White Paper

Locating rogue 802.11n and legacy 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. A draft 802.11n home wireless router is an example of a rogue device that a network manager encounters. 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 omnidirectional method and the unidirectional 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

FLUKE networks

Locating rogue 802.11n and legacy 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 only 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.

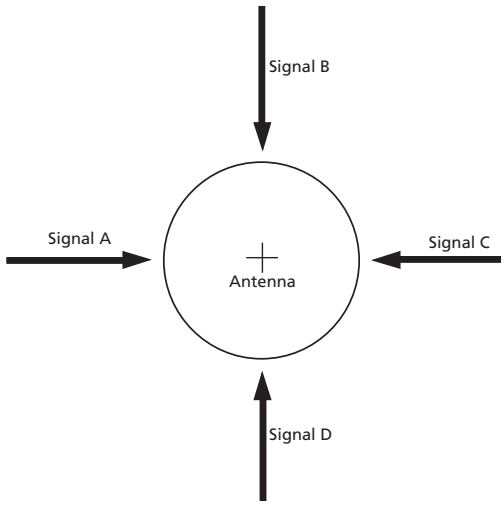

Figure 1 – Omnidirectional antenna pattern

Search tools

The network manager must arm himself with an appropriate search tool before beginning a rogue access point search. It will be quicker and easier to hunt down suspected rogue devices when armed with the right search tool. A WLAN device search tool consists of three parts: a portable computing platform, a WLAN radio card, and suitable software. The computing platform can be either a laptop PC or a handheld WLAN network tester. A PC is a general-purpose platform while a network tester is engineered for specific tasks. The WLAN radio card can be either integrated into the platform or a plug-in card (i.e. ExpressCard, CardBus). The WLAN radio card must be compatible with the target access point. For example, use an 802.11a card if hunting rogues in an 802.11a environment. Multi-application cards, like 802.11a/b/g cards, are useful when it is unclear which technology the rogue access point is using. An 802.11n radio card is generally not required for locating 802.11n access points. An 802.11a or 802.11g card works well when hunting down 802.11n access points. 802.11n access points operate in mixed mode by default, allowing legacy non-802.11n cards to identify and locate 802.11n access points. This assumes that software utilized by the search tool is written to incorporate 802.11n detection and location. Software is the final component of the search tool. Search software must be compatible with both the computing platform and radio card. As a minimum, it must provide signal strength measurement information.

Figure 2 – Standard WLAN radio card with omnidirectional antenna

Search methods

The two most common search methods we use to find the physical location of a rogue access point are the "omnidirectional" method and the "unidirectional" method. The search method you employ depends upon the search tool at your disposal.

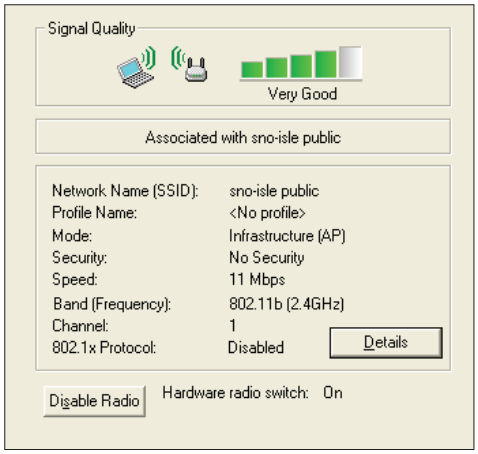

Figure 3 – Software utility signal strength meter

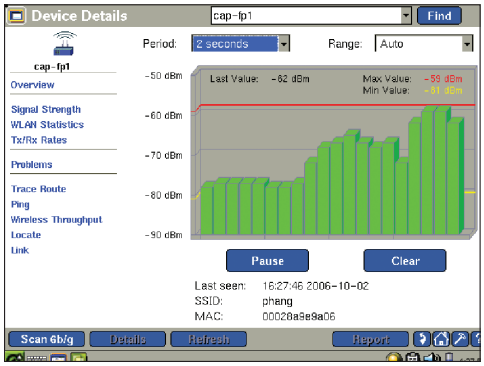

Figure 4 – Signal strength graph optimized for rogue hunting

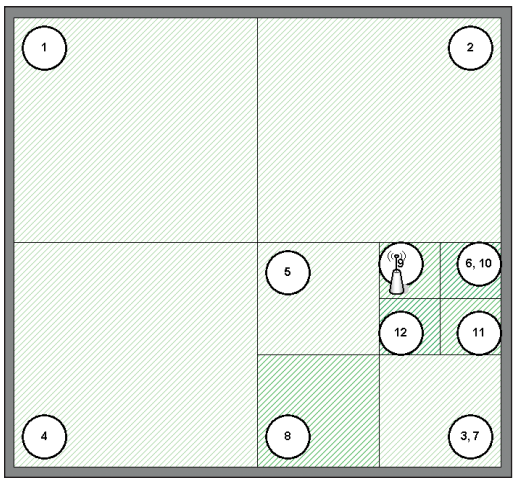

Figure 5 – Omnidirectional method search pattern

Omnidirectional method

The omnidirectional method is most appropriate when your search tool consists of a radio card with an omnidirectional antenna. 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 omnidirectional 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.

