ONLINE REPORT SPONSORED BY:

aruba
a Hewlett Packard
Enterprise company

CAMPUS TECHNOLOGY

SNAPSHOT: THE CONNECTED CAMPUS

GOING BEYOND WIRELESS TO ENSURE CAMPUS SUCCESS.

INSIDE

NETWORK SMARTS CAN ENSURE SMOOTH OPERATIONS

Supporting a mobile-first campus doesn't have to be an IT burden.

From lecture halls to residence halls, student centers to stadiums, today's students expect a consumer-like, always-on network experience, anywhere and anytime. These high expectations greatly increase the burden on IT to keep the network responsive and secure.

The proliferation of all sorts of mobile and IoT devices is increasing the number of connections on a campus, yet there is little corresponding increase in budgets. IT is expected to do much more with less. That means simplicity and ease-of use is a top priority for IT. Innovations in wired network infrastructure can make the job of the network manager far easier. Here are three key features to look for when considering a campus network upgrade.

Automation: When a new device connects to the network or when students walk across campus carrying a connected device, network technology should proactively ensure they remain connected to the best access point—instead of waiting on a weak signal, an over burdened access point, or on helpdesk intervention. Using machine learning, network software automates network tuning to ensure the absolute best performance even in dense environments. A smart network can also ensure everyone stays connected even if a controller fails.

Simplicity: To provide simple and secure access for mobile and IoT devices, every user on the network must be identified, profiled, secured, and monitored. To simplify this process and avoid involving the helpdesk, look for software that automates connectivity and monitors ongoing security of new devices constantly connecting to the network.

Visibility: Dashboards can provide granular visibility into both wired and wireless networks. Look for dashboards designed to monitor both the wired and wireless networks, not one or the other. Dashboards should help IT managers proactively watch the network for the health and performance of all connected devices, and provide quick insights into potential issues and performance concerns. ●

Checklist: Get Wired for Mobility and IoT with a Mobile First Switch

Look for advanced switch technology that allows for switch placement at the network core or access level that can:

- Dynamically segment traffic (for a better user experience and security) based on user and device
- Allow management by many of the same tools that manage the wireless network (thereby simplifying IT operations)
- Provide real-time analytics to detect and resolve issues before users are aware of a problem
- Leverage older cabling, but still support faster speeds
- Provide bandwidth and Help to manage large research data sets over the campus network
- Enhance network functions (like supporting voice and video traffic) while assisting with policy enforcement
- Dynamically prioritize Quality of Service (QoS) and PoE for optimal wireless AP performance.
- Automate for simplified deployment and provisioning of devices

As a whole, look for capabilities that significantly improve data traffic visibility and manageability, while reducing the burden on IT. Look for solutions that can lead to faster problem detection, diagnosis, resolution, and and administration, translate to fewer complaints and rock-solid connectivity.

SWITCH INTELLIGENCE IS THE NEW WIRELESS SECURITY TOOL!

Improve device and user security with intelligent switches, network insights, and analytics

With an average of 80 percent of network traffic coming from wireless devices, it's easy to focus on the wireless aspects of the network when dealing with security issues. However, every wireless communication must pass through a port on a wired switch—meaning threat detection and mitigation is also very much a part of the wired network.

Traditional security perimeters are no longer enough, so higher education institutions are adopting new approaches to keeping their networks secure. They still use typical network edge protections—such as passwords and firewalls—but now include more sophisticated solutions as well.

Network visibility and security starts with a well thought out set of network management policies is a critical part of managing users and devices. A secure campus network should include networking management software that provides adaptable, flexible policy management for monitoring all of the campus's users—students, faculty, staff, and guests.

With the switch port as the traffic cop of so many mobile and IoT devices, switch security must be a part of network planning. By leveraging security management and authentication tools that work in conjunction with switches to dynamically segment device and user traffic on the network, network administrators can be assured that the network is helping to keep traffic separate, and therefore, improving security.

Finally, user and entity behavior analytics (UEBA) helps network managers use analytics to detect potential illicit behavior earlier and intervene more quickly. Sophisticated software uses advanced machine learning and UEBA to detect and prevent attacks. Using both supervised and unsupervised machine learning models, software can monitor user and device behavior. It can then automatically and immediately alert network managers to attacks that have evaded more traditional perimeter defenses. ●

Security Remains Top of Mind

Information security remains at the top of the list of IT issues in higher education, according to an annual survey from Educause. In 2017, security again took the top spot for the third year in a row in the report "Top 10 IT Issues and Strategic Technologies for 2018." Educause creates the list through a series of discussions with two dozen IT leaders from a variety of educational institutions. The group presents a list of topics, then the entire Educause membership votes. The results are the top 10 issues with which educators are most concerned.

