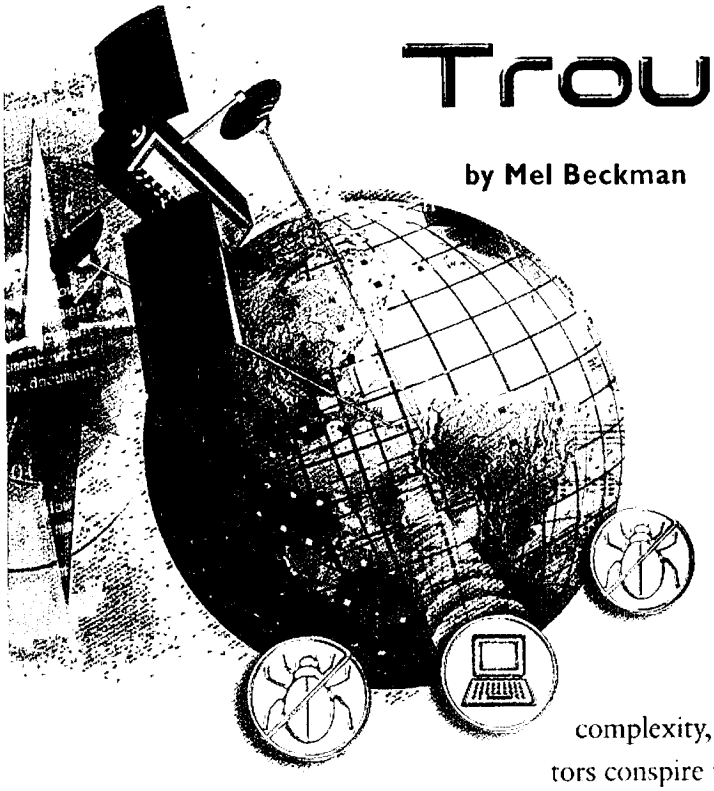


Troubleshooting Wi-Fi Networks

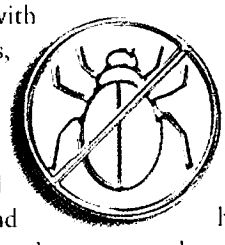
by Mel Beckman

Track down wireless networking bugs and kill them dead

MOST IT PROFESSIONALS WILL TELL YOU that wireless networks are easy to set up but fiendishly difficult to keep running well. Wi-Fi's convenience comes at the price of increased complexity, reduced reliability, and problematic security. All of these factors conspire to make Wi-Fi network troubleshooting difficult.

Because of the vagaries of RF communications, it's even more important to be systematic in your troubleshooting plan than you are with wired networking problem solving. With a well-organized approach, Wi-Fi bugs can be found and squashed, but you'll need some special knowledge and tools to get the job done.

To succeed at Wi-Fi troubleshooting, you need to understand some basic diagnostic techniques, know which Wi-Fi design factors can cause problems, purchase some troubleshooting tools, and learn a few tricks of the trade. Armed with this information and some inexpensive software tools, you'll be well equipped to kill Wi-Fi bugs dead.



Be Clear on the Approach

Before doing any Wi-Fi troubleshooting, you should consider the kind of problem you're experiencing and select one of two broad attack plans. You can then apply a few basic diagnostic tests to isolate the problem and decide on a fix. As with any network troubleshooting, however, you must be systematic. The shotgun technique — trying random possibilities in the hope you'll stumble on the problem — will only eat up your time and leave the bugs buzzing around your head.

The two classes of Wi-Fi problems are "new network" and "existing network." Ask yourself the question, "Has this ever worked?" If the answer is "no," then you're dealing with a new network and can feel free to strip the problem down to the simplest configuration. If the answer is "yes," then you're working in a production network, which requires careful incremental changes and tests to avoid breaking the network further.

If your network has never worked, you should simplify the network configuration as much as possible, get that configuration working, and then gradually add more complexity, testing each step of the way. For example, if you've just built a non-working network with five access points (APs) and 50 VPN clients, back off your setup to a single non-VPN client with a single AP. Get that working first, and then add the VPN configuration. Once you've got that running, add another AP. By incrementally enlarging the Wi-Fi topology, you'll be debugging fewer things at one time. And any change you make that breaks the accumulating network will be easy to reverse to return to a working network before your next attempt.

