ANNIE Online Architecture

Geoff Savage

20 April 2016

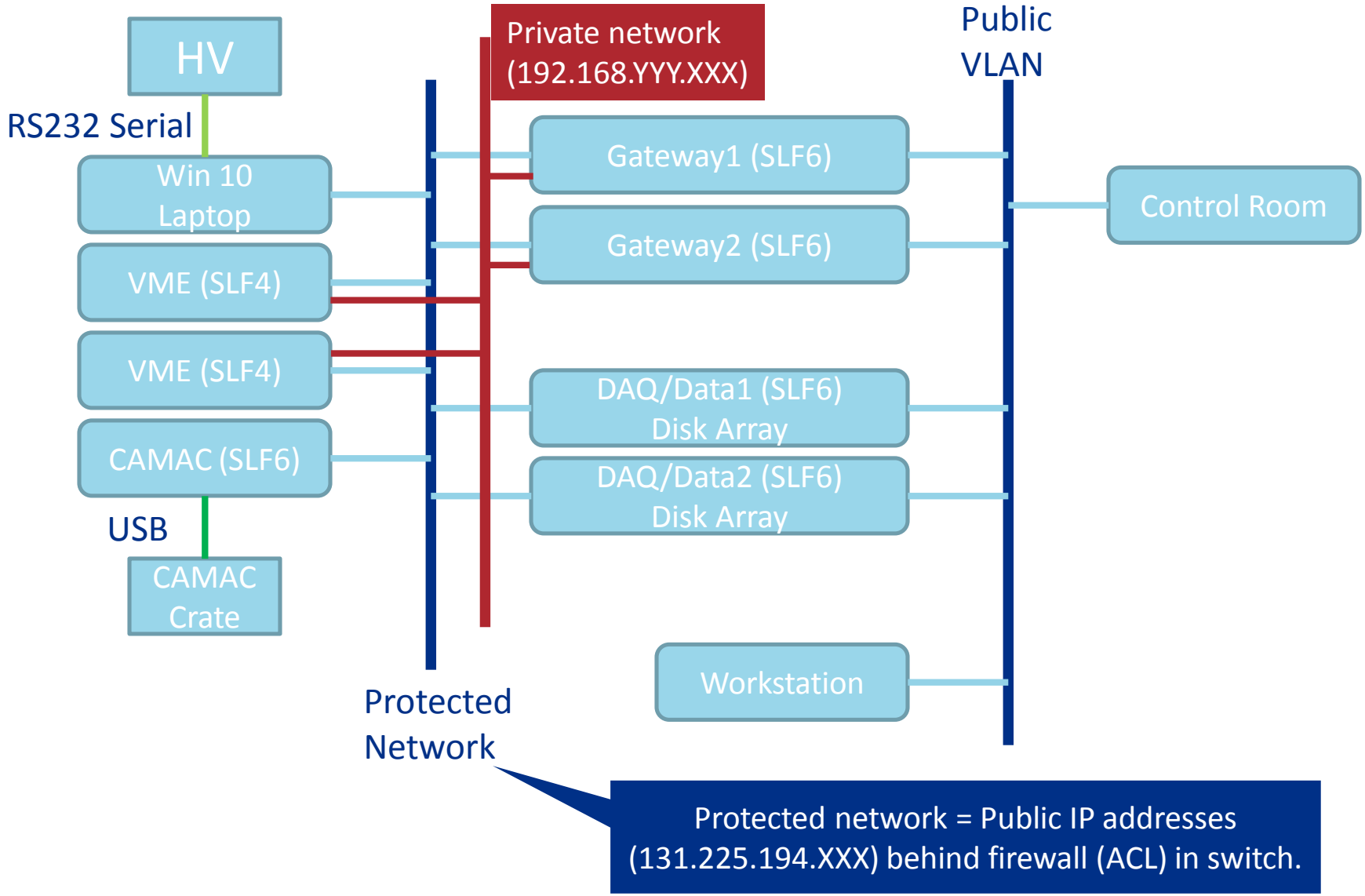
ANNIE Computing Requirements

- DAQ computers
  - Data disks
  - Web server
- HV Computer - Windows 10, unsupported at Fermilab
- Embedded VME processors – unsupported at Fermilab
  - Developers would like to pull data from a repository onto systems in the private vlan for software updates
  - What time is it? Access to Network Time Protocol (NTP) server
  - PXE boot of VME processor (3/16/2016)
- Gigabit connections between systems
- From System Administrators
  - Two of each system type (hot spare)
  - Console server
  - Remote power cycle (I'm not certain of this.)

