Cisco Expo 2009

Integrated Security for Wireless LAN

Solutions and Architectures Team - Flavien Richard

Presentation will start at 10.30am

About this WebEx session

1. VoIP usage
2. Recording will be used
3. Local panelists to help
4. Chat possibility
5. Q&A at the end
6. Survey after leaving the session

Secure Wireless 2.0 Overview

1. Secure Wireless 2.0 published on Cisco.com:

   Wireless and Network Security Integration

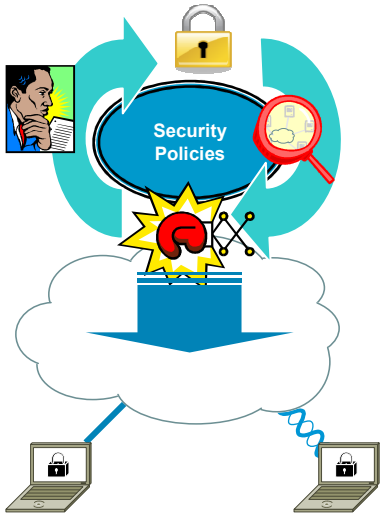
   http://cisco.com/en/US/docs/solutions/Enterprise/Mobility/secwlandg20/sw2dg.html

2. Focus is on integrating and extending general Enterprise network security to an Enterprise WLAN

   Defense-in-depth designed and integrated into the end-to-end architecture

   802.11 fundamental and enhanced security features

   General network security elements, plus any WLAN-specific features

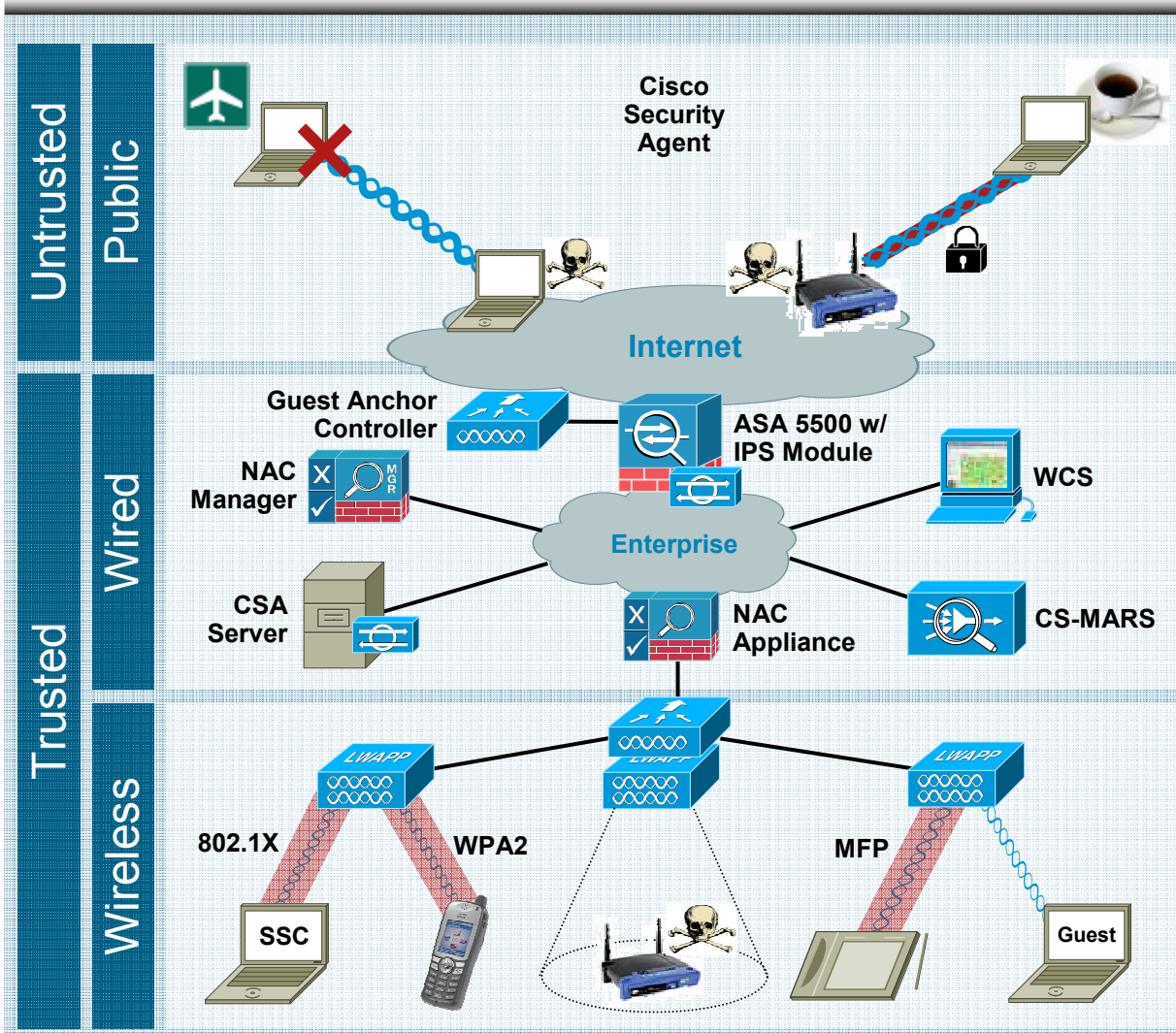


3. The goal being: consistent security policy enforcement across both the wired and wireless network

   Critical to effective network security

   Not a WLAN overlay

Secure Wireless Solution Architecture



Endpoint Protection

- Host intrusion prevention
- Endpoint malware mitigation

Traffic and Access Control

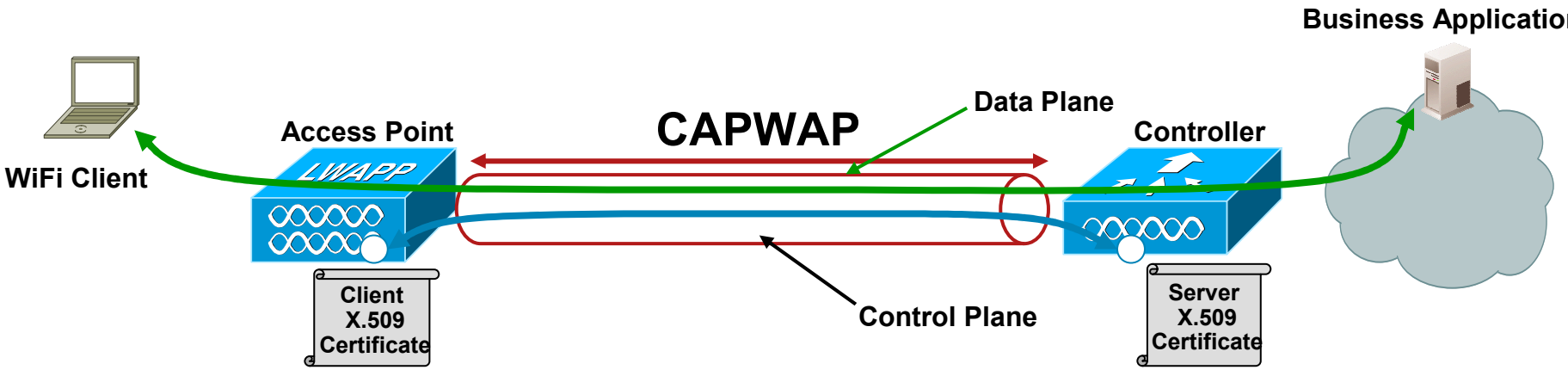
- Dynamic, role-based network access and managed connectivity
- WLAN threat mitigation with IPS/IDS
- (Device posture assessment)

WLAN Security Fundamentals

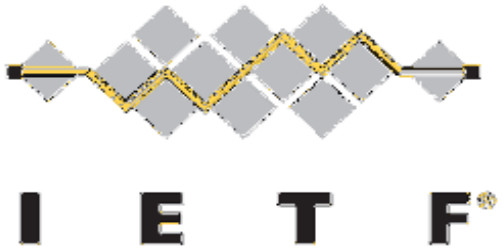
- Strong user authentication
- Strong transport encryption
- RF Monitoring
- (Secure Guest Access)

Cisco Unified Wireless
CAPWAP Protocol Security

1. CAPWAP (IETF standardized protocol) is used between APs and WLAN Controller
2. CAPWAP carries control and data traffic between the two
   - Control plane is AES-CCM encrypted, Authentication by X.509 Cert.
   - Data plane is not encrypted today
3. It facilitates centralized management and automated configuration
4. Open, standards-based protocol



WLAN Controller Join Process
Mutual Authentication



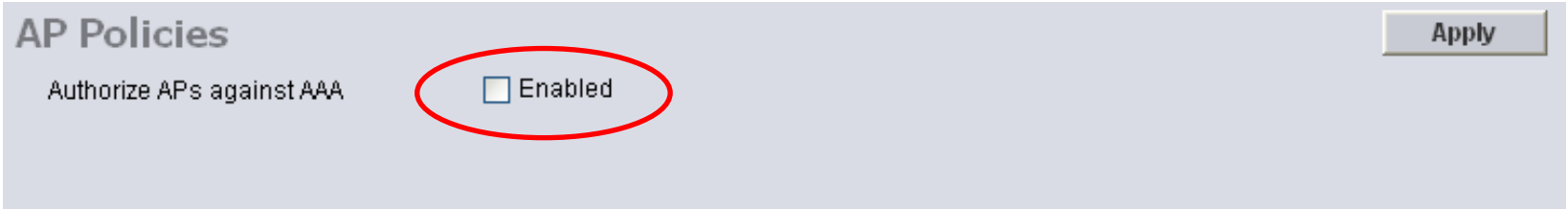
1. AP's CAPWAP Join request uses the AP's signed X.509 certificate
2. WLAN Controller validates the certificate before sending an CAPWAP Join Response
3. If AP is validated, the WLAN Controller sends the CAPWAP Join Response which contains the controller's signed X.509 certificate

As of 11/2008, the certificate can be Cisco-installed at manufacturing or your own company certificate

