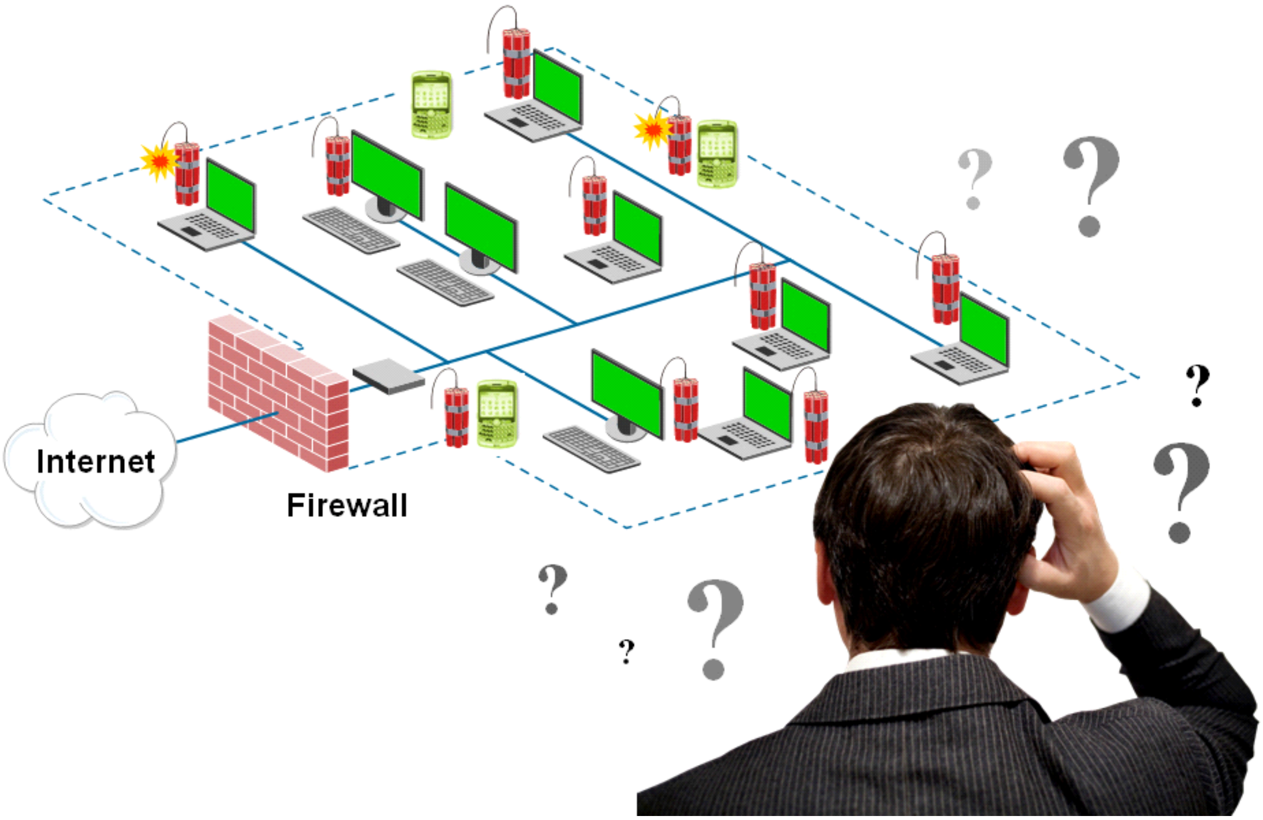
Conquering the Minefield of Soft Rogue APs in the Enterprise

A Whitepaper by AirTight Networks

www.airtightnetworks.com



Conquering the Minefield of Soft Rogue APs in the Enterprise

Dr. Hemant Chaskar

Director of Technology, AirTight Networks

Overview

A soft access point (AP) is a laptop or other wireless enabled device which performs traffic forwarding between its wireless interface and some other interface which is connected to the secure network. A soft AP can show up as rogue access point on the enterprise network. This can happen inadvertently, for example, when an employee has used a company owned laptop as an AP to share Internet connection at home and later forgets to disable the sharing. A soft AP can, however, be maliciously installed as it is perfect hacker “solution” to put a rogue AP on a network while evading wire-side controls such as 802.1x, NACs and wireside-only rogue AP scanners.

