Secure Mobility

Introduction

- Wireless Security vs Mobility Security
- LWAPP
- Key Mobility Characteristics to consider in your overall architecture
  - Roaming
  - Authentication
- NAC integration
- Firewall Integration
- IPS Integration
- CSA
- ASA

Wireless Security

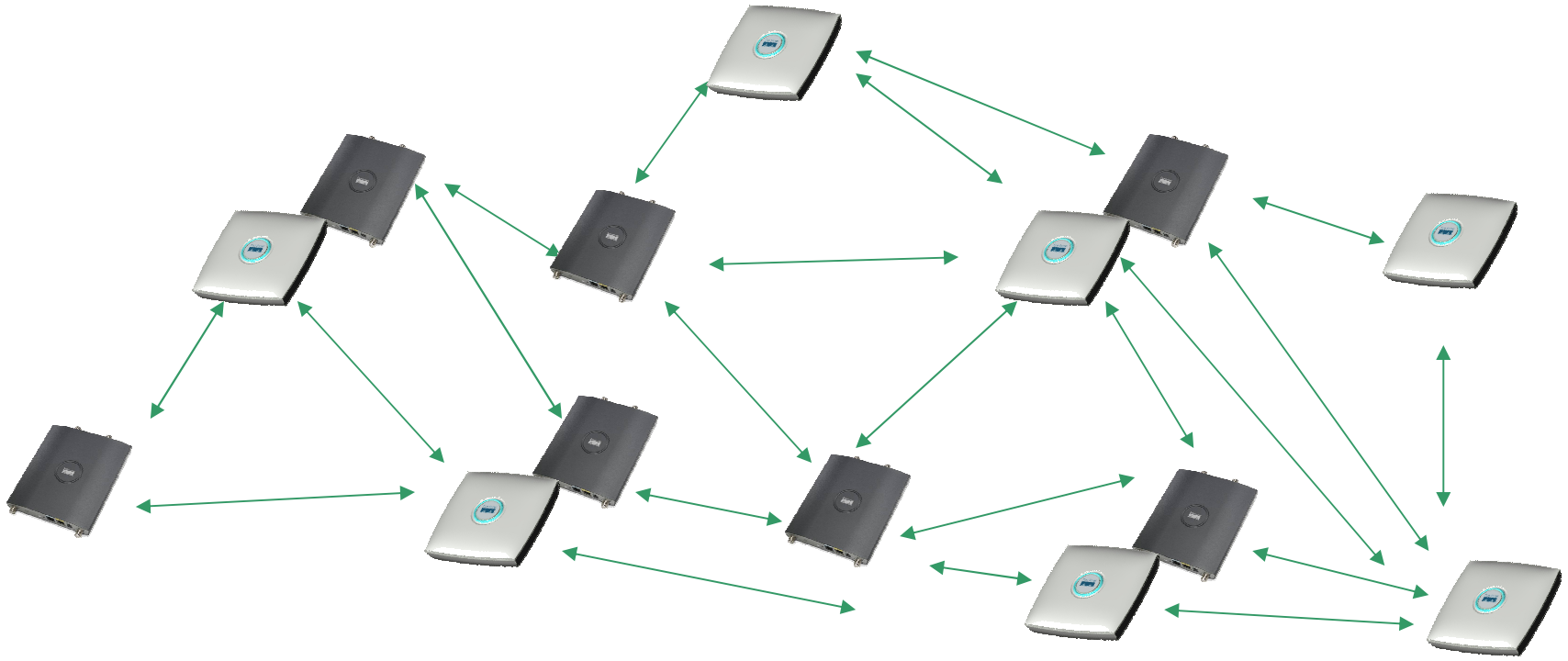
- Wireless Security is fundamentally a discussion about how to make a WLAN secure
- Cisco's WLAN products are industry leading, and world class

Mobility Security

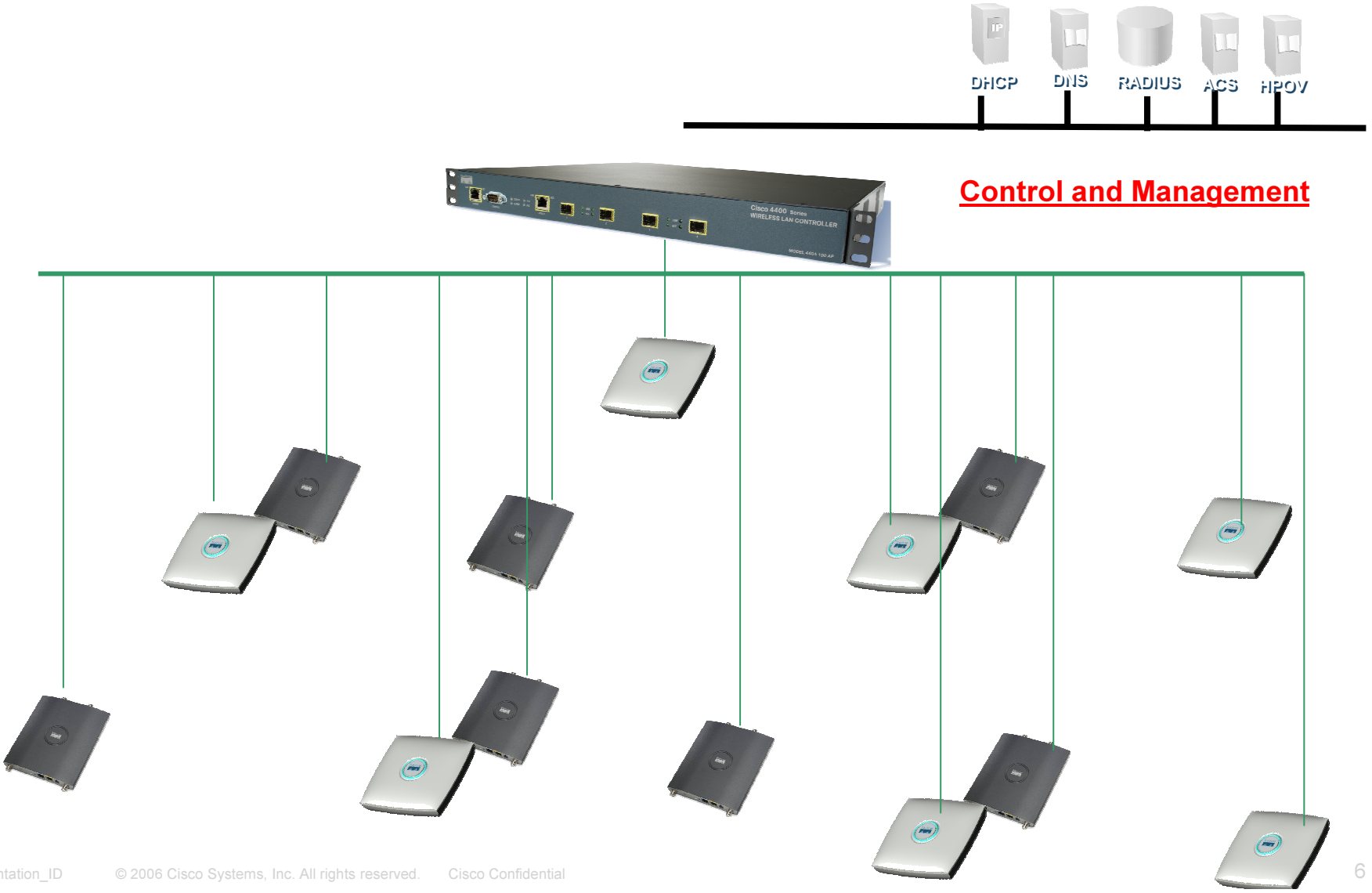
- Mobility Security is a discussion about how to protect your mobile devices, and how to protect your network from the impacts of mobility
- It is a discussion about integrating you wireless security plans with your overall network security plans.
- Wireless Security is still part of the discussion, but so is CSA, NAC, IPS, and Firewalls

Autonomous Deployments Originally Had Little Coordination

- Each AP had its own view of the network – like standalone cell towers
- No hierarchical view of the RF – or the network



