FOCUS

FOCUS BRIEF

Top 7 Considerations for Your Wireless Network

James E. Gaskin | June 01, 2010

Introduction

It's a wireless world outside, with cell phones, Blackberries, netbooks, and more relying on various wireless data networks to connect and communicate. Adding or upgrading your WLAN (Wireless Local Area Network) inside the business adds flexibility, convenience, and keeps data available everywhere inside your company.

Wireless networks come at a cost, however, both in money and management time. Security concerns jump when you add wireless components to your network. So here are the Top 7 Considerations when adding or upgrading a WLAN for your business.

Considerations

1. Site Surveys and Wireless Signal Obstacles

Wireless networks aren't magic, they're radio. Just as your car radio signal drops because of distance or obstacles like buildings, mountains, and tunnels, your wireless network signal has limitations. In fact, a WLAN signal is much less robust than a radio station because of the frequency used. While a mountain will block a radio station, a file cabinet might block your network connection.

Avoid placing access points close to windows, because the signal goes through glass as easily as it goes through air. Broadcasting your network to the world invites security issues and wastes bandwidth your users need.

The most common wireless network types, 802.11b and 802.11g, are "two wall" technologies. This means the signal can only go through two normal walls before it becomes too degraded for use. Extra thick walls, or plaster walls with a steel mesh inside will degrade or stop the signal more quickly. Floors and ceilings count as wells, too, so learn to think in three dimensions while placing access points.

Placing access points intelligently will support the most users with the fewest number of access points. Start by placing access points in the middle of the office and check the signal levels. If you have only a few wireless clients to support, you may get by using a laptop with a good signal strength meter in the wireless client utility (check your results with a second and third laptop). Larger companies should invest in wireless testing tools (some software tools are free or darn cheap) to speed the process. Search for "wireless network survey tools" for a quick list of thousands of options.

Larger companies will need a site survey which can be expensive but speeds deployment and reduces the number of access points by locating them correctly. Smaller companies can usually get by without a survey if their physical location is limited. An extra access point or two goes a long way toward user satisfaction, so pad your budget a bit to ensure happier users.

2. Changes in Network Infrastructure

Adding wireless to your network requires more than just a couple of access points plugged into your existing router. In fact, wireless access points are one of the major reasons companies invest in switches with PoE (Power Over Ethernet). Placing access points on the ceiling is much faster and less expensive when you don't need to run electrical power through conduits to each location. Small companies may be able to use a single wireless access point built into their main router as their only wireless infrastructure, but you know what they say about "best laid plans." The flexibility of an extra access point or two is worth the expense.

When planning for user capacity, take into consideration more than just laptops and some wireless-enabled desktops. Will iPhone users start surfing via their WiFi interface? iPad users certainly will. Check with your phone service manager, because wireless desk phone handsets can eat up a fair amount of wireless bandwidth.

Your network hardware, software, and management processes will change more when you add wireless networking than you expect. Use the addition or expansion of a WLAN to examine and update your existing infrastructure. Bolting a new, high speed wireless network to an outdated and overworked router will only lead to complaints.

3. Router Upgrade

Your router, the connection point for internal networks to the outside world, may not be suitable for a WLAN. Even routers than don't include wireless support need to accommodate different network configurations to support a WLAN.

A wireless network will have a different network address range than your wired network, and your router must support at least two network ranges. Companies with visitors often provide a "guest network" login in the lobby or throughout the building. This requires another network address range that should be separated from all your internal network resources. After all, a guest should see your Internet connection, but not your internal auditing files.

If your router does support WLAN connections, and you've had the router more than three years, upgrading is recommended for security reasons alone. Wireless networks require authentication protocols that have changed drastically the last few years. Older routers are less secure, and often don't work at all with newer security protocols included on the most recent laptops and other devices.

Include the cost of a new router in your wireless budget. You may not need it, but better to be prepared than insecure.

4. Rethink Security

Wired networks have one great security edge: hackers have to be inside your building to connect to your network. Wireless networks, especially when configured incorrectly, broadcast to the world. Security must be ratcheted up a couple of notches when you add wireless.

