LLNL-PRES-442431

LLNL Site Update:
Wireless/Wired Mobility Solutions

July 15, 2010

Robin Goldstone

Associate Program Leader for Networks and Convergence

S&T PAD - Computation / ICCD

Lawrence Livermore National Laboratory

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

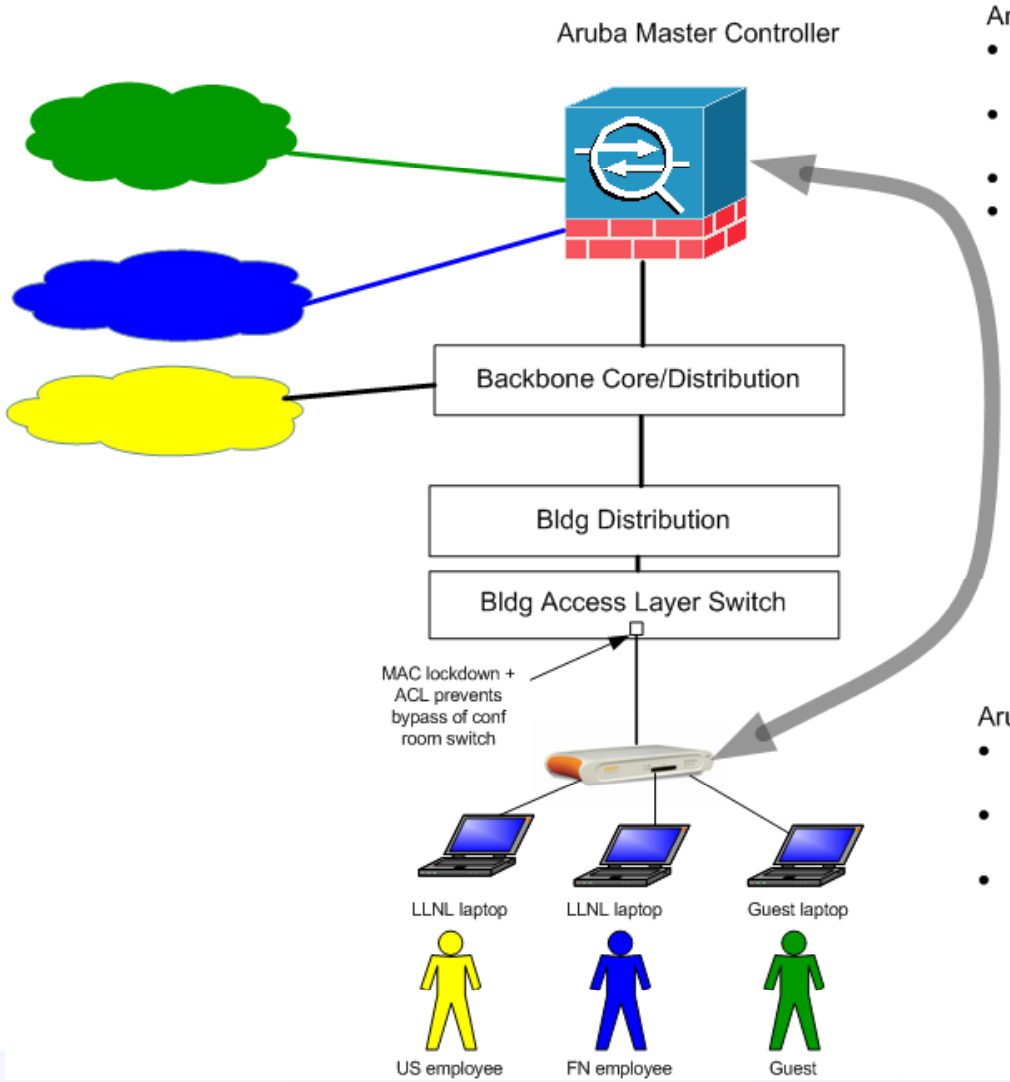
LLNL Mobility Capabilities

- WiFi current state
  - 802.11b/g solution from Aruba Networks
  - Approximately 240 APs in 35 buildings
  - Employee and Guest access provided
  - Air Defense WIDS solution
  - Customer pays for deployment, institution provides ongoing support and maintenance
- Planned upgrades
  - Replace Air Defense with Aruba Airwave – IN PROGRESS
  - Begin deploying 802.11n APs
  - Upgrade TKIP encryption to AES
  - **Implement Captive Portal Network (CPN) wired conference room solution**
- Future work
  - Upgrade PEAP authentication to EAP-TLS -> terminate Employee wireless on Yellow (restricted) Network
  - WiFi in Limited Areas?

