



Wireless that Works!

By Rahul Sukumar, Senior IT Specialist

You've spent an entire year rolling out a campus-wide, ultra-redundant, high-capacity, ultra-secure wireless network. You followed best-practice guidelines in regards to access point placement, density, and security. Additionally, you had the wireless vendor double-check your implementation plan. But something's just not right... Your users are complaining of dead spots, poor performance, and dropped connections - definitely not something you expected from an enterprise-class system! Looking into the configuration of your switches, access points, and wireless devices only leads to dead ends. What could be wrong? Below you will find some not-so-obvious solutions to common wireless woes.

Dead Spots

The most obvious cause of dead spots is lack of RF coverage, but simply adding more access points in a trouble area may not be the best solution. Strategic placement of access points is more important than one might think – changing the angle of an antenna by 30 degrees may be enough to shed more RF “light” down a dark hallway.

Antenna types also play a big role in determining coverage. Using an AP's built-in antenna in a long, narrow corridor might be less effective than using an omni-directional antenna mounted horizontally on a wall.

Poor Performance

Numerous factors can affect the performance of your wireless network including weak signal strength and low-end hardware in your devices. But RF interference may be the single biggest drag on throughput (and one of the easiest to fix). You're probably familiar with the usual culprits of this bothersome phenomenon (microwave ovens, cordless phones, etc), but it's also important to remember that your network may be interfering with *itself*.

Although the FCC has allocated 11 channels to the 802.11b/g standard, just 3 of them are completely non-overlapping. If you have 3 access points in a room, and assign them channels 1, 6, and 11, no interference will occur. However, adding a 4th access point to the mix will force two of these radios to fight for the same frequency, resulting in a substantial performance hit. And depending on their sensitivity, your wireless devices may get confused by the interference and drop their connection altogether. Using a wireless monitoring tool, such as NetStumbler, will allow you to analyze the number of access points your wireless client can see in a given area (and which channel those APs are operating on). Even if your pre-installation site survey planned for low interference from neighboring access points, traditional methods used during the survey likely ignored interference from radios located on adjacent floors. Manually adjusting power levels and channels on access points can help reduce interference, if not eliminate it.

Also keep in mind that wireless networks are only as strong as their weakest link. For example, if you have placed an access point on the 8th floor near a window that overlooks the park, wireless devices may successfully connect to your network from several blocks away. However, since signal strength at that location will be very weak, clients that connect will be forced to use extremely low data rates, effectively slowing down everybody else while the access point “waits” for that one slow client. Solving this problem could be as simple as changing a setting within your access point or wireless switch: set the minimum allowed connection rate to 50% of the maximum.

Dropped Connections

Like poor performance, dropped connections can occur for any number of reasons. Some are relatively obvious (interference, for example) but some are a little harder to identify. Dropping a connection while a device is stationary can be indicative of a hardware problem. Flashing to the latest firmware and/or upgrading device drivers could improve stability.

Dropped connections while roaming, though, are especially frustrating. Assuming you've already ruled out hardware problems, configuration errors, and interference, try using multiple wireless network cards from different manufacturers to see if the problem is consistent among different chipsets. Intel® wireless chipsets, commonly integrated into Centrino® based laptops, have been widely reported to suffer from “sticky-client

syndrome” where the device fails to roam to another, closer access point even if it’s currently associated AP is several hundred feet away.

The authentication/encryption mechanisms you employ on your WLAN will also have a significant impact on a device’s ability to roam seamlessly. WPA with 802.1x authentication, for example, must go through multiple steps before successfully associating with an access point. If problems are encountered during any one of these steps, authentication will fail and the whole process will start over again, leading to connectivity interruptions. You could solve this problem by moving to a quicker authentication and/or encryption method, but you’ll be compromising the security of your network. Thankfully, emerging standards are on the way to help resolve these issues without sacrificing security. WPA2, based on the 802.11i amendment to the 802.11 standard, has certain provisions that should greatly improve security and roaming ability.

Wireless networks will probably never be as reliable as their wired counterparts. But after a fair amount of tweaking, you can get pretty close; and building a stable WLAN for data devices today will help ensure reliability of future applications, such as wireless voice and location tracking. For more information on wireless technology, including details on emerging standards, visit the WiFi Alliance’s website at www.wi-fi.org. Of course, you can always contact your friends at Vitalize as well! www.getvitalized.com or call 610-444-1233 today.