Baseline Assessment Report

Performed for:

ECR | **EL CAMINO REAL CHARTER HIGH SCHOOL**

EL CAMINO REAL CHARTER HIGH SCHOOL

Date of Report	09/04/2019
Revision	6
Assessed By	James Joyner

Contents

Executive Summary

El Camino Real Charter High School (ECRCHS) engaged NIC Partners to perform an IT infrastructure audit in order to ensure that they have all the equipment in place to support their planned technology requirements. The infrastructure to be included in the assessment included the following: routing, switching, cabling, wireless access points, a wireless heat map performed during regular school hours datacenter, network security, and printer connectivity.

The sections below detail the scope of the assessment and the high-level findings. NIC Partners invites ECRCHS to further discussion regarding any element of this report. Supplemental data including reports from Ekahau wireless survey software, the printer discovery information, and the cabling discovery information, shall be provided as separate deliverables.

The overall state of the network could be described as 'very good'. The routing/switching design is solid, wireless coverage and performance are satisfactory in classroom areas, and IT is making use of important security features at both the network perimeter and the endpoints. With a planned Internet capacity of 5 Gbps (and a 1 Gbps backup circuit), ECRCHS meets the bandwidth recommendations set forth by SEDTA and the FCC.

High-level recommendations for future projects include:

- Implement redundancy in the network core and perimeter to ensure continued network update in the event of a hardware failure
- Some network equipment has passed the 'end of sale' date, but the 'end of support' dates have not yet been published by the manufacturer. HPE will typically support equipment up to five years beyond the 'end of sale' date. It is recommended to check with the manufacturer for the true "end of support" date and allocate budget to replace the equipment prior to the 'end of support' date.
- The current wireless access points support the 802.11AC Wave 1 protocol. This is sufficient for today's wireless clients, but newer clients will have support for the 802.11AX protocol. The newer protocol adds features that lead to increased speed in the dense wireless environments prevalent in schools. It may not be economically feasible to replace wireless access points as soon as new technology is released; it may be more prudent to establish a budget for a cyclical refresh of wireless equipment every ~3-5 years.

Scope of Discovery

Network Devices

Data was collected on the following types of network devices:

- Routers/Switches
- Wireless Infrastructure
- Network Security (firewalls, VPN, content filters)
- Datacenter Equipment
- Printers

Supplemental Collection and Discovery

Additional areas of data collection and assessment (included as a Data Addendum):

- Assessment of Cabling
    - Identifies MDF/IDF locations and indicates on map
    - Identifies and documents fiber type and quantities
    - Identifies on map where the fiber traverses
    - Identifies and documents copper patch cable type and quantities
- Wireless Heat Map Assessment
- Printer Inventory Assessment

Tools Used

NIC Partners used the following tools to gather data from the network and interpret the results:

- NetformX DesignExpert
- NetBrain Workstation CE
- Interviews with ECRCHS
- Site walks

Business Requirements

Technology-related Goals and Objectives

At the time of this writing, all established technology-related goals or objectives have been implemented. ECRCHS is finalizing a UPS project that will provide more stability of electrical infrastructure and reduce downtime caused by power fluctuation or outage.

Future Plans Affecting Network Infrastructure

Campus Additions, Closures, or Changes

None expected at this time

Plans for Campus Modernization

ECRCHS will want to consider the replacement aging hardware and physical infrastructure. Hardware refresh discussions have been considered internally by ECRCHS, but timelines have not yet been established.
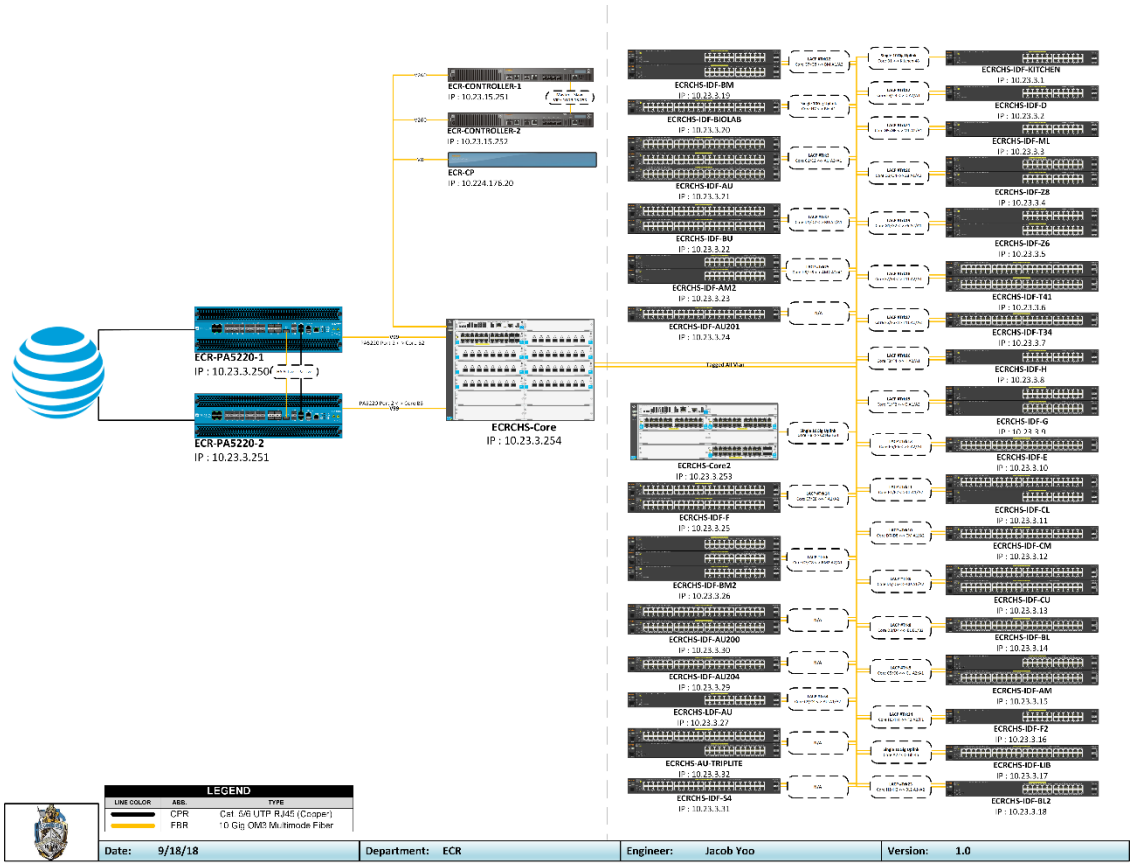
Business-critical Services

Critical Applications on Network Infrastructure

The services critical to ECRCHS are wireless services (1-to-1 network), the next-gen firewall features within the Palo Alto firewalls, VoIP/Jive, and Aeries.

Findings

Routers/Switches

Routers/Switches: Inventory

The table below shows the quantities of individual switches, by model. Note that many of these switches are stacked or modules within a chassis of a modular switch. Stacked switches and modules within the chassis will often appear as a single logical entity with modules or blades instead of individual units. The data below, however, was based on individual switch units rather than stacks.

Model	Description	TOTAL
J9727A	**Aruba 2920 24G POE+ Switch**	22
J9729A	**Aruba 2920 48G POE+ Switch**	26
J9986A	**24-Port Gigabit PoE+ v3 ZL2 Mod**	2
J9990A	**Aruba 20p PoE+ / 4p SFP+ v3 zl2 Mod**	2
J9993A	**Aruba 8p 1G/10GbE SFP+ v3 zl2 Mod**	6
	Grand Total	**58**

The two charts below show the relative quantity of each switch model.

Donut chart legend:
- ■ 24-Port Gigabit PoE+ v3 ZL2 Mod J9986A — 4%
- ■ Aruba 20p PoE+ / 4p SFP+ v3 zl2 Mod J9990A — 3%
- ■ Aruba 2920 24G POE+ Switch J9727A — 38%
- ■ Aruba 2920 48G POE+ Switch J9729A — 45%
- ■ Aruba 8p 1G/10GbE SFP+ v3 zl2 Mod J9993A — 10%

Bar chart values:
Model	Quantity
J9986A — 24-Port Gigabit PoE+ v3 ZL2 Mod	2
J9990A — Aruba 20p PoE+ / 4p SFP+ v3 zl2 Mod	2
J9727A — Aruba 2920 24G POE+ Switch	22
J9729A — Aruba 2920 48G POE+ Switch	26
J9993A — Aruba 8p 1G/10GbE SFP+ v3 zl2 Mod	6

Most switches on the ECRCHS network are Aruba 2920 48-Port PoE+ (J9729A) and Aruba 2920 24-Port PoE+ (J9727A). The core switches are Aruba ZL2 modular switches, each containing multiple line cards.

