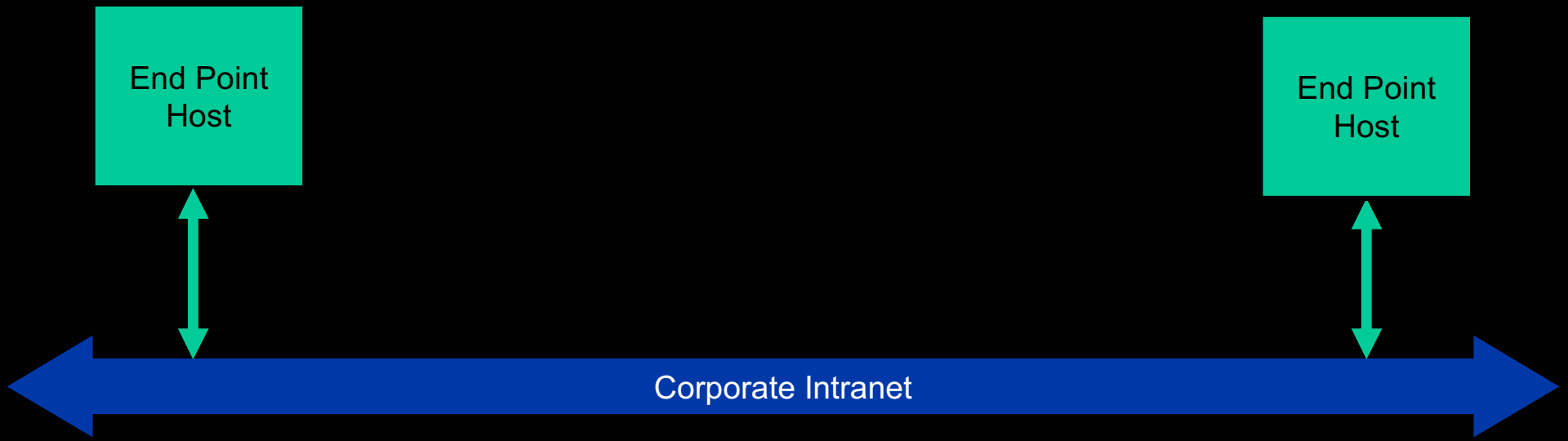
HIP-based Implementation of Secure Mobile Architecture (SMA)

Steven C. Venema
(Steven.C.Venema@Boeing.com)

