

Making WLANs Work Reliably and Cost-Effectively in a Multimedia World

A Guide for Small/Medium Business and Public Hot Zone Operators



Executive summary

Administration of small-to-medium business wireless LAN (WLANs) or independent hot spots at hotels, stores, transportation centers, and other public venues are often frustrated by consumer product limitations, but have no time or budget for enterprise-class solutions. These companies need an affordable, easy-to-use alternative that is still robust and scalable enough to extend the reach of their wireless LANs, support existing and next generation services and provide reliable and predictable Wi-Fi performance.

This paper examines the opportunities and challenges associated with operating a small-to-medium business WLAN or public hot spot. It explains the benefits of a self-configuring platform that can deliver Wi-Fi more reliably, to increasingly diverse devices and applications, covering larger areas and higher user densities, while minimizing total cost of ownership. Finally, this paper introduces the Ruckus ZoneFlex wireless LAN system and its attempt to fill the gap between current low AP and high-end WLAN platforms.

In the beginning

Wi-Fi has become the access method of choice for users at the office, at home, and on the road. According to Wi-Fi research from InStat, nearly 200 million Wi-Fi chipsets were sold in 2006 alone, reflecting the technology's expanding usefulness for a wide variety of applications and devices. Last year, over 95 percent of laptops sold incorporated Wi-Fi, as did many new PDAs, smart phones, and voice over IP (VoIP) handsets. By the end of 2008, Wi-Fi is expected to be an inherent capability in all LAN purchases.

Gartner Group estimates that 64 percent of businesses have already deployed Wi-Fi, from isolated trials to campus-wide rollouts. Surveys show that Wi-Fi is no longer a niche technology, used largely for Internet access in conference rooms. Two out of three companies with WLANs use Wi-Fi as an Ethernet replacement in cubicles and offices, while one quarter use Wi-Fi

to support core business applications like inventory management and manufacturing automation.

In addition, many workers now access the Internet and business applications through public Wi-Fi hot spots at hotels, airports, and many other venues frequented by travellers. Roaming access provider iPass reports that the number of enterprise user Wi-Fi sessions jumped 54 percent during 1H06. ABI Research predicts that Wi-Fi hot spots will grow from 143,700 in 2006 to 179,500 this year, driven largely by expansion within the retail and hospitality sectors.

As Wi-Fi becomes pervasive, user expectations rise fast. To not only survive but thrive, today's casual data WLANs must mature into reliable "hot zones" – larger, higher-capacity WLANs that deliver predictable service to increasingly diverse and demanding users. For small-to-medium businesses and hot spot operators, short on time and budget, the trick is to accomplish this mission-critical transformation with minimal cost and complexity.

Table 1
Something's Missing: Today's SMB WLAN Choices

WLAN Requirement	Enterprise Wi-Fi	Consumer Wi-Fi
Easy to configure, deploy and manage		✓
Affordable		✓
Simple to secure		
Self-optimizing, self-healing	✓ -	
Extended Wi-Fi coverage (no dead spots)		
Automatic RF management	✓	
Interference avoidance		
Support for isochronous (delay-sensitive) traffic	✓ -	
Centralized management	✓	
Automatic client configuration		
Reduced cabling (wireless AP meshing)		