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 an omnidirectional 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.

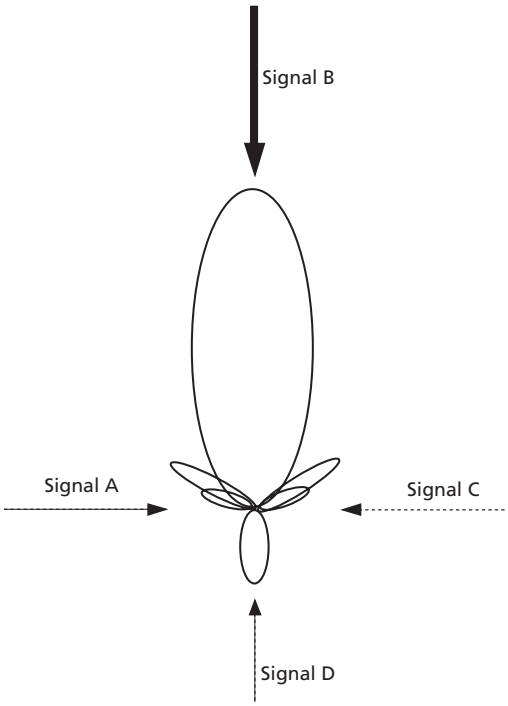

Figure 6 – Unidirectional antenna pattern

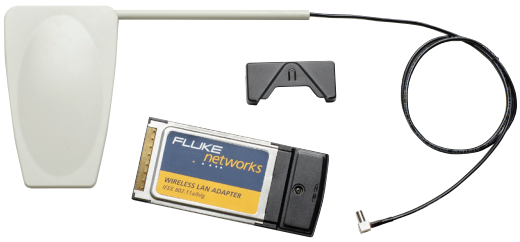

Figure 7 – Card with external unidirectional antenna

Unidirectional method

The other search methodology to find the physical location of the rogue access point is the "unidirectional" method. The unidirectional method is most appropriate when your search tool consists of a radio card with a unidirectional antenna. A unidirectional antenna maximizes the signals from one direction while signals from other directions are suppressed. Figure 6 shows the pattern for an unidirectional 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 omnidirectional method, the unidirectional 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 unidirectional 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 this smaller search area, starting at the center, pointing the antenna

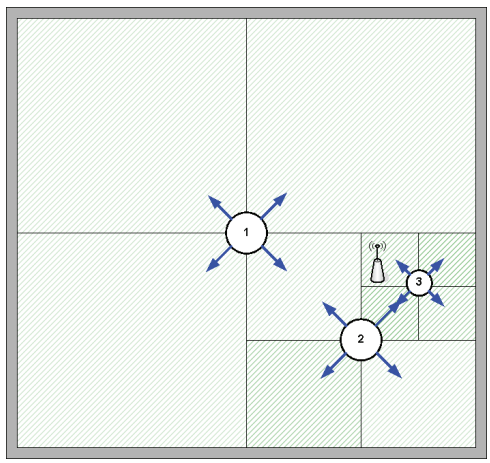

Figure 8 – Unidirectional method search pattern

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.

Methods compared

In our example, the number of segmentations and measurements were the same for both omnidirectional and unidirectional searches. What should be obvious is that the omnidirectional 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 omnidirectional 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 unidirectional method, you can rotate the antenna ± 180° in the vertical axis to gain additional insight into which floor the rogue AP resides.

	Omnidirectional search method	Unidirectional search method
Tools required	WLAN radio card with integrated omnidirectional antenna, computing platform with RF signal strength measurement software	Unidirectional (external) antenna, WLAN radio card with antenna jack, computing platform with RF signal strength measurement software
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 unidirectional 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 search tool 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. 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.

What is 802.11n?

802.11n is a draft IEEE standard with the objective of dramatically increasing the throughput of wireless local area networks (WLANs). While an 802.11b WLAN has a maximum data rate of 11 Mbps and 802.11a and 802.11g have a maximum data rate of 54 Mbps, a greenfield 802.11n WLAN can achieve a maximum data rate of 600 Mbps. 802.1n achieves this rate using MIMO technology, increased channel size, higher modulation rates, and reduced overhead.

