

Modernizing Higher Education Network Infrastructures



Executive Overview

Higher education institutions are experiencing tectonic shifts in a new generation of students that are always connected. Smart devices and video streaming have replaced paper, pencil, and chalkboards. Classrooms are hybrid with local and remote attendance. Labs are leveraging on-line resources including research and lab equipment. All administrative activities are e-enabled including registration, course selection, grading, attendance, professor communication, and school news. New applications including wayfinding, security checkpoints, crowdsourcing, artificial intelligence monitoring, and asset tracking are addressing security challenges. Conventional classrooms are being re-designed with video streaming, large screen monitors, flexible furniture, and collaborative workspaces. Universities are in this transition with unknown end states; they must continue to re-invent themselves to stay relevant with this in-line world.

Higher education institutions must modernize their network infrastructures to meet these demands. This modernization involves an ecosystem of network technologies, both wired and wireless, where bandwidth, mobility, location intelligence, endpoint authorization, security mitigation, data privacy, and operation efficiencies are integrated, when considering any type of replacements, upgrades, or new campuses. Integration is the key to success as the combination of Wi-Fi, switching, zero trust security, cloud control, localized dataplanes, and operation automation lead to better long term innovative outcomes.

Network Related Education Needs



New Demands Being Placed on the Network

Below are ten of the more common network demands that higher education institutions are facing.

1. Bring Your Own Devices (BYOD): Different from corporate enterprises where businesses can mandate the endpoints employees are allowed to use, with device certificates (CERT) and 802.1x-based EAP-TLS authentication technologies, over 95% of devices within higher education institutions are unmanaged. The network must accommodate these devices while protecting critical data, blocking hackers, and preventing ransomware attacks.
2. Protecting the Trusted 5%: Specific resources, especially those in science, computer, engineering, and photography labs need to be tracked and protected. This requires a single authentication method coupled with asset tracking and location intelligence. Many expensive older devices, where replacement is not an option, do not support modern network authentication protocols.

3. **Decentralized Control:** Multi-campus universities, as well as universities where many schools (i.e school of business, school of engineering) operate autonomously, require a way to connect easily to other departments, the cloud, and to the internet while protecting their resources.
4. **Large Scale, Mass Mobility and Roaming:** Universities have unique Wi-Fi roaming requirements, where at the top of the hour, thousands of students are moving from one location to another. As they move across 100's of access points they need to remain connected and authenticated. This requires a highly scalable authentication and authorization system coupled with connectivity remaining active as they roam.
5. **Fiber Optic Building Constraints:** Many universities are pillars of their state or community where they have been established for decades. These universities have brick and mortar structures that are not easily retrofitted with modern optical cabling. Also they lack convenient places in which they can attach and wire access points through the plenum. This makes it challenging to update the network with modern fiber plants, backbones and Wi-Fi technologies. These universities need to preserve buildings like this, while meeting the needs of today's online students.
6. **Large Entertainment Centers:** Larger universities have stadiums and entertainment centers that they run as a business and make open to the public. These entertainment sites have unique Wi-Fi requirements including high density endpoints to access point ratios, offering concession services with location intelligence, and maintaining control over large crowds.



7. **Real Time Video Demands:** Multi-cast and real time video conferencing sessions are running concurrently across 100's of classrooms at any given time. As universities move to the online world, it is becoming standard practice to have all classes available via real time video conferencing. Multiple concurrent real time video sessions require higher bandwidth, with efficient traffic delivery protocols.



8. **Regulatory Requirements:** Universities with medical schools have regulatory requirements, specifically HIPAA. These universities must have network security measures in place including network segmentation, access control, and breach notification (when there is a problem).
9. **Non Disruptive Upgrades:** As everyone and everything depends upon the network it must remain operational 7x24. This means that there are no outage windows even during the break periods as schools maintain skeleton crews that still require the network. Upgrades, and changes must be automated and non disruptive.
10. **IoT Controllers:** IoT devices have become mainstream within universities as they work to conserve energy and become more environmentally friendly. These devices control critical infrastructure resources including lights, HVAC, perimeter security, and a myriad of other physical assets. These devices must be protected, monitored and easily managed from within the network.

Network Modernization Technologies

Over the past 5 years, there have been many new, open standard innovations within the network industry, where cumulatively, universities can modernize their networks to meet these connected, online education demands.