Conference Room CPN Motivations

- WiFi is not widely deployed yet, not currently permitted in large portions of the Lab.
- Wired network access in LLNL conference rooms has limited functionality
  - No DHCP – requires manual configuration to get on network
  - Some areas use MAC lockdown or keep conference room ports disabled by default due to lack of access control
- Desired conference room solution
  - Provide controlled access for both employees and guests
  - Guests use same credentials as guest wireless network
  - Isolate non-LLNL computers from LLNL computers at layer 2
  - Provide role-based access to appropriate network segment
    - Yellow for US Citizen Employees
    - Blue for Foreign National Employees
    - Green for Guests

CPN Notional Network Topology



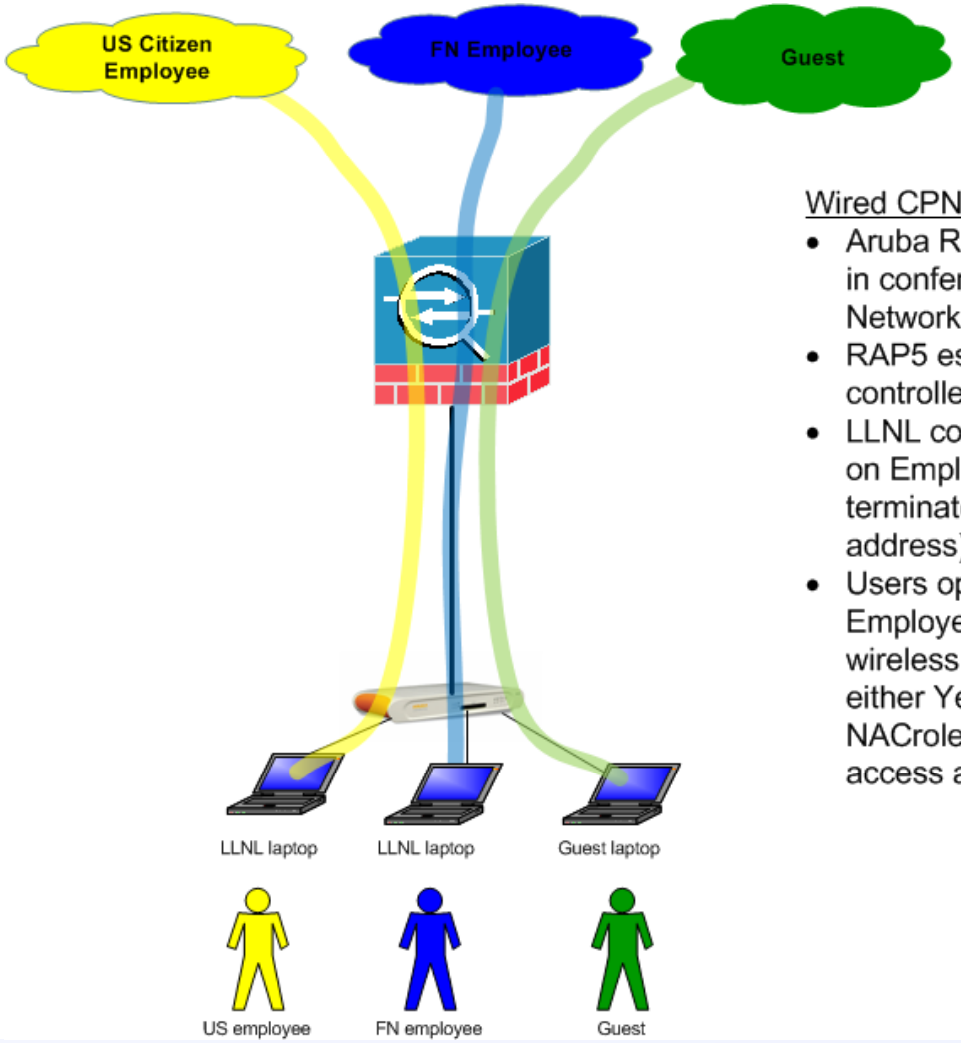
Aruba M3 Master Controller function:

- Terminates IPsec tunnels from RAP5 devices as well as wireless APs.
- Authenticates users against LLNL Active Directory or Guest RADIUS servers.
- Applies firewall policy based on user role.
- Routes user traffic to Internet or internal LLNL networks as appropriate.

Aruba RAP5 conference room switch function:

- Maintains IPsec tunnel to master controller over Yellow network.
- Assign device to proper VLAN (employee or guest) based on MAC verification.
- Routing and policy enforcement performed remotely on Master Controller.

CPN Usage Model



Wired CPN (Employee, Guest)

- Aruba Remote Access Points (RAP5) is deployed in conference rooms utilizing existing Yellow Network infrastructure.
- RAP5 establishes encrypted tunnel to Aruba M3 controller.
- LLNL computers that connect to RAP5 terminate on Employee CPN segment; non-LLNL computers terminate on Guest CPN segment (based on MAC address).
- Users open web browser and authenticate. Employees use AD credentials, guests use guest wireless credentials. Employees are granted either Yellow or Blue network access based on AD NACrole attribute. Guests receive Green network access after successful authentication.