If your network is already in production, you can't very easily simplify it without disrupting the parts that are working. And even if you can, you shouldn't. Instead, you should follow the Golden Rules of Network Troubleshooting to isolate your problem. These three rules won't uncover every bug, but they have such a high success rate that you should consider them before doing anything else. The rules are as follows:

1. *It's the Cable, Stupid.* "What?" you ask. "The cable? But this is a *wireless* network — there are no cables!" Wrong! "Wireless" networks have plenty of cables. And just as it is with networks everywhere, cables are the number one cause of network troubles. If there's a single cable associated with the device you are having trouble with, such as the cable between a failed AP and your LAN switch, then *replace it before going any further.* Because cables fail so often, and can fail in such subtle ways, it's important to rule out cabling before moving on to more time-consuming problems.
2. *It's the Last Thing You Did.* The network was working, and now it's not. What did you do? Experience shows that whatever change you last made to your network has a high probability of being the cause of your current problem. The quickest way to rule out this cause is to simply undo the

most recent change. For example, if you changed the client's Wi-Fi configuration, or an AP's settings, or even just the name of your VPN server, try reversing that action to see if your problem disappears. No matter how innocuous the alteration, check it to make sure you've eliminated this common cause of trouble.

3. *Only Change One Thing at a Time!* The exclamation point is on this rule for a good reason: you'll be very tempted to ignore this rule in the heat of battle. But you must be strong and resist the urge to short-circuit systematic testing. If you change two (or more) things and your network starts working, you'll still have to go back and test each of those changes individually anyway. The vast majority of networking problems have a single cause; changing many things at once will only obscure that cause. An important corollary to this rule is that after making a change and testing it, if the change didn't help, *reverse it* to restore your network to its original state before you go on to the next test.

If you take this advice to heart, you'll consistently find solutions to your Wi-Fi problems. With these guidelines in mind, you're ready to learn some basic troubleshooting techniques.

Basic Communication Tests

If your problem is that one or more devices simply can't communicate on the network, then a short checklist of basic tests will help you narrow down the problem:

1. **Verify that your client device has established a Wi-Fi association.** You can check this in the client's Network Adapter control panel and in the AP's list of associated devices. The latter check requires that you know the Media Access Control (MAC) address of the problem client. If you don't have an association, nothing else you do will solve your problem. You must establish an association first. Verify that the SSID in the client matches that of the AP, that the AP isn't filtering clients by MAC address, and that the client and AP are communicating on the same 802.11 channel. Every Wi-Fi network should employ two-way authentication and data encryption, so verify that your authentication values (VPN user ID and password or digital certificate) and encryption keys are correct. Don't depend on WEP or WPA for Wi-Fi security (see "WEP and WPA Can Be Harmful," below). You should also ensure that the signal strength is adequate. If possible, move the problem client closer to the AP to see whether that solves the problem.
2. **Verify the client's IP address.** In Windows, use the command-line IPCONFIG command to display the assigned IP address. If the IP is statically configured, make sure the subnet mask

WEP and WPA Can Be Harmful

The first 802.11 access points (APs) sported an encryption technology called Wired Equivalent Protection (WEP). Initially operating with 64-bit keys (later enhanced to 128-bit keys), WEP suffered from fundamental flaws in its RC-4 encryption algorithm that let persistent crackers defeat it after a few hours of traffic analysis. This was decidedly not equal to wired protection, and WEP became a source of embarrassment for Wi-Fi vendors. Worse, WEP uses the same shared key for every client, so once hackers crack one client, they have access to them all. A third problem with WEP is that it slows AP performance due to the computation complexity of the encryption involved.

A supposed fix to WEP came along in the form of a standard called Wi-Fi Protected Access (WPA). WPA used the same flawed RC-4 encryption as WEP to permit users to upgrade existing APs to the new standard but changed the encryption keys periodically, making the interloper's job more difficult. Unfortunately, WPA still used the same shared key with every client and defaulted back to the first shared key whenever a client tried to use an invalid key, which means an attacker can inject spoofed packets to cause the client and AP to revert to the first SSK at will. After capturing enough traffic, the hacker can recover the original key, and WPA's protection is lost.

