Secure Wireless: Integrity of Information on the Move

Welcome!

Contents

Business Adoption of Wireless Expands

Third Wave

Enterprise-wide Wireless and Mobility Deliver Benefits for Everyday Workers via Business Process Improvement, Sustained Competitive Advantage, and Revenue Growth

Second Wave

Opportunistic Wireless Deployment Augment Employee Productivity

First Wave

Siloed Vertical Applications Deliver Departmental Benefit

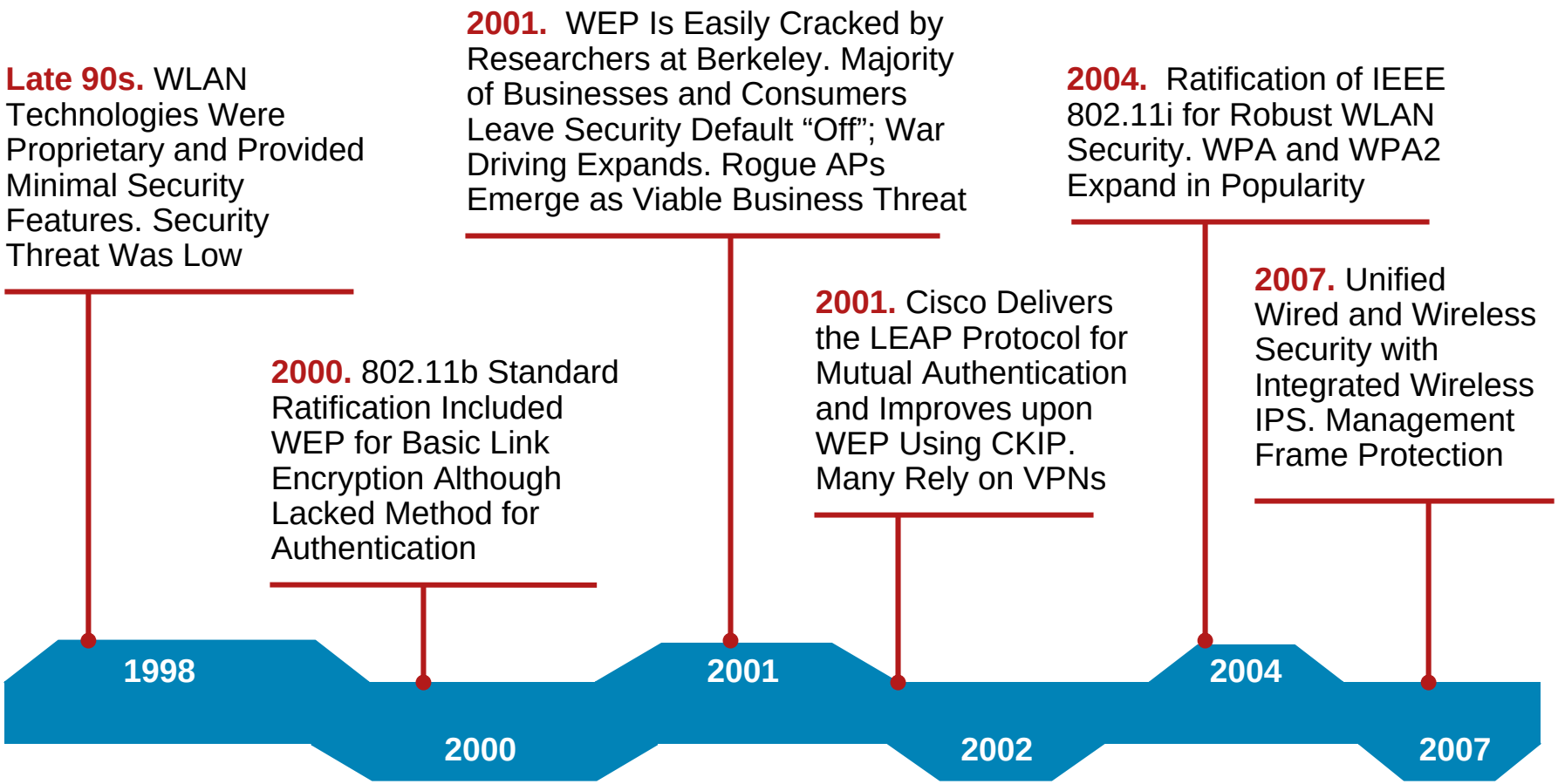
The Business Case for Wireless

- Enhanced customer experience
- Improved supply chain management
- Customer self-service
- Partner, customer and employee loyalty

