Device Classification Guide

Revised Date: May, 2015

Introduction

Designing networks for BYODs implies offering RF conditions that will allow these devices to properly connect, maintain their connection while in the cell, and roam seamlessly when needed. All BYODs offer the same functions such as Wi-Fi connection management, support for real time applications over Wi-Fi, roaming, and so on. However, the chipset and the underlying operating system both dictate variations in the behavior that might affect your design. For example, some devices are dual band, and some are not. Some devices probe often, making them easy to locate even in the sleep mode. Some devices stop probing when the screen is turned off, conserving battery but making the location of the devices challenging.

Some operating systems partially implement roaming optimization protocols, such as 802.11r (Fast Transition—to expedite secure roaming), 802.11k (Radio Resource Measurements—to discover neighboring APs faster), 802.11v (Wireless Network Management—to increase the lifetime of the battery by reducing unnecessary exchanges with the AP while the BYOD is in the sleep mode), or 802.11u (Internetworking with External Networks—to automatically associate with Wi-Fi networks connecting to your phone service provider network in a secure manner).

Some devices also offer enhanced security with 802.11w (Protection of Management Frames—to protect from spoofing attacks). To help you design your wireless network, and decide what options to configure on your controller, see the following table that lists the main BYOD models in the market, their probing and roaming behavior, and their support for roaming or security optimization protocols.

	Radios				Standards						Location			
	2.4 GHz	5 GHz	11n	11ac	11r	11k	11u	11v	11w	DFS Channels	Probing Frequency	Roaming Behavior	mDNS	Sleep Mode Behavior
iPhone 5s/i8.0	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	30 min.	AP signal is < -70 dBm	Discovery: Bluetooth + Network Mirroring: Network Wi-Fi Direct	Probes with the real MAC for 20 minutes, then sends probes alternating between the real and changing fake MAC with a 135 s cycle.
iPhone 5/i7.0/7.1	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	30 min.	AP signal is < 20 dB	Discovery: Bluetooth + Network Mirroring: Network	Probes broadcast every 30 minutes.
iPhone 6/6+ i8.0 (8.0.0, 8.0.1, 8.0.2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	30 min.	AP signal is < -70 dBm	Discovery: Bluetooth + Network Mirroring: Network Wi-Fi Direct	Probes with real MAC 12 s, no probes for 140 s, then probes with fake MAC for 18 minutes
Samsung S4 / Android 4.2.2 /4.4.2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	285 s	AP signal is < 25 dB	None	Probes broadcast only, every 131 s.
Samsung S5 / Android 4.4.2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	300 s	TBD	None	Probes broadcast only, every 300 s.
Samsung S6 / Android 5.0.2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	300 s	AP signal is < 25 dB	None	Probes broadcast only, every 300 s.
HTC One (M8)	Yes	Yes	Yes	Yes	No	No	No	No	No	Yes	Never	AP signal is < 25 dB	None	Probes broadcast only, every 285 s.
Microsoft Surface 2	Yes	Yes	Yes	No	No	No	No	No	Yes	No	TBD	TBD	None	TBD
Microsoft Surface 3	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes	TBD	TBD	None	TBD