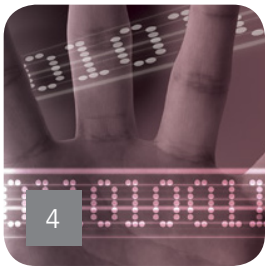
Deploying and Securing a Wireless LAN

an internet.com® Networking eBook

Contents...

Deploying and Securing a Wireless LAN

This content was adapted from Internet.com's Wi-Fi Planet, eSecurity Planet, Enterprise Networking Planet, and Practically Networked Web sites. Contributors: Jim Geier and Michael Horowitz.



Define Your Wireless LAN Deployment Risks

By Jim Geier

When planning a wireless network installation, be sure to carefully assess and resolve risks. Otherwise unforeseen implications, such as RF interference, poor performance, and security holes will wreak havoc. By handling risks during the early phases of the deployment, you'll significantly increase the success of a wireless network.

The following are common risks to consider:

Unclear Requirements

If you deploy a wireless network without first clarifying requirements, then the wireless network may not satisfy the needs of the users. In fact, poor requirements are often the reason why information system projects are unsuccessful. As a result, always define clear requirements before getting too far with the deployment.

For example, you may install 802.11g today to support needs for a moderate number of users accessing e-mail and browsing the Web. Ten months from now, your organization may increase the density of users or need to utilize multimedia applications demanding a higher-performing solution. The organization would then be facing a decision to migrate to 802.11n. Start off right after carefully considering requirements so that you choose the right technologies from the beginning.

RF Interference

Devices such as 2.4 GHz and 5 GHz cordless phones, microwave ovens, and neighboring wireless networks, can cause damaging RF interference that impedes the performance of a wireless network. To minimize the risk of RF interference, perform a wireless site survey to detect the presence of interference, and define countermeasures before installing the access points.

The problem with RF interference is that it's not always controllable. For example, you may deploy a 2.4 GHz 802.11n wireless network in an office complex, then three months later the company next door installs a wireless network set to the same channels. This results in both wireless networks interfering with each other. A possible solution to minimize this risk is to utilize directive antennas that ensure transmit and receive power of your wireless network falls only within your facility. This would limit the impact of the interfering wireless network. You could also specify the use of 5 GHz 802.11n, which offers more flexibility in choosing channels that don't conflict with others.

Security Weaknesses

The potential for an unauthorized person accessing corporate information is a significant threat for wireless networks. An eavesdropper can use a freely-available wireless network analyzer, such as WireShark, to passively receive and view contents of 802.11 data frames. This could disclose credit card numbers, passwords, and other sensitive information.

Avoid security risks by carefully assessing the vulnerabilities of a wireless network, and define effective security policies based on the value of information you need to protect. In some cases, you may simply need firewall protection. Other applications may require effective forms of encryption. 802.1x port-based authentication will also provide added security.

We'll discuss security more in depth later in this eBook.

Applications Interfaces

In some cases, interfaces with applications located on various hosts and servers can bring about major problems when using a wireless network. A relatively short loss of connectivity due to RF interference or poor coverage area causes some applications to produce errors. This occurs mostly with legacy applications lacking error recovery mechanisms for wireless systems.

For example, a user may be using an inventory application by scanning items and entering total counts via a keypad on the scanner. If loss of connectivity occurs after scanning the bar code and before entering the count, the host-based application could log the use out without completing the inventory transaction. As a result, the application on the host may record an incorrect or invalid value for the inventory item.

To avoid these types of risks, carefully define the types of applications the wireless user devices will interface with. If needed, incorporate solutions such as wireless middleware (such as NetMotion) to provide adequate handle recovery mechanisms related to wireless networks.

By identifying and solving these potential risks, you'll have a much more successful wireless network deployment. ■

Minimize WLAN Interference

By Jim Geier

Radio frequency (RF) interference can lead to disastrous problems on wireless LAN deployments. Many companies have gotten by without any troubles, but some have installations that don't operate nearly as well as planned. The perils of interfering signals from external RF sources are often the culprit. As a result, it's important that you're fully aware of RF interference impacts and avoidance techniques.

Impacts of RF interference

As a basis for understanding the problems associated with RF interference in wireless LANs, let's quickly review how 802.11 stations (client radios and access points) access the wireless (air) medium. Each 802.11 station only transmits packets when there is no other station transmitting. If another station happens to be sending a packet, the other stations will wait until the medium is free. The actual 802.11 medium access protocol is somewhat more complex, but this gives you enough of a starting basis.