Every wireless access point sends an SSID (Service Set IDentifier), a unique number attached to wireless data packets to differentiate that WLAN from others. Do not confuse this with a security measure, because changing your SSID away from the default setting, and turning SSID broadcast off, only slows down hackers by about sixty seconds. This is a network identifier, not a security tool. Change it from the default for easier internal management, but don't think it blocks anyone.

Security client tools are like using WPA (WiFi Protected Access) and WPA2 for authentication. These supersede the earlier WEP (Wired Equivalency Protocol) that wasn't, unfortunately, near as equivalent as the industry hoped. In fact, if your company handles customer credit card information, the PCI (Payment Card Industry) audits demand you use at least WPA for wireless security, or you fail the audit.

Wireless client authentication deep dives into far too many details for this discussion. Just be aware that adding a WLAN to your network requires a complete security approach, not just some piecemeal kludge to get a few laptops connected.

5. Clamp Down on Unauthorized Access Loopholes

A "rogue" access point is one that users set up for themselves, usually by going to an electronics superstore and buying a consumer router with wireless support for $30. No security, no authentication, and no management, but they blow a giant hole in your security wall.

The second way users either purposefully or accidentally destroy your security is through turning on Ad Hoc mode on their wireless client software. Early on, when Internet connections were limited, a laptop with an Ad Hoc connection helped others get to the Internet. Today they just help hackers.

Use regular sweeps with wireless monitoring tools to find and quickly close both these loopholes. Discourage such experimentation by users by including ensuring everyone who wants wireless access has it, and by offering to solve wireless problems for users immediately. Users unhappy with IT are most likely to "help" IT by creating their own wireless networks.

6. Plan for Upgrades

You may find older laptops and wireless client access cards may not support WPA2, or even WPA. That is one example of upgrades to plan for, but not the only one.

Security protocols change regularly, and updated implementations of popular security tools offer much better protection than older hardware and software. This may mean updating some firmware on your wireless access points, or replacing an older router that can't be updated. Your wireless budget needs don't stop when you turn on the network.

The most critical area to plan for is upgrading your WLAN hardware to support 802.11n, the latest wireless protocol approved for use by the standards committee. Speeds in 802.11n are many times faster than 802.11b and 802.11g, and the signals go further with higher quality. The speed and increased user count supported by 802.11n equipment is well worth the upgrade, when you get to it.

Beyond that, always plan for security upgrades. Test for security leaks, like rogue access points, regularly, and that may mean buying tools as the wireless user base increases. Keep your software, including on clients, wireless access points, and routers, up to date. Most of the time, a firmware upgrade will be enough. Be prepared that older equipment will reach a point where it must be replaced, and that point will usually be decided by a needed security upgrade.

7. Invest in a WLAN Controller

Small companies can get by managing wireless clients as they manage wired network clients: manually. This method is popular because it's cheap, not good, and more than a dozen or so users seems to be the point where the manual method becomes painful. Unfortunately, small companies tend to ignore management needs rather than upgrade to automated tools.

Larger companies, because they can amortize costs over more users, rely on automated tools. One that's critical for companies with more than a couple of wireless access points is a WLAN controller. These tools use less intelligent wireless access points but manage, configure, and secure them more completely than so called "fat" access points do. In addition, they provide a single management interface for all wireless access points and users. A WLAN controller is highly recommended as a management upgrade that saves time and increases security.

Conclusion

As in life in other areas, doing things right takes a bit more time, effort, and often money. Doing a wireless network cheap can cost you a fortune. One of the largest and most expensive data breach thefts of customer information ever, from T.J. Maxx, occurred at a retail store through their unsecured wireless network. The cybercriminals actually did their work in the comfort of their own car in the parking lot.

Done well, a wireless network offers user freedoms not possible any other way. Building a proper wireless network will be much easier when following the seven considerations presented here. Think security first, and the rest will fall into place easily.

Recommended Reading

- Hub and Spoke vs. Mesh Wireless Networks
- The Top 5 Business Networking Myths
- Networking for SMBs: 10 Things You MUST Have to Compete