动，延迟和数据包的丢失。数据包到达时间的标号产生抖动，表现为声音的不连贯。延迟或丢失的音频或视频数据包可以通过缓冲进行平滑。但 VoIP 数据包延迟，可使电话无法拨通和使用。

对 VoWLAN，无线系统必须能够在短短几毫秒内适应变化的无线电频率（ RF ）环境。保持一个更强壮，更可靠的 Wi - Fi 链接到的 WIFi 语音终端是至关重要的，这样才能

克服低或波动信号的引起的语音质量恶化和传统 VoWiFi 具有的电池问题。SIP、H.323 协议和其他专有 VoIP 虽然协议不同，但对性能的要求要求是一致的。

影响传统 802.11 WiFi 网络上语音业务的问题



通常传统的 AP 在所有时间都以最高的功率发射，希望可以“强行通过”传输路径上降低信号和范围的干扰和障碍。但结果是，WiFi 手机的电池很快耗光，同时增加 Wi - Fi 使用者之间的干扰。

因此可迅速重新计算最优路径和将语音流按照最佳路径进行传输的 Wi - Fi 系统可以减少双方的延迟和手机的功率消耗。将语音流按照特定的最佳路径传输到特定的 WiFi 手机，可以增加整体的覆盖范围，让手机在任何特定的距离保持更高传输速率，减少漫游（如果存在多个 AP）。完成这一功能需要实时监控每 WiFi 用户的 QoS 和算法。

通过最大限度地提高传输信号的强度和接收灵敏度，语音手机可以在更短的时间，以更低功耗发送相同的信息。这可以通过使用智能 Wi - Fi 天线，将信号以波束方式直接有针对地发送到语音手机，可以减少重播，延长电池的使用寿命，提高用户的满意程度。

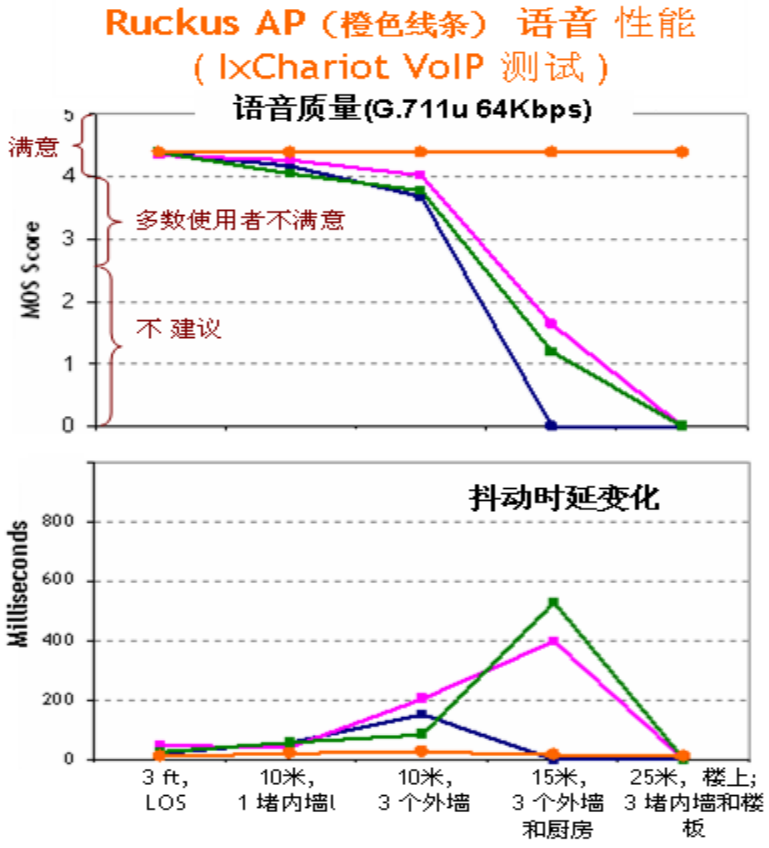
Ruckus 的 BeamFlex 技术扩大了覆盖范围，将语音流按照特定的最佳路径传输到特定的 WiFi 手机，降低了手机的消耗功率。同时 SmartCast 的智能、自适应的 QoS 技术，简化了手机的配置，提高了 WiFi 手机的普及性，对 VoWLAN 业务实现了端到端的控制。

因此，室内 AP 面临着许多技术挑战，从而其性能很难预测，更不用说控制了。当谈到语音业务时，连贯性和可靠性是至关重要的。象 802.11n 标准这样的改善不会使语音业务有任何更好结果一-事实上，在高吞吐量的数据将增加无线电波的竞争和干扰。

用户必须部署可靠的、可提供可预见的 QoS 的无线设备，选择正确的 CPE 以满足消使用者的期望和进行有效的竞争。因此必须了解影响 VoWiFi 的因素，并寻求创新的、针

对此类（VoWiFi）应用解决方案：AP 不仅要支持 WMM，而且能有效地处理与物理层的挑战，是部署话音，甚至运营商级话音业务的关键。

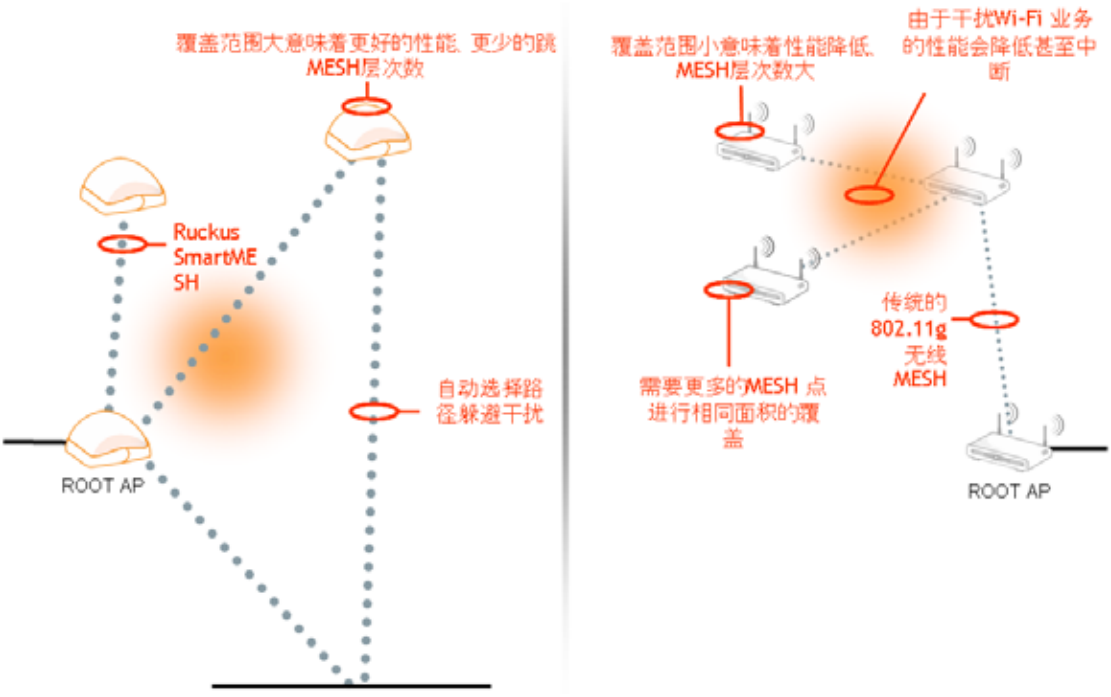
不是所有的AP都是相同的	
传统WiFi AP	智能AP（智能天线技术）
尽力而为的VoWiFi	运营级别的VoWiFi
无法管理无线信号频谱的发射	可以直接管理无线信号频谱的发射
50米半径覆盖	超过100米半径覆盖
无法控制无线信号的路径选择	动态、自适应无线信号路径选择
AP和手机没有同步	AP和手机之间的低功耗同步，确保不漏接来电
单或双全向天线，相互干扰	通过定向，高增益天线阵列子系统自动避免或减轻干扰
没有集成的QoS机制	语音流量的优先级，队列以及调度都优于数据和其他非延迟敏感业务



3．5 Ruckus 的智能网状网－SmartMesh

智能的 Ruckus Wi – Fi AP 是一个获得专利的创新，使 AP 能将无线信号以波束的方式，选择传播路径是 Wi - Fi 信号传输得更远，更快和更可靠。智能 Ruckus WiFi AP 技术由三

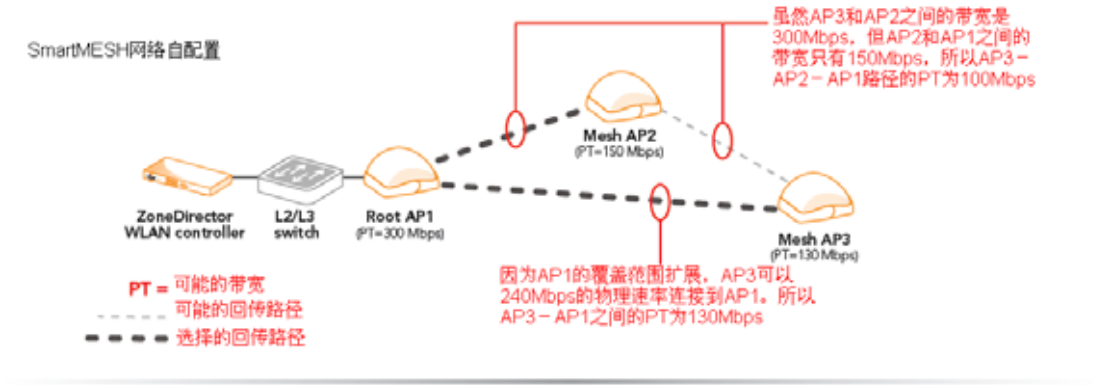
个部分组成：智能天线阵列，智能射频路由软件和智能的 QoS。Ruckus 智能 AP 能够选择无线信号的传输路径，避免干扰，得到更高的性能。如下图



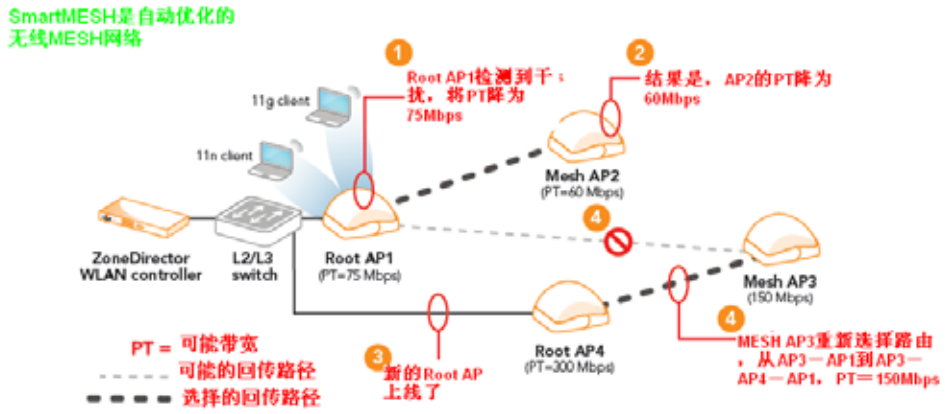
面对干扰，传统 AP 要么丢弃数据包或降低传输数据率，从而降低了系统吞吐量。

Ruckus SmartMESH 的智能 AP 具有独特的功能，可以找到一个信号路径以避免干扰，从而防止数据包丢失和维护更高的传输速率。

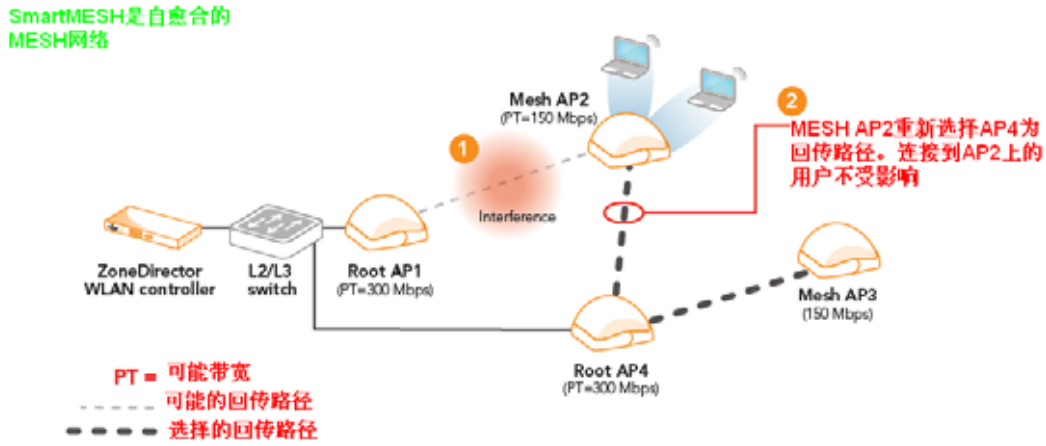
Ruckus 的 SmartMESH 的配置和组网，以及网络拓扑的形成是全自动的。用户无需对各 AP 进行详细配置就可以在 10 分钟内形成一个无线 MESH 网络。



Ruckus 的 SmartMESH 网络是自动优化的网络。SmartMESH 网络中的智能 Ruckus AP 会不断检测其工作环境和上行链路的带宽状况，自动地实时地选择最佳的回传路径，以使整个无线 MESH 网络具有最佳的性能和最好的稳定性、可靠性。



