



El Camino Charter High School

Technology Committee Meeting

Date and Time

Thursday October 17, 2019 at 5:30 PM PDT

Location

El Camino Real Charter High School, Room A-203, 5440 Valley Circle Boulevard, Woodland Hills, CA 91367

The Technology Committee is a standing committee of the Board of Directors of El Camino Real Alliance.

For committee meeting materials, please go to the school's main office, or call (818) 595-7500. Some board meeting materials are also posted in the school's website (<https://ecrchs.net> - click the ECR Board tab).

INSTRUCTIONS FOR PRESENTATIONS TO THE COMMITTEE BY PARENTS AND CITIZENS

El Camino Real Alliance ("ECRA") welcomes your participation at ECRA's Technology Committee meetings. The purpose of a public meeting of the Technology Committee is to conduct the affairs of ECRA in public. Your participation assures us of continuing community interest in our charter school. To assist you in the ease of speaking/ participating in our meetings, the following guidelines are provided:

1. Agendas are available to all audience members at the meeting.
2. "Request to Speak" forms are available to all audience members who wish to speak on any agenda items or under the general category of "Public Comments." "Public Comments" is set aside for members of the audience to raise issues that are not specifically on the agenda. However, due to public meeting laws, the Committee can only listen to your issue, not respond or take action. These presentations are limited to three (3) minutes and total time allotted to non-agenda items will not exceed thirty (30) minutes. A member of the public who requires the use of a translator, in order to receive the same opportunity as others to directly address the Committee, shall have twice the allotted time to speak. The Committee may give direction to staff to respond to your concern or you may be offered the option of returning with a citizen-requested item.
3. You may also complete a "Request to Speak" form to address the Committee on Agenda items. With regard to such agenda items, you may specify that agenda item on your "Request to Speak" form and you will be given an opportunity to speak for up to three (3) minutes before the item, and total time allocated to agenda items will not exceed six (6) minutes for a discussion item and nine (9) minutes per vote item. A member of the public who requires the use of a translator, in order to receive the same opportunity as others to directly address the Committee, shall have twice the allotted time to speak, and the total allocated time shall be appropriately increased as well.
4. When addressing the Committee, speakers are requested to state their name and adhere to the time limits set forth. In order to maintain allotted time limits, the Committee Chair may modify speaker time allocations or the total amount of allotted time for an item.
5. Any public records relating to an agenda item for an open session of the Committee which are distributed to all, or a majority of all, of the Board members shall be available for public inspection at 5440 Valley Circle Blvd., Woodland Hills, California, 91367.

Consent Agenda: All matters listed under the consent agenda are considered by the Committee to be routine and will be approved/enacted by the Committee in one motion in the form listed below. Unless specifically requested

by a Committee member for further discussion or removed from the agenda, there will be no discussion of these items prior to the Committee votes on them. The Executive Director recommends approval of all consent agenda items.

In compliance with the Americans with Disabilities Act (ADA) and upon request, El Camino Real Alliance may furnish reasonable auxiliary aids and services to qualified individuals with disabilities. Requests for disability related modifications or accommodations shall be made 24 hours prior to the meeting to Daniel Chang, in person, by email at d.chang@ecrchs.net, or by calling (818) 595-7537.

Agenda

	Purpose	Presenter	Time
I. Opening Items			5:30 PM
A. Call the Meeting to Order		Beatriz Chen	1 m
B. Record Attendance and Guests		Beatriz Chen	1 m
C. Public Comments		Beatriz Chen	30 m
II. Technology Committee			6:02 PM
A. Review Technology Network Assessment Conducted by NIC Partners	Discuss	Beatriz Chen	15 m
Review of the Technology Network Assessment report conducted by NIC Partners.			
B. Discuss and Possible Vote on Recommendation to Board on E-Rate Eligible Items	Vote	Beatriz Chen	15 m
Review and possibly vote on recommendation to Board regarding E-rate eligible items (items budgeted for 2019-2020 school year).			
III. Closing Items			6:32 PM
A. Adjourn Meeting	Vote	Beatriz Chen	1 m

Cover Sheet

Review Technology Network Assessment Conducted by NIC Partners

Section: II. Technology Committee
Item: A. Review Technology Network Assessment Conducted by NIC Partners
Purpose: Discuss
Submitted by:
Related Material: ECRCHS Network Assessment Report R6 2019-09-13 notes (1).pdf



Baseline Assessment Report

Performed for:



EL CAMINO REAL CHARTER HIGH SCHOOL

Date of Report 09/04/2019

Revision 6

Assessed By James Joyner



Contents

Executive Summary3

Scope of Discovery.....4

 Network Devices4

 Supplemental Collection and Discovery.....4

 Tools Used4

Business Requirements5

 Technology-related Goals and Objectives.....5

 Future Plans Affecting Network Infrastructure5

 Campus Additions, Closures, or Changes.....5

 Plans for Campus Modernization.....5

 Business-critical Services.....5

 Critical Applications on Network Infrastructure5

Findings.....6

 Routers/Switches6

 Routers/Switches: Inventory6

 Routers/Switches: EoX Milestones9

 Routers/Switches: Software Versions and Recommendations.....9

 Routers/Switches: Scoring and Analysis11

 Wireless.....17

 Wireless: Inventory17

 Wireless: EoX Milestones.....18

 Wireless: Software Versions and Recommendations18

 Wireless: Scoring and Analysis.....19

 Network Security.....26

 Network Security: Features in Use26

 Network Security: Inventory28

 Network Security: EoX Milestones.....28

 Network Security: Software Versions and Recommendations28

 Network Security: Scoring and Analysis.....28

 Datacenter.....43

 Datacenter: Inventory.....43

 Datacenter: EoX Milestones43

 Datacenter: Scoring and Analysis.....44







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  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.  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

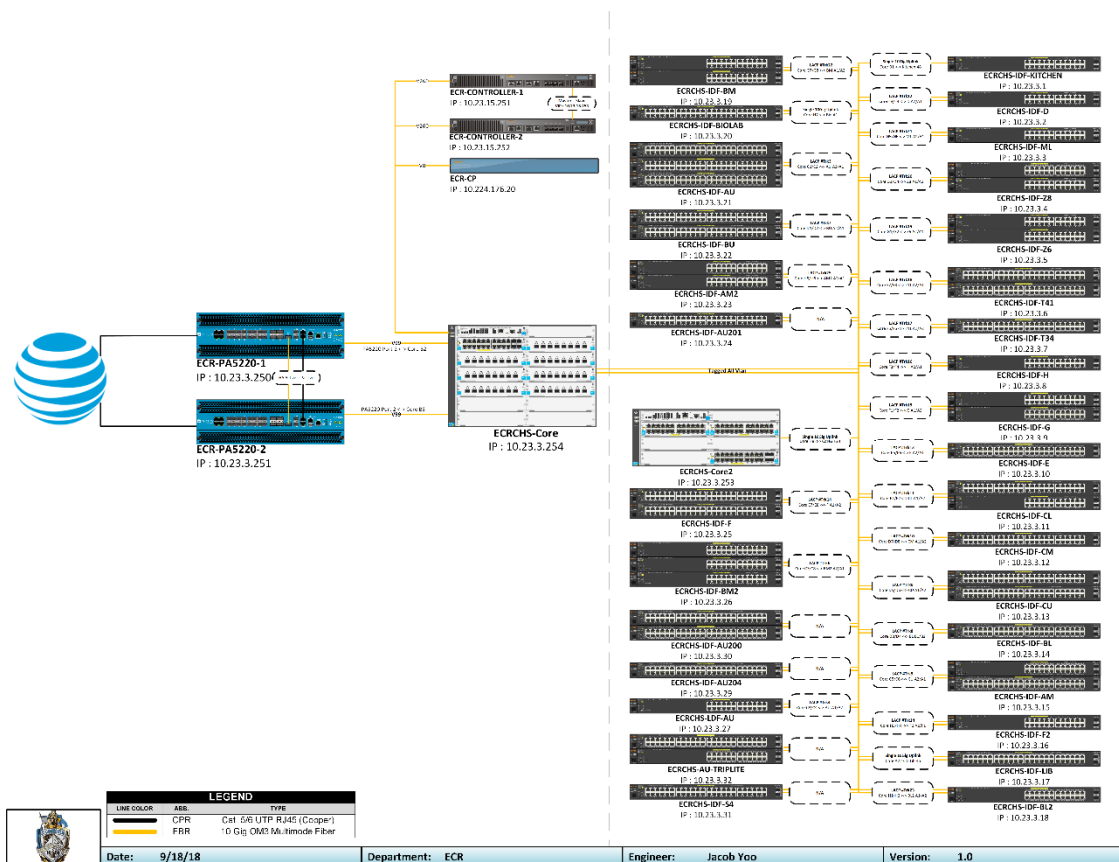
The services critical to ECRCHS are wireless services (1-to-1 network), the next-gen firewall features within the Palo Alto firewalls, VoIP/Jive, and Aeries.



Findings

Routers/Switches

Routers/Switches: Inventory

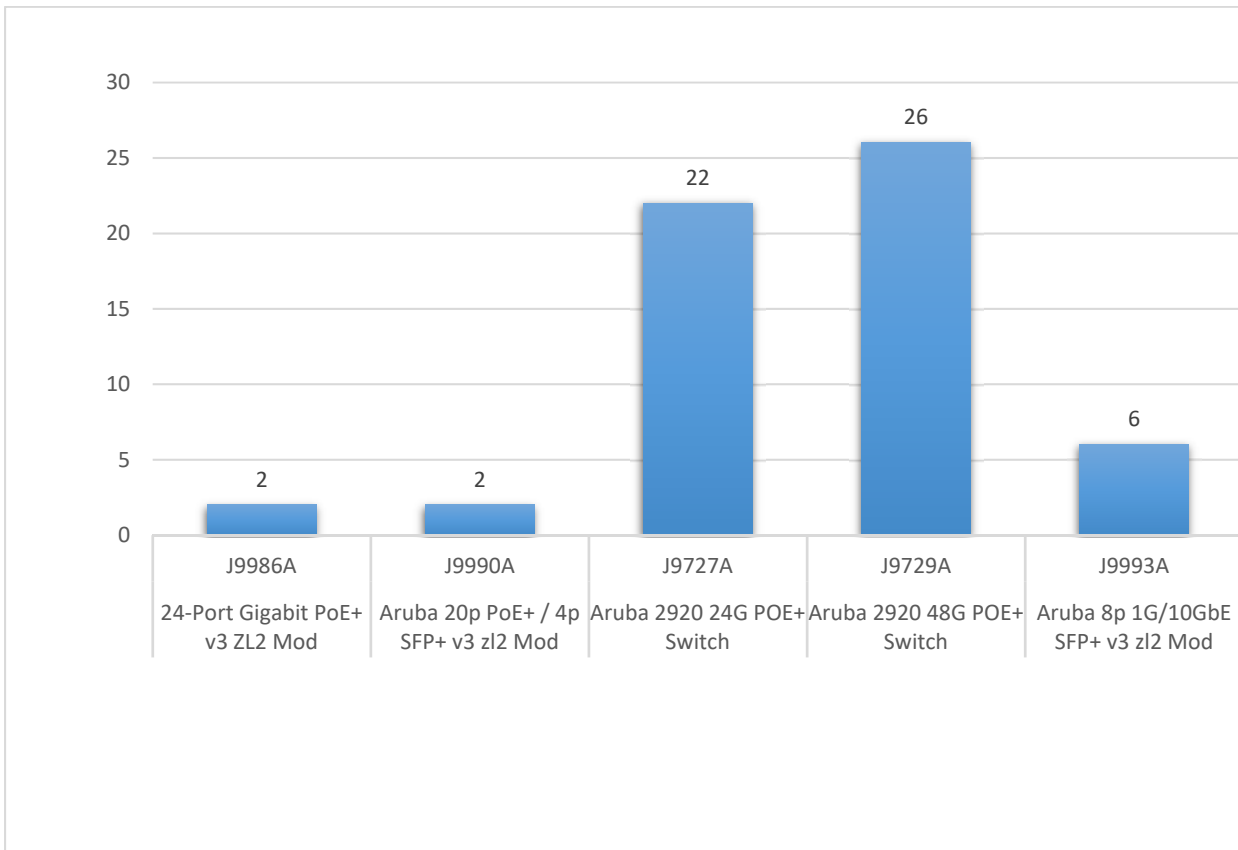
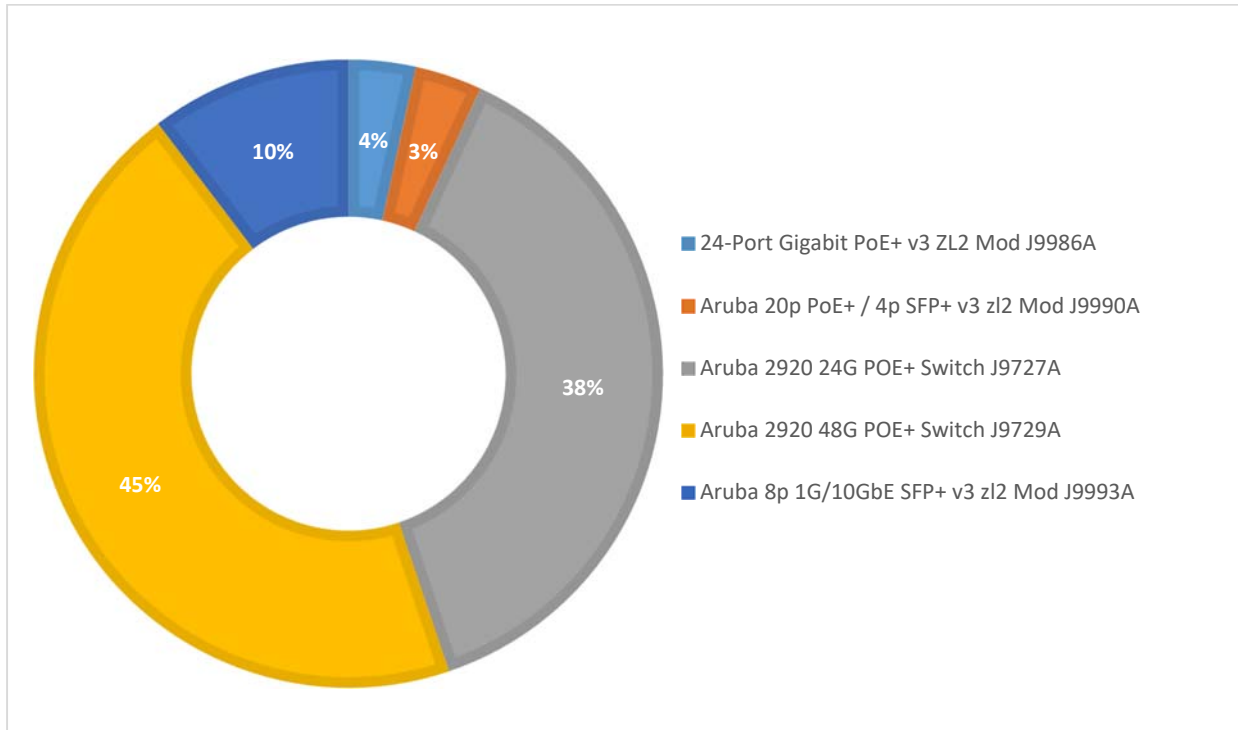


The table below shows the quantities of individual switches, by model. Note that many of these switches are stacked or modules within a chassis of a modular switch. Stacked switches and modules within the chassis will often appear as a single logical entity with modules or blades instead of individual 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 z12 Mod	2
J9993A	Aruba 8p 1G/10GbE SFP+ v3 z12 Mod	6
Grand Total		58



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





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 L22 modular switches at the core of their network. The largest of these switches is an Aruba 5412R L22, 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 L22, 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 line card slots and one (1) open/available management slot.