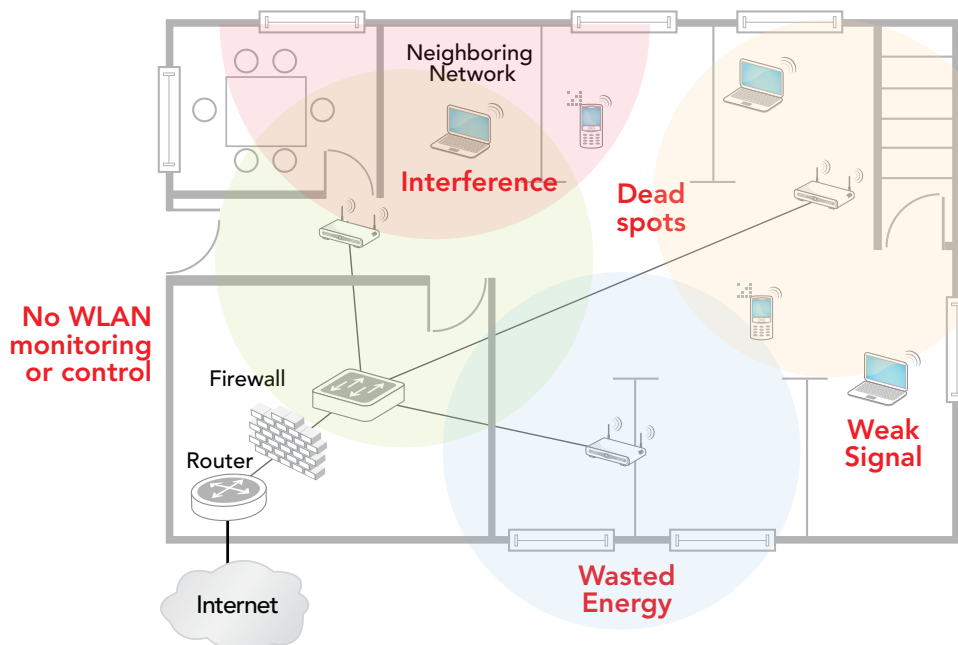
Overcoming today's challenges

Many business WLANs actually start with consumer-grade access points (APs). These APs are placed wherever wireless access is desired – initially in conference rooms and lobbies, later throughout offices and other work areas. This type of unplanned organic growth may have been satisfactory when Wi-Fi was a novelty, but as dependence and utilization grow, limited coverage and uneven performance and compromised security quickly starts to disappoint users and frustrate administrators.

While lack of formal planning plays a role, consumer-grade APs are just not up to the task of creating a comprehensive, reliable business-grade WLAN. These APs use inefficient omni antennas to cover a circular area of limited diameter. As Wi-Fi transmissions are absorbed and reflected by walls and other obstacles, those circles shrink from 300 feet wide in open space to under 50 feet inside a typical office.

Covering a larger office (or a hotel or school) requires multiple APs, but the outcome is often spotty. At the edge of each circle, weak signal delivers unreliable low-rate connections. Dead spots in between prevent or break user sessions, requiring repeated log-ins, application restarts – even reboots.

Figure 1
Office WLAN using consumer-grade access points



To eliminate dead spots, some organizations try deploying consumer APs more densely. However, with only three non-overlapping 802.11b/g channels to choose from, this can generate disruptive co-channel interference between adjacent APs. In the end, total capacity does not improve, problems increase, user experience degrades, and administrators struggle to manage numerous APs, each operating autonomously.

Larger enterprises overcome these challenges by deploying sophisticated WLAN switching systems and RF management suites. According to Gartner, 80 percent of enterprises are now revisiting their WLAN designs to cope with growing demands and external interference. Many are spending thousands on site survey tools (average cost \$10K), WLAN controllers (\$2-30K), wireless intrusion prevention servers (\$5-20K), WLAN management platforms (\$4-30K), and location tracking appliances (\$2-14K). Once the cost of design, installation, management, and maintenance are added, total cost of enterprise WLAN ownership is roughly double that of the infrastructure investment.

Clearly, those high-end solutions would be overkill for SMBs and hot spot operators. Not only are enterprise products too expensive, they require experienced IT staff and RF experts. Within SMBs, IT staff is stretched thin performing a myriad of tasks and unprepared to be RF or Wi-Fi experts.

Meanwhile, as WLAN usage and footprint grows, the operational and performance problems associated with consumer-grade APs will only get worse. To survive, companies that are too big for consumer gear but too small for enterprise suites must find another way to operate more reliably.