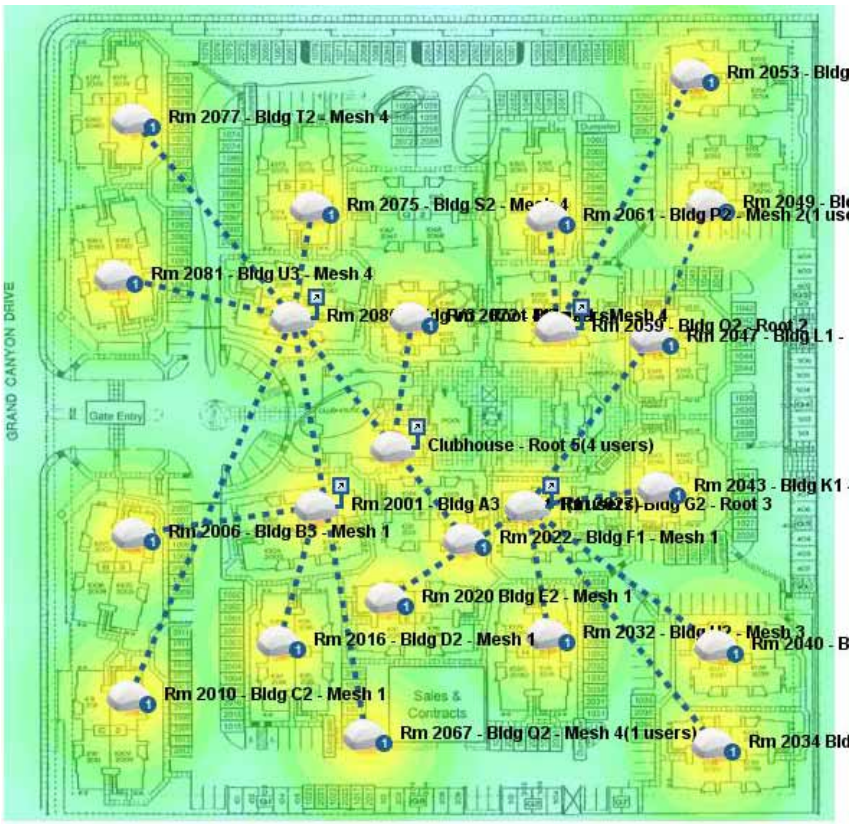
Ruckus 的 SmartMESH 是自动愈合的无线 MESH 网络。其智能 AP 会一直尝试找到一个最佳信号路径以避免干扰，从而防止数据包丢失和维护更高的传输速率。如果不能找到一个符合传输质量的信号路径，如果检测到上游 AP 的性能急剧下降，下游 SmartMesh 的 AP 上的自动拓扑软件（见下图 ）将会自动地重新找到新的回传路由。



Ruckus 的 SmartMESH 可以充分发挥 802.11n 技术的优势，得到最佳的无线传输性能。Ruckus Smart-N 自适应智能天线可以

- 通过 WiFi Tx/Rx 信号路径确保 multipath（Spatial Muxplexing）
- 为 11n spatial multiplexing 和 channel bonding 而优化。

以下是某大型无线项目应用 MESH 的拓扑图未例：



四、 深圳 XXX 工厂无线局域网方案建议

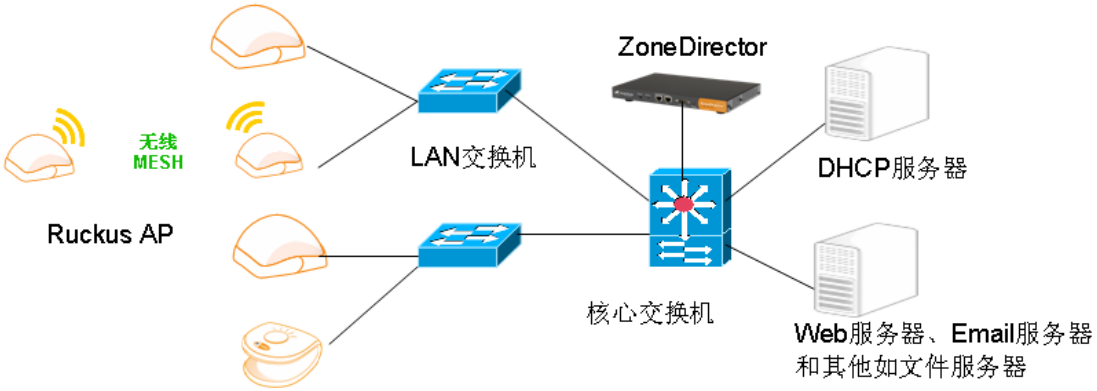
根据无线网络需求和无线网络设计原则，结合 Ruckus 无线系统技术及产品的特点，方案的设计分为：无线组网方式设计、多业务区分设计、网络及用户管理、网络安全防护设计、移动漫游、兼容性和计费设计七个部分。

4.1 无线组网方式设计

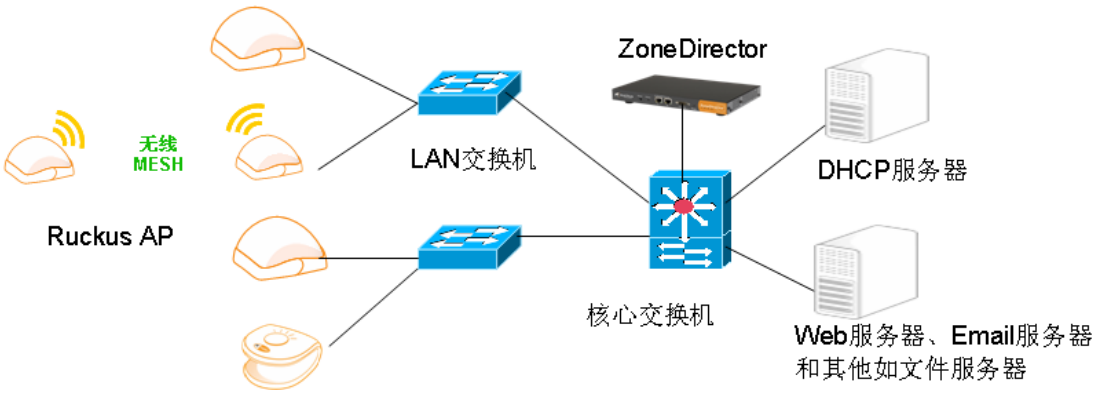
Ruckus 无线系统的组网方式有两种，集中式组网和分布式组网。可以根据不同的网络规模和管理方式，考虑选用以下不同档次的 ZoneDirector 和 FlexMaster 集中网管系统进行组网。

4．1．1 小型无线局域网(5 到 50 个 AP)集中式组网

如果整个无线系统的 AP 数量较少（少于 50 个），而且大部分都集中在一定区域内通过以太网交换机相连，那么可以采用单台 ZoneDirector1000 来组网。该 ZoneDirector1000 管理所有的 AP。如下图。



即使部分 AP 不是集中在特定区域内通过以太网交换机相连而是通过其他宽带连接，那么也可以采用单台 ZoneDirector1000 来组网，通过该 ZoneDirector1000 远程管理其他的 AP。如下图。

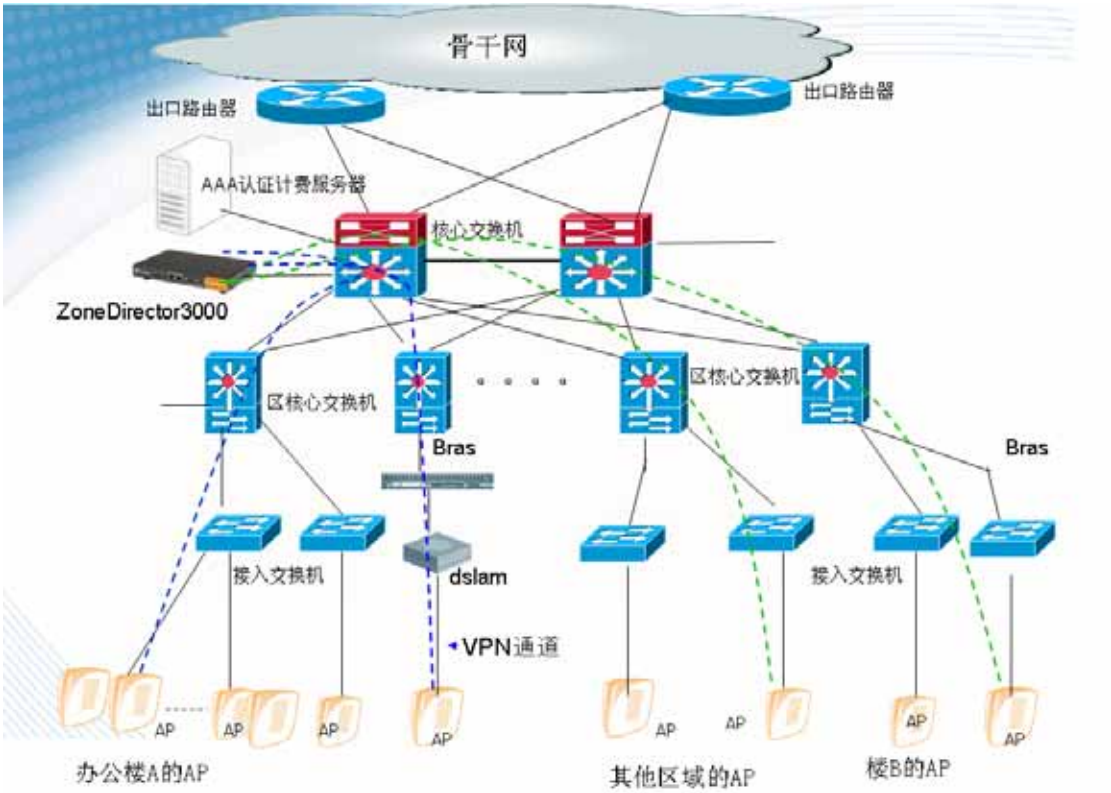


配置为 ZoneDirector1000+AP

4．1．2 中型无线局域网(50 到 250 个 AP)集中式组网

如果整个无线系统的 AP 数量比较多，且大部分也都集中在一定区域内通过以太网交换机相连，即使部分 AP 不是集中在特定区域内通过以太网交换机相连而是通过其他宽带连接。那么也可以采用单台 ZoneDirector3000 来组网。该 ZoneDirector3000 管理所有本地或远程的 AP。如下图。

配置为 ZoneDirector3000+AP。

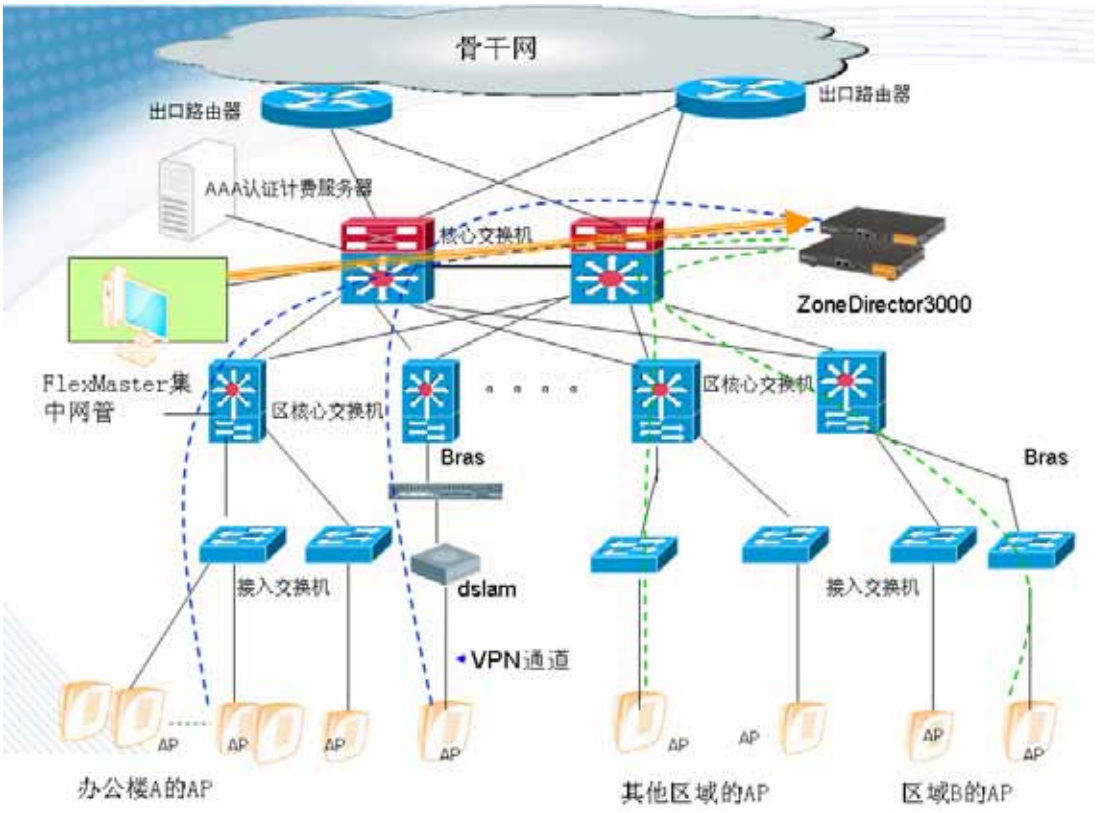


4．1．3 大型无线局域网(250 个 AP 以上)集中式组网

如果整个无线系统的 AP 数量比较多，而且大部分也都集中在一定区域内通过以太网交换机相连（即使部分 AP 不是集中在特定区域内通过以太网交换机相连而是通过其他宽带连接）。而用户还是决定采用集中式组网。那么可以采用多台 ZoneDirector3000 来组网。这些 ZoneDirector3000 管理所有本地或远程的 AP。一些要求较高的用户会采用双机或多机或 N+1 的方式加强网络冗余备份。在网络中心则设置 FlexMaster 网管系统管理所有 ZoneDirector3000 来设定所有无线局域网设置。