ECRCHS utilize two (2) Aruba 5400R LZ2 modular switches at the core of their network. The largest of these switches is an Aruba 5412R LZ2, populated with one (1) Aruba 5400R zl2 Management Module J9827A, one (1) Aruba 20p PoE+ / 4p SFP+ v3 zl2 Mod J9990A, and six (6) Aruba 8p 1G/10GbE SFP+ v3 zl2 Mod J9993A. Expansion of this switch is currently possible, as the switch has five (5) open/available line card slots and one (1) open/available management slot.

The second core switch is an Aruba 5406R LZ2, populated with one (1) Aruba 5400R zl2 Management Module J9827A, two (2) Aruba 24-Port Gigabit PoE+ v3 ZL2 Mod J9986A, and one (1) Aruba 20p PoE+ / 4p SFP+ v3 zl2 Mod J9990A. Expansion of this switch is currently possible, as the switch has three (3) open/available lien card slots and one (1) open/available management slot.

Both Aruba 5400R LZ2 switches feature hot-swappable redundant power supplies and cooling fan trays.

The 5400R LZ2 modular switches can utilize multiple management modules within the same chassis, in an active/standby configuration, to eliminate the downtime caused by a management module hardware failure. Implementing a second management module within the 5400R LZ2 switches would allow ECRCHS to utilize non-stop routing and switching to continue traffic during a failover from the active management controller to the standby.

It is recommended by NIC Partners to provide core switching and routing redundancy to maximize uptime and reduce the impact of a failure within the network.

HPE/Aruba J9729A | 2920-48G-PoE+

HPE/Aruba J9990A

HPE/Aruba J9727A | 2920-24G-PoE+

HPE/Aruba J9993A

HPE/Aruba J9986A

Routers/Switches: EoX Milestones

The data below indicates devices which have reached certain end-of-life milestones, as described in the visual alerts legend.

At this time, it appears that ECRCHS's Aruba 2920 POE+ switches have reached the 'end of sale' milestone. This means that HPE/Aruba is no longer manufacturing these devices and will generally discontinue support and engineering for the product after five years. NIC Partners recommends replacing these items as soon as budget permits.

The good news is that none of the Brocade ICX switches discovered in the network are listed on Brocade's product end-of-life portal.

EoX Milestones visual alerts legend color schema:

EoX Milestone	Visual	Description
EoS		End of Sale (No more orders for the item)
EoE		End of Engineering (No more updates for the item)
LDoS		Last Day of Support

Total Qty	Description	Model	EoS	EoE	LDoS
23	Aruba 2920 24G POE+ Switch	J9727A	3/31/18	3/31/23	3/31/23
27	Aruba 2920 48G POE+ Switch	J9729A	3/31/18	3/31/23	3/31/23
1	Aruba 5406R zl2 Switch Chassis	J9821A	current	current	current
1	Aruba 5412R zl2 Switch Chassis	J9822A	current	current	current
2	Aruba 5400R zl2 Management Module	J9827A	current	current	current
2	Aruba 5400R 2750W PoE+ zl2 PSU	J9830B	current	current	current
2	24-Port Gigabit PoE+ v3 ZL2 Mod	J9986A	current	current	current
2	Aruba 20p PoE+ / 4p SFP+ v3 zl2 Mod	J9990A	current	current	current
6	Aruba 8p 1G/10GbE SFP+ v3 zl2 Mod	J9993A	current	current	current

Routers/Switches: Software Versions and Recommendations

The table below shows the version of operating system software that is present on the discovered switches, along with the version of operating system that is current by the manufacturer. For stability and security, the manufacture recommends using the current release of the operating system software recommended for the device. Using a release older than the current release is not recommended and may contribute to technical issues or expose vulnerabilities within the network.
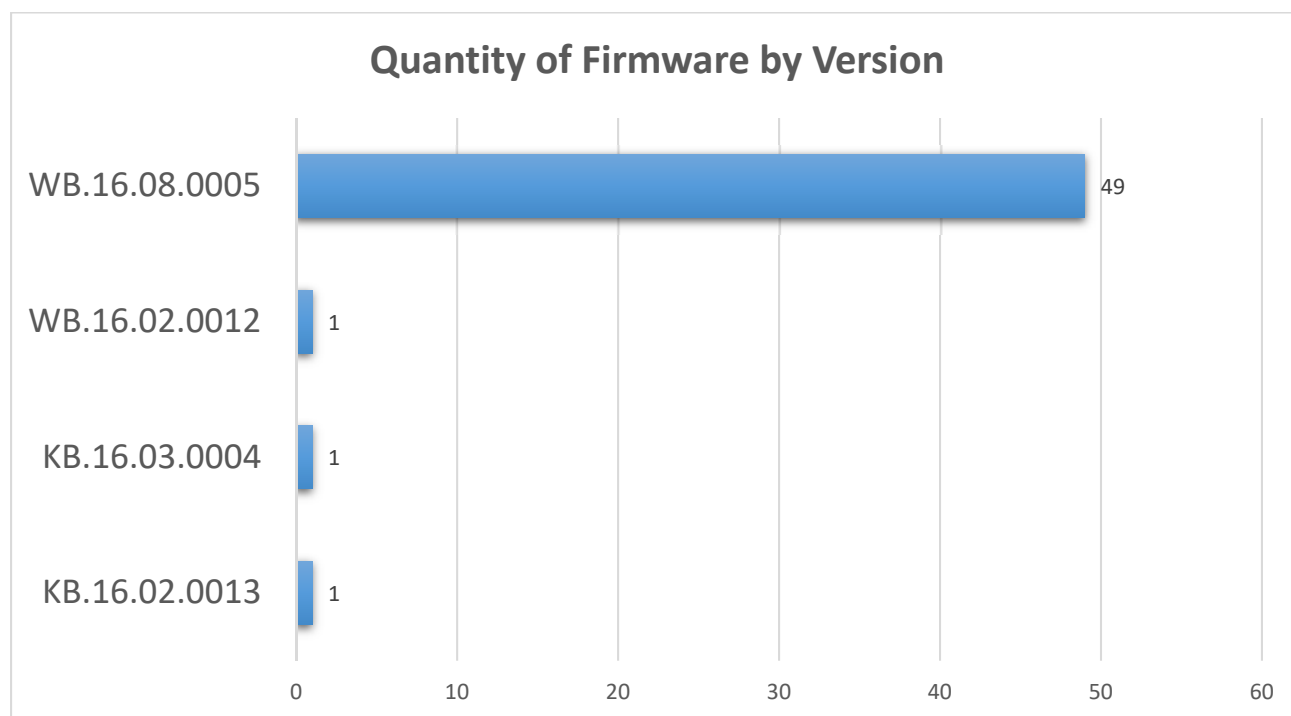
NIC Partners recommends upgrading all older release versions to a current release version within the same software branch. For example, the Aruba J9727A (ECR_DMZ) is currently on the software branch WB.16.02, using revision x.0005 but the current release of that branch is x.0027. NIC Partners recommends upgrading this switch to either WB.16.02.0027 or upgrading the branch to WB.16.08.0005.

Both versions would be acceptable, as they are both listed under the current release section of the software download page.

#	Manufacturer	Model	Installed Version	Current Version(s)	Recommendation
27	HPE/Aruba	J9729A	WB.16.08.0005	WB.16.08.0005	No Change
22	HPE/Aruba	J9727A	WB.16.08.0005	WB.16.08.0005	No Change
1	HPE/Aruba	J9727A	WB.16.02.0012	WB.16.02.0027	WB.16.08.0005	Upgrade
1	HPE/Aruba	J9821A	KB.16.02.0013	KB.16.02.0027	KB.16.03.0007	Upgrade
1	HPE/Aruba	J9822A	KB.16.03.0004	KB.16.03.0007	Upgrade

The graph below shows a quick overview of how many devices on the network are running each discovered version of software. The vast majority of Aruba 2920s are running version WB.16.08.0005, which is listed as a current release within the HPE software download portal.

Quantity of Firmware by Version

Version	Quantity
WB.16.08.0005	49
WB.16.02.0012	1
KB.16.03.0004	1
KB.16.02.0013	1

Components Assessed

- **Backbone port speed/capacity**

    o The campus network is typically divided into edge ports and backbone ports. The edge ports, which connect to PCs, wireless access points, and other networked devices, are aggregated into a small number of backbone ports for transport between IDFs and/or the WAN/Internet. Therefore, it is important that the backbone has enough capacity to quickly transport traffic from several edge ports simultaneously.

- **Edge port speed**

    o The main purpose of a network switch is to take data from one or more edge ports and aggregate it into a higher-speed backbone port for connectivity throughout the campus.

    o Edge ports in the campus network will be connected to devices like PCs, laptops, wireless access points, IP phones, and Internet-of-Things (IoT) devices. The vast majority of these devices will have Gigabit network cards installed. Older units, or devices that don't require much throughput, might have 10 or 100 Mbps network cards. Servers and storage devices that connect at higher speeds will typically plug into dedicated datacenter switches, so they are not accounted for when planning for campus networks.

    o Some switches support 'multi-gigabit' ports for connecting to high-speed wireless access points. These ports are capable of running 2.5 Gbps, 5 Gbps, or even 10 Gbps over copper cables along with providing power-over-Ethernet on the same cable.