Although stronger than WEP, WPA is not strong enough. It's also not user friendly. Its improved security depends on the enterprise deploying a complex public key infrastructure (PKI) and users choosing good starting keys, practices not enforced at all by the standard or by any current implementation. Users choosing keys from known dictionary words are vulnerable to offline cracking, in which a hacker analyzes a large volume of recorded Wi-Fi traffic to deduce the encryption key. WPA also adds to the computational load on the AP, making it difficult for a WPA-protected AP to support a large number of protected clients.

An alternative approach that addresses all of the problems of both WEP and WPA is to use existing VPN technology to encrypt traffic from the Wi-Fi client through the AP to a VPN server on the wired LAN. This has the advantage of removing the security burden from the AP and leveraging an authentication infrastructure already in place at most enterprises. Every client has a unique key, and both sides of the conversation are authenticated, preventing AP spoofing. VPN-based encryption has the advantage of being built in to the operating systems for most all wireless devices.

Wireless switches have become the natural control point for Wi-Fi-oriented VPNs, and Wi-Fi vendors have rallied to support open VPN protocols, such as IPSec (see "Buyers Guide: Wireless Switches" on page 30). Centralized VPN encryption also simplifies wireless roaming because no security re-association is needed when wireless clients move from one AP's coverage to another's. However, you don't need a wireless switch to use VPN protection in your WLAN. You can construct a reliable VPN server from an old Windows 2000 server, following the instructions posted at *dridoctor.com*. Alternatively, you can use a VPN security appliance, such as the Cisco VPN 5000.

— *M.B.*

is set correctly. If the IP is dynamically assigned by Dynamic Host Configuration Protocol (DHCP), verify that the correct DHCP server supplied the address. If the client hasn't received a DHCP assignment, or it has a self-assigned 169.254.x.x address, try temporarily assigning an unused static IP address to see whether that restores connectivity. You can then concentrate on diagnosing the DHCP problem. In both cases, confirm that the active interface is in fact the wireless adapter. On most clients, if a wired interface is available, it will take priority over any wireless path.

3. **Verify the client gateway address.** If the gateway address isn't set correctly, you won't be able to communicate via your local wired LAN. In Windows, you can check this with the IPCONFIG command or with the NETSTAT –R command. Note that the gateway address *must* be in the same logical subnet as the client's IP address. Inspect the client subnet mask closely to verify that the gateway is in fact in the same subnet.
4. **Verify the client name server settings.** Often a client's connectivity is fine, but the configured name servers are either incorrect or unreachable. You'll check reachability in an upcoming step, but you should be able to confirm the name servers are configured correctly by inspection.
5. **Ping the AP.** If your APs are on the same logical network as your clients (they don't have to be in a bridged configuration), attempt to ping the AP from the client. If you can't get a response, there is likely an RF signal quality problem preventing communications. Check out the later suggestions for identifying network design and interference problems. If you can ping the AP, then you've at least established that the RF link is functional. Ensure that you don't experience serious packet loss when varying the size of ping packets in the ping command (but don't attempt packets larger than the Ethernet maximum of 1,500 bytes).
6. **Ping a local IP address.** Locate another device on your wired LAN and ping it. If this fails, then the AP may have a problem communicating with the LAN. Suspect a bad cable, and check basic LAN connectivity issues in your Ethernet switch. Common problems are incorrect Ethernet rate settings (e.g., 10 Mbps vs. 100 Mbps) or nonmatching duplex values (half- vs. full-duplex). In general, it's a good idea to statically set Ethernet speed and duplex, rather than to depend on the notoriously problematic autoconfiguration capabilities of your Ethernet switch. If you can ping a local address reliably, you're most of the way to a working connection!
7. **Ping the gateway address.** If you can't reach the gateway, the client can't communicate outside of the local LAN. Verify that the gateway is operational and that the subnet mask configured in the gateway matches that configured in the client. Also check any intervening devices and cables to rule out transport failures in your LAN.
8. **Ping the DNS servers.** This isn't always possible, especially if your DNS servers are behind a firewall, which often blocks pings for security reasons. If you can't ping DNS, but other wireless clients can, then you should suspect a routing problem or transport failure on the path to the DNS server. However, if you can ping a DNS server, and the server is on a different network, you'll have confirmed that you have off-network routing.
9. **Perform a DNS lookup.** DNS is essential for general Internet access because without it the client can't translate fully qualified domain names to destination IP addresses. Even if you can ping a DNS server, the server may not be correctly handling DNS queries. Use the NSLOOKUP tool in interactive mode to send a known query to the DNS server and verify its response. For example,

```
NSLOOKUP
>server 192.168.5.10
>www.mit.edu
  NAME: DANDELION-PATCH.mit.edu
  ADDRESS: 18.181.0.31
```

