WHITE PAPER

A Guide to Effectively Managing Enterprise Wi-Fi Networks

Introduction

Not so very long ago, wireless LAN access was a novelty in the corporate world, largely reserved for curious engineers and privileged executives. Back then, managing the radio activity on a wireless network was often as simple as making sure the CEO could use a notebook computer to gain intranet access from the conference room down the hall. These days, radio frequency (RF) management involves overseeing and controlling all the devices and all the activity on a enterprise wireless LAN – and chances are that it's a great deal of activity. RF management is a challenging job that grows more challenging as Wi-Fi gains in popularity.

These days, a typical enterprise wireless LAN can span multiple buildings at multiple sites. Thousands of employees and their mobile computers may use the Wi-Fi network not only for data access, but for voice and video applications, too. Wi-Fi is increasingly becoming a default feature in electronic devices ranging from hospital infusion pumps to phones, let alone notebook PCs. The demand for enterprise mobility is expected to grow dramatically during the next few years, driven by the uptake of applications such as mobile e-mail and mobile workforce management applications. The number of mobile applications that enterprises deploy to their employees is likely to grow by 30 percent per year through 2011, according to the consultancy Gartner, Inc.[1]

Thus, the person in charge of the enterprise wireless LAN has the daunting task of ensuring that employees have ubiquitous, consistent, secure access to the Wi-Fi network, from myriad mobile devices. And in order to meet that challenge, it's important that a WLAN can address the many facets of RF management.

RF management is an all-inclusive challenge that includes taking care of every access point and client device on a wireless network – while catching every device that doesn't belong there. In order to avoid making WLAN administration a full-time headache, IT administrators who are deploying or extending enterprise WLANs must make sure that RF management is not an afterthought. In fact, RF management should be a top priority.

The many aspects of RF management

RF management includes the following tasks: planning and building the WLAN,

- Monitoring and optimizing the performance of the WLAN
- Maintaining WLAN security
- Managing all the devices that utilize the WLAN

It's not simple, but if tackled holistically, RF management is feasible.

Planning the network

An effective wireless-LAN plan helps network administrators avoid spending time and money on trial-and-error deployments -- not to mention the headaches associated with complaints about weak Wi-Fi signals. Planning a WLAN involves choosing reliable network hardware, of course. But initially it involves studying the users and the site of the network to ensure that requirements are met. Whether you're implementing a network from scratch or expanding an existing one, RF planning must be a top priority.

The person tasked with planning a wireless LAN must answer many questions:

- Who will be using the wireless LAN, and for which applications? (Providing real-time video feeds from wireless security cameras requires more bandwidth than providing basic e-mail access, for example)
- Is voice one of these applications the network will support? (Voice transmissions are especially sensitive to network delay and jitter.)
- Should some applications be prioritized over others?
- Will mobile users require fast, secure roaming among the access points on the network?

The site of the wireless LAN garners questions such as:

- Are the walls in some buildings made of materials that might interrupt radio signals?

[1] Gartner, Inc., Gartner's View of Enterprise Mobility, July 2007.

- Are there structures in the building that might cause multipath propagation of radio signals? (This is a common problem in places such as hospitals and manufacturing plants.)
- Are there areas of the corporate campus that require more bandwidth access than others? (The auditorium may require wireless access to video applications for hundreds of users at once, for example.)
- Are there areas of the corporate campus in which installing Ethernet cables is not an option?
- Are there nearby Wi-Fi signals that might interfere with the enterprise wireless LAN?

Monitoring the wireless network

Stay one step ahead of the users. Monitoring and maintaining the activity on a wireless network can be a daunting task because a network administrator can only be in one place at a time. In a distributed environment, the corporate wireless LAN might span several cities, let alone several buildings. That's no mean feat; even in large organizations, the task of administering the wireless LAN often falls on just one or two people. But to ensure premium performance, network administrators must have constant access to the wireless LAN, in order to perform functions including configuration, analysis, troubleshooting, and recovery.

Effective monitoring means troubleshooting all the switches, access points, users and devices on the wireless LAN, wherever they may roam. Effective RF management means correcting potential problems before they become actual headaches. Proactive management will save the company a great deal of money in the long run, by preventing network downtime. Network downtime is expensive.

To that end, a wireless LAN administrator must keep track of the following:

- What are the average usage patterns of the network throughout the day?
- Is the wireless LAN compensating for heavy loads during unexpected usage surges?
- Are the wireless switches performing correctly? Are they balancing usage loads effectively?
- What's the average bit rate of voice and data transfers?
- Is RF coverage sufficient and consistent across the network?
- Is every individual application on the network performing as it should?

Device management

In addition to keeping track of the wireless LAN infrastructure, network administrators need to keep track of all the devices that need access to the network. An effective network administrator must always know the answers to the following questions:

- How many devices are on the network?
- How many new devices need to be provisioned on the network on any given day? (Do new employees need wireless access for their notebooks or wireless IP phones?)
- Do any devices require software updates or upgrades? And is it possible to deliver the software remotely? Have all the network switches been updated, so that they can deliver new upgrades to each device?
- Are any client devices acting out of the ordinary or neglecting to adhere to network policy?