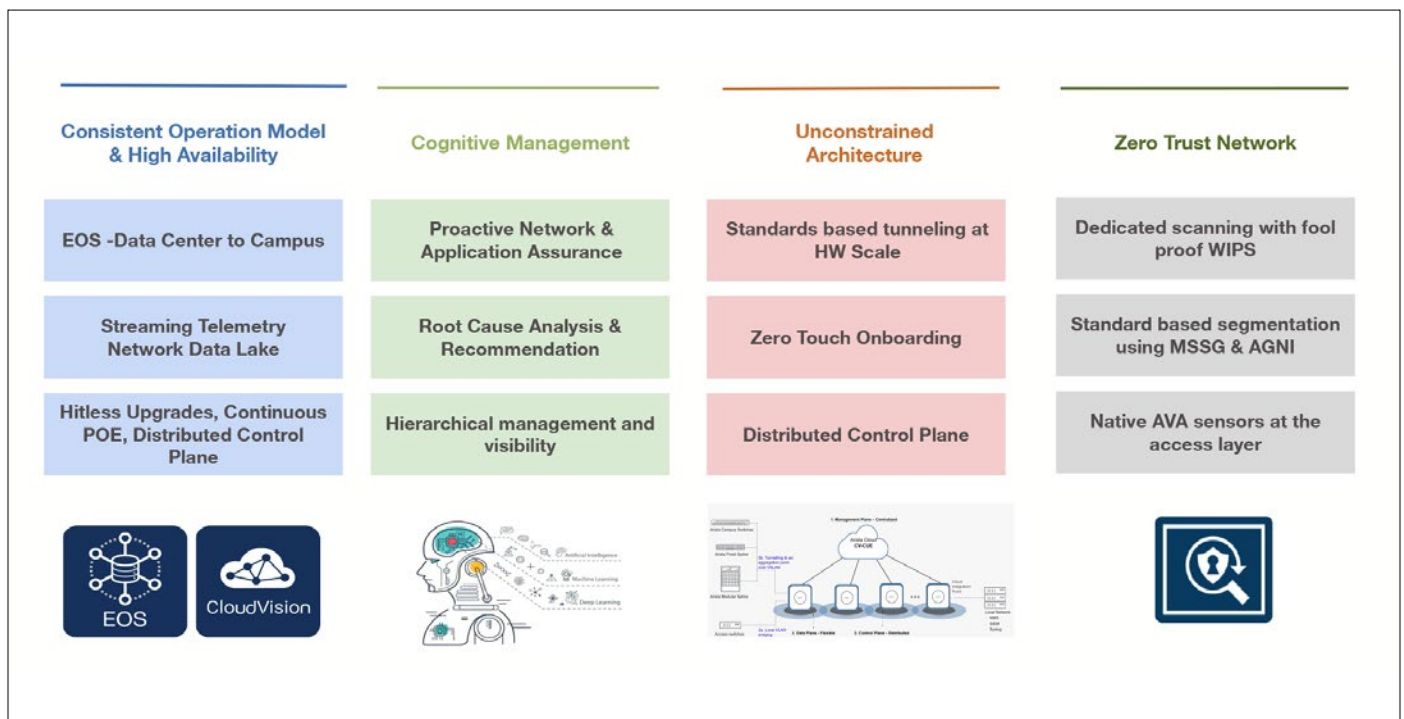
These technologies include the following:

- Simplified, scale out, multi-link, open, two tier topologies with 10/100/400 and 800 Gbps switching interface options.
- Power over Ethernet switches that deliver the wattage demand of more advanced Wi-Fi 6E access points.
- Endpoint identity management and authorization platforms that are cloud based where no local administrators or servers are required.
- Auto-tuning, auto-configuring, location aware, high density/high scale roaming Wi-Fi 6 and 6E access points.
- Location independent segmentation, for ensuring data privacy between students, professors, administration, IoT controllers, and guests.
- Automation where day-to-day operations including upgrades, security patches, configurations, and service ticketing are scripted workflows leveraging open API's and well known software scripting languages.
- Artificial intelligence for root cause and security breach analytics, where machine learning can detect rogue student activities, compromised Wi-Fi access points, transient packet problems, and early detection of hardware problems.

Arista Network Products and Technologies for Higher Education

Arista Networks has pioneered many of the above technologies, as they have become the wired and wireless leader in many data centers, both private and cloud based around the world. Arista has leveraged this leadership in the design and development of their campus offerings, where higher education universities have access to the same technologies that Google, Meta, Microsoft, eBay have deployed within their network infrastructures.

Arista Campus Network Technologies



Below describes these Arista technologies and how they are most applicable for higher education institutions.