Enter The Controller

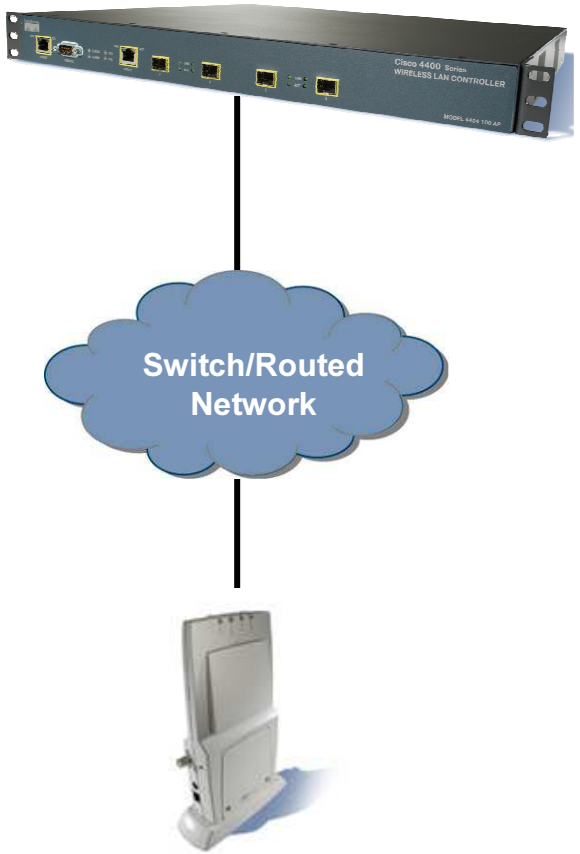


Basic Principals of The Controller

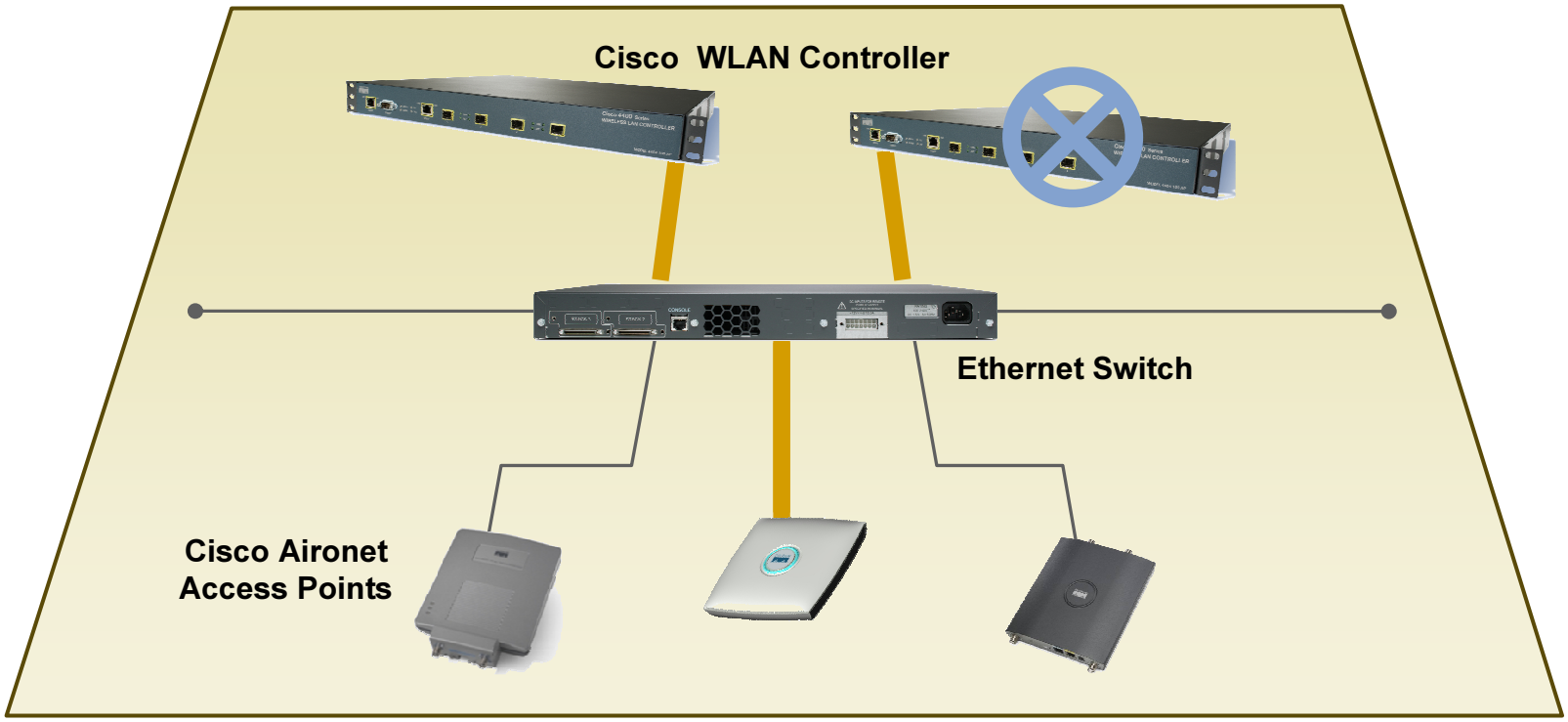
- All access to network resources goes through the controller
  - RADIUS
  - DHCP
  - DNS
- Controller acts as security gateway for clients
- Manages all access points on the network
- No need to resubnet the network for deployment
- A standardized protocol was needed….

LWAPP the Protocol for Centralization

- Defines the authentication and control of wireless access points
- Provides standard interface between controllers and lightweight access points
- Enables flexible deployments
- Each AP is effectively a remote interface on the controller
- Allows controller to:
  - Control the AP channel and power
  - Manage encryption / authentication
  - Deliver wireless prevention/protection
  - Better capacity management
  - Centralized management
  - Dynamic control