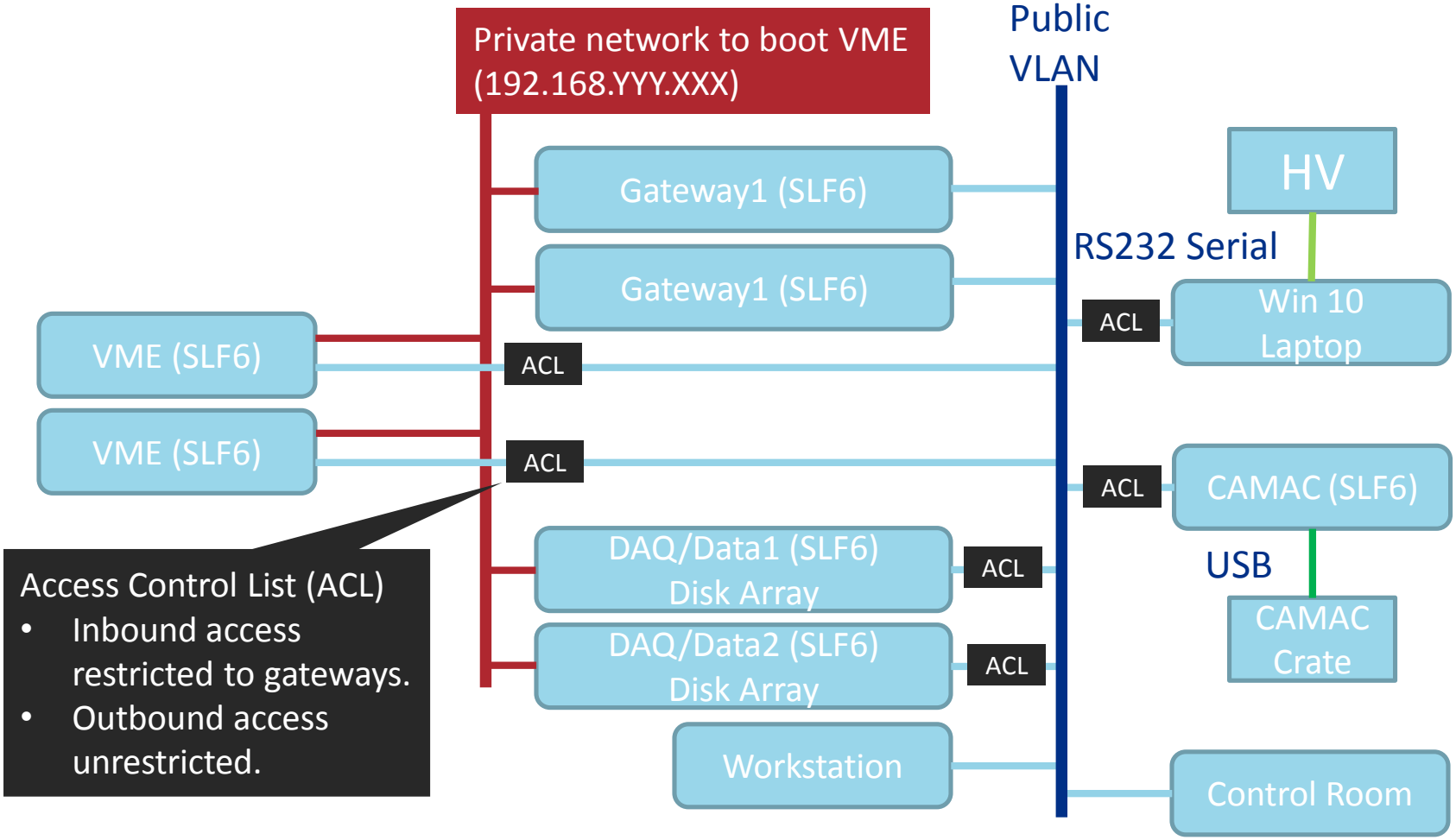
Fermilab Security Requirements

- Direct access to the DAQ nodes must be restricted for a few reasons.
- The DAQ nodes are patched on the ANNIE scheduled not the Fermilab security schedule. Eventually the DAQ computers would be on the public network and not meet the security baseline. They would then be blocked from the network. You could turn on nightly patching at the risk of breaking the DAQ.
- The web server is not registered for access from offsite so it must be accessed via a gateway. And the software patching also applies to the web server software.
- Bonnie and Co. will provide instructions for access via the gateways.

Network, Logical



Network, Physical at SciBoone



Network, Logical Diagram Description

- Vertical bars represent virtual local area network (vlan)
  - Not a physical network switch
  - VLAN options
    - Public – computers that meet the Fermilab security baseline
    - Site-local – computers that don't meet the Fermilab security base line and need access to Fermilab computing resources.
    - Private – computers that don't meet the Fermilab security baseline and don't need access to Fermilab computing resources
  - Public supports direct connections from remote computers
  - Private and site-local require access through a gateway computer
  - Secure connections to public computers through Secure Shell/Kerberos (SSH) or Virtual Private Network (VPN)
- Control room
  - The public network extends throughout the Fermilab site
  - Located in ROCWest