1. **Scalable Simplified Networks** - There are many new open technologies that Arista embraces within their wired and wireless networking products, where universities can truly scale out and upgrade their networks, without forklift upgrades. These technologies include multi-link aggregation (MLAG), where multiple uplinks can be used for both redundancy and bandwidth concurrently. Unlike spanning tree where complex VLAN configurations were required to partially achieve these same benefits, MLAG offers an open standard approach, and is applicable irrespective of the interface speed.

Other technologies including ECMP coupled with MLAG allow the customer to choose between switching and routing depending on whether they want layer-2 switching or layer-3 routing topologies. Universities can now deploy cost affordable 100 Gbps interface technologies leveraging the latest optics, which are now more cost effective than the combination of four 25 Gbps independent ports.

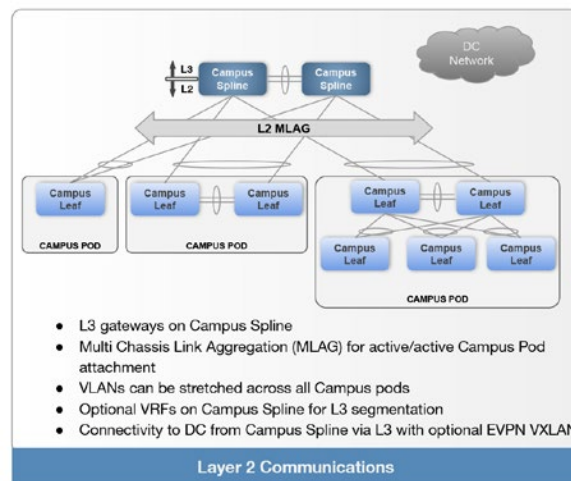
These technologies eliminate unnecessary multi-tier backbones, where designs now are leaf/spine, with leaf switches being deployed at the edge for Wi-Fi access point and endpoint connectivity and spine switches for scaling at switch interconnect backbones. This greatly simplifies designs. Further, these new open network link technology innovations are eliminating older proprietary designs, and switches, where universities were locked into buying from one vendor, with over complex designs that were hard to expand, upgrade and required tribal knowledge to configure.

All of these technologies are available with Arista's campus line of fixed and modular switches, ranging from fixed switches with 16 ports to Arista's high density modular switch with up to 384 Power over Ethernet (PoE) ports per chassis. Customers can choose the best PoE platform for their needs including the CCS-710, CCS-720, CCS-722, and CCS 750.

2. **Multi-tenant, Location Agnostic Topologies** - Fundamental to all higher education institutions is the need to segment and isolate network traffic, based upon communities of interest. The segmentation of traffic offers many benefits including traffic security, application prioritization, traffic filtering, and scalability where segmented traffic is easier to monitor, record, and analyze. Newer segmentation technologies are location independent where endpoint identity is leveraged (versus the physical location aka IP subnet). Location independence aligns better with highly mobile university environments especially with students that may roam between campuses.

While segmentation takes place within the data plane where traffic is forwarding within isolated switching domains, determining membership based upon endpoint identity is equally important especially within highly mobile campuses where the majority of the community are bringing their own devices. The coupling here between the data, control, and management planes is incredibly important.

Arista offers a complete multi-tenant solution, as well as products that are open where they can easily integrate with other multi-tenant networking products. Specifically, Arista switches can be controlled by 3rd party identity and policy management platforms, and/or Arista's Guardian Network Identity (AGNI) cloud based platform can integrate with 3rd party Wi-Fi access points and campus PoE switches. As Arista embraces open standards, universities can choose which hardware switches, access points and cloud based platforms are best for their needs.



MLAG Across Campus Domains

- 3. VXLAN Fabric Technologies for Roaming, Scalability, and Segmentation** - VXLANs were originally designed to overcome the multi-segmentation traffic limitations of virtual machine mobility within data centers. VXLANs offer the same benefits within campus networks where thousands of mobile devices cross IP segment and physical port boundaries as students roam around the campus. VXLAN expands and replaces VLANs as VXLAN provides location independence (layer 3 overlays), as well as supporting a larger number of communities. For universities VXLAN allows different types of devices (CORP-issued, BYOD, Guest etc.) to ride different lanes in the infrastructure.

Specific to campus designs, Arista uses VXLAN for the purpose of tunneling data from Wi-Fi access points to central switch locations where the traffic is terminated, as the enforcement point. These enforcement points provide localized control including authentication, authorization, QoS, security policing, traffic monitoring and packet captures. Moreover, this allows the access points to forward traffic locally without the need for centralized controllers, especially those within the cloud, that have well known single point of failure issues.