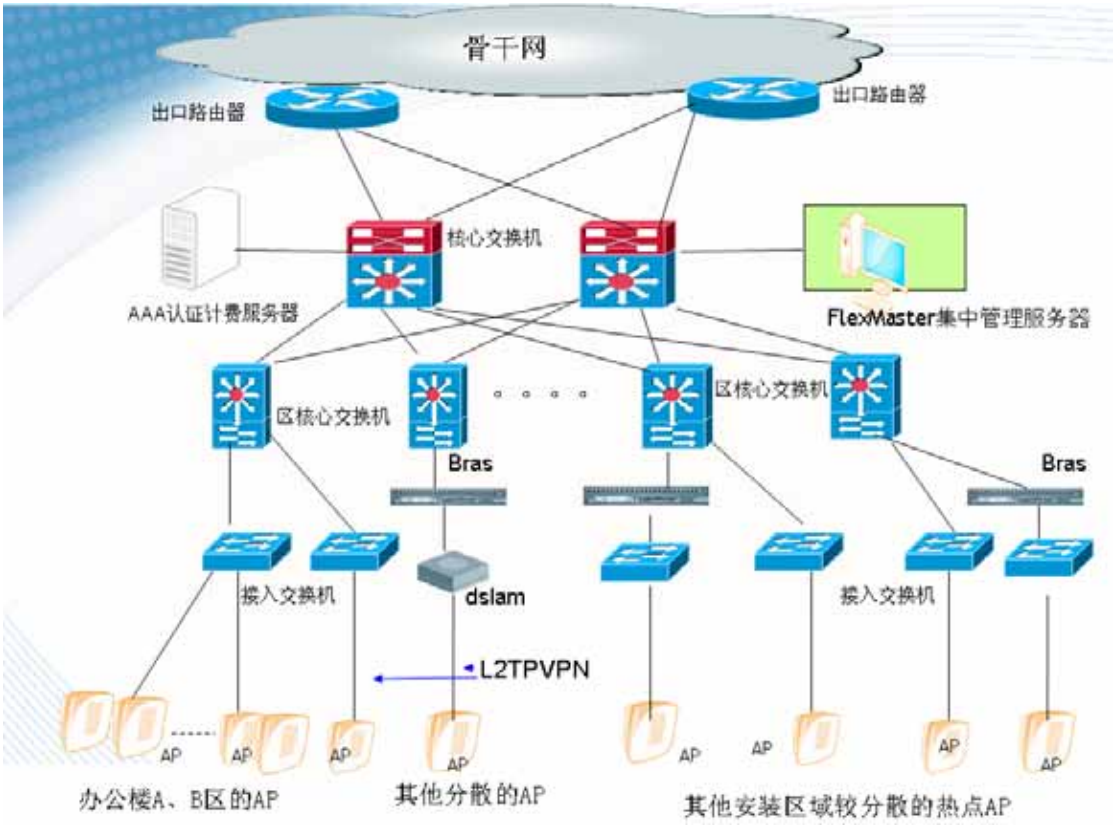
选用 ZoneDirector3000，一般是把 250 个 AP 汇聚到 ZoneDirector3000 上，而视乎 AP 实际数目和网络拓扑，多台 ZoneDirector3000 可分别设置在不同的区局配线间/机房。在网络中心内则一定用 FlexMaster 以管理其它 ZoneDirector3000。

配置为 FlexMaster＋ZoneDirector3000 或 ZoneDirector1000+AP。



4．1．4 大型无线局域网(1000 个 AP 以上)分布式组网

如果整个无线系统的 AP 数量比较多，而且大部分都分布比较分散，接入方式也多种多样(如运营商的热点网络)。那么可以采用 FlexMaster 集中管理系统来管理远端的 AP 进行组网，对所有的 AP 进行配置和管理，设定所有无线局域网设置。如下图。



配置为 FlexMaster+AP。

4．1．6 深圳 XXX 工厂无线局域网的组网设计

深圳 XXX 厂区内共有多幢不同的建筑物，我们会因应每幢建筑物的特点和需要，部部署适当的无线接入点，无线接入点通过有线连接，接入到厂区原有的内部网。所有无线接入点均由一台无线控制器统一集中管理，配置、维护和监控。无线接入点和无线控制器之间只要路由可达即可管理，不需要在同一个 VLAN 下。

总的无线系统拓扑图如下：

艾美特厂区无线系统网络拓扑图

4．2 多业务区分设计

使用 Ruckus 的企业级无线网络系统，可以灵活地配置分为不同的无线接入业务类型。因此，在设计上采用无线局域网多 SSID 技术，每一个 SSID 对应一个 VLAN 或业务。在这里，根据使用需求，我们建议在无线局域网内可以设置两个 SSID，对应两个 VLAN。一

个 SSID 提供给内部员工所用，而另一个 SSID 可给外来的客户使用。由于用户一般把 SSID 看成 VLAN，所以它们都会惯性地以 VLAN 概念来划分 SSID。其实在一个 AP 范围内，不管用户连接到那一个 SSID 它们实际上都是在同一个 802.11 广播域内，因为无线电波的传输是共享。一个最简单的例子就是 AP 把不同的 SSID 名字广播，所以当无线终端在这个 AP 覆盖范围内启动时，它就能同时看到多个 SSID。SSID 的最主要用途是可让无线终端以不同的安全认证和加密方式入网，并且连接到指定的 VLAN，通过核心路由器，还可以对特点的 VLAN 进行控制。

为什么要把不同的安全加密协议设置在不同的 SSID 呢？ 802.11 的标准内定义了不同加密情况时数据包的封装格式，所以在用户的无线接入使用不同的加密程式，例如：WEP,TKIP(WPA),802.11i(WPA2)等等，不同加密方式不能在同一个 SSID 内同时存在的。

用户可根据实际的情况和 802.11 发展来制定以怎样方式来实现无线加密。最常见的做法是使用多个 SSID，例如：一个定义为 OPEN/Static WEP 供客户用，另一个 SSID 则为 TKIP(WPA)专为内部员工使用。未来的发展趋势是新增设一个 802.11i SSID 让员工以过度的方式逐渐从转移到这个 SSID 上。不能一步转到 802.11i 的主因在于很多的无线终端现在尚未支持 802.11i，而是不可能把所有的终端一次更换成最新的软件程序。

在这里，我们设计两个 SSID，一个是 GUEST，对外的，采用 WPA-PSK 单密钥认证加密方式，这种好处是使用方便，维护量小，对于流动性大的宾客访问最好，每三个月修改一次密钥，几秒钟完成配置更改。并且，可以在核心路由器上将这个 SSID 对应的 VLAN 设为只允许上网，不能访问内网，这样安全性更高。另一个 SSID 定义为对内部员工开外，可考虑采用帐号和密码认证方式，802.1x 方式是最常用的，可将帐号密码设于无线控制器内，亦可与原系统外挂的 radius 服务器结合使用。

4．3 无线安全性设计

在 Ruckus 无线系统中，可以在多个层面对系统构筑安全防护，其安全性设计如下：

（1）**多 SSID**：可以根据需要，如用户的种类、应用的种类，在 Ruckus 无线系统中设置多个 SSID，不同的 SSID 采用不同的安全策略，这样可以对不同的用户及应用进行区分服务。另外 SSID 还可以选择隐藏的方式，该 SSID 不广播，用户无法看到，防止非法用户

的连接企图。SSID 还可以选择在某些 AP 上出现，某些 AP 上不出现，限制 SSID 出现的范围也是实现安全性的一种手段。

（2）**加密：**Ruckus 无线系统支持多种加密的方式，二层的加密支持静态 WEP、动态 WEP、TKIP、WPA、802.11i 多种加密方式，三层的加密支持 IPSec VPN 加密，这样使得加密的方式更加的灵活，可以根据实际需求进行选择。

（3）**用户认证提供三种方式：**

① WPA-PSK＋captive portal+VPN。

加密方式采用 WPA-PSK，不建议采用静态 WEP，因为有安全隐患。采用 captive portal+VPN 的认证方式，同时 VPN 还具有三层的加密功能，具有更高的安全性。认证服务器的选择比较灵活，可以使用 RADIUS, LDAP, Windows NT, ActiveDirectory, TACACS，甚至是 Ruckus 交换机内置的帐户数据库。

② WPA+802.11x 加密方式尽量采用 WPA，如果客户端不支持也可采用动态 WEP，认证方式采用 802.11x，认证服务器选择 RADIUS。

③ Dynamic PSK™

Dynamic PSK™是 Ruckus 专利的用户认证和加密技术。传统的无线加密密钥对所有的用户是相同的，相当脆弱；而且长度较短，容易被解码。Dynamic PSK™技术为每一个用户提供一个 64 字节的密钥，实现完整而且非常安全的认证加密手段。

（4）用户的 Role（角色）：每一类用户可以建立一个相关的 Role，每个 Role 有一个用户状态防火墙的设定和带宽控制的设定，这样我们就可以将设定的安全策略加载到每个用户身上。

（6）带宽控制：可以对每个用户设定其可以使用的带宽，一方面可以限制其对网络资源的占有，另一方面，当该客户端中了病毒以后，其病毒发作时不会占用网络全部的带宽。

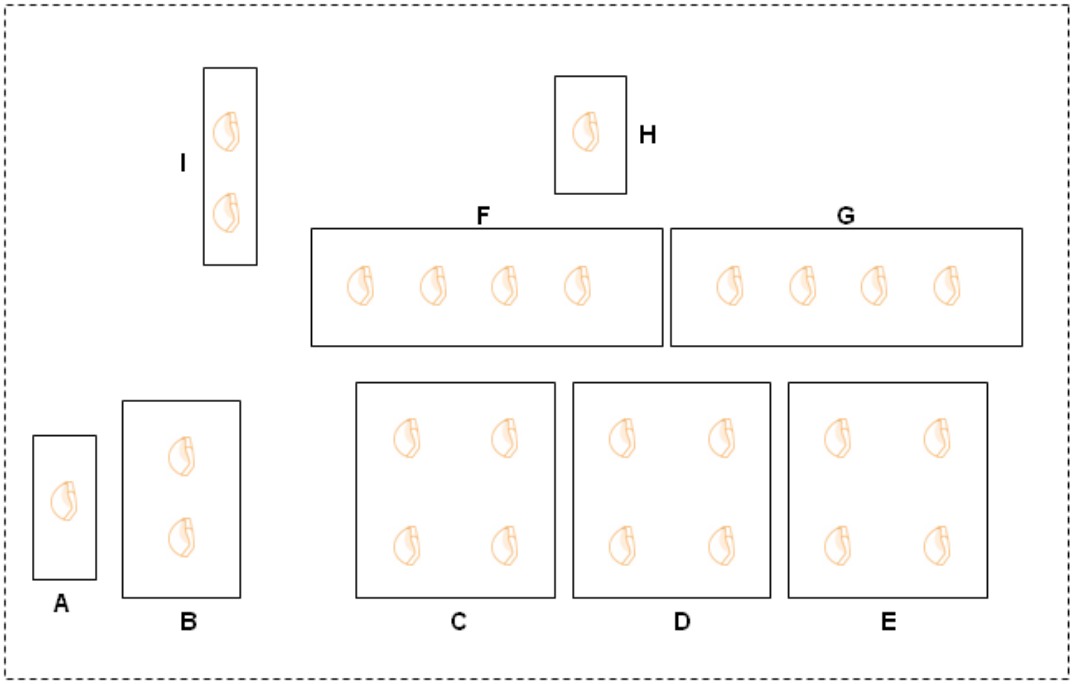
（7）认证系统支持： Ruckus 无线系统支持多种认证系统，诸如 Radius、微软的 AD（活动目录）和在 Ruckus 无线交换机内部的 Internal DB 等等。

五、 深圳 XXX 工厂无线局域网系统建议

5．1 无线覆盖建议

根据无线网络需求及厂区内实地的了解，并结合以往的工程经验，对无线网络覆盖做出以下规划：

艾美特厂区主要接入点分布图



上图是深圳 XXX 厂区内主要建筑物，以及因应建筑物特点的无线接入点分布。

5．2 无线组网实现

以下是各幢建筑物的具体 AP 分布和数量设计：

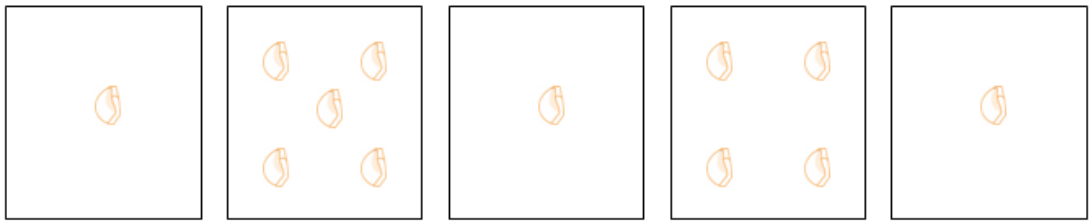
A 栋公寓长 32 米、宽 8 米，因为我们设计每层楼在中心位置部署一个 AP 即可覆盖，整栋大楼共需 5 个 AP

