

Wi-Spy Hardware Interface Specification

Device Enumeration

Wi-Spy enumerates as a low-speed USB HID class device, allowing Wi-Spy to use the standard USB HID driver in Windows. Wi-Spy 1.2 enumerates with Vendor ID/Product ID 0x1781/0x083E. A basic class for communicating with USB HIDs in several programming languages can be found at <http://www.lvr.com/hidpage.htm>.

Receiving Data

In order to receive data from the Wi-Spy hardware a Get Feature Report is sent. The hardware will respond with an 8-byte Feature Report. The structure of this report is:

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
Frequency X	RSSI of X	RSSI of X+1	RSSI of X+2	RSSI of X+3	RSSI of X+4	RSSI of X+5	RSSI of X+6

RSSI is the received signal strength indication and has a value 0-31. X is offset by 2400 MHz (e.g. if X = 0, the frequency is 2400 MHz)

Feature Reports are sent sequentially and are non-overlapping. In other words, the first report will contain RSSI measurements for frequencies 2400-2406 MHz, the second report will contain RSSI measurements for frequencies 2407-2413 MHz, and so on. After sending the feature report contain RSSI measurements for frequencies 2477-2483 MHz the hardware will return to frequency 2400 MHz, and will continue to loop as long as Get Feature Reports are received.

Internally the Wi-Spy hardware has two threads of activity. One thread, upon USB enumeration will continuously loop polling the radio for RSSI measurements and placing the measurements in an array. The other thread, upon receiving a USB Get Feature Report will create and transmit a USB Feature Report containing data from the array.

The software converts the RSSI measurements using the following algorithm:

$$\text{dBm} = \text{RSSI} * 1.5 - 97$$

Software Example

Open source example software can be found at: <http://svn.kismetwireless.net/code/tools/wispy/>