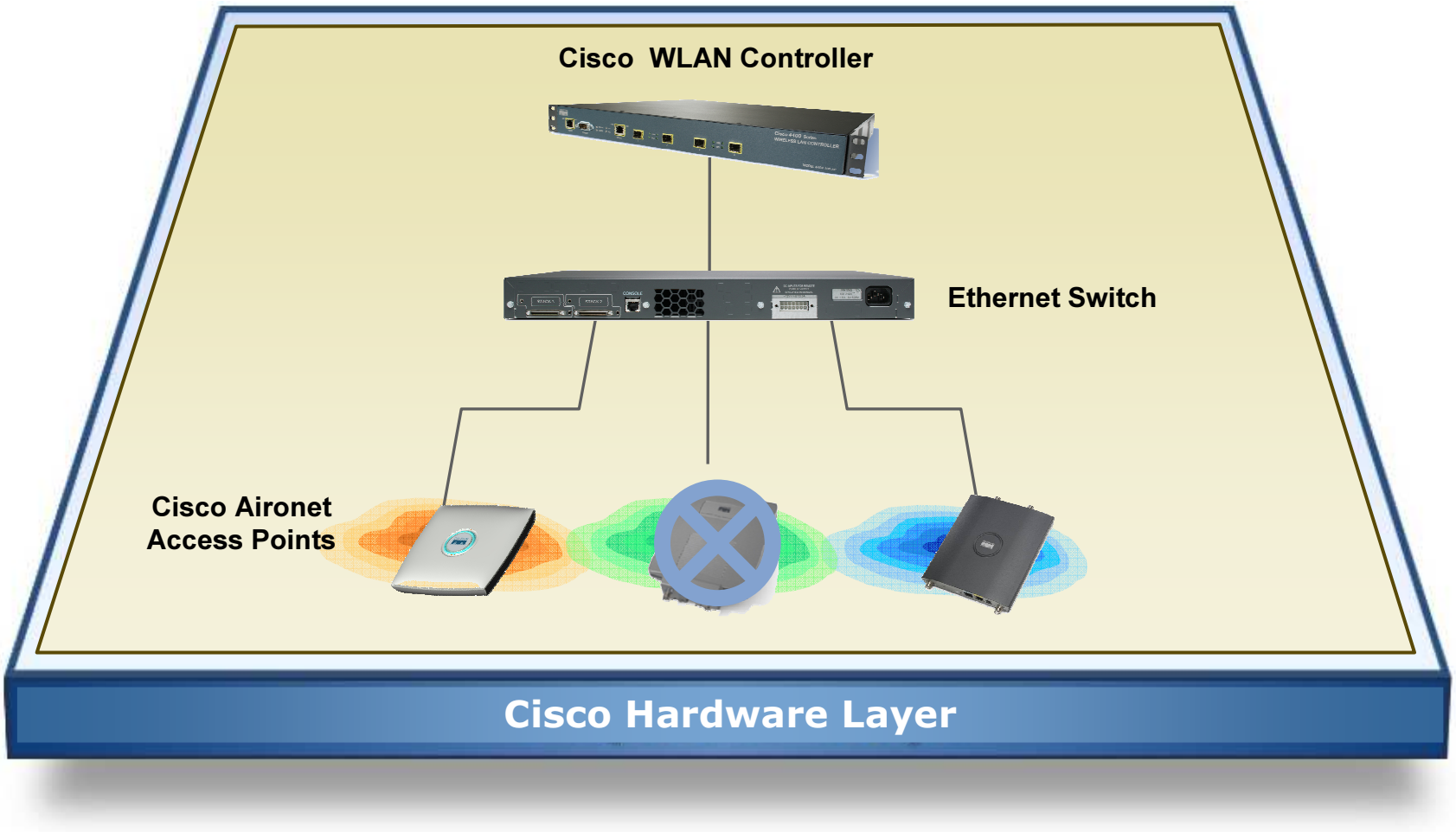


LWAPP Delivers Network Reliability



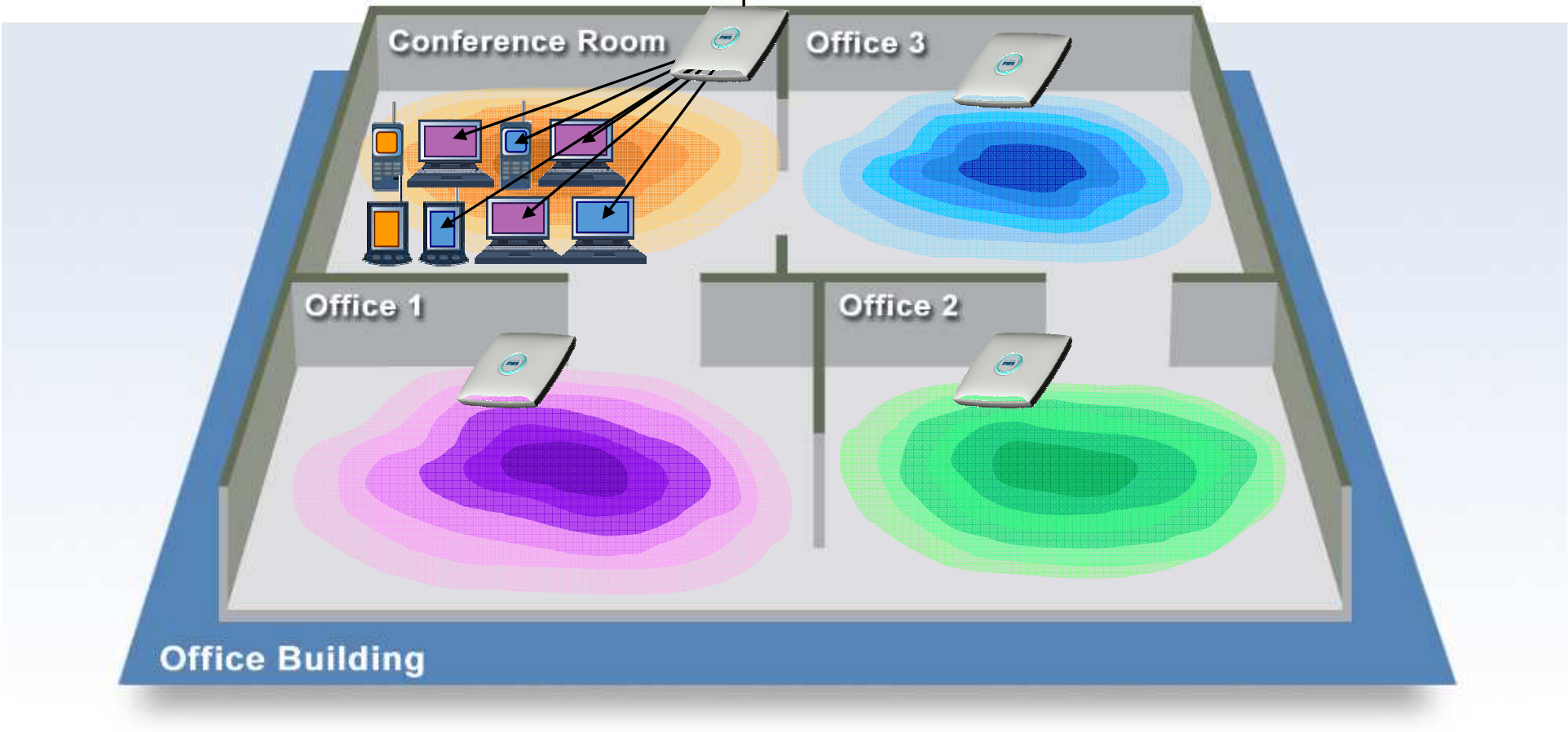
Cisco Hardware Layer

Centralization Delivers RF Reliability



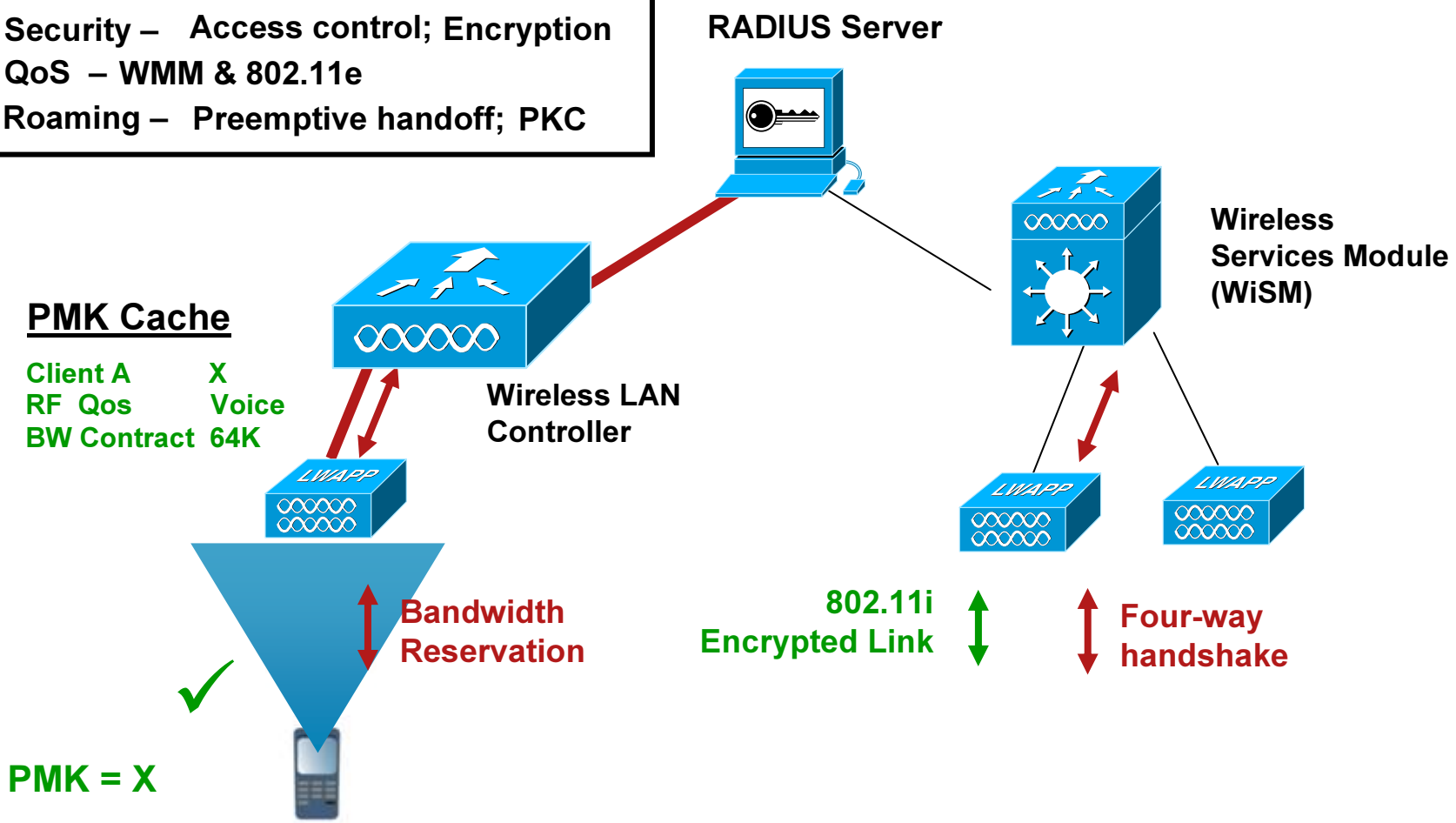
Improved Performance Per User

Solving Performance & Capacity problems in high density areas (e.g. conference rooms, cafeteria)…



Improved Roaming

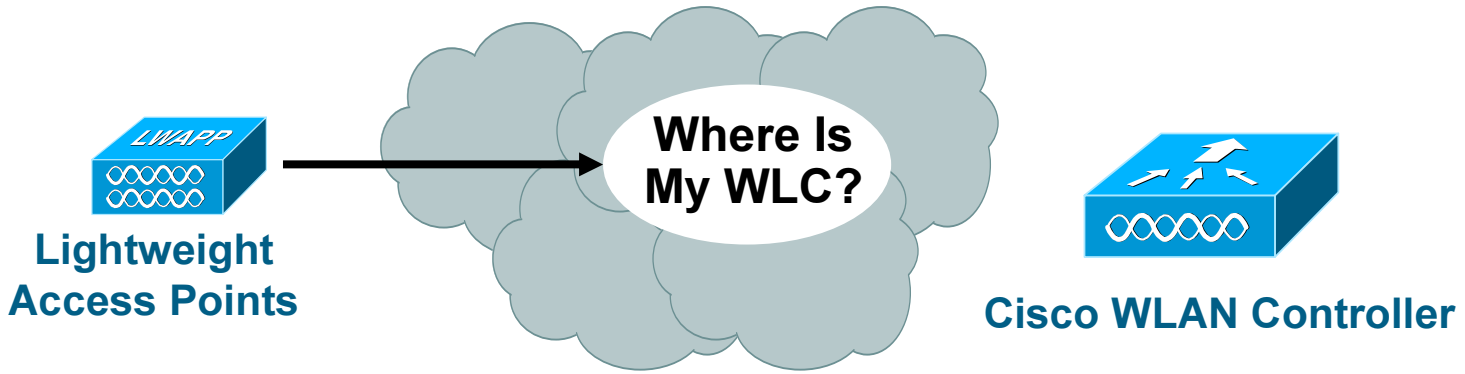
1. Security – Access control; Encryption
2. QoS – WMM & 802.11e
3. Roaming – Preemptive handoff; PKC



Architecture Deployment

Access Points Need to Be Associated with WLAN Controller

- Hunting phase: AP needs to find WLC
- Join phase: AP associates securely with WLC
- Authorization phase: WLC accept or not AP
- Configuration phase: WLC upload firmware (if needed), WLC upload AP configuration



Mobility Products

2700 Location Appliance

3rd Party Products

WiSM (6500)

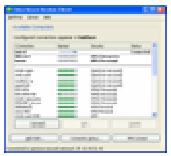
4402 / 4404

WLCM (ISR)

Catalyst 3750G

2100

Antennas & Accessories



Cisco Secure Services Client 802.1x

Cisco 3200 Series

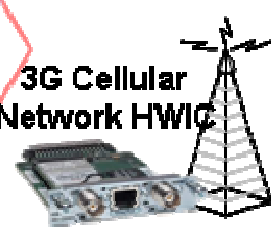
7900's & Dual Mode

1510 Mesh AP

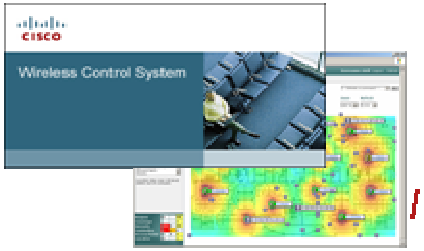
1520 Mesh AP

1400 / 1300 Outdoor Bridges

Broadband Wireless (WiMax)



3G Cellular Network HWIC



WCS / Navigator

Cisco Secure ACS

NAC Appliance / Cisco IPS / CS-MARS / NAC Guest Server

Cisco Spectrum Intelligence

Cisco Compatible Extensions (CCX)

Mobility Express

WLC 526

UC 500

521G

CE 520

Ruggedized

1242G 1242AG

1231G 1232AG

AP1250 (Modular)

1131G 1131AG

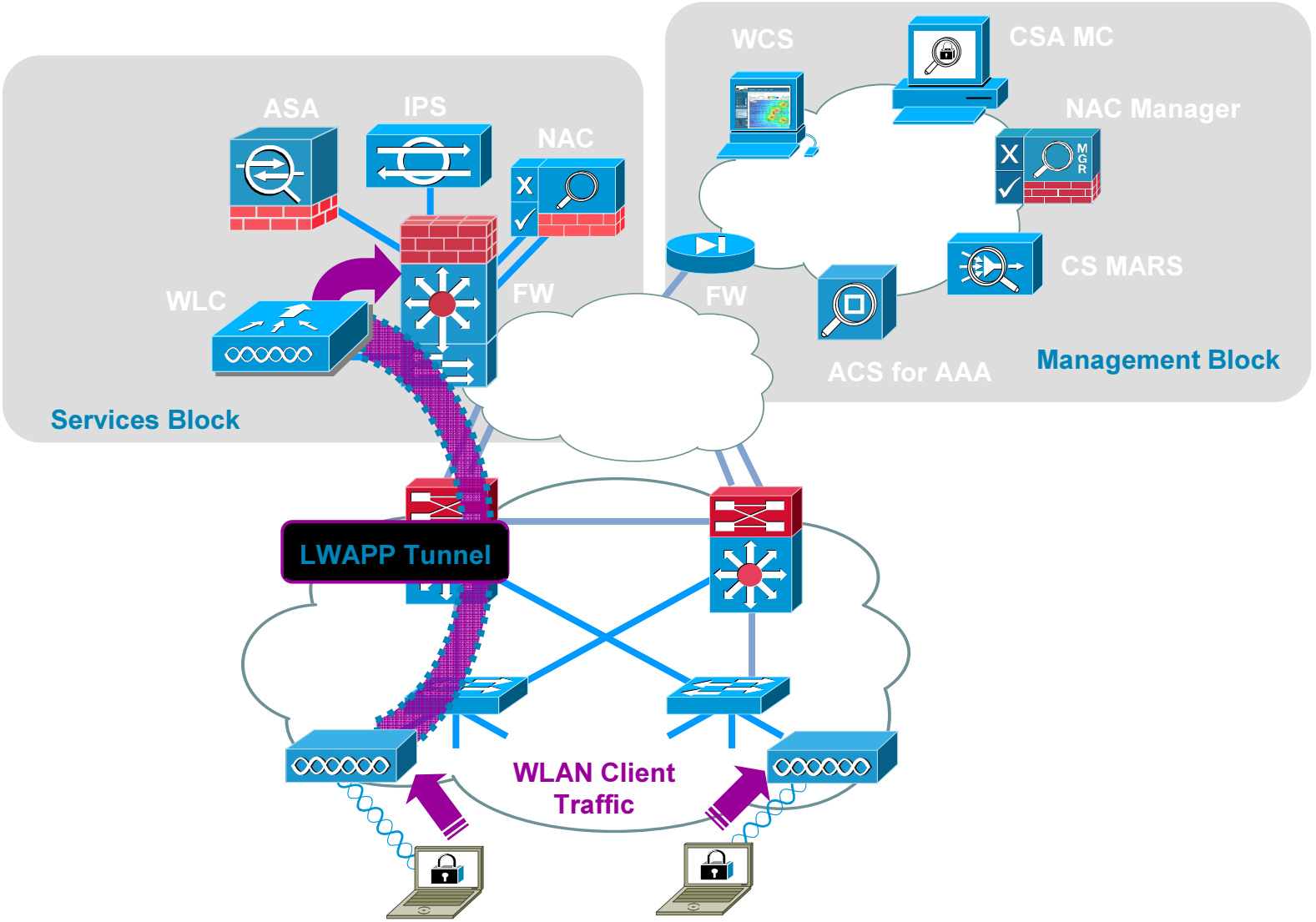
Office

1121G

850W, 870W, 1800W, HWIC-AP

521G (SMB)