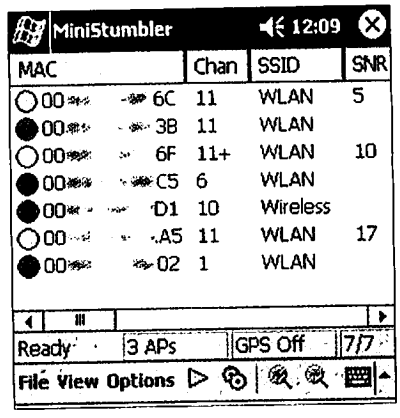


FIGURE 1
A typical scanner running on a PocketPC PDA

As an adjunct to this checklist, you should collect any vendor troubleshooting documents unique to the client or AP devices you employ. Microsoft has a very comprehensive troubleshooting guide for Windows XP wireless clients (see "Wi-Fi Troubleshooting Tools," page 24). If the checklist fails to isolate your problem, you'll have to check other likely causes, such as network design deficiencies or radio frequency (RF) interference. For these tests, you'll need a few dedicated Wi-Fi troubleshooting tools, which are next on the agenda.

A Wi-Fi Troubleshooting Tool Kit

Wi-Fi–specific troubleshooting tools help you measure Wi-Fi signals, verify network coverage, detect interference from other networks, and monitor the traffic in your Wi-Fi realm. You may be able to construct these tools by combining hardware you already have on hand with free software. Or you can purchase off-the-shelf tools tailored specifically for certain diagnostic chores. The directory in "Wi-Fi Troubleshooting Tools" lists a number of free and commercial wireless LAN (WLAN) problem-solving solutions. Here are the tools you'll need:

