Zigbee Packet Analysis

**Lesson 1 – Wireless Spectrum Regulation**

# Wireless Spectrum Regulation

**Lab Description:** In this lab you will look over a few of the regulations that are enforced by the FCC.

**Lab Environment:** Windows Environment with Internet

**Lab Files that are Needed:** Zigbee-join-authenticate.pcap file

### **Download and setup wireshark**

1. Visit Wireshark’s website and download wireshark
2. Install Wireshark with default’s selected
3. Download the zigbee-join-authenticate sample pcap from <https://wiki.wireshark.org/SampleCaptures>
4. Extract the pcap.gz file using 7-zip or another zip file utility tool
5. Open the pcap with Wireshark

**ANALYZING THE ZIGBEE PCAP**

1. In several of the packets sent there is a source of 0x0000, what is the significance of this?
2. What are the four major categories of the MAC frames ZigBee devices use?
3. What version of the protocol Zigbee is being used?
4. What are the protocol(s) in the ZigBee packet capture? Research some into it(them) and see what you can find.
5. What do you think are some reasons why ZigBee is being used?

## What to submit

Screenshots and a description of each part/question in a Word Document or PDF.