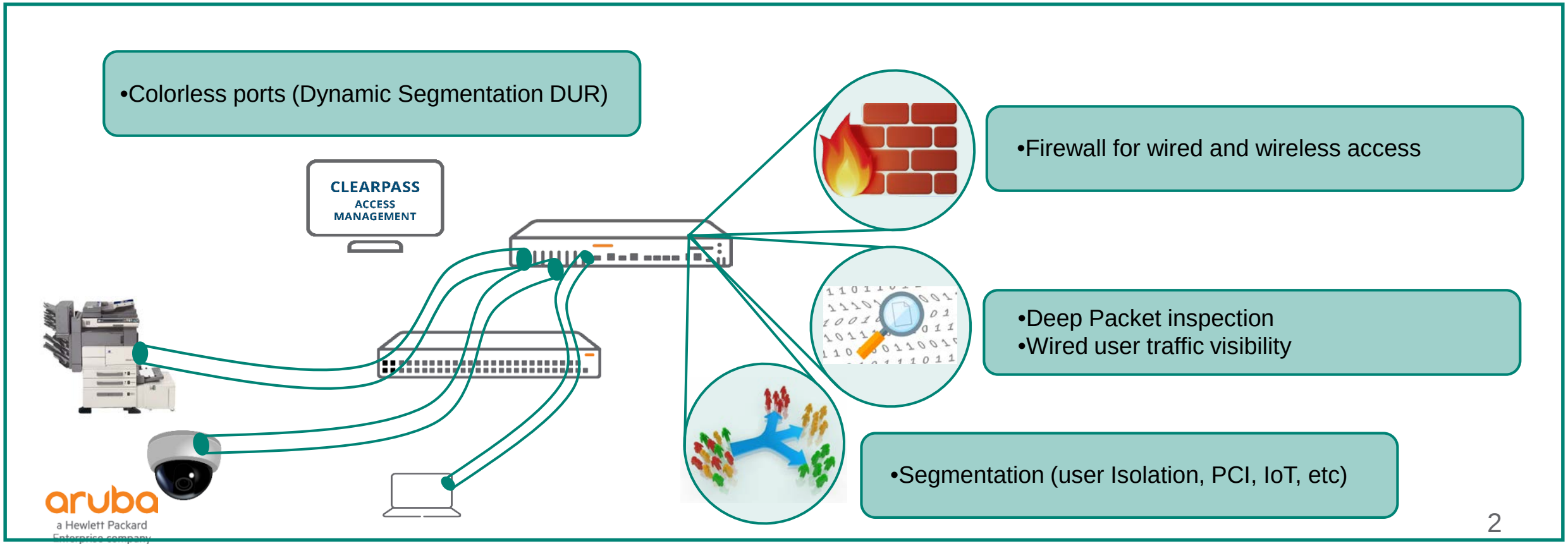
Dynamic Segmentation 2.0

aruba
a Hewlett Packard Enterprise company

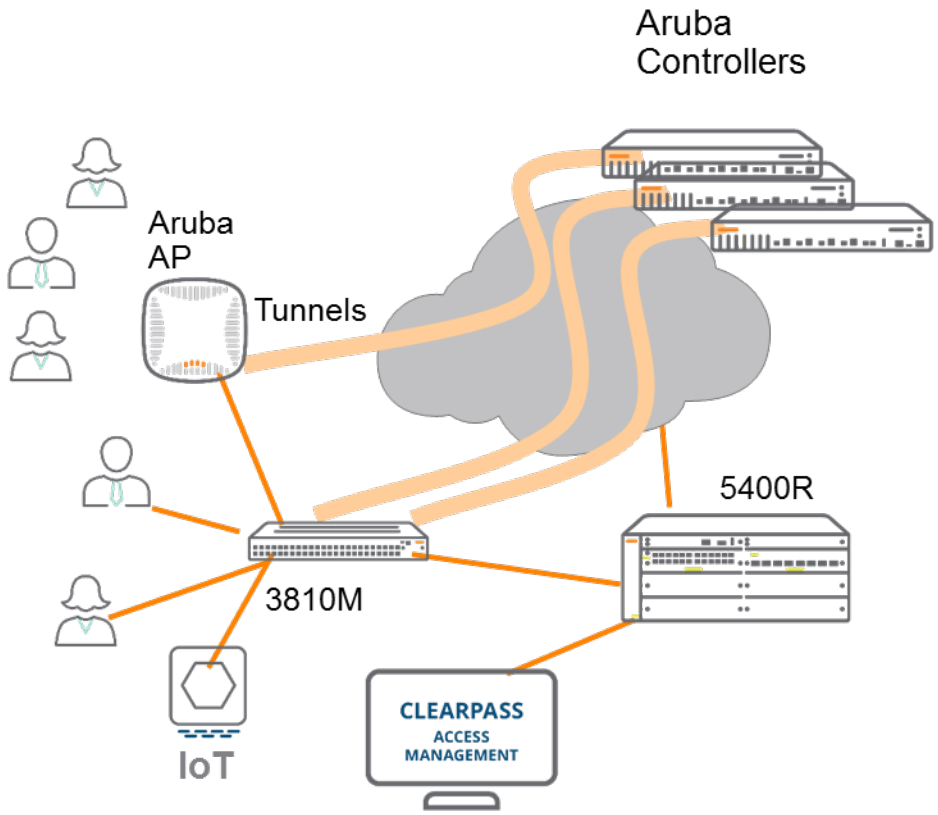
User/Port-Based Tunneling

Solution Benefits

- Applying controller features to wired traffic
- Leveraging integration between ClearPass, controller and switches to create a true dynamic network
- Reducing overhead and by eliminating the need to configure and maintain Vlans and roles across the network



Dynamic Segmentation Secures, Simplifies and Unifies Access



Solution Requirements:
Aruba 2930F, 2930M, 3810 and 5400R Campus Switches (Requires ArubaOS-Switch 16.04 or later)
Aruba Mobility Controllers with AOS 8.1
Aruba Branch Gateways with ArubaOS 8.4 and Aruba Central 2.4.3
Aruba ClearPass Policy Manager

KEY USE CASES

Secure IoT Devices
Dynamically segment IoT traffic in secure tunnels to protect the IoT traffic and protect critical clients' traffic.

Better, Consistent User Experience
Centralized, unified role-based policy and authentication and enforcement delivers same policy and consistent user experience wherever user or IOT device is and however they connect (wireless or wired).

Simplify Operations
Save time and reduce configuration errors by eliminating manual, static configurations of VLANs and ACLs on switches by dynamically applying unified wired and wireless policies and advanced services anywhere in the network. No new networking skills required!

Ensure Branch Security
Utilize ZTP for switches and tunnel specific wired (per port) traffic to controller with Firewall - great for retail PCI compliance, remote education satellite research campuses or healthcare facilities.

Use Built-in Controller Security Services
Take advantage of Aruba mobility controller and branch gateway's built-in security features such as Firewall, packet inspection and finger printing for wired and wireless traffic.