- **Edge port power-over-Ethernet (PoE) capabilities**

    o Network switches are often used as a convenient way to power the devices plugged into them. Not only can this cut down on expensive electrical wiring, but some switches can support time-based scheduling for PoE, which means that unused devices can be shut down at night or on weekends to save power.

    o Classrooms will typically have one or more devices that receive power from switches.

        ▪ Modern wireless access points typically require 802.3at power standards, which means they can draw up to 30W of power each.

        ▪ IP phones might require 802.3af power standards, which means they will draw between 7W and 15.4W of power each.

        ▪ Video surveillance cameras may draw PoE. Energy efficient models may draw as little as 15.4W while PTZ models might draw 30W-60W each.

- **Switch redundancy**

    - A well-designed network would eliminate as many single points of failure as possible. Providing redundancy for edge switches might not be the most efficient use of the network budget, but it could be argued that providing redundancy for core switches at each campus is an expedient use of monetary resources. The core is what all of the edge switches plug into; an outage in the core would affect the ENTIRE network while an outage at the edge would only affect a portion of the network.

    - Some network switches have features that enable quick recovery from outages. Some platforms have self-healing features that diagnose issues and automatically reboot services that are malfunctioning. Other platforms might take advantage of stacking technologies such that an outage of a single switch in an IDF would result in the other switches staying online and connected.

Backbone Port Speed/capacity   Score: 4/5

1 = Single 1 Gbps uplink from IDF to core

2 = Multiple (aggregated) 1 Gbps uplinks from IDF to core

3 = Single 10 Gbps uplink from IDF to core

4 = Multiple (aggregated) 10 Gbps uplinks from IDF to core

5 = 40+ Gbps uplink from IDF to core

Notes

- Most IDFs across the ECRCHS campus have multiple 10 Gbps uplink to the campus core. From there, the 10 Gbps WAN connects switches to the datacenter and Internet.

Analysis

With the transition towards single-mode fiber in the campus backbone comes the ability to run very high speeds on the backbone network. Some high-end campus LAN switches position 40 Gbps or 100 Gbps as the target speed for backbone ports. Unfortunately, the cost for 40G or 100G transceivers can be very expensive. The current sweet spot for education is probably the aggregation of two or more 10 Gbps ports from each IDF to the MDF. If redundant core switches are utilized in the MDF, it makes sense to provide dual 10G ports from the IDF and aggregate them together for an increase in usable capacity.

To prevent unnecessary outages caused by failing infrastructure or connectivity faults, NIC Partners recommends the use of redundant switching, that utilizing multiple 10Gbps uplinks back to the core, for all network segments that are critical to ECRCHS day-to-day operations.

Edge Port Speed/capacity <u>Score: 4/5</u>

1 = Less than 100 Mbps

2 = 100 Mbps

3 = n/a

4 = 1,000 Mbps

5 = Multigigabit capability (2.5G/5G/10G)

Notes

- Aruba 2920 switches provide 1 Gbps to the edge.

Analysis

The speed for wired endpoints in the classroom tends to be targeted towards the 1 Gigabit (1,000 Mbps) mark. Any speed above that would likely overwhelm the backbone ports, which typically run at 10 Gbps. The only situation where it currently makes sense to go above 1 Gbps (outside of the datacenter) is for connectivity to wireless access points. To provide for faster uplink speed to wireless access points - while still providing PoE over copper - some switches will provide a small quantity of 'multigigabit' ports. These ports are capable of pushing 2.5 Gbps – 10 Gbps over copper cabling. The maximum speed of these ports is determined by the type and quality of the copper cable used between the switch and the wireless access point.

In ECRCHS's environment, 1 Gbps to the edge is currently sufficient. If the high school WAN links are ever increased beyond 10 Gbps, it might make sense to look at multigigabit switch ports for the 802.11AC Wave 2 and future 802.11ax wireless access points.

Edge Port PoE Capabilities   <u>Score: 3/5</u>

1 = No PoE or pre-standard PoE

2 = 802.3af (type 1), 15.4W per port

3 = 802.3at (type 2), 30W per port – up to 12 ports @ 30W

4 = 802.3at (type 2), 30W per port – up to 24 ports @ 30W

5 = 802.3bt (type 3/4), 60W per port

Notes

- 802.3bt is expected to be standardized in September of 2018, but is not yet a standard. Some manufacturers have developed pre-standard technologies (such as Universal PoE) that are capable of delivering 60W per port and beyond.

- Aruba 2920-48G-PoE+ can power up to 12 ports at 30W per port with the internal power supply. Adding an external power supply will allow all 48 ports to provide 30W of PoE.

Analysis

Higher PoE capabilities are better, as a switch with higher PoE budgets can power more devices and devices that have high power requirements. A proper PoE design would take into consideration the capacity of the electrical circuits feeding the switches; care must be taken to not overload the typical 15A circuits found in most environments. Consider that a dedicated 15A circuit at 120V will provide ~1,800W of power. Three switches providing 30W of power per port, at 24 ports per switch, will result in ~2,160W of power (and an overloaded circuit). Note, however, that most networked devices will not pull their maximum PoE budget at all times, so it is unlikely that all ports would be providing 30W of power at the same time.

NIC Partners recommends working with the Facilities team to provide extra electrical circuit capacity to the IDFs prior to an equipment refresh. At the very least, the IT Department needs to be aware of the inline power requirements vs the electrical capacity in each IDF.

Switch Redundancy   Score: 1/5
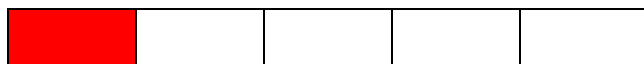
1 = No redundancy.

2 = Portion of core switches have a redundant partner. IDFs connected to only one core switch.

3 = Portion of core switches have a redundant partner. Critical IDFs connected to both.

4 = Each core switch has a redundant partner. Each IDF is connected to both core switches.

5 = Each core switch has a redundant partner. IDFs are connected to both. Dual power supplies/grids.

Notes

- ECRCHS has two core switches, in different form factors, but the switches are not configured for redundancy and would not prevent an outage caused by a core switch failure.

- With few exceptions, IDF switches are home-run to MDF.

- Stacked switches utilize multiple uplink to MDF.

Analysis

Adding redundancy for the District's core equipment could significantly assist with overall network uptime. Having two core switches, configured for redundancy, eliminates the threat of downtime from:

- Software glitch affecting an individual device

- Software update procedure which requires reboots

- Issues affecting a single strand or pair of fiber between IDF and MDF

- Failure of core switch's power supply

For these reasons, best practices for enterprise-grade networks include the use of redundant hardware in places where uptime is critical (i.e. core switches).

Wireless

Wireless: Inventory

The table below shows the quantity of wireless devices installed throughout ECRCHS's campus.

Manufacturer	Model	Qty
HPE/Aruba	7210 Controller	2
HPE/Aruba	AP-224	42
HPE/Aruba	AP-225	288