RF interference involves the presence of unwanted, interfering RF signals that disrupt normal wireless operations. Because of the 802.11 medium access protocol, an interfering RF signal of sufficient amplitude and frequency can appear as a bogus 802.11 station transmitting a packet. This causes legitimate 802.11 stations to wait for indefinite periods of time before attempting to access the medium until the interfering signal goes away.

To make matters worse, RF interference doesn't abide by the 802.11 protocols, so the interfering signal may start abruptly while a legitimate 802.11 station is in the process of transmitting a packet. If this occurs, the destination station will receive the packet with errors and not reply to the source station with an acknowledgement. In return, the source station will attempt retransmitting the packet, adding overhead on the network.

All of this leads to network latency and unhappy users. In some causes, 802.11 protocols will attempt to continue operation in the presence of RF interference by automatically switching to a lower data rate, which also slows the use of wireless applications. The worst case, which is fairly uncommon, is that the 802.11 stations will hold off until the interfering signal goes completely away, which could be minutes, hours, or days.

Sources of RF Interference

With 2.4 GHz wireless LANs, there are several sources of interfering signals, including microwave ovens, cordless phones, Bluetooth-enabled devices, FHSS wireless LANs, and neighboring wireless LANs. The most damaging of these are 2.4 GHz cordless phones that people use extensively in homes and businesses. If one of these phones is in use within the same room as a 2.4GHz (802.11b or 802.11g) wireless LAN, then expect poor wireless LAN performance when the phones are in operation.

A microwave operating within 10 feet or so of an access point may also cause 802.11b/g performance to drop. The oven must be operating for the interference to occur, which may not happen very often depending on the usage of the oven. Bluetooth-enabled devices, such as laptops and PDAs, will cause performance degradations if operating in close proximately to 802.11 stations, especially if the 802.11 station is relatively far (i.e., low signal levels) from the station that it's communicating with. The presence of FHSS wireless LANs is rare, but when they're present, expect serious interference to occur. Other wireless LANs, such as one that your neighbor may be operating, can cause interference unless you coordinate the selection of 802.11b/g channels.

Use Tools to "See" RF Interference

Unless you're Superman, you can't directly see RF interference with only your eyes. Sure, you might notice problems in using the network that coincide with use of a device that may be causing the interference, such as turning on a microwave oven and noticing browsing the Internet slow dramatically, but having tools to confirm the source of the RF interference and possibly investigate potential sources of RF interference is crucial. For example, MetaGeek's Wi-Spy is a relatively inexpensive USB-based Wi-Fi spectrum analyzer that indicates the amplitude of signals across the 2.4GHz frequency band. Figure 1 is a screenshot of the Wi-Spy display with a microwave oven operating 10 feet away.

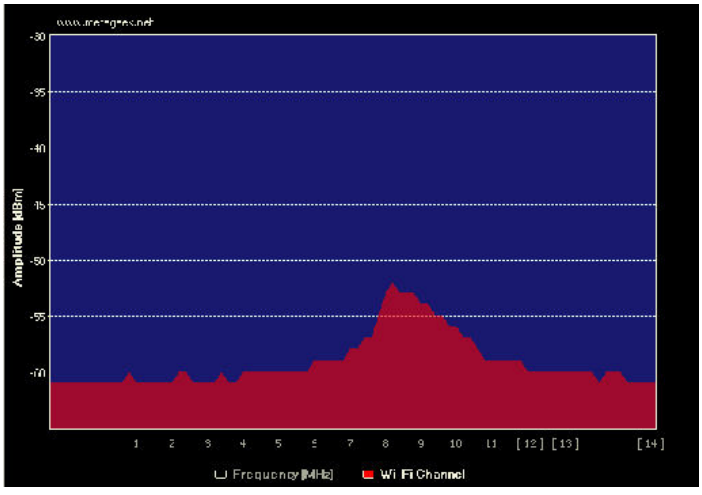


Figure 1

This clearly shows relatively high-level signals emanating from the microwave oven in the upper portion of the 2.4GHz frequency band, which indicates that you should tune any access points near this microwave oven to lower channels. To simplify matters, MetaGeek has an interference identification guide that you can use with Wi-Spy to help pinpoint interfering sources. The benefit of using a spectrum analyzer in this manner is that you can identify the interference faster and avoid guessing if a particular device is (or may) cause interference.