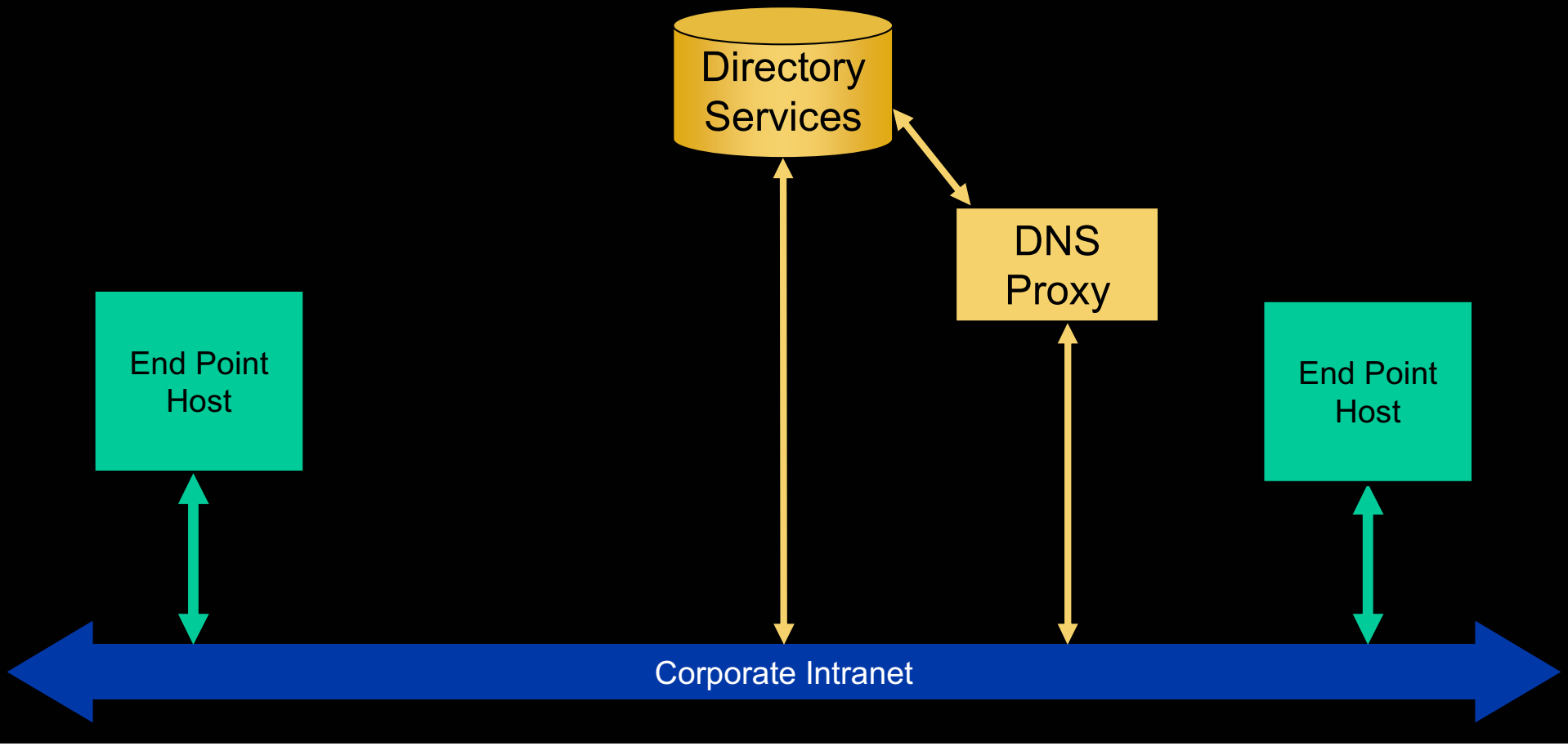
Boeing SMA Overview

- **Boeing implementation of SMA integrates HIP with…**
  - **Directory and Location services**
  - **Corporate PKI**
  - **Network-based policy enforcement**
- **Motivation**
  - **Network user diversity: Vendors, suppliers, guests**
    - **Need to limit who can access what resources**
  - **WLAN-equipped factory equipment: Access limitations**
  - **Roaming**
    - **External 802.11 service providers**
    - **Seamless roaming across diverse media (e.g., WLAN⇔Cellular)**
- **Benefits**
  - **Reduced network management complexity**
  - **Support mobility across arbitrary media**
  - **Identity and location-based access policy enforcement**