The report states information security is defined as "developing a risk-based security strategy that keeps pace with security threats and challenges."

Other studies on network security confirm education administrators have good reason for concern. For example, reflecting the effect of the Internet of Things (IoT) on security concerns everywhere, not just on college campuses, a 2017 report from ISACA (an independent association focused on providing best practices for information systems professionals) reported the IoT has now surpassed mobile as a potential avenue for cyberattacks.

The report surveyed IT security leaders worldwide and found a whopping 97 percent of respondents have seen IoT usage rise over the past year. "As IoT becomes more prevalent in organization, cybersecurity professionals need to ensure protocols are in place to safeguard new threat entry points," says the ISACA. That certainly points to the need for better wired and wireless security awareness and protocols on campus.

CAMPUS NETWORKS HANDLE BIG RESEARCH DATA

Universities must be able to support scientific studies and process large data volumes.

University researchers often need to move massive amounts of data between the campus and the cloud or across different research institutions. The data volumes can be huge, amounting to petabytes of information crucial for scientific collaboration. These data volumes can choke a standard network.

In the past, universities have set up special "science networks," separate from the campus network, to handle that massive traffic. With that approach, a "science DMZ" is built near the campus perimeter and optimized for high-performance scientific applications and data transfer.

Researchers' desktops, servers, and data services are isolated within this special high-speed zone. However, having a separate network just for research introduces its own problems, since enforcing network policies, including security, can be spotty.

Institutions like the University of Kentucky are taking a fresh approach. With cutting-edge network technology, they're using advanced switch technologies to enable scientific data to reside on the campus network. Now researchers can stay on the campus network but also take a high-speed path through it and to the cloud. The switches act as normal switches, but enable software rules for research data when necessary.

There are several advantages to this approach. First, the research portion of the network becomes part of the university network, with the "science DMZ" subject to standard network policies and security constraints. It also creates a secure data pathway for research that moves data many times faster than previously.

The University of Kentucky, using these high-performance switches has smashed performance bottlenecks. A massive transfer that would have taken a month to complete can now be done in less than eight hours. ●

University of Kentucky Moves Data with Ease

In order to move massive data loads to the cloud and to other research universities, the University of Kentucky has created an SDN-enabled campus network. With more than 30,000 students, faculty, and staff, the university needed a solution that wouldn't impact network performance. They also needed to keep the research network as part of the university's overall network. This setup facilitates big data set transfer across campus and to the cloud, without affecting regular network traffic. And the research network lies within the standard network, so the university can consistently enforce security policies.

The university does all this with the Aruba 5400R switch series, a high-performance, low latency Advanced Layer 3 modular switch from Aruba. Using industry-standard OpenFlow and SDN technologies, the research network has been extended all the way to the switch port on the 5400R switch located in a researcher's office or building. Ordinary traffic moves through the 5400R switches in "normal" mode, while scientific flows from researchers are diverted to take a high-bandwidth path.

"The 5400R switch was one of the few switches we tested that implemented the OpenFlow NORMAL rule, allowing SDN switches to act as normal switches until an SDN rule was applied," says Lowell Pike, director of research computing at the university. Now besides keeping the science network secure and manageable, big data transfers between campus and research sites on Internet2 are now an astounding 88 times faster.

EASILY SECURE IOT AND USER DEVICES

Separating network traffic by category is helpful as the variety and volume of devices grows.

The Internet of Things (IoT) provides many benefits to a smart campus, including network control of items such as smart lights, HVAC systems, door locks, and other building devices. It is no surprise that the world of bring-your-own-device, or BYOD, has heavily impacted campuses as well. Many institutions are also wrestling with support of wearable and personalized devices students expect to connect to the network. All that connectivity benefits colleges and universities as well as the students, but also introduces management and security concerns.

One way to help secure an IoT network is through called Dynamic Segmentation, in which certain traffic is kept separate from normal network traffic. Network administrators, through policy definitions, can define what traffic they want segmented. Traffic could include student, faculty, staff, or guest devices, for example, as well as typically defined IoT network-connected objects such as security cameras, door locks and air conditioning controls.

With Dynamic Segmentation, the port switch no longer needs to be programmed specifically for each device when that device is added to the network. Aruba's operating system AOS 8 with mobility master, Aruba ClearPass policy management, and Aruba switches work together to recognize the device and the access level required. They can then intelligently direct traffic to the correct controller, no matter the switch port through which that traffic is flowing. As known devices plug into the network, no administrator efforts are needed. The port switch is truly colorless as the orchestration for where and how that device is secured and how it's network traffic flows, is already defined. This is a huge time saver for IT staff.

