Wireless IPS that can reliably differentiate between harmless neighbours, personal hotspots, and network-connected rogues that pose real danger to the company, taking policy-based action to trace, block, and locate the latter.

4. **Wireless Intruders:** Wireless IPS can also detect the malicious WIFI operating nearby

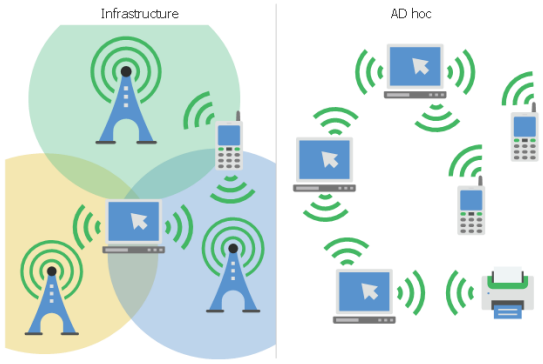
a business airspace. However effective defences requires an updated regularly deployed WIPS sensors. The 802.11 a/b/g sensors must be updated to monitor the new 5 GHz channels, parse 802.11n protocols, and look for new 802.11n attacks.

Furthermore, because 802.11n clients can connect from farther away, WIPS sensor placement must be reviewed to satisfy both detection and prevention needs.

5. Misconfigured APs: The standalone APs were individually-managed, configuration errors posed a significant security threat. Today, most enterprise WLANs are centrally-

managed, using coordinated updates and periodic audits to decrease TCO, improve reliability, and reduce risk. But 802.11n adds a slew of relatively complex configuration options, the consequences of which depend on (highly variable) Wi-Fi client capabilities. Prioritization and segmentation for multi-media further complicates configuration.

6. Ad Hocs and Soft Access point: Wi-Fi laptops have been able to establish peer to



peer adhoc connections that pose the risk because as they circumvent the network security policies. Fortunately, ad hocs were so hard to configure that few bothered to use them.

Unfortunately, that barrier is being lifted by "soft APs" in Windows 7 and new laptops with Intel and Atheros Wi-Fi cards. Those virtual access points can provide easy, automated direct connections to other users, bypassing network security *and* routing traffic onto the enterprise network. Measures used to deter