B 栋办公大楼是重点覆盖区域，长为 42，宽 16 米，因此每层采用 2 个 AP 覆盖，总需要 10 个 AP，在该大楼中心机房，放置一台无线控制器作为统一管理厂区内所有 AP 的平台，其余大楼不需要放置控制器。

C栋大楼的无线接入点分布图 (共需要11个AP)

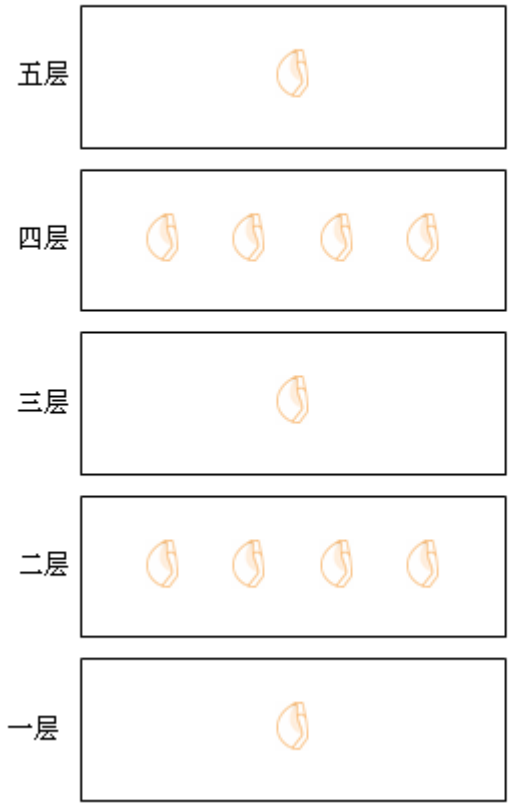
D栋大楼的无线接入点分布图 (共需要11个AP)

E栋大楼的无线接入点分布图 (共需要12个AP)



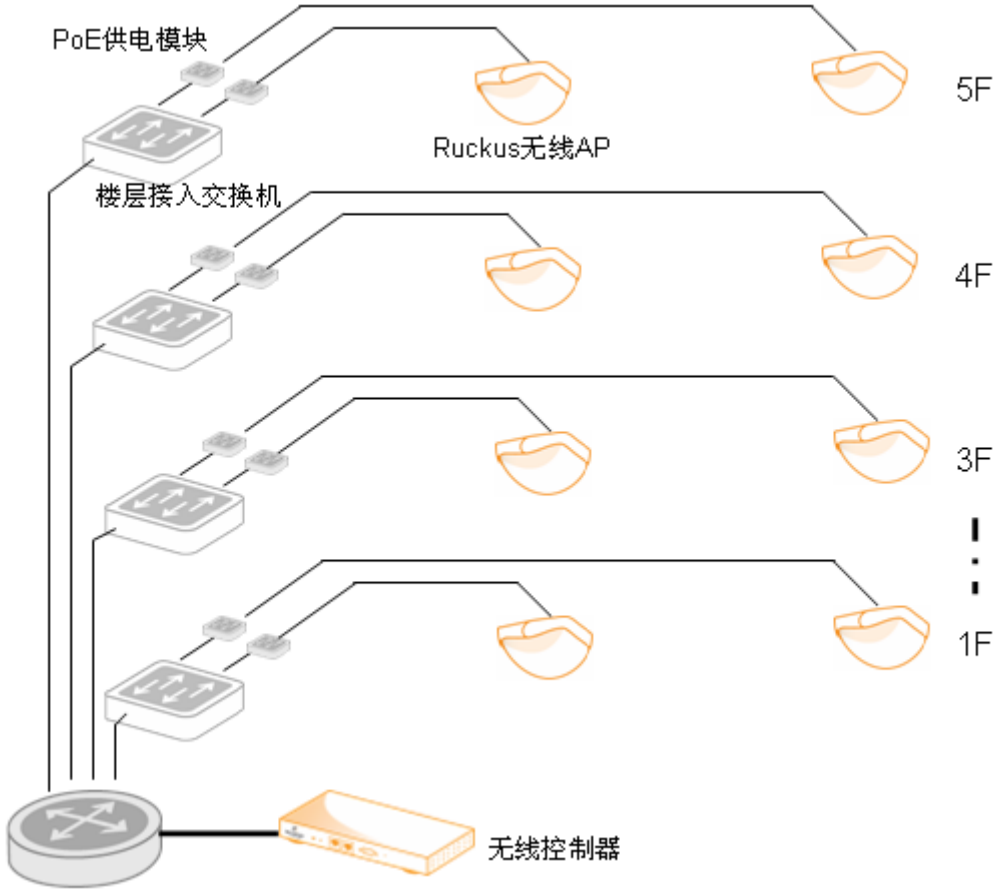
以上三幢建筑均有相似的结构，考虑到建筑物内面积较大，每层约 3000 多平方米，比较空旷，因此建议采用楼层间非对称地部署 AP。例如我们在二层和四层部署较多的 AP，AP 信号可以透射覆盖相邻的楼层，相邻楼层只需增加一个 AP 补充即可。在 E 栋大楼的第二层是办公区域，是重点覆盖区，因此在中央位置多加一个 AP 增强信号和提高冗余性。三栋加起来，共需要 34 个 AP

F栋大楼的无线接入点分布图 (共需要11个AP)



F 和 G 两栋大楼具有类似的结构，长 96 米，宽 30 米，约 3000 平方米，采用非对称方式部署，每幢需要 11 个 AP，总共需要 22 个 AP。

5．3 方案说明



这是一个 54M 的无线覆盖方案，提供 54M 连接速率，采用目前最先进“智能瘦 AP 架构”，第三代无线局域网技术，集中管理，是性价比最优的无线方案；每个 AP 采用 PoE 网线供电方式，无需在 AP 部署位置加装电源，将网线与 PoE 交换机连接供电即可，并通过 PoE 交换机接入原有线网络；

该方案的优势：

1、智能天线阵列，12 根水平和垂直极化高增益天线，具有最强的信号覆盖能力，保障信号品质，比普通 AP 大一倍的覆盖面积；

2、提供智能空中接力 MESH 技术，节省布线，方便扩展覆盖范围；

3、优秀的流媒体传输技术，支持组播视频，支持视频优先专利技术，是目前全球无线视频传输质量是最出色的；

4、方案支持最先进的主动式网管标准 TR-069 协议，可以轻松实现远程集中统一网管；

5、配置和维护成本低，安装和操作方便，具备中英文管理界面；

6、是全球唯一具有抗干扰能力的无线解决方案。

5．4 无线网的安全系统实现

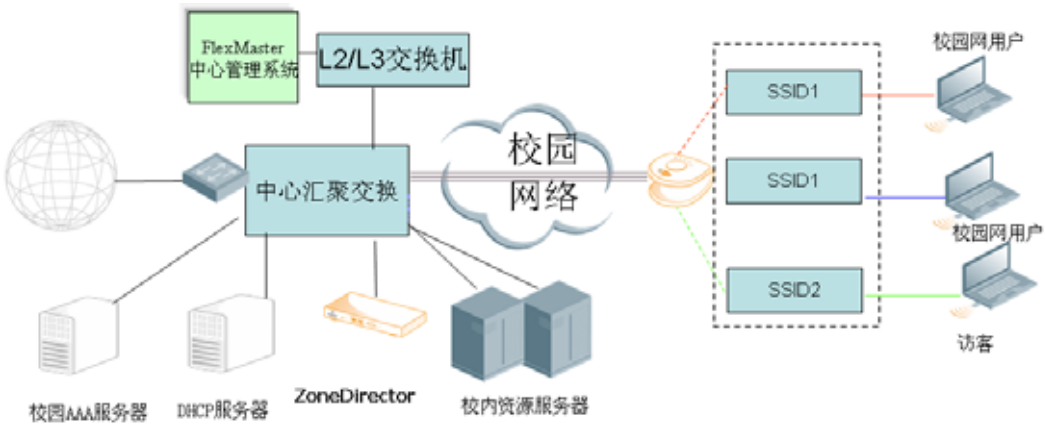
Ruckus 无线网的安全系统实现如下安全功能：

- 接入认证控制： 验证用户， 授权他们接入特定的资源， 同时拒绝为未经授权的用户提供接入。
- 确保链路的保密与数据的完整： 防止未经授权的用户读取或更动在网络上传输的数据。
- 侦测非法接入：防止非法 AP 接入学校的无线网络中。
- 监测和阻断无线攻击： 防止攻击占用某个接入点的所有可用带宽， 导致其他用户的正当接入。
- 根据每个 SSID 设定无线用户的上行、下行带宽：防止 P2P 应用大量占用带宽。

二层用户隔离选择：保证用户数据的安全性。

六、 Ruckus 智能无线网络方案特点

6．1 组网方便



无需重新布线或划分 VLAN，AP 就近接入现有网。在网络的中心或集中交换机处部署无线控制器 ZoneDirector，对 AP 进行同一的 AP、用户接入、安全和无线 RF 管理。

AP 接入网络后，如果需要也可以在网管中心部署（适合于具有多个区域的部署）FlexMaster 集中管理系统。这样各区域采用 ZoneDirector 进行本地无线网络的管理（包括 AP 配置和状态、软件管理、用户认证、安全和无线 RF 管理等），而中心 FlexMaster 对 ZoneDirector 进行统一管理和监控。

ZoneDirector 支持多个 AAA 认证服务器和本地数据库用户服务器。支持 WEBPortal 认证、802.1x 认证等。如果现在采用的是 802.1x 客户端认证的方式，那么现有的用户可以使用同一客户端进行认证接入。

6．2 智能天线技术，更少的 AP 数量，更大更有效的覆盖

AP 的天线是由多根水平和垂直极化天线组成的智能天线矩阵系统，可以提供 4095 种

天线模式，系统控制软件利用构建在 802.1MAC 层协议中的反馈机制不停的为每一个接受设备调整天线模式。通过为每一个接受设备选择一个优化的天线阵列，BeamFlex 能够扩展无线覆盖范围和更高的通讯速度。

在具有多个房间和隔断（包括承重和非承重墙）的二层 400 多平米的居室里，能够提供 15-20M 的稳定的数据流。

这一技术将大大减少用户在热点地区 AP 的部署数量，节省用户的投资。

6．3 有效的支持视频和音频流，智能的 QoS 技术

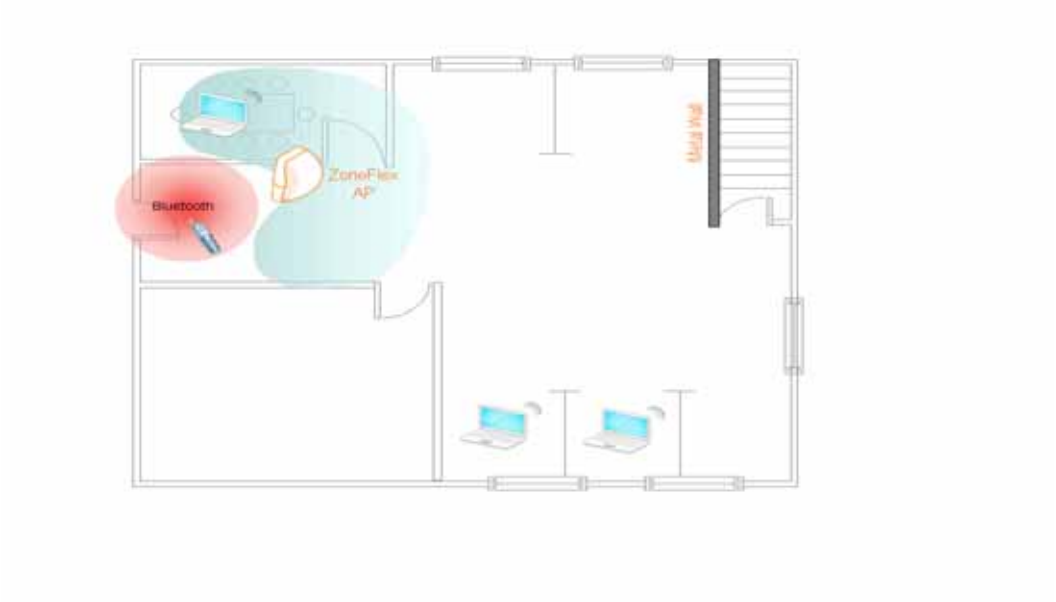
具有专利的 SmartCast 技术包括组播流量处理技术、智能 QoS 和基于“识别应用”的流量自动分类能力。SmartCast 的智能模糊控制技术能够从所有流量中自动的识别和区分流量类型，自动的为不同类型流量标记服务类型。

