*WARNING: This document may not reflect the actual implementation. It was written as a thought experiment and saved. Things may have changed in the coding process. Someday, (in my copious spare time), I may go back and make a formal, corrected document. Or not.*

***Logic Flow for Network Port Scanner and Identifier***

**Consider:**

1. The Fusion’s Single Board Computer (SBC) has two on-board (ie: internal) network interface devices: a Wired Port and a Wireless Port.
   1. In use, it is possible that a user may plug in additional network devices by using USB dongles.
2. Fusion has two modes of operation: Standalone Mode and Community Mode
   1. In Standalone mode, the Fusion provides a Wireless Access Point (WAP). The user connects workstation to this assess point, providing access to the FusionOS GUI.
   2. In Community Mode, the Fusion needs a Wireless Network Interface Controller (NIC) that it uses to connect with the Classroom Server’s Community.
3. Currently, the FusionOS *always* uses the internal Wireless asset as an Access Point. To connect to the Classroom Server’s Community, it requires a WiFi dongle that remains configured as a NIC.
4. The Fusion’s wired network asset (ie: the Wired Port) is always used to connect the Fusion to an upstream network.

**Proposal:**

1. Much like the current system operation, we will continue to use the internal wireless asset as the Wireless Access Point ***unless*** it is the only wireless asset (ie: no dongle) and we need to join a Classroom Community.
   1. If there is no external wireless asset, we will reassign the internal wireless asset to operate as a NIC and use it to connect to the Community.
   2. We will use the internal wireless asset to look for and join a community. If this attempt fails, the internal wireless asset will convert to access point operation and the Fusion will run in Standalone Mode.
2. If there is an external wireless asset, we will utilize it as the NIC device and use the internal wireless asset as an Access Point (as we do today).
3. If multiple wireless dongles are connected to the Fusion, it will use the first non-internal wireless asset as the NIC and ignore the others.
4. If a WIRED network dongle is connected, the Fusion will not intentionally use it, but will continue to use the internal wired asset as a possible network connection.

**Sequence of Operation on Start-Up:**

1. Identify all networking assets.
   1. If there is only one networking asset, we may have a hardware fault.
   2. If there are two networking assets, confirm that there is one wired and one wireless port, and that they are both on-board the SBC.[[1]](#footnote-1)
   3. If there are more than two networking assets, confirm that the two internal assets are present, and then identify the additional [external] devices to identify an external wireless device.
      1. If an external wireless asset is found, assign:
         * WIFI = External wireless asset
         * WAPT = Internal wireless asset
         * ENET = Internal wired asset
      2. If no external wireless asset is found, we need to use the internal asset as the WIFI device to locate and attempt to join a community. If we fail to join a community, we need to convert the internal wireless asset to be the WAPT device.

1. This is accomplished by examining the MAC addresses. The first three octets are the Organizationally Unique Identifier (OUI). These bytes are assigned and registered by the IEEE and the IANA, and will identify the ‘manufacturer’ of the networking hardware. Raspberry Pi currently has two OUIs: B8:27:EB and DC:A6:32. [↑](#footnote-ref-1)