Both Aruba 5400R L22 switches feature hot-swappable redundant power supplies and cooling fan trays.

The 5400R L22 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 L22 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 z12 Switch Chassis	J9821A	current	current	current
1	Aruba 5412R z12 Switch Chassis	J9822A	current	current	current
2	Aruba 5400R z12 Management Module	J9827A	current	current	current
2	Aruba 5400R 2750W PoE+ z12 PSU	J9830B	current	current	current
2	24-Port Gigabit PoE+ v3 ZL2 Mod	J9986A	current	current	current
2	Aruba 20p PoE+ / 4p SFP+ v3 z12 Mod	J9990A	current	current	current
6	Aruba 8p 1G/10GbE SFP+ v3 z12 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.

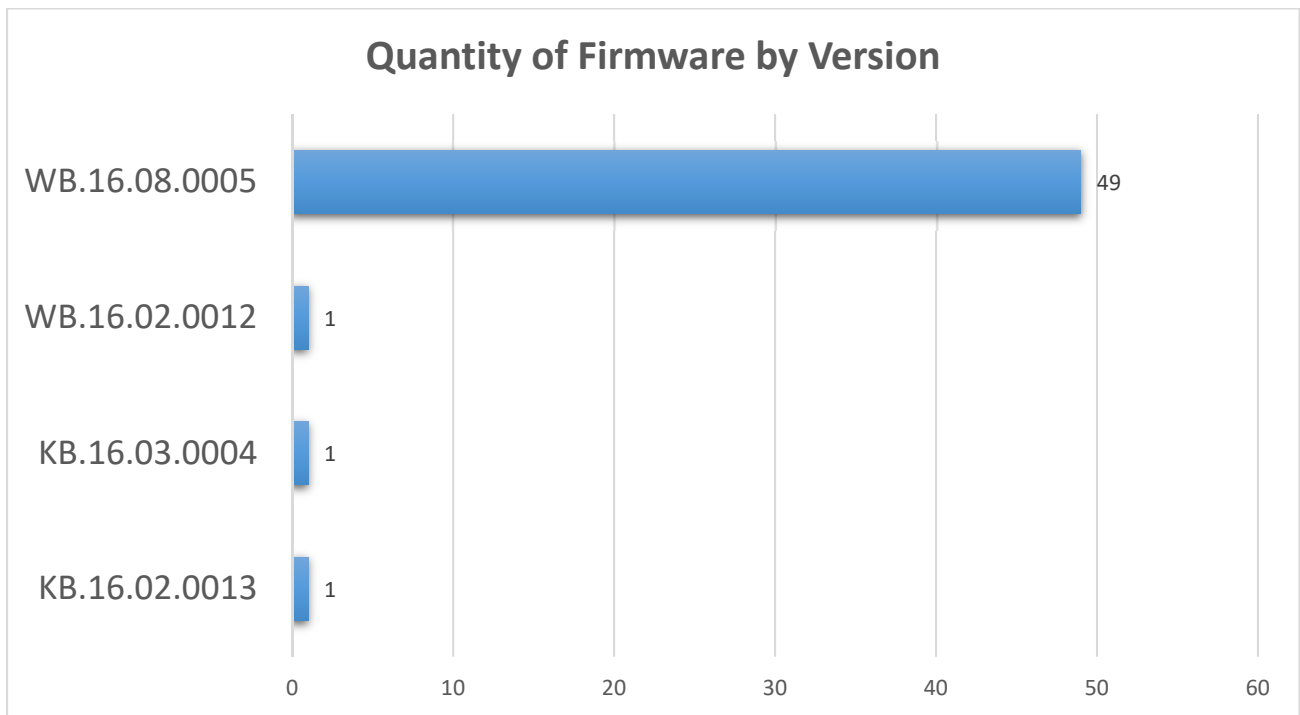
NIC Partners recommends upgrading all older release versions to a current release version within the same software branch. For example, the Aruba J9727A (ECR_DMZ) is currently on the software branch WB.16.02, using revision x.0005 but the current release of that branch is x.0027. NIC Partners recommends 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.





Routers/Switches: Scoring and Analysis

Components Assessed

- **Backbone port speed/capacity**

- 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**

- 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.
- 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.
- 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**

- 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.
- 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.



Scoring

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

Score: 4/5



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

Score: 3/5



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

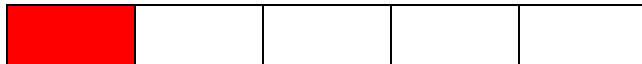
Higher PoE capabilities are better, as a switch with higher PoE budgets can power more devices and devices that have high power requirements. A proper PoE design would take into consideration the capacity of the electrical circuits feeding the switches; care must be taken to not overload the typical 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

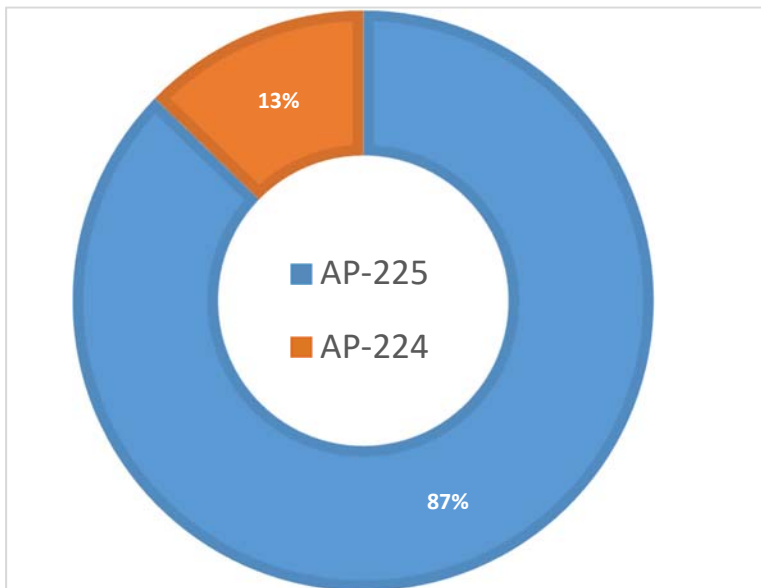
Wireless: Inventory

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



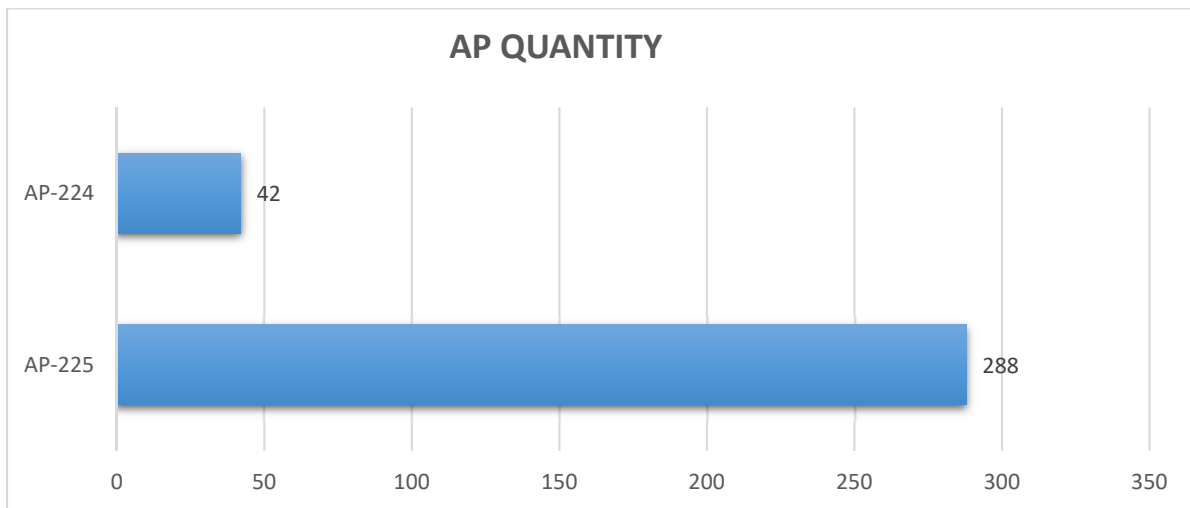
Aruba 7210 Mobility Controller



Aruba AP-225



Aruba AP-224





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>



Wireless: Scoring and Analysis

Components Assessed

- **Speed**
 - 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**
 - 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**
 - 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**
 - 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.

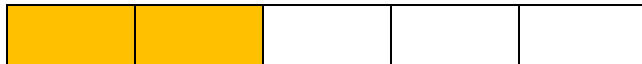


- **Guest/BYOD Accessibility**

- 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 Score: 4/5



- 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**
 - 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**
 - 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**
 - 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**
 - 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**
 - 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

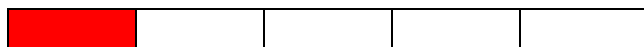
Analysis:

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



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)

Score: 4/5



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.

Notes:

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

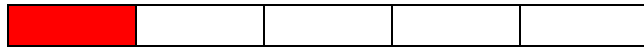
Analysis:

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



Datacenter: Scoring and Analysis

Components assessed

- **Compute**
 - '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**
 - 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**
 - 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**
 - 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)**
 - 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

Score: 3/5



- 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

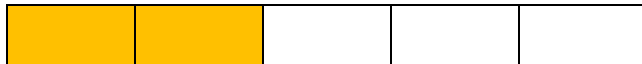


internally hosted applications as business critical. Should business critical services be utilized within ECRCHS local datacenter, NIC Partners does recommended implementing a replication partner to provide redundancy and resiliency against SAN hardware failure.



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

Score: 4/5



- 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.

Cover Sheet

Discuss and Possible Vote on Recommendation to Board on E-Rate Eligible Items

Section: II. Technology Committee
Item: B. Discuss and Possible Vote on Recommendation to Board on E-Rate Eligible Items
Purpose: Vote
Submitted by:
Related Material: eRate Quotes.pdf

Quote Comparison Form 471# 191035242 FRN 1999063850; 1999068921

GIGACOM

SKU	Description	Price
J9822A	5412R ZL2 SWCH Mfr: Aruba	\$2,242.87 FRN 1999063850
J9830B#ABA	ARUBA 5400R 2750W POE+ ZL2 PSU (Power Supply)	\$1,267.50 FRN 1999063850
J9986A	24P 10/100/1000BT POE+ V3 ZL2 Mfr: Aruba (24 Port POE Module)	\$1,755.19 FRN 1999063850
J9993A	8PT 1G 10GBE SFP+ V3 ZL2 MOD Mfr: Aruba (8 Port SFP+ Module)	\$2,340.41 FRN 1999063850
J9150D	ARUBA Compatible 10G SFP+ LC SR 300M MMF XCVR Mfr: ENET Components, Inc. (SFP+ GIBIC)	\$127.00 FRN 1999063850
J9822A	5412R ZL2 SWCH	\$2,242.87 FRN 1999063850
J9829A#ABA	5400R 1100W POE+ ZL2 P/S (Power Supply)	\$602.44 FRN 1999063850
J9993A	8PT 1G 10GBE SFP+ V3 ZL2 MOD (SFP+ Module)	\$2,340.41 FRN 1999063850
J9151E	ARUBA Compatible 10G SFP+ LC LR 10KM SMF XCVR (SFP+ GIBIC)	\$361.75 FRN 1999063850
5PX1500IRT	Eaton UPS 1500 VA	\$724.74 FRN 1999063850
SR42UBEXPND	Triplite Rack 42 unit cabinet	\$689.97 FRN 1999063850
JL322A	ARUBA 2930M 48G POE+ 1 SLOT SWCH	\$3,091.44 FRN 1999063850
JL086A#ABA	ARUBA X372 54VDC 680W PS (Power Supply)	\$313.23 FRN 1999063850
JL083A	ARUBA 3810M 2930M 4SFP+ MOD (SFP+ Module)	\$617.15 FRN 1999063850
J9150D	ARUBA Compatible 10G SFP+ LC SR 300M MMF XCVR	\$127.00 FRN 1999063850
J9151E	ARUBA Compatible 10G SFP+ LC LR 10KM SMF XCVR	\$361.75 FRN 1999063850
JW321A	ARUBA IAP-324 US INSTANT 4X4:4 11AC AP	\$683.81 FRN 1999063850
JW001A	ARUBA AP-ANT-13B 2.4/5G 4/3DBI OMNI	\$68.98 FRN 1999063850

