

Wi-Net Window and Rogue Access Points

The Wi-Net Window (WP150) has several features that make it ideal for detecting and locating rogue access points:

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a cracker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can ignorantly or maliciously install an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind typically target open networks that are used by the general public, but they can also be used to compromise a company's internal network. These are often called an Evil Twin or man-in-the-middle attack.

In addition, there are other wireless network security issues that the Wi-Net Window can help to identify.

Detecting Rogue Access Points

The WP150 performs a continuous search for Access Points (APs) while in SCAN mode. Whenever a new AP is identified the WP150 issues an audible tone. The newly discovered AP should then be verified to determine if it is authorized or not. Thus a WP150 is essential when performing a mobile site survey to detect the presence of all access points.

The WP150 has a couple of unique features that make it even more suited for ferreting out rogue access points. These features include detecting an AP with a hidden SSID and scanning for channels outside of the regulatory domain.

Hidden SSID

Most access points have the option to not broadcast, or hide, their SSID. This essentially makes the AP "invisible" to normal computer users. The only way to connect to such an AP is to already know its SSID. Some consider this a security measure while others consider it a pain in the neck. From the perspective of a rogue access point, it is a great way to operate "under the radar" and remain undetected by a majority of wireless network users.

Ever since the release of version 1.05, the Wi-Net Window has been able to detect networks with hidden SSIDs. Because the SSID is not known, these networks are represented by a sequence of 10 asterisks, similar to a hidden password on a computer.



Since these networks are typically revealed via passive scanning, the signal strength update rate can be somewhat erratic.

Regulatory Domain Channels

The Wi-Fi specification allocates 14 channels for wireless network operation. These channels are further restricted depending on the operating domain (i.e. country). For example, the United States and Canada only allow operation with channels 1 through 11. Most of Europe allows up to channel 13 and Japan allows channels 1 through 14. Many access points can be configured for a particular domain or region.

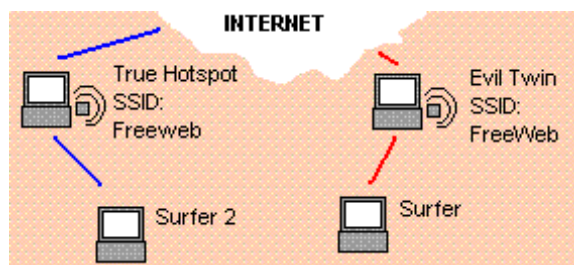
What does this mean for a rogue access point? If you want to keep a rogue access point undetected, you would set it to a channel outside of your region's channel list. For example, operating your AP on channel 13 in the US makes it undetectable by any computer that is "correctly" configured for the region.

Fortunately the Wi-Net Window passively scans all 14 channels in order to detect any operating AP. If an AP is detected above channel 11, that channel is then actively scanned to allow better signal strength measurements and subsequent tracking of its physical location (see **Locating Rogue Access Points** below).

Evil Twin

An evil twin, or man-in-the-middle attack, is achieved by creating a fake hotspot or AP. People mistakenly connect to the "evil" access point and all of their Internet transactions are thus compromised. These types of attacks are most often thought of in the context of open wireless networks in public places such as an airport or coffee shop. They can also occur if someone sets up an access point external to your facility. Then if an employee inadvertently connects to the external AP, your security is breached.

This becomes an even bigger security issue because many laptops are configured to automatically connect to the AP with the strongest signal. In most cases the computer user is not even aware what network he is connected to.



The WP150 has a couple of features to aid in detecting this potential attack. Frequently the "evil" access point is actually a laptop computer operating in ad hoc mode. Ad hoc is a mechanism in wireless networking that allows two computers to connect without the need for an access point. Many wireless drivers do not differentiate between, or identify, ad hoc connections versus access points.

The Wi-Net Window, in advanced mode, uses an **adhoc** label for any network operating in this manner. Typically ad hoc networks are rare, so detecting one is usually a cause for concern.

An ad hoc label might also appear if an employee has a laptop with a misconfigured wireless adapter. This could allow someone to externally connect to the laptop and use it to gain access to your wired network. The laptop's wireless adapter should be immediately reconfigured, or disabled, to eliminate this potential threat.

Additionally, the WP150 specifically checks for the operation of evil twin access points. When two access points are detected with matching channels and SSIDs, the network is labeled with a **t** (or **twin** in advanced mode). An audible "Twin Warn" alarm is sounded every 7 seconds when this condition exists.

The “Twin Warn” alarm is initially disabled, but can be activated in the WP150’s Audio Setup menu. The SSID comparison mechanism ignores the case of the letters, thus “**Freeweb**” is considered a match to “FreeWeb”.

Locating Rogue Access Points

Once a suspected rogue access point, or evil twin, is detected, how do you locate its physical location? There are two ways to converge on a rogue access point using the Wi-Net Window. The first is possible with a standard WP150; the second method requires additional equipment.