一个 AP 可以支持 3-4 个 并发 MPEG-2 或 1—2 个 10M HD 视频流（距离 20 米，包括背景流量）

6．4 抗干扰能力强

智能天线系统通过检测射频和多径问题以及邻居网络噪声带来的干扰，能够实时重新自我配置和调整，使得 AP 在一个不断变化的环境中从多种不同质量的信号传输路径中立即选择一个最优的传输路径。

在办公楼中，由于 AP 众多，在每个频道都有多个 AP，因此无法通过跳频来解决干扰问题，而又不想因为缩小功率而减少覆盖范围，Ruckus AP 可以通过改变传输路径来避开干扰，保证数据的可靠传输。如下图，AP 通过改变传输路径，避开手机的干扰。



AP 通过改变传输路径，将信号有效覆盖到承重墙后边的区域。

6．5 用户密度高

单个 AP 可以同时支持 50（2942）或 100（7942）个以上用户接入，是目前可支持用户最多的 AP。单纯的覆盖范围广在用户接入密度高的场合，实际上是个缺点。因为用户会发现他看到 AP 的信号良好，但却连接不上。会造成大量的投诉和降低用户的体验。

6．6 安装部署简单方便

新 AP 可以自动发现 AC 或集中管理系统，自动更新软件版本和初始化配置。安装人员无需查看需要安装或更换的 AP 的版本、配置，无需现场调试和测试，插上电连上线， GO!。一个网络里版本的统一非常重要，版本不统一，设备工作状态就不一样，会对维护和管理造成相当的困扰。

BeamFlex 技术对 AP 的安装位置没有特殊的要求，可以安装在方便安装（如具有以太网接口的几乎任何地方）。这样不仅方便了安装，还节省了安装成本。

另外，内置的 MESH 技术可以扩展覆盖不方便布线的区域。

6．7 可预测的性能

无线和有线的最大不同，在于其不确定性很大，而这点也是无线网络维护和运营的难点。BeamFlex 智能天线技术和 SmartCast 技术使预测 AP 的性能成为可能。大大降低了维护和运营的成本，增加用户的体验。

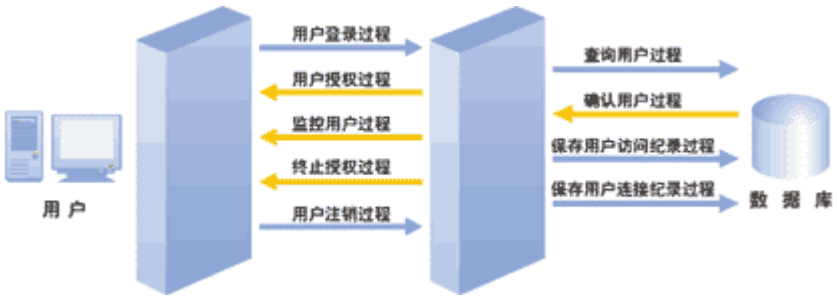
6．8 实时监视无线 RF 环境

可以实时看到 AP 所处的无线频谱分布。非常有助于诊断解决一些间断出现的性能不稳定问题。

目前全球有超过 120 个运营商部署了我们的解决方案。香港 PCCW 的多业务（数据、语音和视频）、全业务无线热点网络目前的 AP 数量已经超过 3500 个。

七、 网络认证系统原理

7、1 服务流程



1) 用户登录过程

用户登录，输入账号和密码，账号和密码加密传送到计费服务器。

2) 查询用户过程

向后台数据库查询用户资料。

3) 确认用户过程

计费服务器向后台查询用户的资料和授权设置，确认用户的身份。如果身份合法，允许用户使用；否则登录失败，无法使用服务。

4) 用户授权过程

根据用户的授权设置，对使用的功能进行授权，包括时间授权、功能授权、带宽授权、访问限制授权、过滤授权和信用授权，按照该用户的收费费率进行计费。

5) 监控用户过程

实时监控用户的使用情况，并根据每个用户的授权进行判断是否接受或拒绝用户所要求的服务，并将用户使用情况送到后台数据库进行纪录。

6) 保存用户访问纪录过程

将用户的使用过程中产生的纪录文件送到后台数据库保存。

7） 终止授权过程

用户的使用权限超过预先设定的阀值（如累计时间、流量、信用等参数）后，将给用户警告，并且终止对用户授权，强制结束服务。

8） 用户注销过程

用户要去退出服务，注销用户的授权。

9) 保存用户连接纪录过程

将用户连接纪录包括登录时间、结束时间、流量、服务内容纪录和产生费用等资料纪录在数据库内。

10) 用户登录过程

用户登录，输入账号和密码，账号和密码加密传送到 2033 BMG 计费服务器。

11) 查询用户过程

向后台数据库查询用户资料。

12) 确认用户过程

计费服务器向后台查询用户的资料和授权设置，确认用户的身份。如果身份合法，允许用户使用；否则登录失败，无法使用服务。

13) 用户授权过程

根据用户的授权设置，对使用的功能进行授权，包括时间授权、功能授权、带宽授权、访问限制授权、过滤授权和信用授权，按照该用户的收费费率进行计费。

14) 监控用户过程

实时监控用户的使用情况，并根据每个用户的授权进行判断是否接受或拒绝用户所要求的服务，并将用户使用情况送到后台数据库进行纪录。

15) 保存用户访问纪录过程

将用户的使用过程中产生的纪录文件送到后台数据库保存。

16) 终止授权过程

用户的使用权限超过预先设定的阀值（如累计时间、流量、信用等参数）后，将给用户警告，并且终止对用户授权，强制结束服务。

17) 用户注销过程

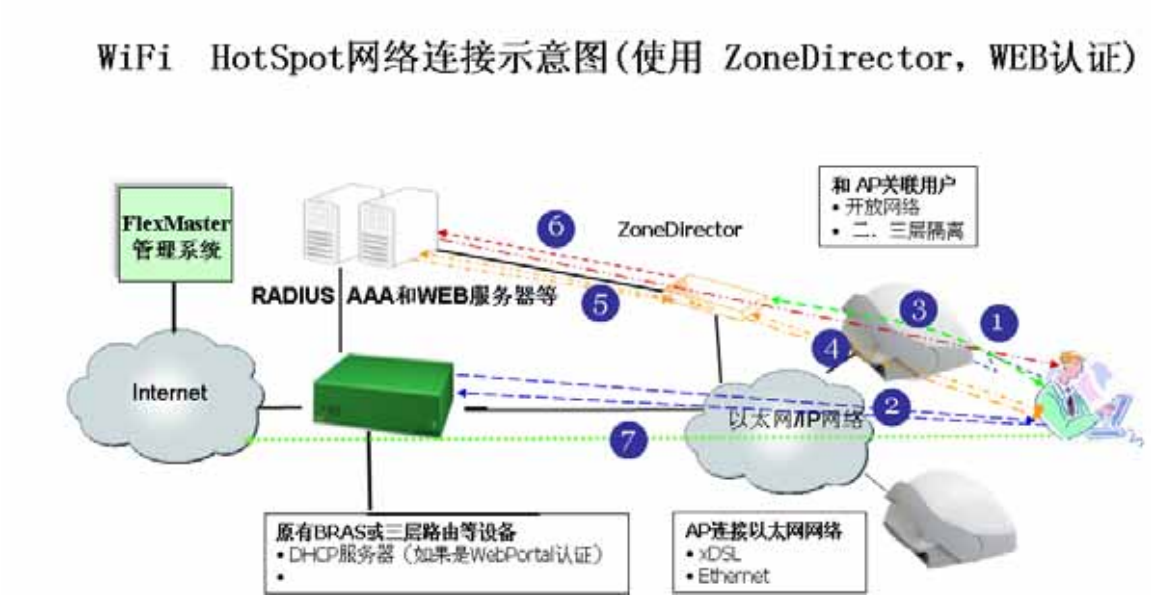
用户要去退出服务，注销用户的授权。

保存用户连接纪录过程

将用户连接纪录包括登录时间、结束时间、流量、服务内容纪录和产生费用等资料纪录在数据库内。

7、2 计费系统集中工作方式

7．2．1　Portal 认证



Ruckus ZoneFlex 2925/2942/7942 AP 通过以太网或 IP 线路连接到网络，通过 ZoneDirector 进行 SSID、无线信道、发射功率、Rouge AP 检测和无线加密、认证等管理。

根据要求，ZoneDirector 将创建一个公开的、没有加密的 AP 热点 SSID，用户可以通过该 SSID 接入到网络当中。无论用户想访问的网页是什么，ZoneDirector 弹出 WEB 认证节目（包括欢迎、认证连接等），通过认证后用户就可以访问 Internet 网络了（也可以重定向到缺省的网页）。

可以根据热区内 AP 数量的多少，由一个或多个 ZoneDirector 可以管理一个热区内的所有 AP。

如果需要，未来可以在中心部署 FlexMaster 管理所有的 ZoneDirector，从而管理网络中的所有 AP。

AP 可以通过以太网或 DSL 链路接入网络。ZoneDirector 没有 DHCP 服务器功能，所以

需要外置的 DHCP 服务器或使用 BRAS 提供 DHCP 服务器为客户端分配 IP 地址的功能。

如上图所示，用户接入的流程如下：

(1) 用户开机后，检测到 SSID 有效；

(2) 客户端发起 DHCP 请求，经认证设备转发到 DHCPServer。DHCPServer 为用户分配 IP 地址；

(3) 用户打开浏览器，HTTP 请求被 ZoneDirector 捕获，并重定向到登录界面；

(4) 用户输入用户名和密码，并传送到 ZoneDirector；

(5) ZoneDirector 将用户名和密码发送到 AAA 服务器进行认证；

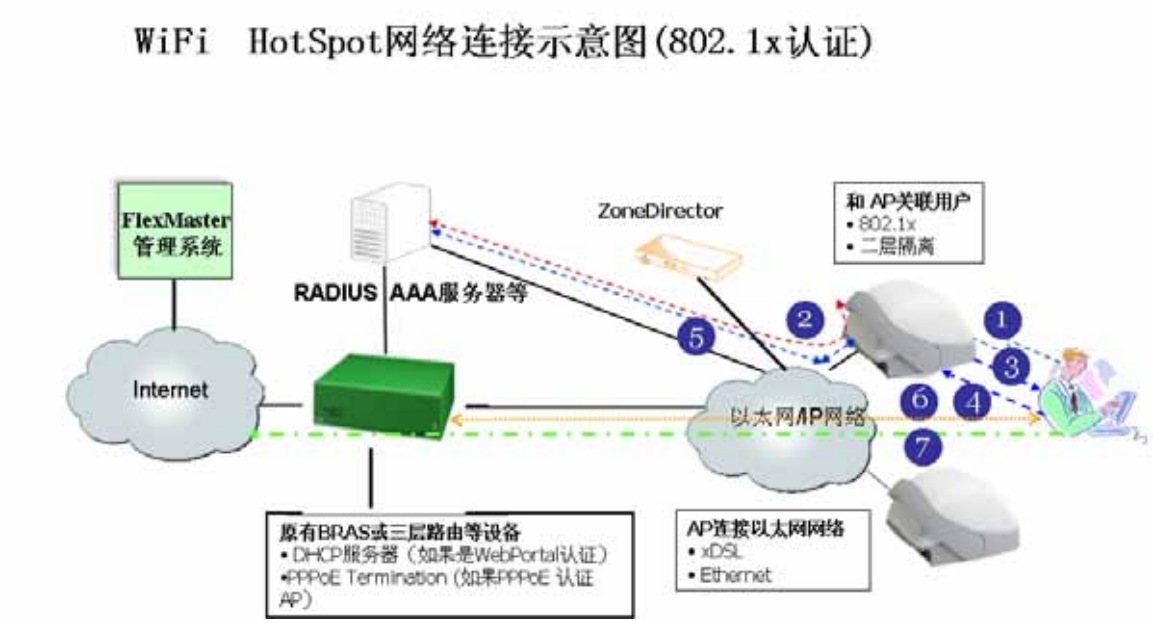
(6) 认证通过后，ZoneDirector 将 Web 页面重定向到 ZoneDirector 指定的 WEB 服务器页面；同时出现计时窗口；

(7)用户可以上网，AAA 服务器计费开始；

Web＋DHCP 实现简单，无需客户端和相关配置，扩展性也好。

无线网络的认证方式我们建议使用如下方式：在无线控制器中设定使用 Web-Portal 方式认证。当用户接入无线网络后，需要使用浏览器访问校园网或 Internet，会弹出认证界面，用户输入用户名和密码后送到相关服务器进行验证，如果认证通过后用户就能够访问校园网和 Internet，如果访问 Internet 就会产生计费，同时计帐到该用户帐号上。

7．2．2　802.1x 认证



Ruckus ZoneFlex 2925/2942/7942 AP 通过以太网线路连接到网络，通过 FlexMaster 或 ZoneDirector 进行 SSID、无线信道、发射功率、无线加密等管理。DHCP 服务器可以使用原有的 BRAS 或新的服务器。这里的 PPPoE 可用于当 AP 通过以太网连接到网络时，AP 获得 IP 地址(AP 可以通过 DHCP、静态设置或 PPPoE 等获得 IP 地址)从而连接 FlexMaster 管理系统进行管理。