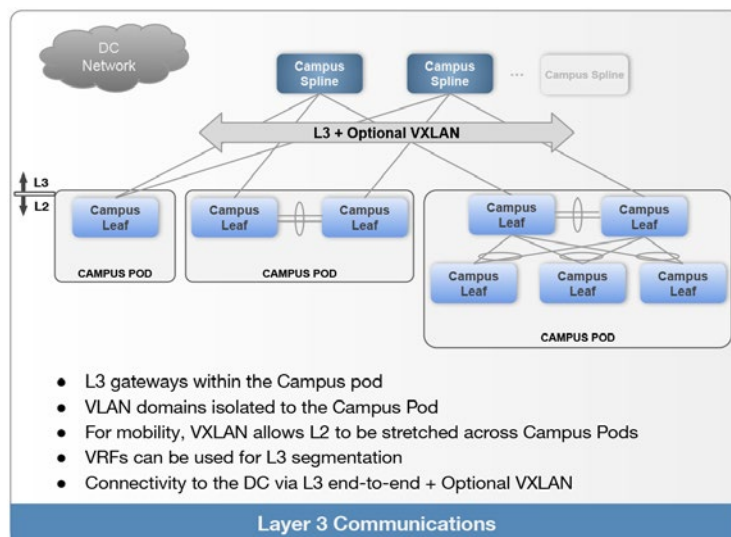
Another use case for VXLAN, is addressing the time out scenarios when there are large scale roaming events within EVPN fabrics. In these scenarios, host connections on the Wi-Fi network fail, as it can take over 100ms to reconverge the host within the EVPN fabric. Arista has a patent-pending implementation specific to their access points where the AP's themselves work around the convergence time issue, and maintain the endpoint connections. Arista's solution leverages VXLAN, to handle these higher convergence time scenarios. This solution works on both Arista switches as well as with any 3rd party switches as VXLAN is an open protocol.

While technically VXLAN design specifics are beyond the scope of this document, the use cases here are compelling as VXLAN addresses many of the scale, mobility, enforcement point, failover, and bandwidth requirements that higher education institutions are facing today. All of Arista campus PoE switches and access points provide VXLAN forwarding, tunneling and termination capabilities, including Arista's newest most economical 16 port fixed CCS-710 switch. Universities need to consider a migration from VLAN to VXLAN deployments as they modernize their network.

- 4. Wired and Wireless Unification** - It is clear that configuring a switch port is very different from configuring an access point as the switch port is physical and manages electrical signals, while the access point is virtual and manages radio signals. However there are several important benefits when these two technologies leverage the same dataplane, monitoring and management information.

These include the following:

- **Multi-tenant segment partitioning:** Well segmented campus networks require tight integration between the SSID's on the access points and the virtual LANS (VLANs and VXLANs) on the wired switches. The most secure approach requires real-time fabric intelligence, and auto configuration updating between the access point and switch forwarding planes to ensure that these virtual technologies are synchronized. Configured independently of each other, without any type of forwarding plane policing, leads to security holes where unwanted or non essential active virtual LANS, whether it is an SSID, or a VLAN is a point of vulnerability.