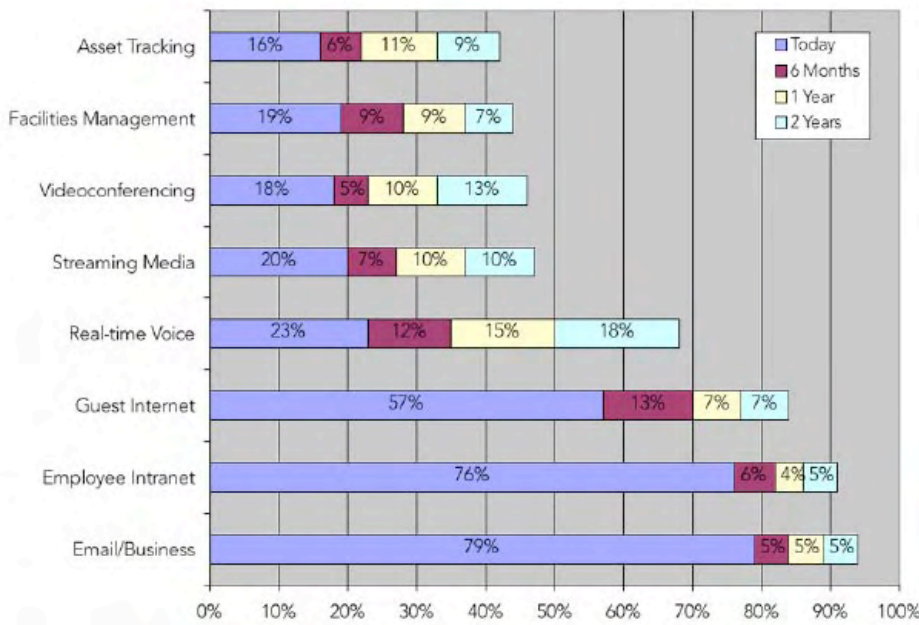
Meeting tomorrow's demands

Wi-Fi applications are expanding rapidly beyond guest Internet, employee Intranet, and email access. These casual data applications still represent the lion's share of WLAN traffic, but more demanding multimedia applications

are poised for growth. As shown in Figure 2, real-time voice calls, streaming media (webcasts, podcasts), and interactive videoconferencing were already in use at 18-23 percent of the companies surveyed last year. By the end of 2008, a whopping two out of three companies expect to be running VoIP over Wi-Fi, and almost half plan to use WLANs to carry streamed and/or live multimedia feeds.

Figure 2

Growing diversity of business WLAN applications
(source: 2006 State of the WLAN Report, Webtutorials)



Today, business WLANs are dominated by laptops. Tomorrow, those WLANs will be required to support a far more diverse collection of business devices, including Wi-Fi-enabled projectors, printers, smart phones, and VoIP handsets. For example, ABI Research expects Wi-Fi phone shipments to grow from 1.8M in 2006 to 15M in 2011. Over 325M dual-mode (cellular + Wi-Fi) phones will also ship that year, for use in Fixed Mobile Convergence (FMC) initiatives that route calls over corporate LANs, Wi-Fi APs, and fixed-mobile networks.

Public hot spots will experience similar growth in applications and devices. Consumer video applications like YouTube, IPTV, and Slingbox have already taken hold. A few hot spots now advertise support for Skype softphones and handsets as a

competitive differentiator. In fact, analysts predict that voice over Wi-Fi will be heavily-used by guests and staff in hospitality WLANs. For example, Wi-Fi communicator badges are quickly replacing those old walkie-talkies carried by hotel and conference center staff.

To keep tomorrow's users happy and productive, today's casual data WLANs must grow into robust multimedia hot zones. This means delivering predictable, secure coverage that blankets the entire service area with sufficient capacity and density. It also means satisfying the diverse constituencies who share the

same airwaves by delivering the class of service appropriate for each user, device, and application. WLAN operators that prepare to meet these escalating demands will thrive in the multimedia age.

Getting from here to there

Meeting these increasingly stringent demands without working yourself into the ground or breaking the bank requires a new kind of platform -- one specifically designed for the target environment. Whether you are building a small-to-medium business WLAN or a public hot spot, you will need an affordable, easy-to-use platform that is still robust and scalable enough to enable footprint, capacity, and service expansion. What essential characteristics should you look for in your next WLAN platform?

Simplified installation and configuration.

Given limited staff and RF expertise, small-to-medium businesses and hot spot operators need to be able to quickly install and configure all the requisite WLAN components such as controllers and APs. Wizard-based configuration systems that provide easy-to-understand setup are a must. Additionally, a platform that can find and activate new APs on its own, make automated post-deployment adjustments to reduce dependence on pre-deployment site surveys and expert set-up, is a sound investment.

IT-lite deployment. Gartner Group estimates that enterprise AP installation runs \$500 to \$2000 per client. A significant portion of that cost involves supplying power and network connectivity

Making WLANs Work Reliably and Cost-Effectively in a Multimedia World

to each AP. Look for APs that can reduce or eliminate those costs. Using Ethernet cables to deliver DC power (802.3af) is one good option. Another is using Wi-Fi to create a wireless mesh between APs thereby eliminating Ethernet cables to APs altogether – particularly when the AP must be located out of reach of the existing Ethernet drops. Merely place APs anywhere and add power. The APs then find the best performing RF path to the root or backhaul AP wired to the network.