Aruba 7210 Mobility Controller

13%

■ AP-225

■ AP-224

87%

Aruba AP-225

Aruba AP-224

AP QUANTITY

AP-224 42

AP-225 288

0   50   100   150   200   250   300   350
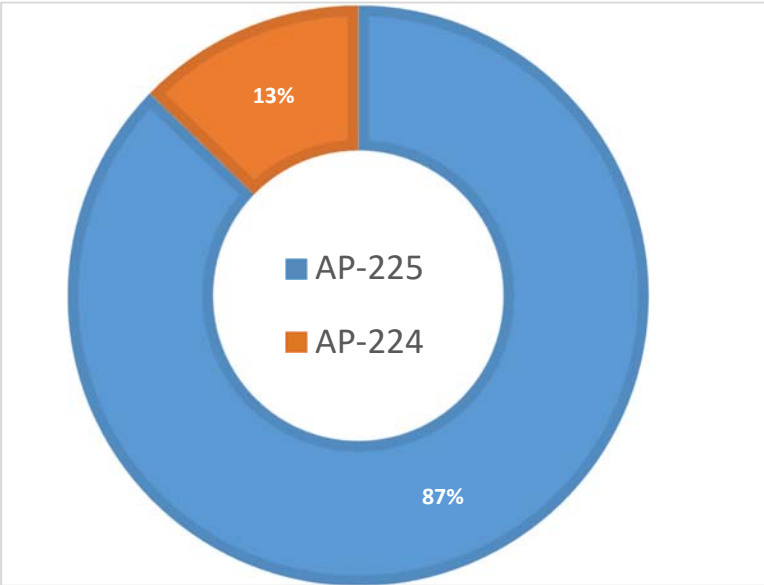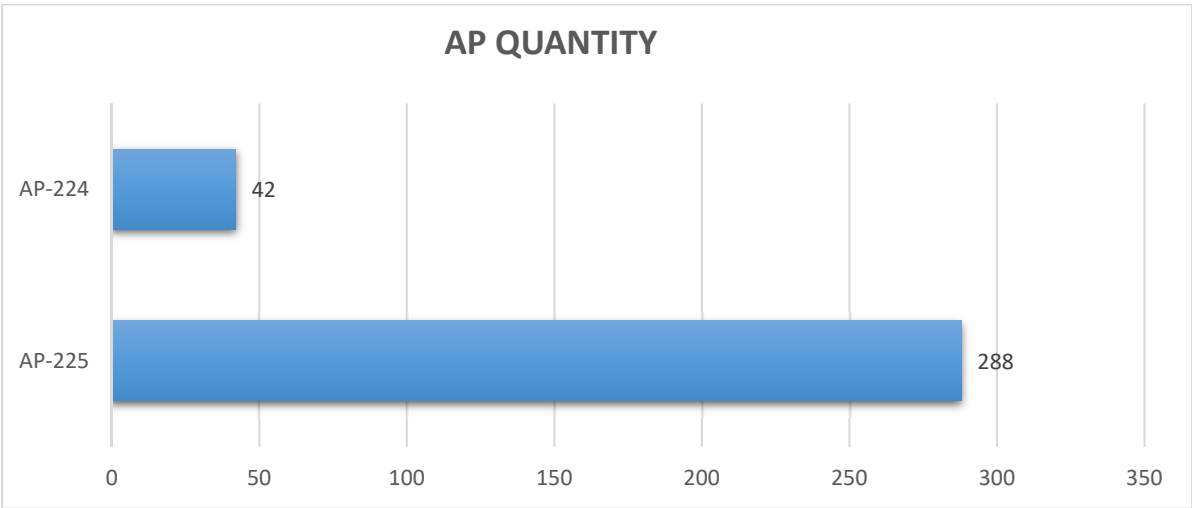
Wireless: EoX Milestones

The data below indicates devices which have reached certain end-of-life milestones, as described in the visual alerts legend.

According to the End-of-Life Product Listing published by Aruba, none of the documented wireless devices have end-of-life data published, which means they are current models that will be supported by Aruba for at least five years.

EoX Milestones visual alerts legend color schema:

EoX Milestone	Visual	Description
EoS		End of Sale (No more orders for the item)
EoE		End of Engineering (No more updates for the item)
LDoS		Last Day of Support

Qty	Manufacturer	Model	EOS	EOE	LDoS
2	HPE/Aruba	7210 Mobility Controller	current	current	current
42	HPE/Aruba	AP-224	current	current	current
288	HPE/Aruba	AP-225	current	current	current

Wireless: Software Versions and Recommendations

The table below shows the version of Aruba operating system software that is present on the wireless access points, along with the version of operating system that is current by the manufacturer.

NIC Partners recommends using the current software revision released by the manufacturer, unless there are specific limitations which restrict the ability to upgrade the versions of the software.

Model	Installed Version	Current Version	Recommendation
Aruba7210	6.5.4.10_67757	6.5.4.13_71051	Upgrade

Aruba advises upgrading ArubaOS to a minimum version of 6.5.4.13 to address serious vulnerabilities present in older versions running on the Aruba Mobility Controller. An attacker could use these vulnerabilities to execute arbitrary code on the underlying operating system with full system privileges.

NIC Partners recommends upgrading both Aruba 7210 Mobility Controllers to ArubaOS 6.5.4.13 or later.

Additional information from the manufacturer:
https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2019-004.txt

Components Assessed

- **Speed**

    o The overall 'speed' of a wireless access point is typically determined by the wireless protocol standard it supports as well as the number of transmit & receive antennas available. This results in a maximum 'physical' interface speed, although the actual speed provided to the clients depends heavily on the capabilities of the clients. Additional factors to take into consideration include wired uplink port speed and beamforming capabilities.

- **Radio capacity**

    o The capacity of a wireless access point is largely determined by the number of radios per unit with the caveat that most clients are using 5 GHz service and few are using 2.4 GHz service. Beyond that, the manufacturer's design and software will make a difference in how well the wireless clients can be serviced in dense environments. Here is where you will find a manufacturer brag about large amounts of DRAM, air-time fairness rules, or code which is optimized to handling dense environments.

- **Spectrum Analysis**

    o In today's dense wireless environments, it is common to find devices that can interfere with the wireless signal. Therefore, it is important for the wireless access point to be able to rapidly detect these interfering signals and adjust themselves accordingly. The best designs will include a radio that is dedicated to performing real-time spectrum analysis and can act upon real-time events with containment protocols or channel adjustments.

- **Manageability**

    o The ability to manage a solution is a very important factor to the success of a wireless network. The management software should ideally be accessible from anywhere (including a mobile device), and should provide real-time reports with clear indications about what the potential issues are and how they can be remedied. If the wireless access points are dependent upon the management software for its resources, then the reliability of this component could easily affect the reliability of the entire solution.

- **Guest/BYOD Accessibility**

    - A modern wireless platform should have an easy way to create guest and BYOD portals which are used to on-board clients and enforce security rules (i.e. prevent access to internal resources). There should be disparate ways to enforce access permissions, such as displaying acceptable use agreements, allowing for sponsored access with time limits, and using two-factor authentication to tie a user's identity to an email address or phone number.

Speed   Score: 2/5
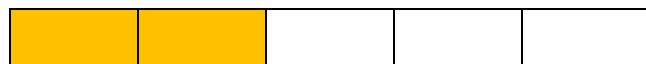
1 = 802.11N or earlier

2 = 802.11AC Wave 1, 2x2:2 or better

3 = 802.11AC Wave 2, 2x2:2

4 = 802.11AC Wave 2, 3x3:3

5 = 802.11AX 4x4:4 or better

Notes

- ECRCHS has the following types of APs installed:

  - (42) Aruba AP-224   13%   802.11AC Wave 1, 3x3:3

  - (228) Aruba AP-225   87%   802.11AC Wave 1, 3x3:3

Analysis

All ECRCHS's wireless access points are 802.11AC Wave 1 (3x3:3).

In general, it is rare to find low-cost wireless clients that have more than 2 transmit/receive spatial streams. At first appearance it may seem like wireless access points with 3 or 4 antennas are overkill. Modern wireless access points, however, can use extra antennas to improve the signal for its clients through the use of beamforming technologies.

The 802.11AC Wave 2 and 802.11AX protocols provide new features such as multi-user MIMO (MU-MIMO), which increases total network performance and improves the end user experience in dense environments. Therefore, NIC Partners highly recommends the use of enterprise-grade 802.11AC Wave 2 or 802.11AX wireless access points in all classrooms and areas where multiple wireless devices will be used (gyms, libraries, MP rooms, etc).

Radio Capacity Score: 5/5

1 = Single 2.4 GHz radio, entry-level hardware design

2 = Single 2.4 GHz radio + single 5 GHz radio, entry-level hardware design

3 = Single 2.4 GHz radio + single 5 GHz radio, mid-level hardware design

4 = Single 2.4 GHz radio + single 5 GHz radio, hardware optimized for capacity

5 = Dual software-assigned radios (2.4 or 5 GHz), hardware optimized for capacity

Notes

- ECRCHS has the following types of APs installed:
    - (42) Aruba AP-224   13%   Category 5 (dual software-defined radios)
    - (228) Aruba AP-225   87%   Category 5 (dual software-defined radios)

Analysis

All ECRCHS's wireless access points fall in the high-capacity category. This means that they have software-defined radios which can adjust themselves to handle large quantities of 802.11n or 802.11AC clients in a small geographical region (i.e. classroom).

Spectrum Analysis　　　　　Score: 4/5

1 = No capability for spectrum analysis

2 = Shares existing radio(s) for spectrum analysis, can only detect wifi interferers

3 = Shares existing radio(s) for spectrum analysis, can detect non-wifi interferers

4 = Shares existing radio(s) for spectrum analysis and wireless security, can detect non-wifi interferers

5 = Dedicated radio for spectrum analysis and wireless security, can detect non-wifi interferers

Notes

- ECRCHS has the following types of APs installed:
    - (42) Aruba AP-224　　13%　　Category 4
    - (228) Aruba AP-225　　87%　　Category 4

Analysis

The Aruba APs can use any or all the radios on each wireless access point to examine the spectrum for interference (including non-wifi interferers). They perform this function by periodically going 'off channel' to scan through the usable channels in both the 2.4 GHz and 5 GHz spectrums. This functionality can be configured to happen as often as once per second. Any time the radio has to go 'off channel' to look for interferers, that is time spent not servicing clients attached to the radio. Therefore, doing so too frequently will lead to a degradation in performance. If the scan is performed too infrequently, some interferers may not be detected or there may be a delay in detection. Some manufacturers solve this problem by providing a dedicated radio for spectrum management and wireless security detection/prevention functions.

