

Wireless Networks

*Keeping your network running smooth and secure
with the latest security and site analyses*



A wireless network can be one of the most important features of your business, creating efficiencies, enhancing mobility, and allowing for real-time communication. To derive those benefits, there are two major aspects to wireless networks that require constant observation, security and performance. Both the security of your wireless network and optimization of its performance can have serious effects to the bottom line. However, Wireless Builders' years of wireless network experience will give your company the tools and knowledge necessary to keep your wireless network secure and fully optimized.

Wireless Security

Just as you don't want unwelcome visitors in your facility, the same holds true for your wireless network. Should someone gain access to your network, that person could possibly have access to all of your files and business information, as well as have the ability to infect your system with viruses and worms.

A wireless network's security can be compromised by weak encryption of data packets, rogue access points, and RF coverage outside of your facility. Additionally more often than not, companies will go too long without re-evaluating their wireless infrastructure.



Wireless Maintenance

Many times, additional handhelds, laptops, PDA's, and access points are added to the network to fulfill a short-term demand. While this temporary solution may solve the immediate needs, over time, the overlapping of these solutions can cause interruptions in connectivity, dead spots, and/or unnecessary redundancies. Additionally, changes in the physical infrastructure of the facility, coupled with un-installed firmware and software upgrades, can make your wireless network perform much differently than it has in the past.

The Solution

Wireless Builders has developed a process for checking both the efficiency and the security of your wireless network. This process begins with a preliminary consultation and results in your IT staff having the knowledge and tools to properly maintain and secure your network.

The wireless network analysis takes stock of your facility's wireless network and evaluates the efficiency of your network. The wireless security analysis uses security auditing tools to uncover any possible security leaks in your network.



Wireless Network Analysis vs. Wireless Security Audit Which do I need?

While both services are similar in their structure and set-up, they produce different results. The network analysis gives you information about how well your network is performing, if you are getting the most out of each access point, and also analyzes the equipment that is connected to your network. Are your batteries giving you full-day coverage, and can an additional access point bring better coverage to lacking areas?

The security analysis gives you information about how easy it is to gain access to your network, especially from unwanted individuals. Is your network reaching its security potential or are you allowing unwanted visitors to gain access to your network?

Wireless Network Analysis



Preliminary consultation -

Before the analysis of your wireless network, a wireless RF systems engineer will sit with you to gain an understanding of your network, expectations, needs, and requirements. This ensures that the work we do will meet your standards and expectations. Here the engineer will go over how your network was designed, where you want your coverage to be, how strong you need your coverage and what problems you are having with your network.



Spectrum analysis of your wireless network -

A Wireless Builders wireless RF systems engineer will walk through your facility with a handheld Spectrum Analyzer to determine the exact radio propagation at each strategic location. This activity will give a good description of possible trouble spots and uncover any objects that might interfere with your network.



Validation of infrastructure layout -

At this stage, the systems engineer will review the physical hook-up of each access point, as well as review the cabling throughout your facility. This ensures proper connection of your access points, hubs, switches, and routers.



Access point audit -

In this step, the systems engineer reviews your access points, ensuring they are up to date on firmware revisions, as well as validating their configuration. The access points are also analyzed to determine the signal propagation and threshold.

