

Locating rogue wireless access points

An unauthorized, rogue access point can compromise the security of a wireless network by exposing the company's network to the outside world. To remove this security vulnerability, the network manager must first detect the presence of a rogue AP on his network and then locate it.

The two most common search methods to find the physical location of a rogue AP are the convergence method and the vector method. Each method has its advantages and each requires different tools.

An understanding of these methods will assist the network manager in his task of keeping his wireless network secure.

[Table of contents](#)

| | |
|--|----------|
| Locating rogue wireless access points | 2 |
| Convergence method | 2 |
| Vector method | 4 |
| Methods compared | 5 |
| Practical considerations | 5 |
| Stay vigilant | 6 |
| About Fluke Networks | 6 |

Locating rogue wireless access points

A “rogue” access point can compromise the security of a wireless network. We call an access point (AP) a rogue when someone installs it without the knowledge or approval of the company’s network manager. Maybe an employee innocently brings a wireless router into the office from home to provide temporary wireless access for a meeting. A more sinister scenario is someone from outside the office installing an AP to get free internet access or to hack the network to see what they can uncover. In either case, the unauthorized AP does not have the appropriate security settings applied, either through ignorance or purposefully. Such an AP exposes the company’s network to the outside world.

Solutions are available to help a network manager detect the presence of a rogue AP on his network. However, knowing that a rogue is present is half the task. The network manager must then identify the physical location of the AP. Once found, he can remove it from the network or re-configure it with the proper security mechanism.

The two most common search methods we use to find the physical location of a rogue access point are the “convergence” method and the “vector” method. The search method you employ depends upon the tools at your disposal.

Convergence method

The convergence method is most appropriate when your locating tool kit consists of a radio card with an omnidirectional antenna and a signal strength meter. An omnidirectional antenna radiates or receives equally well in all directions. It is also called a “non-directional” antenna because it does not favor any particular direction. Figure 1 shows the pattern for an omnidirectional antenna.

A standard wireless LAN radio card for a notebook PC uses an omnidirectional antenna. In this application, an omnidirectional antenna is convenient since the signal strength will remain the same regardless of the direction you point your PC.

The convergence method also requires a signal strength meter. We use the meter to measure the RF signal from the rogue AP. The stronger the signal, the closer you are to the AP. There are several types of meters. The most common is the software utility that usually ships with the radio card installed in your notebook PC. While these simple utilities vary by manufacturer, they usually display signal strength graphically. A problem with these utilities is that it is difficult to note small differences in signal strength with their simplistic, graphical chart.