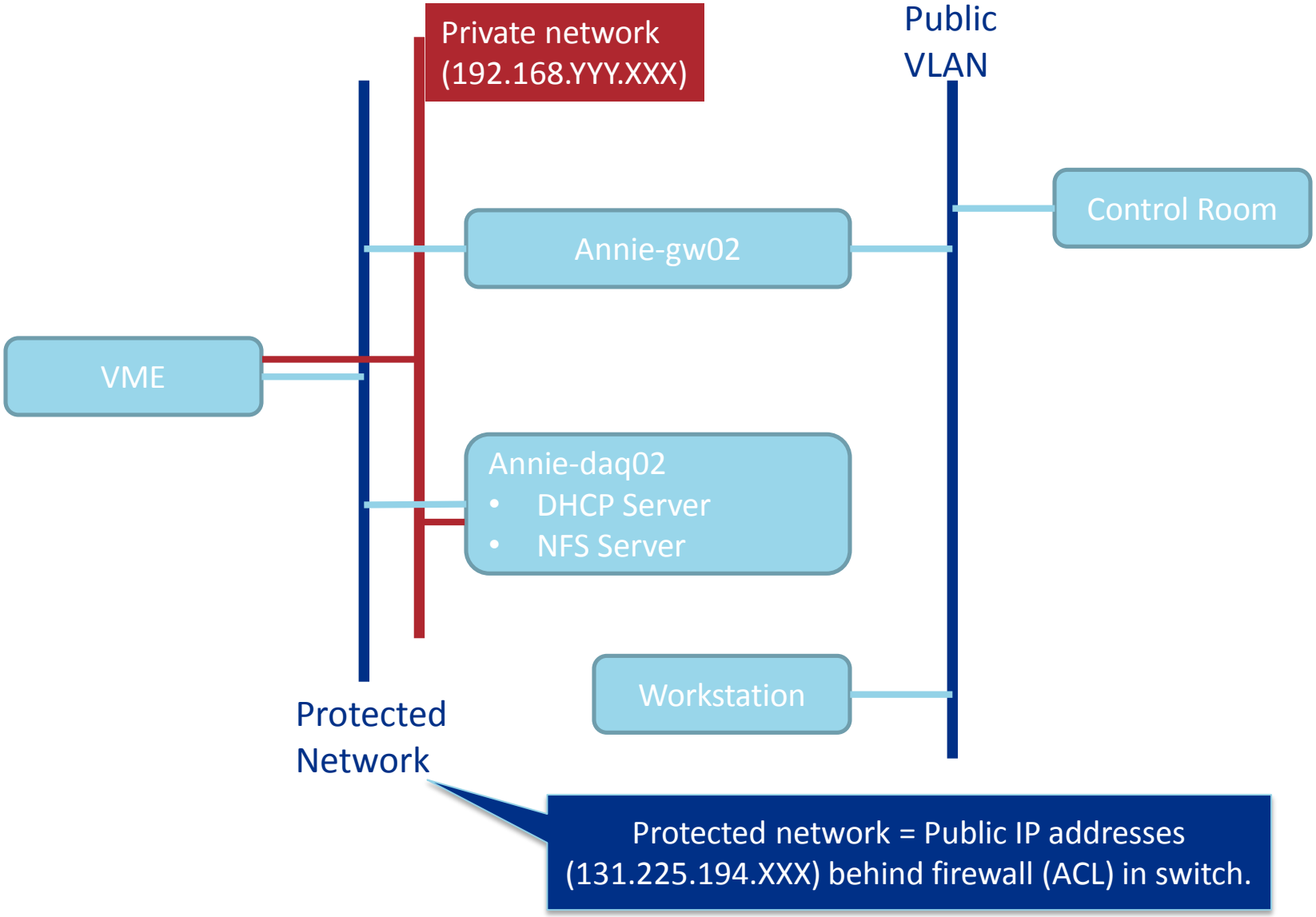
Protected Network

- Requirements fo ANNIE vme processors don't fit any of the three standard network types: public, site-local, or private.
  - Access to offsite file repository
  - Access to ntp server at Fermilab
- The solution is to create a protected network using public IP addresses and an Access Control List (ACL) in the network switch
  - Computers on the protected network have access from outside Fermilab blocked by the ACL
  - Think of an ACL as a firewall that prevents access from the outside to the inside
  - To get network access outside Fermilab the computers need public IP addresses
- This configuration requires additional steps for configuration
  - Assign all ANNIE computers IP addresses in the vlan used at SciBoone, vlan 196
  - Relay the IP numbers for the private network computers to the networking group
  - Networking group makes a change request
  - Once the change request is approved the ACL can be put in place
- See RITM0357514 for the ongoing action

Private Network

- The VME processors require a private network to boot
- Then they use the protected network for data acquisition
- All the computers only have two network interface cards (NIC)
  - This was fine for the original plan
  - Now we have two options
    - Add a NIC to the computers involved in the VME processor boot infrastructure
    - Modify the network connections
- Testing VME processor booting
  - As of 3/22/2016 I don’t have any NIC cards in hand
  - Instead the network connections at DZero will be modified to accommodate the boot infrastructure needed

VME Network Boot at DAB, 3/22/2016 – 1/2



VME Network Boot at DAB, 3/22/2016 - 2/2

- Network Changes
  - Use the unmanaged switch for the private network
    - At SciBoone this will use the 48-port switch and a registered private network, non-registered will work at DAB for now
  - No changes to annie-gw02
  - Connect vme 10/100 NIC to private network
  - Connect vme 1GB NIC to public network
    - Request public IP address
  - Connect annie-daq02 to private network
    - Keep public network connection
  - Block access to public IPs for daq02 and vme
    - Logins to daq02 must now go through gw02
    - Official change request from the network group required
- Software configuration
  - Sys admins: configure dhcp and nfs server for daq02
    - Jonathan provides software requirements
  - Jonathan modifies vme board configurations and tests