Overlay Architecture Solution
Enables smooth integration with existing segmentation such as VLANs means no ripping and replacing entire switching infrastructure

aruba
a Hewlett Packard Enterprise company

Dynamic Segmentation Enhancements

Simplified Network Implementation

- Remove VLAN coordination between controller and switch as a pre-configuration requirement
- Enable controller policy to enforce broadcast and multicast client isolation

Visibility Enhancements

- Representation in the controller GUI of tunneled clients
- Aruba AirWave tunnel clients view, switch to controller visibility

Client traffic isolation - Policy for IoT

- Single controller – Role Based Policy
- Cluster – IP and L2 based ACL for client isolation

Device Attributes in User Roles

- Downloadable User Roles (DUR) will allow additional client attributes as well as device attributes to address common deployment scenarios
- Example CLI:

```
aaa authorization user-role name “test”
    vlan-id 200
    vlan-id-tagged 201-456
    reauth-period 120
    cache-reauth-period  360
    device
        port-mode
        poe-alloc-by-class
        poe-priority critical
        admin-edge-port
    exit
Exit
```

- Note that device attributes are applied per-port and not on a per-client basis

Tagged VLAN IDs

Allows multiple tagged VLANs to be associated with a particular client. Useful for AP deployments.

Port Mode

Authenticates only the first client on the port and bypasses authentication for subsequent clients. Useful for AP deployments.

PoE Alloc By Class

Assigns the PoE class for a device. This prevents the device from requesting more PoE power than what is allocated by the power class.

PoE Priority

Sets the PoE priority for the device. APs typically will be set to “critical”.