The WP150 has an omnidirectional antenna. This generally means that it picks up signals from all directions equally. But, the WP150’s antenna does exhibit some directional behavior that greatly helps to locate a signal source. The antenna picks up the strongest signal when it is pointing directly at the source. Therefore, hold the Wi-Net Window horizontal to the ground, in front of your body, and rotate in a circle. Once you decide where the signal source is strongest, a couple of steps in that direction should prove it by displaying an even stronger signal. In general, if you are able to move around in an environment it is not too hard to isolate the source of a signal. During this process you may need to pause occasionally in order to allow the WP150 to reacquire and display updated signal strengths.

Directional Antenna

If a more precise directional ability is desired, then a different antenna would be the next step (this is possible since the WP150’s antenna is detachable). What is required is a directional antenna that is reasonably small. That way the user can rotate the antenna and just detect signals within a small arc in front of it. A “yagi” style antenna is probably best for this, but any small directional antenna will work. The antenna doesn’t need a lot of gain (around 8dBi) and the higher gain ones tend to be larger. In some cases an additional adapter might be required to match the small antenna connector on the Wi-Net Window.

As one example, this directional antenna is meant for mounting on the side of a PC. It could just as easily be attached to the back of the Wi-Net Window.

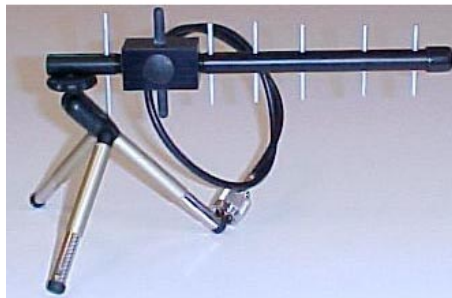


This antenna is priced around \$40 and is identified as:

WRYF2400-80 = 8 dBi Yagi Flag Directional Antenna, 2.4 - 2.5 GHz Frequency range

One source for it is at: <http://winncom.com/moreinfo/item/WRYF2400-80/index.html>

Another example is a yagi antenna attached to a small tripod:



The tripod might serve as enough of a handle, or a real handle could replace it. There are a variety of handles used in photography that are compatible with a tripod mount. This antenna is more expensive (>\$100) and is much larger than the first one. You definitely need an adapter in order to match this to the connector on the Wi-Net wireless card. One source for this antenna is:

http://store.signull.com/product_info.php?cPath=21&products_id=82

General Wireless Network Security

Concern over security has greatly increased as wireless networks have become commonplace in businesses and homes. This rapid deployment is stimulated by low equipment costs and the increased convenience of wireless operation. Unfortunately the ease of installing a wireless access point means that security settings are often ignored due to the desire to “just get it working”.

Security concerns are so prevalent that some industries have established standards for measuring security within their organization. One such group is the Payment Card Industry (PCI), which has created a Data Security Standard (DSS) (www.pcisecuritystandards.org). Essentially this is a security standard for companies that are handling credit card transactions. This is focused on securing both wired and wireless networks. Many elements of this standard are applicable to a wide range of wireless security concerns. The following are a couple of highlights based on articles and presentations on the PCI DSS.

Use Encryption

A surprising number of access points are still operating without encryption. The PCI DSS requires encryption and goes further to strongly recommend WPA or WPA2 encryption. The less secure WEP encryption is only allowed under very special circumstances.

So, as the first step in securing your facility, you should ensure that all access points are encrypted. This is easily accomplished with the Wi-Net Window because encrypted networks are clearly identified with a reverse video ‘E’ (E). Immediately track down unencrypted APs and take them offline or reconfigure them to use strong encryption.

Carefully Select SSIDs

An access point’s SSID is its beacon to the world. It is an indication that it is present and available. One common mistake when installing an AP is to continue using the default SSID that came with the equipment. This then becomes an attractive target for a potential hacker. A default SSID is a red flag



that the AP hardware has been minimally configured. A network with an SSID of **Linksys** will certainly be chosen for an attack over one named **Fred_123**. At least Fred knew enough to rename his SSID.

As a performance note, keeping the equipment's default SSID, and channel, also increases the likelihood that it will conflict with a similarly default-named network in the same area. This can create confusion as employees connect to the wrong network and cannot reach the resources they are expecting.

Another aspect to selecting an SSID is that it shouldn't be too specific. That can provide a hacker with another kind of incentive. For example, stay away from SSIDs such as: **BankXYZ** or **Accounting** or **Launch Codes**. These are all much too attractive for a hacker to ignore.

The Wi-Net Window is a valuable tool for identifying default SSIDs and for locating SSIDs that reveal too much information, or that draw unnecessary attention to themselves.

Conclusion

Wireless security is an ongoing concern. Techniques and technology rapidly evolve so awareness must be maintained. Frequent site surveys and rigorous access point management are an important part of overall network security procedures.

About JDSU

JDSU (www.jdsu.com) offers instruments, systems, software, services, and integrated solutions that help communications service providers, equipment manufacturers, and major communications users maintain their competitive advantage at each stage of the network lifecycle.

A variety of wired and wireless network testing instruments are available from JDSU including the Wi-Net Window Wireless Tester (www.jdsu.com/test_and_measurement/products/descriptions/Wi-Net).