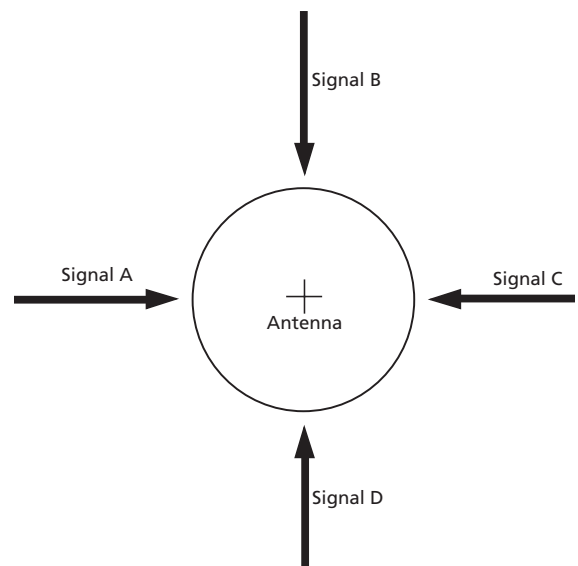


Figure 1 - Omnidirectional antenna pattern



Figure 2 - Standard WLAN radio card with omnidirectional antenna

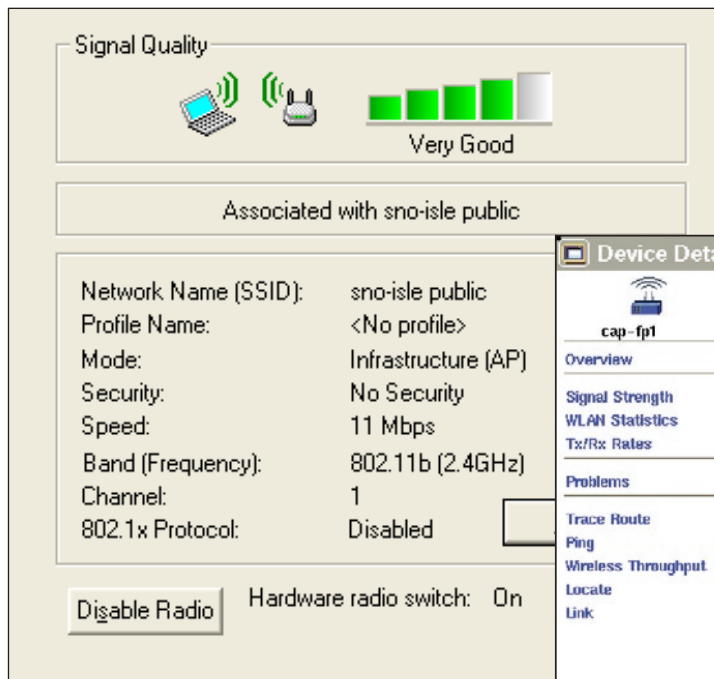


Figure 3 - Software utility signal strength meter

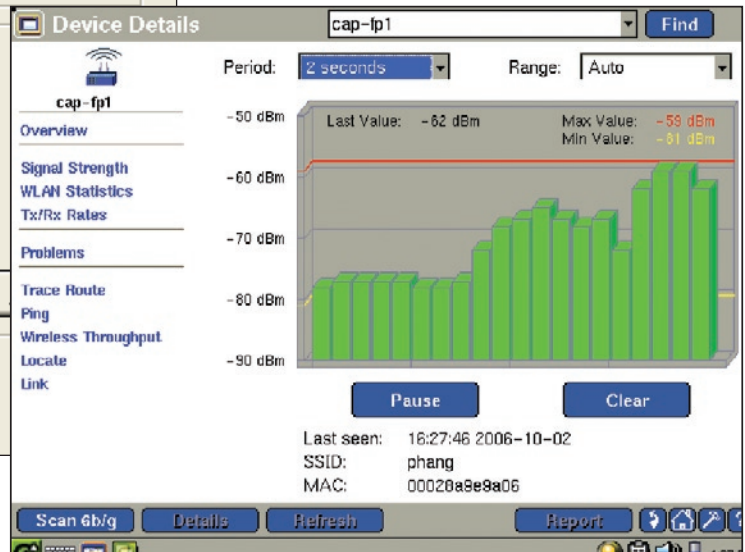


Figure 4 - Signal strength graph optimized for rogue hunting

Third-party software is also available for your notebook PC that provides better signal strength measurement capability. These third-party applications provide more detailed measurements and larger, more usable graphs. If you do not want to use your notebook PC, handheld RF signal strength meters are an option. These instruments are often designed for the rogue-hunting task and display signal strength information in a user-friendly format to speed location as in Figure 4.

To perform a convergence rogue AP search, arm yourself with an omnidirectional antenna-equipped radio card and a signal strength meter. Associate your radio card with the target AP. Walk your site while monitoring signal strength on your meter until you have a rough estimation of where to begin your rogue hunt. Mentally picture your search area as a large rectangle segmented into four quadrants. See Figure 5. Walk to one corner of your search area. Record the signal strength. Walk to the second corner. Record the signal strength. Walk to the third corner and record the signal strength. Then walk to the final corner and record the signal strength. By comparing signal strength recordings, you know that the target AP is in the quadrant with the strongest signal strength measurement – in our example, the bottom right quadrant. Now mentally picture your new search area as this quadrant segmented into four smaller quadrants. Repeat the signal strength measurement exercise for this smaller search area, moving from corner to corner and recording signal strength. In our example, the top right sub-quadrant presented the strongest signal strength. Repeat the process again, segmenting the search area into ever smaller quadrants. In our example, three segmentations – or twelve measurements – were required to get close enough to find the target AP. Additional segmentation and measurements may be required if your initial search area is larger.

