

Non-WiFi Interference Combat Guide (www.blog.airtightnetworks.com)

Interference source	Nature of interference	Remedy principles
Microwave oven	Affects upper end (high channel numbers) of 2.4 GHz WiFi spectrum when microwave is running (heating food). When running, interference duty cycle is about 50%.	<ul style="list-style-type: none"> i) Deploy APs as far as possible from known microwave locations - at least 100 feet away, lesser distance will do if there are intervening obstacles such as walls. ii) Even then, degraded performance for users close to microwave oven is unavoidable.
Bluetooth	Bluetooth frequency hopping sweeps across entire 2.4 GHz WiFi spectrum.	<ul style="list-style-type: none"> i) Bluetooth interference is generally not a major concern due to its frequency hopping, narrow band transmission (1 MHz), intermittent activity and low transmit power. Still to be conservative, tell users to not use high power (class 1) Bluetooth on enterprise premises. ii) If users operate continuous transmission Bluetooth applications too close to WiFi client, they may see some performance hit on WiFi client, though it will be localized to those users. Bluetooth mice, headsets are generally not a concern.
Baby monitors	Affects 2.4 GHz WiFi spectrum.	<ul style="list-style-type: none"> i) Though this source is often cited, it is unforeseeable that employees will bring baby monitors (and babies to be monitored with them) to office. So in practice, baby monitors are not a concern for enterprise WiFi networks. It is highly unlikely that baby monitors in homes surrounding the office will generate interference enough to reach office WiFi networks (unless you have wall touch neighborhood around office). ii) I would like to hear your story if you have indeed faced baby monitor interference in enterprise WiFi networks.
Cordless phones	The digital cordless phones which operate in 2.4 GHz and 5 GHz bands can cause interference to WiFi in respective spectrums.	<ul style="list-style-type: none"> i) Here again, most enterprises do not use cordless phones on office premises. Cordless phones are primarily used in homes. Further, even those used in enterprises mostly use 900 MHz DECT technology. So in practice, they are not a concern for enterprise WiFi networks. It is highly unlikely that interference from cordless phones in homes surrounding the office will generate interference enough to reach office WiFi networks (unless you have wall touch

		<p>neighborhood around office).</p> <p>ii) I would like to hear your story if you have indeed faced cordless phone interference in enterprise WiFi networks (even when you don't have cordless phones as part of enterprise infrastructure).</p>
Analog wireless cameras	<p>These cameras are typically used for video surveillance and are older generation. The newer generation is digital technology including co-existing WiFi transmission. Analog cameras operate in 2.4 GHz WiFi band and depending on which channels they are tuned to, they cause constant background interference on respective WiFi channels.</p>	<p>i) Check with your office security staff if they use analog wireless video surveillance cameras. Deploy your APs as far away as possible from known analog camera locations - at least 100 feet away, lesser distance will do if there are intervening obstacles such as walls. It won't hurt to consider upgrade of analog cameras to digital versions during WiFi deployment project at incremental cost. If possible, check if your neighborhood premises use analog wireless cameras and position your APs away from them.</p> <p>ii) Even when APs are placed away from analog cameras, degraded performance for users close to analog camera locations is unavoidable.</p>
Jammer	<p>Jammer refers to deliberate generation of interference, typically out of malicious intent (DoS attack). Jammer can create interference in both 2.4 GHz and 5 GHz spectrums. Depending on its intensity, it can degrade or even completely wipe out WiFi communication.</p>	<p>i) Since jammer is a source which cannot be a priori known, only remedy for jammer is to detect it when it happens and then physically mitigate it.</p> <p>ii) Ask your access point vendor or wireless security sensor vendor for jammer attack detection capability.</p>

AP operation in 5 GHz:

In general, you will notice that many of these non-WiFi interference sources (Microwave oven, Bluetooth, baby monitors, many cordless phones, surveillance cameras) operate in 2.4 GHz band. So one solution to avoid them altogether is to operate APs in 5 GHz band (802.11a/n). The flip side however is that AP coverage will be smaller in 5 GHz. Also if you have any legacy clients, they will not be able to operate in 5 GHz band.