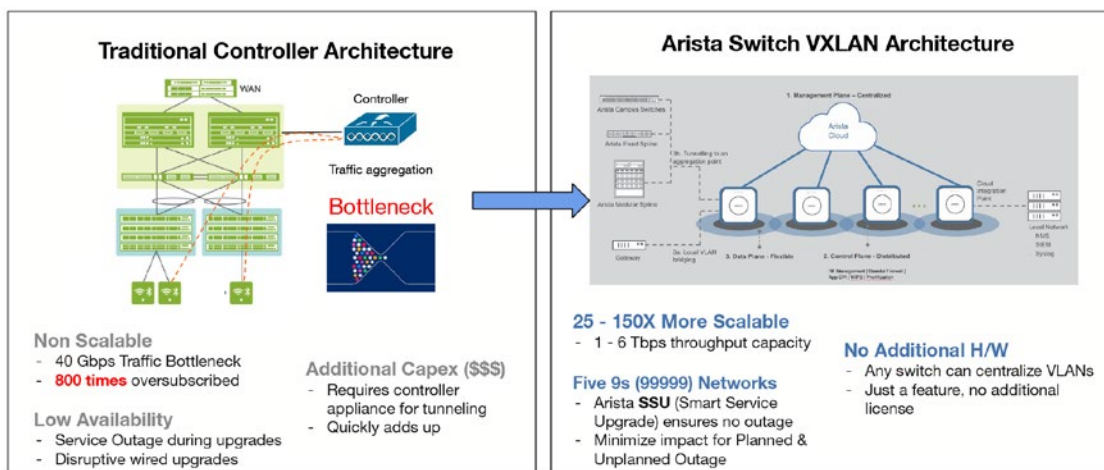
VXLANs Across Campus Domains

To overcome this challenge, customers often deploy centralized controllers, with tunnels from the access points and the switches. The controller acts as the enforcement point and resolves issues associated with extraneous SSID's and VLANs. The downside here is that controllers are single points of failures, especially when hosted remotely from within a cloud, and there are often scalability challenges, as controllers can become bottlenecks in larger networks.

A better solution is localized forwarding with auto propagation of the VLANs as well as pruning where the access points and switches are synchronizing themselves. This approach provides local forwarding intelligence within the access points and switches. This eliminates single points of failures, and provides more scalable wired and wireless network designs.

Arista offers both options here where customers can choose between a controller approach with tunneling, or a more decentralized approach with auto-VLAN propagation. The controller based approach provides interoperability with 3rd party switches, where customers can decide to use Arista access points within an existing switch fabric. Or given the option of a full building or floor replacement, universities can go with the better option where Arista switches in conjunction with Arista access points can be deployed controllerless, with Arista's auto-VLAN propagation technologies.

Arista Tunneling Benefits for Campuses



For those interested in knowing more about this auto-vlan propagation technology, determination of the VLANs is done between the access points and the AAA/Radius Server. The propagation once determined is done between the Arista switch and the access points via the Multiple VLAN Registration protocol (MVRP).

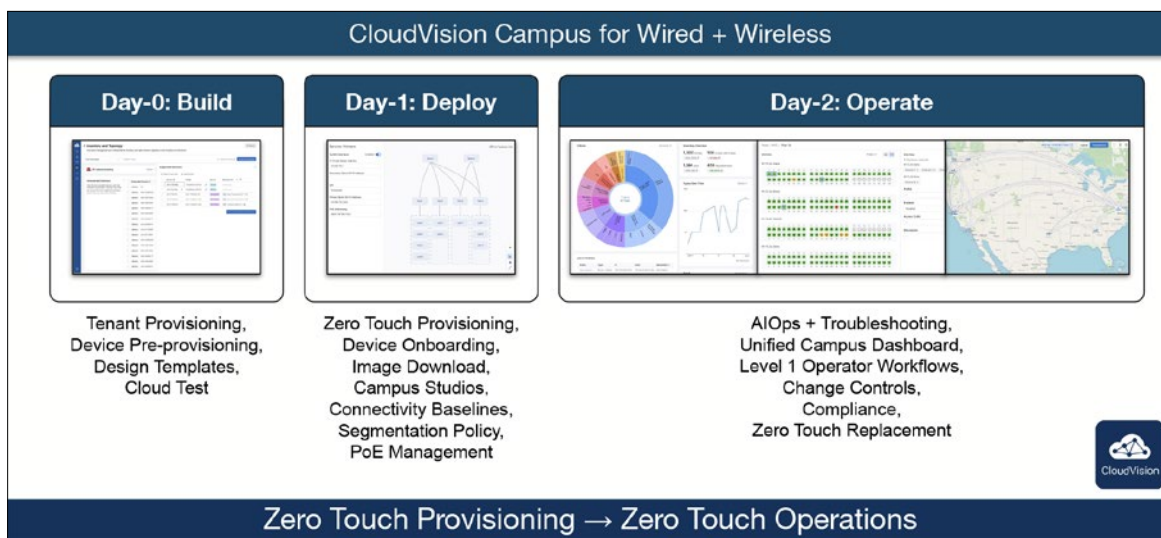
- .1x AUTH of APs: Leveraging EAP-TLS with Certs, administrators can tightly control by location (switch port) which access points and VLANs can be enabled between Arista switches and Arista access points. The example here is a switch port in a public location where a student or a guest tries to connect their own access point and hack into the network. With this authorization technology the switch port blocks the rogue access point traffic as well as removing any VLANs from that port. Further, Arista allows the definition of a VSA (Vendor-Specific Attribute) in the AAA/RADIUS Server that informs the switch if the access point can propagate VLANs from itself to the switch. This is an optional VSA for added security to allow VLAN propagation from access points.
- Integrated/optimized roaming in EVPN fabric: Higher education institutions have a unique use case, where there are large roaming events, albeit between classrooms and buildings concurrently at the top of each hour, and/or between campuses as universities consolidate under one name and provide access between sites. The biggest technology challenge is keeping the host active, where the user does not need to re-authenticate or start new sessions with their applications, especially those where they are streaming data. Specifically within the EVPN control plane, the occurrence of the same mac address seen in multiple places can get it blacklisted (removed from the fabric). Arista has an integrated wired and wireless solution where the access point maintains the host connection in conjunction with host tables on the switches.