Access Point Authorization Configuration

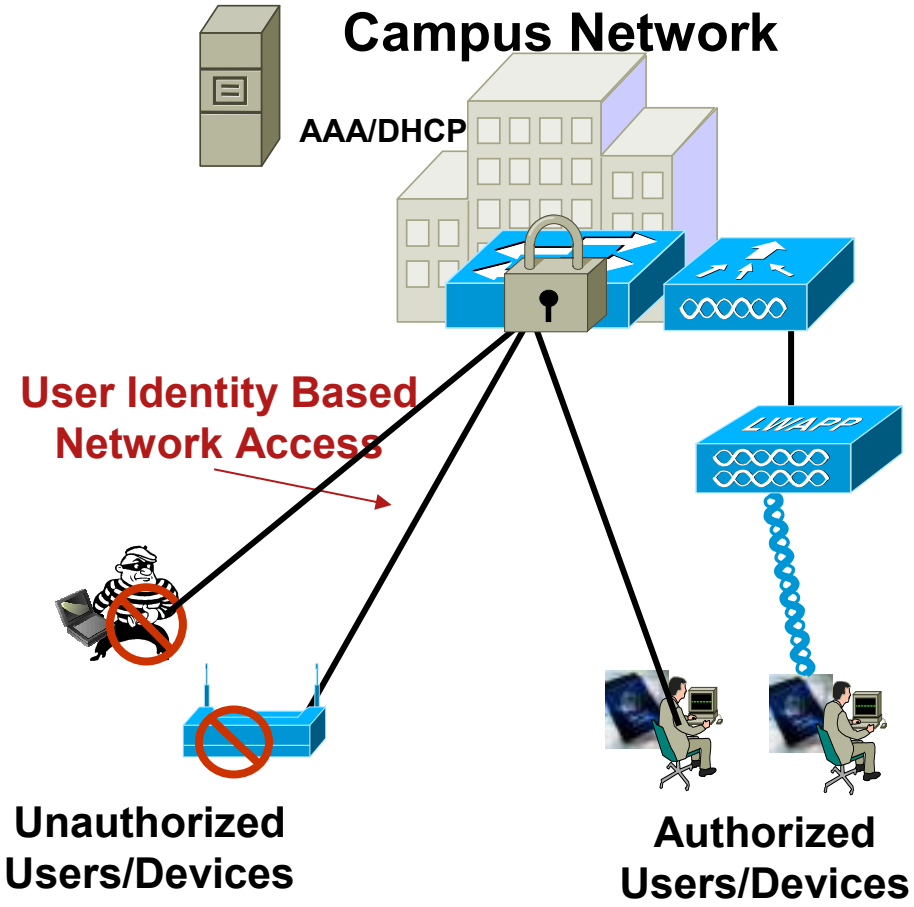
1. Enforcing AP Policies will require authorization of APs prior to association to Cisco WLAN Controllers based upon their identities (MAC addresses)
2. Without AP policies, any lightweight Cisco AP will be able to associate to a Cisco WLAN Controller

In Web GUI, go to Security > AAA > AP Policies



AP Wired Port Authentication with 802.1X

1. Authenticates any wireless access point plugged into a wired port
2. AP presents 802.1X authentication to join the wired network
3. Any AP without credentials is denied access to the wired or wireless network
4. Proactively eliminates rogue APs on the wired network
5. Facilitates secure AP provisioning



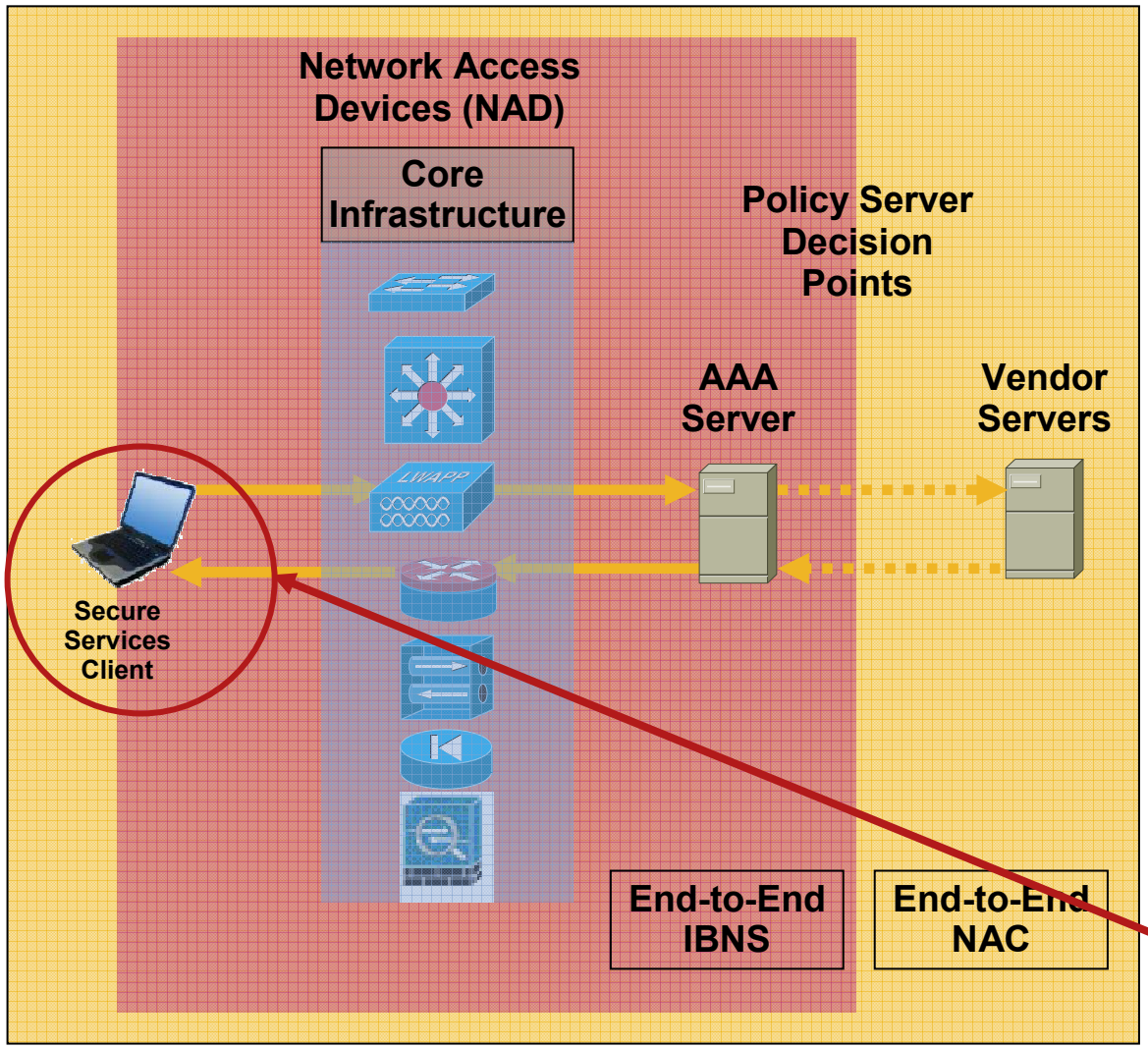
End-to-end Wireless Security

1. A Secured Infrastructure for wireless is not enough!
2. You need an enterprise-grade Supplicant*
3. You need an enterprise feature-rich (AAA) Authentication Server

* The client software used for WLAN authentication is called a supplicant, based on 802.1X terminology.

End-to-End Security Framework

Secure Services Client delivers wired/wireless 802.1X



- Single solution for all connectivity methods
- Architectural extension of RADIUS solution
- Easy connection for end-users
- Embedded intelligence in NAC-capable Cisco infrastructure
- Leverage existing network and security management software
- 802.1X integration with Cisco SSC Supplicant

Cisco Secure Services Client
Drivers for CSSC

What End Users want	Balancing the Needs of End Users and IT Administrators	What IT Administrators need
Intuitive - Easy to configure and use		Respect and enforce enterprise security policies
Immediate access to network without intervention		No user tampering No override
Connectivity at office, home and public hotspots		Easy to Manage and Easy to Deploy
Status at a glance		
Manage from the tray icon		One connection at a time - No bridging – No packet storms

Look for the 802.11 Security Standards

1. Key 802.11 Security Standards

   WPA (Wi-Fi Protected Access)

   - Wi-Fi Alliance standard for WLAN authentication and encryption prior to 802.11i
   - Developed to address the known WEP issues while supporting legacy hardware
   - Uses 802.1X/EAP + TKIP encryption

   WPA2 or **802.11i**

   - 802.11i is the IEEE standard for WLAN security
   - WPA2 is the Wi-Fi Alliance standard for WLAN authentication and encryption which includes the 802.11i security recommendations
   - Uses 802.1X/EAP + AES encryption

2. IEEE 802.11i defines WLAN security standard
3. WPA certifies standards compliance for system interoperability

Wi-Fi Protected Access

1. Should I use WPA or WPA2?

Gold, for NIC/OS supporting it and critical information transfer

Silver, only if you have legacy clients (TKIP vulnerability exploited today)

Lead, if you absolutely have no other choice (i.e., Application Specific Devices)

Gold

WPA2/802.11i

- **EAP-Fast**
- **AES**

Silver

WPA

- **EAP-Fast**
- **TKIP**

Lead

Dynamic WEP

- **EAP-Fast/LEAP**
- **VLANs + ACLs**

CSA (Secure Agent) Wireless Policy Controls

Enabling Per-Application QoS prioritization.

Disabling Wireless NIC when wired connection is active.

Restricting certain connections – certain SSIDs, encryption, ad-hoc.

Requiring VPN connection when out of the office.

802.11 Management Frame Vulnerability

1. 802.11 management frames are NOT authenticated

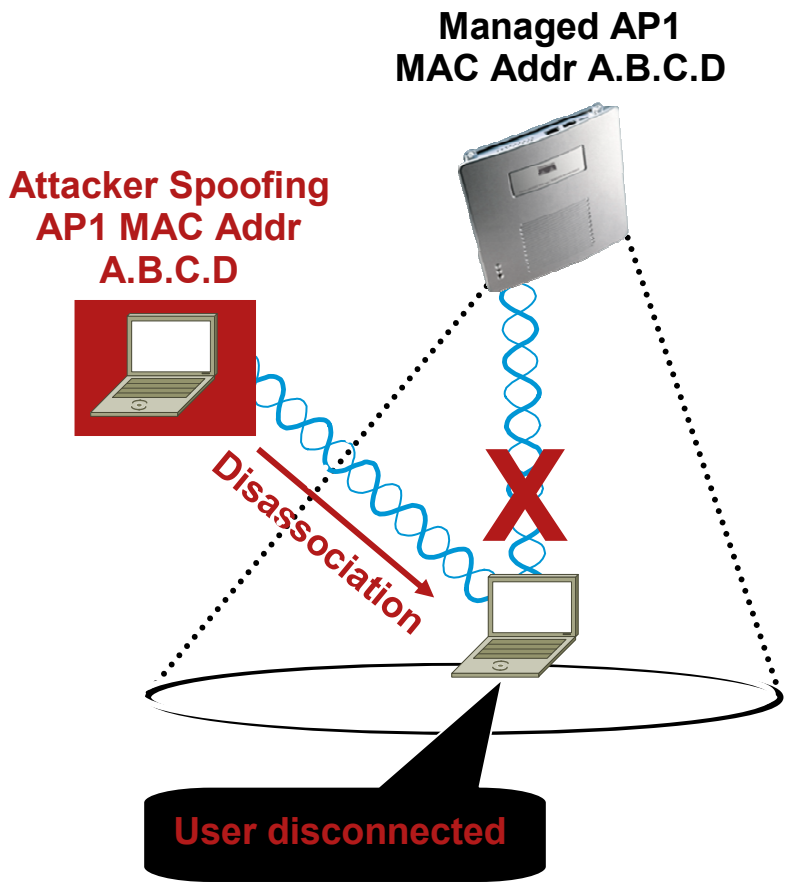
   Anyone can spoof an AP's MAC address or SSID and send an 802.11 management frame on behalf of that AP

