



Ruckus Makes Noise in the WLAN Space

By Andrew Garcia, eWeek Labs Reviewer

Ruckus Wireless' ZoneFlex Smart WLAN is well worth a look for businesses considering a move to a controller-based architecture.

Ruckus Wireless' ZoneFlex Smart WLAN solution goes out of its way to make wireless networking simple for business customers.

With its easy initial setup and ongoing management, innovative client configuration tools and outstanding use of advanced antennae technologies to lengthen the functionality of the network, ZoneFlex is well worth a look for small businesses considering a move to a controller-based architecture.

I tested the ZoneDirector ZD1006 (\$1,200), which is licensed to support six access points. The ZoneDirector 1000 series (up to \$6,000) will support up to 50 concurrent APs (access points), which will allow customers to grow their network to support a much larger floor space over time. Ruckus also recently announced the 3000 series of appliances, which support up to 250 APs.

I tested the ZoneDirector in conjunction with Ruckus' ZoneFlex 2942 (\$349) 802.11b/g APs. The 2942 features Ruckus' BeamFlex technology, which employs beamforming techniques to dynamically select the right antennae combination to optimize an active client's performance at longer distances. Each access point has 12 embedded antennae (6 in a horizontal deployment, 6 vertical), allowing a total of 4,096 distinct antenna combinations which allow each access point to support a wider coverage area than standard access points using two or three diversity antennae.

To ease initial setup of a ZoneFlex network, Ruckus uses many tools that would be quite familiar to someone accustomed to setting up home networks. For instance, when I first plugged in the ZoneDirector appliance,

the device automatically advertised itself via UPnP (Universal Plug and Play), allowing me to easily locate it for configuration. The configuration page automatically launched a wizard that walked me through the setup of two WLANs: a production network that I could secure with the full gamut of wireless security protocols (WPA and WPA2 are supported in both PSK and Enterprise flavors), as well as an unencrypted guest network.

When first connected to the network, Ruckus APs will automatically broadcast their presence to the network, allowing the ZoneDirector to automatically pull the device under management and push out the configuration profile. After initial network deployment, administrators should disable the AutoApprove feature on the ZoneDirector, which will force the administrator to manually approve devices before they can join the network.

The ZoneDirector 1000 series supports a maximum of four concurrent WLANs, which meant that I could simultaneously advertise a data network, a voice network, a guest network and one other at the same time (the ZoneDirector 3000 supports eight WLANs). Unfortunately, every AP that reports to the ZoneDirector will get the same WLAN configuration, so I could not target the guest network to advertise only in access points supporting public areas, such as lobbies or conference rooms. Ruckus will need to resolve this problem as they continue to grow its solutions to target larger network deployments.

The ZoneDirector offers a limited number of self-healing services. The ZoneDirec-

tor can adjust an AP's radio channel when it detects interference. I found this feature to be a little bit too sensitive, with radios flopping between channels several times per minute in some instances. Unfortunately, the product's sensitivity threshold is not configurable.

In addition to interference detection, periodic channel scans also provide some intrusion prevention services, such as support for detecting rogue access points or

for blocking clients who repeatedly fail authentication or make excessive wireless requests. The solution only handles over-the-air rogue detections, so the

system could not distinguish between APs connected to the same wired network and APs that simply share the same airspace.

I particularly liked ZoneDirector's Web-based configuration and management pages. The product's dashboard employs a customizable widget-based structure, which allowed me to select the views of my network I wanted to see by default—such as the most active APs or clients, the current status of my devices, or the most recent system alerts. I could further drill down into specific management pages for more information, including an interactive map page from which I could predict coverage areas for my network or locate potential rogue APs, a set of user and guest pass management pages or a viewer for in-depth logs that report unusual activities of external devices.

I especially liked the speedy search function that powers the log, which enabled me to quickly find all instances of a particular kind of alert or of activities pertaining to a specific device.



Ruckus ZoneFlex Smart WLAN System

"Ruckus has truly set a high bar for innovation on the client side."

By default, users of the guest network are redirected to a captive portal Web page, where they are required to enter temporary guest credentials in order to access the network. Corporate users are allowed to create guest passes, provided the wireless administrator has assigned them the proper permissions (via a Role). The wireless administrator can also centrally control the life of guest passes by expiring the passes a certain amount of time after the pass is either created or first used. Once a guest user connects, they are then denied access to any networked resources on the local subnet – and administrators can further customize the network to deny access to other subnets as well.

ZeroIT

While the ZoneFlex solution certainly eases WLAN deployment and management for less technical shops, Ruckus has truly set a high bar for innovation on the client side. Ruckus' ZeroIT feature truly makes it simple to deploy the strongest levels of wireless security, allowing customers to deploy WPA2 using either certificate-based authentication or dynamically pre-shared keys with a minimum of administrator interaction needed on the client machines—as long as the clients are running Windows XP with SP2.