Manageability   <u>Score: 4/5</u>

1 = No centralized management – all wireless APs are autonomous

2 = On-premises wireless controller, no redundancy

3 = On-premises wireless controllers – with redundancy, or located at each site

4 = All infrastructure controlled through single management platform with independent control plane

5 = All infrastructure controlled through single cloud interface and/or mobile management app

Notes

- Aruba AirWave deployed as an on-premises virtual machine running on Microsoft Hyper-V virtual infrastructure.

- Aruba Central, a cloud-hosted (public) network management portal, is available from Aruba – not currently used at ECRCHS. The hosted instance of Aruba is likely to require an annual fee.

Analysis

The Aruba Wireless platform offers central management and reporting in the form of the Aruba Airwave software. The software may be installed locally on a virtual machine or dedicated appliance, or a cloud-based network management service, Aruba Central, is available for an annual charge.

ECRCHS may want to consider cloud-hosting the network management, through Aruba Central, as it would place the onus of providing adequate hardware resources and disaster-recovery on the manufacturer rather than the ECRCHS IT Department.

Guest/BYOD Accessibility Score: 4/5

1 = No security / open access

2 = Pre-shared key authentication

3 = Pre-shared key authentication or open authentication with restricted access rights to resources

4 = Authentication tied to identity (AD account or email) with variable access rights based on role

5 = Self-provisioning portal with MDM software for BYOD users. Sponsorship portal for guests/visitors.

Notes

- ECRCHS students are not allowed BYOD devices.

- Teachers/Staff are allowed BYOD phones and are placed on a fully isolated zone within the DMZ

- Dot1x authentication is utilized and managed through Aruba ClearPass. Blacklists are also in use to prevent recognized malicious sources from attempting to access the system.

- Data loss prevention (DLP) technical controls have been removed due to ECRCHS internal privacy policies.

Analysis

ECRCHS is utilizing Aruba Clearpass to manage BYOD devices within the isolated DMZ zone provided for Teachers/Staff to use. The ECRCHS Bring-Your-Own-Device policy enables staff to connect their mobile phone device to a wireless access point. ECRCHS utilizes network policies to isolate the device from the internal network, by utilizing a physically isolated zone within the DMZ. Devices are monitored for malicious activity or unusual behaviors, but Data Loss Prevention (DLP) technical controls have been turned off in response to ECRCHS privacy policies. This solution provides resiliency against rogue devices and malicious intent, while providing the phone internet connectivity via the wireless access points. Without utilizing DLP technical controls, this solution will not identify or prevent a transmission of personally identifiable information (PII) or restrict the transmission of sensitive data over the BYOD network.

Network Security

Network Security: Features in Use

Security Features in Use	Yes	No
Perimeter Firewall	**Y**	**N**
IPS	X	
Antimalware	X	
URL filtering	X	
Redundancy	X	
Virtual FW instances		X
Endpoint Protection	X	
DNS Filtering	X	
Email filtering	n/a	n/a

Standalone Content Filter	Y	N
Granular policies for web-based applications	X	
File sandboxing	X	
Reputation scoring	X	
Antivirus & Antimalware	X	
HTTPS decryption ability	X	
Layer 4 traffic monitor	X	
External Data Loss Prevention policies		X

Standalone Mail Filter	Y	N
Anti-Spam	n/a	n/a
Anti-Virus	n/a	n/a
Data Loss Prevention	n/a	n/a
Email Encryption	n/a	n/a
Image Analysis	n/a	n/a
Outbreak Filters	n/a	n/a
Quarantines	n/a	n/a
SMTP Authentication	n/a	n/a
SPF/DKIM in use	n/a	n/a

- Note: Standalone mail filter is not needed because ECRCHS is using hosted email service (Google) with its own set of filters

Security Features in Use	Yes	No
Protection for Endpoints	**Y**	**N**
Anti-malware	X	
Anti-virus	X	
IDS	X	

SIEM	Y	N
Asset Discovery	X	
Vulnerability Assessment	X	
Intrusion Detection	X	
Behavior Monitoring	X	
Event Correlation	X	

DNS filtering	Y	N
Region-based blocking rules		X
Ability to identify internal IP addresses		X
Ability to identify users		X
Tie-in to Active Directory		X
Protection of roaming users		X

Cloud application visibility & control	Y	N
Application Discovery	X	
Threat Protection	X	
Data Security and Compliance	X	
Integration and Orchestration	X	

Flow Analyzer	Y	N
Rule-based detection	X	
Machine learning feature		X
User identity / Active Directory integration	X	
Enabled for network core segment	X	
Enabled for network edge segment	X	
Enabled for Datacenter segment	X	
Enabled for Wireless segment	X	

Network Security: Inventory

Manufacturer	Model	Qty
Palo Alto	PA5220	2

Network Security: EoX Milestones

Total Qty	Description	Model	EoS	EoE	LDoS
2	Palo Alto 5200 Next-Gen Firewall	PA5220	Current	Current	Current

Network Security: Software Versions and Recommendations

#	Manufacturer	Model	Installed Version	Current Version(s)	Recommendation
2	Palo Alto	PA5220	**Unknown**	**Unknown**	**n/a**

Network Security: Scoring and Analysis

Components assessed

- **Security Policies**
  - The creation of effective security policies is an important aspect of network security that is often overlooked. Effective policies – communicated with and acknowledged by end users – sets the basis for the activities allowed or disallowed on the network. This, in turn, dictates the need for security products and services and generates the requirement for funding to be in place for their procurement and operation.

- **Auditing Process**
  - Having someone on staff who is highly skilled in network security is a luxury that not all organizations can afford, yet it is important to hold regularly-scheduled audits of both internal and perimeter security in order to identify where weaknesses lie. Whether the audits are performed via internal resources or by external specialists, the key factor is establishing regularity of audits.

- **IoT Security**
  - Whether or not they realize it, all organizations are participating in the 'Internet of Things', where low-cost or embedded devices are connected to the network. It is important for every organization to maintain a strategy indicating how these devices should be connected to the network, who is allowed to deploy them, and how they should be managed and secured. In the (likely) event that one of these devices is compromised, the organization should have a clear understanding of how to identify

and respond to the incident.

- **Perimeter Firewall**
  - The perimeter firewall, which protects the organization from 'external' threats on the Internet, is often the most well-known and easily-recognized component of network security. It is extremely important for keeping threats out of the internal network. The perimeter firewall should be capable of performing analysis of network traffic at speeds matching or exceeding that of the connection to the Internet, and it should support 'next-gen' firewall features which include the ability to filter based on applications and content rather than simple IP address and port settings.

- **Datacenter Firewall**
  - Many organizations neglect to filter the traffic between their internal users and their datacenter. This layer of security should be considered as important as the perimeter firewall. Many organizations choose to dedicate a separate appliance (or pair of highly-available appliances) for their datacenter, but this is not always necessary. If the perimeter firewall is co-located in the datacenter and has enough power to handle the additional connectivity, it may be possible to use the same appliance (or HA pair) for both purposes simultaneously. On the other hand, dedicating separate appliances for the datacenter might be required to meet performance thresholds or for other capacity-related reasons. In any case, the datacenter firewall should also make use of 'next-gen' features which include application visibility and control. One of the more prevalent datacenter design philosophies centers on the 'zero trust' model, which assumes that all traffic is threat traffic unless proven otherwise. This implies that east-west traffic (between servers or VMs in the datacenter) should be filtered just as well as north-south traffic.

- **Web Content Filtering**
  - Web content filtering requirements vary depending on the organization; K-12 school districts require heavy filtering while Higher Education ECRCHSs might not filter their traffic at all. Most commercial or other enterprise accounts have requirements that fit somewhere in between. Many 'next-gen' firewalls can perform web content filtering in addition to their traditional duties, yet such functionality may not be sufficient for all organizations. It is, therefore, important for the organization to identify clear requirements regarding what it needs to filter, what legal requirements they must meet, and what performance threshold it must achieve.

- **Mail Filtering**
  - Email – whether hosted on-prem or in the cloud – is a common transmission vector for computer viruses and malware. Recent statistics indicate that close to 90% of malware is delivered through email. It is, therefore, critical that a strong mail filtering solution be in place. To be effective, the mail filter must support frequent automatic updates of its signature database, and support features like sandboxing and automatic quarantining of

potential threats.

- **DNS Filtering**
  o Nearly every device on the network uses DNS to identify the IP addresses of servers and endpoints with which they communicate. DNS filtering is a simple and effective way to stop endpoints from communicating with malware distribution points on the Internet, and it can help prevent existing malware within the network from reaching command & control points, effectively neutering their ability to exfiltrate data from your network.

- **Endpoint Protection**
  o Endpoint protection is more than just 'antivirus software'. The endpoint is where the majority of malware infections occur, and an infected endpoint can be used by cybercriminals as a hopping-off point to more critical resources within the network.