- Decrease asset location and replacement
- Decrease moves/ adds/changes
- Mitigate cost of non-regulatory compliance
- Lower communications expense

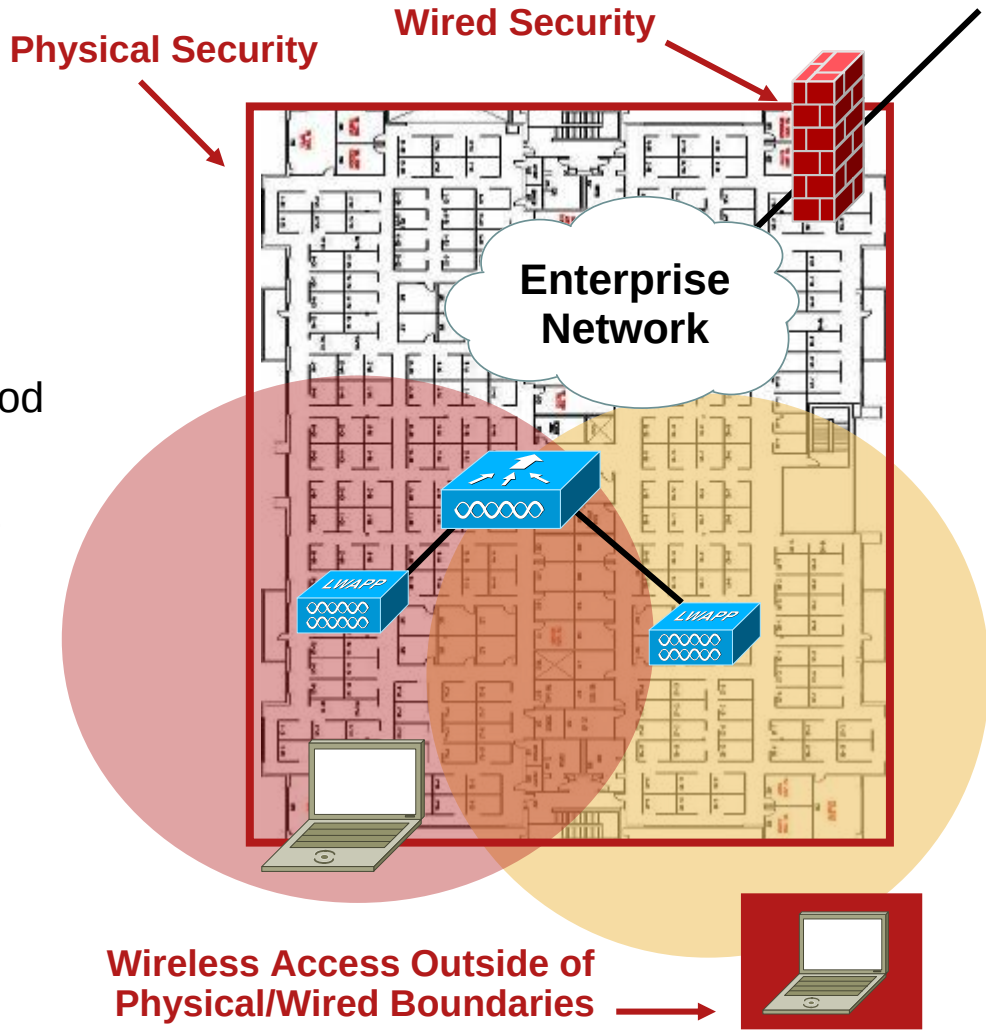
- Accelerated decision making
- Rich collaboration for internal and external meetings
- Real-time access to critical information

Evolution of Wireless Security Challenges



Why Are Wireless LANs Prone to Attack?