Users configure their wireless security by first plugging into the wired network, where they log into the ZoneDirector, then down-

load a client configuration applet. The applet ensures the client is running Windows XP with SP2, then automatically configures operating system's integrated wireless supplicant with the appropriate network and encryption settings.

I did notice that the applet does not check for Microsoft's Wi-Fi Protected Access 2/ Wireless Provisioning Services Information Element (Microsoft KB 893357), a patch that adds WPA2 support to Windows XP, and that is required to enable ZeroIT to work properly.

While administrators can choose to pass through authentication requests to an existing RADIUS server or an Active Directory, ZeroIT requires users to authenticate to the local authentication server in the ZoneDirector. Still, using ZeroIT was absolutely the easiest way I've seen to deploy enterprise-grade, certificate-based wireless security, as the applet includes a certificate to client machines to use EAP-TLS. End users will need to be walked through a Windows Certificate installation wizard to complete the setup—a potentially daunting step for some users, even if the wizard only requires the user to click through the default settings to get the wireless network running.

IT administrators may instead opt for ZeroIT using Ruckus' DynamicPSK, which automatically generates a unique pre-shared key for each user. In an ordinary PSK (pre-shared key) secured network, everyone would

use the same key—meaning that every computer would need to be reconfigured when the key is changed. With DynamicPSK, each user has their own key, and administrators can easily configure the key expiry interval for each user, thereby creating an automated, periodic, key rotation.

Each user's pre-shared key appears to be tied to both the client computer and the wireless adapter itself, as in tests I found I could not successfully install the applet on a PC

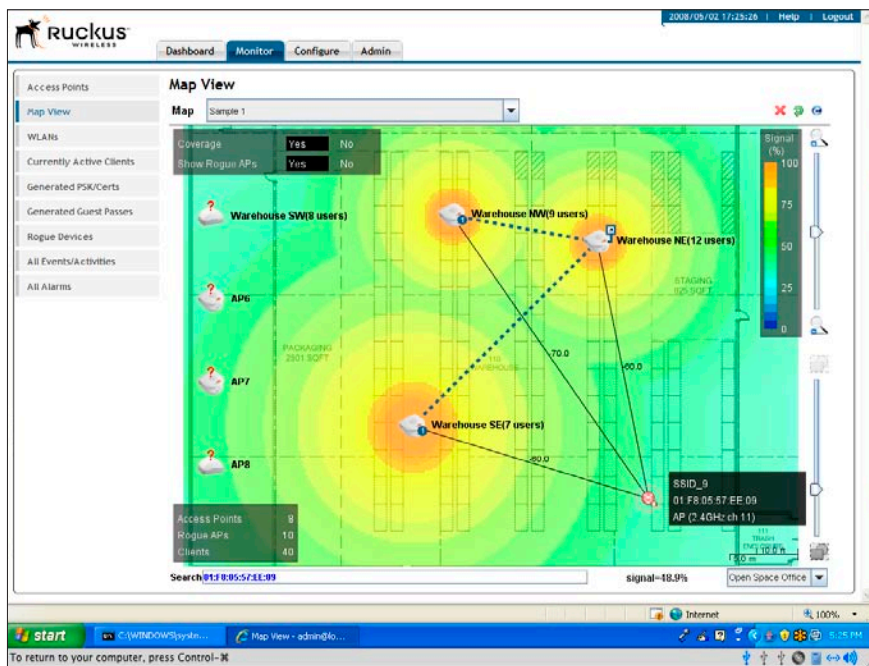
"Ruckus' ZeroIT feature truly makes it simple to deploy the strongest levels of wireless security."

other than the one from which I generated the applet, nor could I use a different wireless adapter in the same PC.

802.11n Support

With firmware release 3.0.1.0 build 109, Ruckus also added 802.11n support into the ZoneFlex solution. With that release, I could join and manage a new ZoneFlex 7942 802.11n access point (\$699) to my ZoneFlex network in the same manner as legacy APs. In ZoneDirector, the only management difference for 802.11n was an additional field that allowed me to define whether the 11n AP utilized a standard 20 MHz channel or a wide 40 MHz channel.

Although most business-class 802.11n solutions operate in both the 2.4 GHz or 5 GHz bands, the ZoneFlex 7942 only operates in the 2.4 GHz band. Customers that want to reduce the potential for interference may therefore opt to stick with standard 20 MHz channels, which will limit their network's top-end performance. Indeed, in my preliminary performance tests, which I conducted amid the over-saturated RF in our downtown San Francisco offices, I squeezed a maximum of around 80 Mbps out of the ZoneFlex 7942--adequate numbers for an 802.11n solution. ■



The Ruckus ZoneDirector's Map View displays WLAN and WLAN mesh topology, signal coverage as well as rogue APs.