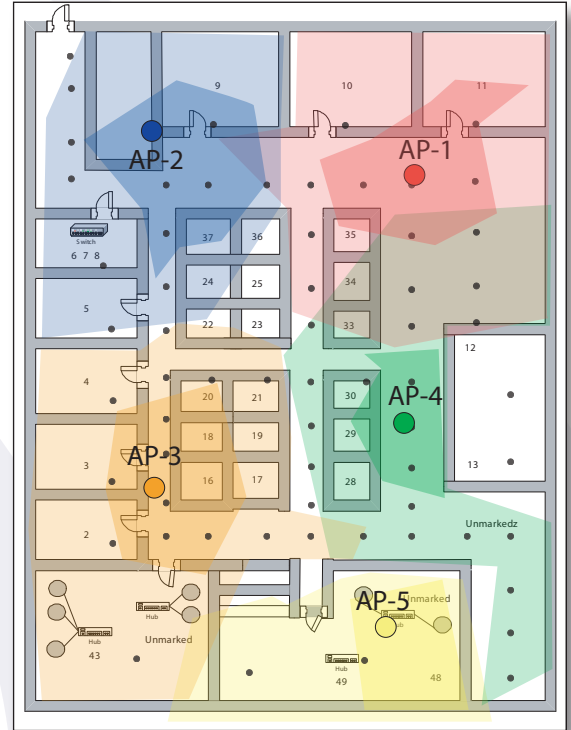


RF terminal audit (handheld & vehicle mount) -

At this point in the evaluation, the systems engineer will review all firmware, making sure it is up to date, validate configuration settings, and check open issues against known fixes in newer versions. The engineer will also check to make sure keyboards are functioning, and any vehicle mounts are securely in tact. Most importantly, the engineer will check to ensure the device has good communication with your wireless network.



Along with looking at the device, the engineer will also inspect the batteries. (It is not uncommon for batteries to start losing their ability to hold a charge.) The Wireless Builders RF systems engineer will review the batteries in your hardware devices, making sure the contacts are clean, and they can still hold their charge. A software package can be placed on each hardware terminal to monitor the charge of each device from a centralized location.



Sample Topology Diagram - a color coded AP coverage diagram illustrating redundancies, overlap, no-coverage zones (if any) and signal strengths as measured throughout the facility is part of the complete report you receive after the wireless site survey and security audit.



Wireless Security Audit



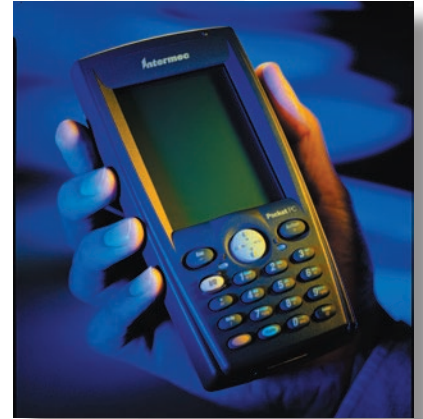
Preliminary consultation -

Similar to the preliminary consultation of the network analysis, a wireless RF security engineer will discuss the security aspect of your network, what measures have been put in place to ensure network security, how secure you need your network, what type of encryption is running and what type you need. Here your expectations, needs, and requirements will be discussed.



Security audit of your wireless network -

A Wireless Builders RF security engineer will walk around your facility using security auditing tools that essentially try to gain access to your wireless network without authorization. This step is important in understanding how secure your network currently is, as well as determining radio propagation at strategic locations.



Rogue access point detection -

Rogue access points are access points that are on the network without authorization from the IT department. While they generally don't interfere with the efficiency of your wireless network, any security measures put in place can be completely compromised by rogue access points. They are typically the entry point for outsiders to gain access to your network. As in many cases, they are installed with default configurations that lack any type of security technology.



Wireless security analysis -

Wireless Builders has developed many installation methods and integration techniques to ensure your wireless network is as secure as possible. Wireless Builders security engineers take security one step further by understanding the intricacies of radio propagation throughout your facility. A security engineer will walk around both the inside and outside of your facility with a spectrum analyzer and security auditing tools to detect possible threats, as well as look for any vulnerabilities in your wireless network.

In the end, an audit of your wireless network from Wireless Builders will make all the difference in the world.

Intrusion Detection System

Wireless Builders has developed an intrusion detection system for monitoring your wireless network, its usage, as well as any outside devices that are trying to gain access to your network.

The intrusion detection system sets up a network of "drones" to monitor activity on your wireless network. Wireless drones are strategically placed throughout your facility. Inside these drones are antennas that transmit radio signals back to your server. At the server location, you can see what IP and MAC addresses are trying to gain access to your network, which access points are being used and by what equipment.

With this software solution, you can tell when someone is trying to access your network. With the GPS addition, you can physically pinpoint the location of the intruding device. This system will also detect rogue access points if they are ever added to your network.

