Beyond the Site Survey:
RF Spectrum Management for Wireless LANs

A Farpoint Group White Paper

Document FPG 2003-201.1
September 2003
Introduction

Our primary objective in the further development of wireless networks of any form today is to narrow, if not eliminate, the behavioral and performance differences that distinguishes wireless from wireline. So, while it is most certainly true that a wireless LAN is, in fact, a local-area network and therefore at least in theory capable of handling any mission suitable for a LAN, the “wireless” part of “wireless LAN” often gets in the way. The primary reasons for this are the vagaries of the radio channel, that property of the universe that allows data to move through the air in much the same fashion as it travels through wire. The core issue here is that the air does not behave like wire when serving as a carrier for electromagnetic waves. In fact, the fundamentally variable nature of the radio channel, due primarily to the fading of radio waves as they move through space and interact with other radio waves and physical objects of all forms, is occasionally baffling if not maddening to even experienced users (and sometimes even engineers!). Unintentional interference to signals from other devices operating on the same frequencies is becoming a concern as the installed base of wireless LANs and related devices multiplies. The laws of physics being what they are, we continue to learn from experience new techniques to accomplish that most desirable goal as noted above. This White Paper will look at what can be done at the physical (radio) later to improve the performance of wireless-LAN systems.

Enter (and Exit) the Site Survey

As it turns out, the vast amount of experience that we as an industry have garnered over the more than ten years that WLANs have qualified as an industry have enabled what are in many cases radically new approaches to implementing and managing radio-based LANs, and we will cover these below. But to begin, consider at the outset that staple of WLAN installations, the site survey. A site survey is designed to give anyone installing a wireless LAN an idea of the coverage to be expected for any given access point (AP) installed, and is the basic radio frequency (RF) planning tool available to most WLAN managers. Those of us with long histories in the industry have spent many happy (and sometimes not) hours in this activity. If you’ve not had the pleasure of such an exploration yourself, here’s the process. Typically, an access point is placed and powered (but not connected to the backbone network) in a given location, initially determined in most cases by simple guesswork. The person conducting the site survey then runs the site survey application, provided by the vendor of the wireless LAN equipment, on a mobile computer. By walking around and noting the relative signal strength at a given location, the placement of each access point can then be roughly determined. It’s a time-consuming and often costly process, but that’s not the worst of it. Consider these other factors – the site survey:

- **Does not consider other RF traffic or interference** – By its very nature, a site survey looks only at wireless-LAN signals; the radios involved in WLANs can’t really deal with other non-WLAN signals which therefore show up only as interference. Since interference tends to be intermittent and manifests itself in most cases as lower throughput, a site survey usually won’t reflect interference at all, even if it’s relatively strong.

- **Does not consider the instantaneous nature of the radio channel** – The behavior of the RF channel varies strongly with both time and the movement/location of each user. A site survey might therefore show great results that do not hold up in production use.

- **Does not consider capacity** – Perhaps most importantly, site surveys are unconcerned with both throughput and overall capacity. Note performance demands will change both over time as more users are added, and as user load demands change, as well as due to the varying and uneven distribution of wireless users with respect to any given AP. Coverage is usually a poor choice as a point of optimization – capacity is today the key concern, especially as WLAN prices continue to fall. And note that since the AP is not connected to real traffic during the site survey, only signal strength and not actually traffic volumes can be considered.

- **Does not consider changes in infrastructure** – Over the life of any given installation, changes to the
building itself (or even the arrangement of metal fixtures or furniture), the need for additional access points, the discovery of previously undetected sources of interference, and other factors will dictate changes in the WLAN infrastructure. Repeating a site survey might result in the conclusion that a wholesale change to the infrastructure is required, when in reality all that is really required is re-balancing with respect to channel assignment, transmit power, and the reconfiguration of backhaul connections.

- Front-loads WLAN installation efforts with a potentially expensive, labor-intensive activity – Site surveys can be expensive, since they require experienced, competent individuals to do the work. A comprehensive site survey (which most VARs and dealers, unsurprisingly, always seem to want to perform) can literally cost as much as the required access points themselves – and more!

The above discussion led us to the conclusion some time ago that site surveys are of little value, especially when conducted before any equipment has been installed. Site surveys made a lot of sense back when access points cost on the order of US$2,000, and were the size and weight of a desktop PC — both not all that long ago. Today, however, as throughput requirements have grown and the use of WLANs has become much more horizontal (general) in nature, site surveys in most cases are not the most productive use of one’s time or money.

We will grant, however, that it may be necessary in some cases to perform an RF sweep in place of a site survey, whenever an otherwise unsolvable RF-related problem is suspected. In this case, a device known as a spectrum analyzer is used to visualize the amount of energy in the particular radio frequency band in question (usually the 2.4 or 5.2 GHz. bands). The spectrum analyzer can be quite useful in finding undesirable RF emissions of all types, but we must caution that most are designed for use by engineers and are thus not really an item most end-user organizations would possess. The good news is that we’ve only rarely seen a need for such devices, although the increasing use of unlicensed products is bringing the issue of RF spectrum management to a head rather quickly.