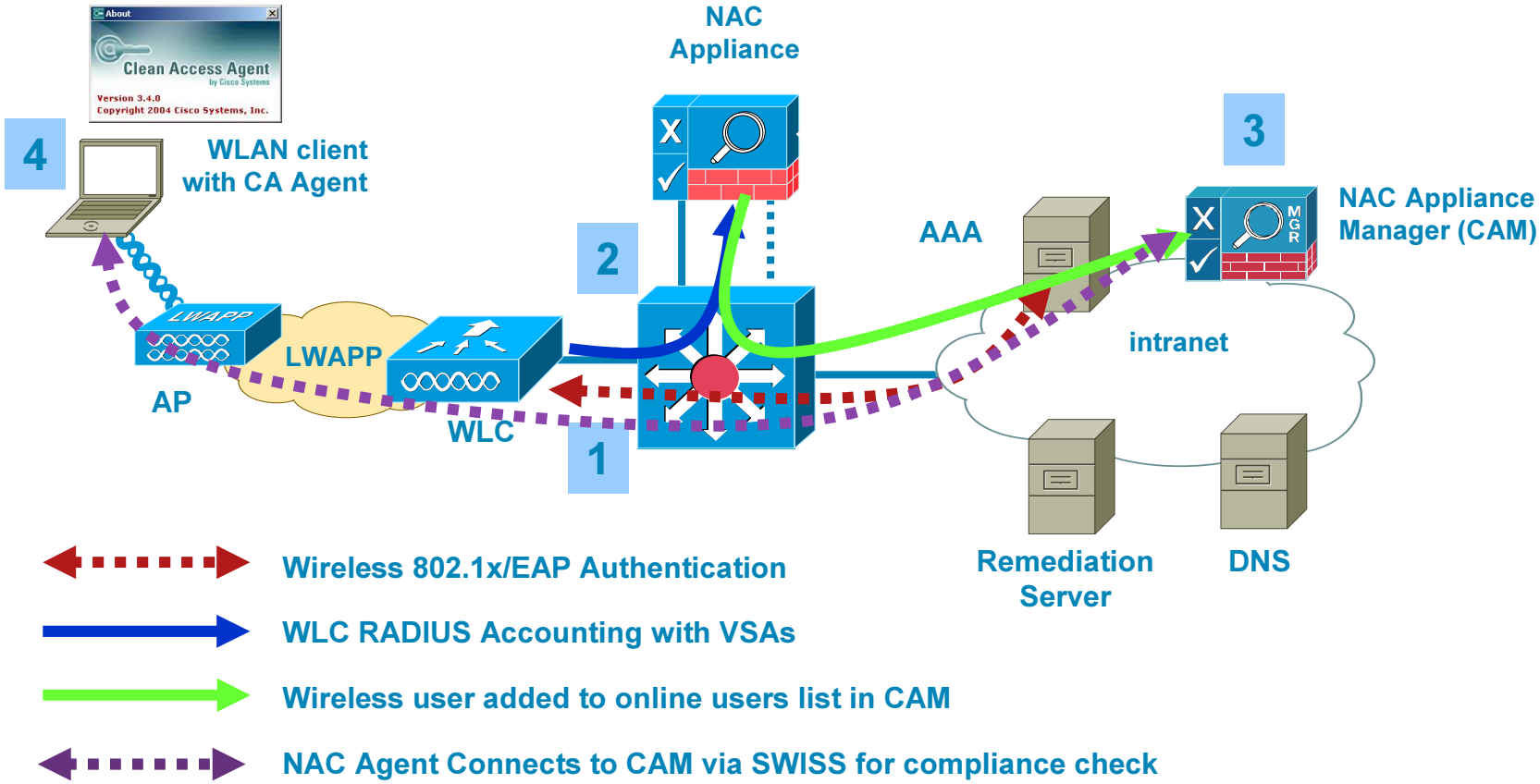
Secure WLAN Solution Architecture



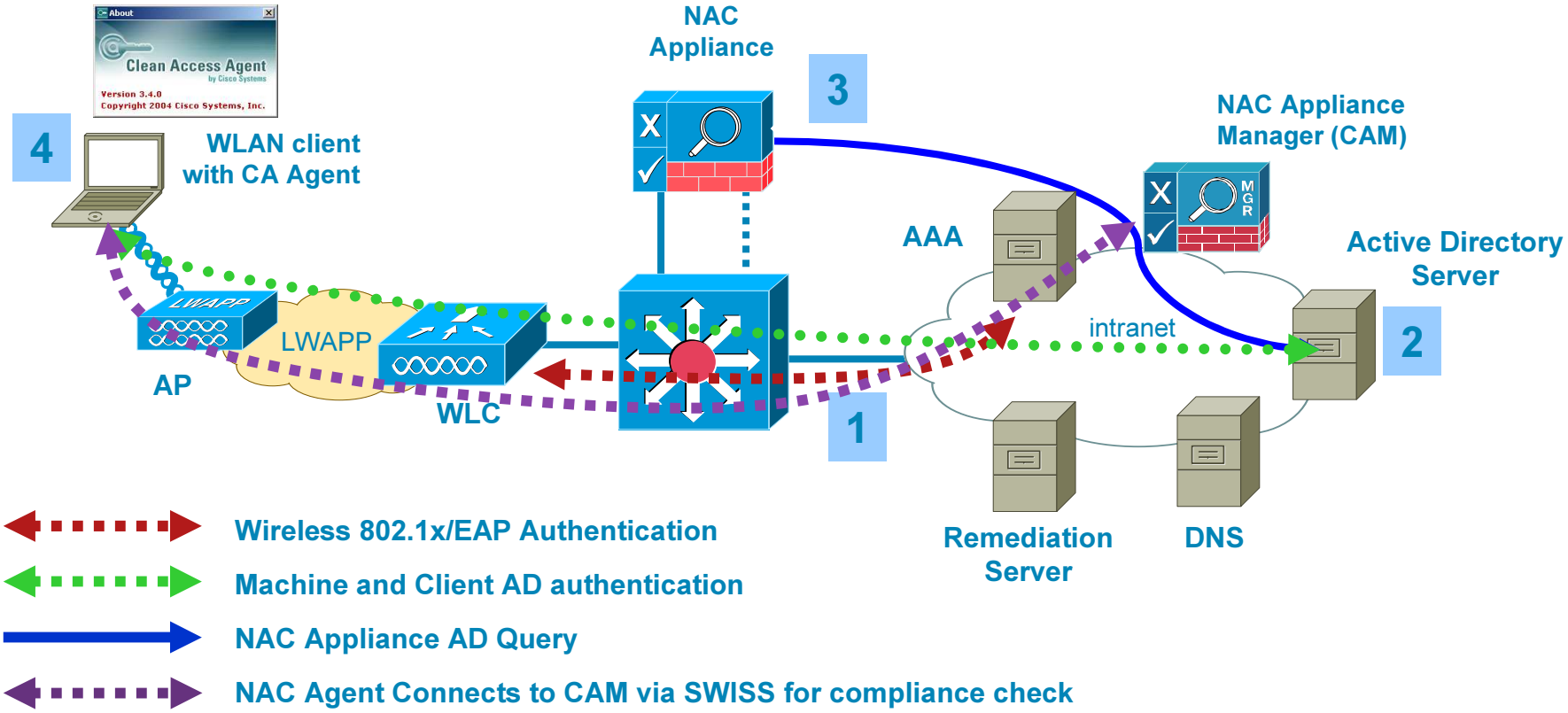
WLAN clients with NAC Agent, CSA, CSSC

NAC Appliance integration with the CUWN

NAC Appliance Integration on a WLAN: VPN SSO

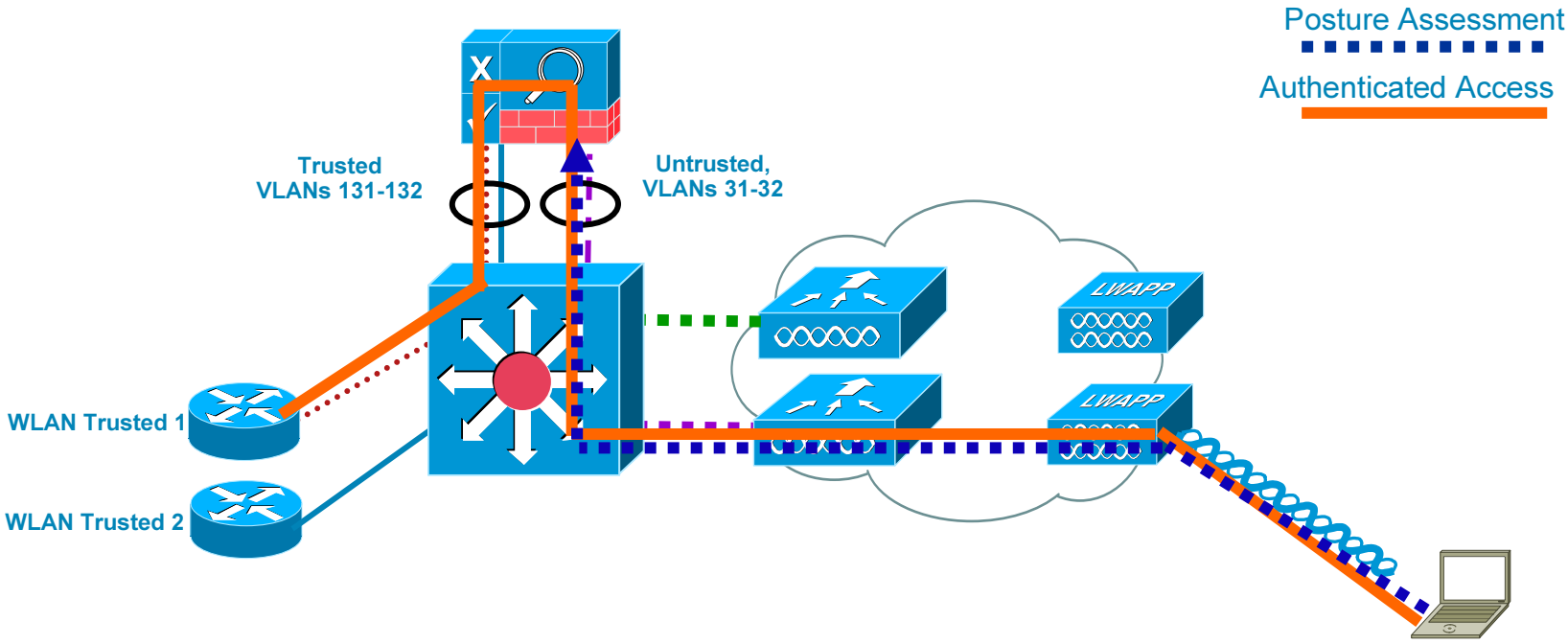


NAC Appliance Integration on a WLAN: Active Directory SSO



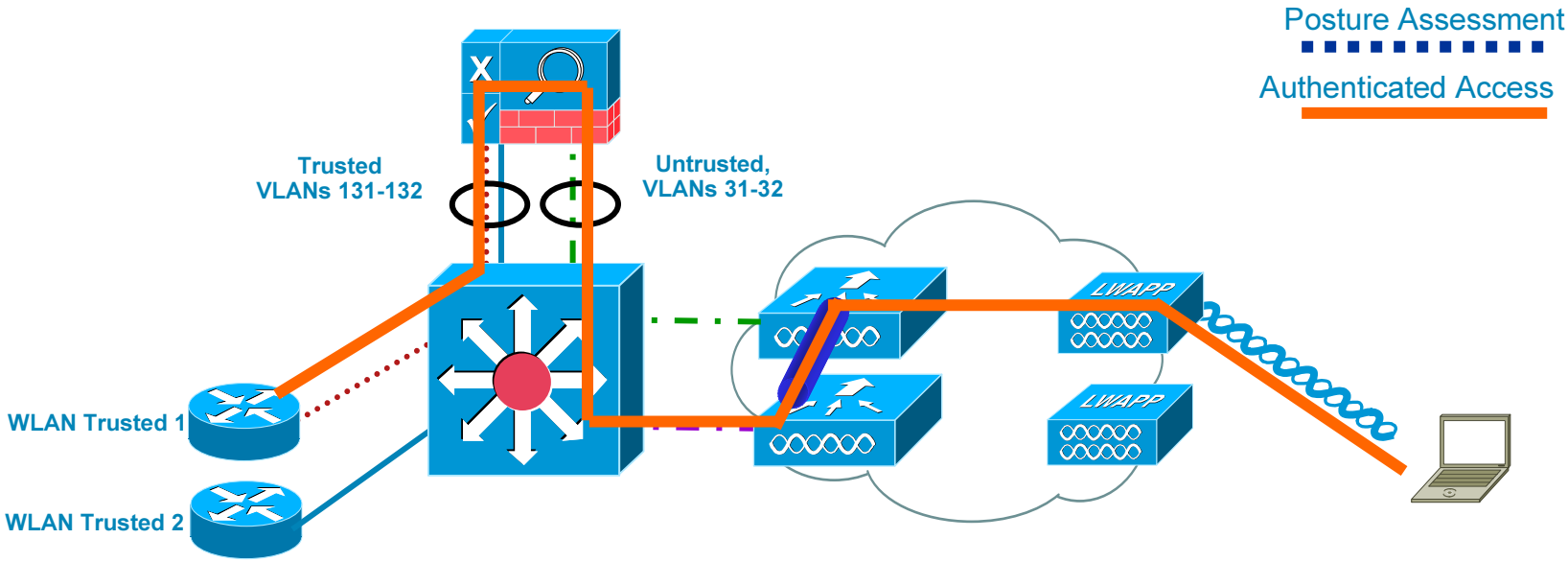
NAC Appliance and Wireless Roaming Considerations: Layer 3 Roaming