Computer Descriptions

- Scientific Linux Fermilab (SLF)
  - Scientific Linux (SL) with Fermilab configured Kerberos support
  - SLF4 does not meet the Fermilab security baseline as SLF4 is no longer supported
  - Current version is SLF6 (SLF7 is on the horizon)
- Computers
  - Unsupported Operating System (OS) – private network
    - Windows 10 computer – high voltage (Marcus/Matthew)
    - SLF4 Linux embedded processor in VME crate (Jonathan Eisch)
  - SLF6 Linux computer for CAMAC (Matt/Carrie)
    - USB to CAMAC controller (CCUSB)
  - SLF6 Linux computers (Ben, depends on DAQ requirements)
    - DAQ
    - Data storage – disk array
    - Monitoring
    - Run Control
  - SLF6 Linux computer for gateway (x2)
    - Provide access to other computers
  - SLF6 Linux workstation at SciBoone Hall
    - In case you forget to bring your laptop
- Always have a least two identical computers for each function.

Computer Inventory

- DAQ computers
  - annie-daq01
  - annie-daq02
- Gateway computers
  - annie-gw01
  - annie-gw02
- Control room computers
  - annie-cr-01
  - annie-cr-02
- Test stand systems (shared home area in nfs)
  - annielx01
  - annielx02
- s-access-sciboone-1 (8-port switch)
  - Vlan 194
  - http://mrtg.fnal.gov/MRTG-SiteMap/MiniBooNE.html
  - Mitpc = 131.225.194.136

