

# Wireless network monitoring

## Rogue access point

A rogue access point is any wireless access point that has been installed on a network's wired infrastructure without the consent of the network's administrator or owner, thereby providing unauthorized wireless access to the network's wired infrastructure.

There are two types of rogue access points:

If an unauthorized access point is found connected to the secure network, it is the rogue access point called "wired rogue". Wired rogue can pose a security threat to large organizations with many employees, because anyone with access to the premises can install an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties.

An access point set up by an attacker outside a facility with a wireless network is also called an "evil twin,". Evil twin picks up beacons (signals that advertise its presence) from the company's legitimate access point and transmits identical beacons, which some client machines inside the building associate with. As long as wireless security is enabled, this type of attack cannot compromise the user's machines. However, it can cause harm by slowing down the connections or causing users to lose connections with the real network.

## Detection of rogue access points

In order to detect rogue access points, two conditions need to be tested:

- if access point is in the managed access point list – compare wireless MAC address (also called as BSSID) of the access point against the managed access point BSSID list
- if access point is or is not connected to the secure network

It is possible using static IP address on your network instead of having them assigned by a DHCP server. This would mean that whoever installed the rogue access point would need to manually assign an IP address to the access point before it could gain access to the network.

Rogue access points can be detected by performing a walking audit around the facility with sniffer software in a laptop or PDA running tool for detecting all wireless networks within a broadcast area. More reliable approaches are to install probes that constantly monitor the wireless network looking for

changes or install server software that monitors both wired and wireless sides of the network.

To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points.