Self-tuning. The single-most time-consuming and frustrating aspect of WLAN administration is dealing with change. New APs are added, existing APs fail, obstacles and users move, and environmental conditions vary – all impacting optimal channel assignment, power output, and antenna positioning. Even if you could tweak parameters to respond to those changes, doing so would take RF expertise and full-time supervision – and adjustments still wouldn't occur fast enough. Instead, look for a platform that tunes itself, dynamically adjusting RF settings to automatically mitigate interference, fill coverage gaps, and deliver predictable performance.

Increased capacity. AP range and capacity directly impact cost of ownership. Upgrading from 802.11 b/g to 802.11n can make your WLAN less complicated and costly as 802.11n APs can cover larger areas at higher data rates. However, more raw bandwidth does not always result in proportionally higher throughput and doesn't guarantee higher user and session density. Start with APs that can support more than a handful of simultaneous sessions and APs that automatically loadshare. Then look for features (broad channel support, adaptive directional antennas) that allow those APs to be placed in closer proximity without interference. With twice as many radios in each AP, 802.11n will be an interference nightmare without integrated interference mitigation.

Tiered service levels. Tomorrow's diverse devices and multimedia applications will require WLANs that adapt to their unique needs. Just throwing more bandwidth at multimedia is not enough – streaming video will gobble capacity, slowing data and rendering VoIP unusable. Deploy only APs that let you prioritize traffic using 802.11e Wi-Fi Multimedia (WMM) access categories: voice, video, best-effort, and background without tedious or complex administration. In addition, look for optimizations important to your users, like intelligent queuing to reduce VoIP latency and power-save to conserve handset battery life. By delivering premium service to selected

users, SMBs can allocate resources appropriately and hot spot operators can tap opportunities to earn more revenue.

Robust but simple security. For SMBs, strong encryption and authentication do the trick. Start with APs that support standard 802.11i security, including WPA and WPA2, using PSK and 802.1X authentication. Then seek out new capabilities that provide automatic client security configuration. New systems now provide the ability for the network itself to configure the wireless and security settings on end user laptops. Another key criteria is the integration with your AD or RADIUS server if already in place. In a perfect world, every client would support these strong security measures. But, as more users and devices connect to your WLAN for a wider variety of reasons, one-size-fits-all security will not cut it. Those with guests may require login portals, while those with embedded devices may need MAC filters. Look for a platform that lets you assign role-based security policies using multiple SSIDs and VLANs to segregate those clients and control their traffic flow.

Reduced maintenance. SMBs and hot spot operators cannot afford to baby-sit their networks, nor can they spend a lot of time tuning them. However, you still want the ability to quickly determine how your WLAN is operating and who is using it. Look for a platform with a centralized easy-to-use console that lets you see the entire WLAN at a glance, then drill down to trouble-shoot or update APs. Too much information is overwhelming but too little information is just as bad. Make sure that you can visualize RF status, device locations, user connections, recent alerts, and historical reports at a level of detail that is right for you.

Introducing Ruckus ZoneFlex

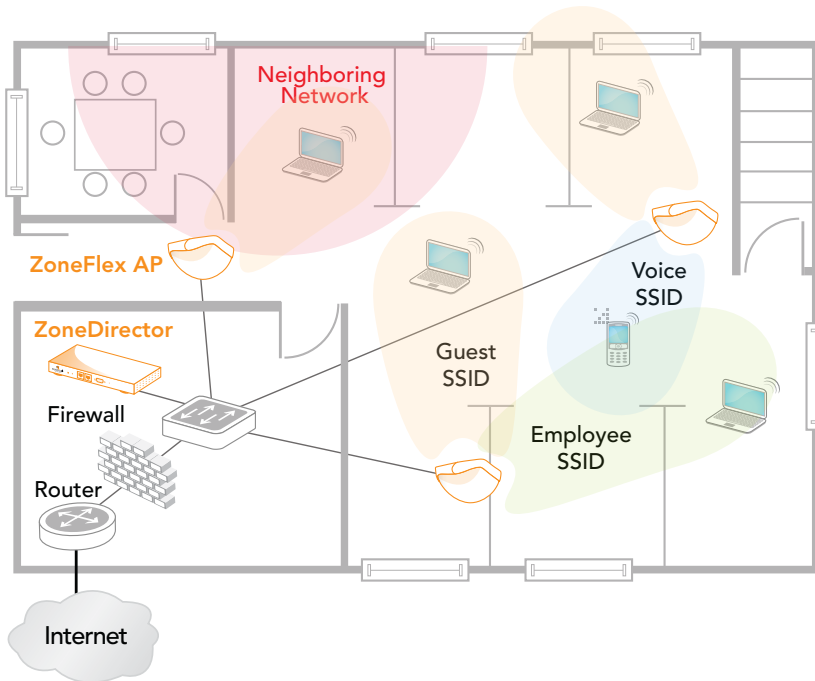
ZoneFlex is a family of products developed to fill the gap between unreliable consumer-grade APs and pricey, complicated enterprise WLAN systems.