- **SIEM**
  o The Security Information and Event Management system (SIEM) is a critical component of security operations. The purpose of the SIEM is to receive logs and SNMP traps from network infrastructure and critical applications, and to sort out the important information from the routine and mundane notifications.

- **Cloud Application Visibility & Control / CASB**
  o With the majority of applications now running in the 'cloud' rather than on-prem, the IT Department potentially loses a measure of control over the way end users access content and how they are permitted to use their systems. A Cloud Access Security Broker (CASB) can remedy this by providing three vital functions:
    - Identity Security – Provides defense against compromised accounts and malicious insiders
    - Data Security – Protects against data breaches and exposures via data-loss prevention policies
    - Application Security - Discovers and controls malicious cloud apps connected to your environment

- **Internal Network Visibility & Anomaly Detection**
  o Most organizations commit the bulk of their resources securing the perimeter of their network, yet they lack visibility into threats which originate inside their network. Such threats may include targeted attacks on servers and network infrastructure, exfiltration of valuable data, or even denial of service attacks. If the threats originate from the internal network (i.e. from an employee) then the perimeter defense systems are not liable to see and prevent them from occurring. This is where products that focus on packet accounting (Netflow, sFlow, etc) and analysis can help.

Security Policies   Score: 4/5

1 = No security policies developed

2 = Policies have been developed, but not adopted by end users (or policies are obsolete and forgotten).

3 = Policies have been developed and adopted for some aspects of information security, but not all aspects are fully developed or enforced.

4 = Policies have been developed and adopted for the use of internal infrastructure and applications by employees, contractors, guests, and students. Data loss prevention policies are either not developed or not enforced.

5 = Policies have been developed and adopted for the use of internal infrastructure and applications by employees, contractors, guests, and students. Data loss prevention policies are in place and are enforced. There is regular participation from (and feedback to) the organization's executive team.

Notes:

- ECRCHS employs a compliance officer to develop and enforce internal security policy
- Data loss prevention (DLP) technical controls have been removed due to ECRCHS internal privacy policies.
- Security audits are performed annually

Analysis:

ECRCHS's Security and compliance is managed by a full-time compliance officer. Security audits are conducted on an annual basis.

NIC Partners recommends regularly reviewing existing security policies and analyzing their effectiveness within the organization. Additionally, ECRCHS will want to consider implementing a security awareness program for all staff.   Each employee must individually understand the need for security, the part that they play, and how to protect themselves from various types of attacks.

Auditing Process   Score: 4/5

1 = No security audits have been performed

2 = One or more security audits have been performed in the past, but there was little done to rectify the problems found and reported in the audit.

3 = One or more security audits occur each year – perhaps with a 'canned' penetration testing tool – but problems are not formally logged or tracked.

4 = Regular security audits of both internal and external resources are scheduled with external contractors, or with an internal 'red team'. Problems are addressed in an ad-hoc manner with little formal structure in place.

5 = Regular security audits of both internal and external resources are scheduled with external contractors, or with an internal 'red team'. An internal or external ticket system is used to track problems that need to be fixed, and security updates are regularly performed.

Notes:

- Regular security audits are performed once a year
- The internal help desk is responsible for tracking security issues

Analysis:

A regular routine of internal and external penetration testing, with follow-up for corrective actions, is a good practice to provide critical insight into unknown vulnerabilities that could potentially be exploited within the ECRCHS environment.

The security audit will often utilize external consulting services to perform the penetration testing. The security consultants would conduct internal and external tests that utilize real-world attack methods and tools to provide an impartial report of all actively exploitable attack-surfaces discovered.

After corrective action has been taken by internal IT staff, a follow-up test is recommended and should be conducted to confirm the proper remediation of all vulnerabilities expressed in the audit.

IoT Security   Score: 3/5

1 = No IoT device strategy has been developed or is in place.

2 = A strategy for deploying and securing IoT devices has been developed but has not formally been rolled out across the organization.

3 = A strategy for deploying and securing IoT devices has been developed and rolled out across the organization, but the strategy does not meet the security objectives of full segmentation and vulnerability mitigation.

4 = IoT devices are segmented from other devices within the organization, and processes are in place to regularly identify and address vulnerabilities in IoT devices.

5 = IoT devices are segmented from other devices within the organization, and processes are in place to regularly identify and address vulnerabilities in IoT devices. Information Technology (IT) and Operations Technology (OT) teams work together to define common business and security policies.

Notes:

- Utilizing Aruba Clearpass and Aruba Airwave to manage devices

Analysis:

According to Jacob Yoo, El Camino Real Charter High School has a strategy for handling IoT devices. There is a BYOD security zone that funnels traffic directly outside of the network, without the ability to speak to other devices on the 'internal' security zone. IoT devices are connected to the BYOD security zone so they cannot impact the security of internal devices.

ECRCHS could benefit from developing process and procedure to proactively identify the make and model of all IoT devices on their network, and routinely scan them for vulnerabilities. It is important to stay current on software/firmware release notes and be aware of when upgrades are required to prevent the potential exploitation of security vulnerabilities.

Perimeter Firewall   Score: 5/5

1 = Throughput does not match ISP speed, IPS and anti-malware features are not enabled or supported, and firewall supports a low capacity for connections-per-second.

2 = Throughput does not match ISP speed, IPS and anti-malware features are enabled, and firewall supports a low capacity for connections-per-second.

3 = Throughput matches ISP speed, IPS and anti-malware features are enabled, and firewall supports a low capacity for connections-per-second.

4 = Throughput matches ISP speed, IPS and anti-malware features are enabled, and firewall supports a medium capacity for connections-per-second.

5 = Throughput matches or exceeds ISP speed, IPS and anti-malware features are enabled, and firewall supports a high capacity for connections-per-second.

Notes:

- The PA-5220 supports ~8 Gbps of throughput with features turned on
- The PA-5220 is sufficiently sized an ISP connection up to 10 Gbps (currently at 5 Gbps)

Performance and Capacities	PA-5220
Firewall throughput (HTTP/appmix)[1]	17/20 Gbps
Threat Prevention throughput (HTTP/appmix)[2]	8/9 Gbps
IPsec VPN throughput[3]	8 Gbps
Max sessions	4,000,000
New sessions per second[4]	150,000
Virtual systems (base/max)[5]	10/20

Analysis:

The Palo Alto 5220 utilized at ECRCHS is sufficiently sized for the campus. There are no concerns with its feature set or specifications.

Datacenter Firewall   Score: 1/5

<table>
<tr><td style="background-color:red"> </td><td></td><td></td><td></td><td></td></tr>
</table>
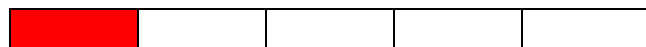
1 = No firewall is in place to protect datacenter network from internal user segment(s)

2 = Firewall is filtering north-south traffic to/from the datacenter, but advanced inspection features are disabled. The firewall throughput or connections-per-second characteristics may not be properly sized.

3 = Firewall is filtering north-south traffic to/from the datacenter, but advanced inspection features are disabled. The firewall throughput and connections-per-second characteristics are properly sized.

4 = Firewall is filtering north-south traffic to/from the datacenter, and advanced inspection features are enabled. The firewall throughput and connections-per-second characteristics are properly sized.

5 = Datacenter is segmented with virtual or physical firewall(s) filtering east-west traffic as well as north-south traffic. Advanced inspection features are enabled.

Notes:

- Datacenter equipment and software are on the same firewall security zone as the internal endpoints.
- Network segmentation is used to separate the datacenter components from other systems on the internal network, but such traffic does not flow through the firewall.

Analysis:

For the optimal protection of datacenter resources (including sensitive data stored on local servers), NIC Partners recommends connecting on-premises datacenter equipment through a separate security zone in order to have the firewall filter traffic between internal users and the servers.

In this case, there is a caveat: ECRCHS is hosting most of its critical systems in the cloud, including the student information system (SIS), email, and learning management system (LMS). Since there is not much sensitive data stored locally, this requirement might not be high on the list of priorities to address.

Web Content Filtering   Score: 5/5

1 = Web content filtering is not used or has not been deployed.

2 = Web content filter does not meet functionality requirements, and is not properly sized.

3 = Web content filter meets functionality requirements, but is not properly sized.

4 = Web content filter meets functionality requirements and is properly sized for throughput and connections per second.

5 = Web content filter meets functionality requirements and is properly sized for throughput and connections per second. Includes advanced traffic inspection functionality, including malware protection.

Notes:

- The Palo Alto 5220 firewall is performing web content filtering for internal endpoints.
- 'External Data Loss Prevention' policies are disabled due to privacy concerns.

Analysis:

The Palo Alto firewall is performing web content filtering services, and it appears to be sized properly to handle the amount of traffic generated by a typical high school.

Since the current filtering capabilities employed by the Palo Alto are meeting the needs of the administration, NIC Partners does not have any further recommendations regarding web filtering.

Mail Filtering   Score: 4/5

1 = Mail filtering is not used or solution has not been deployed.