   Anyone can spoof a client's MAC address and send an 802.11 management frame on behalf of that client

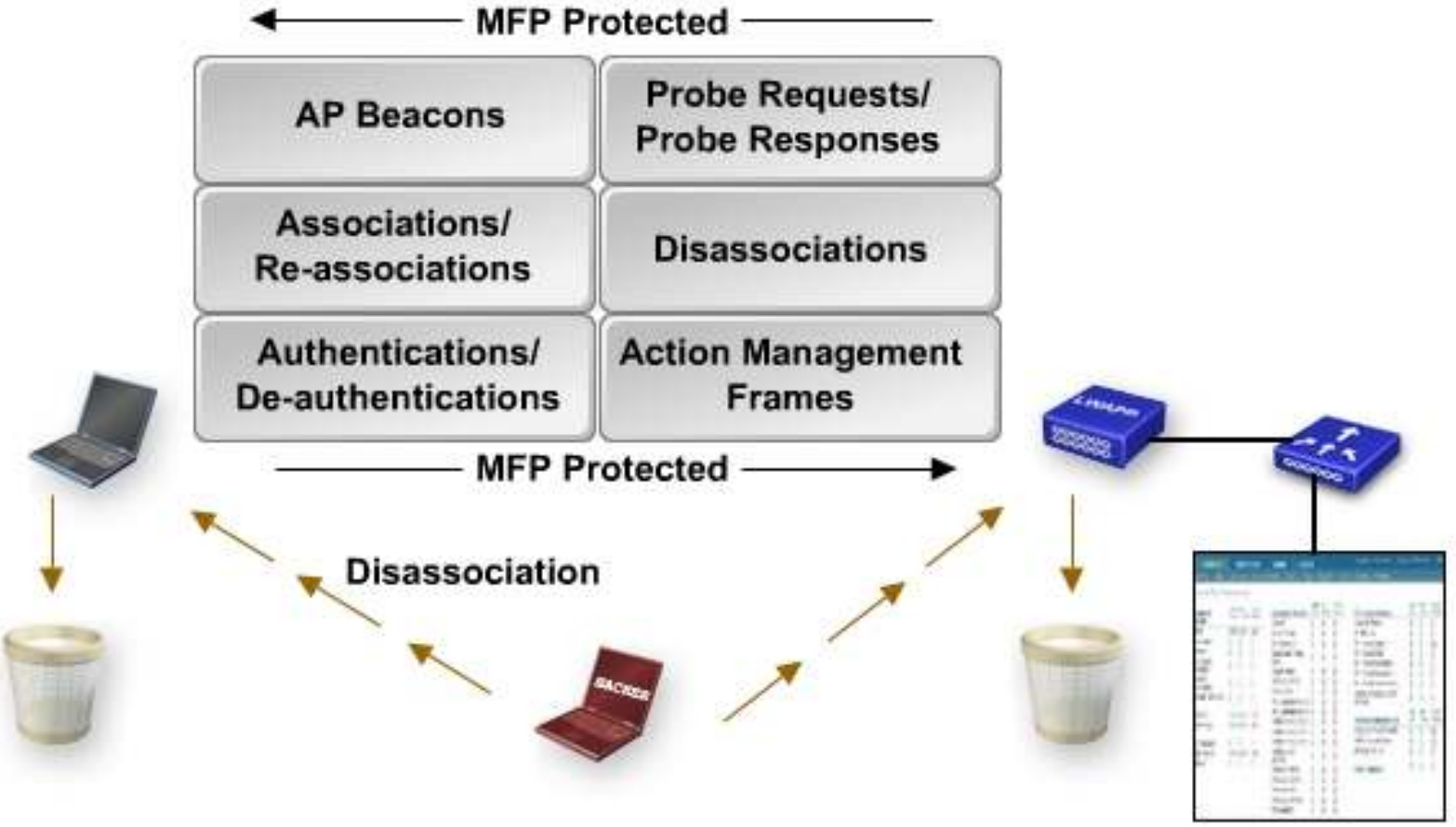
2. Threats:

   802.11 Denial of Service (DoS) attacks by spoofing AP or client 802.11 de-authentication or disassociation frames to disconnect users

   Rogue AP or MITM (man in the middle) avoids detection by spoofing valid AP MAC or SSID



Problem	Solution
Wireless management frames: Are not authenticated, encrypted, or signed. Are a common vector for exploits.	Insert a signature (Message Integrity code/MIC) into the Management frames. Clients and APs use MIC to validate authenticity of management frame. APs can instantly identify rogue/exploited management frames.



Cisco Management Frame Protection (MFP)

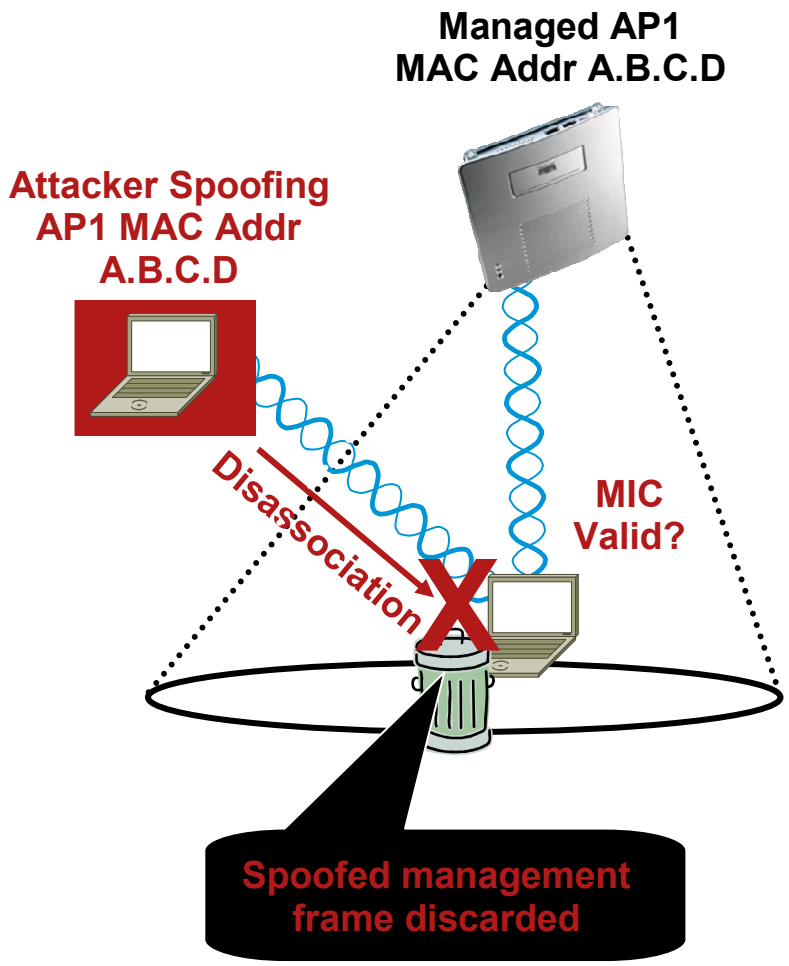
1. Infrastructure MFP support

   Introduced since Unified Wireless 4.0

2. Client MFP support

   Introduced with CCX version 5 clients

   Being ported as a standard called **802.11w**



Security Policies
Overview

1. While doing Authentication, policies can be pushed for users :

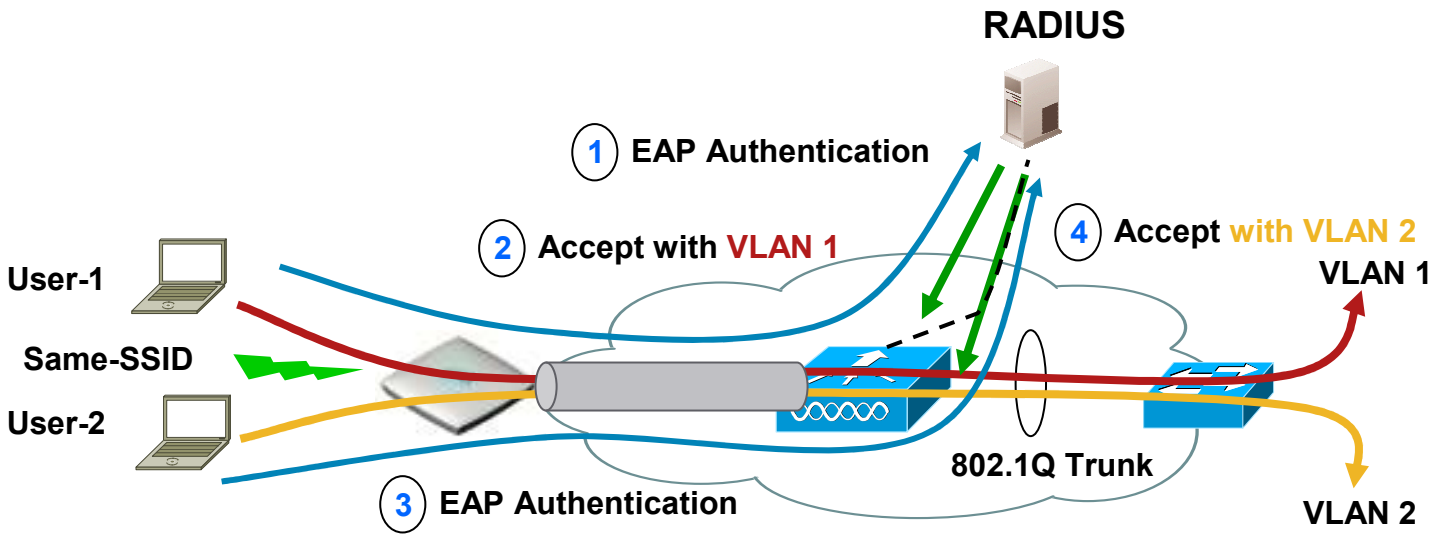
   Dynamic VLAN association

   ACL Profiles

   QoS Profiles

Security Policies
Per User Dynamic VLAN Assignment

1. Users, using the same SSID, can be associated to different wired VLAN interfaces (Dynamic VLAN association)
2. Association will depend of the RADIUS configuration for the user or user group.