Dynamic Segmentation is specifically designed for cloud, mobile, and IoT requirements, which makes it ideal for college campuses. A policy-based software feature offered by Dynamic Segmentation helps with policy enforcement between the wired and wireless network. It also saves network managers time in managing vast numbers of devices that need network access.●

How Dynamic Segmentation Helps Manage IoT

According to estimates by industry researcher Gartner, there will be 20.4 billion IoT devices connected to enterprise networks by 2020. Campus network administrators can certainly expect the same or an even greater degree of influx of devices onto their campuses. Estimates already suggest individual students now bring multiple personal devices to campus and expect to connect them all to the network. The profile of many – but not all – of these devices is the opposite of traditional wired user access: minimal bandwidth, unmanaged by IT, inability to securely authenticate, and a high requirement for PoE power.

It therefore makes sense to embrace network management technologies that can better control policies and security settings for multiple connections and devices, including a constant influx of new devices. Switches supporting Dynamic Segmentation are one example. Dynamic Segmentation is a technology that allows wired users and wired ports to securely tunnel traffic back to mobility controllers for unified policy enforcement point. Using a unified policy simplifies policy management and ensures consistent access and permissions across both wired and wireless users, and IoT devices. This allows the campus access switch to be a security enforcer by implementing role-based policies at the edge of the network.

ARUBA LEADS IN UNIFIED WIRED AND WIRELESS

Universities and campuses need full network simplicity and scalability

While many may look to Aruba Networks, a Hewlett Packard Enterprise Company, as a leader in the wireless networking space, its line of wired networking products and technologies is equally strong. In fact, as wireless solution development has advanced rapidly over the past 15 years, many innovations were modeled after advances made earlier in wired networking.

Fast forward to today, and Aruba is delivering switch smarts whose innovative value is modeled after what they have learned from the wireless world. As wireless traffic continues to grow, every communication must still pass through a wired switch. Although often overlooked, that fact makes switches the real core of an intelligent and programmable network.

In fact, switches and ports play a more critical role than ever in the wired network structure. Today, switches not only handle more traffic and provide traditional wired connectivity, but also are an important aggregator of wireless access points and connector of IoT devices. And with technologies like IoT and cloud on the rise, the security and stability of the wired and wireless network is more critical than ever. Ports on the switch are more important than ever.

While the past several decades in networking have been defined by static, closed-networking solutions designed for the client-server era, Aruba is changing that. Here are some examples:

- **Aruba 2930M, 2930F switches:** Designed for performance and easy deployment, the 2930s are scalable Layer 3 that offer plenty of PoE+ power, Smart Rate mult-gigabit Ethernet, stacking and open REST APIs. As with the wireless side of the network, Aruba ClearPass Policy Manager and Aruba AirWave let network managers quickly provision and manage the switches.
- **Aruba 3810 switch series:** The 3810 series is an powerful Advanced Layer 3 series with backplane stacking, low latency, and resiliency. The series is a good solution for a highly mobile campus network. Like the 2930M, it supports HPE Smart Rate multi-gigabit Ethernet, making it ready for use with high-speed APs, power users and IoT devices.
- **ArubaOS 8:** A university campus is a highly complex mobile environment that must support thousands of students, faculty, staff, and guests. ArubaOS 8 allows secure central management of complex networks, including Dynamic Segmentation that extends a mobile first architecture to wired ports in the network, providing unified policy and protection. ArubaOS 8 with Mobility Master, gives administrators the ability to quickly scale the network in the face of increased demand for mobile and IoT devices.
- **Aruba AirWave:** With its granular visibility into both wired and wireless networks, AirWave is the only network management platform designed specifically for mobile devices and apps. Offering simplicity and improved workflows, Aruba AirWave can assist with deploying and managing both wireless and wired networks.
- **Aruba NetInsight:** Using predictive analytics against network data, Aruba NetInsight delivers valuable guidance for improving network performance and the mobile experience of users. Its automatic predictive capacity continually collects data on network use and performance, allowing for better network design and management.
- **Aruba ClearPass:** With the convergence of cloud, a rapidly growing number of devices to support, and technologies such as IoT, the network is more important than ever. It's also a greater challenge to support. Aruba ClearPass can help by allowing predefined policies for both wireless and wired devices, that can differentiate users based on role, device, and location. This allows for enforcement of what BYOD devices can onboard the network, regardless of user type, along with which apps they can access, and from what location. ●