2 = Basic mail filtering functionality is employed, including blacklist/greylist/whitelist

3 = Mail filter employs reputation scoring

4 = Mail filter employs reputation scoring and advanced malware protection for the inbound direction only.

5 = Mail filter leverages advanced malware protection and scans both incoming and outgoing mail. Data Loss Prevention policies are used to prevent exfiltration of sensitive information.

Notes:

- ECRCHS leverages the advanced mail filtering features, provided by Google within the G-Suite
- Email is cloud hosted and managed by Google
- Gmail DLP is a feature available within Gmail but it is not enabled due to privacy concerns.

Analysis:

- Google G Suite for Education is an enterprise-level solution with the security features required by a K-12 school district. G Suite claims to have built-in security features (such as advanced anti-phishing, security center, mobile management, etc.) that give admins ways to manage users, control devices, ensure compliance, and keep data secure.

DNS Filtering   Score: 4/5

1 = No filtering of DNS traffic is in use

2 = Custom DNS blacklists or sinkholes are used (i.e. geo-blocking)

3 = Free, consumer-focused DNS filtering service (OpenDNS Home, Cloudflare 1.1.1.1) is being used

4 = Professional DNS filtering service with analytics is being used

5 = Professional DNS filtering service with analytics is being used. Agents are used on mobile devices to keep them protected while roaming.

Notes:

- DNS filtering is managed by the Palo Alto 5220s. The datasheet indicates that the PA-5220 will perform the following functions:
    - Identifies, controls, and inspects DNS traffic.
    - Blocks DNS queries to malicious domains as a means of breaking the C2 channel.
    - Identifies compromised hosts on the network through DNS sinkholing.

Analysis:

DNS filtering is a simple method of stopping many forms of malware without needing any special software to be installed on the endpoints.

ECRCHS is has deployed sufficient measures for the filtering of DNS queries.

Endpoint Protection   Score: 5/5

1 = No endpoint protection is used on Microsoft Windows and/or Apple MacOS devices

2 = Endpoints are protected with traditional signature-based platform.

3 = Endpoints are protected with software leveraging both traditional signature-based platform and exploit prevention to stop file-less attacks.

4 = Endpoints are protected with software leveraging both traditional signature-based platform and exploit prevention to stop file-less attacks. Endpoint protection indicates network trajectory of malware, showing when and where the malware has spread to.

5 = Endpoints are protected with software leveraging both traditional signature-based platform and exploit prevention to stop file-less attacks. Endpoint protection includes cloud-based analysis of unknown files, and is capable of retrospectively quarantining files that were previously marked as 'safe' or 'unknown'. Endpoint protection indicates network trajectory of malware, showing when and where the malware has spread to.

Notes:

- ECRCHS is utilizing the cloud-based MDM features of Microsoft Intune, along with Defender ATP and Palo Alto Traps, for its endpoint devices.

Analysis:

Threat & Vulnerability Management (TVM) is a built-in capability in Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) that uses a risk-based approach to discover, prioritize, and remediate endpoint vulnerabilities and misconfigurations. With Microsoft Defender ATP's Threat & Vulnerability Management, customers benefit from:

- Continuous discovery of vulnerabilities and misconfigurations

- Prioritization based on business context and dynamic threat landscape

- Correlation of vulnerabilities with endpoint detection and response (EDR) alerts to expose breach insights

- Machine-level vulnerability context during incident investigations

- Built-in remediation processes through unique integration with Microsoft Intune and Microsoft System Center Configuration Manager

SIEM   Score: 2/5
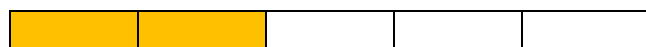
1 = No central collection of logs is in use

2 = One or more log collection systems are in use, but are independent of each other (no correlation).

3 = SIEM collecting log data is in use and log entries are regularly reviewed

4 = SIEM collecting log data is in use and log entries are regularly reviewed. SIEM platform contains analytical capabilities and can proactively notify administrators of anomalies.

5 = SIEM collecting log data is in use and log entries are regularly reviewed. SIEM platform contains analytical capabilities and can proactively notify administrators of anomalies. SIEM platform contains advanced features including data visualization and search capabilities.

Notes:

- Using Kiwi Syslog Server for aggregation of syslog data
- Keywords are defined for proactive alerting of specific events
- Microsoft Intune is used to manage assets

Analysis:

The purpose of a Security Information and Event Manager is to collect and correlate data from multiple sources, and present data in a way that is easily digestible to the administrator.

ECRCHS is capturing data from multiple sources, but it is potentially disaggregated across several platforms (Kiwi Syslog, Palo Alto, Microsoft Intune). This sort of environment may suffice as long as all of the systems are regularly monitored. However, overall security and awareness of network events could be improved by pointing all of this data to a central SIEM which employs normalization of data and correlation of events between disparate systems to identify problems on the network in real-time.

Examples of software that provide SIEM functionality include (in no order or preference) Splunk, Motadata, Alienvault, Datadog, and Sumo Logic.

Cloud Application Visibility & Control (CASB)   <u>Score: 4/5</u>

1 = No CASB platform is in use

2 = CASB platform options are being explored or demonstrated, but there is little to no adoption within the organization.

3 = CASB platform is in use and is used in the production environment across the organization, but features are limited or platform is not widely adopted.

4 = CASB platform is in use and is widely adopted across the organization.

5 = CASB platform is in use and is widely adopted across the organization. Advanced features, such as DLP enforcement and two-factor authentication, are leveraged to enhance data security.
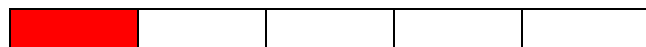
<u>Notes:</u>

- Using Microsoft Cloud App Security as part of Office 365 Academic subscription

<u>Analysis:</u>

ECRCHS is leveraging their subscription with Microsoft 365 to use Microsoft Cloud App Security. This software fulfills the role of a cloud application security broker.

Internal Network Visibility & Anomaly Detection   Score: 5/5

1 = No network visibility & anomaly detection platform is in use.

2 = Specific network segments are monitored for anomalies with one or more server NICs in promiscuous mode. Monitoring/Visibility platform is limited in scope and feature set.

3 = Specific network segments are monitored for anomalies with one or more server NICs in promiscuous mode. Monitoring/Visibility platform has extensive features that are geared to security analysis and intrusion detection.

4 = Specific network segments are monitored for anomalies using network TRAPs that forward traffic to a centralized collector. Monitoring/Visibility platform has extensive features that are geared to security analysis and intrusion detection.

5 = Netflow/sFlow traffic is forwarded from network equipment to centralized collector, where network visibility & anomaly detection platform analyzes traffic and sends reports and proactive notification of anomalies and potential intrusions.

Notes:

- Sending sFlow to Aruba Airwave software, but Airwave does not provide User and Entity Behavior Analytics (UEBA) or Network Traffic Analysis (NTA).
- Using PRTG to monitor switch port statistics, but PRTG does not provide UEBA or NTA.

Analysis:

Aruba switches have been configured to send sFlow traffic to Aruba Airwave software. Airwave offers the following key features:

- Unified Wired and Wireless Network Management
- Broad Visibility and Control
- Proactive Troubleshooting
- Physical and Virtual Appliances
- Enhanced Security and App Visibility

Airwave is an excellent solution for managing and monitoring network equipment. Forwarding sFlow to Airwave allows it to present a view of network traffic, including web categories, client destinations, VoIP analytics, etc. It does not, however, provide User and Entity Behavior Analytics or Network Traffic Analytics (from a security standpoint).

Aruba's UEBA/NTA platform is 'IntroSpect'. A partial list of competing products might include Forcepoint Insider Threat, Fortinet FortiInsight, Palo Alto Cortex XDR, Securonix NTA, and Cisco StealthWatch.

Datacenter

Datacenter: Inventory

Device	Description
Huawei RH1288 v3	Hypervisor Server
Huawei RH1288 v3	Hypervisor Server
HP DL360 Gen9	Hypervisor Server
Huawei Oceanstore 5300	Primary Storage
HP Storeonce	Backup Storage
Huawei 24p SFP+	Backend Switch for SAN
HP DL380 Gen8	Server for Active Directory

Datacenter: EoX Milestones

EoX Milestones visual alerts legend color schema:

EoX Milestone	Visual	Description
EoS		End of Sale (No more orders for the item)
EoE		End of Engineering (No more updates for the item)
LDoS		Last Day of Support

Device	EoS	EoE	LDoS
Huawei RH1288 v3	12-31-2018	12-31-2023	12-31-2023
HP DL360 Gen9	10-31-2018	10-31-2023	10-31-2023
Huawei Oceanstor 5300 **V3**	12-31-2018	12-31-2023	12-31-2023
HP Storeonce	unknown	unknown	unknown
Huawei 24p SFP+	unknown	unknown	unknown
HP DL380 Gen8	6-13-2016	6-13-2021	6-13-2021

Components assessed

- **Compute**

  o 'Compute' describes the processor 'horsepower' available to run applications and virtual machines. In general, the amount of compute capability should be balanced against the needs of the applications and services being run in the datacenter to prevent 'server sprawl'.