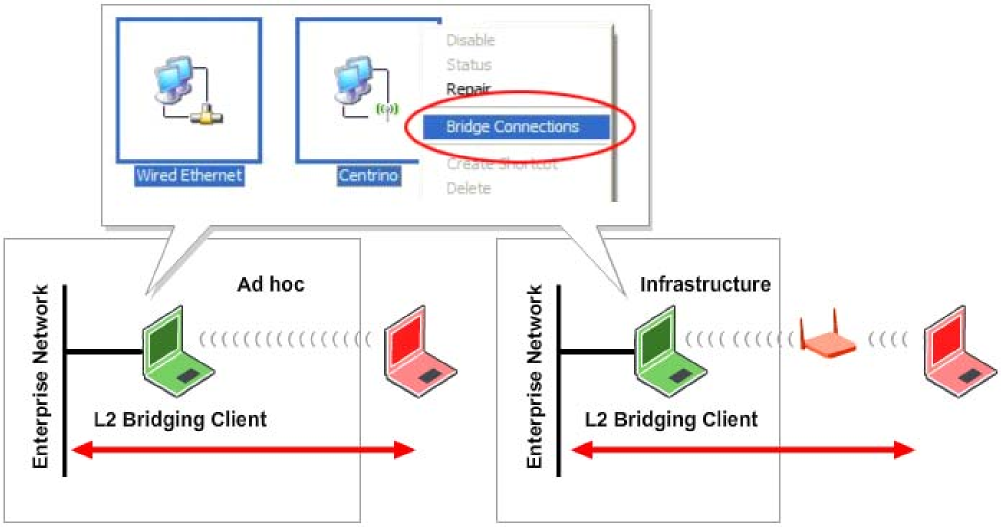
Recently, soft APs increasingly have been found in enterprise networks. One main reason behind this is the ease with which end user devices enable soft AP configuration on embedded WiFi interfaces. In most cases, only couple of clicks is what it takes to enable soft AP on the end user device. Notably, while conventional rogue APs required bringing in unmanaged hardware such as home grade WiFi router into the enterprise, soft APs are embedded already in the end user devices.

This paper reviews some of the commonly found ways to convert WiFi enabled devices into soft APs. Here Windows OS is used as example, but similar configurations can also be done on many end user devices including the handheld devices such as PDAs and smart phones. The paper also suggests what steps you can take to protect your network from soft AP threats.

Commonly Found Soft AP Configurations

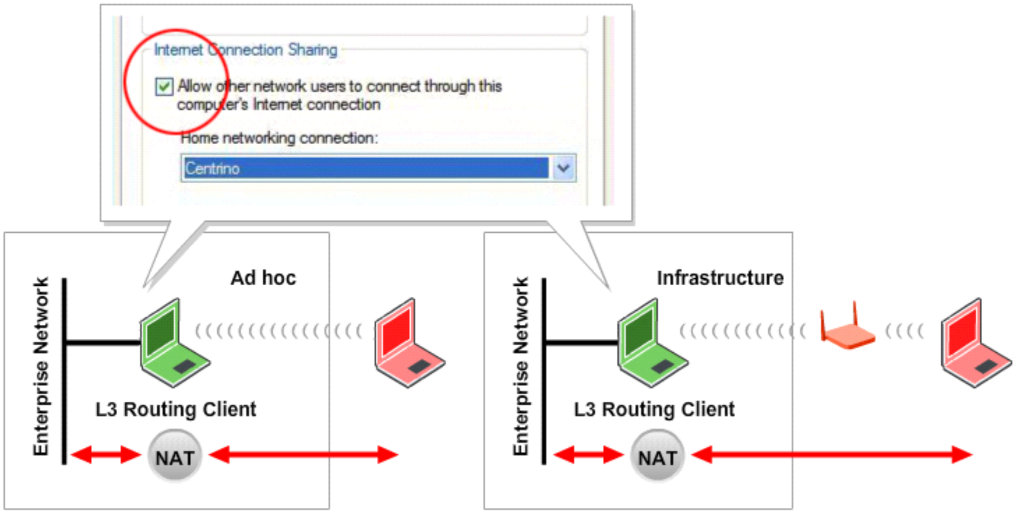
The following are some commonly found soft AP configurations.

1. Windows Network Bridge:



A network bridge can be created between the wired Ethernet interface and the wireless WiFi interface of a Windows laptop. If the wired Ethernet interface is connected to the enterprise network, the network can be accessed by intruders from outside of premises who connect wirelessly to the WiFi interface. The intruders will have layer 2 access to the enterprise network.