At the same time, the network administrator needs to know the location of all the mobile devices on the wireless LAN. This is a vital task for several reasons. For one thing, mobile users have a tendency to lose their mobile devices – they tend to fall out of pockets and purses, and it's helpful to know whether the device was lost within the confines of the corporate network. Furthermore, networked devices are often shared by several users, increasing the likelihood of loss. Whether devices are stolen or simply misplaced, losing them will result in unexpected, unwanted expenses for the company.

Securing the network

Indeed, effective RF management isn't just a matter of keeping constant track of the devices that belong to a corporate wireless network. It's also a matter of keeping track of the devices that don't belong there.

In order to maintain a secure wireless LAN, a network administrator should be able to control the level of access for each user, device, or application depending on job function and security clearance. For example, a company might want to provide complimentary Web access for a visiting contractor, while making sure that the visitor does not have wireless access to the company's CRM database.

Furthermore, the network administrator needs to be able to detect rogue access points anywhere on the network – and to disable them immediately in case they are performing malicious functions. The same goes for unauthorized client devices; it's important that the network administrator has a means of telling the difference between authorized and unauthorized devices.

If a client device is stolen or, more likely, lost, the network administrator must have the ability to lock those devices out of the network until they are in the right hands again

Location tracking is a key part of wireless LAN security as well. It's important to pinpoint the location of access points and devices that do not belong on the network, in order to determine the likelihood that the network is in jeopardy. The ability to find the exact location of the rogue device lets network administrators gauge whether there is any real risk to the wireless LAN. Let's say, for example, that someone has been hiding in the back seat of his car, attempting to use the Wi-Fi network to usurp confidential company data. Finding out where a strange signal is coming from will increase the likelihood of locating the offender.

Preventing intruders means preventing criminals from stealing financial data or information about a company's customers. Protecting that information means maintaining customer confidence and, consequently, retaining customers.

Furthermore, catching unauthorized devices before they do any damage to the network will mitigate the likelihood of network downtime.

Many corporate networks are subject to various government regulations and industry policies that require companies to protect customer data. These include the Payment Card Industry standard (PCI), which requires companies to ensure the protection of their customers' credit card data, and the Health Insurance Portability and Accountability Act (HIPAA), which addresses the security of patient data.

It is incumbent on the network administrator not only to keep track of network activity, but to keep a record of that activity, in case of an audit. To that end, an effective RF management system must include both diagnostic and reporting tools. Each regulation carries different penalties for lack of compliance. Failure to prove compliance with a regulation generally results in hefty fines and bad publicity for a company.

A holistic approach to RF Management – the left hand must know what the right hand is doing

As Wi-Fi has gained in popularity and purpose, the wireless industry has introduced a multitude of tools that address the various aspects of RF management. While each tool may be effective at performing a single function, the problem is that the tools may not work together.

Network administrators often hire outside help to plan and build the wireless network because it can be a complex process, and because they generally are not trained RF experts. But when it comes to monitoring the network once it is up and running, the responsibility lies with the network administrator. It's important that the wireless network plan makes sense to those who are administrating it, and not just those who designed it. In other words, in order to ensure a properly managed wireless LAN, there must be a seamless transition from planning the network to monitoring it.

Furthermore -- especially when the management staff is small -- there must be synergy among the monitoring system, the security mechanisms, and the location tracking applications. By investing in a tightly-integrated RF management system from a single vendor, network administrators can avoid the integration problems of melding together disparate systems from multiple vendors, subsidiaries, and internal departments.

Fortunately, Motorola offers all the tools necessary to plan, manage, monitor, and secure a wireless LAN.

Motorola offers a complete portfolio of management tools to simplify the complex task of RF management. With these tools, network administrators can monitor, maintain, and send software upgrades to every switch, access point, and client device on the corporate wireless LAN. The Motorola RF management suite includes the following:

- **Motorola Mobility Services Platform**
  The heart of Motorola's RF management suite, MSP RF Management Edition offers a single, comprehensive view into a company's wireless LAN, providing an interface to other tools in the suite.

- **Motorola LAN Planner**
  LAN Planner lets network administrators or systems integrators design a wireless LAN that will deliver the superior performance from the start, factoring in stairwells, steel walls, and other possible interference issues.

- **Motorola RF Management Software**
  Once a wireless network is up and running, network administrators can use Motorola's RF Management Software to monitor and manage the activity on the wireless LAN, enabling immediate discovery and troubleshooting of potential problems.

- **Motorola Wireless Intrusion Prevention System (WIPS)**
  Motorola's comprehensive Wireless Intrusion Protection System (IPS) server software automatically takes necessary steps to mitigate malicious activity from rogue access points or unauthorized client devices.

Conclusion

RF management is a daunting task, but with the right tools and a holistic approach, it is easily manageable. Network administrators can be assured of a secure, effectively-managed wireless network by investing in Motorola's comprehensive RF Management Suite. The ability to monitor, secure, and upgrade the wireless network from a single, centralized console will save both time and money for any company with a wireless LAN.

For more information about Motorola Enterprise WLAN products visit:
http://www.motorola.com/enterprisewlan

MOTOROLA

motorola.com

Part number WP-RFMGMT. Printed in USA 09/07. MOTOROLA and the Stylized M Logo and Symbol and the Symbol Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. ©2007 Motorola, Inc. All rights reserved. For system, product or services availability and specific information within your country, please contact your local Motorola office or Business Partner. Specifications are subject to change without notice.