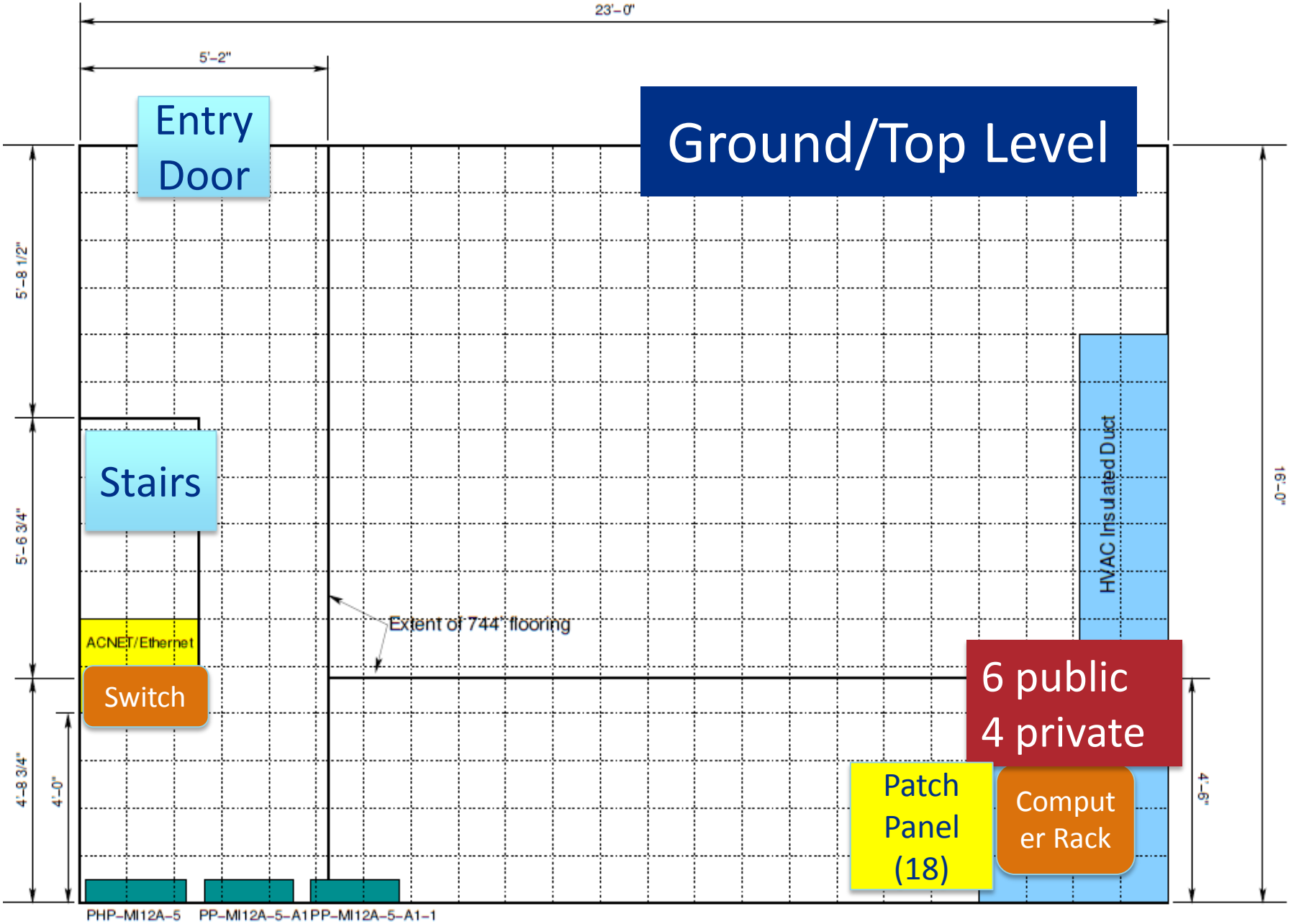
Network Switch Location Decision

- In consultation with the networking group we will be installing the 48-port network switch where the 8-port network switch is currently located at SciBoone
- We entertained the idea of putting the switch in a computer rack if the computer rack was on the middle level to minimize the length of the copper network cables.
- The computer rack is on the top level so we will not be moving the new network switch to a different location.
- Instead we will be running copper cables from the top level to the necessary locations in the SciBoone Hall.
- My recommendations for these cable runs are in the next few slides.

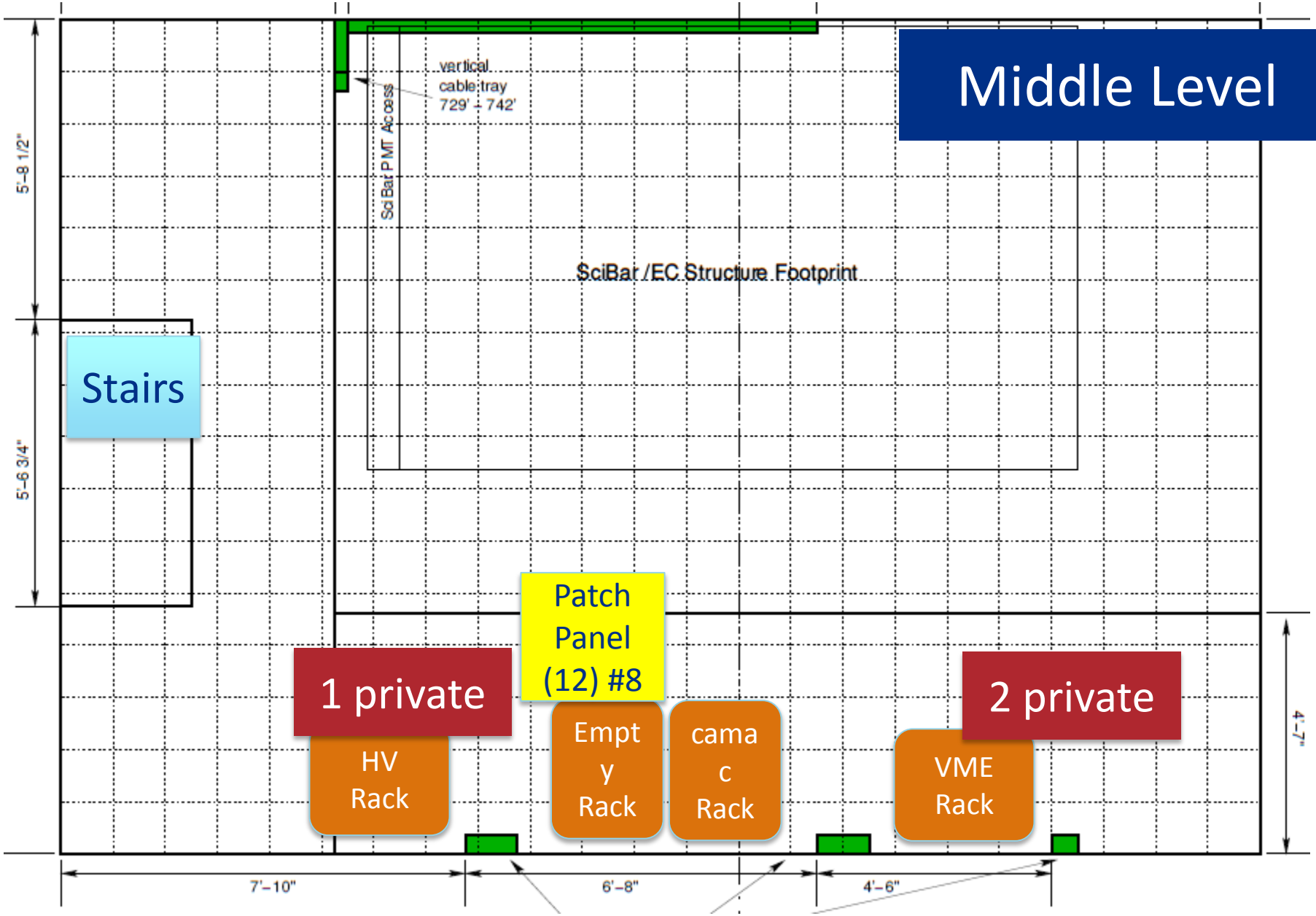
Network Patch Panel Placement

- Ground/Top Level
  - Short computer rack in the far corner away from the entry door
  - 18 spigots on patch panel
    - Four computers on public and private network (8 spigots)
    - Serial console server (1 spigot)
    - Networked PDU (1 spigot)
    - 8 spigots for expansion
- Middle Level
  - Rack #8 under the splitter panel at the top
  - 12 spigots on patch panel
    - Three private network devices
    - Much uncertainty in needing additional computers here
- Bottom Level
  - No idea where to put a patch panel
  - 6 spigots on patch panel
    - One spigot for MITPC
    - One spigot for ANNIE workstation
  - The ANNIE water tank takes up most of the floor space on the bottom level
  - I don’t see additional computing on this level