By combining smart ZoneFlex multimedia APs with a turn-key centralized control system, Ruckus has enabled painless deployment of robust, full-featured WLANs priced and simplified for the SMB market. ZoneFlex was created with small-to-medium businesses and hot spot operators in mind, using drag-and-drop interfaces, wizards and automation to simplify installation and operation.

And ZoneFlex was designed to do much more than simply address the headaches associated with today's casual data WLANs. By using smart Wi-Fi antenna technology to pick the best signal path and steer around sources of interference, ZoneFlex squeezes the most out of your airspace. ZoneFlex can help you expand your WLAN's footprint, capacity, and services by creating a reliable Wi-Fi hot zone that requires fewer APs than any other enterprise WLAN system.

ZoneFlex can be deployed in an office environment (see Figure 3) or a public hot spot, using a single ZoneDirector to automatically discover, provision, and manage up to 25 ZoneFlex Smart Wi-Fi APs.

Figure 3
Office WLAN based on Ruckus ZoneFlex



As a plug-and-play system, the ZoneDirector integrates seamlessly with your existing network. Simply plug the ZoneDirector into your LAN and point-and-click to create per-SSID roles that reflect your performance and security needs. ZoneDirector does the rest – from dynamically selecting and adjusting AP transmit power levels and channel assignments to automatically configuring a unique Pre-Shared Key (PSK) on every client.

ZoneDirector enforces your policies by authenticating users through a built-in captive portal, PSK, or 802.1X, consulting an internal database or your existing AD or RADIUS server. Each ZoneFlex AP then delivers the requested class of service, supporting up to 20 concurrent voice calls and 50 data clients.

By supporting multiple SSIDs, each with its own broadcast, quality of service, security, and management parameters, ZoneFlex APs can deliver tiered services that support different users, devices, and applications from a single platform.

ZoneFlex APs are less expensive than enterprise APs and far more powerful and robust. These APs implement Ruckus-patented beam steering (BeamFlex™) and quality of service (SmartCast™) technologies.

SmartCast uses advanced heuristics to automatically classify Wi-Fi packets, managing transmit queues to deliver high-quality multimedia services – including voice and streaming video.

BeamFlex uses smart antenna arrays to extend AP range and coverage 2 to 4 times by dynamically steering traffic along the optimum path to each client (see Figure 3). By detecting, rejecting, and avoiding RF interference, BeamFlex not only enables high-density WLANs -- it does so while delivering more predictable and reliable service without manual tuning and constant tweaking. In short, ZoneFlex APs adapt automatically to your environment, avoiding administrator and user frustration.

These same RF engineering techniques have been extended network-wide. Network BeamFlex extends the benefits of increased range and interference mitigation across a multi-AP environment. This results in fewer APs deployed, higher-levels of performance to end users and the elimination of Wi-Fi dead spots. Network BeamFlex also adds wireless meshing, leveraging best signal path determination to enable a high-performance AP mesh that reduces deployment costs and continually adjusts to ensure optimal user performance.

Making WLANs Work Reliably and Cost-Effectively in a Multimedia World

The ZoneFlex family offers many other features designed to simplify installation and maintenance and reduce total cost of ownership. For example, ZoneFlex APs support PoE to make the most of power drops and switch ports. Additionally, no-touch Wi-Fi PSK configuration enables strong security in situations where it would not otherwise be practical (public hot spots, guest WLANs), without adding any IT effort.

And ZoneDirector delivers many enterprise-class WLAN management and monitoring features, from rogue AP detection to performance reporting, without introducing enterprise complexity or cost.

ZoneFlex is the ideal next step for small-to-medium businesses and hot spot operators that have outgrown consumer APs and casual data WLANs. Learn more about how ZoneFlex can help you deliver reliable Wi-Fi to increasingly diverse and demanding users, adding capacity and range with limited IT staff and budget.

Visit www.ruckuswireless.com



Ruckus Wireless, Inc.

880 W. Maude Avenue. Suite 101

Sunnyvale, CA 94085 USA

TEL +1 650-265-4200 FAX +1 408-738-2065