See : http://www.cisco.com/warp/public/114/dynamicvlan-config.pdf

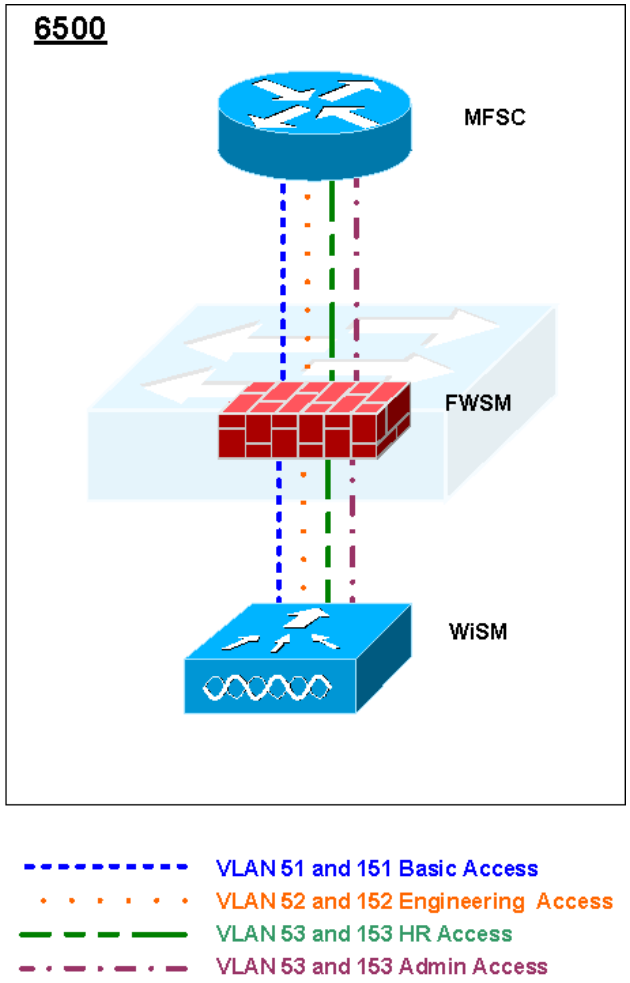
Cisco Firewall Integration Scenario:
User Group Access Policy Enforcement

1. Restricts user group access to permitted network resources only
2. 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
3. VLAN mapped to different firewall VLANs and subject to different firewall policy

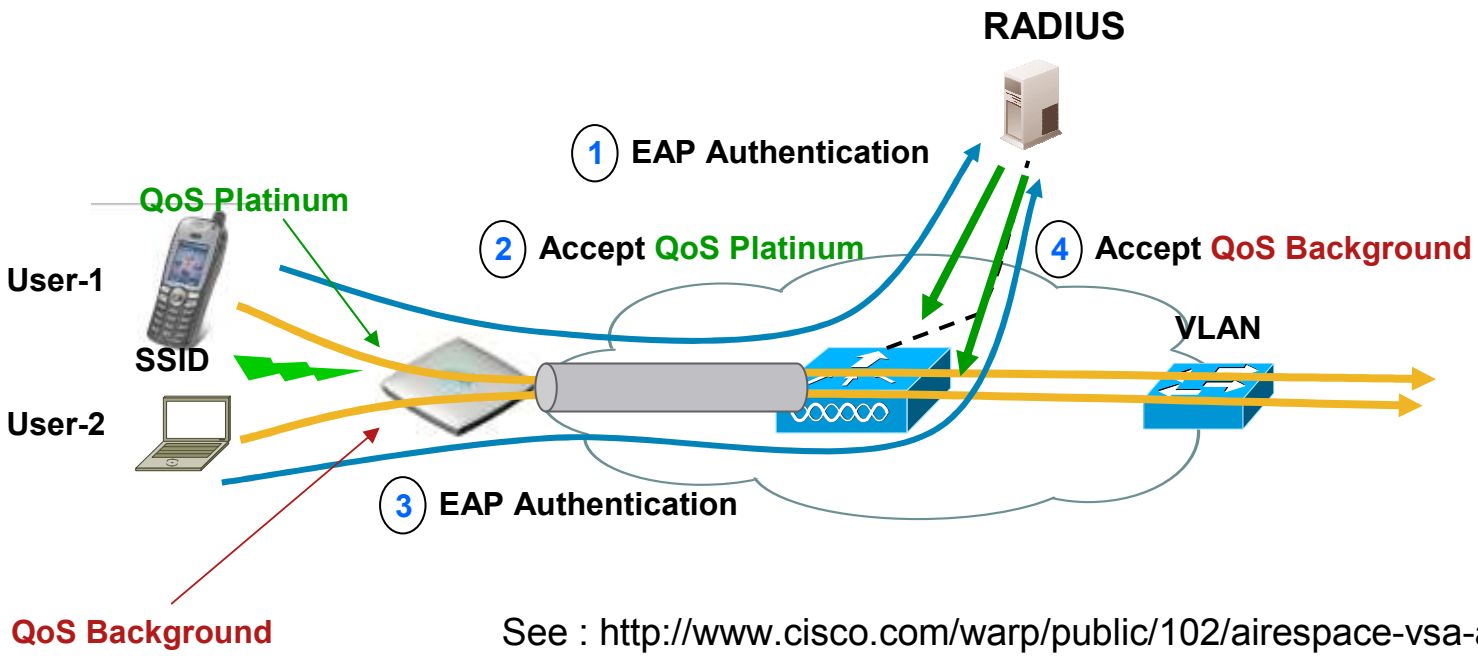
   VLAN mapped to a specific virtual context (user group) in the firewall

   Firewall policy enforced per user group



Security Policies
Per User Dynamic QoS Profile Assignment

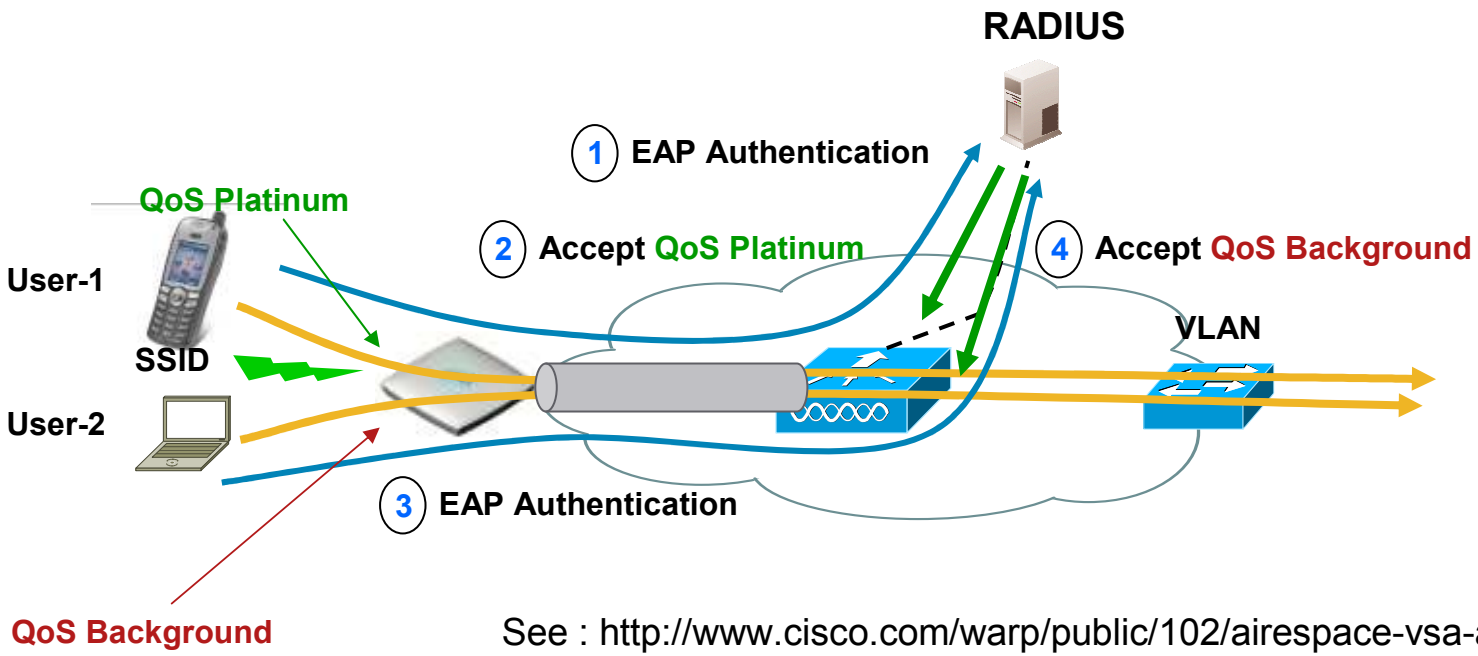
1. RADIUS will push QoS Class for the user
2. The QoS will be applied on the radio interface



See : http://www.cisco.com/warp/public/102/airespace-vsa-acs-config.pdf

Security Policies
Per User Dynamic QoS Profile Assignment

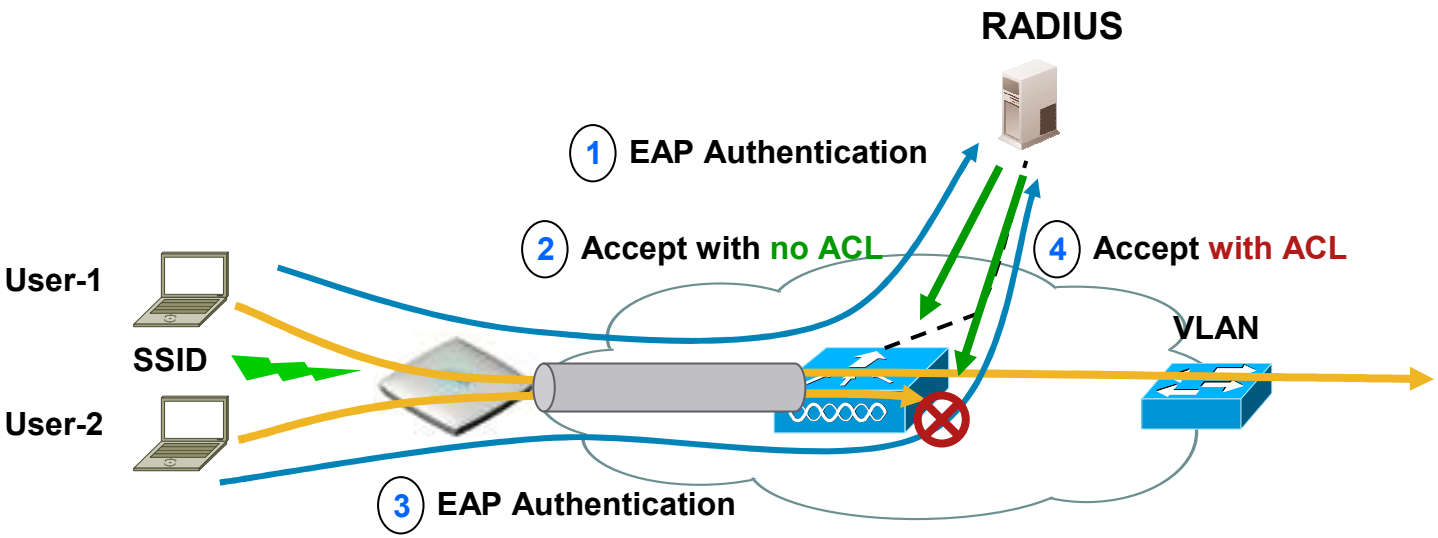
1. RADIUS will push QoS Class for the user
2. The QoS will be applied on the radio interface