Connectivity Before L3 Roam



NAC Appliance and Wireless Roaming Considerations: Layer 3 Roaming

Connectivity After L3 Roam (Symmetrical Tunnel)

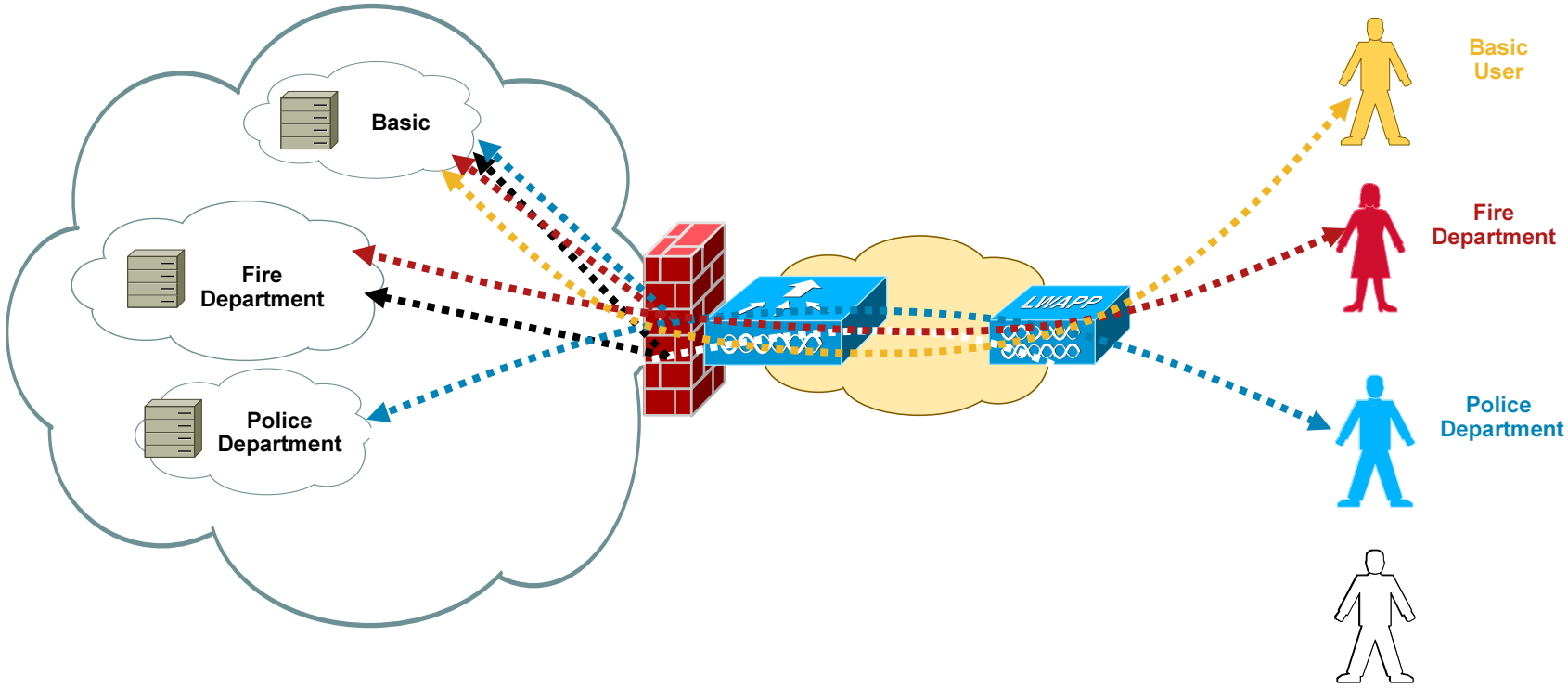


Firewall Integration with the CUWN

User Group Access Policy Enforcement

Firewall Integration on a WLAN Sample Scenario

- To separate users ACL's may suffice, but legal or policy reasons may require a firewall
- Different firewall policies are required for different classes of users sharing the same WLAN infrastructure



User Group Access Policy Enforcement

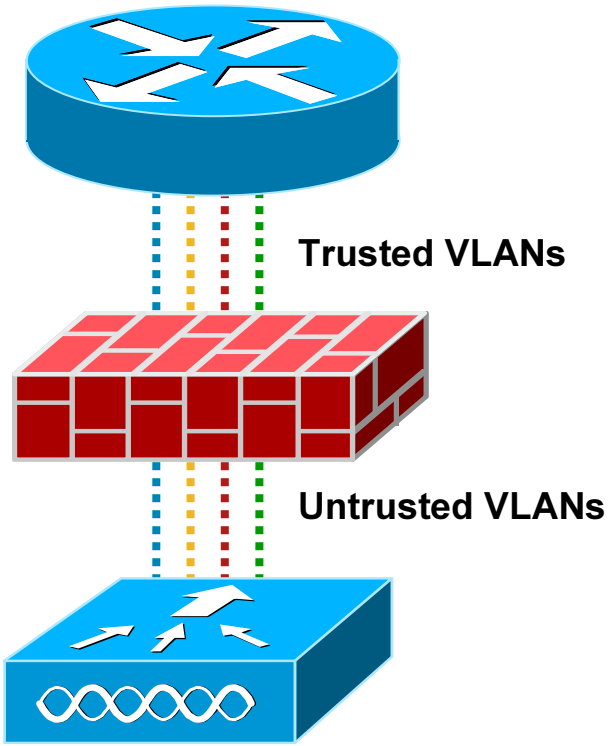
Firewall Integration on a WLAN Sample Scenario

- Restricts user group access to permitted network resources only
- 802.1X allows a common WLAN but different user group VLAN assignment based upon AAA policy

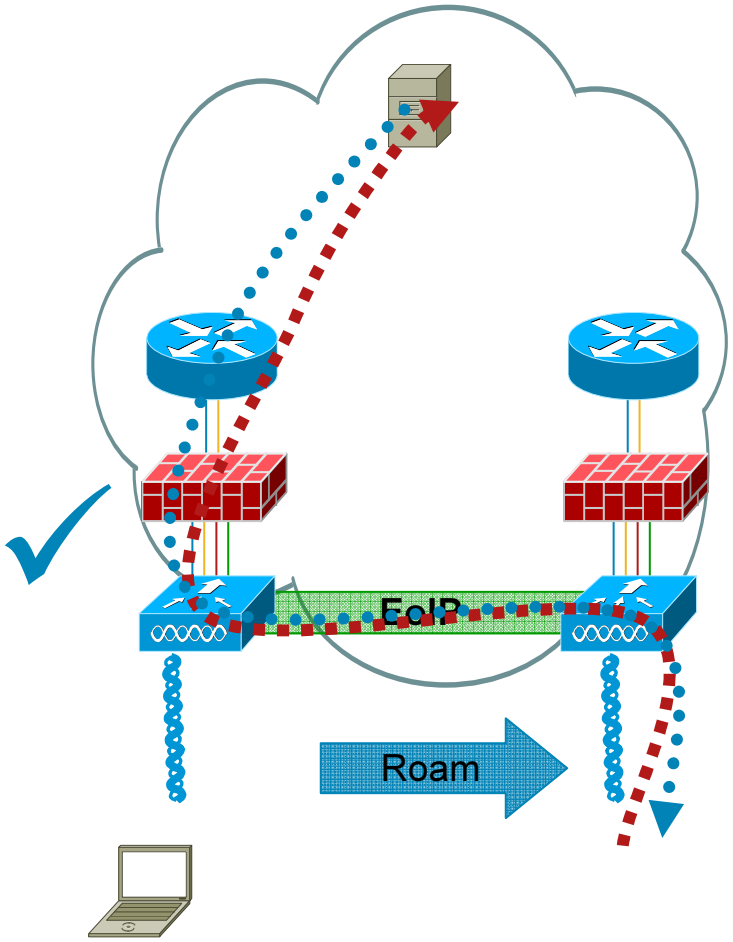
  Single SSID with RADIUS-assigned VLAN upon successful 802.1X/EAP authentication
- VLAN mapped to different firewall VLANs and subject to different firewall policy

  VLAN mapped to a specific virtual context (user group) in the firewall

  Firewall policy enforced per user group
- Design Guide Example uses multiple contexts, and transparent mode



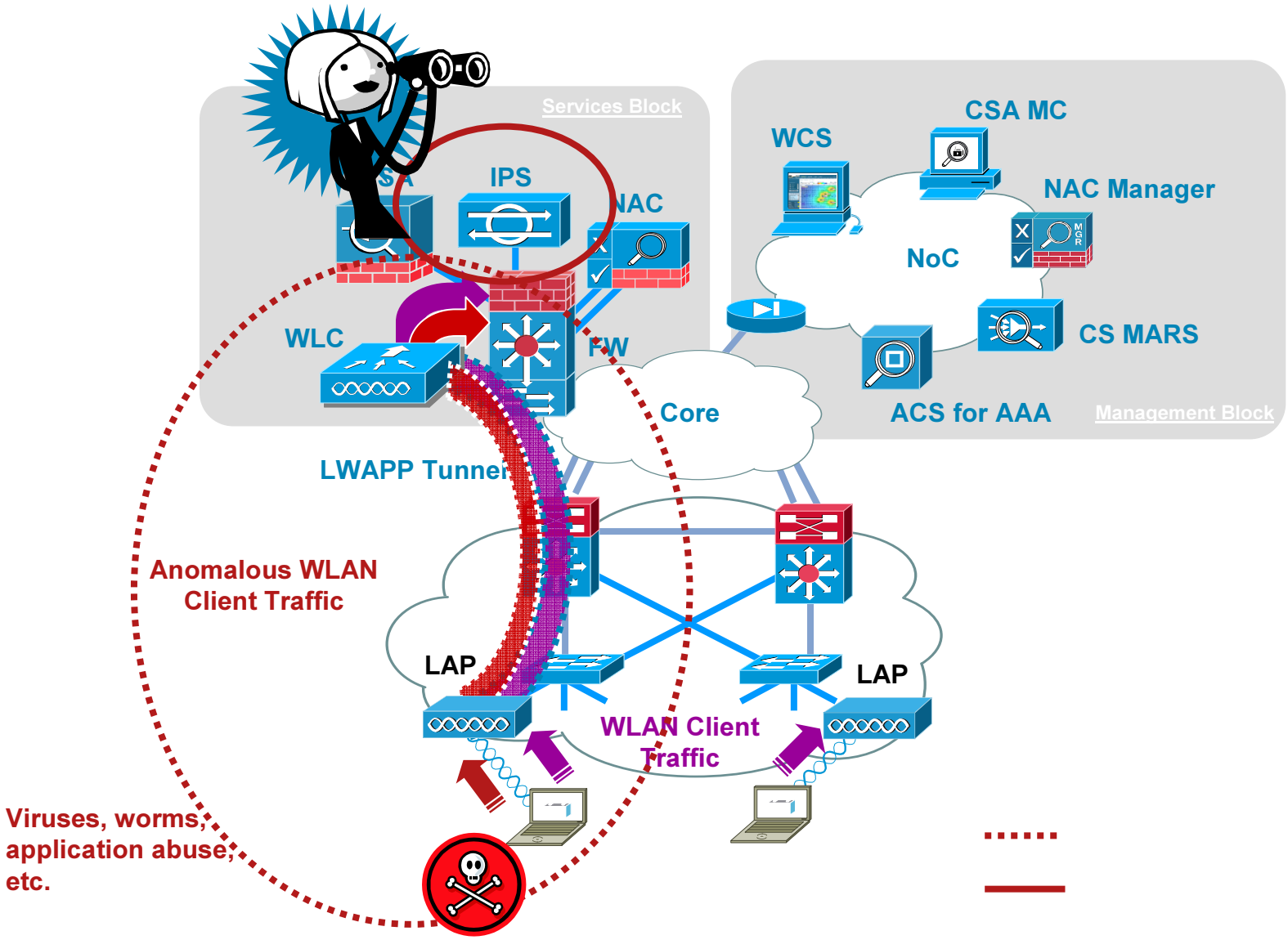
Firewalls and Wireless Roaming: Symmetric Roaming