GOLDEN STATE (GST)

SKU	Description	Price
J9821A	Aruba 5406R z12 Switch	7,504.25 FRN 1999063850
U4832E	HPE Networks 54xx/82xx z1 Startup SVC [for J9821A]	2,759.99 FRN 1999063850
J9830B	Aruba 5400R 2750W PoE+ z12 PSU	3,220.50 FRN 1999063850
J9830B ABA	INCLUDED: Power Cord - U.S. localization	incl. FRN 1999063850
J9986A	Aruba 24p 1000BASE-T PoE+ v3 z12 Mod	3,970.89 FRN 1999063850
JL322A	Aruba 2930M 48G PoE+ 1-slot Switch	6,659.47 FRN 1999063850
H2CA6E	HPE 3Y FC 4H Exch A 2930M 48G P Swt SVC [for JL322A]	2,577.99 FRN 1999063850
JL086A	Aruba X372 54VDC 680W Power Supply	671.25 FRN 1999063850
JL086A ABA	INCLUDED: Power Cord - U.S. localization	incl. FRN 1999063850
JL083A	Aruba 3810M/2930M 4SFP+ MACsec Module	1,325.99 FRN 1999063850
J9583A	HPE X410 1U Univ 4-post RM Kit	135.45 FRN 1999063850
J9150D	HPE X132 10G SFP+ LC SR Transceiver	1,100.25 FRN 1999063850
J9151D	HPE X132 10G SFP+ LC LR Transceiver	2,997.89 FRN 1999063850
9PX6K	Eaton UPS	5,125.21 FRN 1999063850
9PXE8M180RT	ERM	1,198.75 FRN 1999063850
CWR-18-26PD	Middle Atlantic CWR-18-26PD	859.89 FRN 1999063850
CWR-26-32PD	Middle Atlantic CWR-26-32PD	1099.26 FRN 1999063850
DWR-35-22PD	Middle Atlantic DWR-35-22PD	1497.85 FRN 1999063850
JZ152A	Aruba AP-318 (RW) 802.11n/ac Dual 2x2:2/4x4:4 Radio 6xRPSMA Connectors	1,502.23 FRN 1999063850
JW795A	Aruba AP-314 802.11n/ac 2x2:2/4x4:4 MU-MIMO Dual Radio Antenna Connectors AP	1,045.55 FRN 1999063850
JX963A	Aruba AP-365 (EG) 802.11n/ac Dual 2x2:2 Radio Integrated Omni Ant Outdoor AP	1,100.78 FRN 1999063850
JW009A	AP-ANT-1W 2.4-2.5GHz (4dBi)/4.9-5.875GHz (6dBi) Hi Gain	62.25 FRN 1999063850
JH395A	HPE FF 5940 48SFP+ 6QSFP+ Switch	15,112.28 FRN 1999063850
H25H4E	HPE 3Y FC 24x7 5940 Fixed 48G SVC [for JH395A]	13,097.25 FRN 1999063850
JG552A	HPE X711 Frt(prt) Bck(pwr) HV Fan Tray	399.89 FRN 1999063850
JC680A	HPE 58x0AF 650W AC Power Supply	785.36 FRN 1999063850
JC680A ABA	INCLUDED: Power Cord - U.S. localization	incl. FRN 1999063850
JD092B	HPE X130 10G SFP+ LC SR Transceiver	1,400.52 FRN 1999063850
JD094B	HPE X130 10G SFP+ LC LR Transceiver	2,725.37 FRN 1999063850
JW834A	HPE Aruba Mobility Controller 7240XM (US) - network management device	3,275.00 FRN 1999068921

OMICRON

SKU	Description	Price
Extreme 7148	48 port 1Gb/10Gb Ethernet RJ-45 + 4xQSFP+	\$ 27,699.99 FRN 1999063850
Extreme 7124T	24 port 1Gb/10Gb Ethernet RJ-45 + 4xQSFP+	\$ 22,399.99 FRN 1999063850
Extreme 220-48P	48 port Gigabit Layer 3 POE+ (370W) + 4x10Gb SFP+	\$ 1,999.99 FRN 1999063850
HPE	AF462A 7200VA AC 200/208V 4U	\$ 4,199.99 FRN 1999063850
Extreme AP3935E	Enterprise-Class Dual Band/Dual Radio 802.11ac/a/b/g/n Indoor	\$ 1,039.99 FRN 1999063850

CYTRANET

N/Q **		FRN 1999068921
N/Q **		FRN 1999063850

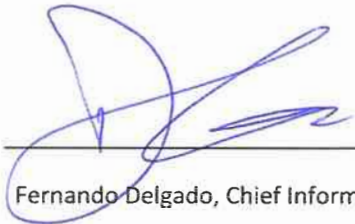
FRUBU

N/Q **		FRN 1999063850
N/Q **		FRN 1999068921

** No Quote

ECRCHS 2019 eRate Internal Connections Quote Eval Form 471# 191035242 FRN 1999063850

Factor	Max Points	Cytranet	Frubu	GigaKOM	Omicron	GST
Prices/Charges	30	20	10	25	15	20
Prior experience	25	0	0	15	0	25
Completeness of Solution	20	10	5	15	5	20
Local Vendor	15	0	0	15	0	15
Management Capability	10	5	5	10	5	10
	100	35	20	80	25	90



Fernando Delgado, Chief Information Officer

3/25/19

Date



12881 166th Street
 Cerritos, CA 90703
 www.gstes.com
 (562) 345-8700

OP53732 E-Rate_ERCHS_2019-2020



Prepared by:

Golden Star Technology
 Min Joo
 (562) 345-8744
 Fax (562) 546-1290
 mjoo@gstes.com

Prepared for:

El Camino Real Charter High School
 5440 Valley Circle Blvd PO# PO1212
 Woodland Hills, CA 91367
 Fernando Delgado
 f.delgado@ecrchs.net
 (818) 595-7575

Quote Information:

Quote #: 054053
 Version: 2
 Quote Date: 03/25/2019
 Expiration Date: 06/30/2019

Hardware

Line	Item	Description	Price	Qty	Ext. Price	Taxable
1	J9821A	HPE 5406R z12 Switch - Manageable - 3 Layer Supported - Modular - 4U High - Rack-mountable - Lifetime Limited Warranty	\$7,504.25	1	\$7,504.25	<input checked="" type="checkbox"/>
2	U4832E	HPE Care Pack - Service - On-site - Installation and Startup - Physical Service	\$2,759.99	1	\$2,759.99	<input checked="" type="checkbox"/>
3	J9830B	Aruba Power Module - 2750 W	\$3,220.50	2	\$6,441.00	<input checked="" type="checkbox"/>
4	J9830B ABA	INCLUDED: Power Cord - U.S. localization	\$0.00	2	\$0.00	<input checked="" type="checkbox"/>
5	J9986A	HPE 5400R 24-port 10/100/1000BASE-T PoE+ with MACsec v3 z12 Module - For Data Networking 24 RJ-45 1000Base-T LAN - Twisted Pair Gigabit Ethernet - 1000Base-T - 1 Gbit/s	\$3,970.89	6	\$23,825.34	<input checked="" type="checkbox"/>
6	JL322A	Aruba 2930M 48G POE+ 1-Slot Switch - 48 Ports - 2 Layer Supported - Modular - Twisted Pair	\$6,659.47	1	\$6,659.47	<input checked="" type="checkbox"/>
7	JL086A	HPE Aruba X372 54VDC 680W 100-240VAC Power Supply	\$671.25	1	\$671.25	<input checked="" type="checkbox"/>
8	JL086A ABA	INCLUDED: Power Cord - U.S. localization	\$0.00	1	\$0.00	<input checked="" type="checkbox"/>
9	JL083A	HPE Aruba 3810M 4SFP+ Module - For Data Networking, Optical Network Optical Fiber 10 Gigabit Ethernet - 10GBase-X4 x Expansion Slots - SFP+	\$1,325.99	1	\$1,325.99	<input checked="" type="checkbox"/>
10	J9583A	HPE Rack Mount for Power Supply	\$135.45	1	\$135.45	<input checked="" type="checkbox"/>



12881 166th Street
Cerritos, CA 90703
www.gstes.com
(562) 345-8700

Hardware

Line	Item	Description	Price	Qty	Ext. Price	Taxable
11	J9150D	Aruba 10G SFP+ LC SR 300m OM3 MMF Transceiver - For Data Networking, Optical Network 1 LC 10GBase-SR Network - Optical Fiber Multi-mode - 10 Gigabit Ethernet - 10GBase-SR - Plug-in Module	\$1,100.25	1	\$1,100.25	<input checked="" type="checkbox"/>
12	J9151D	Aruba 10G SFP+ LC LR 10km SMF Transceiver - For Data Networking, Optical Network 1 LC 10GBase-LR Network - Optical Fiber Single-mode - 10 Gigabit Ethernet - 10GBase-LR - Plug-in Module	\$2,997.89	1	\$2,997.89	<input checked="" type="checkbox"/>
13	9PX6K	Eaton 6kVA Tower/Rack Mountable UPS - 3U Rack/Tower - 3 Minute Stand-by - 110 V AC, 220 V AC Input - 200 V AC, 208 V AC, 220 V AC, 230 V AC, 240 V AC Output - 1 x NEMA L6-20R, 2 x NEMA L6-30R, Hardwired	\$5,125.21	2	\$10,250.42	<input type="checkbox"/>
14	9PXEBM180RT	Eaton 5/6 kVA EBM	\$1,198.75	6	\$7,192.50	<input checked="" type="checkbox"/>
15	CWR-18-26PD	Middle Atlantic CWR Series Rack, - For Patch Panel - 18U Rack Height 24" Rack Depth - Wall Mountable - Black Powder Coat - Steel - 250 lb Maximum Weight Capacity	\$859.89	3	\$2,579.67	<input checked="" type="checkbox"/>
16	CWR-26-32PD	Middle Atlantic CWR Series Rack, - For Patch Panel - 26U Rack Height x 19" Rack Width x 30" Rack Depth - Wall Mountable - Black Powder Coat - Steel, Plexiglass	\$1,099.26	3	\$3,297.78	<input checked="" type="checkbox"/>
17	DWR-35-22PD	35 SP. (61 1/4") DATA WALL RACK WITH PLEXI DOOR, FITS 20" DEEP EQUIP., BLACK FINISH	\$1,497.85	3	\$4,493.55	<input checked="" type="checkbox"/>
18	JZ152A	Aruba AP-318 IEEE 802.11ac 2 Gbit/s Wireless Access Point - 5 GHz, 2.40 GHz - MIMO Technology - Beamforming Technology - 1 x Network (RJ-45) - USB - Ceiling Mountable, Pole-mountable, Wall Mountable	\$1,502.23	15	\$22,533.45	<input checked="" type="checkbox"/>
19	JW795A	Aruba AP-314 IEEE 802.11ac 2.10 Gbit/s Wireless Access Point - 5 GHz, 2.40 GHz - MIMO Technology - Beamforming Technology - 1 x Network (RJ-45) - USB - Wall Mountable, Ceiling Mountable	\$1,045.55	14	\$14,637.70	<input checked="" type="checkbox"/>
20	JX963A	Aruba AP-365 IEEE 802.11ac 1.27 Gbit/s Wireless Access Point - 5 GHz, 2.40 GHz - MIMO Technology - Beamforming Technology - 1 x Network (RJ-45) - USB - Wall Mountable, Pole-mountable	\$1,100.78	14	\$15,410.92	<input checked="" type="checkbox"/>



12881 166th Street
 Cerritos, CA 90703
 www.gstes.com
 (562) 345-8700

Hardware

Line	Item	Description	Price	Qty	Ext. Price	Taxable
21	JH395A	HPE FlexFabric 5940 48SFP+ 6QSFP+ Switch - Manageable - 3 Layer Supported - Modular - Optical Fiber - 1U High - Rack-mountable	\$15,112.28	1	\$15,112.28	<input checked="" type="checkbox"/>
22	JG552A	HPE X711 Front (Port Side) to Back (Power Side) Airflow High Volume Fan Tray - Front to Back Air Discharge Pattern	\$399.89	2	\$799.78	<input checked="" type="checkbox"/>
23	JC680A	HPE HP 58x0AF 650W AC Power Supply - 110 V AC, 220 V AC	\$785.36	2	\$1,570.72	<input checked="" type="checkbox"/>
24	JC680A ABA	INCLUDED: Power Cord - U.S. localization	\$0.00	2	\$0.00	<input checked="" type="checkbox"/>
25	JD092B	HPE SFP+ Module - 10GBase-SR10	\$1,400.52	1	\$1,400.52	<input checked="" type="checkbox"/>
26	JD094B	HPE SFP+ Module - 1 x 10GBase-LR10	\$2,725.37	18	\$49,056.66	<input checked="" type="checkbox"/>
27	JW009A	Aruba AP-ANT-1 Antenna - 2.40 GHz, 4.90 GHz to 2.50 GHz, 5.88 GHz - 5.8 dBi - Indoor, Wireless Access Point, Wireless Data NetworkDirect Mount - Omni-directional - RP-SMA Connector	\$62.25	6	\$373.50	<input checked="" type="checkbox"/>
28	JW834A	Aruba 7240XM Wireless LAN Controller - 2 x Network (RJ-45) - USB	\$3,275.00	1	\$3,275.00	<input checked="" type="checkbox"/>

Subtotal: \$205,405.33

Quote Summary

Description	Amount
Hardware	\$205,405.33

Subtotal: \$205,405.33

Tax: \$18,539.71

Total: \$223,945.04

TERMS AND CONDITIONS

All prices and descriptions are subject to change without notice.