Take Action to Avoid RF Interference

The following are tips you should consider for reducing RF interference issues:

1. Analyze the potential for RF interference.

Do this before installing the wireless LAN by performing an RF site survey. Also, talk to people within the facility and learn about other RF devices that might be in use. This arms you with information that will help when deciding what course of action to take in order to reduce the interference

2. Prevent the interfering sources from operating.

Once you know the potential sources of RF interference, you may be able to eliminate them by simply turning them off. This is the best way to counter RF interference; however, it's not always practical. For example, you can't usually tell the company in the office space next to you to stop using their cordless phones; however, you might be able to disallow the use of Bluetooth-enabled devices or microwave ovens where your 802.11 users reside.

3. Provide adequate wireless LAN coverage.

A good practice for reducing impacts of RF interference is to ensure the wireless LAN has strong signals throughout the areas where users will reside. If signals get to weak, then interfering signals will be more troublesome, similar to when you're talking to someone and a loud plane flies over your heads. Of course this means doing a thorough RF site survey to determine the most effective number and placement of access point.

4. Set configuration parameters properly.

If you're deploying 802.11g networks, tune access points to channels that avoid the frequencies of potential interfering signals. This might not always work, but it's worth a try. For example, as pointed out earlier in this tutorial, microwave ovens generally offer interference in the upper portion of the 2.4GHz band. As a result, you might be able to avoid microwave oven interference by tuning the access points near the microwave oven to channel 1 or 6 instead of 11.

5. Deploy 5GHz wireless LANs.

Most potential for RF interference today is in the 2.4 GHz band (i.e., 802.11b/g). If you find that other interference avoidance techniques don't work well enough, then consider deploying 802.11a or 802.11n networks. In addition to avoiding RF interference, you'll also receive much higher throughput.

The problem with RF interference is that it will likely change over time. For example, a neighbor may purchase a cordless phone and start using it frequently, or the use of wireless LANs in your area may increase. This means that the resulting impacts of RF interference may grow over time, or they may come and go. As a result, in addition to suspecting RF interference as the underlying problem for poor performance, investigate the potential for RF interference in a proactive manner.

Don't let RF interference ruin your day. Keep a continual close watch on the use of wireless devices that might cause a hit on the performance of your wireless LAN. ■

How to Secure Your WLAN

By Michael Horowitz

Securing a wireless network isn't a hard task. The cheat sheet is relatively small. However, the technical press continues to be flooded with articles and blogs containing technical mistakes.

Take, for example, everyone's trusted information source, Consumer Reports magazine. I'm a big fan of the magazine, having subscribed to the hard copy edition for years. But they seem out of their league when it comes to computers.

On Aug. 6, 2009, a blog posting at the magazine's Web site suggested using WEP security for wireless networks. This is very poor advice. A week after the posting, an editor corrected it to say they recommend WPA security. This too, is not the best option. Even after being shamed into a correction, they still got it wrong.

Let me try to offer up just what most people (and Consumer Reports) need to know about securing a wireless network.

Starting at the Beginning

To begin with, there are four types of Wi-Fi networks (a, b, g, and n). But the security is not tied to any one type.

If you can connect to a wireless network without entering a password, then there is no security. In this context, the term "security" refers to encrypting data as it travels over the air. The idea being to prevent a bad guy from capturing all the information coming into and out of a victims' computer and, in effect, looking over their shoulder despite being a few hundred feet away.

Wi-Fi networks offer three security options: WEP, WPA, and WPA2. As a simplistic introduction, think of WEP as bad, WPA as just fine, and WPA2 as great.

WEP is the oldest security option and it has been shown to be very weak. It may be better than no security at all, but not by much. Don't use it. Other than Consumer Reports magazine, the last recommendation to use WEP was issued in 2005.

WPA is technically a certification, not a security standard, but since it includes only one security protocol, TKIP, they are often confused. When people refer to WPA security, they are really referring to the TKIP protocol.

The combination of WPA and TKIP is not the best, but it's reasonably good. If you have a choice, you should opt for the best security (next topic), but if you don't have a choice (more later) TKIP is reasonably strong.

WPA2 is also, technically, a certification rather than a security standard. WPA2 includes two security standards: TKIP and CCMP. If you are using TKIP, it doesn't matter whether the router is WPA or WPA2. TKIP is TKIP either way.