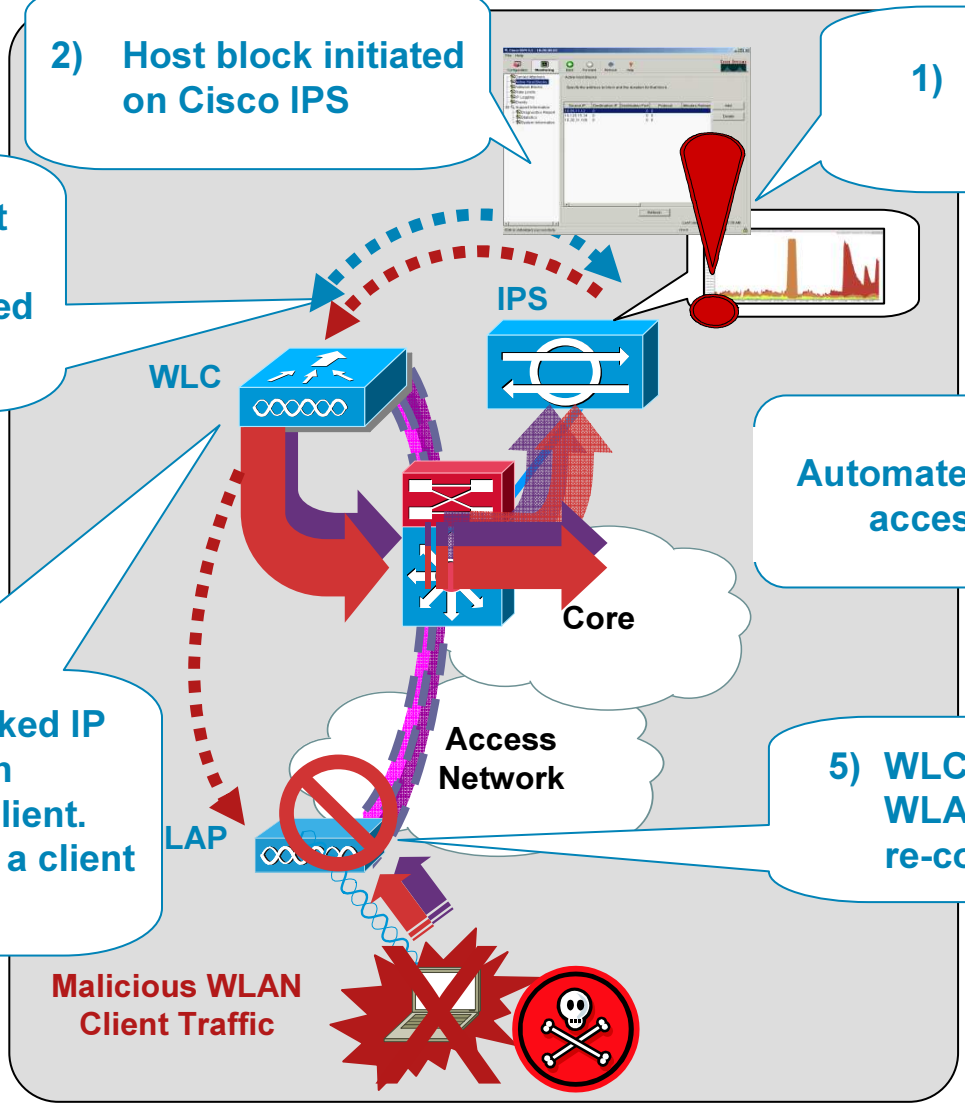
- Client Roams
- Traffic to client is tunneled
- Traffic from client is tunneled
- Symmetric roaming feature ensures all client traffic goes through the same firewall
- Firewall state information is maintained and client traffic continues