A standard web interface allows a single user to monitor network usage, and uses e-mail and pop-up alerts to signal possible intrusions of the network.

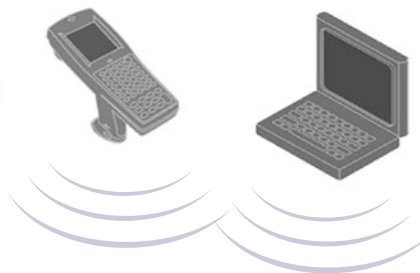
Using this system you can blacklist any MAC address to prevent unwanted individuals from jumping on your network.

Intrusion Detection System



Wireless Devices

Wireless devices, such as laptops, PDAs, portable data collectors, fax machines, and other equipment can connect to your network through a series of access points strategically placed throughout your facility.

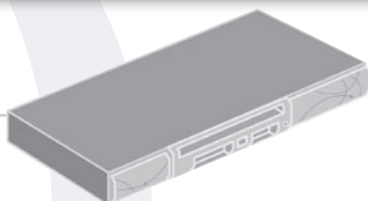
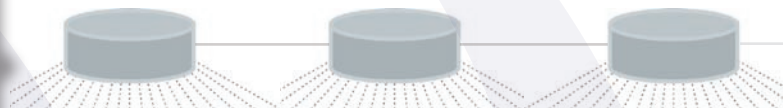


Access Points

The access point takes the information from your wireless devices and transmits it to the wireless switch which then connects to your server. The access points also send data from the server to your wireless devices.

Wireless Drones

Wireless drones monitor radio frequency activity on your network. They send data back to the intrusion detection system; this data includes what IP and MAC addresses are connected to your wireless network as well as the amount of activity and usage on your network.



Wireless Switch

The wireless switch is the central hub for all information that is transmitted between your access points and your server.

Intrusion Detection System

The Intrusion detection system gathers the data that is sent to it from the drones and passes that data on to the server. The system can either connect directly to the server or connect to your wireless switch, which would then pass the data on to the server. With the GPS addition, the location of the intruding device can be detected.

GPS Attachment



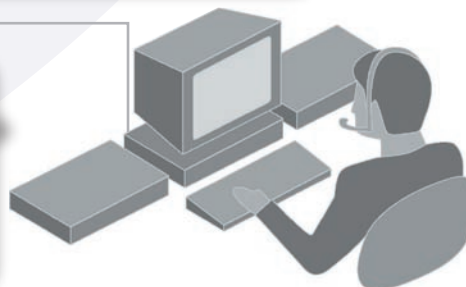
The Server

The server is the main piece of your network; the server stores and transmits data between both your hard-wired network and wireless network. It is not uncommon for many software programs to run directly from a server and to be emulated on wireless devices using terminal emulation.



Monitoring Station

The information from the Intrusion Detection System can be viewed and monitored from a central computer. Here, e-mail and pop-up alerts can inform your IT staff of possible intruders and vulnerabilities in your network.



About Wireless Builders

Wireless Builders is a world class integrator of 802.11 networks, bringing decades of experience within multiple industries, including Fortune 50 companies, to its projects. Wireless Builders specializes in the design and implementation of wireless networks in office buildings, warehouses, schools, hospitals, and other venues.

Wireless Builders' professionals are certified network engineers with the required knowledge of operating systems and protocols to design superior systems. Regardless of hardware or software, Wireless Builders will work with your company to ensure successful project.

The project management team at Wireless Builders works with you from the initial site survey to the final training of your IT staff. We also offer rapid response service contracts to keep your wireless network live.

Wireless Builders documents the key elements of your wireless network. We provide you with a detailed report so you can understand how to maintain the system. Depending on the services you require, our documentation may include: site survey results with diagrams of your facility, hardware and software specifications, photos of access points and antennas, and performance recommendations. Prospective customers, please contact us for more information.

For more information contact:

Wireless Builders
2220 Boston Street
Baltimore, MD 21231

877.ALL.WIFI (255.9434)
info@wirelessbuilders.com
www.wirelessbuilders.com