- "Open air"
  - No physical barriers to intrusion
  - Silent attacks
- Standard 802.11 protocol
  - Well-documented and understood
  - Most common attacks against WLAN networks are targeted at management frames
- Unlicensed
  - Easy access to inexpensive technology



Wi-Fi Security Myths

No Wi-Fi = Good Security

Wrong!

- A single rogue access point creates enormous risk
- Traditional security measures (firewall, wired IDS/IPS, VPNs, NAC, etc.) don't address
- Perpetrated unknowingly often by your own employees

A Handheld Walk-Around Survey Is Sufficient (i.e. AirMagnet)

Wrong!

- Would you turn on your firewall only periodically?
- Not practical for branch or remote offices with no local IT personnel
- Laborious and expensive

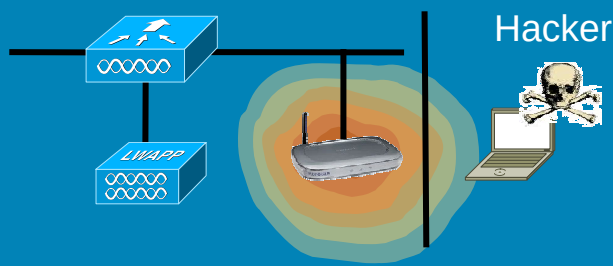
I Use 802.11i, WPA or VPN, so My Network Is Secure

Wrong!

- Only protects authorized clients and infrastructure
- No impact on unauthorized infrastructure (i.e. rogue APs) or unauthorized connections (i.e. ad hoc networks)