IPS and CUWN Integration

Cisco IPS for General Client Traffic Threats and Anomalies

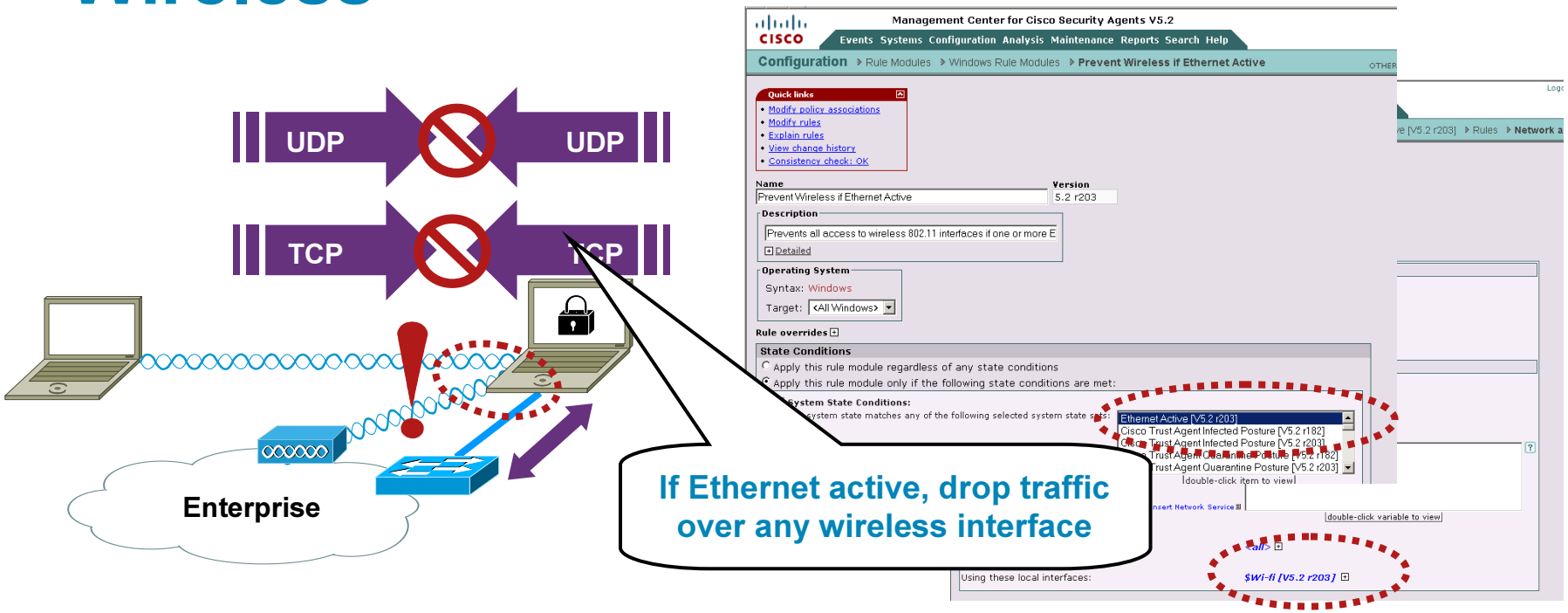


Cisco WLC and IPS Integration for Automated Threat Mitigation



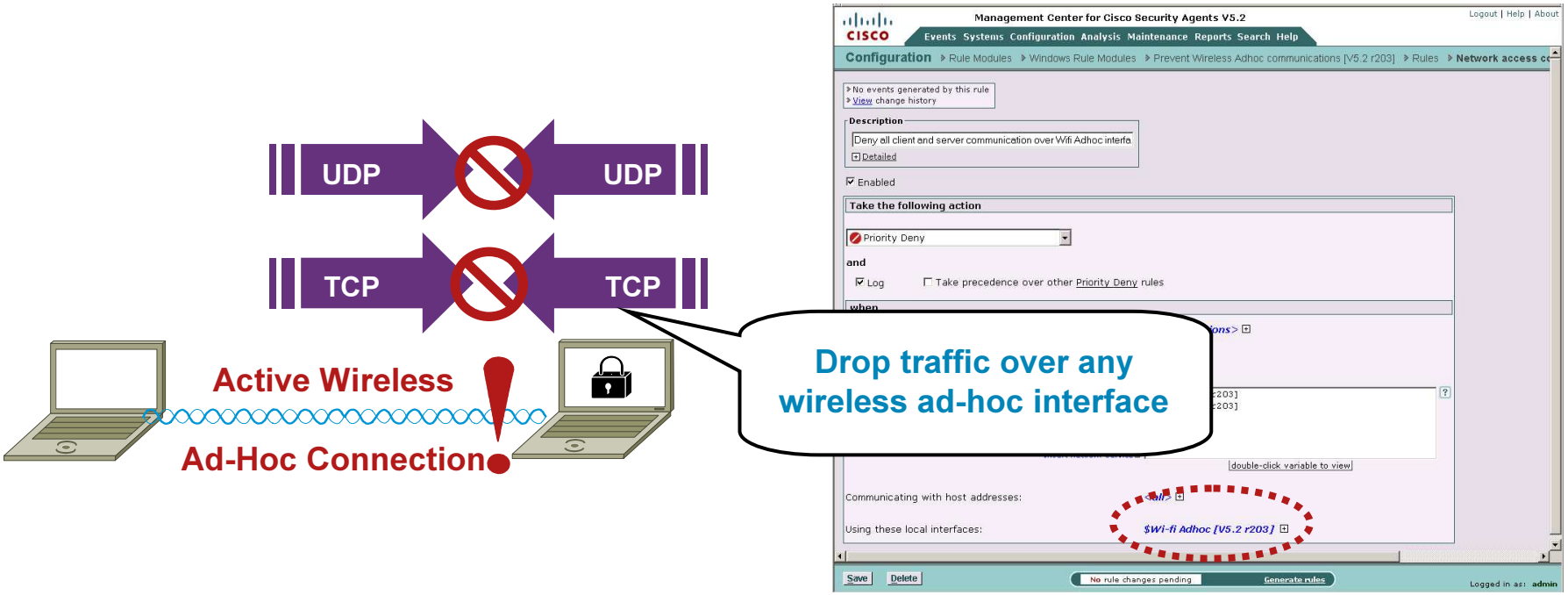
CSA and WLANs

CSA for Simultaneous Wired and Wireless



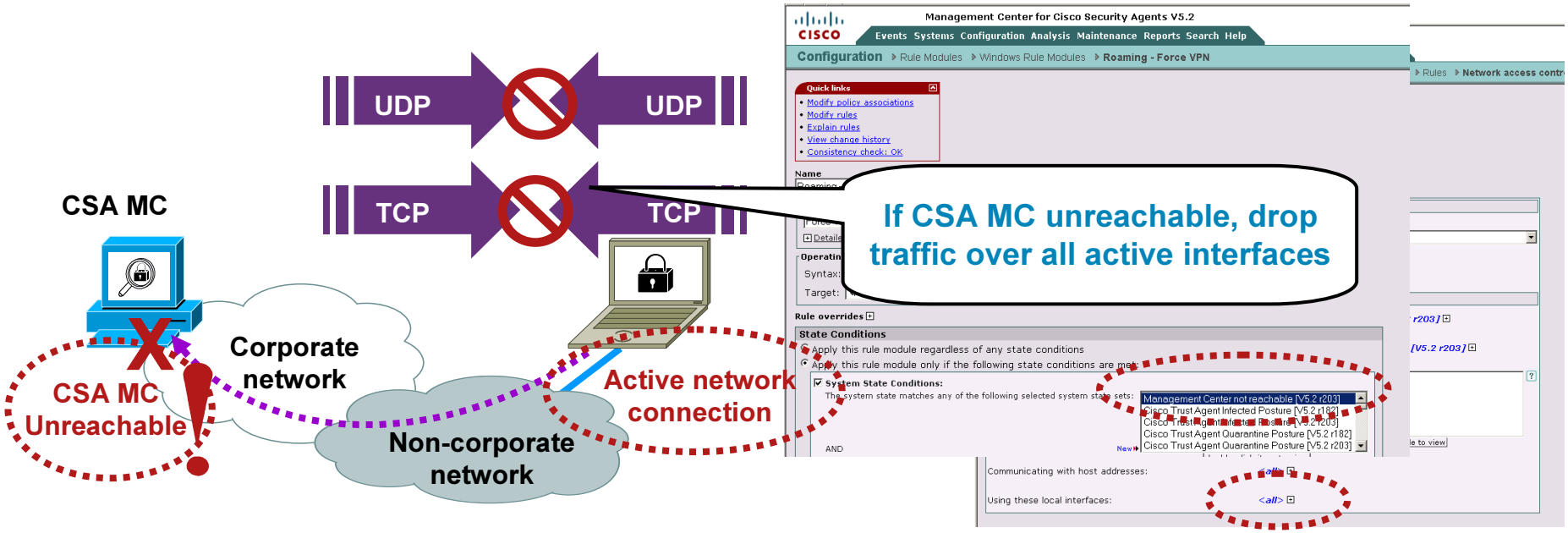
- **Prevent bridging of unauthorized devices into corporate network**
  - If both an Ethernet and a wireless connection are active, filter all wireless traffic
  - No impact on wired interface traffic
- **If using CSSC supplicant, leverage its simultaneous wired and wireless feature to disable WLAN connections when a wired connection is active**

CSA for Wireless Ad-Hoc Connections



- Prevent unauthorized and insecure wireless ad-hoc connections
  - Filter traffic over any wireless ad-hoc connection
- Complement with monitoring of wireless ad-hoc connections from network-side
  - Wireless IDS/IPS features of the WLC

CSA for Forcing Corporate Connectivity



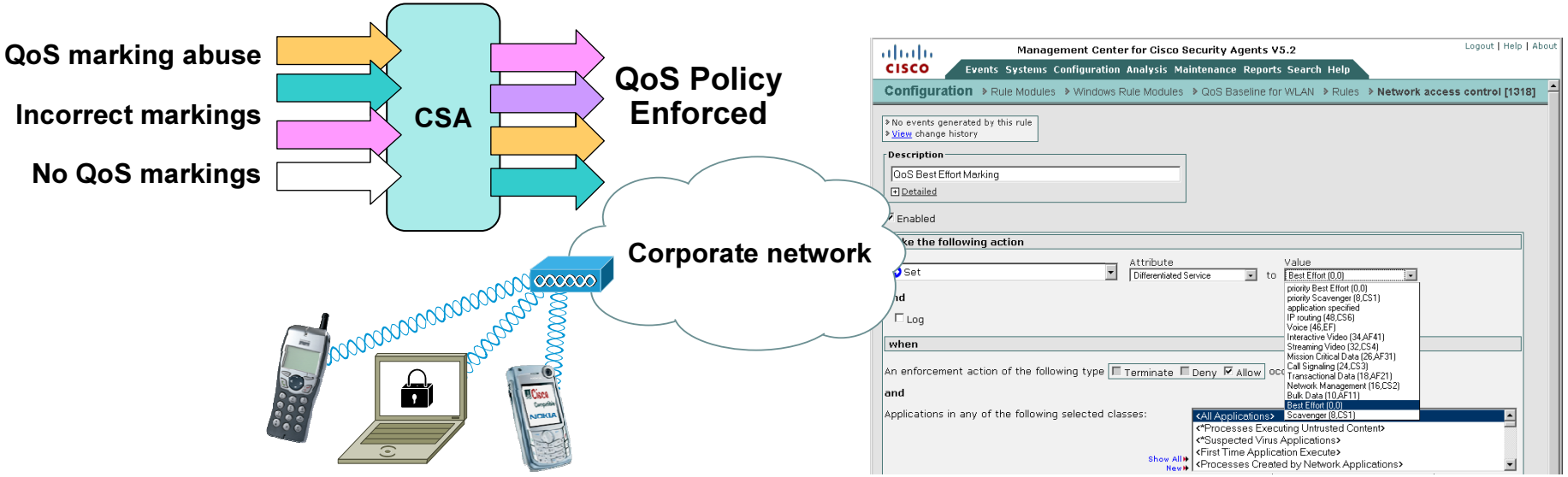
- Force connectivity to corporate network when out of office

  If a network connection is active AND the CSA MC is unreachable, filter all network traffic until the CSA MC is reachable

  HTTP/HTTPS allowed for 5 minutes to allow hotspot sign-up

  Pop-up notifies user to connect their VPN

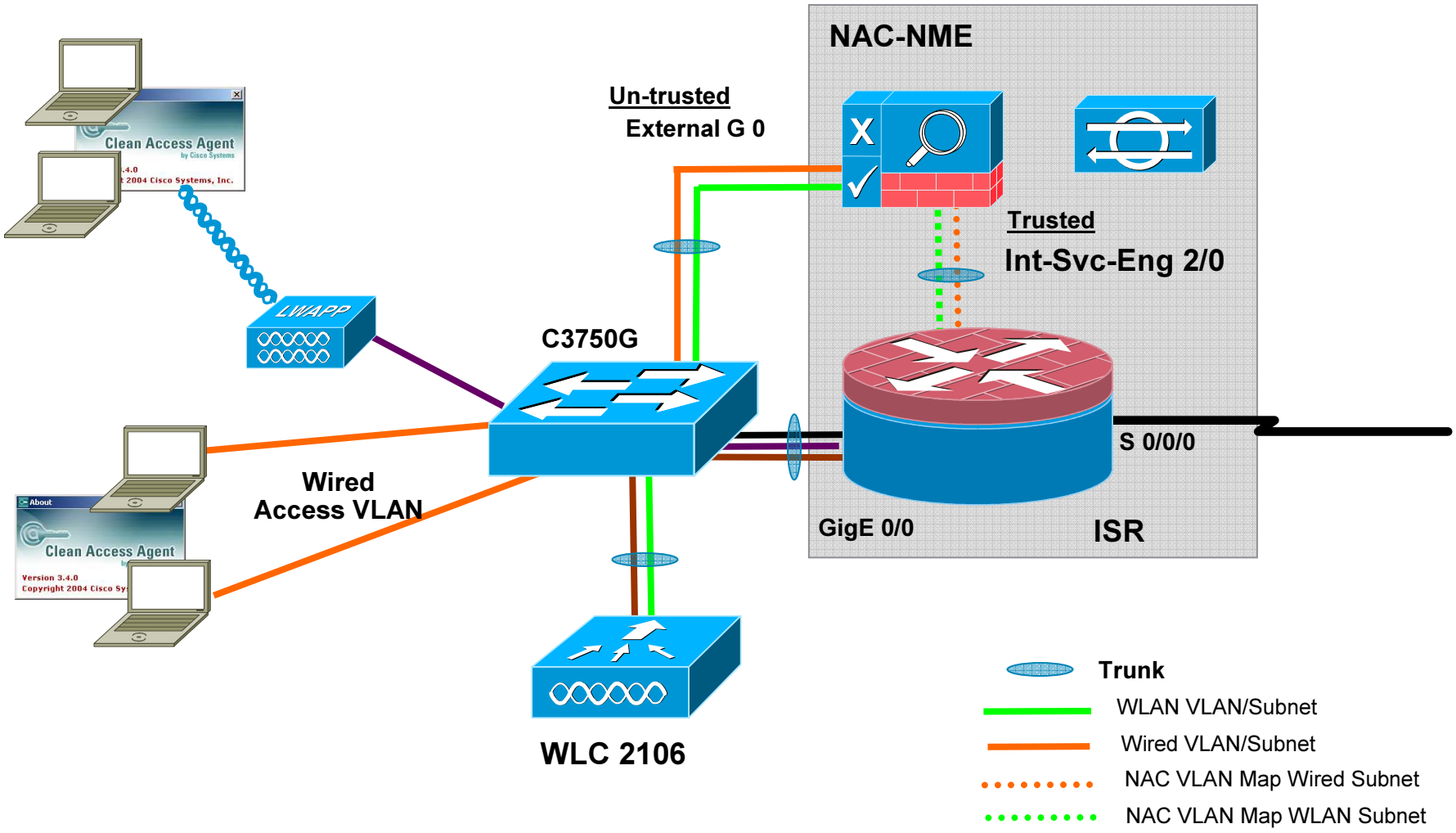
CSA for Upstream 802.11 QoS Policy



- Ensure resiliency of business critical & latency-sensitive applications
  - Enforce QoS policy on the 802.11 RF medium
    - Prevent QoS marking abuse and misuse by 802.11e & WMM devices
    - Enable QoS marking for legacy devices and applications
- CSA Trusted Endpoint QoS
  - Sets or re-marks upstream QoS markings to ensure traffic is classified and prioritized according to policy
  - At a minimum, mark all traffic as best effort