- **Storage**

  o Storage refers to the capacity to store virtual machines and files within the datacenter. Virtual machines require very fast storage to work optimally while files can be stored on slower disks or in the cloud if they are not often accessed.

- **Datacenter Network**

  o The datacenter network should provide high-speed and redundant connections to each server host, and should uplink to the network core at high speed. The ideal switches for this environment would have an operating system tailored for reliability and high-speed interconnects, with feature support for protocols like VXLAN and virtual port-channels.

- **Cloud**

  o The use of 'cloud' technologies, such as software-as-a-service or infrastructure-as-a-service, enables an organization to outsource server equipment and maintenance to an external provider. The optimal use of cloud technologies may be different for each organization, but they should at least be familiar with the various offerings.

- **Disaster Recovery Systems (DRS)**

  o Each organization should have a system prepared to allow for the preservation and restoration of critical data and applications. This system needs to cover both minor incidents (such as accidental file deletion) and major incidents (such as damage from natural disasters). An optimal disaster recovery system would include the ability to host datacenter operations from two or more geographically disparate locations, and would leverage cloud technologies for additional storage and/or operating capacity.

Compute   Score: 4/5

1 = Severely underpowered servers / full utilization

2 = Mildly underpower servers / ½ to ¾ utilization

3 = Sufficient processing power but no spare capacity for handling host outages

4 = Sufficient processing power with spare capacity for one or more host outages

5 = Full optimization of compute power with blade-based hosts and stateless computing

Notes:

- Most services have been migrated to the cloud.

- There are (3) servers with identical specifications (32 cores, 128 GB of RAM) running Microsoft Hyper-V in a clustered environment. These are hosting the on-prem virtual machines, and are sufficient for the current requirements.

Analysis

ECRCHS has migrated most of its applications to the cloud (Microsoft, Google, etc.) so the need for on-prem compute capacity is minimal. The majority of virtual machines in use today are needed for the functionality of the local network: Aruba Clearpass, Aruba Airwave, Help Desk, Domain Controller, and various monitoring tools.

The current servers in use today appear to provide sufficient capacity to handle the assigned load. Since the hypervisors are configured as a high-availability cluster, the failure of one of the servers should not impact the operating environment.

Storage   <u>Score: 3/5</u>

🟨	🟨	🟨		

1 = SAN or NAS with spinning drives only

2 = SAN with tiered storage (flash + spinning drives)

3 = SAN with tiered storage (flash + spinning drives) and inline compression or de-duplication

4 = All-flash SAN with multi-protocol capabilities, inline compression and de-duplication

5 = Redundant all-flash SAN with multi-protocol capabilities, inline compression and de-duplication

Notes

- Using a mix of traditional spinning-disk storage and flash storage, the Huawei Oceanstor 5300 delivers high performance tiering of data, which supports online de-duplication and online compression. This platform is a SAN, which is meant for virtual server storage by a hypervisor.

- Using iSCSI storage protocol from hosts to Huawei Oceanstor 5300 over multiple 10G SFP+ links.

- Huawei Oceanstor storage appliance (in use with Hyper-V environment) has tiered storage with flash and spinning drives.

- ECRCHS is utilizing an isolated backend-network switch for all iSCSI traffic between the hypervisor hosts and the storage controller. This is considered an industry best practice configuration and is an ideal network design for ECRCHS's Storage Area Network.

Analysis

ECRCHS utilizes a Storage-Area-Network (SAN), with 10G links and an isolated back-end switch, over iSCSI protocol to provide storage to their hypervisor hosts. The features supported with the Huawei Oceanstor 5300 are sufficient for providing low-latency storage for a small number of virtual machines.

Most enterprise grade networks are in one of two camps:

1) Traditional converged storage system with high-speed drives (i.e. flash) and redundancy connected to stateless hosts running hypervisors for virtualization (i.e. VMWare or Hyper-V)

2) Hyper-converged systems, where nodes with compute and storage are scaled out as needed

ECRCHS is in the first camp. Storage and compute can be grown and sized independently to meet resource requirements of internally hosted applications. Though the storage is not flash-based, it utilizes flash-tiering to provide near-flash speeds while utilizing hybrid disks for cold storage.

In most situations, NIC Partners would recommend implementing a replication partner for the current production SAN, though ECRCHS utilizes cloud for business-critical servers and does not consider

internally hosted applications as business critical. Should business critical services be utilized within ECRCHS local datacenter, NIC Partners does recommended implementing a replication partner to provide redundancy and resiliency against SAN hardware failure.

Datacenter Network Score: 2/5
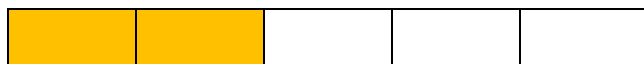
1 = Standard campus switches running at 1 Gbps to hosts / 1 Gbps uplink. No redundancy.

2 = Standard campus switches running at 1 Gbps to hosts / 10 Gbps uplink. No redundancy.

3 = Redundant campus switches running at 1 Gbps to hosts / 10 Gbps uplink.

4 = Redundant switches with 10G or 25G uplinks to network core. Switch OS designed for datacenters.

5 = Redundant switches with 40G or 100G uplinks to network core. Switch OS designed for datacenters.

Notes

- Servers are connected to campus switches utilizing 10G links (both frontend and backend)

- Most campus switches are not configured for redundancy

- ECRCHS is not utilizing redundancy at the core and would not withstand a backplane or management module failure

Analysis

The server hosts are currently being plugged into entry-level campus switches, which may not deliver the kind of performance required of an enterprise-grade virtualized datacenter. As ECRCHS is utilizing cloud for all business-critical servers, the use of campus switching is not as concerning.

It is important to note that NIC Partners would not recommend hosting of systems, that are critical to ECRCHS business, in the current on-premise infrastructure without re-architecting for resiliency against common hardware failures.

Cloud   <u>Score: 4/5</u>

1 = No use of cloud hosted technologies today

2 = Use of SaaS (software as a service) platforms, such as Microsoft Office 365

3 = Use of SaaS platforms plus cloud storage for long-term archives or backups

4 = Use of SaaS platforms plus Amazon S3 or Microsoft Azure for compute/storage

5 = Use of SaaS platforms plus Amazon S3 or Microsoft Azure set up with public-facing services

Notes

- ECRCHS makes use of Microsoft SaaS Services and Google G-Suite.
  - Application platforms are hosted in Microsoft Azure
  - Microsoft Azure Active Directory is being used for endpoints
  - Microsoft Intune is being used for device management, auditing, and reporting
- ECRCHS utilizes multiple service offerings included with the Google G-Suite.
- SaaS applications in use, include Google Apps. Online file shares are provided by Google Drive.

Analysis

ECRCHS has made great progress in its use of cloud technologies to extend the capabilities of the IT department and reduce its datacenter footprint. It is recommended that ECRCHS performs a financial analysis of the cost benefits/reductions provided by the cloud platforms vs. the cost of hosting services locally. NIC Partners recommends determining the cost of retrieving data that might be lost from a natural disaster, as services like Microsoft Azure often charge much higher fees for data retrieval than they would for the storage of said data.

Disaster Recovery Systems   Score: 3/5

1 = No disaster recovery plan or backups in use

2 = Regularly scheduled backups of critical data, but no planning for organization-wide disasters

3 = Regularly scheduled backups of critical data, some planning for disasters, no scheduled testing

4 = Regularly scheduled backups WITH scheduled testing, some planning for disasters

5 = Regularly scheduled backups WITH scheduled testing, multiple modes of recovery for disasters

Notes

- Veeam is used for local backups
- Data in cloud (Google, Azure) relies upon cloud service provider to ensure data integrity and backup/restoration services

Analysis

ECRCHS makes use of cloud services to eliminate the local presence of critical systems. For these systems residing within the cloud, ECRCHS utilizes the services provided to ensure data integrity and availability of cloud servers.

For local servers, residing within the ECRCHS datacenter, Veeam is used to backup servers and store recovery points on an external storage device (HP Storeonce).

The general rule for backups is '3-2-1': Have three copies of your data in at least two different physical locations, and one of them should be cloud. ECRCHS is currently storing single copy of the backup data and would benefit from second copy, stored in a different physical location.

NIC Partners recommends that ECRCHS utilize a distributed cloud-based storage service, such as amazon S3 or Amazon simple storage service, as a second copy for the backups of servers hosted in Amazon cloud and on-prem.

Additionally, NIC Partners recommends having a written disaster recovery plan in place with regularly scheduled testing of backup/recovery scenarios to ensure that everything works when it is most needed. The plan should include everything from physical facilities to connectivity between schools and the Internet, to where data should reside within the network and how it can be accessed in the event of a datacenter outage.