- 5. Operations** - Historically, managing networks, whether wired or wireless has been approached by vendors with siloed tools and best practices. This results in too many ineffective tools, with high renewal licensing costs. All customers, including higher education, have goals on reducing the number of management tools and vendors as well as automating many of their processes with integrated service ticket workflows. By successfully reducing the number of tools and automating common operating tasks, customers save on licensing fees and salaries.

Core to these challenges are antiquated management protocols, especially SNMP which is non real time, and CLI where only a few highly trained technicians can determine the issue. Moreover, the old tools for tasks approach, where there are configuration, monitoring, asset tracking, inventory, discovery, traffic analytics, mapping, etc also need to be integrated as all of these tasks are interrelated.

Arista realized these shortcomings when they designed both their extensible network operating system (EOS) and their CloudVision network operations management platform. Together these two software platforms provide real-time telemetry and multi-functional management capabilities for addressing these long time operation issues. Moreover, Arista has developed a universal network data repository where network data from Arista access points, switches, and their recently released network identity platform (Arista Guardian for Network Identity) is gathered. Known as Data Lake, this repository provides correlated management data. Arista will increasingly leverage this datasource as they enhance their artificial intelligence capabilities. Today Wi-Fi networks leverage AI for auto-tuning, root cause analytics across a broad number of systems, and security detection and mitigation.

Arista Cognitive Campus Management



CloudVision is the first engineered solution which borrows concepts from the web stack of being able to get all states from every device, curate the data into a scalable storage system built on HDFS, and create a true Data Lake of all states in every network device. Data Lake exposes these states over well-defined and standard APIs. Customers can either choose CloudVision for configuring, monitoring, tracking, analyzing, reporting and resolving issues or they can develop their own tools leveraging these API's. Moreover, these API's are open where 3rd party providers including ServiceNow, and VMware, Splunk and others can integrate.

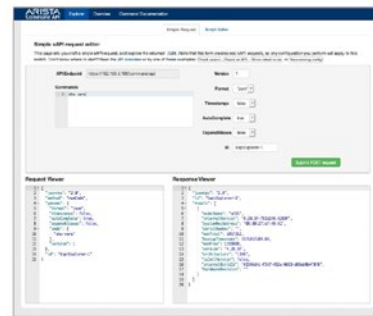
- 6. Automation** - All customers, especially higher education institutions managing large networks, with 1000's of access points, and upwards of 200K endpoints need processes to help them scale. Managing day to day operations with large monitor screens, global discovery tools, and multi-discipline operations teams is costly. Repetitive manual tasks that are error prone, especially those that are configuration related are better solved via automation.

As a result many customers are placing a high priority on automation. Specifically device detection, system upgrades, security patch roll outs, tenant services, configurations, monitoring, root-cause analysis etc. Different from pre-package operation tools, automation requires customization, as every customer has their own process and procedures. Automation must offer programmable workflows with an open programming interface. Moreover the network infrastructure must have open API's especially within the operating system to ensure successful implementation.

Automation is core within cloud infrastructures as this is the only way they can scale to thousands of users and be profitable. Adoption of the cloud has proven this way forward, and customers with private networks are beginning to follow, leveraging cloud best practices.

EOS for Open Automation Programming

- One Extensible Operating System (EOS) across all platforms
- Built-in ready to use API for all switches
- API instruction that perform like CLI commands
- Easy to manipulate responses – JSON
- Web based browser 'Explorer' to verify and test interaction
- Works with many programming languages (and standard libraries)
- Highly optimized Python library (pyeapi)
- Use on- or off-box



```
Python 2.7.9 (v2.7.9:648dcafa7e5f, Dec 10 2014, 10:10:46)
[GCC 4.2.1 (Apple Inc. build 5666) (dot 3)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>> import pyeapi
>>> switch = ['veos1']
>>> node = pyeapi.connect_to(switch[0])
>>> output = node.enable('show version')
>>> print output[0]['result']['version'], output[0]['result']['systemMacAddress']
4.20.3F 08:00:27:a7:49:41
```