Secure Mobility - Branch

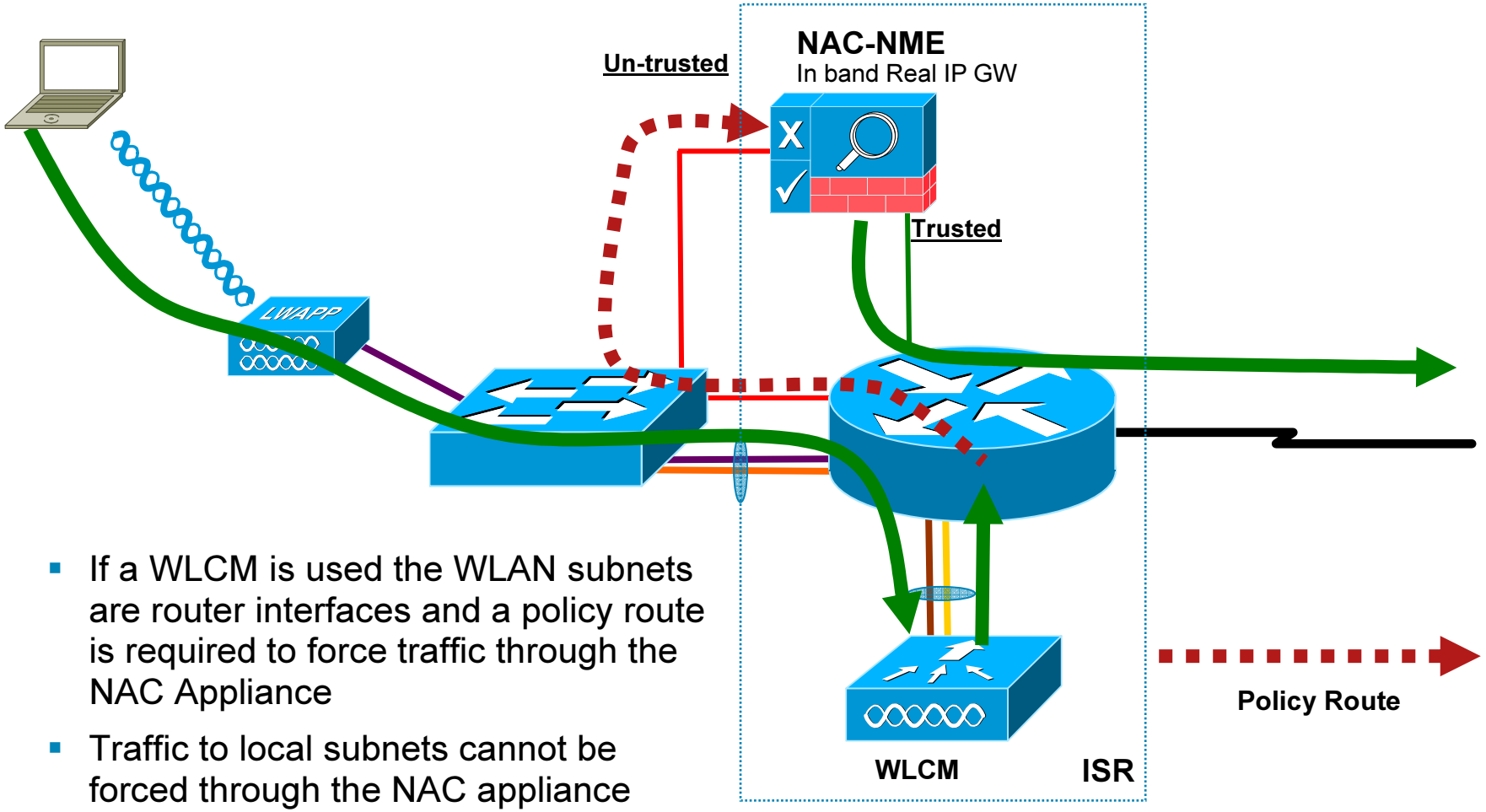
Basic Branch Topology



Branch Summary

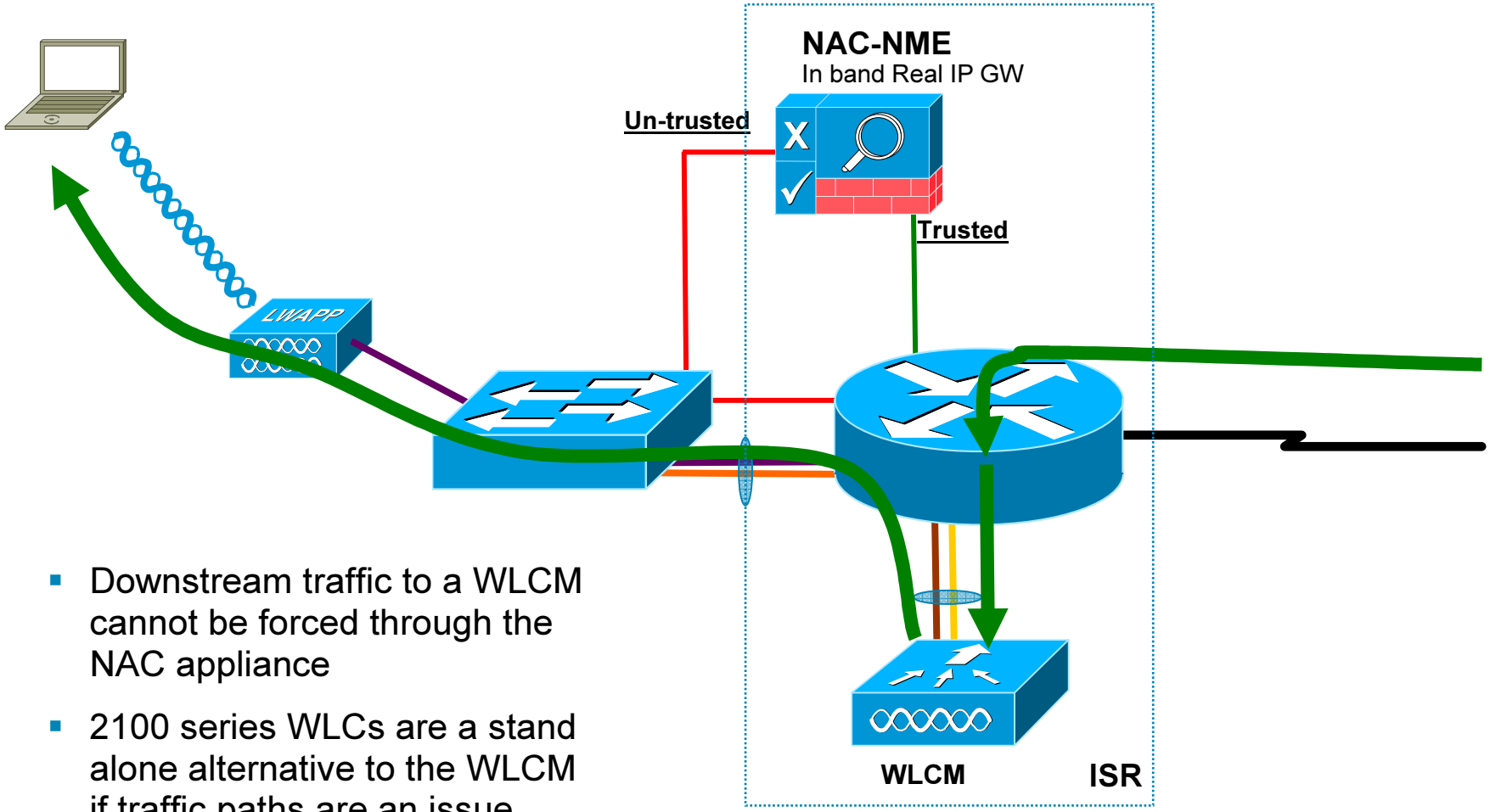
- Basically it is a same rules apply as in the campus
- Need to remember is the branch targeted products have limited HA support
  - 21XX – One up link
  - WLCM – Connected to ISR backplane
  - NAC appliance - No statefull failover
  - IOS Firewall - No statefull failover
- Need to remember the H-REAP doesn’t support IBNS

NAC Appliance and WLAN in a Branch



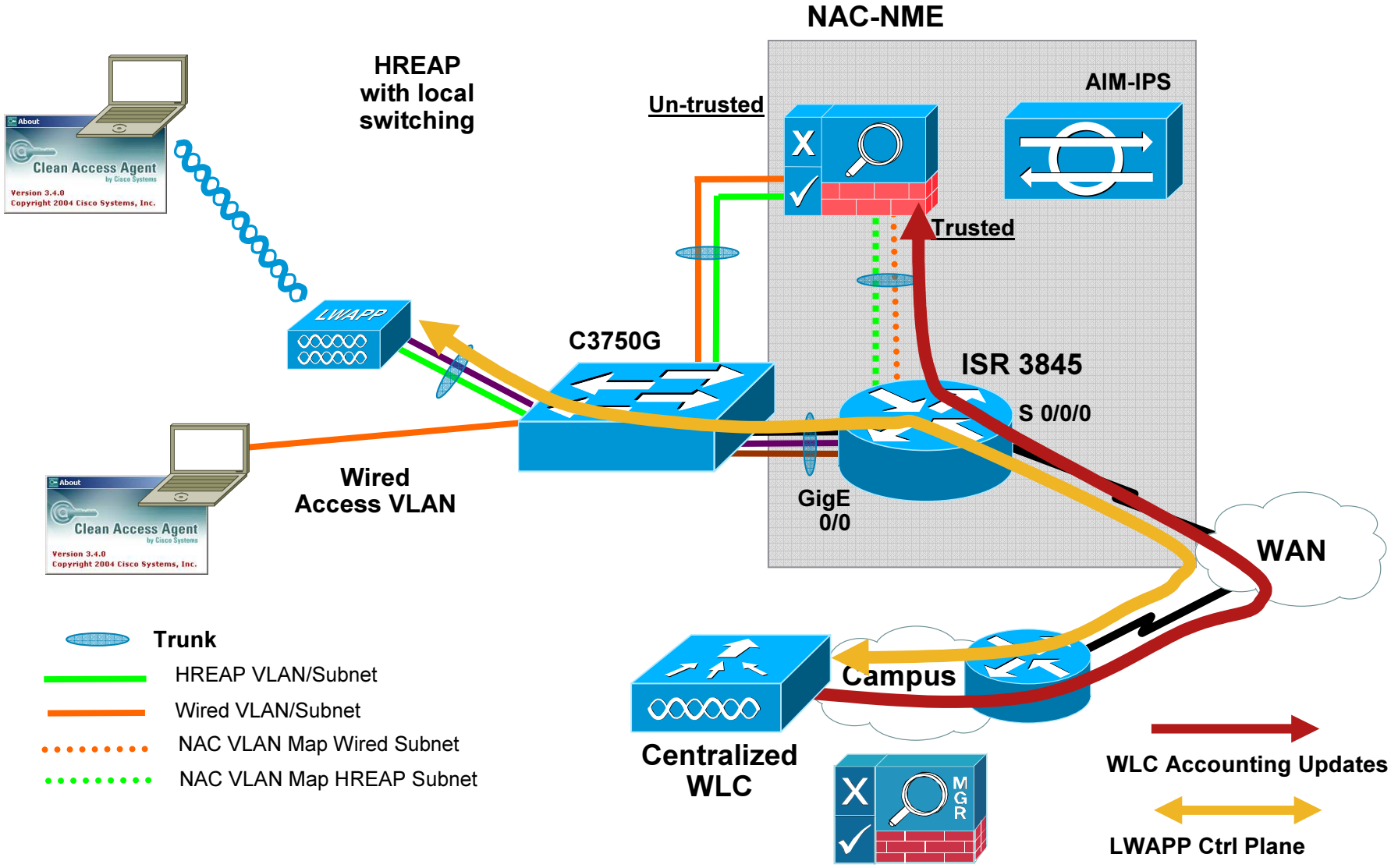
- If a WLCM is used the WLAN subnets are router interfaces and a policy route is required to force traffic through the NAC Appliance
- Traffic to local subnets cannot be forced through the NAC appliance
- The NAC appliance can either be a network module or a standalone appliance

Secure Wireless 2.0 NAC-NM + WLCM



- Downstream traffic to a WLCM cannot be forced through the NAC appliance
- 2100 series WLCs are a stand alone alternative to the WLCM if traffic paths are an issue

Secure Wireless 2.0 - HREAP + NAC NM & Centralized WLC



Key Takeaways

- Know that Mobility Security is different from Wireless Security
- Key design considerations in CUWN integration
- Know the Key components of the Secure Wireless DG
- Location of ESE Design Guides

Secure Wireless Design Guide

- **The current Guide can be found at:**

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/secwlandg20/sw2dg.html