THIS PRICE LIST IS A QUOTATION ONLY AND IS NOT AN ORDER OR OFFER TO SELL. No contract for sale will exist unless and until a purchase order has been issued by you and accepted by Golden Star Technology Inc. ("GST"). Acceptance by GST of any offer is expressly conditioned upon your assent to the Terms and Conditions of Sale set forth in GST's invoices.

The prices contained in this list may not be relied upon as the price at which GST will accept an offer to purchase products unless expressly agreed to by GST in writing. Products quoted were selected by GST based on specifications available at the time of the quotation, and are not guaranteed to meet bid specifications. Product specifications may be changed by the manufacturer without notice. It is your responsibility to verify product conformance to specifications of any subsequent contract. All products are subject to availability from the manufacturer.



12881 166th Street
Cerritos, CA 90703
www.gstes.com
(562) 345-8700

The freight costs listed are estimates. Shipping costs may vary based on time of purchase, quantity ordered, shipment carrier and warehouse sourced. Actual shipping costs will be calculated during shipment and will be reflected on your invoice. For hardware product(s), manufacturer warranty will begin upon physical delivery of the hardware products(by) by the customer or GST warehouse. For software product(s), the manufacturer warranty will begin upon electronic or physical receipt of the software product(s) by you or GST.

GST is not responsible for compliance with regulations, requirements or obligations associated with any contract resulting from this quotation unless said regulations, requirements or obligations have been passed to GST and approved in writing by an authorized representative of GST.

Customer Signature

Date



GIGAKOM PROPOSAL for

El Camino Real Charter High School Internal Connections and/or BMIC 470 # 190026259

E-Rate 2019 – 7/1/2018 to 6/30/2019

SPIN # 143027209
FCC # 0011991395
Certified Small Business Micro # 40936
DIR Registration # 1000003984
Contractor License # 910431
CPUC # U-1202-C

Date: 3/20/2019

GigaKOM respectfully requests that the information in this proposal not be used or disclosed, in full or part, for any purpose other than that for which it was originally furnished without prior written permission of GigaKOM.

HQ: 3615 Kearny Villa Road, Suite 201 | San Diego, CA 92123 | Phone: 858-769-5408 | Fax: 858-565-2453



Table of Contents

1.	COVER LETTER	3
2	GIGAKOM CONTACTS	4
3	INTRODUCTION – DESCRIPTION OF FIRM.....	5
4	EXPERIENCE AND QUALIFICATIONS	6
5	CERTIFICATIONS, TRAINING AND SPECIALIZATIONS:.....	7
6	MASTER CONTRACTS AND PURCHASING AUTHORIZATIONS	8
7	METHODOLOGY FOR PROVIDING SERVICES	9
	Support Services	13
8	PRICING.....	19
9	UNIVERSAL SERVICE PROGRAM RESTRICTIONS AND INVOICING.....	23
10	SPECIAL NOTES AND CONDITIONS	23
11	REFERENCES	26
12	APPENDICES	31



1. Cover Letter

March 20, 2019
Fernando Delgado
5440 VALLEY CIRCLE BLVD
WOODLAND HILLS, CA 91367

Dear Fernando Delgado,

GigaKOM thanks you for the opportunity to present our Category 2 erate proposal. We have carefully constructed a complete technical solution that will serve your District for many, many years.

GigaKOM is a full-service *Information Technology Solutions Provider*, as we specialize in full cycle IT Solutions. We have partnered with the industry's best network and system manufacturers to provide you with cost effective, superior products and services. Our staff is highly qualified and is always available to assist you with any of your technical needs. GigaKOM is your strategic partner and trusted advisor. We will engage with you to create and execute your strategic goals. GigaKOM's engineers hold the highest level of certifications and training with multiple manufactures including Cisco, HPE, Aruba, Aerohive, Ruckus, Extreme, Microsoft, VMWare, and many more.

GigaKOM is a California Corporation providing IT services and support since 2003. Additionally, GigaKOM is a certified Small Business with the State of California, Department of General Services. We have completed projects from a single-server upgrade to the design and installation of complete data centers.

Thank you for your consideration and the opportunity to partner with El Camino Real Charter High School on this erate Category 2 Project.

Dean Kolesar **Account Manager**

P 818-588-5188
F 858-565-2453
deankolesar@gigakom.com

GigaKOM
3615 Kearny Villa Road
Suite 201
San Diego, CA 92123
www.gigakom.com



2 **GigaKOM Contacts**

The GigaKOM contacts for this proposal are:

Contacts:

Dean Kolesar
Account Manager
Phone: (818) 588-5188
Fax: (858) 565-2453
deankolesar@gigakom.com

Greg Argendeli
VP Engineering Services
Phone: (858) 769-5403
Fax: (858) 565-2443
arg@gigakom.com

Office Locations

- MAIN OFFICE/San Diego
3615 Kearny Villa Road, Suite 201
San Diego, CA 92123
- Los Angeles
9107 Wilshire Blvd. Suite 450
Beverly Hills, CA 90210
- Northern California
3511 Thomas Road, Suite 9
Santa Clara, CA 95054
- Bay Area
1600 Harbor Bay Parkway, Ste 100
Alameda, CA 94502
- Central California
4450 California Ave, Suite 192
Bakersfield, CA 93309
- Fresno
1713 Tulare St
Fresno, CA 93721



3 Introduction – Description of Firm

This proposal is for GigaKOM to assist El Camino Real Charter High School with Category 2 Internal Connections for E-Rate Eligible Network and Telecommunications Systems.

GigaKOM is a full service *Information Technology Solutions Provider*. We specialize in Technology for Education. Our vision is to improve the stability of each and every network we service. We have partnered with the industry's best network and system manufacturers to provide you with cost effective, superior products and services.

Our staff is highly qualified and is always available to assist you with any of your technical needs. GigaKOM has delivered solutions ranging from desktops, mobile devices, and classroom technology to complete networks and data centers including virtualization. Our solutions ensure access to the vast array of technology resources that are available to improve your District's efficiency and learning experience. GigaKOM's engineers hold the highest level of certifications and training with multiple manufactures including Cisco, HPE / Aruba, Aerohive, Ruckus, Microsoft, VMWare, Xirrus and more.

GigaKOM is a California Corporation providing IT services and support since 2003. Additionally, GigaKOM is a certified Small Business with the State of California, Department of General Services.

GigaKOM is an established vendor that has been providing ERATE and non-ERATE services for the fifteen years throughout California, utilizing employees that have been in the program since year one (including a former California Certified ERATE Trainer). We have completed projects from a single-server upgrade to the design and installation of complete school data centers.





4 Experience and Qualifications

GigaKOM is a full service *Information Technology Solutions Provider*. Our vision is to improve the stability of each and every network we service. We have partnered with the industry's best network and system manufacturers to provide you with cost effective, superior products and services.

Our staff is highly qualified and is always available to assist you with any of your technical needs. GigaKOM has created solutions ranging from desktops to complete networks that ensure access to the vast array of technology resources that are available to improve your business efficiency. GigaKOM's engineers hold the highest level of certification.

GigaKOM has completed multiple enterprise level implementations in all the areas below, as well as technologies not listed. Please see References section for a sample of projects completed.

Systems Integration:

GigaKOM provides professional computer solutions and services to improve the client's technological capabilities.

Infrastructure design and installation, Integration services, and Implementation management are mission-critical to any technology project. GigaKOM integrates these services to provide a single source for all computing needs. Below are samples of the ways that GigaKOM can assist our Education clients.

Local and Wide Area Network (LAN/WAN) Design & Implementation Services:

GigaKOM helps organizations design, install, and maintain enterprise-wide systems for voice, video, and data communications. Utilizing industry standard technology and certified engineers and project managers, GigaKOM works with organizations to ensure stable, robust, and expandable solutions for our client's needs. Network documentation and infrastructure testing capabilities are an integral part of the LAN/WAN services.

Security Services:

GigaKOM provides our clients with the programs and tools necessary to ensure network security at all levels. GigaKOM analyzes, recommends, installs security systems, and assists in establishing policies and procedures to provide the highest level of technology security available. GigaKOM provides an array of security provisions: physical security, desktop provisions, virus protection software, firewalls, intrusion detection systems, and internet filtering capabilities.

Hardware and Software Services:

GigaKOM, through its experience and partnerships, offers a high level of expertise in product selection, purchasing, installation, and maintenance – from desktop computers to the entire network infrastructure. GigaKOM offers a hardware/software asset management and license compliance service.

Cloud Computing, Virtualization and Thin Client:

GigaKOM guides businesses in decision and implementation of Cloud, Virtualization and Thin Client solutions.

Cloud Computing provides for decentralization of hardware, risk and recovery advantages, as well as Access-Anywhere capabilities.

Thin-client technology transforms networks from a collection of decentralized computer devices into a centrally manageable computing environment, providing low-cost, standardized, easily updateable, and centralized systems.



Virtualization provides many benefits including fail-over and redundancy solutions, leveraging hardware utilization, and cost savings in power, facilities and management.

Network Management and Maintenance:

GigaKOM provides comprehensive network maintenance solutions client tailored to meet each individual client's network requirements. From hardware warranty programs, to labor support and complete network management programs, GigaKOM has the program and expertise to keep networks running at their optimal capabilities.

GigaKOM wants to be your Partner in Educational Technology. We are certified by all major IT manufacturers and specialize in servicing clients throughout the South Western United States.

5 Certifications, Training and Specializations:

For a full list of GigaKOM certified personal please reach out to hr@gigakom.com
Listed are some of our Partner and Certifications

Cisco

Company Certification

- Premier Certified Partner

Specializations

- Advanced Unified Communications
- Express Foundation
- Cisco Capital Financing
- Cisco Smart Care Services
- Cisco Smart Care



Professional Certification and Training

- CCIE, CCNP, CCDA and more

Microsoft

Company Certification

- Authorized Partner

Specializations

- Educational Licensing Authorized



HPE - Aruba

Company Certification

- HPE Aruba Gold Partner
- Networking Elite



Specializations

- Public Sector

VMWare

Company Certification

- Professional
- Educational Licensing



Xirrus Wireless



Company Certification

- Gold Certification

Aerohive Wireless

Company Certification

- Elite Certified Partner



Ruckus Wireless

Company Certification

- Certified Partner



MileStone

Company Certification

- Gold Certification



Extreme Networks

Company Certification

- Gold Certified Partner



6 Master Contracts and Purchasing Authorizations:

In order to best serve our Government and Educational clients, GigaKOM has multiple purchasing vehicles available. Our contracts include:

Details at: <https://goo.gl/XaDLCC>

CMAS Contract ID 3-17-70-2346J

- Cisco Networking Equipment / Services
- HPE Networking Equipment / Services
- Aruba Networking Equipment / Services
- HP Computer Systems / Services
- Data Communications – Equipment



CMAS Contract ID 3-13-70-2346E

- Technical Labor Services

CMAS Contract ID 3-12-70-2346F

- Axis



CMAS Contract ID 3-13-70-2346H

- Aerohive Networks
- Ruckus Networks
- Network Security Products / Services
- Network Systems



CMAS Contract ID 3-18-70-2346K

- APC products / services
- Tripp Lite products / services
- Network Systems
- Security products / services



CMAS Contract ID 3-18-70-2346M

- Extreme Networks products / services
- Network Systems
- Security products / services





GSA Schedule GS-35F-0143R

- APC
- Ergotron
- HP, HPE, HPi
- Lenovo
- NEC
- Sony
- Tripplite
- Xerox



GSA Schedule GS-35F-0349S

- Cisco Networking Communications
- Hewlett Packard Enterprise
- Hewlett Packard, Inc



WSCA NASPO Contract AR-233

- Cisco Networking Communications
- Cisco Maintenance
- Cisco Services
- Cisco Servers
- Cisco Software



WSCA Contract – HP

- HP ProLiant Hardware
- HP Blade Systems
- HP Storage Products
- HP Printer
- HP Personal Computer Hardware
- HP Services
- HP Accessories



SPURR contract ID #SMC-ER-025

- AplianSys CacheBox



Educational Licensing Agreements

- Microsoft
- VMWare



For further information on these contracts please contact your GigaKOM sales representative for terms, conditions and product pricing.

Contracts listed are for reference and referral. Contracts listed may be utilized at part or all of product and service fulfillment. No bid is considered to be under one or any of the above contracts unless specifically outlined within the purchase agreement and confirmed by both parties. Additional fees may be charged by the Government Agency in association with the contract. Please refer to terms of schedule.

7 Methodology for Providing Services

GigaKOM proposes the following phased approach for new component integration into your network. With this approach GigaKOM will define activities needed to successfully deploy and operate new system(s) and optimize performance during the lifecycle of the solution.

Phase approach includes:

1. Preparation and Response Phase



2. Assessment Phase
3. Implementation Phase
4. Operation and Optimization Phase

Delivery Timetable:

- Hardware- within 14 business days from Client PO
- Installation – based on Client schedule

In Preparation and Response Phase, GigaKOM will respond to client's solution request based on requirements specified and propose a High Level Design and product to address client's needs.

Assessment Phase will determine if the existing system infrastructure, sites, and operational environment are able to support its proposed system.

During the Implementation Phase, GigaKOM will install the new technology into the client's network, ensuring it is integrated without disrupting the network or creating points of vulnerability.

During the Operation and Optimization Phase, GigaKOM will ensure that the newly implemented solution is operating efficiently and is highly available. GigaKOM, at client request, will propose a Maintenance support structure to help ensure that the client's networks are operating at peak performance, resolve problems quickly as they arise, and adapt the architecture, operation, and performance of the network to change.

Preparation and Response Phase:

In this phase GigaKOM will analyze client needs and identify and confirm the product in High Level Design Development. We will list all necessary parts numbers and any additional hardware that will needed to deliver the solution. We will allocate key members of the team trained and certified in the technology (per client requirements).

Assessment Phase:

GigaKOM will prepare for your deployment with a comprehensive site assessment that evaluates the readiness of your current facilities infrastructure to support the new technology. GigaKOM will identify physical, environmental, electrical and procedural modification that should be made prior to implementation. As part of the assessment GigaKOM will provide Assessment Analysis documents for each of the below specified actions with findings and the mitigation plan with any potential costs.