What is RF Spectrum Management?

First of all, we must point out that the radio spectrum used by wireless LANs and similar devices is unlicensed. What this means is that any product that meets the regulatory specifications for a device operating in one of the unlicensed bands can be freely used by anyone. Most countries reserve at least some spectrum for unlicensed operation, usually involving low-power devices like cordless phones and wireless LANs.

The catch, however, is that these devices must accept any interference which might be present in the band where they are operating – unlike licensed users, there’s no recourse to the regulator when interference adversely affects one’s installation. Couple this with the variable and often difficult behavior of the radio channel as noted above, and anything called RF spectrum management (RFSM) at first glance appears to be an abstract, theoretical concept. In reality, though, there are many steps that wireless LAN network managers, armed with appropriate contemporary WLAN products, can take to dramatically improve the performance of their networks, and the productivity of their users. The good news is that these systems and tools are beginning to appear – and that they represent a significant advance over the site survey. Just as network management has aided us in activities at Layer 3 (the network layer) of the protocol stack, RF spectrum management is now producing real returns in Layer 1 (the physical layer), which to this point has been beyond the reach of most users. RF spectrum management is in fact yielding meaningful improvements in performance, manageability, return on investment, and even total cost of ownership.

Elements of RF Spectrum Management

While we’re really at the dawn of the whole concept of RF Spectrum Management, Farpoint Group believes that a number of key capabilities can be identified at present that form the core of RFSM activities:
Farpoint Group White Paper — September 2003

Beyond the Site Survey: RF Spectrum Management for Wireless LANs

• Plan (and implement and configure) – As we noted above, the functionality of most site survey applications and procedures leave a lot to be desired. One of the obvious first-step improvements is to allow installation planning using CAD drawings of proposed installations (see Figure 1). This allows both a “big picture” visualized evaluation of the task as well as a convenient way to document the installation. We need to stop short here and caution that, yes, while “virtual” site surveys using the CAD environment are possible, we do not believe that most users will have sufficient knowledge of the interaction between radio waves and building construction to build an adequate model of the installation. Indeed, when it comes to final placement and number of access points, this part of the process really needs to wait until an initial installation has taken place.

A more realistic approach is to design wireless LAN systems with the ability to self-configure. While this at first glance might seem complex, products with this capability are now appearing. In general, a self-configuring infrastructure is one that is constantly monitoring the radio environment, something that is really not too difficult for access points. For example, each AP in an installation can, in turn, listen to all activity around it. From this, the AP can be calibrated to the environment, a process we'll discuss in more detail below. It’s important, of course, that such information be recorded for review – centralized configuration and calibration management is a must in any RFSM approach. Such a self-configuring capability has the potential to dramatically simplify upgrades, additions, reconfigurations, and even provide such features as self-healing in the event of a failure and dynamic capacity management.

The bottom line is that we believe the technologies required to automate much of the planning that otherwise would have been trial-and-error or site-survey based now exist, and that they will become standard features in WLAN systems. Initial configuration, calibration, and the re-calibration that is inevitably necessary as infrastructures grow and change, need not be time-consuming, labor intensive tasks. And, of course, such capabilities also benefit the installation in terms of lower support requirements, less network management staff time, higher effective uptime, and improved productivity and satisfaction for users.

• Monitor – The concept of remote monitoring, sometimes called RMON after the Internet Engineering Task Force (IETF) standard of the same name, has been around for some time. In a nutshell, RMON allows a central station to gather statistics, both instantaneously and historically, from other network elements. These statistics can include information relating to throughput, errors of various forms, and many other possibilities. The data can also be used to trigger alarms based, again, on both instantaneous conditions and historical trends.

Figure 1: A key element in RF spectrum management is being able to visualize the installation. (Illustration courtesy Aruba Wireless Networks)
It has become obvious that such RMON functionality is critical to the operation of any LAN, and a wireless LAN is really no different. In the wireless case, however, statistics gathered can include retry rates, sources of interference (and in some cases the location of these interferers), collisions, fragmentation rates (how often packets are broken into smaller packets, which can occur when radio conditions become congested or otherwise degraded), and the effective channel rate, which will vary based on loading, range, and decisions made within the infrastructure as to what the channel rate should be. For example, the channel rate for 802.11b products is normally 11 Mbps, but the specification and implementation allow this rate to fall back to 5.5, 2, and 1 Mbps based on conditions (although the specific mechanisms for downshifting and upshifting this rate are up to the given manufacturer of the equipment being used).

The regular review of monitored information, usually in statistical form, can be of great assistance to network management staff in both solving ongoing problems and in managing WLAN infrastructure growth.