The best security option is CCMP and it's only available in WPA2. Here again, the security protocol is often confused with the certification. When people refer to WPA2 security, they are really referring to CCMP.

But no one refers to CCMP (don't ask what it stands for). For whatever reason, the CCMP security protocol is referred to, incorrectly, as AES. When you are configuring a router, you need to first select WPA2, then you need to select AES (rather than TKIP) to get the best possible security and encryption.

WPA TKIP Flaws

The TKIP security protocol (often referred to as WPA) is flawed. The first flaw came to light in November 2008, the second one just recently. But neither flaw is serious.

The first flaw can be defended against simply by disabling Quality of Service (QoS) in your router. Very few people make use of QoS.

The second flaw was described by security expert Steve Gibson as mostly theoretical. For example, it requires that the victim's computer be out of radio reception range from the router. The bad guy has to connect to the router on one side and the victim on the other side. The bad guy has to be logically and physically positioned between the victim and the router.

Neither flaw lets the bad guy recover the password, and they only support decrypting very small data packets. None of these small packets will contain any of your data. It's not the flaws themselves that make WPA2-AES the best option, but the fact that they are cracks in the dam. Who knows what will turn up next? There are no known flaws in WPA2-AES, which was developed last and built on and improved the work in the earlier security protocols.

Problems Getting to WPA2

Everyone who can should opt for WPA2-AES, but there may be roadblocks.

WPA2-AES requires more computational horsepower than WPA-TKIP. Older routers may not have sufficient horsepower. If your router does not offer WPA2, you can check for a firmware update, but most likely you'll have to buy a new router to get the best security. Then too, since it is the latest and greatest, WPA2-AES may not be supported on the computer, smartphone, gaming machine, Internet radio, or whatever other device you want to use with your wireless network.

For example, Windows XP SP2 does not support WPA2, even if it has been kept up to date on patches. A "hotfix" (KB893357) needs to be installed to add WPA2 support to Windows XP SP2.

A WPA2 router may offer both TKIP and AES simultaneously. Start with AES only and hope for the best. Only choose this option if you have to in order to support an older device.

The AES-CCMP security protocol was a long time coming. Rather than wait, some hardware manufacturers added early versions of the protocol to WPA routers. Since these were based on draft, rather than final versions of the protocol, they may or may not work with newer hardware and software.

Still, if replacing an old WPA router is a big deal, I suppose it's worth a try.

Two Other Aspects of Security

WPA and WPA2 both come in two flavors, Personal and Enterprise. In the Personal version there is a single password; in the Enterprise version each user of the wireless network gets his or her own password. The Personal version is also known as Pre-Shared Key, or PSK for short.

Technically, the best security for consumers and small businesses is WPA2-PSK-AES-CCMP. This entire alphabet soup falls down, however, if you chose a poor password.

Data is still traveling over the air and can be captured and saved by a bad guy who can then try to guess the password offline – thousands of guesses a second for days on end.

Perhaps no one will attack the network you connect to this way, but if they do, the only defense is a long, reasonably random password. WPA and WPA2 support passwords up to 63 characters long. Better yet, think "pass sentence" rather than password. ■

Twelve Key Wireless Network Security Policies

By Jim Geier

With a wireless network, you must consider security policies that will protect resources from unauthorized people. Let's take a look at what you should include in a wireless network security policy for an enterprise.

Consider the following recommendations:

Activate 802.11 Encryption to Make Data Unintelligible to Unauthorized Users

As mention earlier, WEP has weaknesses that make it inadequate for protecting networks containing information extremely valuable to others. There are some good hackers out there who can crack into a WEP-protected network using freely-available tools. The problem is that 802.11 doesn't support the dynamic exchange of WEP keys, leaving the same key in use for weeks, months, and years.

For encryption on enterprise networks, aim higher and choose WPA, which is now part of the 802.11i standard. Just keep in mind that WPA (and WEP) only encrypts data traversing the wireless link between the client device and the access point. That may be good enough if your wired network is physically secured from hackers. If not, such as when users are accessing important information from Wi-Fi hotspots, you'll need more protection.