See : http://www.cisco.com/warp/public/102/airespace-vsa-acs-config.pdf

Security Policies
Per User Dynamic ACL profile Assignment

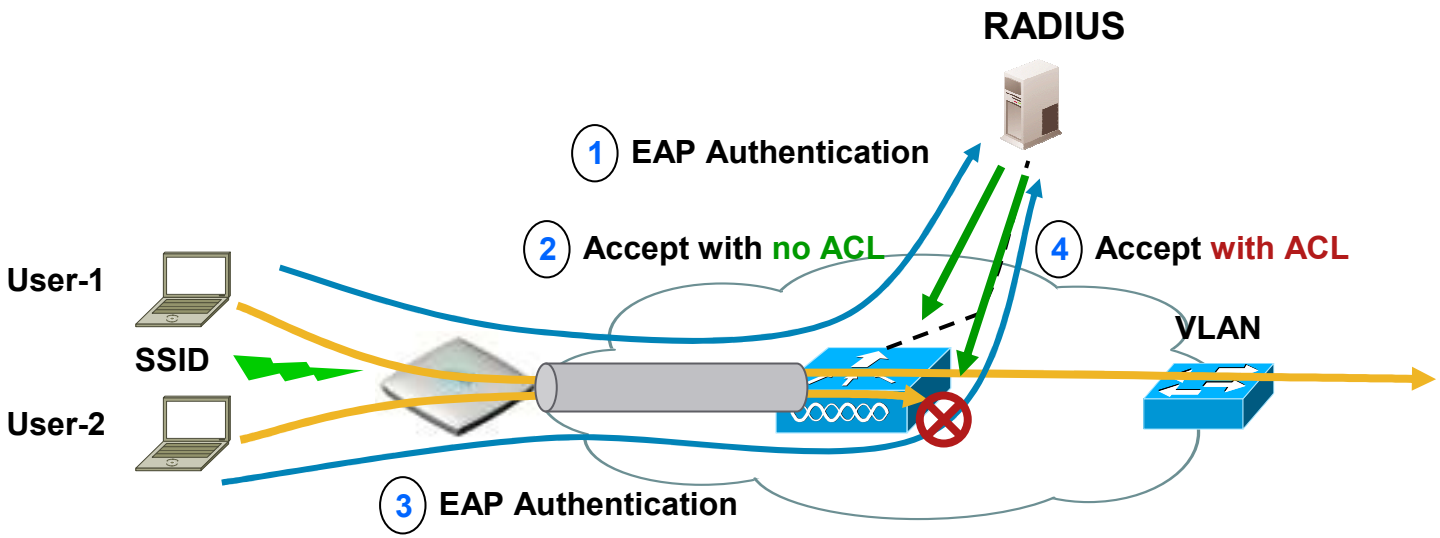
1. ACL must be configured in WLAN Controller
2. RADIUS will push ACL name depending on user or user group policies



See : http://www.cisco.com/warp/public/102/Per-User-ACL-WLC.pdf

Security Policies
Per User Dynamic ACL profile Assignment

1. ACL must be configured in WLAN Controller
2. RADIUS will push ACL name depending on user or user group policies

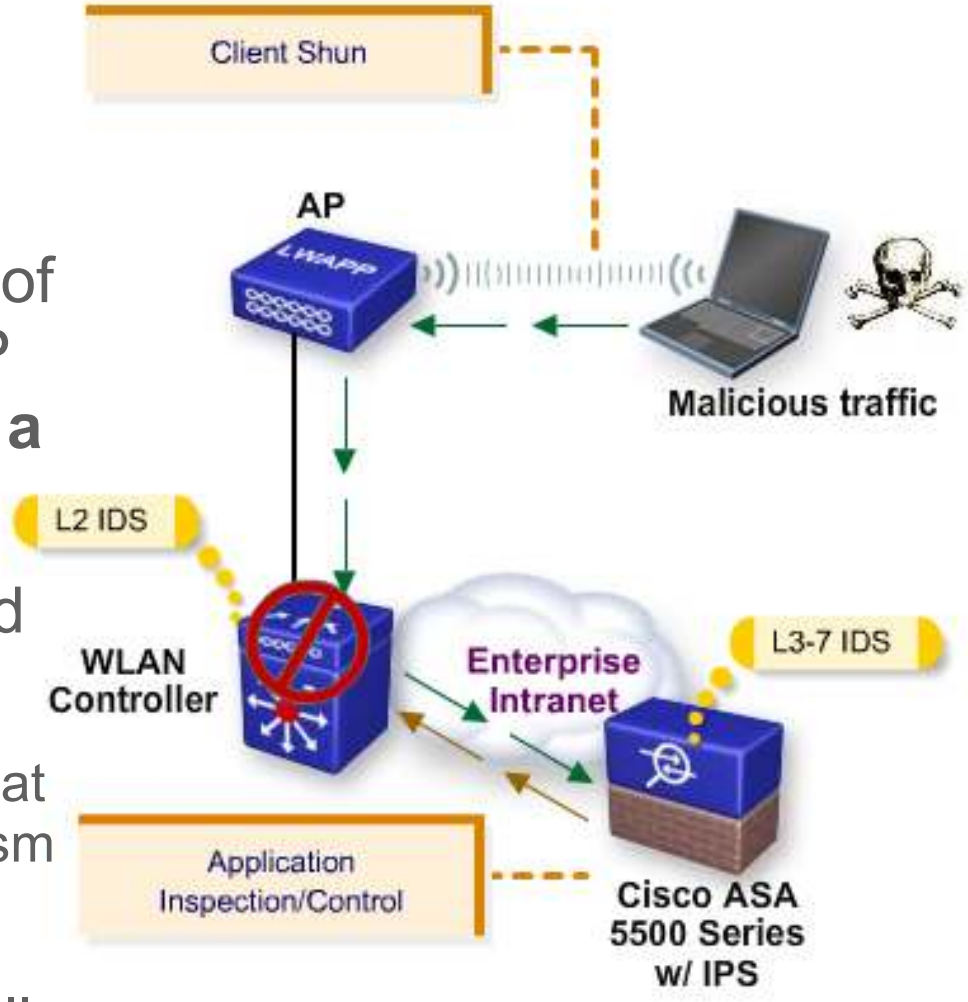


See : http://www.cisco.com/warp/public/102/Per-User-ACL-WLC.pdf

Wired IPS Event and Client "Shunning"

1. Upon trigger of IPS system (Cisco IPS 4200 appliance, ASA or Cat6k modules), for instance from a known type of exploit (Nimda, Sasser, TCP stack exploit, etc.), **activate a "shun" event**
2. A shun event can be invoked either inline or offline

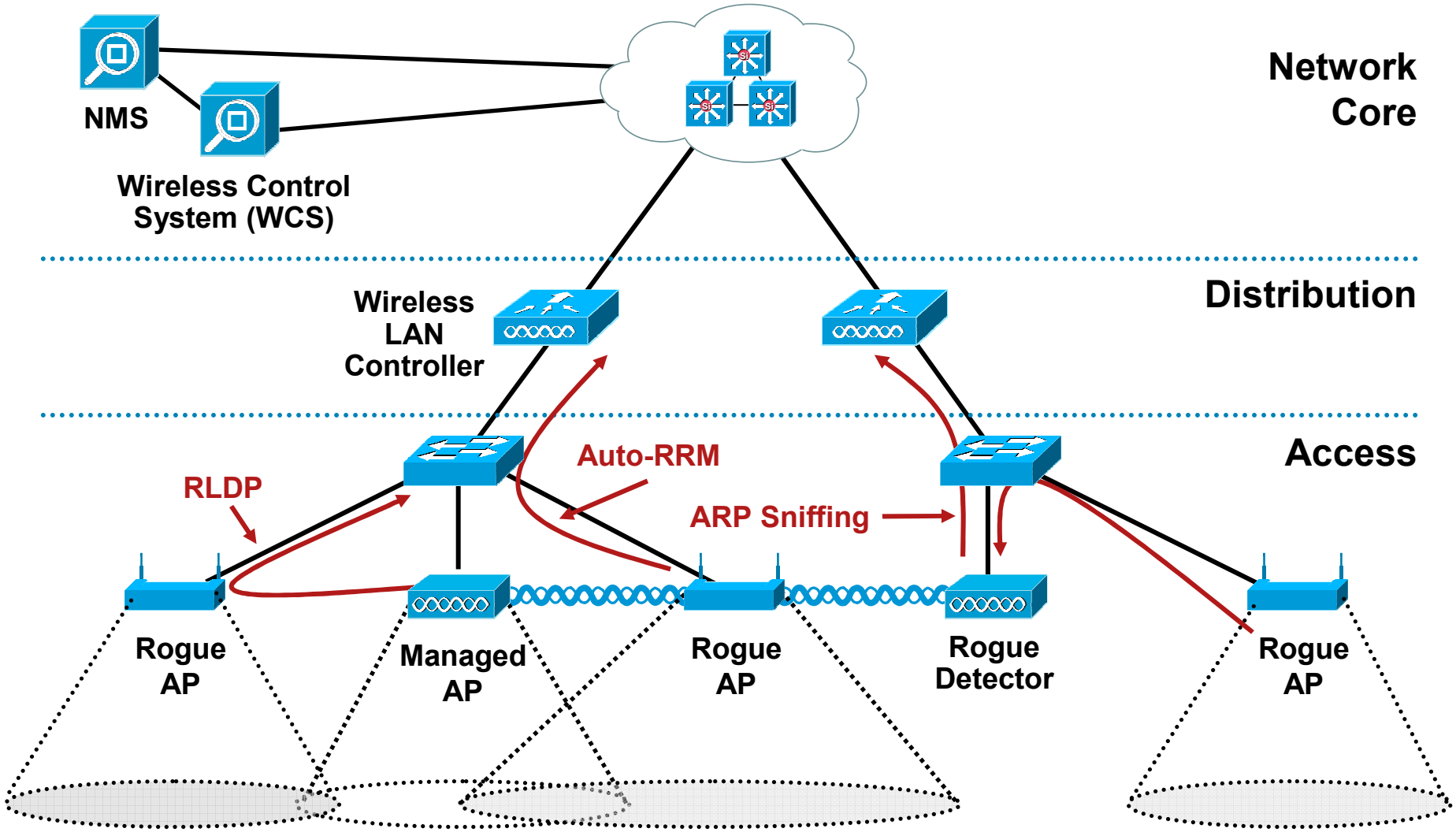
   Wireless "shun" may be invoked at controller via offline mechanism
3. Invokes client exclusion (blacklisting) at Cisco controller