- **Signal Scanner** — This is nothing more than a portable Wi-Fi

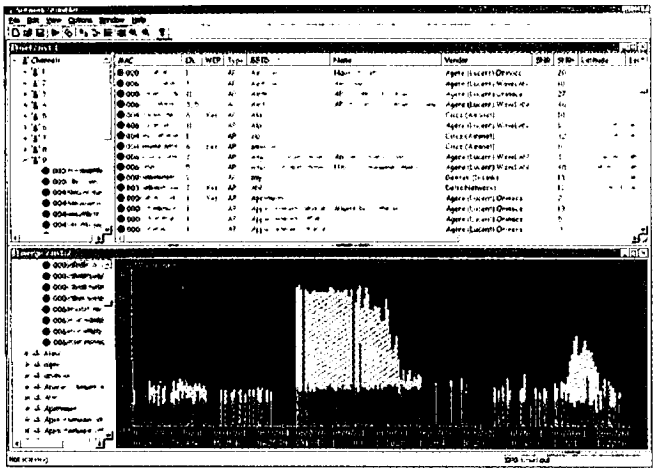


FIGURE 2
NetStumbler freeware can provide useful information

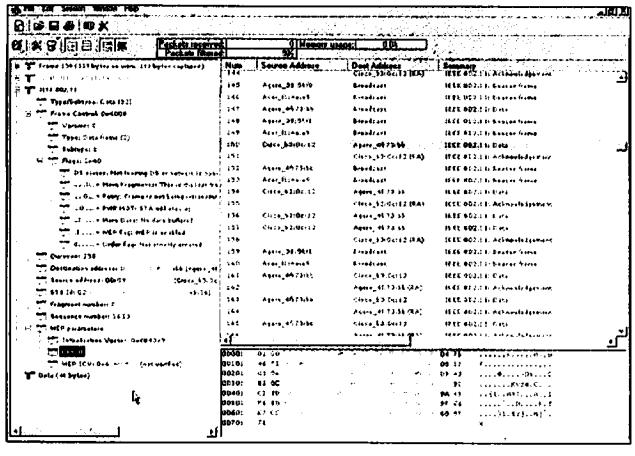


FIGURE 3
Etherreal is an open-source packet sniffer

client with the same Wi-Fi configuration settings used by your regular user clients. A PDA with built-in 802.11 networking makes an excellent scanner. You can roam your facility, monitoring signal strength to each of your access points to verify adequate signal coverage, and you can establish working associations with APs. Some PDAs, and most any notebook computer, will also be able to provide the necessary authentication credentials to establish a secure connection into your WLAN. You can enhance this tool by adding network discovery software, such as NetStumbler or miniStumbler. Figure 1 illustrates a typical scanner running on a PocketPC PDA. (Please note that the distortions in all figures for this article are deliberate to obscure sensitive actual information.)

- Network Discovery Tool — This is the same tool used by hackers engaged in so-called war driving, the practice of traveling around cities looking for unsecured wireless networks in homes and businesses. You'll use this tool to measure signal strength and to identify neighboring networks that may be interfering with your own WLAN and to detect rogue APs.

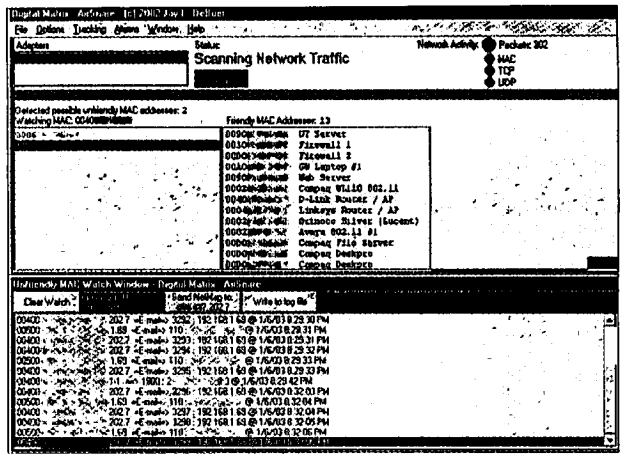


FIGURE 4
AirSnare monitors networks for rogue clients

Typically you'll need the power of a notebook computer to get the full benefit out of this troubleshooting aid. Figure 2 shows the popular NetStumbler freeware in action.

- Packet Sniffer — This is the equivalent of a LAN packet analyzer, which is able to capture packets exchanged by clients and APs and decode them. However, a Wi-Fi sniffer incorporates the additional logic necessary to identify associations between clients and APs and to decode the additional packets WLANs use to moderate wireless communications. Some Wi-Fi packet sniffers have the intelligence to warn of potential intrusions, but few are as sophisticated as dedicated security scanning tools, which is the last tool in this list. Figure 3 depicts the open-source Etherreal program.
- Security Scanner — A security scanner is a combination Wi-Fi network discovery tool and packet sniffer, plus analysis software designed to scan your network for vulnerabilities. These are sometimes termed intrusion-detection or vulnerability assessment tools. You can perform some security scanning tasks using the previously mentioned tools, but you'll only be able to verify that your network is safe at the time you run the manual scan. A security scanner is on the job full time, constantly monitoring your network for intrusions, misconfigured devices, rogue access points, and other security issues. The scanner will alert you when it detects a problem. At a minimum, you should have a basic scanner on hand to conduct local security surveys. Ideally, though, you'll employ such scanners throughout your network to continuously watch for security compromises. Figure 4 shows the AirSnare rogue-client monitoring tool.

Read on to see how you'll use these tools in real-world troubleshooting scenarios.

Designed to Fail?