- **Troubleshoot** – The ability to fix problems detected by the monitoring process is the next step in RFSM. While RFSM does allow a high degree of self-healing (for example, dynamically re-configuring AP transmit power levels and channel assignment to automatically compensate for a failed AP), it’s also important to receive notification of such conditions as active attacks, intentional and unintentional interferers, rogue (unauthorized) APs, user out-of-range situations, and co-channel interference, just to name a few. Note that it’s also possible to handle many of these conditions dynamically as well. But even in the case where this isn’t always possible, such as a user that wanders out of range, at least a notification can be provided to allow network managers to decide on the installation of new APs to handle such situations (or remind users that coverage is not available by design in certain locations).

- **Optimize** – A primary function of network management overall, of course, is to keep the network up and (efficiently) running, a challenge compounded by factors noted in this White Paper that are not found in the wired world. A good example, as we noted above, is calibration, which in this context is used to describe the requirement to set channel assignments and transmit power levels so as to optimize both coverage and capacity. Note that the calibration process (see Figure 2) must be dynamic in order to consider both changes in the radio environment as well as the addition of new APs.

![Figure 2: The calibration process automatically configures (and re-configures) access points, providing an optimal result with minimal hands-on involvement (illustration courtesy Aruba Wireless Networks)](image)

Two additional examples of optimization include:

1. **Load balancing** – Wireless users are inherently mobile, and a phenomenon we inle-
Bunching can occur quite frequently. Bunching results when a relatively large number of users are associated with a single access point, as is often seen in a conference room, waiting area, or other high-traffic spot. It can also occur when a relatively small number of users have large demands for capacity, and in this case we call it traffic bunching. Regardless, the AP in question is likely to be swamped, with a corresponding and usually noticeable falloff in overall throughput. The immediate solution is to assign some traffic to other APs on other radio channels, thereby making better use of RF resources and providing greater capacity. Of course, if bunching is a frequent problem (and as such needs to be part of regular monitoring activity), more APs can address the problem quite well. This is another reason why RFSM must produce good management reports, with high and low watermarks and well as thresholds for alarms and trend reporting (noting, for example, new users and their impact over time). RFSM greatly simplifies the process of re-configuration and re-calibration after infrastructure additions are made to a given installation or user loads change—even temporarily.

2. **Bandwidth allocation**—Regardless of the number of users, it’s often desirable to offer higher throughput to certain classes of users. For example, senior management might be offered priority throughput in an enterprise, or public-access WLAN subscribers might have the options of buying “silver” or “gold” service. Both the prioritization of user traffic as well as the placement of hard limits on throughput for a given user are possible. Traffic can also be prioritized for latency management, as might be required for voice or video service. Varying RF conditions can affect the ability to provide these services in a meaningful way, so it’s critical that RFSM be a part of any bandwidth allocation policy scheme.

Figure 3: The RF Spectrum Management cycle. (source: Farpoint Group)

There are many other possible optimizations that affect not only users, but network managers as well. We can think of the key elements of RFSM as really being part of a cycle (see Figure 3), with planning leading to an installation, monitoring being used to gather necessary statistical and event-based information, troubleshooting being used to isolate and eliminate problems as they occur (and to ideally identify trends that will lead to problems before they would otherwise become evident), and optimizing resources so as to get the most from the investment in infrastructure and related services provided to users. Since history shows us that networks are never really finished, and must grow and evolve with
new technologies as well as ever-increasing user expectations and demands, the optimization process inevitably leads to new planning for more capacity, features, coverage, and reliability. RFSM therefore needs to be a core element of any enterprise-scale or public-access WLAN installation. The investment made in such functionality will quickly result in payback in terms of both hard-dollar savings and soft-dollar benefits.

Finally, while the whole subject of security is usually reserved for discussion of activities at Layer 2 (inherent 802.11 functionality) and Layer 3 and above, there are a number of RFSM functions that can assist in making a WLAN more secure. First of all, the ready identification of rogue APs prevents any traffic from flowing through these unauthorized ports. Forced disassociations, whereby the infrastructure causes a client to drop its connection with a given AP, can be used to correct the problem if it has proceeded to the stage where a connection has been established (and this can happen surprisingly quickly, so continuous monitoring is becoming a requirement). It’s also possible to lock out given users, although MAC-address spoofing can make this activity difficult. Finally, active monitoring can detect attempts at intrusion, as well as identify and interrupt man-in-the-middle attacks, to which 802.11-based WLANs are particularly susceptible.

The Future of RF Spectrum Management

The availability of RF spectrum management tools is one of the most significant developments in the history of wireless LANs, and one which we believe will have a far-ranging impact on both users and the WLAN industry. As RFSM solutions are accepted as the primary vehicle for eliminating complexity, efficiently resolving problems, reducing total cost of ownership (TCO), and just generally providing a more satisfying user experience, yet another barrier to the eventual ubiquity of WLANs is removed. The next step in the evolution of RFSM is, we believe, the integration of this functionality with related network, system, and enterprise management tools. Of course, we can expect additional core RFSM functions over time, provided by WLAN system vendors that understand their importance in creating – and keeping – satisfied customers.