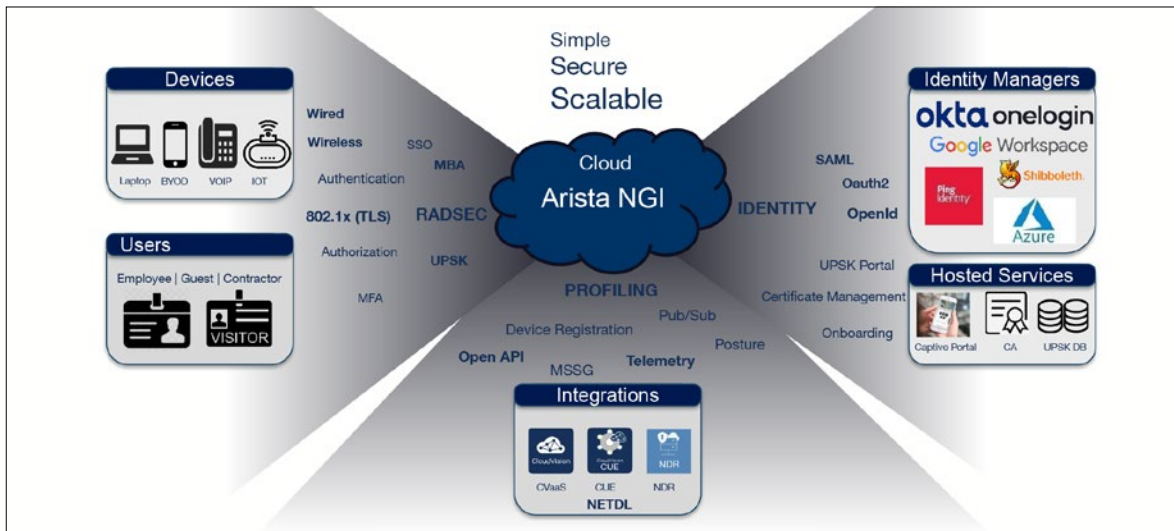
CloudVision greatly accelerates any automation undertaking with the following two notable technologies:

1. The first element is that of configuration automation with CI/CD pipeline. Arista has taken the approach that configurations objects are to be managed similar to code. This means that configuration changes are checked into a source code system, like GitHub, and are picked up by CloudVision for pushing into the network elements. This action provides easy audits and actions such as removing new configurations (very similar to reverting to code changes). The whole configuration change procedure can then be made part of a CI/CD pipeline allowing continuous but controlled configuration of network elements. These configuration changes can then be coupled with Arista Validated Designs that allows customers to start with a tested configuration and make incremental changes to the configuration as needed.

2. The second element of automation is coming from the Data Lake, which allows several ways for customers to consume telemetry data from the network elements (switches, access points etc). The data from Data Lake can be directly consumed, or CloudVision defines several APIs, including using Google RPC (gRPC), to obtain the data. CloudVision can then process the data for configuration changes, fault identification. Moreover, for applying Machine Learning algorithms on the data etc.

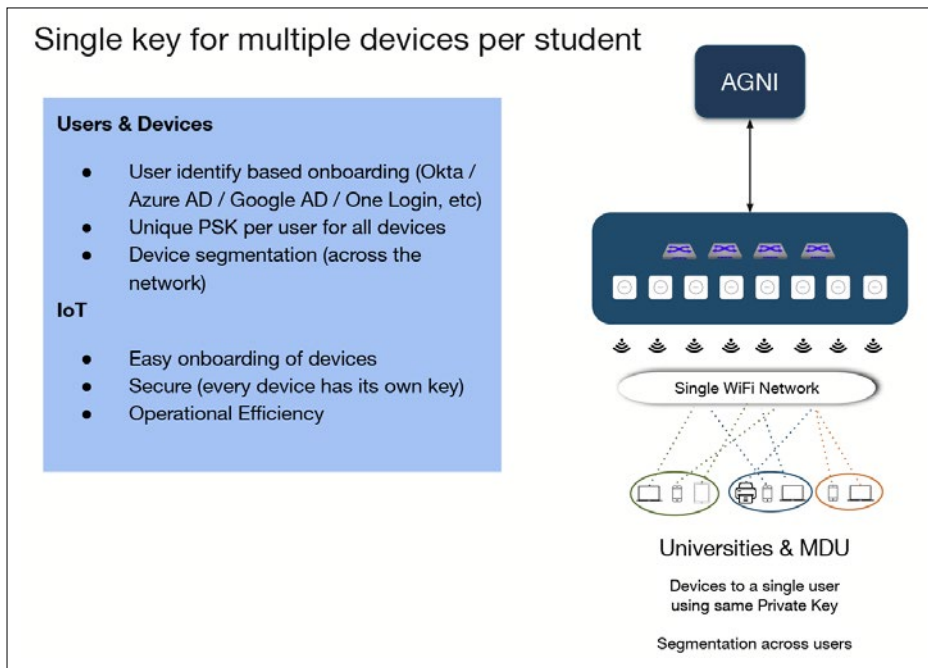
7. **Network Identity and Authorization** - The market transition from IT issued devices that attach to the network (desktop, laptops, printers) has given way to Bring Your Own Devices (BYOD), where anything with a wired or wireless network interface can be attached. While this has reduced the friction between higher education institutions and their student community, BYOD comes with a set of security challenges and these unmanaged devices can easily be bad actors. The only and best way to control this is to segment these devices and the user communities into protected and unprotected network segments, via device and user identity management. Moreover, endpoint identity platforms are better integrated with the network identity platforms, where compromised endpoints are isolated or blocked from communicating on the network.

