Proposed Test Procedure for FCC DFS Testing of Access Points operating in Sensor Mode as a DFC Client

Summary:
An Access Point operating in Sensor Mode is standard transmitter hardware and firmware as any other 802.11 abgn Access Point Transmitter performing the additional function of network monitoring. The Access Point in Sensor Mode uses the same modulation, data rate, transmit power output as when the hardware would be operating as an standard Access Point Transmitter in a (multi-transmitter/collocated) Access Point. The Access Point in Sensor mode is operating in what would be considered as a DFS CLIENT.

(FYI: Both NIST and the FCC currently have Access Points that operate in Sensor mode installed to maintain network security)

The Access Point operating in Sensor Mode is part of a secure wireless network system. The secure wireless network is designed to inhibit any unauthorized device from access to the Wireless Local Area Network. A computer server connected to the network maintains a list of authorized access points and mobile units that comprise the secure WLAN. The Access Point operating in Sensor Mode operates under the Control of another Access Point to utilize the network; it pseudo-randomly monitors the WLAN channel traffic.

If an “Unauthorized Mobile Unit” attempts to access the network; the AP Sensor upon detection, will transmit a standard “IEEE 802.11 Deauthentication Message data packet to both the “Unauthorized Mobile Unit” and to the Access Point with the intent to interrupt / deny network access.

AP sensors are available in three configurations. The first configuration has the AP Sensor collocated in the same housing with a standard Access Point Transmitter; second, as a Access Point in a separate housing; and third as an Mini-PCI card that can be installed in an Access Point with an open Mini-PCI Slot.

ISSUE:
Currently a DFS Client must demonstrate 4 attributes to be judged compliant by the FCC.

There are 4 things that a DFS Client has to do to pass DFS testing.

- Associate with a Master AP
- Channel Move (Testing done with Channel Loading)
- Channel Closing Transmission Time (Testing done with Channel Loading)
- Non-occupancy (30 Min)

DFS Client Testing currently requires Channel Loading --> the Streaming of a specific (TestFile.mpg) Video or Audio during two of the tests. The currently defined DFS Channel Loading is not possible or demonstrative of an AP Sensor’s normal mode of operation.

RESOLUTION:
Motorola is proposing that Channel Loading during the DFS Client Channel Move and Channel Close tests use the AP Sensor's "Normal Transmission of packets."
This accomplishes the required loading with the same level of traffic that the channel would see during normal operations of the AP Sensor,

To accomplish the Channel Loading, we set up a Secure Network with a sensor and DFS Master Access Point and an "Unauthorized Device" continuously trying to access the network.

- The "Unauthorized Device" will use the Media Player Classic to try to play the TestFile.mpg file that is located on the secure network.
- The AP Sensor will detect the Unauthorized Device and transmit the Deauthentication messages.
- The DFS Master AP will detect the radar, and send the channel Close beacon.

REQUEST:
Approve the use of this alternate Channel Loading procedure for the DFS testing of Access Points in Sensor Mode

Sensor Test Procedure

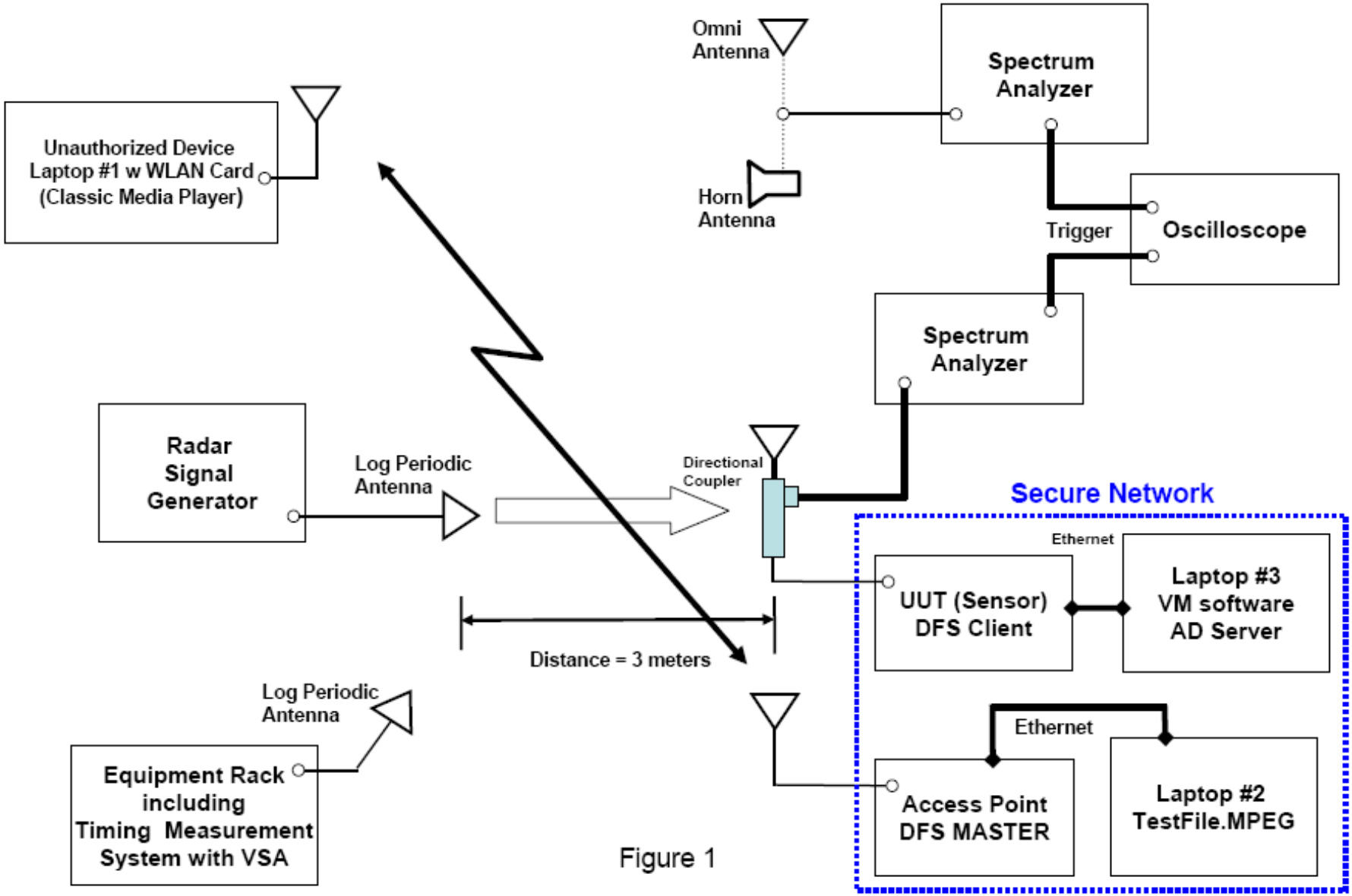

Figure 1