Methodology for Assessment:

Site Readiness Assessment, We will prepare for your deployment with a comprehensive site assessment that evaluates the readiness of your current facilities infrastructure to support the new technology. You will identify physical, environmental, and electrical modifications that should be made prior to implementation.

There are three activities associated with the site readiness assessment service component.

- Prepare for a site readiness assessment
- Conduct a facility site(s) survey
- Perform a site assessment gap analysis.



The site readiness assessment service component assesses the ability of the client's site facilities to accommodate the new technology system. Following completion of the site survey, you will identify any gaps with site requirements specifications.

Network Readiness Assessment: GigaKOM will prepare for your solution deployment by assessing the readiness of your existing network infrastructure and determining any modifications that should be made prior to implementation. The modifications could include physical and logical configurations, solution capacity, quality of service (QoS), and solution resiliency, security, and integration with existing legacy platforms. The network readiness assessment service component assesses the client's existing network infrastructure and applications to verify its ability to support the proposed technology system. This service also analyzes the physical and logical configuration of the network and analyzes network design issues, such as scalability, Quality of Service, network resiliency and security, and the potential effects of integrating the proposed system with existing infrastructure.

Operations Readiness Assessment: GigaKOM will prepare for your technology solution deployment with a comprehensive assessment that evaluates the readiness of the people, processes, and tools in your current operations and network management infrastructure for both voice and data to support the new solution. The operations readiness assessment service component assesses the current state of clients' operations and network management infrastructure, including people, processes, and tools, to identify issues and opportunities for improvement.

In addition, the operations readiness assessment identifies issues pertinent to defining, monitoring, and maintaining the proposed system service-level requirements, which are measured through availability, capacity, and security metrics. It also identifies the client's support model and associated skills and knowledge requirements.

- GigaKOM will collect and verify information about current operations support infrastructure
- GigaKOM will identify client support model
- GigaKOM will identify skills and knowledge requirement to support new solution

Implementation Phase:

During the implementation phase, GigaKOM will install the new technology into the client's network, ensuring it is integrated without disrupting the network or creating points of vulnerability.

Steps for Implementation Phase

- Project Planning
- Kickoff
- Staging
- Deployment
 - Core Components Rollout
 - System Integration
 - System Migration (as requested per client)
- Training
- Closeout Documentation

Project Planning:

During project planning GigaKOM will develop the project management, escalation, and communication plans, and conduct an internal kick-off meeting.



Kickoff:

During implementation project kickoff GigaKOM will conduct the kickoff meeting with all parties involved in the deployment of system. At the meeting parties will review and confirm implementation milestones, roles, and responsibilities using a project plan, as well as review the escalation and communication plans to ensure everyone is on the same page, and share the plan for leading the project to a successful completion. The District will be provided access to an on-line portal with the ability to view and track the project as phases are planned and implemented.

Staging:

During staging, GigaKOM will stage the communications hardware and software to be installed in the client's network. GigaKOM will test the solution components in a non-production lab environment. After the successful completion of staging, the hardware delivered to the client site and made ready for the implementation phase.

Deployment:

- Core Component Rollout: During core product implementation, GigaKOM will install, configure, integrate, and test the solution components, providing an implemented, production-ready solution, making it available for the integration of existing users and services from existing infrastructure to the new solution.

-Legacy System Integration: The legacy systems as applicable will undergo an integration of the client's network solution components and requires the validation of integration options that are compatible with the new solution. GigaKOM will perform the test and integration between the systems.

Training:

GigaKOM will prepare and conduct end-user training and staff training. GigaKOM will give customized training to each user group according to the staff training plan and train end users only on those features they are allowed to use according to business policy.

Closeout Documentation:

During as built documentation, as the final stage of Implementation phase GigaKOM will compile documentation of the current system in an as built solution binder. In the binder, you will include logical and physical topology maps, IP schemes, serial numbers, application configurations, and legacy migration or integration configurations. Additionally, you will finalize network documentation that reflects as built information for the client, including specific design requirements and configurations.

- Compile documentation into a as built solution binder
 - o Logical and physical topology maps
 - o Dial plans
 - o Serial numbers
 - o Legacy configurations
 - o Application Configuration

Operation and Optimization phase:

During the operation phase, we will justify client network investment protection by ensuring that the newly implemented solution is operating efficiently and is highly available. During operations setup, we will set up the client to provide operational support to the network, including development of an operational support plan and an Ongoing Support Handoff Kit. Assisting the client in developing processes to manage the system in ongoing operations mode, including system administration and



backup, assessment management, and scheduled maintenance is another aspect of the operations setup.

- Develop an Operation Support Plan
- Assist the client in developing process to manage the system

Incident Management: During incident management, we will classify, prioritize, isolate, and resolve incidents and track and monitor incidents. Any required changes to the system are submitted to the formal change management process, and incidents are tracked and managed in a case management system. It is also important to manage real-time incidents with the system components via the incident-management process, which includes multiple levels of support that create and maintain the status of an incident through resolution and closure.

- Classify, prioritize, isolate and resolve incidents
 - Incidents are tracked and managed in case management system - Autotask
- Incident Management Steps:
1. Identify Incident
 2. Classify and prioritize the incident
 3. Isolate the incident
 4. Recover from incident outage
 5. Validate resolution
 6. Track and monitor progress
 7. Close the incident

Support Services

GigaKOM 's delivery of Support Services is dependent on the services required and specified by the client. Based on the services requested, GigaKOM follows the standard Methodologies for delivering the types of services as defined below.

Support Services can include the following components:

- **Manufacture maintenance agreements**
 - Software Downloads, bug fixes, security patching and technical
 - Hardware replacement warranties
- **Hardware replacement time and materials funding pools.**
- **Labor based technical support**
 - On-site technical support
 - Remote technical support
 - Remediation of technical issues
 - Labor based maintenance of network components to insure equipment operates at manufacture and industry specified performance levels.
- **Cable plant repair, upkeep and maintenance**

Based on the requested services from the client, GigaKOM would be prepared to meet expected maintenance windows as specified by the school.

For Basic Maintenance involving GigaKOM technical support, we provide a 24x7 contact number as well as a web-portal for the reporting of troubles on a client network.



Manufacture maintenance agreements

GigaKOM has partnered with most network manufactures to provide warranty solutions where available to provide eligible maintenance agreements.

For Maintenance agreements, GigaKOM will work with the district to verify eligible equipment identification, validate warranty levels and any End-of-support issues. GigaKOM will procure the maintenance contract with the manufacture and insure warranty is provided under the District's name and copies of the contract will be provided to the district.

For ineligible components or services, including Hardware warranties, GigaKOM will identify such components to the District and provide the District options to procure these services outside of E-rate funding.

Hardware replacement time and materials funding pools.

Within E-Rate guidelines certain funding is available for time and materials repair and replacement for the maintenance and upkeep of eligible equipment. Where appropriate GigaKOM will work with District to identify the eligible equipment.

Labor Based Technical Support:

Labor based technical support solutions are available to provide On-site technical support, remote technical support, remediation of technical issues designed to maintain eligible network components to insure equipment operates at manufacture and industry specified performance levels.

Our Solutions provide:

- Access to qualified technical assistance
- Ongoing operating system software updates and upgrades
- Systems diagnostics and remediation on select devices
- On demand and scheduled on site technical support

To be scheduled with GigaKOM and the client, based on recommendations from GigaKOM, we provide solutions that include:

- Network Device Configuration Backup
- Scheduled Network Software Upgrades
- Network Device IOS and Enhancement Review
- Weekly Windows Server Security and Health Check
- Server Operating System and Security Patching

GigaKOM Standards for Performance

- Initial Engagement and Yearly Network Discovery and Mapping
- For all activity performed on a network, status reports of actions taken and tasks completed are provided.

Network Restoration Process

Client desires the support and restoration of Network down problems caused by E-rate eligible equipment or cable plant.

Description: The following activities will be done by the GigaKOM over the term of the project as services are required.



- 1) Receive incident or request notification from Client personnel. This notification will come from the Client personnel who receive and respond to the initial problem call from the end user, and will only be forwarded to the GigaKOM technicians when it appears to be related to E-Rate eligible equipment.
- 2) Record all problem and request tickets in the GigaKOM ticket management system.
- 3) Perform "second level" incident and request handling using GigaKOM remote engineers. If necessary, we will dispatch a local GigaKOM field engineer. Additional engineers will be dispatched as needed to meet the service response requirement and will be dispatched immediately for more critical network down situations.
- 4) Provide "ownership to resolution" of GigaKOM handled incidents, report on the progress of problem resolution, confirm resolution of the incident with Client personnel, and log final resolution. Please note that in accordance with SLD guidelines, GigaKOM can provide eligible maintenance services as long as the equipment at issue is thought to be eligible. If the issue is determined to be caused by ineligible equipment, this will be reported back to Client personnel, and further work must be handled through Project Change Control.
- 5) Prioritize activities in accordance with documentation and procedural standards developed by GigaKOM and agreed to by Client.
- 6) Coordination and scheduling of GigaKOM resources.

Clients under a labor-based maintenance contract will be covered under the below Billing and Service Delivery Schedule unless specifically altered under contract.

BILLING AND SERVICE DELIVERY SCHEDULE

I Response Times:

GigaKOM provides for a 24 hour Client Service Center access number, as well as on-line trouble ticketing portal. For tickets opened via one of these methods GigaKOM will provide during standard working hours:

Response Times and Escalation Schedule

Priority	Description	Response Times	Escalation Policy	Billing Rate for Services
Critical (Priority 1)	Network down or critical impact to business operations. GigaKOM and end user will provide full-time resources to the situation resolution	1 Hour: Diagnostics begin 2 Hour: technician assigned Next Business Day or better: on-site dispatch if necessary	1 Hour: Service Supervisor 8 Hours Director of Operations 24Hours: President / CEO	Critical tickets are billed double rate with a minimum 2 hour billing. Standard labor terms apply
High (Priority 2)	Operations of a Network are severely degraded; client business operations are negatively impacted.	2 Hour: Diagnostics Begin 4 Hours: Technician assigned	4 Hour: Service Supervisor 24 Hours: Director of Operations	High priority tickets are billed at a one and a half (1 ½) rate with minimum 2 hour billing.



	GigaKOM and end user will commit full-time resources during normal business hours to address situation.	Next Business Day on-site dispatch if necessary	48 hours: President / CEO	Standard labor terms apply.
Medium / Normal (Priority 3)	Operational performance of the network is impaired. Business functions remain functional. GigaKOM and end user are willing to commit resources during standard business hours to restore service to satisfactory levels.	4 to 8 Hours: diagnostics and technician assigned On-site dispatch (if required) as scheduled with End User.	24 Hour: Service Supervisor 48 hours: Director of Operations 72 Hour: Department Manager	Billing rate as quoted. Standard labor terms apply.
Low (Priority 4)	Assistance or information requested. Typically product capabilities, installation or configuration issues.	8 Hour: Initial response.	72 Hours: Service Supervisor	Billing rate as quoted. Standard labor terms apply

(all times listed are based on standard working hours)

The clock starts on all issues once the support request has been added to our Autotask ticketing system

II Definitions:

The service priority Critical, High, Medium, or Low is set at the initiation of the ticket and remains at that level through completion

- Critical Priority is defined as a complete network down event or an event that has a critical impact to business operations. GigaKOM may assign multiple concurrent resources to critical events. The client may request the ticket to be assigned to this priority based on the client’s business objectives.
- High Priority is defined as an event where operations of a network are severely degraded and business operations are negatively impacted. GigaKOM may assign multiple, concurrent resources to critical events. The client may request the ticket to be assigned to this priority based on the client’s business objectives.
- Medium Priority is defined as an event that impairs the operational performance of the network, business operations remain functional but may be degraded. GigaKOM and the client are willing to commit



resourced during normal business hours to restore service. Unless otherwise requested by the client, this is the default level for all service tickets.

- Low Priority is defined as a general assistance or informational request. Network Performance degradation is negligible. This level of service is most commonly associated with initial installation or configurations tickets. The client may request the ticket to be assigned to this priority based on the client’s business objectives.

III Standard Labor Terms

Travel:	Not billed unless specified in contract.
Standard: specified	All billing in 1/2 hour increments unless otherwise
Critical Priority:	2.0 x rate, 2 hour minimum billing
High Priority:	1.5x rate, 2 hour minimum billing
Overtime:	1.5 x rate, 1 hour minimum billing
Weekend:	1.5 x rate, 2 hour minimum billing
Holiday	2.0 x rate, 4 hour minimum billing

Coverage

Standard: 8:00am to 5:00pm Monday through Friday PST

Overtime: Monday through Friday 5:00pm to 8:00am the following day

Weekend: Friday 5:00pm to 8:00am Monday

Holiday: 5:00pm prior day to Holiday to 8:00am the day after the holiday

Holidays

New Year’s Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, Day after Thanksgiving, Christmas Eve, Christmas Day.

A fee of \$250 will be assessed for client cancellation of dispatched engineer, or client not being ready.

IV Billing Information

GigaKOM will invoice labor against the contract on a bi-weekly basis. Failure to pay invoices may lead to delays or suspension of GigaKOM services.

Hours used against a contact will be tracked by GigaKOM and will be available to client upon request. In certain instances GigaKOM may exceed the contracted hours in the delivery of service. GigaKOM will invoice any additional hours at the rate agreed to under the contract and



will provide notice to the client when overages occur. Once identified, GigaKOM will work with client to establish a change order or new contract for continuing services.