Utilize IPSec-Based Virtual Private Network (VPN) Technology for End-to-End Security

If users need access to sensitive applications from Wi-Fi hotspots, you should definitely utilize a VPN system to provide sufficient end-to-end encryption and access control. Some companies require VPNs for all wireless client devices, even when they're connecting from inside the secured walls of the enterprise. A "full-throttle" VPN solution such as this offers good security, but it becomes costly and difficult to manage when there are hundreds of wireless users (mainly due to the need for VPN servers). As a result, consider implementing 802.11 encryption when users are operating inside the enterprise and VPNs for the likely fewer users who need access from hotspots.

Utilize 802.1X-Based Authentication to Control Access to Your Network

There are several flavors of 802.1x port-based authentication systems. Choose one that meets the security requirements for your company. For example, EAP-TLS may be a wise choice if you have Microsoft servers.

Establish the Wireless Network on a Separate VLAN

A firewall can then help keep hackers located on the VLAN associated with the wireless network from having easy access to corporate servers located on different, more secured VLANs (i.e., not accessible from the wireless network). In this manner, the wireless network is similar to a public network, except you can apply encryption and authentication mechanisms to the wireless users.

Ensure Firmware is Up-to-Date in Client Cards and Access Points

Vendors often implement patches to firmware that fix security issues. On an ongoing basis, make it a habit to check that all wireless devices have the most recent firmware releases.

Ensure Only Authorized People Can Reset the Access Points

Some access points will revert back to factory default settings (i.e., no security at all) when someone pushes the reset button on the access point. We've done this when performing penetration testing during security assessments to prove that this makes the access point a fragile entry point for a hacker to extend their reach into the network. As a result, provide adequate physical security for the access point hardware. For example, don't place an access point within easy reach. Instead, mount the access points out of view above ceiling tiles. Some access points don't have reset buttons and allow you to reset the access point via an RS-232 cable through a console connection. To minimize risks of someone resetting the access point in this manner, be sure to disable the console port when initially configuring the access point.

Disable Access Points During Non-Usage Periods

If possible, shut down the access points when users don't need them. This limits the window of opportunity for a hacker to use an access point to their advantage as a weak interface to the rest of the network. To accomplish this, you can simply pull the power plug on each access point; however, you can also deploy power-over-Ethernet (PoE) equipment that provides this feature in a more practical manner via centralized operational support tools.

Assign "Strong" Passwords to Access Points

Don't use default passwords for access points because they are also well known, making it easy for someone to change configuration parameters on the access point to their advantage. Be sure to alter these passwords periodically. Ensure passwords are encrypted before being sent over the network.

Don't Broadcast SSIDs

If this feature is available, you can avoid having user devices automatically sniff the SSID in use by the access point. Most current computer operating systems and monitoring tools will automatically sniff the 802.11 beacon frames to obtain the SSID.

With SSID broadcasting turned off, the access point will not include the SSID in the beacon frame, making most SSID sniffing tools useless. This isn't a foolproof method of hiding the SSID, however, because someone can still monitor 802.11 association frames (which always carry the SSID, even if SSID broadcasting is turned off) with a packet tracer. At least shutting off the broadcast mechanism will limit access.

Reduce Propagation of Radio Waves Outside the Facility

Through the use of directional antennas, you can direct the propagation of radio waves inside the facility and reduce the "spillage" outside the perimeter. This not only optimizes coverage, it also minimizes the ability for a hacker located outside the controlled portion of the company to eavesdrop on user signal transmissions and interface with the corporate network through an access point. This also reduces the ability for someone to jam the wireless LAN – a form of denial-of-service attack – from outside the perimeter of the facility. In addition, consider setting access points near the edge of the building to lower transmit power to reduce range outside the facility. This testing should be part of the wireless site survey.

Implement Personal Firewalls

If a hacker is able to associate with an access point, which is extremely probable if there is no encryption or authentication configured, the hacker can easily access (via the Windows operating system) files on other users' devices that are associated with an access point on the same wireless network. As a result, it's crucial that all users disable file sharing for all folders and utilize personal firewalls. These firewalls are part of various operating systems, such as Windows XP and Vista, and third-party applications as well.

Control the Deployment of Wireless LANs

Ensure that all employees and organizations within the company coordinate the installation of wireless LANs with the appropriate information systems group. Forbid the use of unauthorized access points. Mandate the use of approved vendor products that you've had a chance to verify appropriate security safeguards. Maintain a list of authorized radio NIC and access point MAC addresses that you can use as the basis for identifying rogue access points.