MIMO, multiple-input multiple-output, technology is central to 802.11n. A MIMO radio has multiple antennas, each with its own transmitter, and is capable of sending multiple radio signals simultaneously. A MIMO receiver also has multiple antennas, each with its own radio. A MIMO system is comprised of a number of transmitters and receivers, typically 1 to 4. A 2x1 MIMO system has two transmitters and one receiver; a 4x4 system has four transmitters and four receivers. A MIMO system can combine multiple signals using advanced algorithms to obtain a received signal that has a much improved signal-to-noise ratio (SNR) than traditional single antenna systems. This allows much more information to be carried on the signal and recovered by the receiver. Range is also significantly improved.

All 802.11 networks operate in the same 2.4GHz and 5GHz RF spectrum, with some variation by country. This spectrum is segmented into multiple channels of certain width. Wider channels allow more information to be transmitted per cycle. 802.11b channels are 22MHz wide. 802.11a and 802.11g channels are 20MHz wide. 802.11n can optionally use 40MHz wide channels. The 40MHz wide channels in 802.11n are two adjacent 20MHz channels bonded together. By efficient use of the two 20MHz channels, 802.11n achieves slightly more than twice the data rate with 40MHz channels compared to 20MHz channels.

All 802.11 networks use encoding techniques to transmit information on the radio signal. The original 802.11 standard used phase shift key (PSK) encoding for a 1 Mbps data rate. 802.11b uses quaternary PSK (QPSK) encoding for a data rate up to 11 Mbps. 802.11a and 80211g use a different methodology, orthogonal frequency division multiplexing (OFDM), to achieve a data rate up to 54 Mbps. 802.11n continues to use OFDM but in a slightly improved manner to increase the data rate to 65 Mbps maximum for a single transmitter radio. However, 802.11n is not limited to a single transmitter. Thanks to MIMO technology, a two transmitter MIMO system can achieve a maximum data rate of 130 Mbps (2 x 65 Mbps), a three transmitter system 195 Mbps, and a four transmitter system 260 Mbps. Moreover, if the 40MHz wide channel scheme is employed, data rates are more than doubled: 135 Mbps, 270 Mbps, 405 Mbps and 540 Mbps for one, two, three, and four transmitter systems respectively.

When information is encoded on the radio signal using OFDM encoding, 802.11 utilizes a guard interval between successive transmissions to ensure that distinct transmissions do not interfere with one another, as can occur in multipath environments. This quiet period between transmissions is overhead that limits data rate. 802.11a and 802.11g use an 800ns guard interval. 802.11n can optionally use a 400ns guard interval, reducing the overhead and increasing the data rates. See following table.

802.11n also addresses the efficiency of the MAC protocol. There is a substantial amount of overhead in the MAC layer protocol. This overhead limits effective throughput. 802.11n significantly improves the MAC protocol efficiency by enhancing block transmissions, block acknowledgements, frame aggregation and interframe space.

802.11n greenfield maximum data rate				
No. Transmitters	*20MHz channel*	*40MHz channel*	*20MHz channel*	*40Mhz channel*
	800ns guard interval	*800ns guard interval*	*400ns guard interval*	*400ns guard interval*
1	65 Mbps	135 Mbps	72 Mbps	150 Mbps
2	130 Mbps	270 Mbps	144 Mbps	300 Mbps
3	195 Mbps	405 Mbps	216 Mbps	450 Mbps
4	260 Mbps	540 Mbps	288 Mbps	600 Mbps

Using an 802.11a/g radio to locate 802.11n access points

An 802.11n access point can operate in one of two modes: mixed mode and pure 802.11n mode. Mixed mode accommodates networks where 802.11a, 802.11b or 802.11g devices are present. An 802.11n access point operating in mixed mode will transmit a radio preamble and signal field that legacy 802.11a and 802.11g radios can decode. This provides enough information for legacy access points and clients to understand that another access point is transmitting, and the length of the transmission. An 802.11n access point may employ additional protection mechanisms to protect the integrity of transmissions. The cost of operating in mixed mode is additional overhead, which results in considerably lower effective data throughput for 802.11n devices operating in a mixed environment.

Most draft 802.11n APs operate in mixed mode by default. This facilitates location of draft 802.11n APs using legacy 802.11a/g WLAN radio cards. These radio cards can decode sufficient information from the 802.11n beacons for rogue AP location tasks.

References

Carr, Joseph J. "Directional or Omnidirectional Antenna?" Universal Radio Research.
http://www.dxing.com/tnotes/tnote01.pdf

"802.11n: The Next Generation of Wireless Performance." Cisco Systems, Inc.
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/ps8382/prod_white_paper0900aecd806b8ce7_ns767_Networking_Solutions_White_Paper.html

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 802.11 WLAN analysis and a/b/g/n AP rogue hunting features