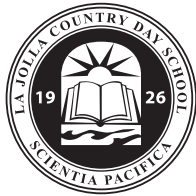


LA JOLLA COUNTRY DAY SCHOOL

College-Preparatory Chooses Aruba for Secure Network Access



Like many campus networks today, La Jolla Country Day School (LJCDS) has seen the usage of its wireless network explode over the past few years. In fact, it wasn't long ago that only a small percent of the school's users wanted wireless connectivity.

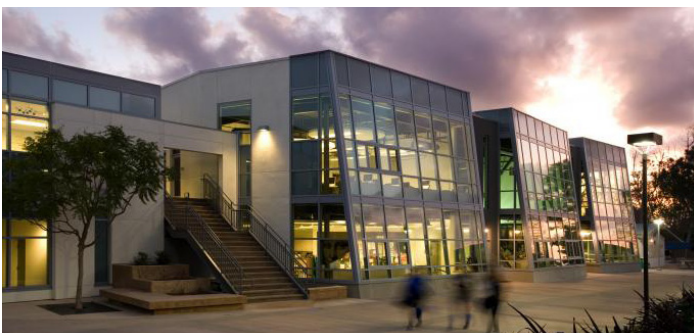
But now because of the growing number of laptops and smart devices on campus, wireless access is considered a must have. These new demands to support bring-your-own-device (BYOD) initiatives, and the versatility of devices meant coming up with a new wireless access and security plan.

LJCDS' original wireless infrastructure was setup for one service-set identifier (SSID) for faculty and staff to access to specific campus resources, and an open SSID for guests that allowed those users to reach the Internet.

It didn't take long for the faculty and staff SSID to become public knowledge, which meant that unknown users were connecting to the campus network. Because the original wireless solution was in need of an upgrade, it was the perfect opportunity to upgrade their infrastructure, while also adding advanced authentication capabilities.

The goal for the LJCDS IT team was to install a new controller-based wireless infrastructure and separate components with proven interoperability to provide the following services:

- Role-based user authentication
- Intuitive, identity-aware policy management
- Advanced AAA/RADIUS functionality
- Network access control (NAC) for endpoint health checks
- And, the ability to capture comprehensive user and device information



CHALLENGE

- Offer wireless access with advanced security.
- Create user-based policies.
- Dynamically support **bring-your-own-device** initiative.

SOLUTION

- Aruba ClearPass Policy Manager™.
- Role- and device-based policy management.
- Integrated RADIUS, context- based policy rules engine and reporting.

RESULTS

- Interoperability with Active Directory, NAC and existing switches from multiple vendors.
- Flexible user and device differentiation for any user role and any device.
- Cost savings through increased efficiency in user community and IT tasks.

IMPROVING CAMPUS-WIDE WLAN SECURITY

Because the existing Brocade wireless solution was not controller-based, it required someone to manually touch each of the 85 access points (APs) on campus every time an SSID needed to be changed. As a result, the IT team first set out to find a new wireless solution.

To address this and other management issues associated with the old solution, a new Aruba Networks controller-based solution with APs was chosen and deployed. The next step was to identify NAC and RADIUS solutions that worked with Aruba and also met usability and cost requirements.

"None of the vendors we initially looked at worked for us," said Gabe Gador, senior network and systems engineer at LJCDS. "For example, we looked at Bradford Networks, but the cost was ridiculous and it didn't include RADIUS. Another vendor wanted us to put a device in every closet which was overkill. So we reached out to our Aruba sales team for some help."

On the advice of the Aruba team they visited other local Aruba customers to see what they were using for NAC and AAA services. During their visits, LJCDS found that the University of San Diego (USD) had effectively accomplished what they had in mind. After finding what they needed, LJCDS hired a local consultant to model the USD deployment for their network and put the plan in place.



The next step involved contacting the NAC vendor for the solution that was in place at UCD and implementing that component at LJCDS. After that it was on to finding the right AAA solution. Microsoft's RADIUS solution was looked at, but the feeling was that it was cobbled together.

LJCDS also looked at Juniper's SBR FreeRADIUS offering, but felt that it wasn't very free at all. So, IT officials took the lead from USD and looked at the solution from Aruba to satisfy role-based policy management and RADIUS requirements.

"Input from USD was that the Aruba ClearPass Policy Manager™ was full-featured and intuitive, and that their support was top notch," said Gador. "They were right. The Aruba platform is extremely useful when it comes to authentication and role-based assignments, and it seamlessly worked with our Aruba controllers, HP and Brocade switches, NAC solution and active directory server."

Aruba's built-in policy engine, RADIUS server, visibility features, and troubleshooting tools provide the necessary post-deployment support features needed to streamline management processes.

ROLE-BASED WIRELESS ACCESS POLICIES

Role-based wireless access policies, which take advantage of 802.1X and RADIUS for authentication and authorization, are created on Aruba's ClearPass Policy Manager. When a student is identified during the authentication process, they are assigned appropriate network access.

When a teacher or staff member is identified, they receive broader access to resources within the network. A separate web filter component also leverages Aruba's role-based differentiation which is defined to restrict access to unwanted Internet sites.

One major advantage in the new model is that the authentication process works regardless of device type, which is very important as students, faculty, staff and guests are allowed to use personal devices, and some prefer Microsoft and some prefer Apple.

"Because each new component was purchased separately, we later found out that Aruba's built-in NAC component would have provided all of the functionality we really needed, and at a cost savings," commented Gador. "Even with just the policy engine and RADIUS features, the Aruba platform is a better investment than the standalone NAC solution that was chosen."

ENHANCED ACCESS TO EDUCATIONAL RESOURCES

With students expectations set for the ability to use their own Windows laptops, MacBooks, and iPads, IT officials added Active Directory accounts for all students in grades 9-12 to support BYOD. This captures user authentication data needed to gain wireless visibility into users' habits, such as where they're connecting and the health of their devices.

"Aruba ClearPass just works as expected, it has a good solid interface, and it is very visual – which is great because we did not want to add complexity," said Gador. "LJCDS has a small IT staff that touches so many devices and is responsible for so many things, that it's great to easily find the exact information you need to solve authentication questions."

"The ClearPass Policy Manager solution is very intuitive when compared to others, and eliminates having to re-read the entire manual to get up to speed," he added.

Based on the outcome of the program, the plan is to then roll out access to everyone from middle school to grade 12. Overall success will come when the staff, students, and others are each accounted for, happy, and the IT team is on to the next project.

LA JOLLA COUNTRY DAY SCHOOL

La Jolla Country Day School is an independent college-preparatory school serving 1,050 students from age 3 through Grade 12.

LJCDS is accredited by the California Association of Independent Schools (CAIS) and the Western Association of Schools and Colleges (WASC). In addition, the school is a member of the National Association of Independent Schools (NAIS) and the Council for the Advancement and Support of Education (CASE).



www.arubanetworks.com

1344 Crossman Avenue, Sunnyvale, CA 94089
1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com