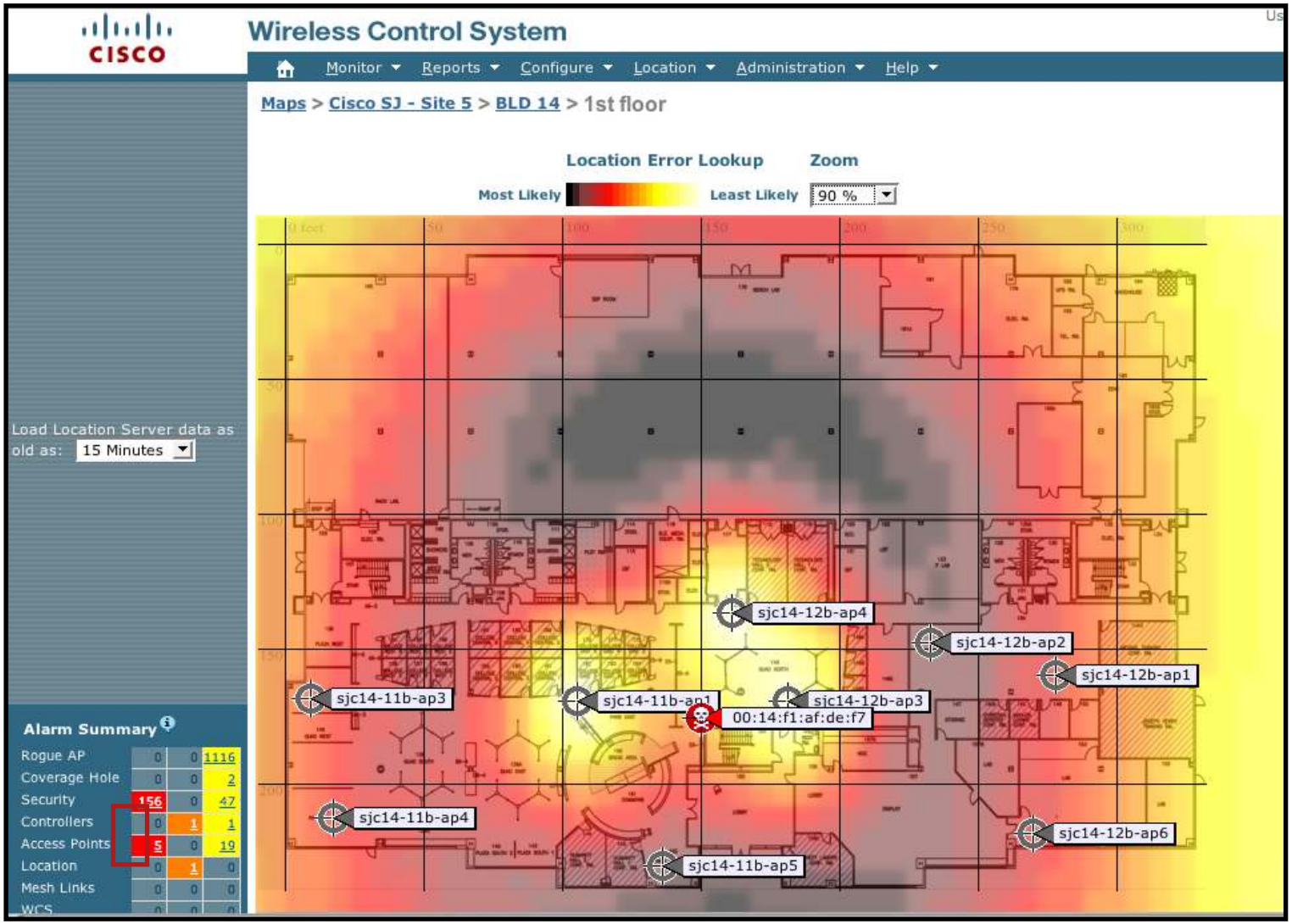
Wireless: Rogue Devices

1. **What is a Rogue?**
   - Any device that's sharing your spectrum, but not managed by you
   - Majority of rogues are setup by insiders (low cost, convenience, ignorance)
2. **When is a Rogue dangerous?**
   - When setup to use the same ESSID as your network (honeypot)
   - When it's detected to be on the wired network too
   - Ad-hoc rogues are arguably a big threat, too!
   - Setup by an outsider, most times, with malicious intent
3. **What needs to be done?**
   - Classify
   - Detect
   - Reporting, if needed
   - Track (over-the-air, and on-the-wire) and Mitigate (Shutdown, Contain, etc)

Cisco Unified Wireless IDS Implementation



Map Rogue AP in WCS



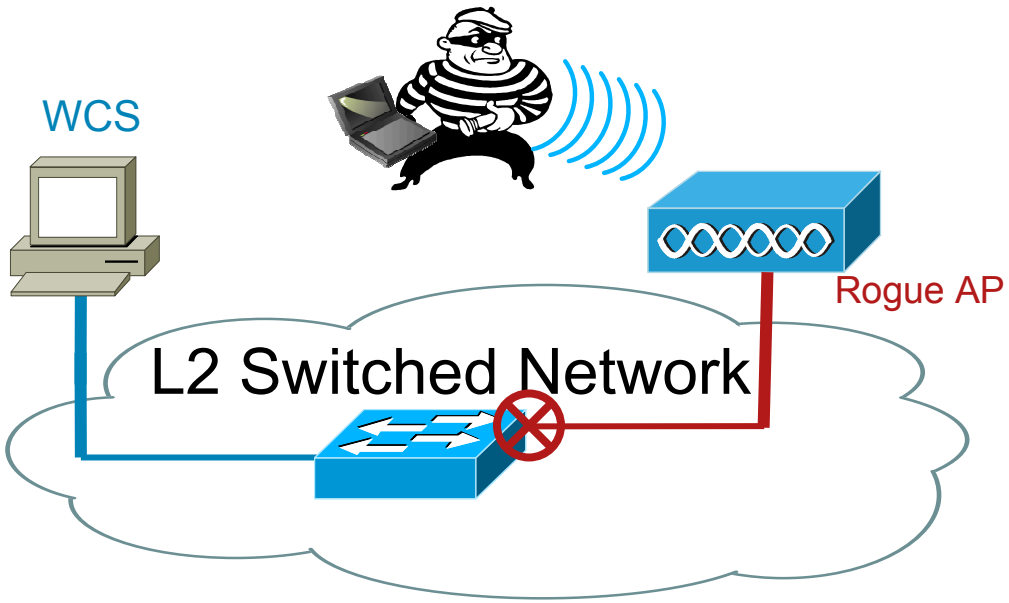
Rogue Switch-Port Tracing and Disabling

Features

1. Uses WCS to identify location of a rogue AP on the wired network and disables the port
   - Uses CDP trace and OUI rules
2. Integrated into the existing rogue detection and containment workflow and reporting in WCS
3. Tracing "on-demand" by operator
4. Operate across all Catalyst switches: 6500, 4500, 3750, 3560, and 2900

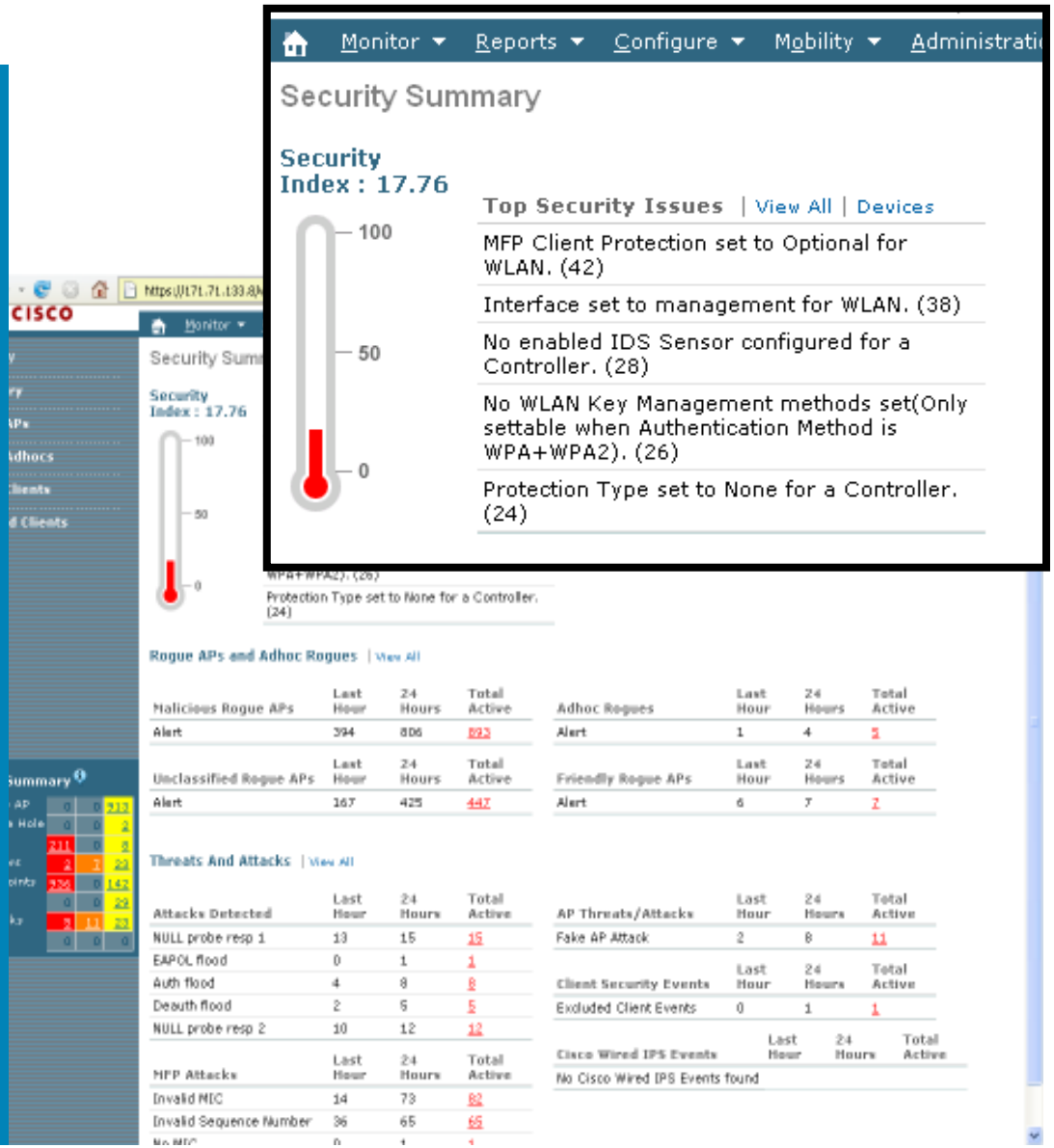
Benefits

1. Reduces time and resources spent searching for rogue access points
2. Can be used to disable rogue APs in remote locations
3. Protects the wired and wireless network from attacks