With these recommendations in mind, you have a basis for forming a solid security policy. When deciding on which techniques to implement, however, be sure to consider actual security needs. ■

Troubleshooting Poor WLAN Performance

By Jim Geier

After installing a wireless LAN, you might find that it doesn't support applications as well as you expected. Users may complain of erratic connections and slow performance, which hampers the use and benefits of applications. When this happens, you'll need to do some troubleshooting. Start by finding the root cause of the problems.

The table below gives you some pointers on what to look for, specifically the characteristics of signal level, noise level, and retry rate that relate to the root causes of poor wireless LAN performance.

	Signal Level	Noise Level	Retry Rate
RF Interference	n/a	High	High
High Utilization	n/a	n/a	High
Coverage Hole	Low	n/a	High
Bad Access Point	None	n/a	Not Connected

RF Interference

RF interference occupies the air medium, which delays users from sending/receiving data and causes collisions and resulting retransmissions. The combination of high noise levels and high retry rates generally indicates that RF interference is impacting your wireless LAN. You can use tools such as AirMagnet Analyzer or NetStumbler to measure noise. AirMagnet also has tools for testing retry rates, and most access points store retry statistics that you can view through the admin console.

If the noise level is above -85dBm in the band where users are operating, then RF interference has the potential to hurt performance. In this case, the retry rates of users will be above 10 percent, which is when users start feeling the effects. This can occur, for example, when wireless users are in the same room as an operating microwave oven.

Once you diagnose the problem as being RF interference, then figure out where it's coming from and eliminate the cause. If the symptoms only occur when the microwave oven or cordless phone is operating, then try setting the access point to a different channel. That sometimes eliminates the interference.

Take a quick scan of other wireless LANs operating in your area. If you see that others are set to the same channel as yours, then change your network to non-conflicting channels. Keep in mind that there are only three channels (1, 6, and 11) in the 2.4GHz band that don't conflict with each other. Most homes and small offices will have their access point set to channel 6 because that's the most common factory default channel. For this reason you may need to avoid using channel 6 with the access points near the perimeter of your enterprise.

If you can't seem to reduce RF interference to acceptable levels, then try increasing RF signal strength in the affected areas. You can do this by increasing transmit power,

replacing default antennas with units that have a higher gain, or placing the access points closer to each other. This increases the signal-to-noise ratio (SNR), which improves performance.

High Utilization

When there are large numbers of active wireless users, or the users are operating high-end applications such as Wi-Fi phones or downloading large files, the utilization of the network may be reaching the maximum capacity of the access point. With this condition, the retry rates will be relatively high (greater than 10 percent), even if signal levels are high and noise levels are low (i.e., high SNR). The result is lower throughput per user due to the additional overhead necessary to retransmit data frames.

You can increase the capacity and resolve this problem by placing access points closer together with lower transmit power to create smaller radio cells. This "micro-cell" approach reduces the number of users per access point, which enables more capacity per user.

Another method for handling high utilization is to move some of the applications to a different frequency band. For example, you might consider having Wi-Fi phones interfacing with a 5GHz 802.11a network and data applications running over 2.4GHz 802.11b/g.

Coverage Holes

After installing a wireless LAN, changes may take place inside the facility that alter RF signal propagation. For example, a company may construct a wall, which offers significant attenuation that wasn't there before. Worse, perhaps an RF site survey was not done prior to installing the network. These situations often result in areas of the facility having limited or no RF signal coverage, which decreases the performance and disrupts the operation of wireless applications.

Indications of a coverage hole include low signal level (less than -75dBm) and high retry rates (greater than 10 percent), regardless of noise levels. The signal in this situation is so low that the receiver in the radio card has difficulties recovering the data, which triggers retransmissions, excessive overhead, and low throughput. For instance, a user will likely experience a 75 percent drop in throughput when operating from an area having low signal levels.

To counter coverage holes, you need to improve the signal strength in the affected areas. Try increasing transmit power, replacing the antennas with ones having higher gain, or moving access points around to better cover the area. Keep coverage holes from popping up unexpectedly in the future by performing a periodic RF site survey, possibly every few months.

Bad Access Point

In some cases, the root cause of poor performance may be an access point that has failed. Check applicable access points for broken antennas, status lights indicating fault conditions, and insufficient electrical power. Try rebooting the access points, which often resolves firmware lockups. Make sure that the firmware is up to date, however, to minimize lockups in the future. ■