对于一个地点具有多个 AP 的应用场合（如学校），也可以采用 ZoneDiretor 对其范围内的 AP 进行管理，同时 FlexMaster 远程对 ZoneDirector 进行管理，从而对 AP 进行管理。

AP 或 BRAS 等都可以通过任何 IP 网络与 AAA 系统进行通信。

根据 802.1x 的要求，FlexMaster 或 ZoneDirector 将创建一个加密的支持 802.1xAP 热点 SSID。

如上图所示，用户接入的流程如下：

（1）　用户开机后，检测到 SSID 有效，通过 802．1x 客户端软件发起请求；

（2）　AP 检测到该请求后，向 AAA 发出请求，AAA 服务器发出响应；

（3）　用户端弹出对话框，要求输入合法的身份标识，如用户名及其密码。

（4）　用户端将身份标识传送到 AP；

（5）　AP 将相应信息发送到 AAA 进行认证。认证通过

（6） 如果认证通过，则 AP 到 DHCP 服务器的端口打开。客户端软件发起 DHCP 请求，经认证设备转发到 DHCPServer。DHCPServer 为用户分配 IP 地址。

（7） 用户可以上网了。认证服务器开始对用户计费。

（8） AP 通过定期的检测保证链路的激活。如果用户离开或异常死机，则 AP 在发起多次检测后，自动认为用户已经下线，于是向认证服务器发送终止计费的信息。

IEEE 802.1x 具有以下主要优点：

（1）实现简单。IEEE 802.1x 协议为二层协议，不需要到达三层，对设备的整体性能要求不高，可以有效降低建网成本。

（2） 认证和业务数据分离。IEEE 802.1x 的认证体系结构中采用了“受控端口”和“非受控端口”的逻辑功能，从而可以实现业务与认证的分离。用户通过认证后，业务流和认证流实现分离，对后续的数据包处理没有特殊要求，业务可以很灵活，尤其在开展宽带组播等方面的业务有很大的优势，所有业务都不受认证方式限制。

八、售后技术服务

根据实际需要，我公司可向买方提供远程通信维护方式（采用电话指导或远程维护终端）和现场故障抢修两种技术支持方式。

1) 我公司每天设有 24 小时值班的（RSC）支援中心，买方如有任何问题，可随时进行咨询并得到答复；我公司根据故障报告内容并考虑用户观点进行电话直到或远程维护

2) 我公司设有用户服务数据库，用户可进行有关问题的查询，并将有关问题通报我公司，以便提高服务请求的追踪和反应工作

3) 我公司设有技术服务中心及备件库，配备足够数量的经验丰富的工程师及备件

4) 当我公司与买方协商后，如果以下各方面已提供了措施，则用户服务请求被认为已经解决：

   A. 故障部分的更新或修改可以解决问题或修正错误

   B. 在故障部分做特殊处理，再在以后的定期或专门软件更新中来改正

   C. 申告的故障或问题没有严重到需要立刻修复的程度，但日后的定期或专门软件更新中可以解决（若用户要求，我公司可以提供预先解决办法，但费用不包括在本协议所规定的费用中，而应按我公司当时的价格另行支付）

   D. 提供定期或专门更新软件包即可排除故障或解决问题

   E. 系统运作已达到设计要求，用户的要求可在将来版本满足

   F. 身高的故障或问题不是系统本身的问题，如有可能，指出问题或故障的来源

   G. 申告的问题无法得到解决，并作出解释（不影响系统的正常运行）

5) 如果我公司地区用户服务中心无法解决用户服务请求，将有我公司进行支援服务，如果需要派人到现场解决，考虑到交通和出入境或问题本身的复杂程度等客观因素，支援服务时间和期限后双方协商确定，买方对此应全力配合

6) 维修方式，出现故障板件时，买方可在我公司技术服务中心更换好的板件。保修期内维修、更换等一切费用有我公司负责；在保修期满后，根据双方签定的支持服务协议，我公司对板件维修收取费用，当损坏板件不可能修复时，我公司按备件价格优惠收费

7) 在现场故障抢修过程中，我公司如需使用买方现场器材时，买方应配合提供我公司将对设备的运行、维护情况进行跟踪记录并存入重点用户档案。在系统设备运行期间，我公司技术服务中心工程师将定期走访或电话询问用户，以了解设备运行情况。并向用户提供定期报告，总结报告期内发生的服务请求解决活动、设备运行情况和必要的技术建议等。根据具体情况，必要时我公司技术服务中心工程师到现场指导维护工作

8) 我公司的现场支持服务根据我公司的四级故障级别划分来确定响应时间：

故障级别	现场响应时间（非偏远地区）
一级故障	乘坐最快的交通工具
二级故障	24 小时内
三级故障	一周之内
四级故障	不到现场，电话指导服务

我公司设备的四级故障划分界定如下，详细的故障分类见下面表格。

一级故障：设备在任何环境中运行出席那的紧急系统中断或服务中断，导致设备的基本功能不能实现或全面退化

二级故障：指系统或服务中出现的较严重的性能退化

三级故障：指系统或服务中出现的较一般的性能退化

四级故障：不会对系统或服务功能带来直接影响的故障

故障等级划分

故障现象	一级故障	二级故障	三级故障	四级故障
不能处理任何接入	★			
风扇故障	导热过热而使设备损坏		★	
用户验证无法通过	★			
记账包丢失		10%		
路由失败		★		
被动掉线频繁		★		
死机	完全	经常	偶尔	
局部功能不能实现			★	
主板的硬件或软件故障		部分用户不能	用户使用不正常	不影响用户使用

维修保证

（1） 保修期限

a. 设备和硬件质量保修期为设备终验之日起十二个月

b. 软件的质量保证期为终验通过之日起十二个月

c. 保修期外如需维修，需收取一定的费用

（2） 服务范围

a. 技术支持服务

b. 电话咨询服务

c. 硬件支持服务

d. 投诉受理服务

e. 培训服务

f. 信息资料服务

g. 区域维护服务

（3） 产品质量保证

a. 我公司保证网上运行的设备符合买方的技术规范要求

b. 我公司保证在网上运行设备软件的一致性

c. 我公司承诺对软件的完善、升级负责

d. 保修期内产品质量保证

在保修期内：买方应派受过培训的合格热源按照维护手册对设备维护操作。由于我公司提供的设备或软件有缺陷，我公司负责更换有缺陷的设备和软件。由于火灾，水灾，磁电串入，强雷击，强电等不可抗拒原因造成产品设备损坏，我公司负责维护，费用有买方承担。

e. 保修期已满后质量产品保证

在保修期满后，我公司保证继续为设备提供修理和维护，对软件的完善，升级负责。服务方式，内容及费用可由双方签定支持服务协议来保证。

九、设备配置清单

根据需求，我们设计两个方案，方案一是覆盖重点区域，方案二是全覆盖。

以下汇总所有 AP 的分布：

方案一：部分覆盖

建筑物	一层	二层	三层	四层	五层	总数量
A 栋公寓	1	1	1	1	1	5
B 栋办公大楼	2	2	2	2	2	10
E 栋车间		5				5
H 栋	1					1
F 栋食堂	2					2
三个门卫	3					3
					总数量：	26

方案一的产品清单：

设备名称	组件编号	产品描述	数量	备注
无线接入点	Ruckus ZoneFlex 2942	符合标准 802.11g 54M 无线接入点，内置 12 根智能天线阵列，两个百兆端口，支持 PoE 供电	26	
定向天线	Directional Antenna	高增益定向天线，用于覆盖门卫区域，含馈线、支架等附件	3	
无线控制器	ZoneDirector 1050	ZoneDirector 1000 系列无线控制器，最大 AP 管理容量为 50 个，双千兆端口	1	
POE 供电模块	PoE Module	双端口支持 IEEE 802.3af PoE 模块，连接 AP，为 AP 供电	26	
布线	Cabling	连接 AP 与接入层交换机之间的布线	26	

方案二：全覆盖

建筑物	一层	二层	三层	四层	五层	总数量
A 栋公寓	1	1	1	1	1	5
B 栋办公大楼	2	2	2	2	2	10
C 栋车间	1	4	1	4	1	11
D 栋车间	1	4	1	4	1	11
E 栋车间	1	5	1	4	1	12
F 栋仓库	1	4	1	4	1	11
G 栋仓库	1	4	1	4	1	11
H 栋	1					1
F 栋食堂	2					2
三个门卫	3					3
					总数量：	77

方案二的产品清单：

设备名称	组件编号	产品描述	数量	备注
无线接入点	Ruckus ZoneFlex 2942	符合标准 802.11g 54M 无线接入点，内置 12 根智能天线阵列，两个百兆端口，支持 PoE 供电	77	
定向天线	Directional Antenna	高增益定向天线，用于覆盖门卫区域，含馈线、支架等附件	3	
无线控制器	ZoneDirector 3100	ZoneDirector 3000 系列无线控制器，最大 AP 管理容量为 100 个，双千兆端口	1	
POE 供电模块	PoE Module	双端口支持 IEEE 802.3af PoE 模块，连接 AP，为 AP 供电	77	
布线	Cabling	连接 AP 与接入层交换机之间的布线	77	

附件一、Ruckus 无线产品简介

无线控制器 - ZoneDirector 3000

Ruckus Wireless ZoneDirector 3000 是首个企业级智能无线局域网系统，它在一个很低的总体拥有成本上，提供了一个安全、可靠，同时又易于扩展的无线局域网解决方案。

Ruckus ZoneDirector 3000 的设计理念力求简洁而易用，通过一个中央点，其最多可以管理 250 台 ZoneFlex 802.11g 以及 80211n 智能无线 AP。

完全不像传统的无线局域网那么昂贵、复杂、难以部署，对任何一个需要高性能无线局域网而又期望其易于实施和管理的企业来说，选用 ZoneDirector 3000 都是再合适不过的了。

ZoneDirector 3000 集成了很多高级的功能，诸如智能天线操纵，智能无线网状结构，以及动态无线安全等，这些都是你在其他的 WLAN 系统中见不到的。

Ruckus ZoneDirector 3000 可以由非无线网络专业人员进行部署和操作，安装非常快速简便。即使是对那些即缺乏 IT 专业人员又预算有限的机构，安装这么一个可靠而安全的多媒体无线局域网，也只不过是几分钟的事情。

Ruckus ZoneDirector 可非常容易的与现有网络、安全和认证系统进行集成；通过网页向导，简单的点击即可很容易的完成配置工作，Ruckus ZoneFlex AP 会自动发现 ZoneDirector，并由 ZoneDirector 对其进行配置。

冗余和安全，Ruckus ZoneDirector 可在一个单一，易于使用和负担得起的无线局域网（WLAN）系统中，提供遍及整个 WLAN 范围的网络、 安全、射频和位置管理。

优势

无与伦比的可伸缩性

最高可支持 250 台 AP，ZoneDirector 3000 可以很容易的为最大的校园部署服务。

Ruckus SmartMeshTM 降低成本以及部署复杂度

集成 SmartMesh 技术，使得部署自动化，无需再为每一台智能 Wi-Fi AP 连接网线电缆。

易于使用，易于管理

集中管理，快速设置，对 IT 管理要求很低，自动、实时地对整个无线局域网（WLAN）优化

简化 IT 管理，部署可以 5 分钟之内完成

基于网页的配置向导能使任何计算机用户在几分钟内配置完毕整个无线局域网（WLAN）。Ruckus ZoneFlex AP 会自动发现 Zone Director。

富有弹性的部署选项

ZoneDirector 可与现有网络和安全架构交互，并为所有 AP 提供动态射频管理，而无需再考虑 AP 定位问题。

监控和故障诊断简单易行

可定制的监控界面，提供了全面的网络简洁视图，并可用于深入诊断各种无线故障。

自动用户安全

无需再对不同 PC 客户端使用唯一的加密密钥进行配置和更新。

完全集成

集网络管理，动态射频管理，位置管理以及 AP 控制于一身，是一个成本极低的解决方案。

先进的无线局域网特性和功能

基于角色的用户策略，内部认证数据库，AP 盗用监测以及每

个 AP 用户入口监测。

易于部署

Ruckus ZoneDirector 能够和现有的交换机、防火墙、认证服务器以及其他网络架构无缝集成。Ruckus ZoneFlex AP(无论是有线 AP 还是使用了 SmartMesh 技术的网状 AP)会自动发现 Ruckus ZoneDirector，并进行自配置，配置完毕后即可对其进行管理。在允许接入前，ZoneDirector 将对所有想接入 WLAN 的用户进行认证和授权。集成了完善射频管理的 ZoneFlex AP 会将射频信号聚焦于客户端的方向，在减少干扰的同时，自动进行性能

最大化和覆盖范围的最大化，并尽量减少所需的 AP 数量。

易于管理

在完成基本配置，开始运行之后，ZoneDirector 将自动管理 ZoneFlex AP 网络——对发射功率的自动调整，以及必要时对射频频道进行指定，以防止相邻 AP 之间的干扰，并在 AP 失效时启用冗余 AP 覆盖。配置的更改可以非常容易地同时应用到多个 AP 或整个网络系统上。可定制的监控界面可实时显示用户接入信息、网络信息和事件情况，同时一个实时地图将显示无线 AP 的位置，以及无线信号的覆盖范围、Ruckus SmartMesh 的拓扑结构等。

