aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

DYNAMIC SEGMENTATION IN HIGHER EDUCATION

Simple and secure access for students, faculty, and staff - that unify wired and wireless networks

The growing number of personal, educational, and facility related IoT devices and the use of education-critical mobility and cloud services are driving digital innovations everywhere. Which leads us to the question — is the network edge smart enough to securely connect all types of devices and users? Legacy wired and wireless networks were created without education-critical mobility, IoT access or security in mind. Today's approach of using manual and static configurations for these ever changing mobile and IoT devices located throughout the university campus and branch networks presents new security risks and has become a cumbersome task that IT teams face every day.

To simplify and secure the network, Aruba Dynamic Segmentation unifies policy enforcement across wired and wireless networks - keeping traffic secure and separate. It's now easy for operations and centrally-managed networks with IoT and IT-managed client devices to co-exist, while optimizing network experience and IT operations end-to-end.

Dynamic Segmentation utilizes intelligence gathered from Aruba's foundational role-based policy capability, user firewalls, alongside rich Layer 7 application visibility and integrated web content filtering.

KEY EDUCATION AND TECHNICAL DRIVERS

Simpler policy administration

Onboarding IoT and client devices have typically required multiple touchpoints - often times requiring the manual configuration of new VLANs, ACLs, or subnets at every hop in the network. Ongoing moves, adds, and changes for large, distributed networks can also be time-intensive and error-prone. Designing a network with strong security while reducing complexity have typically been mutually-exclusive.

Enhancing the user experience

As students or faculty move between classrooms or from buildings to outdoor locations, they expect the same network experience no matter where they connect or how – wired or wireless. And asking them to use a virtual private network (VPN) is a challenge. Any network experience that requires IT support is seen as negative, and students are surely willing to share their experience on social media. User experience – whether employee, faculty or student – affects a school's success. Connecting multiple device types, such as mobile phones, game consoles, printers or personal equipment such as rasperry pi computers, drones, or smart watches is often done without IT's knowledge or support. The expectation is that IT provides a flawless experience while maintaining visibility and management of all things on a secure network.

KEY BENEFITS

- **Better, consistent user experience** – Extend user role, application deep packet inspection and device profiling features from wireless to wired networks
- **Simpler network operations** – save time and eliminate VLAN sprawl by reducing the configuration needed for SSIDs, ACLs, subnets, and wired ports
- **Improved security and device visibility** – ClearPass and Policy Enforcement Firewalls (PEF) deliver enhanced visibility and policy enforcement

In addition, from smart lighting to security cameras or badge readers, IoT devices are rapidly being deployed throughout networks of all sizes. This newfound network connectivity brings many appealing and academic benefits, but also exposes the network to security risks as these devices hop on the same pathways as sensitive student, medical, and university data. These devices rarely have strong security built in and also lack robust authentication. Passwords are stored in clear text, they lack secure supplicants, and they are often physically located in un-secured public areas – which opens the door to network breaches.

Network vulnerability is exposed with the number of IoT/headless devices connected to enterprise networks projected to grow to over 20 billion by 2020.

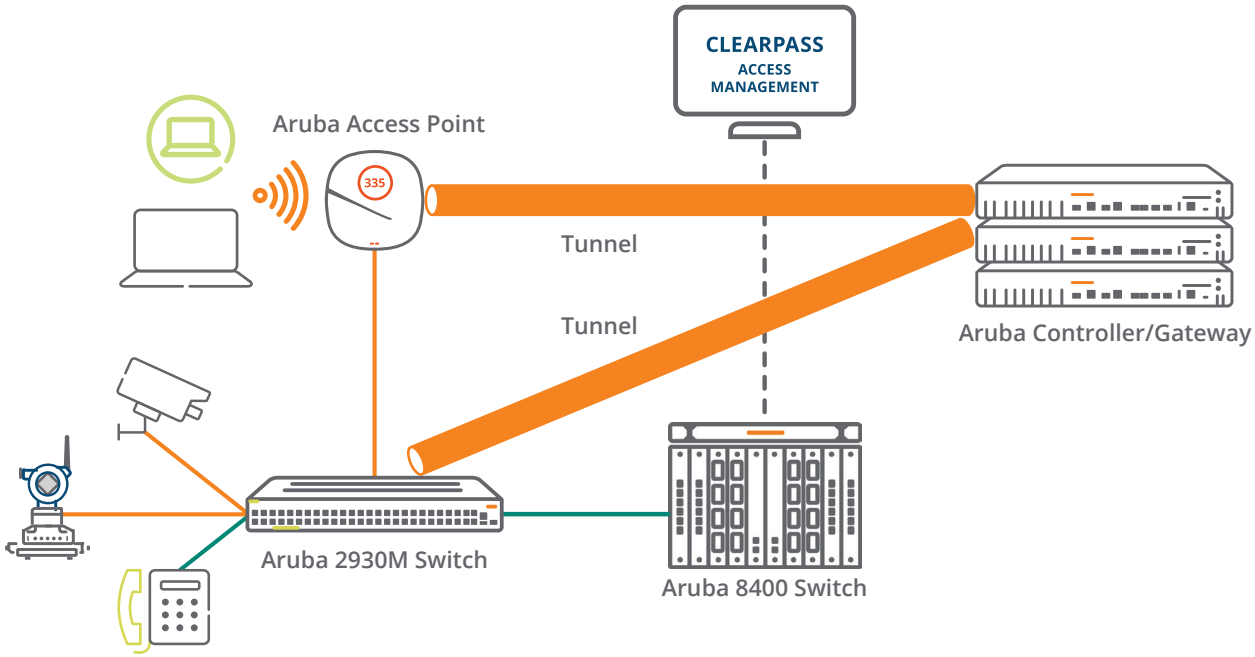
Source: Gartner (January 2017)

EXTENDING WLAN INNOVATIONS TO SWITCHING

Dynamic Segmentation extends Aruba's secure policy management and WLAN policy enforcement capabilities to make wired network access simple and secure. This capability means that wired client devices can be dynamically assigned policies based on port or user role - ideal as the number of IoT devices is projected to hit 20 billion by 2020. Aruba network switches, now backed by ClearPass for policy management and Mobility Controllers for enforcement, play a key role in unifying network access.