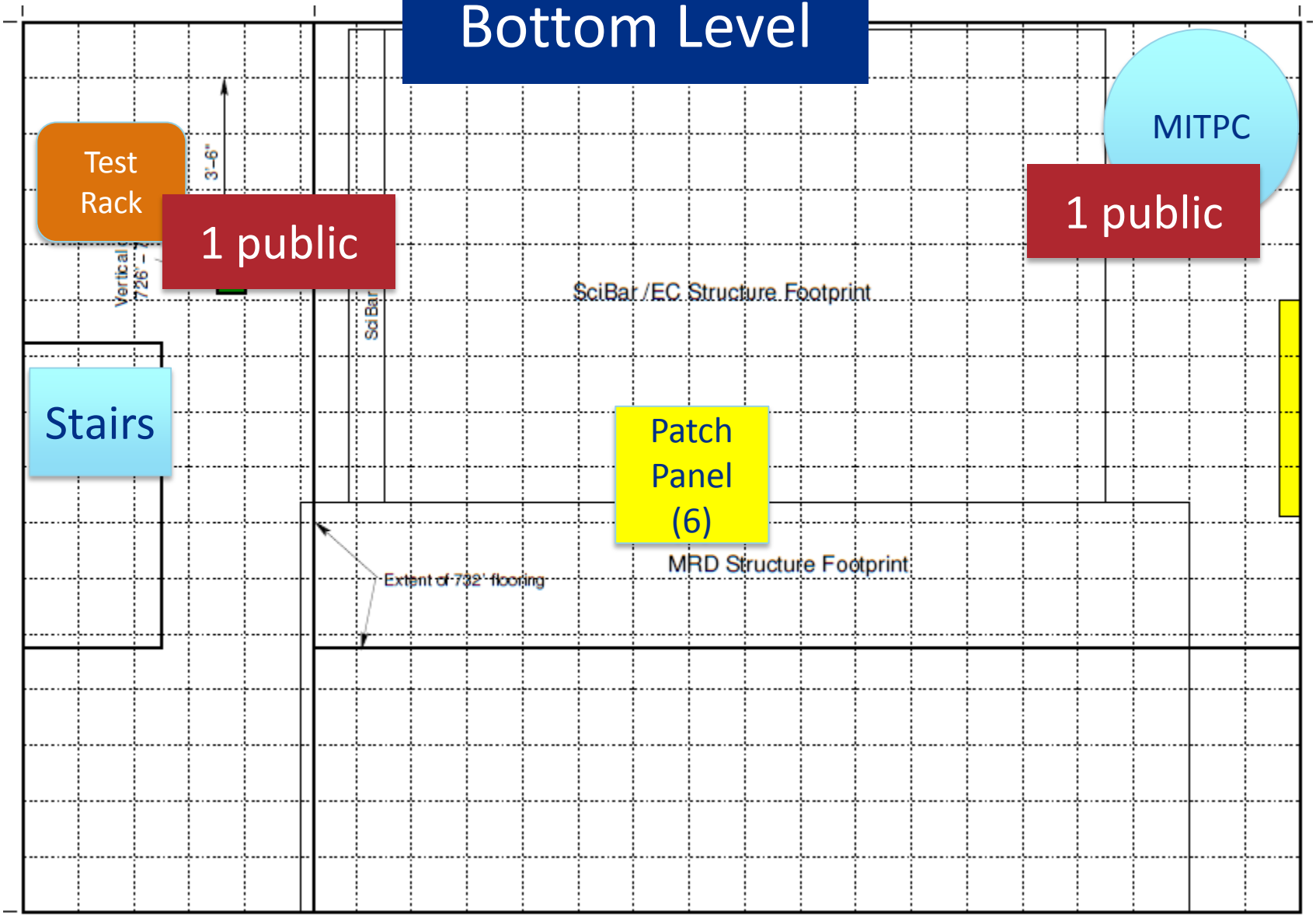
Ground/Top Level



Middle Level



Bottom Level



BACKGROUND INFORMATION

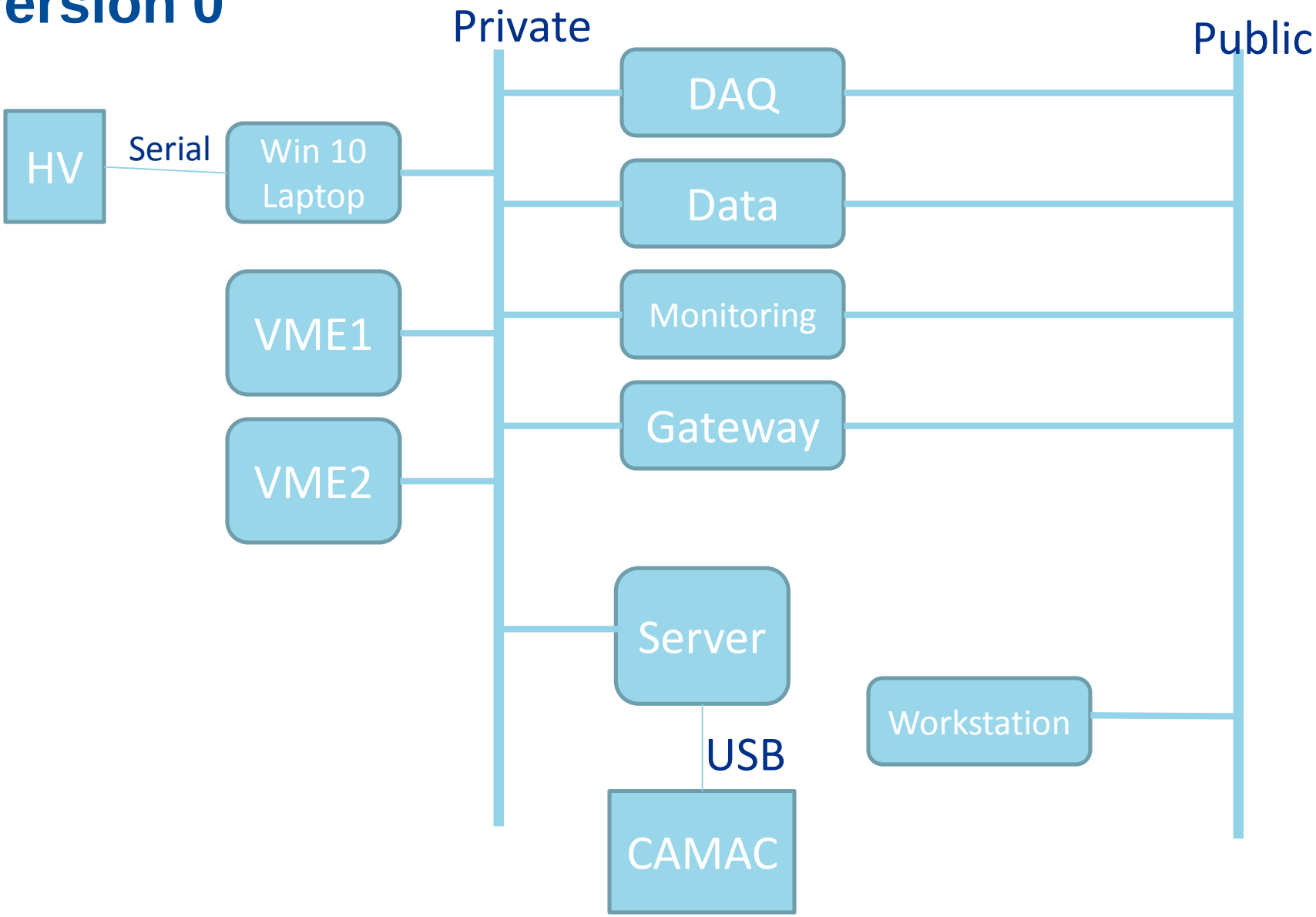
Items for Discussion

- Can the equipment in each VLAN be in different physical locations?
  - What is the performance penalty for having a VLAN span multiple switches?
  - Answer – put computers at SciBoone
- How do we handle outside access from the vme computers?
  - Developers would like to pull data from a repository onto systems in the private vlan for software updates
  - NTP access
  - Answer – routable network
- We need this configuration at Dzero for testing and at SciBoone for production
- GigaBit network connections in both vlans