V Responsibilities and Assumptions

- Client to provide access to systems and facilities to facilitate work.
- Client to provide GigaKOM with access to all equipment covered under this agreement. If such access is not provided, GigaKOM will have reduced or limited ability to address problems and provide resolution.
- Client to provide necessary user names and passwords where applicable.
- Client will identify at least one person to work with GigaKOM throughout the service request. This person will communicate with GigaKOM and provide information on a timely basis.
- For critical and high priority issues, client will provide an escalation / alternate contact to issue timely communications and resources.
- For critical priority issues, client is committed to working with GigaKOM on a 24-hour basis, if required, through problem resolution.
- Client is responsible for providing a contact who is knowledgeable to the technical aspects of the problem.
- Client to provide GigaKOM with a list of key personnel and contact information including after hours and escalations / approvals.
- Client is responsible for having vendor / manufacture service support agreements necessary to maintain, trouble shoot and repair hardware and software issues.
- Client will provide service provider account numbers, circuit ids, contacts and contract information where necessary to facilitate service delivery or resolution.
- Client to provide a list of all contract service agreements, contact names, contact numbers and contract numbers for all service agreements to be managed by GigaKOM.
- Client to provide any additional information required by GigaKOM.
- Client to provide all necessary supplies and accessories, attachments or other devices incidental to the service.
- Client is responsible for data, backups and / or migrations of data. GigaKOM is NOT responsible for the loss of client data during remediation or migration processes.
- Client is responsible for all necessary permits, licenses or authorities necessary for the provisioning of services.
- Client will be responsible for additional materials, equipment, or loaner materials costs necessary to facilitate problem resolution.
- GigaKOM engineers obey all traffic, travel, and safety regulations.

GigaKOM shall not be responsible for service or Service Level Agreement degradation delays due to the lack of client compliance with the above items.



8 Pricing

THIS SECTION IS PROPRIETARY AND CONFIDENTIAL

- Pricing is based on volume pricing and any changes may result in price change and additional shipping charges
- Project performance and payment bond might not be included in the price, if requested they will be added as a line item on the total awarded amount
- GigaKOM recommends at least 10% contingency for project for any unforeseen add, move and changes
- GigaKOM recommends at least 25% contingency for possible China tariff charges

GIGAKOM
 3615 Kearny Villa Road, Suite 201
 San Diego, CA 92123
 Phone: 818-588-5188 Fax: 858-565-2443

D9053WA - E22 - Aruba
 Network Equipment

Number: **2468**

Date: **03/20/2019**

Item #	Mfr. Part	Description	Price	Qty.	Extended
1	5PX1500IRT	Eaton UPS 1500 VA	\$ 724.74	1	\$ 724.74
2	SR42UBEXPND	Tripplite Rack 42 unit cabinet	\$ 689.97	1	\$ 689.97
3	J9822A	5412R ZL2 SWCH Mfr: Aruba	\$ 2,242.87	1	\$ 2,242.87
4	J9830B#ABA	ARUBA 5400R 2750W POE+ ZL2 PSU	\$ 1,267.50	4	\$ 5,070.00
5	J9986A	24P 10/100/1000BT POE+ V3 ZL2 Mfr: Aruba	\$ 1,755.19	6	\$ 10,531.14
6	J9993A	8PT 1G 10GBE SFP+ V3 ZL2 MOD Mfr: Aruba	\$ 2,340.41	1	\$ 2,340.41
7	J9150D	ARUBA Compatible 10G SFP+ LC SR 300M MMF XCVR Mfr: ENET Components, Inc.	\$ 127.00	4	\$ 508.00
8	J9822A	5412R ZL2 SWCH Mfr: Aruba	\$ 2,242.87	1	\$ 2,242.87
9	J9829A#ABA	5400R 1100W POE+ ZL2 P/S Mfr: Aruba	\$ 602.44	4	\$ 2,409.76
10	J9993A	8PT 1G 10GBE SFP+ V3 ZL2 MOD Mfr: Aruba	\$ 2,340.41	12	\$ 28,084.92
11	J9151E	ARUBA Compatible 10G SFP+ LC LR 10KM SMF XCVR Mfr: ENET Components, Inc.	\$ 361.75	96	\$ 34,728.00
12	JL322A	ARUBA 2930M 48G POE+ 1 SLOT SWCH	\$ 3,091.44	1	\$ 3,091.44

Bill To:
 Fernando Delgado
 El Camino Real Charter High School
 5440 VALLEY CIRCLE BLVD
 WOODLAND HILLS, CA 91367
 Phone: (818)595-7500
 Email: erate@ecrchs.net

Ship To:
 Fernando Delgado
 El Camino Real Charter High School
 5440 VALLEY CIRCLE BLVD
 WOODLAND HILLS, CA 91367
 Phone: (818)595-7500
 Email: erate@ecrchs.net



GIGAKOM
 3615 Kearny Villa Road, Suite 201
 San Diego, CA 92123
 Phone: 818-588-5188 Fax: 858-565-2443

D9053WA - E22 - Aruba
 Network Equipment

Number: **2468**

Date: **03/20/2019**

13	JL086A#ABA	ARUBA X372 54VDC 680W PS	\$ 313.23	2	\$ 626.46
14	JL083A	ARUBA 3810M 2930M 4SFP+ MOD	\$ 617.15	1	\$ 617.15
15	J9150D	ARUBA Compatible 10G SFP+ LC SR 300M MMF XCVR Mfr: ENET Components, Inc.	\$ 127.00	4	\$ 508.00
16	J9151E	ARUBA Compatible 10G SFP+ LC LR 10KM SMF XCVR Mfr: ENET Components, Inc.	\$ 361.75	4	\$ 1,447.00
17	JW321A	ARUBA IAP-324 US INSTANT 4X4:4 11AC AP	\$ 683.81	1	\$ 683.81
18	JW001A	ARUBA AP-ANT-13B 2.4/5G 4/3DBI OMNI	\$ 68.98	1	\$ 68.98
*19	Cabling (indoor)	#01 Installation of 1 CAT6 indoor cable runs. THIS ESTIMATE IS BASED ON 24 CABLE RUNS #02 Includes no 48 port CAT6 patch panels, 1 CAT6 24 port patch panels #03 Raceway excluded or provided by customer #04 Cable testing labeling per client requirements (excludes IEEE Cable Certification Tests) #05 All CAT6 jacks to be white #06 All CAT6 cable to be CMR or OSP -NON PLENUM. #07 GIGAKOM STANDARD TERMS AND CONDITIONS APPLY #08 #09 Unless listed explicitly included in the associated GigaKOM quote, the following items are hereby excluded in the proposed work: trenching, direct-burial, new conduit, aerial cabling of any kind, core-drilling, installation of access points over 15' high, installation or modification of AC voltage cabling demolition and removal of existing cable, demolition, modification, or removal of existing cabinets, removal of existing electronics, testing and/or certification of existing cable systems, pre-installation RF heat maps, lift rentals, replacement of existing patch cables, and deployment of any end-user devices. #11 This cabling DOES NOT include IDF cabinet/Rack #12 This estimate includes 1 patch cord	\$ 4,342.76	1	\$ 4,342.76
*20	Cabling (outdoor)	#01 Installation of 1 CAT6 outdoor cable. THIS ESTIMATE IS BASED ON A 24 CABLE RUN #02 Includes no 48 port CAT6 patch panels, 1 CAT6 24 port patch panels #03 Raceway excluded or provided by customer #04 Cable testing labeling per client requirements (excludes IEEE Cable Certification Tests) #05 All CAT6 jacks to be white #06 All CAT6 cable to be CMR or OSP -NON PLENUM. #07 GIGAKOM STANDARD TERMS AND	\$ 5,512.50	1	\$ 5,512.50



GIGAKOM
 3615 Kearny Villa Road, Suite 201
 San Diego, CA 92123
 Phone: 818-588-5188 Fax: 858-565-2443

D9053WA - E22 - Aruba
 Network Equipment

Number: **2468**

Date: **03/20/2019**

		<p>CONDITIONS APPLY</p> <p>#08</p> <p>#09 Unless listed explicitly included in the associated GigaKOM quote, the following items are hereby excluded in the proposed work: trenching, direct-burial, new conduit, aerial cabling of any kind, core-drilling, installation of access points over 15' high, installation or modification of AC voltage cabling demolition and removal of existing cable, demolition, modification, or removal of existing cabinets, removal of existing electronics, testing and/or certification of existing cable systems, pre-installation</p> <p>RF heat maps, lift rentals, replacement of existing patch cables, and deployment of any end-user devices.</p> <p>#11 This cabling DOES NOT include IDF cabinet/Rack</p> <p>#12 Includes 1 patch cord</p>			
*21	Installation and configuration	<p>Installation and configuration services cover the following equipment:</p> <p>2x Aruba 5412</p> <p>1x Aruba 2930</p> <p>1x ARUBA IAP-324</p> <p>1x Eaton UPS</p> <p>1x Rack 42u Tripplite</p> <p>All other work not included in QEGP is excluded.</p>	\$ 1,253.81	1	\$ 1,253.81
21 item(s)			Sub-Total		\$ 107,724.59
			Tax @ 9.5%		\$ 9,178.47
			Freight		as applicable
			Total		\$ 116,903.06
(*) Tax exempted Part(s)					

Quote Valid Until: 07/01/2019

Payment Details

Pay by: Cash On Delivery
 Payment Term Due upon Receipt

Shipping and Delivery Details

Shipping via: UPS Ground

Terms and Conditions

- SPIN: 143027209, FCC # 0011991395, Certified Small Business – Micro # 40936,DIR Registration: 1000003984
1. All areas of Hand holes/ maintenance holes and conduit pathways must be provided and accessible at time of work.
 2. Work shall be performed during normal business hours unless specified in the contact SOW. Additional charges for after hour / holiday work might apply
 3. Parking on site shall be provided by client at no cost to GigaKOM.
 4. Client will provide free and clear access to all working areas.
 5. An onsite contact and access must be provided to GigaKOM prior to job site arrival.
 6. Any down time resulting from the lack of access or client required information, equipment is not the responsibility of GigaKOM and is billable.
 7. A \$250 fee will be billed to client for missed appointment, or site not ready for installation.



GIGAKOM
3615 Kearny Villa Road, Suite 201
San Diego, CA 92123
Phone: 818-588-5188 Fax: 858-565-2443

D9053WA - E22 - Aruba
Network Equipment

Number: **2468**

Date: **03/20/2019**

Erate 2019 guidelines:

Cisco CON-SNT-XXX is 81% eligible, Cisco CON-SW is included free of charge

Terms and Conditions: <https://goo.gl/1439PS>

Labor Billing and SLA: <https://goo.gl/AmM4YG>

The price set forth above is a good faith estimate based on the information received through the date of this Estimate and may change based on updated information. Any price changes shall be communicated to customer through a revised Estimate. This Estimate is valid for 30 days from the day of issue. GigaKOM WILL BILL IN PROGRESS INVOICES. HARDWARE AND SOFTWARE WILL BE BILLED UPON ARRIVAL on customer site or at GigaKOM whichever occurs first. Additional training or Professional Services can be provided at our standard rates. Shipping charged may apply to all orders. Shipping Charges are estimates and will be billed at actual amount if higher. Payment Details Past due amounts subject to finance charges* Customer shall reimburse all costs incurred in collecting past due amounts* *See GigaKOM Standard Terms and Conditions.

For Clients that utilize USAC SLD funding, GigaKOM will, based on agreement, invoice SLD for discounted portion. In case SLD denies payment or SLD does not pay within 90 days, Client will be responsible for full amount. Thank you for your business

Prepared by: **Dean Kolesar** Email: **deankolesar@gigakom.com** Phone: **818-588-5188**



9 **Universal Service Program Restrictions and Invoicing**

The Universal Service program has a number of restrictions on the use of the funds in order to collect discounts. The following restrictions are required for the district to receive the discounts on these services.

- Services and / or products will be limited to only those dealing with technical support of telecommunications and internal connections as specified in the latest version of FCC Document CC Docket No. 96—45 Schools and Libraries Eligibility List. Or the latest rules posted on the SLD web site (<http://www.sl.universalservice.org>). Any services and / or products not covered on the eligibility list must be covered under a separate contract and invoice.
- The services and / or products for which support is sought must be the delivery of services to the classrooms or other places of instruction at schools and libraries that meet the statutory definition of an eligible institution. Discounts are not available for internal connections in non-instructional buildings of a school or school district, or in administrative buildings of a library, to the extent that a library system has separate administrative buildings, unless those internal connections are essential for the effective transport of information to an instructional building of a school or to a non-administrative building of a library. 47 C.F.R. § 54.506
- All services / products must be performed / supplied during the respective E-Rate funding year.
- GigaKOM is experienced, competent and complies with all USAC and SLD policies, programs and requirements for invoicing and billing.

10 **Special Notes and Conditions**

Unless otherwise specified within the client bid or RFP, all implementations are based on a single deployment and installation. Additionally, it is assumed that all work and facilities will be done and available during normal working hours. Should multiple deployments be required, or sites and facilities not be available, additional fees may be applied.

GENERAL EXCLUSIONS

- Unless identified previously within the scope of work, this proposal is not inclusive of fire penetration sleeves, conduit, concrete cores and/or roof penetrations. If required for installation, additional charges will apply.
- Unless identified previously within the scope of work, GigaKOM will install racks in specified locations and in the appropriate manner. Additional charges will apply if the location is not structurally compliant with the installation requested and facilities work is needed.
- Unless identified previously within the scope of work, all existing conduit is expected to be free and clear of debris with an appropriate pull string provided. Additional charges will apply for debris removal or the fishing of conduit.
- Unless identified previously within the scope of work, this proposal is not inclusive of the removal and replacement of furniture during the installation, additional charges will apply, if necessary.
- Unless identified previously within the scope of work, this proposal is based upon normal working hours and does not include weekend or overtime. If weekend or overtime hours are required for this project, additional charges will apply.
- Unless identified previously within the scope of work, this proposal is not inclusive of a Lift rental. If a Lift is required, additional charges will apply.
- Unless identified previously within the scope of work, this proposal is not inclusive of additional labor time required for clean room environments. If clean room environments require special clothing, cleaning of tools, etc, additional charges will apply.