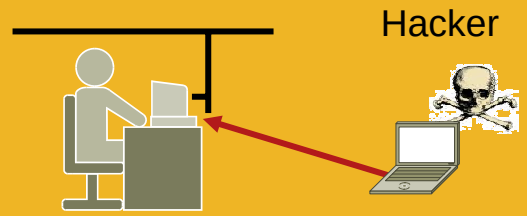
Radio Frequency Based Threats

Rogue Access Points



Employees Unknowingly Create Opening to Enterprise Network

Ad-hoc Wireless Networks

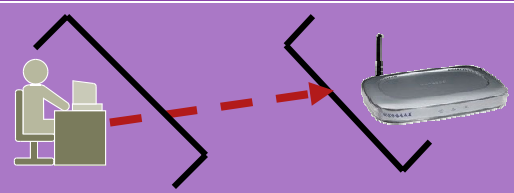


Client-to-Client Connections Bypass Infrastructure Security Checkpoints

Denial of Service Attacks

Malicious Hackers Disrupt Critical Business Services

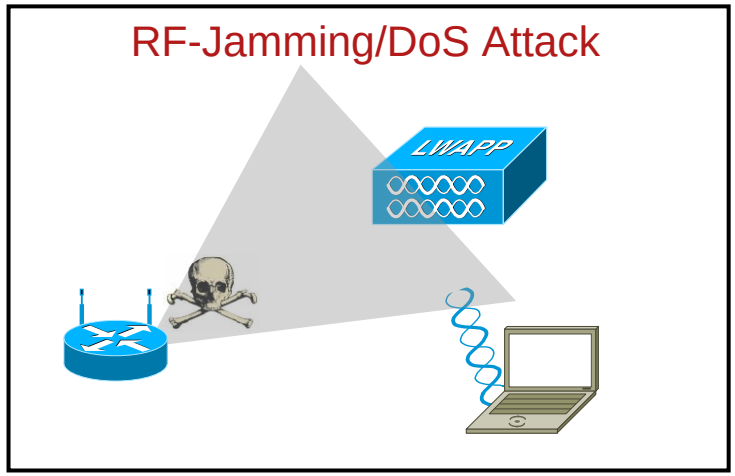
Client Mis-Association

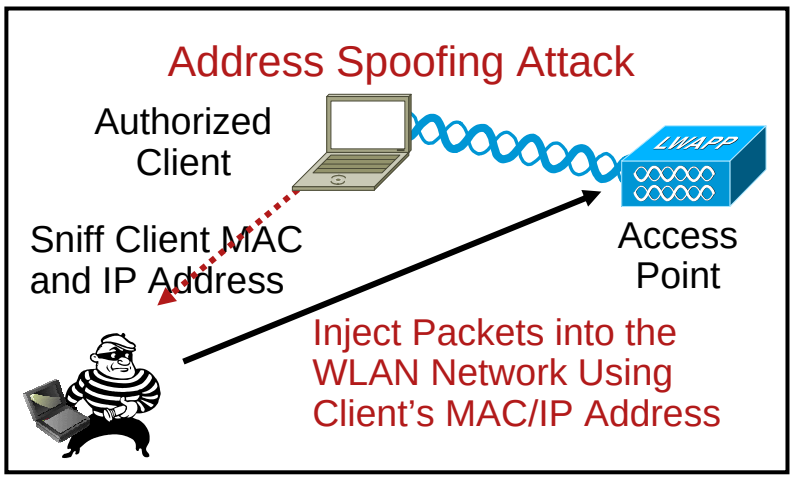


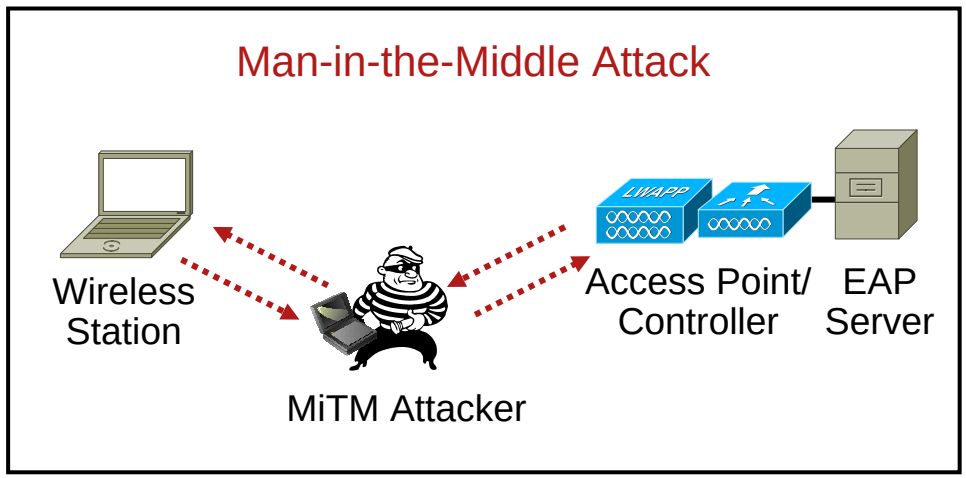
Employees Connect to an External WLAN, Creating Portal to Enterprise Wired Network

Overview of Key WLAN Security Vulnerabilities and Threats

- RF Denial of Service (DoS) attacks
- SSID broadcasting
- Authentication attacks
  - Address spoofing
  - Man-in-the-middle







WLAN Security Vulnerabilities and Threats Summary

- Wireless LAN's have become easy targets for both "traditional" network exploits, as well as criminal elements
- Passive SSID probe sniffing and WEP key attacks are just the first stage in WLAN exploits
- More sophisticated WLAN exploits are likely to employ management frames, as most management packets are not encrypted
- If an attacker can gain access to a WLAN, it is possible to launch a variety of higher-layer exploits over this media

Contents

- 1 Wireless Overview: Drivers and Security Risks
- 2 Secure Wireless for Regulatory Compliance
- 3 Cisco Secure Wireless Solution
- 4 Wireless Security Planning: Benchmark Analysis
- 5 Architectures and Design Principles

The Business Agenda

- Business and security compliance is top-of-mind for executives
- Protecting sensitive business and customer data is the key focus of regulatory compliance requirements