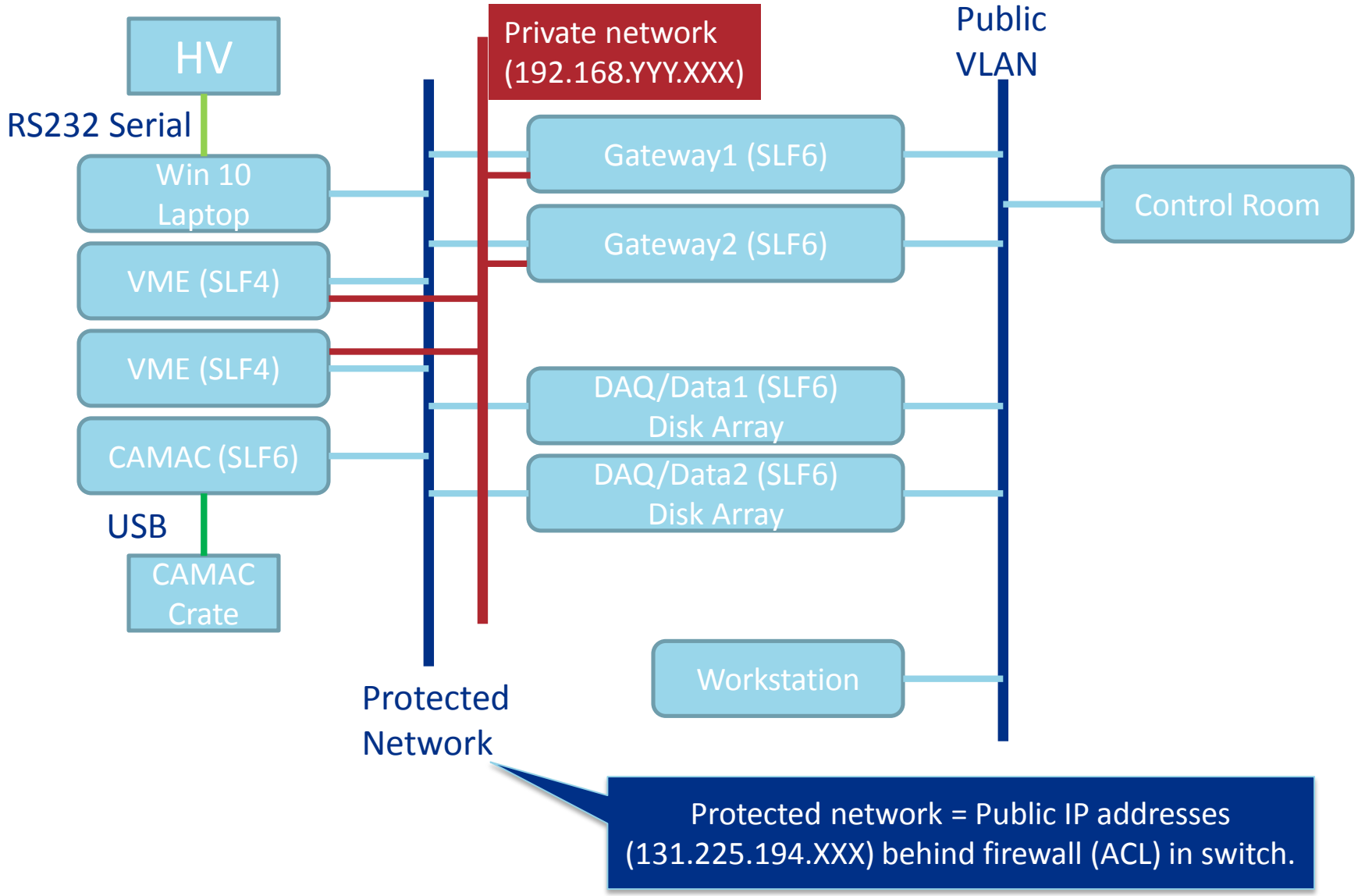
From Ben Richards (2/8/16)

- Jonathan and i sat down and worked out rough data rates for the VME before of 41Mb/s. However that's raw data and there will be a little overhead due to wrapper and things but i wouldn't have thought it was far off. The Psec4 was about 2Mb/s. Other parts eg. Camac and HV I dont know.
- [by the way it would be good if we could combine the DAQ HV and Camac into a single Framework for control and monitoring]
- I am attaching the slides for a talk i made in one of the meetings a while ago that summarised the FADC data rate (see first slide).
- However I have a couple of questions about the slides from Geoff as it will change the data rates.
  - in slide 2 there seems to be separate machines for DAQ, monitoring, Data, and Gateway. Slide 3 says SLF6 Linux computers – DAQ – Data – Monitoring Is this correct? are they intended as separate physical computers or just logical service blocks?
  - I mention this as i thought a single rack mounted server was to run the DAQ, web server, psql server, data storage and possibly gateway. If they are separate your network data rates will increase a lot as all the data to be stored has to pass from the DAQ machine to data storage as well as all the other associated communications. It also means i have to add extra parts to the code to send these messages over the network. This of course can be done, but at the moment hasn't as was going to be on a single computer.
  - From memory Matt mentioned that only a single Ethernet connection to the outside world of Fermilab. This can be expanded with a switch of course, but slide 2 seems to have the DAQ, Data, Monitoring and Gateway bridging the public and private network. I would be very happy if this was the situation however i thought the idea was to use a gateway to bridge the public and private networks?

Version 0


Private
Public
HV
Serial
Win 10 Laptop
VME1
VME2
DAQ
Data
Monitoring
Gateway
Server
USB
CAMAC
Workstation

ANNIE Group Account

- Everyone who reported kerberos principals is not in the .k5login files yet. That's next after this email. So everyone won't be able to login.
- savage@FNAL.GOV
- billl@FNAL.GOV
- wetstein@FNAL.GOV
- jpodczer@FNAL.GOV
- mcgivern@FNAL.GOV
- mchen@FNAL.GOV
- vfischer@FNAL.GOV
- moflaher@FNAL.GOV
- mmalek@FNAL.GOV
- txin@FNAL.GOV
- ecatanom@FNAL.GOV
- msanchez@FNAL.GOV
- brichard@FNAL.GOV
- rsvoboda@FNAL.GOV
- jeisch@FNAL.GOV
- Login as annie on these systems.

Network, Logical – Incorrect Implementation