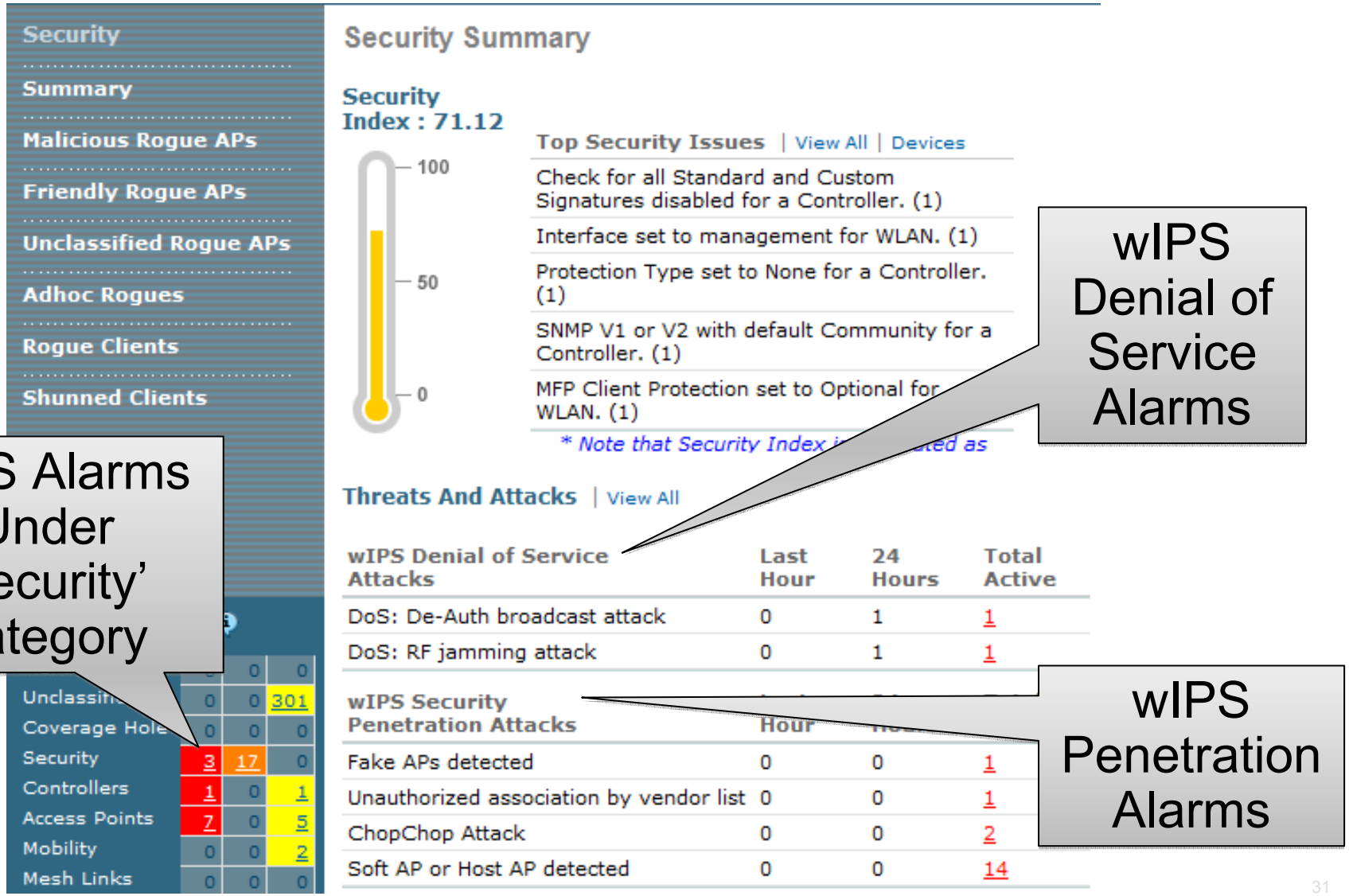


Automated Wireless Security Vulnerability Assessment

- Provides network-wide security health summary
- Proactively monitors entire wireless network
  - WLCs, APs and management interfaces
- Identifies vulnerabilities in:
  - Encryption
  - User/network authentication
  - Threat mitigation
  - Management
- Reduces configuration errors by recommending optimal security settings
- Increases awareness of potential security issues



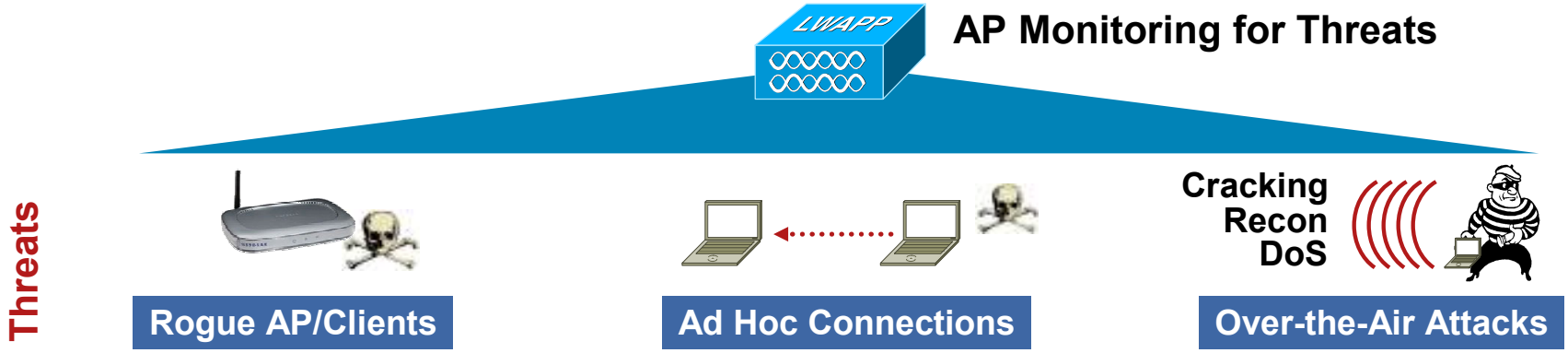
wIPS Alarms on Security Dashboard

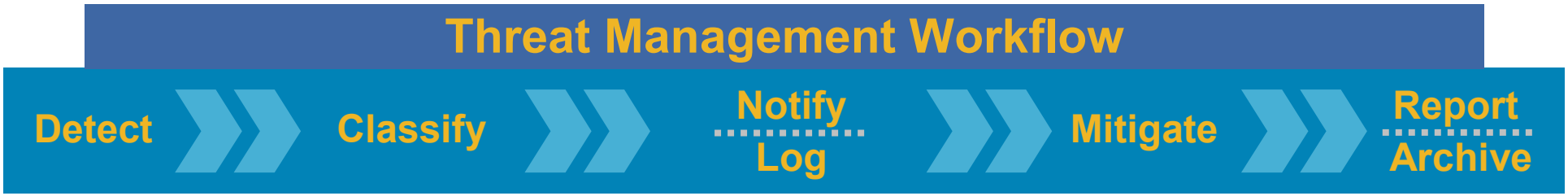


Adaptive Wireless Intrusion Prevention System (wIPS)

Wireless Intrusion Prevention

Purpose and Components





What Is the Threat?

How Severe Is It?

Alert Staff, Raise System Alarm, or Just Log?

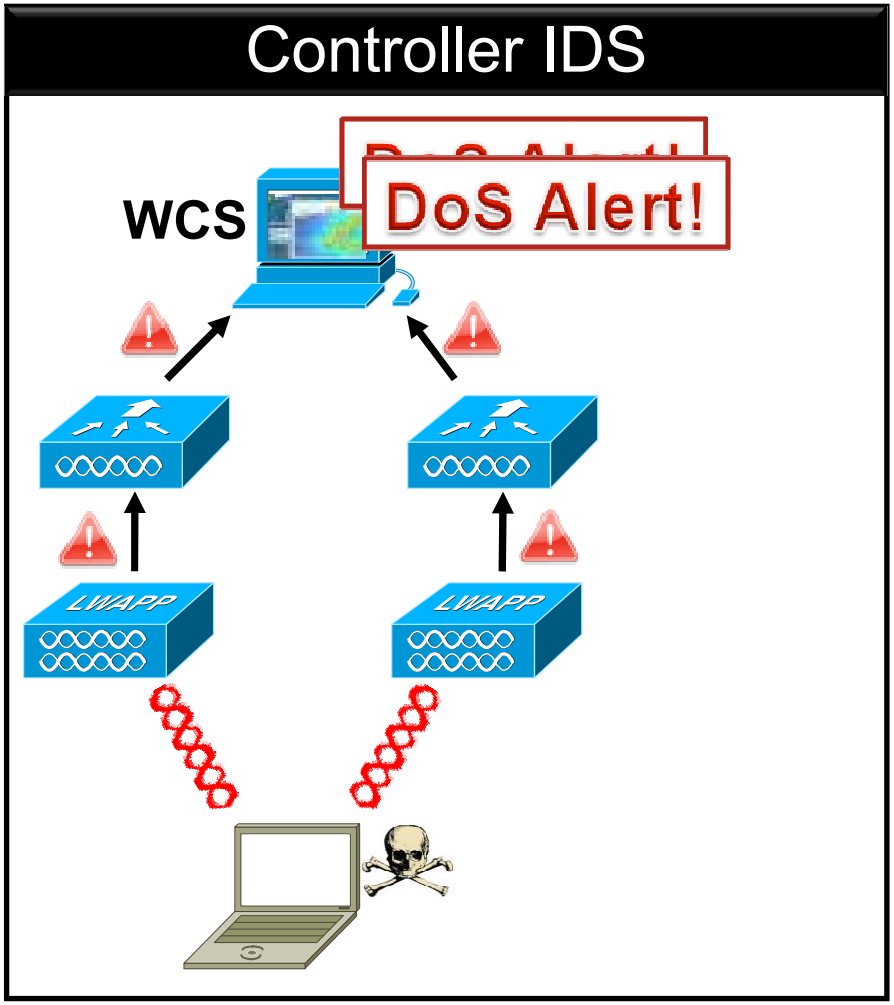
What Action Must Be Taken?