Because Wi-Fi networks are so easy to set up, they're often constructed without much attention to design details. As a result, as the network grows, it gradually strains the limits of Wi-Fi capabilities, eventually becoming unreliable and slow. You can exterminate these pests in advance by carefully designing your

Wi-Fi network before deploying anything. If your network is already built, you can usually tune it up by improving AP placement, installing appropriate antennas, and adding proactive quality measurement systems. Here's a rundown of the most common Wi-Fi design flaws and their fixes:

- **Location, Location, Location** — The first priority in WLAN design is proper AP placement, but many network administrators are lulled by the apparent simplicity of wireless devices into thinking that they can worry about this problem later (or ignore it altogether). It's not uncommon to find APs strewn about an office willy-nilly, placed on file cabinets and in potted plants and periodically rearranged by the nightly cleaning crew. A quality network design starts with a wireless survey to determine the best location for each AP and the best antenna to match the coverage required. To accomplish this task, you experiment with AP locations and antenna types while monitoring coverage and signal strength using your signal scanner.
- **Antenna Type and Tail** — You should pay special attention to antenna selection and orientation because poor antenna installation can both degrade an AP's performance and interfere with neighboring APs. Antennas come in two types: omni-directional and gain. An omni antenna radiates uniformly in all directions on a single plane. Contrary to common belief, a gain antenna doesn't actually amplify the signal at all. Rather, a gain antenna directs the signal more in one direction than another, resulting in a stronger signal (hence the term "gain") and less neighboring interference. Gain antennas have varying coverage angles, from 130-degree planar antennas to one-degree parabolic dishes. In office environments, you should choose antennas designed for ceiling or wall mounting to keep them out of harm's way and to minimize signal attenuation from office furnishings and occupants. The tail of the antenna (the coaxial cable from the AP to the antenna itself) is also an important factor. It should be as short as possible and designed specifically to match the AP and antenna in use. Usually Wi-Fi tails cannot exceed three or four feet in length without seriously weakening the RF signal. This means that your AP must be located very close to the antenna. One way to conveniently accomplish this is to use Power Over Ethernet, which sends electrical power to the AP through your existing Internet cabling, thus letting you more easily place APs in out-of-the-way places.
- **Density Dilemma** — Sometimes a network works fine with a few users but bogs down when the client population increases. The most common reason for this is insufficient AP density to meet the demand. AP density refers to the number of APs in a given area. Although APs have a range of 100 to 200 feet, that doesn't mean you should always spread them out with this kind of spacing. Remember that each AP can communicate with only one client at a time and that all the clients associated with the AP share the available channel bandwidth — about 7 Mbps for 802.11b and 22 Mbps for 802.11a and g. The division isn't linear, either, because each user adds protocol overhead to the channel that further reduces available bandwidth. Thus, four users on an 802.11b network might get only 1 Mbps each because of traffic management signaling. If you put one AP in your 40-user training center, then each user will be getting modem-like performance as the AP apportions the bandwidth among them. The solution is to position more APs operating on noninterfering channels to accommodate a higher user population.
- **Mixed Company** — One convenience of 54 Mbps 802.11g networks is that they can support older 11 Mbps 802.11b clients. But "can" doesn't mean "should." When an 802.11g AP permits associations with 802.11b clients, all clients use the slower 802.11b signaling rate for routine session management traffic. This slows performance for high-speed users considerably. The performance loss isn't significant unless the AP is carrying many users. If that's the case on your network, consider installing a separate AP for 802.11b users configured to use an appropriately noninterfering channel. You can use a network sniffer to identify dual-speed networks. If the networks are carrying many users, it's time to give your 802.11b users their own "slow lane."

Running Interference on Interference

After design deficiencies, the next most common cause of Wi-Fi problems is interference. As you may now realize, a good design can minimize interference problems, but sometimes interference is independent of your design. Here is a list of the main culprits and how to identify and eradicate them:

- **Channel Changing** — Adjacent APs must be on different channels to avoid interfering with each other. The channels available for all 802.11 technologies (a, b, and g) are adequate to achieve this separation even in close quarters, but you must put some thought into your channel plan. One common oversight is to forget that RF signals go through walls, floors, and ceilings and thus can interfere with APs that are out of your purview. Use a network discovery tool to determine which APs have visibility to each other and confirm they are on nonconflicting channels. Keep in mind that adjacent channel numbers always interfere with each other. You must ensure adequate channel number separation, which varies depending on the frequency domain of your network. The degree of channel separation depends on the distance between APs and the power radiated by them.

