Defense in Depth (DoD?)

Figure out number of vlans and how they will be setup on the network in packet tracer. Vlan for wifi, each floor, each class, for security, for Pixar, printers on the network (Nassau residence). Won’t be perfect but will be as close to the real thing as possible.

Cameras on each floor monitoring entrances, exits, hallways, and stairwells. Rfid badges to gain access to buildings. Lobby in each building with a security guard to monitor camera footage, keep shady people out, and prevent tampering with devices.

**Security room /MDF:**

One way window lining the security offices so that they can see who is coming without being seen. Cameras in the hallway monitoring who comes and goes, including who enters the security office. MDF (Main Distribution Frame) equipment is kept in a room inside the security room which requires an rfid card to access and finger print reader to access (what you have and who you are). (further prevents unauthorized people from getting physical access). Cages with a physical lock around the switches and routers, with a keypad electronic lock on the room door (what you have and what you know). Camera inside the room monitoring everything that goes on in the room (preferably behind the locked cage). Camera outside the MDF room monitoring the door. All security computers in every building will also require a chipped card to be inserted to a card reader, if the card is removed the computer locks down. These chips will be part of the security teams normal badge but will not be part of the students badges. Chip readers connected to any terminal that can SSH into the servers, acl’s to restrict all other ip’s from creating remote connections to the server room.

61 vlans (one for each 2960s: Horton 10, laffin 36, Nassau 15)

2 vlans(one for pixar and one for security)

3 vlans (one for Wi-Fi in each building)

--------------------------------------------------------

66 vlans total

Acl to allow established connections only to prevent someone from sending .

Sticky mac for any switch that shouldn’t have devices change. (sticky mac for switches connected to other switches?)

Port filtering (shut off un used ports, and forward common ports to other ports)  
setup minimum password requirement (require min 10 characters requiring letters (capital and lower case) , numbers, and special characters

Email, citrix server, cloud storage, and HTTP server on separate vlans in DMZ of outside connection as well.

Dhcp server, username and password data base on the inside of the DMZ

All servers require a user name, password and temporarily generated key (key chain device)

Etherlink aggregation (etherchannel) or equal cost load balancing spanning tree protocol to prevent layer 2 loops on switches (ch. 3).

Laffin hall classrooms and Horton hall office network will shut down after certain hours to prevent tampering with the network when it is not needed.

OSPF separate area for each building, one for DMZ, and one for backbone

nat to hide the networks

firewalls

strick acls with established connections only allowed

bdpu guard

shutdown un used ports

NAT overload hide the real ip address’ of people on our network

DNS to make sure people are getting to our sites not someone spoofing our school website

ssh only form of remote administration

Wi-Fi with 2 SSID one hidden that is for students and faculty and can connect to the local network. The other SSID is broadcast and only has internet access.

stackable modular switches?? Devices pg 18

find distance between buildings on google maps (see if you can map walking path to follow the trenching work).

2901 or 2811 routers?

Need cost to lay 1200 meters of fiber cable to connect the building to the MDF