**Effective Network Isolation**

Having separate routable networks for different devices of different levels of trust

* Done via router (firewall, switch, Wi-Fi access point) or on the host
* Can connect device via ethernet and assign its own network
  + This would cause the devices on that isolated network to not be able to send outbound connections to other devices on the local network
  + Can only accept inbound connections from the local network
  + Can also be blocked from making direct connections to the internet
    - Could be good if an attacker has gained control via inbound connections
    - This would stop the malware from being able to communicate out

**VLANs**

Virtual LANs – logical separation of networks

* ISL
* 802.1Q
* VLAN technologies

Uses tags in the data packets, based on a physical port that a device is plugged into on a switch, to differentiate VLANs

Work at the data link layer (layer 2) and sometimes at layer 3 as well

A properly configured VLAN won’t allow the devices within it know that there is even an external network or other devices connected to the local network

* Can also have individual devices on their own VLAN
* i.e., laptops never really need to communicate with the other devices in the homes so putting it on a AVLAN may not be a bad idea

VLAN hoping used to be a thing, but their patches have been rolled out for a while now so it is much less likely to happen nowadays

**VLAN technology**

NetCut

TuxCut (Linux)

SniffDet (Linux)

Xarp (Windows and Linux)

ArpWatch (Linux, PfSense: router, firewall)

IP SEC

**ALL TRAFFIC SHOULD BE DENIED UNLESS IMPLICITLY ALLOWED**

**V high end and technically advanced**

Port security/protection

802.1AE (IEEE Standard)

802.1X (IEEE Standard)

DHCP Snooping

* Watches DHCP requests and builds and its own Arp table