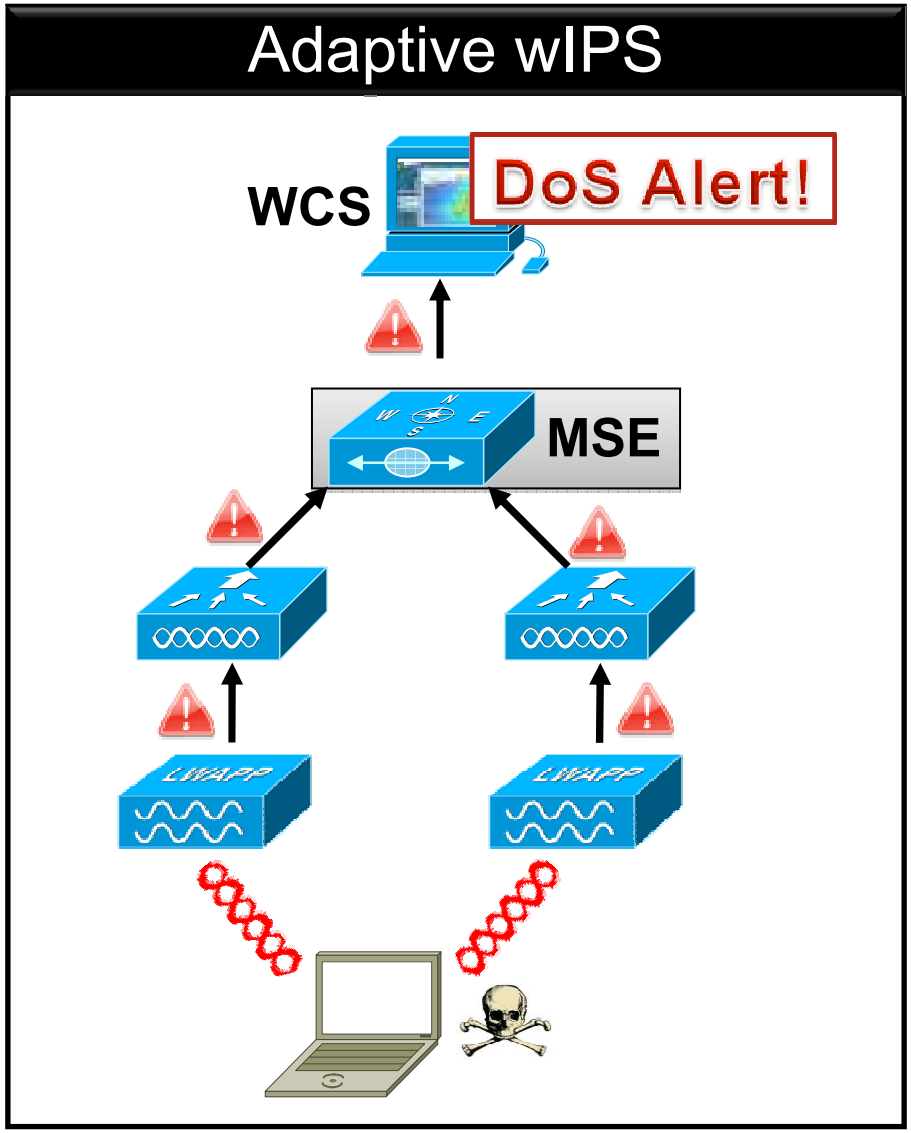
End-to-End Record of Event and Actions

How is this different than controller IDS?

1. wIPS Access Points can detect over 45 different signatures and tools
   - Controller IDS does 17 today
2. wIPS provides forensics (packet capture) abilities
3. wIPS requires an additional hardware (MSE) and dedicated always-on monitoring APs
4. wIPS on MSE provides centralized database for attack correlation and alarm archival
5. wIPS provides an attack encyclopedia

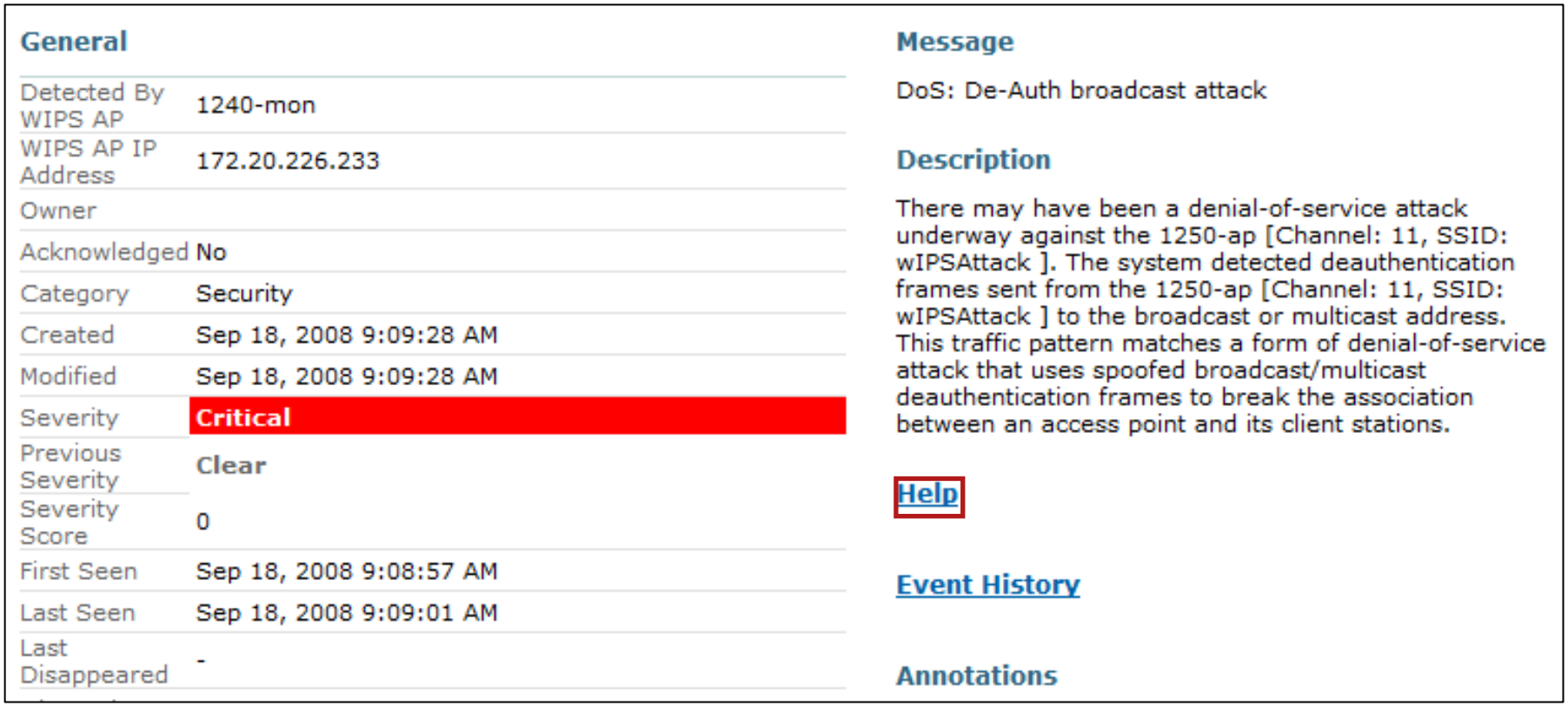
Adaptive wIPS – One Alarm per Attack





Controller IDS has no correlation

wIPS Example Alarm



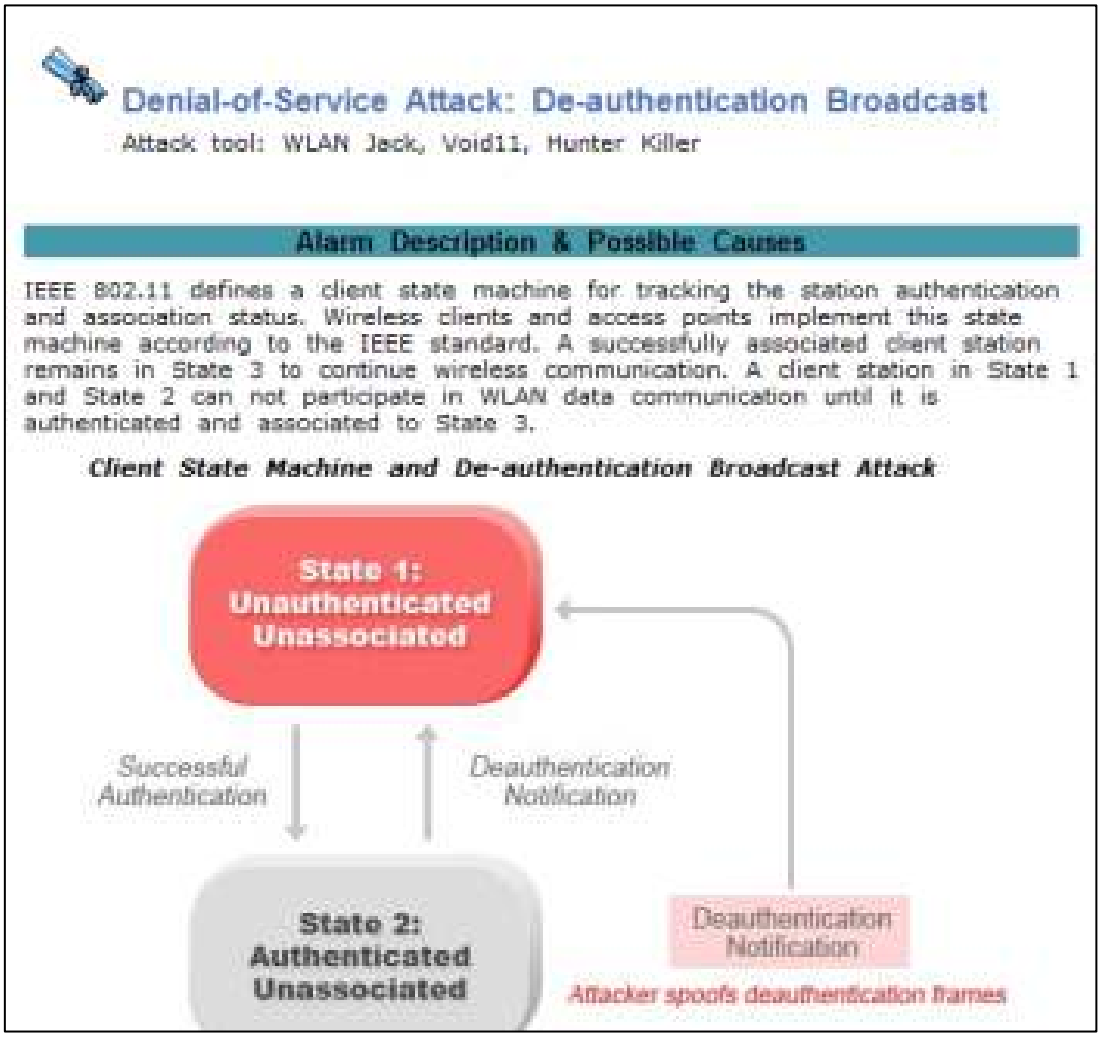
General

Detected By WIPS AP	1240-mon
WIPS AP IP Address	172.20.226.233
Owner	
Acknowledged	No
Category	Security
Created	Sep 18, 2008 9:09:28 AM
Modified	Sep 18, 2008 9:09:28 AM
Severity	Critical
Previous Severity	Clear
Severity Score	0
First Seen	Sep 18, 2008 9:08:57 AM
Last Seen	Sep 18, 2008 9:09:01 AM
Last Disappeared	-

1. Click ‘Help’ for more info on the attack

wIPS Integrated Attack Encyclopedia

1. Available for each alarm
2. Accessible from the wIPS Profile page or by clicking ‘Help’ on each attack alarm



Summary

1. Cisco Unified Wireless, using CAPWAP, brings more infrastructure security.
2. Wireless LAN Security is not an option for enterprise. IEEE 802.11i (EAP/WPA2) should be the target.
3. WLAN Security must be End-to-End. Client supplicant and RADIUS server must be selected with care.
4. Firewall deployment should be common for wired and wireless LANs and not dedicated to a type of access
5. Advanced security is delivered by Adaptive wIDS, MFP and IPS features