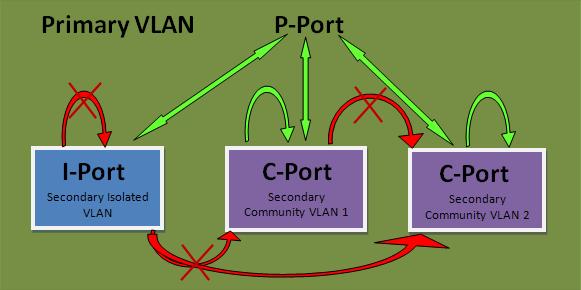
`VLAN:

* <https://www.networkcomputing.com/networking/vlan-implementation-guide-basics>
* As we have learned, a VLAN breaks up a physical layer 2 network into multiple, logical layer 2 networks. In order to move between these layer 2 networks, this traffic needs to be routed at layer 3. So while switches can send data from source devices to destination devices using layer 2 MAC addresses, inter-VLAN routing using IP addressing. This can be either IP version 4 or IPv6, although most enterprise networks still use IPv4 on internal networks.
  + Communicate inside VLAN using MAC Addresses
  + Communicate trans-VLANs using IP Addresses
* Private VLAN:
  + <https://en.wikipedia.org/wiki/Private_VLAN>
  + **Private VLAN**, also known as **port isolation**, is a technique in [computer networking](https://en.wikipedia.org/wiki/Computer_networking) where a [VLAN](https://en.wikipedia.org/wiki/Virtual_LAN) contains [switch](https://en.wikipedia.org/wiki/Network_switch) ports that are restricted such that they can only communicate with a given "uplink"



* + direct peer-to-peer traffic between peers through the switch is blocked, and any such communication must go through the uplink.
* VLAN vs Subnet
  + Subnets exist at Layer 3 of the OSI Model. They are a network level construct and are handled with routers. As a result, subnets are based around IP addresses. Routers carve out ranges of IP addresses and negotiate the connections between them. This places all of the stress of network management on the router.
  + VLANs find their home on Layer 2 of the OSI Model. The data link level is closer to the hardware and less abstract. Virtual LANs emulate hardware, since they act like individual switches.
* https://www.smallnetbuilder.com/lanwan/lanwan-howto/30071-vlan-how-to-segmenting-a-small-lan
  + Steps:
    1. Plan your network
    2. Create the VLANs
    3. Associate switch ports with the VLANs
    4. Test VLAN connectivity
  + Wireless VLAN:
    1. For example, all wireless APs could be grouped into a single VLAN, assigned an identifier not used by any Ethernet workgroup. Edge switches could apply the wireless VLAN's tag to packets received from any AP. Upstream switches could funnel all wireless VLAN traffic towards an Internet access router, and network layer ACLs could prevent wireless VLAN traffic from reaching other destinations inside your company network.

Socket Programming:

* https://www.geeksforgeeks.org/socket-programming-cc/
* Server <-> Smart Microcontroller
  + Sending JSON strings through C socket library
    - <https://stackoverflow.com/questions/32667109/send-and-receive-json-over-sockets-in-server-and-client-application-in-c>
  + Server -> Controller:
    - TCP, socket programming
    - Controller is host, server is client (?)
    - Encryption application is hosted on both devices
      * Both devices hold each other’s keys to validate message
    - We’re sending a JSON string of the schedules:
      * In Java:
        + String strJson = jsonObject.toString();
        + JSONObject js = new JSONObject(strJson);
      * Research JSON library in C++, we might have to incorporate Python
  + Controller -> Server
    - UDP, socket programming
      * Research more, might want TCP
    - Server is host, controller is client
    - Controller sends JSON file detailing status/health of system
    - Same encryption application