  Available channels also vary by country. For example, the U.S. has 11 2.4 GHz channels (802.11b and g), but you can use only channels 1, 6, and 11 adjacently without interference. 802.11a has more channels, and thus a larger selection to avoid interference, but it needs that larger selection because 802.11a APs must be closer together, due to the shorter range of their 5GHz signals. You can use directional antennas and lower power settings to reduce interference between adjacent APs. Determining channel assignments is a task outside the scope of this article, but any Wi-Fi design guide can explain the process in detail.

Sometimes channel interference comes from outside your corporate borders: from a neighboring company in the same building, or from a more distant entity operating a directional antenna shooting its beam into your space. A signal scanner can help you see interfering APs outside your organization; changing channels is often the easiest fix.

- Less Power to You — A common misconception is that the more power RF your APs radiate, the better they will perform. In reality, APs should use the minimum amount of power necessary to cover their assigned area and no more. Additional power increases the likelihood of neighborly interference and can cause clients to switch between APs too frequently. Not all APs have the ability to control transmit power, but if you can select APs with this feature, you'll have an important trick up your sleeve for solving interference problems.

Reducing power can also mitigate interference in multitenant

Wi-Fi Troubleshooting Tools

Whitepapers

"Microsoft's Guide to Troubleshooting Windows XP 802.11 Access"
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifitrbl.asp

WildPacket tutorial on rogue access point detection
http://www.wildpackets.com/elements/whitepapers/RogueAccessPoints.pdf

Open-Source (free) Software

AirSnare
Shareware Windows tool that monitors wireless networks for unknown MAC addresses, to identify rogue clients and access points, alert you to their presence, and monitor their activities.
http://home.comcast.net/~jay.deboer/airsnare/

AirSnort
A Linux-based open-source Wi-Fi packet analyzer that cracks WEP keys.
http://airsnort.shmoo.com/

Etherreal
Freeware Windows and Unix network analyzer with the ability to capture and decode packets from wireless networks.
http://www.ethereal.com/

NetStumbler
A freeware (but not open-source) Windows- and Mac-compatible Wi-Fi network discovery tool. The Mac version is called MacStumbler; a PDA version, miniStumbler, runs on PocketPC-based devices.
http://www.stumbler.net/
http://www.macstumbler.com

Kismet
A Unix-based passive network monitoring tool with the ability to crack WEP keys. Versions exist for Linux and Macintosh OS X. The Mac version is called KisMac.
http://www.kismetwireless.net
http://www.binaervarianz.de/projekte/programmieren/kismac/

Commercial Hardware and Software Products

AirDefense
Hardware-based network security monitor
http://www.airdefense.net/

AireSpace
Wireless-switch–based intrusion detection system
http://www.airespace.com

AirMagnet
Handheld, laptop, and distributed network scanners
http://www.airmagnet.com

AiroPeek
Wireless network protocol analyzer
http://www.wildpackets.com/products/airopeek

AirXone
Wireless intrusion prevention service
http://www.vigilantminds.com/services/wireless.htm

Border Guard Wireless
Software-based intrusion detection system
http://www.stillsecure.com

Network Associates Sniffer Wireless
Wireless network protocol analyzer
http://www.networkassociates.com/us/products/sniffer/wireless/sniffer_wireless.htm

Neutrino Distributed Wireless Sensor
Hardware-based Wi-Fi network security monitor
http://www.networkchemistry.com/products/neutrino

Red-Alert
Hardware-based intrusion detection system
http://www.red-m.com

Wi-Fi Watchdog
Software-based intrusion detection system
http://www.newburynetworks.com

WiSentry
Software-based intrusion detection system
http://www.wimetrics.com/products.htm

offices. If you are causing interference, you should be willing to lower your power to ameliorate the problem. Hopefully, your channel-infringing neighbor will be equally gracious.