易于保密

ZoneDirector 3000 提供了创新的技术，简化和自动化了 Wi-Fi 的安全防护。除了支持企业级的 802.1x 以外，ZoneDirector 3000 还支持一种动态预共享密钥（PSK，Pre-Shared Key）的专利技术，可以简化无线局域网的安全防护工作。

初次使用的用户只需简单的将他们的电脑接入局域网，然后指定一个 URL 地址，即可进入一个一次性认证的捕获网页门户。一旦认证完毕，ZoneDirector 就会自动使用预先指定的 SSID，以及一个动态生成的加密密钥，对用户的系统进行配置。这个密钥会在超出有效期后自动移除，或者是在用户（用户设备）失去信任后而被人工移除。

Ruckus SmartMesh 提高灵活性，降低成本

SmartMesh 能够进行自我管理以及无线网的自我修复。SmartMesh 无需再为每一台 Smart Wi-Fi AP 连接网络线缆，因此系统管理员只要随便找个电源插座，将 ZoneFlex AP 插上去就可以走开了。所有的配置与管理都会通过 ZoneDirector 智能无线局域网平台进行。通过专利的 Ruckus 智能 Wi-Fi 技术，拓展覆盖范围以及动态信号控制，再通过 SmartMesh 技术最小化内部跃点数目（跃点越多，性能下降越多），此消彼长之下，再根据环境的变化自适应调节不同节点之间的 Wi-Fi 连接，从而进一步缩减了所需部署的 AP 数量。

BeamFlex 消除干扰，最大化性能，拓展到达区域

Ruckus BeamFlexTM, 一种专利 Wi-Fi 天线控制技术，能够根据多媒体程序的需求进行自动传输，以确保预期的性能，并拓展覆盖范围，消除无线盲区。

通过 ZoneDirector,BeamFlex 的应用价值从单一的 AP 拓展到了整个系统的 WLAN 和智能无线网结构之上。

ZoneDirector 自动控制所有的 ZoneFlex 智能无线 AP 的信道指定以及发射传输的功率水平。

通过 BeamFlex,ZoneFlex 系统可以持续的为每一个客户端的数据包在不同 AP 之间选择最佳的传输路径——在自动消除干扰的同时，还能确保最高的服务质量。

特点

集中配置 Ruckus ZoneFlex AP 的数量最高可达 250 台

集中软件升级

SmartMesh 控制与监控

实时客户端加入许可控制

可被支持 UPnP 的 PC 非常容易的检测到

易于使用的设置向导

可定制监控界面

动态射频信道以及发射功率管理

内置捕获门户（captive portal）

支持 Active Directory 以及 RADIUS

本地认证数据库

支持 Guest 帐户和 Guest 组使用

动态 PSK ，无需专业 IT 人员

AP 盗用监测以及图形化地图视图

事件管理

性能监控与统计

N+1 冗余备份

通过 FlexMaster 对多个位置以及 ZoneDirector 进行管理

规格

物理特征

电源	• 220 瓦内置电源
	• 输入：100－250V AC，IEC320 接头
物理尺寸	• 35.52cm(长)，43.18cm(宽)，4.39cm(高)
重量	• 14 lbs (6.37 公斤)
以太端口	• 2 口，自动 MDX,
	10/100/1000Mbps 自适应，RJ-45
发光指示	• 电源/工作状态
环境条件	• 工作温度：41° F (5° C)－104° F (40° C)
	• 环境湿度：15% － 95% 无凝露

管理

配置	• 网页用户接口， FlexMaster
统计	• 局域网，无线上网的客户端
自动更新 AP 软件	• 支持
捕获门户（Captive Portal）	• 支持
GUEST 帐号	• 帐号
VLAN 支持	• 802.1Q(每个 SSID)
DHCP 服务器	• 支持
AP 发现与控制	• Layer2 或 Layer3
WLANs（多 SSID）	• 最高达 8 个

安全

无线安全	• WEP,WPA-TKIP,WPA2-AES,802.11i
认证	• 802.1X，本地数据库
	• AAA 服务器，ActiveDirectory，RADIUS
本地认证	• 5000 条记录

多媒体和服务品质

VoIP Tunneling	• 支持
802.11e	• 支持
软件队列	• 每种通讯类型，每个客户端
自动分类	• 启发式
速率限制	• 支持

认证

国家与地区	• FCC（美国），IC（加拿大），CE（欧盟），C-Tick（澳洲），OFTA（中国香港）

性能以及配置支持

可管理 AP 数目	• 最高 250 个
并发用户	• 最高 5000

产品订货信息

型号（订货号）	描述
901－3025－AU00	ZoneDirector3025 支持 25 个 AP
901－3050－AU00	ZoneDirector3025 支持 50 个 AP
901－3100－AU00	ZoneDirector3025 支持 100 个 AP
901－3250－AU00	ZoneDirector3025 支持 250 个 AP

无线控制器 - ZoneDirector 1000

Ruckus Wireless ZoneDirector 1000 是首台能实现集中管理的多媒体无线局域网（WLAN）解决方案控制器，系专为中小型企业（SME），以及热点运营商而开发。

以简约和便于使用作为设计思路的 Ruckus ZoneDirector 1000，其目的在于填补客户端 AP 和高端企业系统之间的空白。这些独立客户端的 AP 往往功能不完善、管理繁复，而高端企业系统又往往使用复杂，成本昂贵，中小企业根本无法负担。

对于那些需要一个安全可靠、易于部署、集中管理、自动优化的无线局域网的小型企业来说，Ruckus ZoneDirector 将会是他们理想的选择。

ZoneDirector 1000 对期望为酒店、机场、学校和公共建筑等地点提供商用级热点业务，如 VoWLAN 、IP 视频、企业安全接入延伸和不同等级服务的热点运营商来说，也是完美的解决方案。

Ruckus ZoneDirector 可非常容易的与现有网络、安全和认证系统进行集成；通过网页向导，简单的点击即可很容易的完成配置工作，Ruckus ZoneFlex AP 会自动发现 ZoneDirector 并由 ZoneDirector 对其进行配置。

冗余和安全，Ruckus ZoneDirector 可在一个单一，易于使用和负担得起的无线局域网（WLAN）系统中提供遍及整个 WLAN 范围的网络、 安全、射频和位置管理。

优势

易于使用，易于管理

集中管理，快速设置，IT 管理简化，自动、实时地对整个无线局域网 （WLAN） 进

行优化。

Ruckus SmartMeshTM 降低成本与部署复杂度

集成 SmartMesh 技术，使得部署自动化，无需再为每一台智能 Wi-Fi AP 连接网线电缆。

无线局域网部署时间不超过 5 分钟

基于网页的配置向导能使任何计算机用户在几分钟内配置完毕整个无线局域网（WLAN）。Ruckus ZoneFlex AP 会自动发现 ZoneDirector。

富有弹性的部署选项

ZoneDirector 可与现有网络和安全架构交互，并为所有 AP 提供动态射频管理，而无需再考虑 AP 定位问题。

三重业务支持

内置于 ZoneFlex 中的智能天线阵列以及精确的 QoS 支持，保证了语音，视频以及数据的可靠传输。

监控和故障诊断简单易行

可定制的监控界面，提供了全面的网络简洁视图，并可用于深入诊断各种无线故障。

自动用户安全

无需再对不同 PC 客户端使用唯一的加密密钥进行配置和更新

集成多种功能

集网络管理，动态射频管理，位置管理以及 AP 控制于一身，是一个成本极低的解决方案。

先进的无线局域网特性和功能

基于角色的用户策略，内部认证数据库，AP 盗用监测以及每个 AP 用户入口监测。

易于部署

Ruckus ZoneDirector 能够和现有的交换机、防火墙、认证服务器以及其他的网络架构无缝集成。Ruckus ZoneFlex AP(无论是有线 AP 还是使用了 SmartMesh 技术的网状 AP)会自动发现 Ruckus ZoneDirector，并进行自配置，配置完毕后即可对其进行管理。在允许接入前，ZoneDirector 将对所有想接入 WLAN 的用户进行认证和授权。集成了完善射频

管理的 ZoneFlex AP 会将射频信号聚焦于客户端的方向，在减少干扰的同时，自动进行性能最大化和覆盖范围的最大化，并尽量减少所需的 AP 数量。

易于管理

在完成基本配置，开始运行之后，ZoneDirector 将自动管理 ZoneFlex AP 网络——对发射功率的自动调整，以及必要时对射频频道进行指定，以防止相邻 AP 之间的干扰，并在 AP 失效时启用冗余 AP 覆盖。配置的更改可以非常容易地同时应用到多个 AP 或整个网络系统上。可定制的监控界面可实时显示用户接入信息、网络信息和事件情况，同时一个实时地图将显示无线 AP 的位置以及无线信号的覆盖范围，Ruckus SmartMesh 的拓扑结构等。

易于保密

ZoneDirector 1000 提供了创新的技术，简化和自动化了 Wi-Fi 的安全防护。除了支持企业级的 802.1x 以外，ZoneDirector 1000 还支持一种动态预共享密钥(PSK,Pre-Shared Key）的专利技术，可以简化无线局域网的安全防护工作。

初次使用的用户只需简单的将他们的电脑接入局域网，然后指定一个 URL 地址，即可进入一个一次性认证的捕获网页门户。一旦认证完毕，ZoneDirector 就会自动使用预先指定的 SSID，以及一个动态生成的加密密钥，对用户的系统进行配置。这个密钥会在超出有效期后自动移除，或者是在用户（用户设备）失去信任后而被人工移除。

Ruckus SmartMesh 提高灵活性，降低成本

SmartMesh 能够进行自我管理以及无线网的自我修复。SmartMesh 无需再为每一台 Smart Wi-Fi AP 连接网络线缆，因此系统管理员只要随便找个电源插座，将 ZoneFlex AP 插上去就可以走开了。所有的配置与管理都会通过 ZoneDirector 智能无线局域网平台进行。通过专利的 Ruckus 智能 Wi-Fi 技术，拓展覆盖范围以及动态信号控制，再通过 SmartMesh 技术最小化内部跃点数目（跃点越多，性能下降越多），此消彼长之下，再根据环境的变化自适应调节不同节点之间的 Wi-Fi 连接，从而进一步缩减了所需部署的 AP 数量。

BeamFlex 消除干扰，最大化性能，拓展到达区域

Ruckus BeamFlexTM, 一种专利 Wi-Fi 天线控制技术，能够根据多媒体程序进行自动传

输，以确保预期的性能，并拓展覆盖范围，消除无线死角。

通过 ZoneDirector,BeamFlex 的应用价值从单一的 AP 拓展到了整个系统的 WLAN 和智能无线网结构之上。ZoneDirector 自动控制所有的 ZoneFlex 智能无线 AP 的信道指定以及传输发射的功率水平。

通过 BeamFlex，ZoneFlex 系统可以持续的为每一个客户端的数据包在不同 AP 之间选择最佳的传输路径——在自动消除干扰的同时，还能确保最高的服务质量。

规格

物理特征

电源	• 外部电源适配器 • 输入：110－240V AC • 输出：12V DC，1A
物理尺寸	• 25cm(长，15.93cm(宽，3.86cm(高)
重量	• 2.2 lbs（1 公斤）
以太端口	• 2 口，自动 MDX，10/100/1000 Mbps 自适应，RJ-45
发光指示	• 电源/工作状态
环境条件	• 工作温度：32° F（0° C）－122° F（50° C） • 环境湿度：15% － 95% 无凝露

管理

配置	• 网页用户接口， FlexMaster
统计	• 局域网，无线网络，以及相关客户端
自动更新 AP 软件	• 支持
捕获门户（Captive Portal）	• 支持
GUEST 帐号	• 帐号
VLAN 支持	• 802.1Q(每个 SSID)
DHCP 服务器	• 支持
AP 发现与控制	• Layer2 或 Layer3
WLANs（多 SSID）	• 最高达 8 个

安全

VoIP Tunneling	• 支持
802.11e	• 支持
软件队列	• 每种通讯类型，每个客户端
自动分类	• 启发式
速率限制	• 支持

认证

国家与地区	• FCC（美国），IC（加拿大），CE（欧盟），C-Tick（澳洲），OFTA（中国香港）

性能以及配置支持

可管理 AP 数目	• 最高 50 个
并发用户	• 最高 1250

Access Point - 室内 ZoneFlex 7942

智能 Wi-Fi 802.11n 多媒体 AP

首台集中管理，支持 Mesh 的 802.11n 智能无线 AP。Ruckus 无线 ZoneFlex 7942 乃是首台集中管理的多媒体无线 AP，体现了 802.11n 的技术优势，提供了无与伦比的传输率。

配合 Ruckus ZoneDirector 中央无线局域网控制器，Ruckus ZoneFlex AP 能够做到即插即用，运行费用极低。 对于那些缺乏或者根本没有 IT 专业人员，财务预算又极其紧张的酒店、学校，以及中型企业而言，Ruckus ZoneFlex 7942 是他们的理想选择；此外，对于那些准备提供商用热点服务（无线语音服务、IP 视频、或者企业安全接入等）的热点运营商而言，ZoneFlex 7942 也是再合适不过了。

802.11n 以提供高数据传输率以及高吞吐量为特色。 Ruckus ZoneFlex 7942 正是通过使用 802.11n 的先进技术，比如空间复用、频道复合，以及帧集成等，并对这些技术进一步完善，从而在产品中体现了 802.11n 的特点。