- Unless identified previously within the scope of work, this proposal is not inclusive of installing horizontal cable in a “sequential-by-building” fashion. If a “sequential-by-building” installation is required, this must be identified prior to cable installation and will require additional charges.
- Unless identified previously within the scope of work, this proposal is not inclusive of any voice or data cross-connects and/or patch cord installation. If cross-connects and/or patch cords are to be installed by GigaKOM, additional charges will apply.
- Unless identified previously within the scope of work, this proposal is not inclusive of any and all plywood backboards within each closet. If plywood backboards are required, additional charges will apply.
- Unless identified previously within the scope of work, cost associated with parking is not included within this proposal. If parking fees are required during the installation, additional charges will apply.
- Unless identified previously within the scope of work, cost associated with securing material on site is not included within this proposal. If adequate secured storage is not able to be provided by the Client, additional charges will apply.
- Unless identified previously within the scope of work, this proposal is based upon utilizing onsite trash receptacles for removal of trash debris. If trash receptacles are not made available, additional charges will apply.
- This proposal requires a minimum 2 weeks notice of installation for any and all modular furniture installed during this project. Additional charges may apply if notice of less than 2 weeks is provided.
- Unless identified previously within the scope of work, this proposal is based upon the Client providing all necessary Ring and String or Conduit necessary for each work station location. Additional charges will apply to each location requiring GigaKOM to provide ring and string or conduit.
- Unless identified previously within the scope of work, this proposal is not inclusive of GigaKOM providing temporary power or sanitary facilities. Additional charges will apply if required.
- Unless identified previously within the scope of work, this proposal is not inclusive of removing any and all existing cable or cable supports. Additional charges will apply if required.
- Telephone Vendor will be responsible for labeling any and all patch panels related to voice circuit extensions. GigaKOM will provide said Telephone Vendor with a Cut-Sheet for each cable location.
- A 25% restock fee will be charged for all returned items. Special order items are non-returnable.
- GigaKOM has several blanket endorsements included in its insurance policies. If separate endorsements are required, additional charges may apply.
- Parking on site shall be provided by client at no cost to GigaKOM
- A \$250 fee will be billed to client for missed appointment, or site not ready for installation

Terms and Conditions

GigaKOM STANDARD TERMS AND CONDITIONS:

LABOR PAYMENT TERMS: Invoices shall be submitted weekly. Invoices are due and payable when submitted. A late payment charge of 1-1/2% per month (18% annually) may be applied to amounts outstanding ten days (10) days after the date of the statement.

EQUIPMENT PAYMENT TERMS: All payments are due upon receipt. For new accounts payments in full prior to shipping. Client agrees to pay finance charge on all over due balances.

INTEREST: If payment is not received by GigaKOM within 15 calendar days of the invoice date, the Client shall pay us interest an additional charge of one-and-one-half (1.5) percent (or the maximum allowable by law, whichever is greater) of the PAST DUE amount per month. Payment thereafter shall first be applied to accrued interest and then to the unpaid principal.

TAXES: Prices shown may not include all sales or other taxes imposed on the sale of goods and services. Taxes now or here after imposed upon sales or shipments shall be added to the purchase price. Buyer agrees to reimburse Seller for any such tax or provide Seller with acceptable tax exemption.

COLLECTION COSTS: In the event legal action is necessary to enforce the payment provisions of this Agreement, GigaKOM shall be entitled to collect from the Client any judgment or settlement sums due, reasonable attorneys' fees, court costs and expenses incurred by GigaKOM in connection therewith and, in addition, the reasonable value of GigaKOM time and expenses spent in connection with such collection action, computed at GigaKOM prevailing fee schedule and expense policies.

SUSPENSION OF SERVICES: If the Client fails to make payments when due or otherwise is in breach of this Agreement, GigaKOM may suspend performance of services upon five (5) calendar days notice to the Client. GigaKOM shall have no liability whatsoever to the Client for any costs or damages as a result of such suspension caused by any breach of this Agreement by the Client.

TERMINATION OF SERVICES: If the Client fails to make payment to GigaKOM in accordance with the payment terms herein, this shall constitute a material breach of this Agreement and shall be cause for termination by GigaKOM.



SET-OFF, BACKCHARGES DISCOUNTS: Payment of invoices is in no case subject to unilateral discounting or set-off by the Client, and payment is due regardless of suspension or termination of this Agreement by either party.

RISK OF LOSS OR DAMAGE: GigaKOM shall assume the risk of loss of, or damage to equipment and materials purchased hereunder until a carrier has received the shipment pursuant to a bill of lading (f.o.b. ship point), at which time the client assumes such risk.

MUTUAL INDEMNITY AND INSURANCE: Each party shall be responsible for, and hold the other party harmless from, any loss sustained by such party relating to death, bodily injury, or damage to tangible physical property which is caused by the negligent acts or omissions of that party's agents or employees. GigaKOM shall maintain, at all relevant times hereto, liability insurance coverage for bodily injury, death, and property damage in an amount no less than One Million Dollars (\$1,000,000.00).

BOND: If required, GigaKOM shall furnish Client, in a form satisfactory to Client, full and duly executed Performance and Payment Bonds, underwritten by a surety or sureties satisfactory to the Client, in the amount requested by client. Cost of such bonds to be paid directly by Client.

ARBITRATION: All claims, disputes, and other matters in question arising out of, or relating to, this Contract or the breach thereof, shall be decided by arbitration in accordance with the Commercial Arbitration Rules of the American Arbitration Association, who shall also act as the arbitrators hereto. The award rendered by the arbitrator(s) shall be final, and judgment may be entered upon it in accordance with applicable California law. Notice of the demand for arbitration shall be filed in writing with the other party and with the American Arbitration Association. The demand for arbitration shall be made within a reasonable time after the claim, dispute, or other matter in question has arisen, but in no event shall it be made after substantial completion of the project for which this Contract is awarded. The forum for disputes hereunder shall be at American Arbitration Association in San Diego County, California.

LIABILITY: GigaKOM shall not, in any event be liable to client for incidental, consequential, or special damages claimed, including without limitation, lost business, lost profit or unavailability of all or part of any system.

WARRANTY (Limited): GigaKOM warrants the products installed under this agreement against defects in material and workmanship from a period of one year from project completion. GigaKOM shall repair or replace defective product during the warranty period with new or like new parts. Returned product becomes the property of GigaKOM when replaced. This warranty is void if installed product is abused, misused or altered. This warranty is exclusive and is Client's only remedy. Without limiting the generality of the foregoing limitations and disclaimers, while a system is not designed, sold, or intended to be used to detect, intercept, transmit or record oral or other communications of any kind, GigaKOM cannot control how the system and its components are used and, accordingly, GigaKOM does not warrant or represent, expressly or implicitly, that use of any software, licensed materials derived there from, will comply and conform to the requirements of Federal, State and or Local statutes, ordinances and laws, or that the use of the system will not violate the privacy rights of the third parties. You shall be solely responsible for using the system you the system in full compliance with applicable law and the rights of third parties. Further, regardless of any prior statements, representations, or course of dealings by any GigaKOM representatives, GigaKOM does not warrant or represent, expressly or implicitly, that any software, licensed materials, or use of any of the same will: result in the prevention of crime or hostile enemy action, apprehension or conviction of any perpetrator of any crime, military prosecution of any enemy force, or detection or neutralization of any criminal, combatant or threat; prevent any loss, death, injury, damage to property due to the discharge of a firearm or other weapon; in all cases detect and plot the location of all firearm discharges within the designated coverage area; the supplied network will remain in operation at all times or under all conditions, any and all warranties, express or implied, of fitness for high risk purposes requiring fail safe performance are hereby expressly disclaimed. You and GigaKOM each acknowledge and agree that the software, license materials, and the system are not consumer goods, and are not intended for sale to or use by or for personal, family or household use.

OWNERSHIP: GigaKOM shall retain ownership of all materials supplied until final payment for same is received. GigaKOM may retrieve from the Client's premises any material supplied where payment has not been tendered. The California Commercial Code shall govern this sale and this order shall not be assignable, and shall bind the representative and successors in interest of the parties.

LIENS: Seller may file a lien within 90 days after furnishing labor, materials, or services to a project as long as preliminary lien notice is sent to Buyer under the provisions of the Construction Lien Law of the state where services are rendered. The lien notice is no way intended to reflect the financial stability of the Buyer, but simply advises the Buyer of Seller's rights to file the lien if required.

RETURNS: Credit may be allowed for goods returned with prior approval and a confirmed return authorization form. A deduction will be made from any credit issued to cover the reasonable cost of handling and restocking charges.

DELAYS: Seller is not responsible for delays in delivery or installation occasioned by acts of God or other circumstances over which the Seller has no control.

MISCELLANEOUS: This Agreement constitutes the entire understanding of the parties with respect to the subject matter of this Agreement and merges all prior communications, representations, and agreements. This Agreement may be modified only by a written agreement signed by the parties. If any provision of this Agreement is held to be unenforceable for any



reason, such provision shall be reformed only to the extent necessary to make it enforceable. This Agreement shall be construed under the laws of the State of California.

11 References

Below is an abbreviated list of similar support provided to K-12 clients

National School District, National City, CA

Joe Ferris, IT Supervisor, (619) 336-7783, joe.ferris@national.k12.ca.us

- Designed and installation of a central data center at the district office.
- Equipment network upgrade LAN / WLAN District Wide for multiple refresh cycles
- Cabling infrastructure design, installation, modifications and support.
- Network maintenance including hardware warranties, equipment support over multiple years

Calexico Unified School District, Calexico, CA

Eduardo Perez, Director of IT, (760) 768-3888, eduardop@calexico.k12.ca.us

- Designed and installation of a central Data Center at the district office
- Server virtualization and domain services district wide
- Entire Network upgrade LAN / WLAN including over multiple refresh cycles
- Cabling infrastructure design, installation, modifications and support.
- Network maintenance including hardware warranties, equipment support over multiple years
- IP Video Surveillance design and Installation

San Pasqual Valley Unified School District, Winterhaven, CA

Kish Curtis, Business Director, (760) 572-2222 x2092, kcurtis@spvusd.org

- District-wide Cisco Hosted VoIP HCS VOIP Deployment
- Entire Network LAN /WLAN upgrade including over multiple refresh cycles
- Server virtualization and domain services district wide
- Cabling infrastructure design, installation, modifications and support.
- Network maintenance including hardware warranties, equipment support over multiple years

Arts in Action Charter, Los Angeles, CA

Stephanie Conde, Director, (323) 266-4371, stephaniec@artsinactioncharter.org

- Entire Network upgrade LAN / WLAN
- Cabling infrastructure design, installation, modifications and support
- Network maintenance including hardware warranties, equipment support over multiple years

Merced County Office of Education, Merced, CA

Dick Chai, Network Manager, (209) 381-6699, DChai@mcoe.org

- Network upgrade and warranty over multiple years County wide
- Support for multiple agencies

Mountain View School District, El Monte, CA

Andres Antilles, IT Support Services, +1 (626) 652-4027, aantilles@mtview.k12.ca.us

- District-wide hosted VOIP Cisco HCS Hosted VoIP deployment- over 1200+ seats
- Entire Network upgrade LAN / WLAN including over multiple refresh cycles



- Network maintenance including hardware warranties, equipment support over multiple years

Aspire Schools, Oakland, CA

John Hicks, IT Manager, (510) 434-5509, John.Hicks@aspirepublicschools.org

- Cabling infrastructure design, installation, modifications and support state wide locations
- Network upgrade LAN / WLAN

Alameda Unified School District, Alameda, CA

Rob van Herk, Director IT, (510) 337-7000 x77140 , rvanherk@alamedaunified.org

- Cabling infrastructure design, installation, modifications and support.
- Network Equipment Refresh and Installation District Wide

SIATech, San Diego, CA

Mark Kiker, CTO , (760) 631-3421, Mark.Kiker@siatech.org

- Network Equipment Refresh and Installation over multiple stet sites
- Network maintenance including hardware warranties

Orange Unified School District, Orange, CA

Tam Huyen, Director IT, (714) 628-4550 , tam.nguyen@orangeusd.org

- Network Equipment Refresh and Installation District Wide

Santa Maria Joint Union High School District, Santa Maria, CA

Lazaro Sanchez, IT Services, (805) 922-4573 , lsanchez@smjuhsd.org

- Network Equipment Refresh and Installation District Wide

Imperial County Office of Education , Imperial, CA

Luis Wong, CTO, (760) 312-6464, luis.wong@k12hsn.org

- Equipment network upgrade LAN / WLAN District Wide for multiple refresh cycles
- Cabling infrastructure design, installation, modifications and support

St John the Baptist School, El Cerrito, CA

Chad Zullinger, Assistant Principal, (510) 234-2244 x2255, czullinger@csdo.org

- Equipment network upgrade LAN / WLAN District Wide for multiple refresh cycles
- Cabling infrastructure design, installation, modifications and support
- IP Video Surveillance design and Installation



National School District
1500 N Avenue National City, CA. 91950

August 7th, 2018

Andrej Komatina
GigaKOM
3615 Kearny Villa Road
Suite 201
San Diego, CA. 92123

Dear Andrej Komatina,

On behalf of the National School District, we would like to take this opportunity to thank you and your entire staff for the excellent job you have done in providing support for our Cisco products through your CareKOM maintenance program and MonKOM network monitoring solution.

Your project managers and engineers have worked tirelessly to provide our students and staff with a solution that meets our immediate needs and will also grow with our future requirements. Your response times have been stellar and the GigaKOM team has always exhibited consistent, excellent customer service over the years. Greg Argendeli, Sasha Krstich and the rest of your team are extremely knowledgeable and always a pleasure to work with.

Thank you again for the professionalism and the expertise you have brought to our district, staff and students. You have proved to be a valuable partner to the National School District and we look forward to many more successful years in partnership.

Sincerely,

Joe Ferris

NSD Technology Services Supervisor



August 7, 2018

The Calexico Unified School District would like to thank you for the service you provided on the Aerohive Access Points project. The district-wide project was successful and completed within a timely manner. GIGAKOM was responsive throughout the project. Employees were always extremely professional in their communications with the district.