- **Unfriendly Officemates** — The least common form of interference, but one still worth evaluating, is RF interference (RFI) from other wireless devices sharing the frequency spectrum with your WLAN. Microwave ovens, 2.4-GHz cordless phones, and BlueTooth devices all generate RFI that affects Wi-Fi equipment. Microwave ovens are the least offenders because a well-shielded unit should radiate very little stray 2.4 GHz energy. Microwave ovens also operate on a 50 percent duty cycle, meaning they generate interference only during one half of every 1/60th second A.C. cycle, limiting their worst-case effect to a 50 percent Wi-Fi speed reduction. 2.4 GHz cordless phones, however, can put a complete kibosh on your Wi-Fi parade and should be excluded from your office environment altogether. Because alternative frequencies are available for cordless phones, this usually isn't a serious limitation. The last offender, BlueTooth, is becoming a more common problem as BlueTooth headsets, modems, GPS receivers, and other continuous transmitters proliferate. You may have to exclude BlueTooth devices from your workplace.

802.11a networks operate in the much less crowded 5 GHz frequency spectrum, making them less vulnerable to interference. However, 802.11a operates over a shorter range than 802.11b/g and has less penetrating power for overcoming office obstructions. The increased density requirement for these networks and the higher cost of components makes them less cost-effective than the 2.4 GHz duo. Because RFI is not a frequent problem on 802.11b/g networks, most wireless users never consider the 802.11a option.

Alas, if you are suffering from RFI, tracking it down can be very difficult without specialized expensive equipment. If an offending device isn't operating in plain sight, you'll need an RF spectrum analyzer to find it. These cost thousands of dollars. One way to mitigate RF noise is to promulgate enterprise-wide policies about the use of devices with interference potential:

- **Rogue's Gallery** — One interference that you may not immediately identify is the rogue AP and client. A rogue AP is an AP installed on your network without your knowledge or permission. Usually this is an accident perpetrated by a well-meaning employee just trying to take advantage of the convenience of wireless, but not always. A rogue client is one not belonging to an authorized user but that's attached to your network using authentic security credentials. A rogue client means that your WLAN security has broken down or the security of the encryption keys has been compromised.

Wi-Fi APs are cheap and trivial to install, so even nontechnical users turn to them as an easy solution to network cabling problems. Sometimes a rogue AP is malicious, however, an attempt to trick legitimate users into giving up passwords or other security credentials or as a way to pass company secrets, in the form of audio recordings or data files, off the premises.

Rogue APs are a serious problem because they're connected directly to your physical wired network and thus have access to all your corporate jewels. A naive rogue installer likely will configure no security on the illicit AP, leaving a gaping hole in your network waiting to be exploited by a circuit-riding war driver. A malicious rogue installer could set up a "honey-pot" (a device intended to look like an authorized AP but with special monitoring software to capture sensitive information) that compromises the integrity of your entire enterprise network.

Unfortunately, rogue APs and clients are very hard to find without a dedicated intrusion detection system. WildPackets, the makers of Etherpeek, have written a comprehensive whitepaper describing an approach to detecting rogues manually (see "Wi-Fi Troubleshooting Tools"), but the process is tedious and imperfect. If the rogue AP is configured as a wireless bridge, its MAC and IP addresses will likely not even appear on your LAN, making it impossible to detect from the wired side.

The only way to find a rogue is to capture its wireless traffic and recognize it as not belonging on your WLAN. One rogue client detector (the freeware AirSnare) runs on your wired network, watching for MAC addresses that aren't on a preapproved list. However, MAC addresses can be spoofed, so this is not a foolproof defense. Some wireless switches can perform rogue detection by listening to your network through your existing APs (see "Buyers Guide: Wireless Switches," page 30). You can also buy dedicated Wi-Fi vulnerability assessment tools that employ separate hardware sensors spread throughout your network to listen for rogues, detect misconfigured clients, and identify network vulnerabilities. Because such sensors are receive-only devices and don't have to establish two-way communications, you don't need to place them as densely as your APs. A WLAN with 10 APs might require only two or three security sensors.

Preventive Medicine

You don't have to wait for your network to break before using your newly acquired Wi-Fi troubleshooting skills. You can start experimenting with diagnostic tools today, examining your network's current behavior and getting a feeling for its baseline performance. You can also review your network design and upgrade it by improving AP placement, antenna installation, and channel assignments. You're also well advised to detect, find, and repel intruders before they've gained a foothold in your WLAN, so select and deploy a Wi-Fi intrusion detection system now before serious problems arise. ■

Mel Beckman is a senior technical editor for iSeries NEWS.