Arista Next Generation Identity/Access



Arista offers a leading cloud based, scalable network identity and authorization platform known as Arista Guardian for Network Identity (AGNI). This platform leverages microservices technologies and is easily configured with Arista wired and wireless infrastructure technologies. AGNI scales to the most demanding infrastructures in support of many of the largest private enterprise infrastructures with over 500K endpoints. AGNI supports all of the common authentication and transport protocols including mTLS, RadSec, UPSK, and others. Further AGNI is integrated with the most commonly adopted endpoint detection platforms including those from Microsoft, Medigate, JAMF, Splunk, and Sumo Logic.








Arista Wireless Segmentation



All higher education institutions should be considering and deploying network identity platforms in response to the explosion of network attached BYOL.

8. Conclusion - Higher education institutions are having to adapt to new ways of providing learning, as they embrace students that have grown up with the Internet, always connected. These students are challenging traditional learning methods, including in person classrooms, human generated intelligence, social norms, paper copy, and manual processes. Their college experience is increasingly held together by the network, including the intranet and the Internet.

Arista Campus Modernization Features

 <p>Ease of use!</p> <p>Intuitive features. Nothing proprietary, all open standard. #ThatWasEasy</p>	 <p>Single OS</p> <p>Single OS across all platforms makes it easy to train, manage, upgrade and extend environment to cloud. #FutureProof</p>	 <p>Lower Costs</p> <p>Lower cost comes from fewer Licensing SKUs. Average Arista quote has 3 or less SKUs (HW/SW/Maint) #BestValue</p>	 <p>Best Support</p> <p>World-class one call support. Engineer who picks up the call works the case until completion. #SuperSupport</p>
 <p>Automators Dream</p> <p>Ranked #1 by customers and advocates as the best network and automation platform on the planet. #Automagic</p>	 <p>Open Standards</p> <p>Everything is Open Standards Networking, nothing proprietary, works with existing networking infrastructure #AlwaysOpen</p>	 <p>Integration</p> <p>Our platform integrates with almost all Firewall, Security, Big Data, Automation, NLB, HCI, Storage, etc. Providers. #inteGREATion</p>	

The network must evolve as higher education evolves with these shifts in learning. New real time applications, BYOD, location awareness, network telemetry, secure partitions and automation are all features that need to be equally factored in when making wired and wireless upgrade decisions. Arista technologies and products are based upon modern day cloud networking principals where these requirements are factored in holistically, including their core network operating and operations management platforms. Arista has integrated dataplane, control plane and management plane approaches where wired and wireless products operate seamlessly in offering the most secure, reliable, scalable solutions.

Santa Clara—Corporate Headquarters
 5453 Great America Parkway,
 Santa Clara, CA 95054
 Phone: +1-408-547-5500
 Fax: +1-408-538-8920
 Email: info@arista.com

Ireland—International Headquarters
 3130 Atlantic Avenue
 Westpark Business Campus
 Shannon, Co. Clare
 Ireland

Vancouver—R&D Office
 9200 Glenlyon Pkwy, Unit 300
 Burnaby, British Columbia
 Canada V5J 5J8

India—R&D Office
 Global Tech Park, Tower A, 11th Floor
 Marathahalli Outer Ring Road
 Devarabeesanahalli Village, Varthur Hobli
 Bangalore, India 560103

Singapore—APAC Administrative Office
 9 Temasek Boulevard
 #29-01, Suntec Tower Two
 Singapore 038989