2. Internet Connection Sharing (ICS):

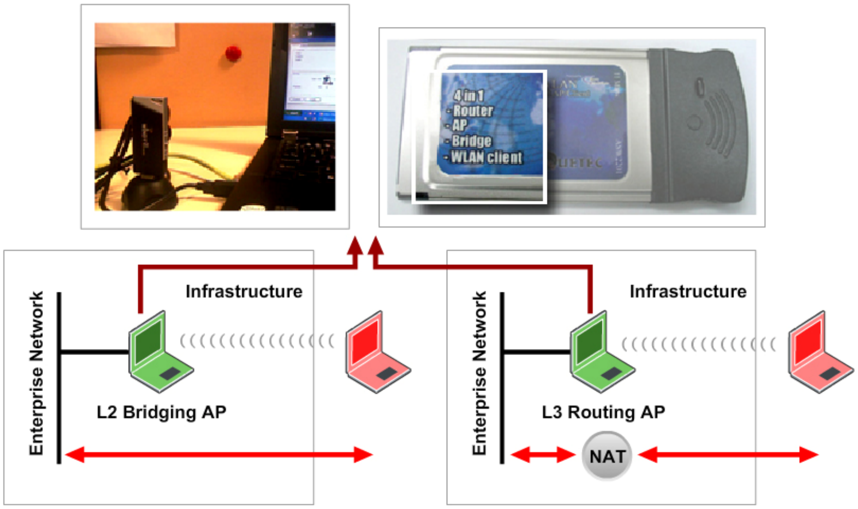

Internet Connection Sharing
☑ Allow other network users to connect through this computer's Internet connection
Home networking connection:
Centrino
Enterprise Network
Ad hoc
L3 Routing Client
NAT
Enterprise Network
Infrastructure
L3 Routing Client
NAT

When Internet Connection Sharing (ICS) is enabled on a Windows laptop, a routing (NAT) service is created between its wired Ethernet interface and wireless WiFi interface. If the wired Ethernet interface is connected to enterprise network, the network can be accessed by an intruder from outside of the premises by wirelessly connecting to the WiFi interface. The intruder will have layer 3 access to the enterprise network.

3. Add-on Devices on Laptop:

External devices can be connected to the laptop to turn it into a soft AP. For example, USB devices such as Windy31 and PCMCIA cards such as WP1200, are available and can act as wireless access points when plugged into the laptop. Devices such as Windy31 also come built in with AP software which auto-installs when the device is plugged into the laptop. The WiFi AP running on such devices can bridge or route traffic to the wired network through the laptop.

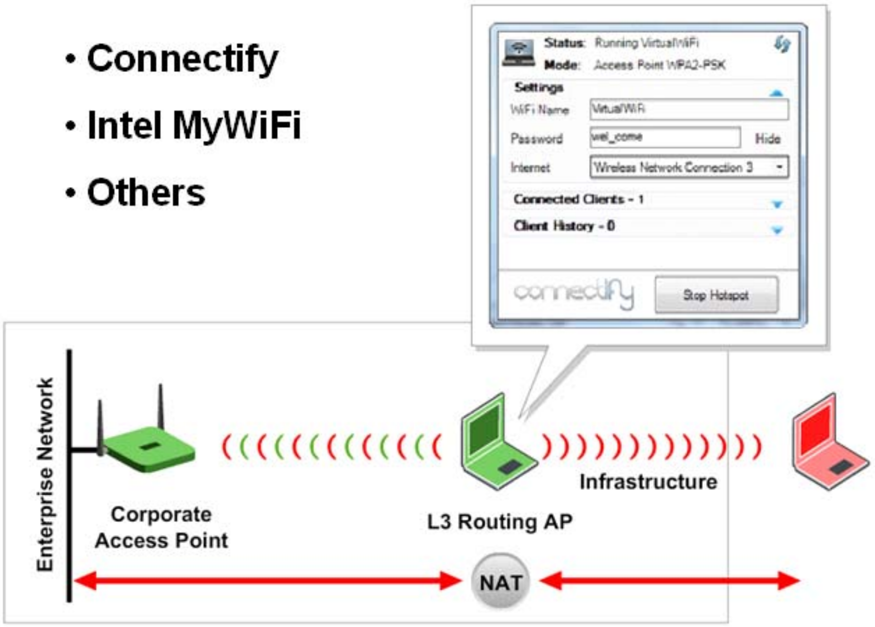
Windy31



4. Virtual WiFi Interfaces (Windows 7):

Windows 7 has introduced the virtual WiFi interfaces feature. This feature enables a single radio interface on the device to act as multiple WiFi devices simultaneously. Software tools such as “connectify” are available to enable both client and AP simultaneously on the radio interface of the Windows 7 laptop. If such radio interface is connected to enterprise network as authorized corporate

WiFi client, unauthorized users from outside of the premises can connect to the AP operating on the same radio interface and then access the enterprise network.