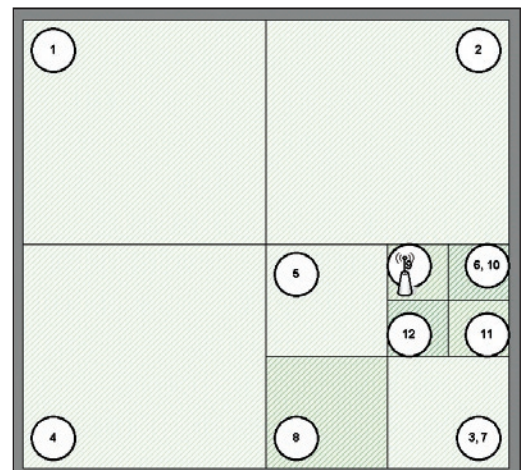


Figure 5 - Convergence method search algorithm

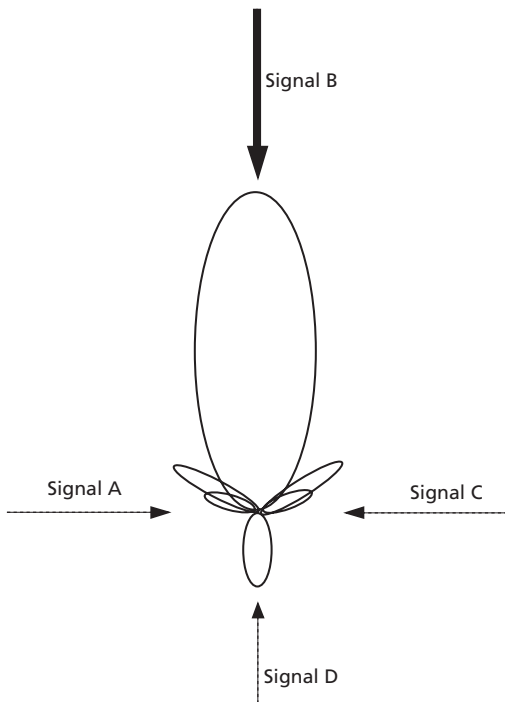


Figure 6 - Convergence method search algorithm



Figure 7 - Card with external unidirectional antenna

this smaller search area, starting at the center, pointing the antenna at each corner and recording signal strength. In our example, the top right sub-area presented the strongest signal strength. Repeat the process again, segmenting the search area into ever smaller areas. In our example, three segmentations – or twelve measurements – were required to get close enough to find the target AP. Additional segmentation and measurements may be required if your initial search area is larger.

Vector method

The other search methodology to find the physical location of the rogue access point is the “vector” method. The vector method is most appropriate when your locating tool kit consists of a radio card with a unidirectional antenna and a signal strength meter. A unidirectional antenna maximizes the signals from one direction while signals from other directions are suppressed. Figure 6 shows the pattern for an omnidirectional antenna.

There are several unidirectional antenna designs. For rogue hunting, an antenna that is external to the radio card makes aiming easier. We need a special radio card designed for such an antenna. These cards typically feature a jack that accepts the antenna plug. When connected to the external unidirectional antenna, the internal omnidirectional antenna is disabled.

As with the convergence method, the vector method requires a signal strength meter. The preferred meter is a portable instrument engineered for the task. The two search methods differ in their search algorithms.

To perform a vector rogue AP search, arm yourself with a unidirectional antenna, a compatible radio card and a power meter. Associate your radio card with the target AP. Walk your site while monitoring signal strength on your meter until you have a rough estimation of where to begin your rogue hunt. As before, mentally picture your search area as a large rectangle segmented into four areas. See Figure 8. Now walk to the center of the search area and point the antenna at one corner of your search area. Record the signal strength. From the same location, rotate 90° and point the antenna at the second corner. Record the signal strength. Point the antenna at the third corner and record the signal strength. Then point the antenna at the final corner and record signal strength. By comparing signal strength recordings, you know the target AP is in the area with the strongest signal strength measurement – in our example, the bottom right area. Now mentally picture your search area as this new area, further segmented into four smaller areas. Repeat the signal strength measurement exercise for

