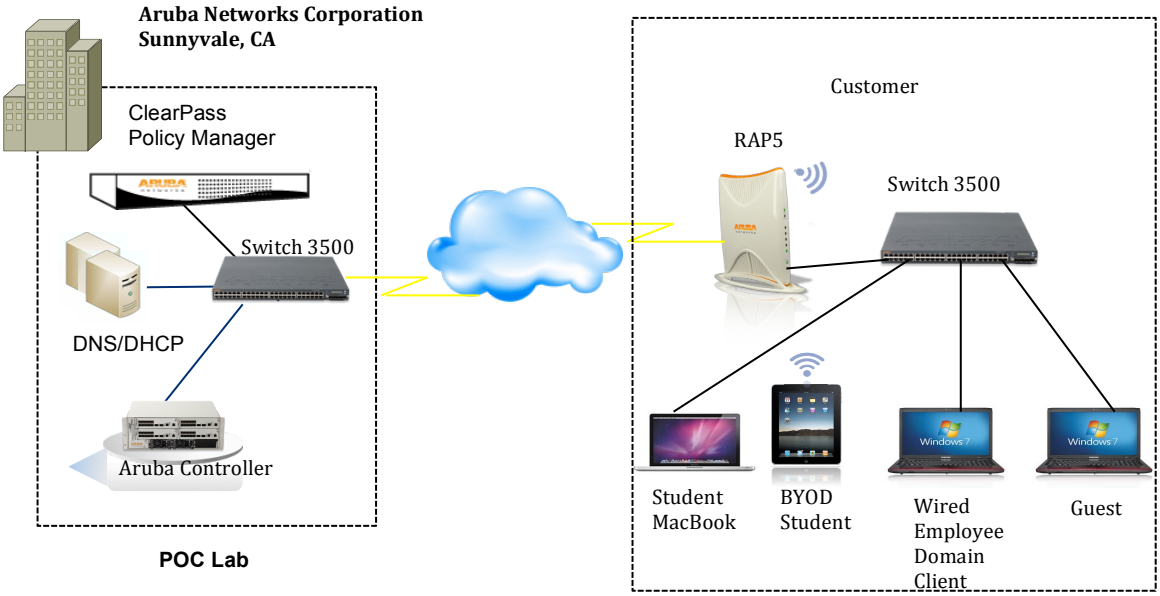
## First very successful LIVE demo of ClearPass:

The Team: Wayne Simms – Account Manager
John Castaldi – Operations Manager
Tim Brophy – CSE
Geoff Giulino –SE
Mark Jordan – POC Lab
Sathya Narayana Gopal - Reference Design Engineer
Garry Gardner - SE

Our Mission:

Demonstrate ClearPass Policy Manager's identity- and device- based network access control across any wired, wireless connection. The customer has deployed an Aruba wireless infrastructure. Their goal is to provide the same level of secure connectivity to their wired network. The Aruba team proposed the Switch 3500. Here's the setup:




Here's the POC lab setup in Sunnyvale, CA thanks to the hard work of Mark Jordan and Sathya Narayana Gopal. Mark did extensive testing to ensure success in the field:

1. ClearPass Policy Manager
2. Aruba controller
3. Switch 3500
4. DNS and DHCP servers

At the customer's campus on the east coast:

1. Switch 3500
2. MacBook Pro
3. iPad
4. Windows Guest machine
5. Windows Domain machine

With the setup above we were able to demonstrate live, a number of onboarding and security scenarios our customer is challenged with.

## 1. Guest access with sponsor approval:

1. iPad connected to PoC-Guest SSID, Wired Switch
2. Self Registration form completed and account awaiting approval
3. Sponsor approves and guest can continue to login

**Result:** Guest Role → Limited to public web browsing

## 2. Executive BYOD iPad

1. iPad connected to PoC-Employee using cached credentials
2. BYOD device detected & iPad forced to device provisioning page
3. Executive authorizes with domain credentials & unique device credentials & supplicant configuration pushed to the iPad
4. iPad disconnected & re-authenticates with new provisioned credentials

## 3. Executive BYOD MacBook

1. MacBook connected to Ethernet switch using cached credentials
2. BYOD device detected & MacBook forced to device provisioning page
3. Executive authorizes with domain credentials & unique device credentials & supplicant configuration pushed to the MacBook for both wired and wireless settings.
4. MacBook disconnected & re-authenticates with new provisioned credentials

**Result:** BYOD Exec → Exec Access Zone + unrestricted bandwidth.

1. Note: We also demonstrated how a student with cached credentials could onboard their BYOD device. After authorizing with domain credentials, unique device credentials & supplicant configuration are pushed to the MacBook for both wired and wireless settings. MacBook disconnects & re-authenticates with new provisioned credentials. In this use case the student MacBook was given a limited access zone (LAZ) role.

4. Corporate Issued Laptop

   1. Windows Laptop connects to PoC-Employee SSID, Wired Switch
   2. Domain & User credentials used during 802.1x authentication


**Result:** Employee Role → unrestricted access

Tim Brophy, Geoff Giulino and Garry Gardner walked the customer through each use case and explained:

1. Role of ClearPass as the policy decision point
2. Role of the Switch 3500 as an enforcement point
3. Advanced profiling
4. AAA services

The SE team also used:

1. ClearPass Policy Manager application to show user logins real-time.
2. The Aruba Mobility controller software showed users in the logon role (CP) and once authenticated in the student, employee, executive or guest roles.
3. We kept up a CLI session on the Switch 3500 to show tunnels coming up.
4. Airwave to show statistics and generate reports.

The customer was so impressed with the live demo, their response was, "this is nirvana, everything we have been searching for in a secure mobile system."

We are looking forward to having this setup in the SE-DEMO lab for all to do a similar demo.