Admin Edge Port

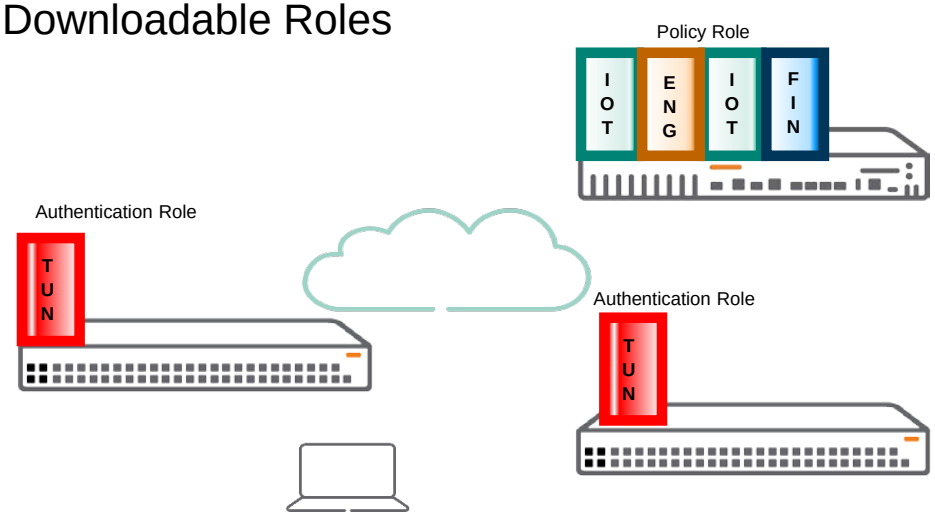
Sets the port to a downlink resulting in faster port bring up

User-Based Tunneling- Deployment models

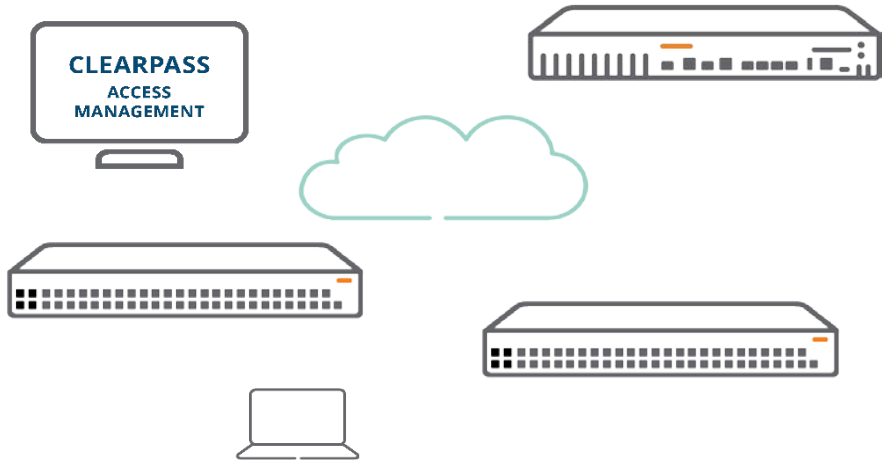
Supported Deployment models

- User/Port-Based Tunneling can be deployed with or without ClearPass
- Both models offer the same visibility and policy enforcement capabilities
- Adding ClearPass will enable a simpler deployment, added security capabilities and create a “smarter” more dynamic network