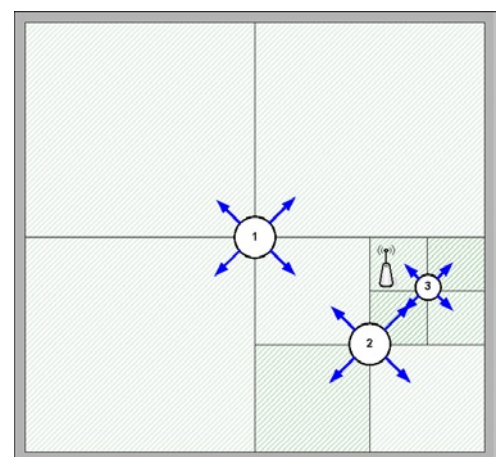


Figure 8 - Vector method search algorithm

Methods compared

In our example, the number of segmentations and measurements were the same for both convergence and vector searches. What should be obvious is that the convergence method requires much more walking about from corner, to corner, to corner making measurements. Such walking slows the rogue hunting process. A more subtle difference between methods is searching for an access point in a multi-floor environment. For example, you suspect there is a rogue AP on the second floor of your four-story office building. Using the convergence method, you identify the location with the strongest signal strength, but you cannot find the AP. Do not blame the measurements – the access point may be on another floor. On the other hand, using the vector method, you can rotate the antenna $\pm 180^\circ$ in the vertical axis to gain additional insight into which floor the rogue AP resides.

| | Convergence search method | Vector search method |
|-----------------------|---|--|
| Tools required | WLAN radio card with integrated omnidirectional antenna, RF signal strength meter | Unidirectional (external) antenna, WLAN radio card with antenna jack, RF signal strength meter |
| Advantages | Uses the most common type of radio card and antenna | Less walking speeds AP location, ability to search in both horizontal and vertical axis facilitates three dimensional searches |
| Disadvantages | More walking results in longer locating times, less suited for multi-floor searches | Requires a special radio card and antenna, generally more expensive |

Practical considerations

In practice, you will likely need to modify your search patterns to account for non-rectangular spaces and the presence of walls, cubicles and other obstructions. Try to keep the antenna at a constant height when making measurements. Holding the antenna above the height of cubicle walls may yield measurements that are more consistent. Remember to think in three dimensions when searching for access points. If you only have an omnidirectional antenna, sampling the signal strength on multiple floors should help infer on which floor to find the rogue AP. When making vector measurements, try to hold other nearby objects still (test unit, arms, body) as you rotate the antenna. It is usually easiest to mount the directional antenna to the signal strength meter (either PC or handheld instrument) and to rotate the measurement platform as a whole rather than rotating just the antenna. Practice your locating techniques using a known access point to become familiar with how sensitive your test gear is to changes in distance from the AP, antenna height, and antenna direction (if unidirectional antenna). Note that metal structures (metal studded walls, metal framed cubicles, vertical window blinds) can distort directional measurements, especially when signal strength is weak. Becoming familiar with the peculiarities of your environment should making for faster AP hunting when the need arises.

Stay vigilant

To keep your network secure, educate employees on the risks associated with setting up unauthorized APs. Update your company's policies as appropriate. Employ a rigorous network access mechanism like IEEE 802.1X. Perform routine security audits, where you look for rogue and unprotected wireless devices, to identify threats. When you identify a rogue AP, quickly hunt it down to remove this security vulnerability from your network. By following wireless network security best practices, you can minimize network security risks.

About Fluke Networks

Fluke Networks provides innovative solutions for the installation and certification, testing, monitoring and analysis of copper, fiber and wireless networks used by enterprises and telecommunications carriers. The company's comprehensive line of Network SuperVision™ Solutions provide network installers, owners, and maintainers with superior vision, combining speed, accuracy and ease of use to optimize network performance. To learn about the EtherScope Series II Network Assistant with 802.11a/b/g WLAN analysis and rogue hunting features, go to www.flukenetworks.com/etherscope.

References

Carr, Joseph J. Directional or Omnidirectional Antenna? Universal Radio Research.

NETWORK SUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to www.flukenetworks.com/contact.

©2006 Fluke Corporation. All rights reserved.
Printed in U.S.A. 11/2006 2794921 H-ENG-N Rev A