ZoneFlex 7942 通过 Ruckus 的专利 BeamFlex 智能天线技术，可以自动适应各种环境的实时变化，保证了始终如一的高性能，并拓展了覆盖范围，以及提供多媒体支持。这意味着所需使用的 AP 数目更少，用户满意度更高，系统性价比更佳，而且无需任何专业人员即可将产品安装在任何需要的地方。

一个基于网页的向导，让任何电脑用户都可以在几分钟之内通过 ZoneDirector 对 ZoneFlex 7942 进行配置，从而建立一个安全可靠的无线局域网。 用户只需将 Ruckus ZoneFlex 7942 接入任何以太网络，即可自动找到 ZoneDirector。 无需射频调节，无需客户端配置，一个真正的即插即用的多媒体无线局域网马上就可投入使用。

优势

突破性的用户性能和密度

高级天线阵列以及精确的 QoS 软件，可以实现并发的 20 路语音通话，100 路并发数据用户，或是每个 AP 300Mbps 的容量。

无需射频专家

智能天线阵列让 AP 定位不再是问题，而通过 ZoneDirector 的动态频道指定以及发射功率管理功能，临近 AP 之间的相互干扰也降到了最低。

SmartMesh 技术极大地降低了部署成本以及复杂度

内置的 Ruckus SmartMesh 技术使得部署完全自动化，再也无需为每一台智能无线 AP 连接网络线缆。

拓展的覆盖范围，意味着 AP 的用量更少

和传统的消费级 AP 以及企业级 AP 相比，方向性、高增益的天线动态组合，让热点运营商以及企业可以成倍（乃至 4 倍）的扩大覆盖范围。

专为无线语音服务优化

特别的天线设计，动态的信号路径选择，以及精确的 QoS 软件，专门为低延迟而进行的优化，保证了高密度的无线语音（Vo-Fi）应用。 节能服务（UAPSD）最大化了手持话机的电池寿命。

支持视频流

Ruckus 智能天线系统及视频 QoS 非常适合进行实时 IP 视频流应用，并被世界范围内超过 100 家的 IPTV 运营商采用。

配置和管理无需 IT 专业人员

基于网页的向导，让你可以在几分钟内配置整个无线网的多台 AP。 一旦配置完毕，无线局域网就可以进行自我管理。

提供商用热点服务

让运营商可以通过提供全新的服务，比如无线语音服务、扩展企业接入、IP 视频应用等等，而获得全新的营收机会。

极高的性能，性价比极佳

基于 IEEE 802.11n 标准，Ruckus ZoneFlex 7942 支持高达 300Mbps 的数据容量。ZoneFlex 7942 的与众不同之处还在于，内置了专利 Ruckus BeamFlex 智能天线技术，可以自动适应射频环境的各种变化，从而帮助无线信号找到最佳路径，并实时回避各种干扰。

每一台 ZoneFlex 7942 都配备科技领先的高增益智能天线阵列，改天线阵列提供了极其卓越的密度与范围。 最高可支持 100 路并发用户数据流，或者 20 路并发语音通话。另外，ZoneFlex 7942 覆盖范围的提升，降低了单位面积内需要部署的 AP 数量。因此，Ruckus ZoneFlex 7942 提供了业界最具性价比的 802.11n 无线解决方案。

易于部署

自我优化的 Ruckus BeamFlex 技术，让 ZoneFlex 7942 可以快速安装，而无需考虑部署位置，也无需进行射频规划。 将任何一台 Ruckus ZoneFlex 7942 接入任意一个以太网，它就能自动发现 Ruckus ZoneDirector，并进行自我配置。

Ruckus ZoneFlex 7942 以及 ZoneDirector 系统可以和现有的安全系统（防火墙、入侵检测系统、认证服务器——包括 RADIUS 以及 Active Director）进行无缝集成。 一个内部认证数据库让企业可以直接部署用户认证，而无需再借助昂贵复杂的外部认证服务器。

易于配置

Ruckus ZoneDirector 会自动配置 Ruckus ZoneFlex 7942 AP。 一个 AP 网络，可以通过 ZoneDirector 基于网页的向导，在几分钟内集中配置完毕。

SmartMesh 提高了灵活性，降低了成本

Ruckus SmartMesh 可以自我组织并自行修复无线网状结构（Mesh）。 SmartMesh 让你无需再为每一台智能无线 AP 连接网线，系统管理员只需找到电源插座将 ZoneFlex AP 接上即可。 所有的配置和管理都会通过 ZoneDirector 智能无线局域网平台进行。 SmartMesh 在通过专利的智能无线技术提升覆盖范围，以及动态信号控制的同时，降低了会导致性能下降的内部跃点数，并自动根据环境的变化调节不同节点之间的无线连接，从而降低了需要部署的 AP 数量。

自动用户安全

配合 Ruckus ZoneDirector，Ruckus ZoneFlex 2942-OT 提供了可靠的、第一类自动强制

用户安全。 对于无线访问的安全问题，通常的方法是对所有的客户端设备都使用某个无线设置进行配置（如某个 SSID 以及加密密钥）。 很多企业典型的做法是让所有的员工使用一个预先共享的单一密钥。而这会带来安全方面的问题，而且操作起来也是让人头痛不已。

802.11n 以及 BeamFlex：致胜组合

作为通向 wi-fi 的全新基础路径，802.11n 开发了全新的高级技术，诸如空间复用、频道符合，以及帧集成等等，以实现更高的数据传输率。

虽然生产商的广告一直在宣传 802. 11n 可以达到 300Mbps 乃至更高的数据传输速率，但实际的用户吞吐量却相差甚远。 这是因为当前的 802.11n 产品应用这些新技术的效果并不理想。 Ruckus 的 BeamFlex 却真正让 802. 11n 的技术优势变成了现实。

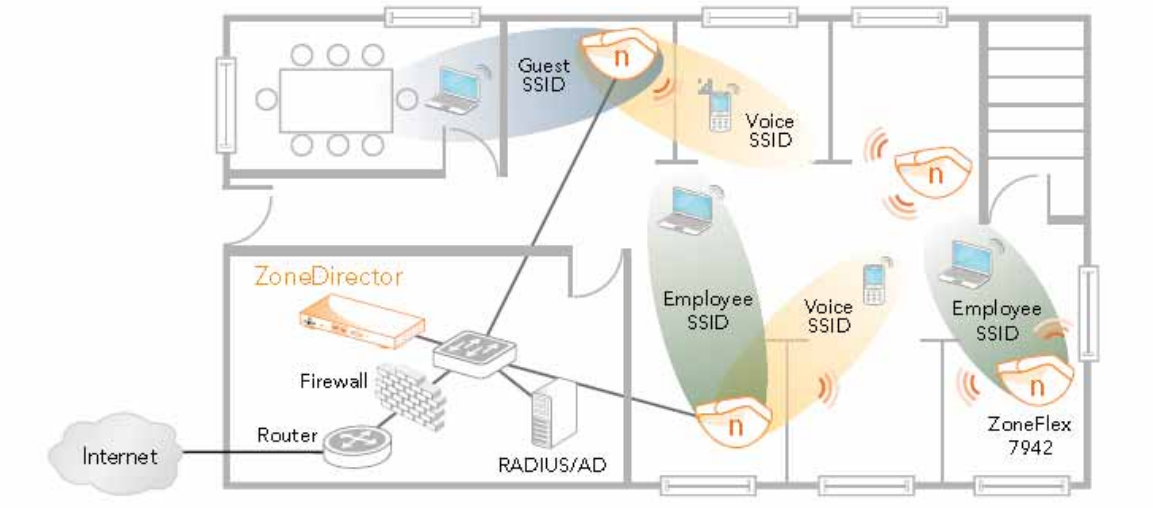
双极智能天线阵列提升空间复用效果

射束控制主动消除干扰，确保空间复用以及空间流的最佳可用路径

信号路径选择控制以及干扰降低，让频道复合变为可能

为每个客户端优化路径，降低了丢包率，保证了更好的接收灵敏性，提升了有效吞吐量，保证了更多的帧集成。

ZoneFlex 7942 智能无线 AP 可以单独模式部署，也可以由 ZoneDirector 统一集中管理。ZoneFlex 7942 也可以用 SmartMesh 进行部署，无需为每台 AP 连接网线。



Ruckus ZoneDirector 以及 ZoneFlex 7942 中的 Ruckus 专利动态 PSK 技术，可以自动实现该过程，以确保与现有用户认证系统的集成。 第一次使用的用户只需简单的将电脑连入

局域网，并访问某个指定 URL 地址，即可进入一个一次性认证的捕获门户。 认证完毕后，ZoneDirector 会使用一个指定的 SSID，以及一个唯一的，动态生成的加密密钥对用户系统进行自动配置。 该密钥会在超出有效期后被自动删除，或者在用户或用户设备失去信任时被人工删除。

商用多媒体热点

ZoneFlex 7942 能让运营商建立新型的热点，并提供多媒体热点服务。通过双极方向性天线系统，ZoneFlex 7942 可以和任何无线手持设备之间建立可靠的连接，并可以稳定支持并发视频流以及无线语音通话。

对不同设备使用多个 SSID

每台 Ruckus ZoneFlex 7942 可以被配置 8 个不同的 SSID，每个 SSID 都有惟一对应的广播，QoS、安全以及管理参数。这样热点运营商可以很容易的针对不同用户或者不同的通讯类型提供分层服务。 企业则可以使用此功能来为不同的客户、承包商，以及雇员使用不同的访问策略，或者对不同的通讯类型进行分段处理。

动态射频管理

Ruckus ZoneFlex 无线局域网天生就具备射频协调性，因为 BeamFlex 可以实时自动的调整无线信号，使其在发向接收者的同时避开相关干扰。Ruckus BeamFlex 并不像全方位天线系统那样朝所有方向都发射同等的信号，因此也就最小化了临近 AP 之间相互干扰的可能。万不得已时，Ruckus ZoneDirector 还可以通过对 ZoneFlex AP 的频道指定以及发射功率进行动态调整，来进一步改善射频环境，而无需人工干预。

特点

集成智能天线系统，提供超过 4000 种的独特组合形式，专为三方服务设计。

自动回避干扰，专为高密度环境优化

提升发射距离/覆盖范围达 2~4 倍

数据容量达 300 Mbps，可支持 80Mbps 的视频吞吐量

每个客户 4 个队列

8 个 BSSID，每个都有唯一的 QoS 以及安全策略

支持 WEP, WPA-PSK, 802.1X

SmartMesh（需 ZoneDirector）

零 IT 以及动态 PSK（需 ZoneDirector）

加入控制/负载均衡（需 ZoneDirector）

捕获门户以及 Guest 账号（需 ZoneDirector）

RADIUS 以及 Active Directory 支持（需 ZoneDirector）

高级射频管理（需 ZoneDirector）

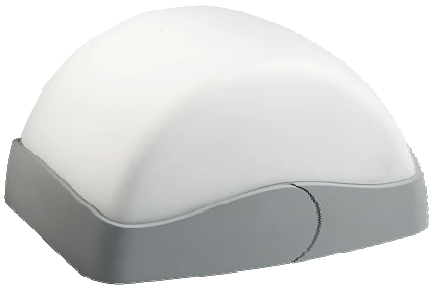
两个 10/100/1000 Mbps 以太网端口，允许 AP 及本地设备的菊花链式连接。

通过以太网取电（PoE），易于部署

可安装于墙壁或天花板上

支持 Kensington 电脑锁

Access Point - 室内 ZoneFlex 2942



电源外置电源适配器
输入: 110-240V AC
输出: 12V DC, 1A
通过以太网线供电

尺寸
19.43cm (L)*14.43cm (W)*10.16cm (H)

重量
550克

天线
内置可配置天线阵列，包括全向高增益和方向单元可支持高达4千个天线组合外置可选
RP-SMA连接头

以太网接口
2个端口，自动MDX和10/100Mbps适应, RJ-45
支持802.3af通过以太网线供电
•
•
LED 显示电源/状态，以太网状态，无
线状态，无线网络质量指示，
Director连接状态
•
固定选件
集成Kennsington固件

运行环境温度:

32° F (0° C) - 122° F
(50° C)
湿度: 15% - 95%无冷凝
•
•
性能
同时支持用户数
50

UDP吞吐量
15-20 Mbps (突发 54 Mbps)
460平方米覆盖
•
VoWLAN语音呼叫
20
QoS和流量控制
业务分类
语音、视频、尽力而为和管理数据

软件队列
每个用户4个队列
自动流量分类自动对组播视频数据包进行业务标记

速率限制
支持

VLAN支持
802.1Q

启发式分类
支持

标准
802.11b/g

支持速率
54,48,36,24,18,12,11,5.5,2,1Mbps
•
无线信道支持
US/Canada: 1-11
Europe (ETSI X30): 1-13
Japan X41: 1-13

自动信道选择

支持

发射功率

23 dBm for wireless-B

23 dBm for wireless-G

可根据国家规范不同配置发送功率

发射功率控制

支持

BSSID数量

8

节电模式

支持

规范和认

证FCC (U.S.), CE (EU), OFTA (Hong Kong) Canada, Australia/ New Zealand

Plenum rating (UL 2043) - in process

无线安全性

WEP, WPA-PSK, WPA-TKIP, WPA2-AES

802.1X, 本地认证数据库支持 RADIUS 及ActiveDirectory

(完)