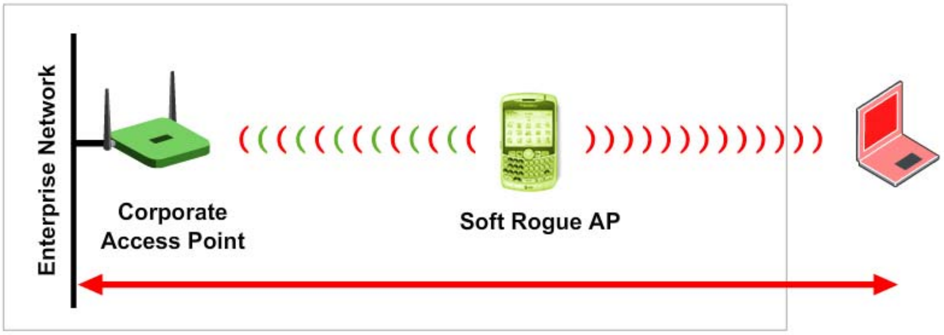


- Connectify
- Intel MyWiFi
- Others

Status: Running VirtualWiFi
Mode: Access Point WPA2-PSK
Settings
WiFi Name: VirtualWiFi
Password: wel_come
Internet: Wireless Network Connection 3
Connected Clients - 1
Client History - 0

Soft APs on Handheld Devices

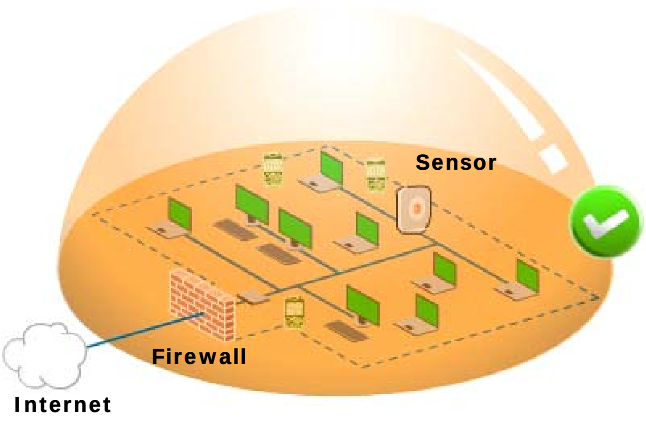
The virtual interfaces mark a significant development as they extend soft AP threat from laptops to handheld devices. The handheld devices typically do not have wired Ethernet interface, so the first three methods are generally not applicable to them. However, with the advent of virtual interfaces, it is now possible to use a WiFi radio in the handheld device to simultaneously act as authorized corporate WiFi client and unauthorized soft WiFi AP.



Protection from Soft APs

Since it is so easy to convert end user laptops and WiFi enabled handheld devices into soft rogue APs, enterprises need to be continuously monitoring to understand if any soft APs are present on their networks.

Monitoring for soft APs requires wireless scanning tools such as wireless intrusion prevention system (WIPS) comprising of wireless monitoring sensors. WIPS sensors can continuously track the wireless activity of end user devices and detect soft AP activity. They can also block soft AP activity over the air.



SpectraGuard$^{®}$ Enterprise
Wireless Intrusion Prevention System

While there are many WIPS offerings available in the market, it is essential to evaluate if they can provide protection against all scenarios of soft APs, before installing them in your network. AirTight Networks offers SpectraGuard$^{®}$ Enterprise overlay WIPS which is capable of protecting against all types of soft AP activity due to its unique active classification™ technology enabled by patented marker packet techniques. It is also worth noting that WIPS also provides protection from many other WiFi threats such as conventional rogue APs, mis-associations, ad hoc connections, WiPhishing, wireless DoS attacks etc. (which are not discussed in this paper), helps meet compliance requirements (e.g., PCI, HIPAA etc.), and also provides performance monitoring and troubleshooting for the WLAN.

For more information on WiFi security, WIPS and AirTight Networks, please visit www.airtightnetworks.com. You can also review recorded webinar on this topic of soft rogue APs at https://admin.acrobat.com/_a1013426351/p54357857/.