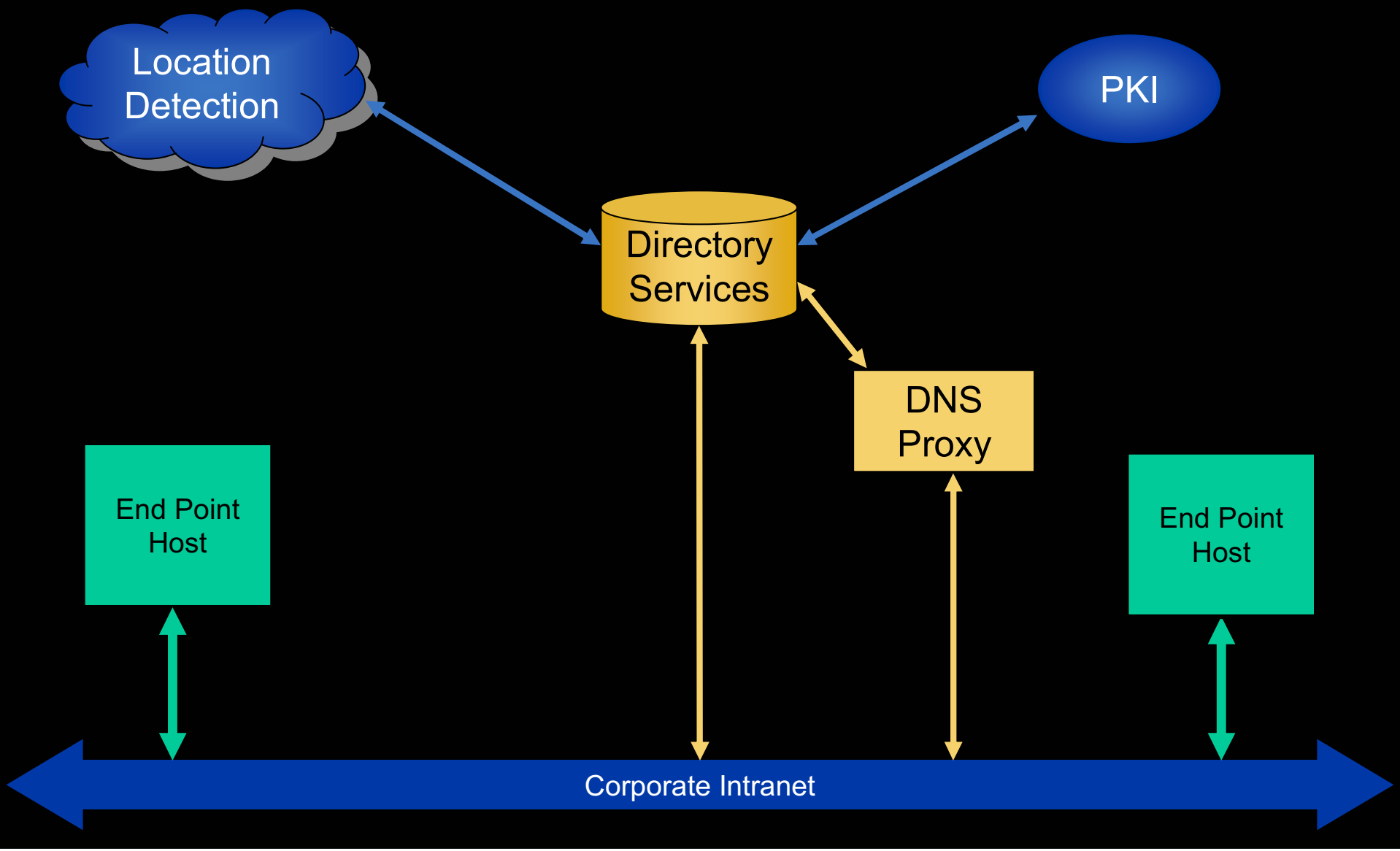
Boeing SMA Components



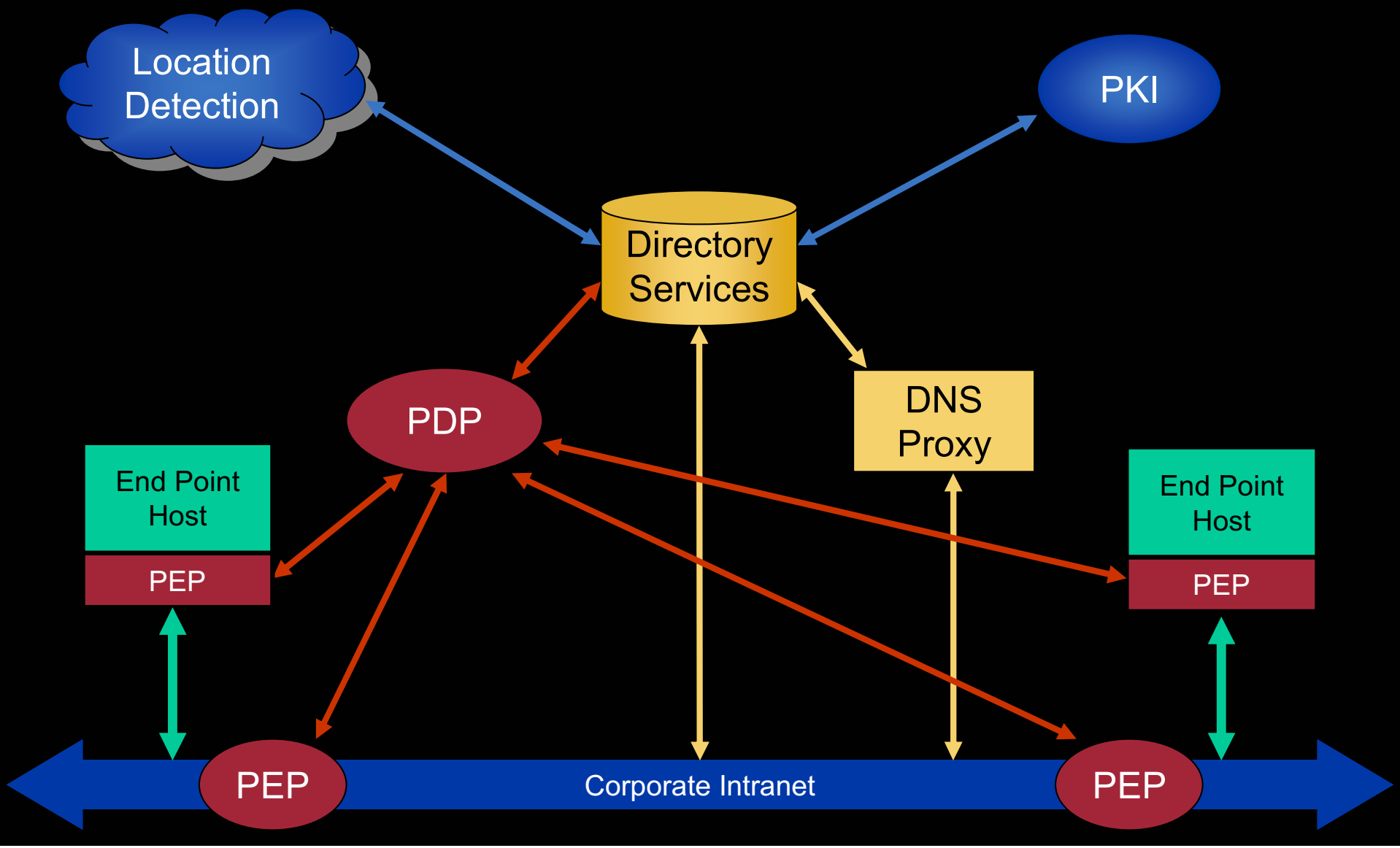
Boeing SMA Components



Boeing SMA Components

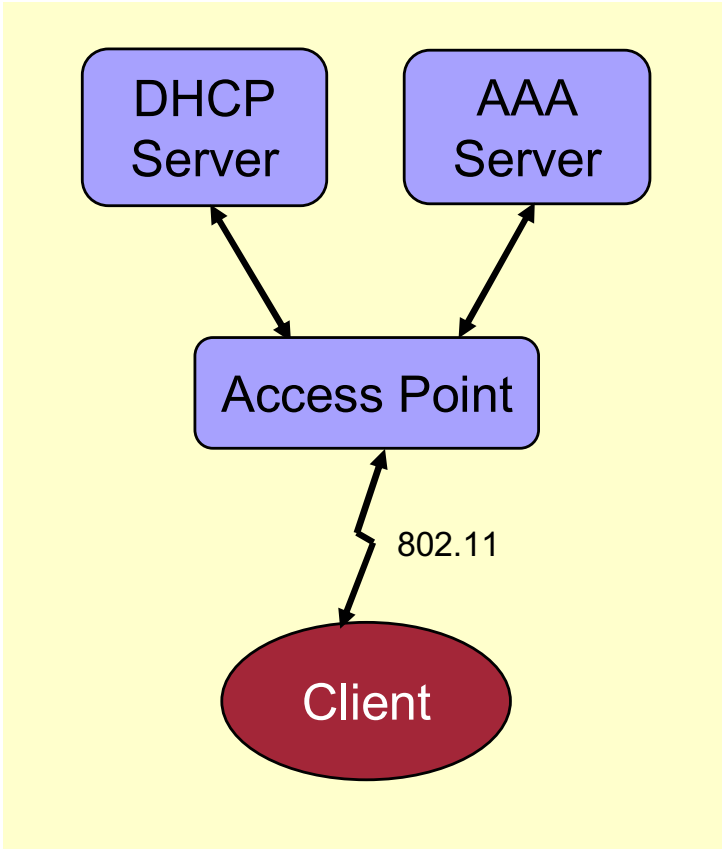


Boeing SMA Components

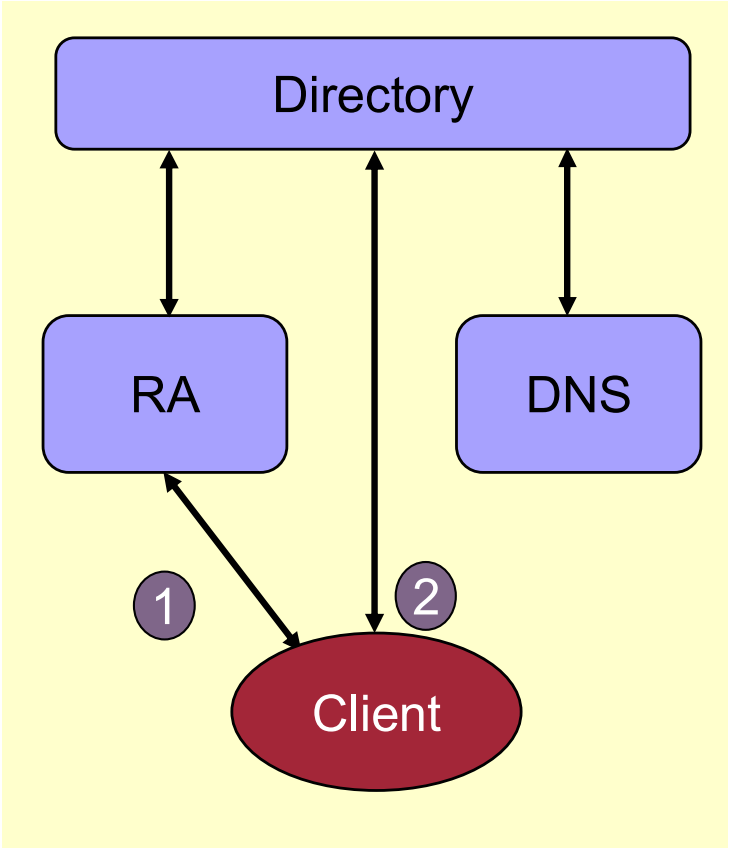


2-Stage Client Provisioning

Generic ISP Provisioning Process



Enterprise Provisioning Process



1) HardCert authentication for TempCert
2) Identity ⇔ IP Update in Directory

Boeing SMA Activities

- **2004: Operational laboratory testbed integrating**
  - **HIP-enabled wired/wireless endpoints**
  - **Smartcard identities tied to corporate PKI**
  - **Directory services with identity-based dynamic updates**
  - **DNS Proxy**
  - **Location services**
  - **Location-based policy enforcement**
- **2005: Scale into a ~100-unit deployment supporting**
  - **Linux & Windows clients**
  - **Cellular⇔WLAN seamless mobility**
  - **Middlebox-based policy enforcement**
  - **HIP-enabled proxies and concentrators**
  - **Publish/Subscribe architecture for efficient updates**

Issues

- **HIP Issues**
  - **Multi-user HIP endpoints and credentials**
  - **HIP Middleboxes for BITW policy enforcement**
  - **HIP Proxy for legacy equipment**
  - **HIP Multicast capability**
  - **HIP H/W acceleration for servers**

- **Related Issues**
  - **Data publication and coherency**
  - **Identity/Location-based network access policy**
    - **Definition, Decision, Enforcement**
  - **QoS**
  - **Deployment and interoperability**