Role-based policies

By implementing Dynamic Segmentation, role-based policy decisions and access rights are made based on the device type, application used, and even the location of the user or device. Originally used to address wireless security, role-based policies segmented network traffic by user type such as employee, guest or contractor, while dramatically simplifying network management by eliminating complex and static network configurations. This powerful capability streamlined IT workflows such as managing access and BYOD policies and ensured better application performance.



Dynamic Segmentation, part of the Experience Edge

Extending dynamic role-based policy management across wireless APs and wired switches provides a fundamentally simple, secure, yet different way to manage and enforce policies for mobility, IoT, and cloud. Aruba's Mobility Controllers/Gateways which enforce ClearPass policy definitions, are now able to dynamically understand and utilize roles for wired devices connecting to the network. This ability eliminates the time consuming and error prone task of managing complex and static VLANs, ACLs, and subnets by dynamically assigning policies.

Layer 4-7 segmentation

The second foundational capability that the Aruba switches leverage is segmentation. The Aruba WLAN architecture keeps traffic secure and separated with the use of tunnels between access points and a controller or gateway. This tunnel-based segmentation provides security such as firewall inspection of high-risk traffic, through the use of Aruba's built-in Policy Enforcement Firewall (PEF). PEF delivers granular context (user, device, app, location), mitigating the need for expensive firewalls for first line of interrogation and defense. With contextual policies based on identities, device type and location, you can satisfy the needs of different groups of users with a single network configuration as traffic flows simply adapt to the assigned roles.

By using this WLAN tunnelling architecture, Aruba switches can now provide a role-based segmentation approach versus the traditional, more manual use of local VLANs. This is ideal for untrusted IoT devices or for providing application visibility, as Aruba switches can now dynamically tunnel selected traffic to the controller for deep packet inspection and device authentication just as an access point does. For example, a student's game console or drone can dynamically be assigned a role with rights that restricts its traffic to a specified server only, eliminating the opportunity for malicious entrance to other parts of the network.

This new segmentation capability improves security posture with tunnelling that can be set-up for either Port-Based Tunnelling (PBT) with all authentication done on the controller or User-Based-Tunnelling (UBT) with authentication done on the switch. Because this segmentation operates as an overlay, it can co-exist with VLAN implementations by utilizing secure tunnels in selected areas with no ripping and replacing of the entire switching infrastructure.

Dynamic Segmentation simplifies and secures wired and wireless networks by establishing the Mobility Controller as a unified policy enforcement engine. Traffic from an AP or Switch are encapsulated in GRE tunnels for inspection by the Policy Enforcement FIrewall (PEF).

THE SOLUTION INGREDIENTS

Aruba Wireless Access Points

To meet the needs of any environment, the Aruba portfolio includes high performance Wi-Fi 6 (802.11ax and Wi-Fi 5 (802.11ac) APs. Built-in AI intelligence, and location services offer IT the automation and visibility needed to deliver an optimal experience, for users and IoT devices.

Aruba Network Access Switches

An integrated wireless-wired foundation is also possible that delivers scalability, security and high performance for campus and branch networks. Dynamic Segmentation uniquely gives IT teams a simple way to apply policies, utilize advanced services and securely segment wired user and IoT traffic anywhere in the network via the tunneling previously mentioned. The following Aruba switches support this functionality: (2930F, 2930M, 3810M or 5400R running ArubaOS-Switch 16.04 or above).

Aruba Gateways and Mobility Controllers

As a crucial part of the solution, controllers or gateways act as a policy enforcer for both wired and wireless traffic. The Aruba Mobility Controller (running AOS 8.1 or later) allows IT to leverage policy enforcement, bandwidth contracts and other traffic restrictions. In a branch environment, the Aruba Central-managed Branch Gateway performs this role. The Policy Enforcement Firewall serves as the underlying network technology in support of these two environments.

Aruba ClearPass Policy Manager with Profiling

Centrally manage and enforce network access policies for wireless and wired access control. Its primary functions are device profiling, authentication, and authorization and policy enforcement. Using ClearPass, once the role and the privileges are defined, they follow the user or device

across wired and wireless access. So, if the user changes to an unknown device, or is on an unsecured network, the policy will automatically change authorization privileges. Downloadable User Roles (DUR) are configured on ClearPass, which eliminates the need to define roles or policies on a switch.

SUMMARY

To better handle a university's critical mobility and emerging IoT connectivity requirements, Aruba's innovative Dynamic Segmentation solution simplifies IT operations and improves security by dynamically applying unified policies and enforcing advanced services anywhere in the network. This ensures that appropriate access and security policies are seamlessly distributed, automatically applied, and independently enforced for all wireless and wired students, faculty, staff, and devices.

SO_DynamicSegmentationinhighered_SK_072619 a00078390enw