Pre-Configuration required Without Downloadable Roles



No Pre-configuration required With Downloadable Roles



aruba
a Hewlett Packard Enterprise company

Higher Ed Reaps Benefists of Dynamic Segmentation

Operational Simplicity in Higher Ed

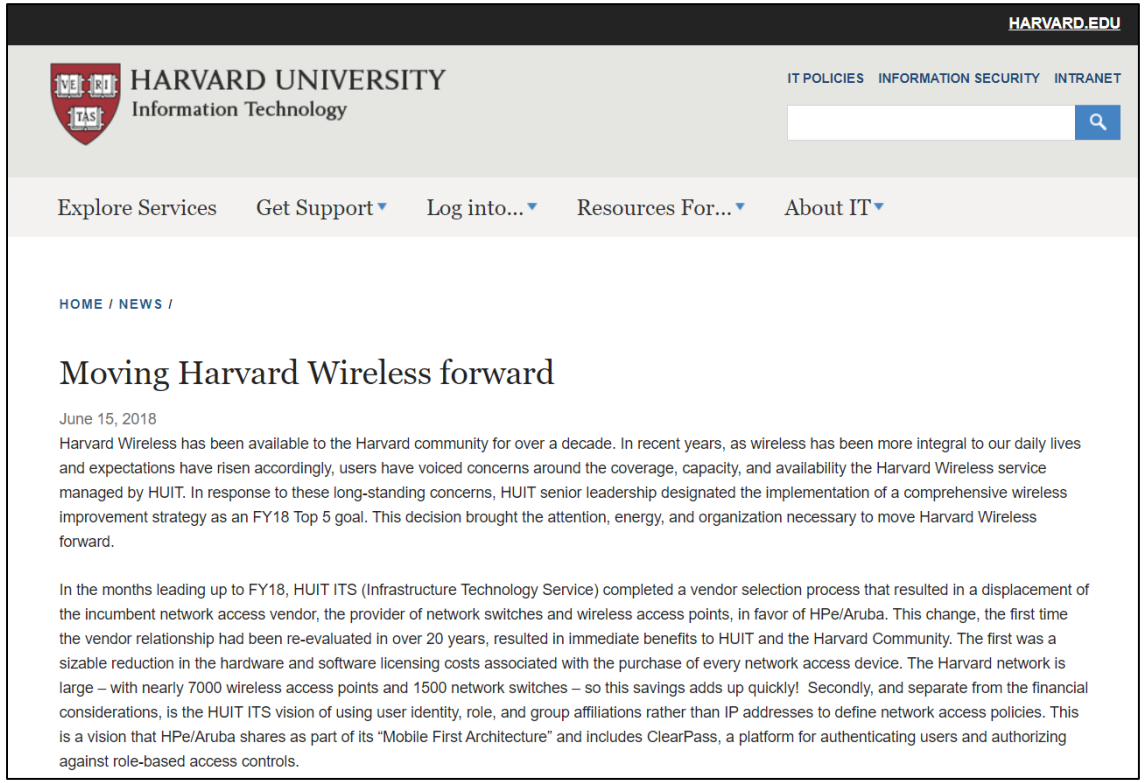
HARVARD UNIVERSITY

"Dynamic Segmentation will simplify 15,000 ports for us"

Use case: Dynamic port policy that follows the device and a single policy regardless of connection method

Solution: 15k switch ports starting with IT buildings and then rolling out to additional buildings on campus

Products: 2930M, 5400R, ClearPass, AOS8 Controller



HARVARD.EDU

HARVARD UNIVERSITY
Information Technology

IT POLICIES INFORMATION SECURITY INTRANET

Explore Services | Get Support | Log into... | Resources For... | About IT

HOME / NEWS /

Moving Harvard Wireless forward

June 15, 2018

Harvard Wireless has been available to the Harvard community for over a decade. In recent years, as wireless has been more integral to our daily lives and expectations have risen accordingly, users have voiced concerns around the coverage, capacity, and availability the Harvard Wireless service managed by HUIT. In response to these long-standing concerns, HUIT senior leadership designated the implementation of a comprehensive wireless improvement strategy as an FY18 Top 5 goal. This decision brought the attention, energy, and organization necessary to move Harvard Wireless forward.

In the months leading up to FY18, HUIT ITS (Infrastructure Technology Service) completed a vendor selection process that resulted in a displacement of the incumbent network access vendor, the provider of network switches and wireless access points, in favor of HPe/Aruba. This change, the first time the vendor relationship had been re-evaluated in over 20 years, resulted in immediate benefits to HUIT and the Harvard Community. The first was a sizable reduction in the hardware and software licensing costs associated with the purchase of every network access device. The Harvard network is large – with nearly 7000 wireless access points and 1500 network switches – so this savings adds up quickly! Secondly, and separate from the financial considerations, is the HUIT ITS vision of using user identity, role, and group affiliations rather than IP addresses to define network access policies. This is a vision that HPe/Aruba shares as part of its "Mobile First Architecture" and includes ClearPass, a platform for authenticating users and authorizing against role-based access controls.

https://huit.harvard.edu/news/moving-harvard-wireless-forward

aruba
a Hewlett Packard Enterprise company