GIGAKOM has done a very good job and I would be happy to recommend your services to other organizations.

Thank you.

Eduardo Perez



From: Lazaro Sanchez
Date: August 29, 2018

GigaKOM was an excellent company to team up with, our school district had a strict requirement for e-rate purchases. GigaKOM's sales team understood our needs and went above and beyond to acquire our core equipment. GigaKom's install team composed of Chi and Sasha was greatly balanced. Their work was energizing and they were extremely motivated, personally committed to the job. During their three-day stint at SMJUHS they worked long hours and made strides every day. Working with their team was an optimal experience, their dedication and promptness was refreshing. They were very knowledgeable in their field and able to conform to our needs. Thank you guys!

Thanks,

Lazaro Sanchez
Computer Network Tech II

[Service](#)

[Request](#) help@smjuhsd.org

Santa Maria Joint Union High School District • 2560 Skyway Dr. • Santa Maria • 93454 • CA



12 Appendices

- Contractor's License
- Summary of Insurance
- Small Business Certification
- CMAS Contracts -details at <https://goo.gl/XaDLCC>
- FCC Green Light Status
- SPAC 2019



Contractor's License Detail for License # 910431

⚠ **DISCLAIMER:** A license status check provides information taken from the CSLB license database. Before relying on this information, you should be aware of the following limitations. [\(hide/show disclaimer\)](#)

- CSLB complaint disclosure is restricted by law ([B&P 7124.6](#)) If this entity is subject to public complaint disclosure, a link for complaint disclosure will appear below. Click on the link or button to obtain complaint and/or legal action information.
- Per [B&P 7071.17](#) , only construction related civil judgments reported to the CSLB are disclosed.
- Arbitrations are not listed unless the contractor fails to comply with the terms of the arbitration.
- Due to workload, there may be relevant information that has not yet been entered onto the Board's license database.

Business Information

GIGAKOM
 3615 KEARNY VILLA ROAD_201
 SAN DIEGO, CA 92123
 Business Phone Number:(858) 769-5408

Entity Corporation
Issue Date 02/08/2008
Expire Date 02/29/2020

License Status

This license is current and active.
All information below should be reviewed.

Classifications

C-7 - LOW VOLTAGE SYSTEMS



Supplier Profile



State of California Certification

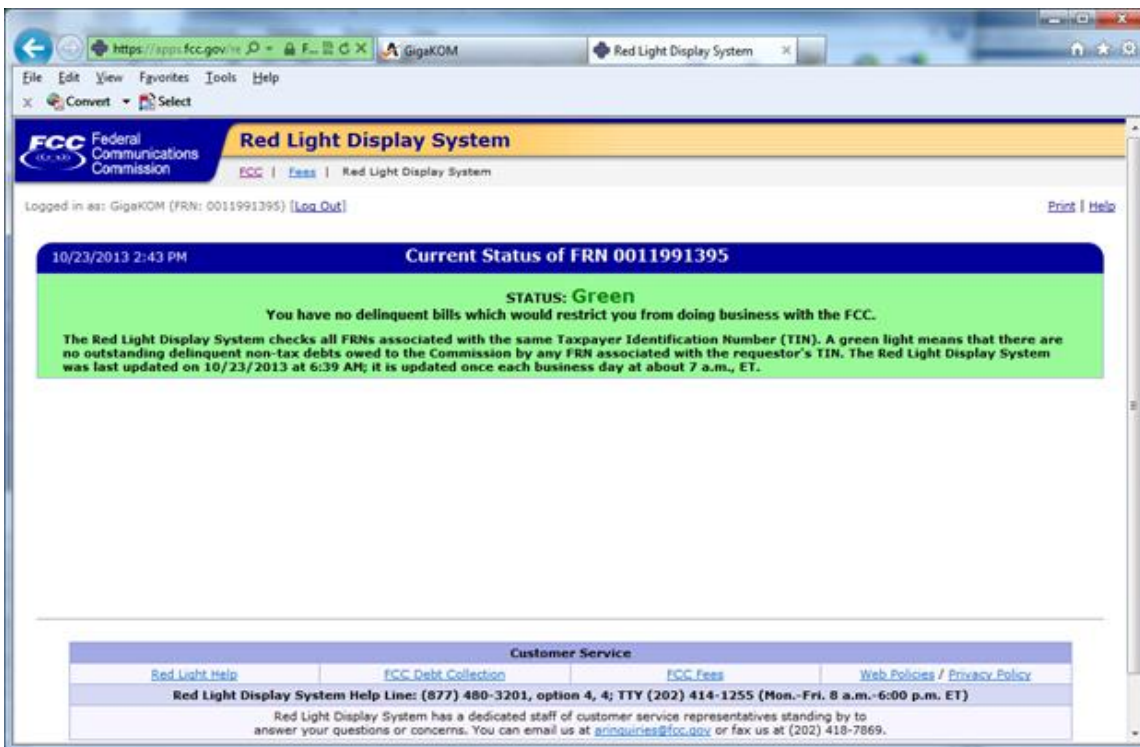
Certification ID : 40936

<p>Legal Business Name GIGAKOM</p> <p>Doing Business As (DBA) Name1 GIGAKOM</p> <p>Doing Business As (DBA) Name2</p> <p>Office Phone Number 858/769-5408</p> <p>Business Fax Number 858/769-5408</p> <p>Business Web Address</p>	<p>Address 3615 Kearny Villa Road Suite 201 SAN DIEGO CA 92123</p> <p>Email: govplace@gigakom.com</p> <p>Total No. of Employees 12</p> <p>Business Types Service</p> <p>Notification Preference Email</p> <p>Service Areas Alameda , Alpine , Amador , Butte , Calaveras , Colusa , Contra Costa , Del Norte , El Dorado , Fresno , Glenn , Humboldt , Imperial , Inyo , Kern , Kings , Lake , Lassen , Los Angeles , Madera , Marin , Mariposa , Mendocino , Merced , Modoc , Mono , Monterey , Napa , Nevada , Orange , Placer , Plumas , Riverside , Sacramento , San Benito , San Bernardino , San Diego , San Francisco , San Joaquin , San Luis Obispo , San Mateo , Santa Barbara , Santa Clara , Santa Cruz , Shasta , Sierra , Siskiyou , Solano , Sonoma , Stanislaus , Sutter , Tehama , Trinity , Tulare , Tuolumne , Ventura , Yolo , Yuba</p>
--	--

View Keywords

View Classifications

Active Certifications ?			
Certification Type	Status	From	To
SB	Approved	08/15/2018	08/31/2020



OMB Control No. 3060 - 0856

FCC Form 473

Do not write in this space.

Approval by OMB
OMB Control No. 3060 - 0856
Estimated time per response: 1.0 hours

Please read instructions before completing. Universal Service for Schools and Libraries
Service Provider Annual Certification Form
(To be completed by Service Provider)

Block 1: Service Provider Information

1. Service Provider Name GIGAKOM	
2. Service Provider Identification Number (SPIN) 143027209	3. Funding Year: July 1, 2019 through June 30, 2020
4. Contact Name Andrej S Komatina	
5. Complete Mailing Address of Contact Person Street Address, P.O. Box or Route Number 4364 Bonita Rd. No.494	
Bonita	CA 91902

Omicron Technologies LLC

543 Edgemont Ave, Lansdale PA 19446-1909
 SPIN 143027415

**FY 2019 CUSTOMIZABLE
 INTERNAL CONNECTIONS PROPOSAL**

Date:	2/23/19
Entity:	
BEN:	
Service Location:	
470 Number:	
Allowable Contract Date:	

Please find unit pricing for all of our offerings below. To obtain your complete proposal amount, simply modify your e-rate discount percentage and the quantity for any desired items in the highlighted fields, and the spreadsheet will calculate all dollar amounts. Please email if you require any other eligible items that are not listed below.

SUMMARY:

Total Proposal Amount:	\$ -	School Share:	\$ -
E-Rate Discount Percentage:	85%	E-Rate Share:	\$ -

DETAILS:

DEVICE TYPE	Brand	Model	Specifications	Unit Price	Quantity	Extended Price
Switches	Netgear	GSM7224P	24 port Gigabit Layer 2 POE+ w/4xshared SFP	\$ 819.99		\$ -
	Netgear	GSM728TTP V2	24 port Gigabit Layer 3 POE+ w/4xGigabit SFP	\$ 629.99		\$ -
	Netgear	GS752TP V2	48 port Gigabit Layer 3 POE+ (380W) with 4xGigabit SFP	\$ 759.99		\$ -
	Netgear	GS748T	48 port Gigabit Layer 3 (no POE) with 2xGigabit SFP and 2xcombo Gigabit SFP	\$ 509.99		\$ -
	Ubiquiti	ES-24-500W	24 port Gigabit Layer 3 POE+ (500W) w/2xGigabit SFP	\$ 899.99		\$ -
	Ubiquiti	ES-24-LITE	24-port Gigabit Layer 3 (no POE) w/2xGigabit SFP	\$ 329.99		\$ -
	Ubiquiti	ES-48-500W	48 port Gigabit Layer3 POE+ (500W) w/2x10Gb SFP+ and 2xSFP	\$ 1,259.99		\$ -
	Ubiquiti	ES-48-LITE	48-port Gigabit Layer 3 (no POE) w/2x10Gb SFP+ and 2xSFP	\$ 639.99		\$ -
	Extreme	7124T	24 port 1Gb/10Gb Ethernet RJ-45 + 4xQSFP+	\$ 22,399.99		\$ -
	Extreme	220-24P-10GE2	24 port Gigabit Layer 3 POE+ (185W) + 2x10Gb SFP+	\$ 1,329.99		\$ -
	Extreme	220-24T-10GE2	24 port Gigabit Layer 3 (no POE) + 2x10GbSFP+	\$ 999.99		\$ -
	Extreme	7148	48 port 1Gb/10Gb Ethernet RJ-45 + 4xQSFP+	\$ 27,699.99		\$ -
Extreme	220-48P-10GE4	48 port Gigabit Layer 3 POE+ (370W) + 4x10Gb SFP+	\$ 1,999.99		\$ -	
Extreme	220-48T-10GE4	48 port Gigabit Layer 3 (no POE) w/4x10GbSFP+	\$ 1,599.99		\$ -	
Wireless	Netgear	WAC510	GigE 802.11ac Wave 2 Dual Band	\$ 97.99		\$ -
	Netgear	WAC740	4x4 Dual Band Wireless-AC	\$ 754.99		\$ -
	Netgear	WC7600	Wireless Controller for 50 access points, 10GbE, 1U	\$ 2,499.99		\$ -
	Ubiquiti	UAP-AC-LR-US	802.11ac Long Range	\$ 229.99		\$ -
	Ubiquiti	UAP-AC-HD-US	802.11ac Wave 2 Dual Band	\$ 509.99		\$ -
	Extreme	AP3935E	Enterprise-Class Dual Band/Dual Radio 802.11ac/a/b/g/n Indoor	\$ 1,039.99		\$ -
	Extreme	AP3965E	Enterprise-Class Dual Band/Dual Radio 802.11ac/a/b/g/n Outdoor	\$ 2,239.99		\$ -
Extreme	CS210	Wireless Controller for 100 managed access points, 10GbE, 1U	\$ 21,629.99		\$ -	
Firewalls	Juniper	SRX340	Security Appliance, 16 port, GigE	\$ 1,625.99		\$ -
	Sonicwall	TZ500	Security Appliance, 8 port, GigE	\$ 1,659.99		\$ -
	Barracuda	BNGF180A-TP3	Next generation firewall/security appliance	\$ 1,744.99		\$ -
	Watchguard	M370	150 user small/medium site, 8x1Gb ports 1U, 3yr	\$ 5,999.99		\$ -
	Watchguard	M470	450 user small/medium site, 8x1Gb ports 1U, 3yr	\$ 6,999.99		\$ -
	Watchguard	M570	600 user medium site, 8x1Gb ports 1U, 3yr	\$ 9,999.99		\$ -
	Watchguard	M670	850 user medium site, 8x1Gb ports 1U, 3yr	\$ 14,999.99		\$ -
	Watchguard	M4600	1,500 user enterprise site, 8x1Gb ports, 1U, 3yr	\$ 22,999.99		\$ -
Watchguard	M5600	HQ firewall for distributed enterprise, 8x1Gb ports, 4x10Gb fiber, 1U, 3yr	\$ 59,999.99		\$ -	
Racks	StarTech	RK2236BKF	22U 36" server cabinet with casters	\$ 719.99		\$ -
	StarTech	RK2536BKF	25U 36" server cabinet with casters	\$ 779.99		\$ -
	StarTech	7236CABINET	41U cabinet, 22" width, 27.6" depth, built in fans, solid steel	\$ 1,359.99		\$ -
	StarTech	4POSTRACKBK	42U adjustable 4 post open frame rack	\$ 379.99		\$ -
	StarTech	RK4242BK24	42U cabinet, 24" width, adjustable depth, solid steel	\$ 989.99		\$ -
	StarTech	RK4242BK30	42U cabinet, 30" width, 37" depth, solid steel	\$ 1,334.99		\$ -
UPS	APC	SC450RM1U	450VA 120V 1U	\$ 169.99		\$ -
	APC	SMT1500RM2UC	1440VA AC 120V 2U	\$ 1,369.99		\$ -
	APC	SMX2200RMLVUS	2200VA AC 120V 2U	\$ 1,519.99		\$ -
	APC	SYRMXR4B4	4x lead acid batteries, AC 200/208V 4U	\$ 4,019.99		\$ -
	HPE	AF462A	7200VA AC 200/208V 4U	\$ 4,199.99		\$ -

All pricing is subject to final confirmation at time of order. If you require on-site installation, check this checkbox:
 To accept this proposal, return a completed copy via email to charles@omicrontechnologies.net
 A final contract that includes any shipping or installation costs will then be forwarded to you.

On-Site Installation