Sarbanes-Oxley	Publicly Traded Companies Must: • Maintain an adequate internal control structure and procedures for financial reporting • Assess the effectiveness of internal control structures
HIPAA	For Patient Information, Firms Must: • Maintain administrative, technical and physical safeguards to ensure integrity and confidentiality • Protect against threats or hazards; unauthorized uses or disclosures
PCI	All Merchants Using Payment Cards, Must: • Build and maintain a secure network • Protect and encrypt cardholder data • Regularly monitor and test networks, including wireless

Business Impact of Lack of Compliance

- Direct financial ramifications
  - FTC fines
  - Compensation payout to customers
  - Cost of external security audits
  - Lost customer confidence
- Research shows substantial indirect costs associated with brand damage
- "The fall in share price attributed to a security incident is estimated at 2.7% over one day, increasing to 4.7% over three days"*

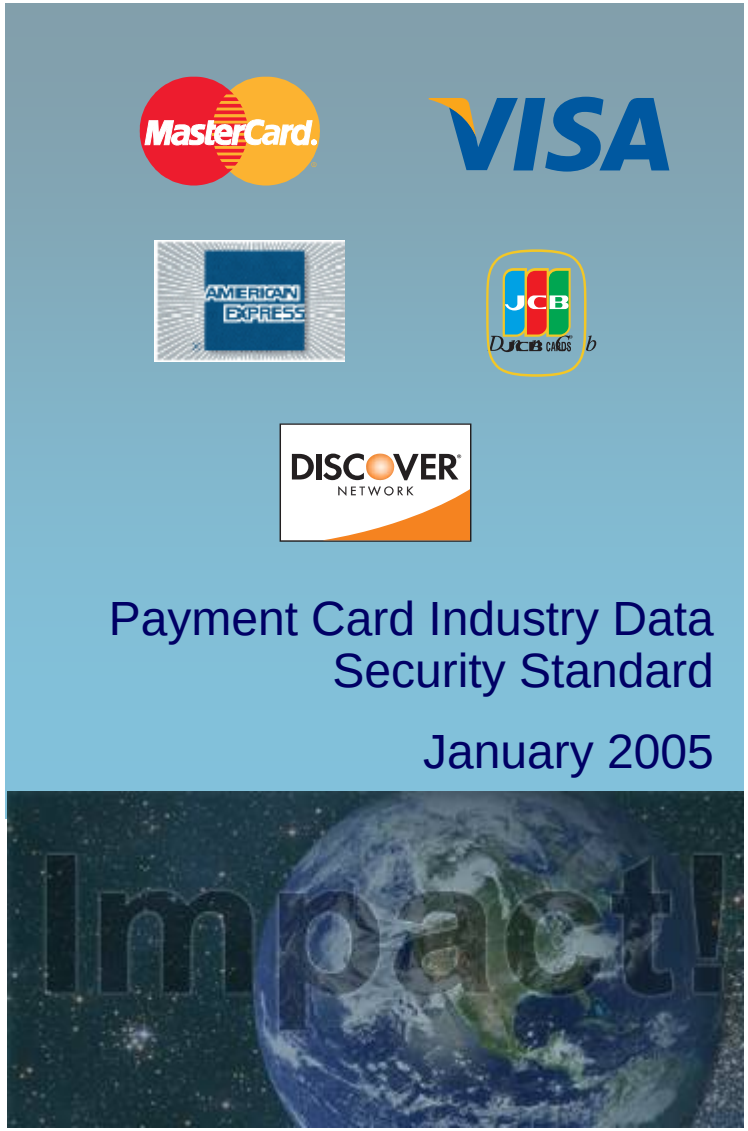
*Source: "The Financial Impact of IT Security Breaches: What Do Investors Think?" Information Systems Security, 2003

Case Study

- Company: Large retailer
- Issue: Data breach due to poor wireless security
- Ramifications:
  - 20 years of third-party security audits mandated by FTC
  - Compromise of 1.4 million credit cards and 96,000 checking accounts
  - Company losses related to security breach ranged from $6.5m to $9.5m

The PCI Data Security Standard

- Published January 2005, ver. 1.1 released Sept 7, 2006
- Impacts **all** who
  - Process
  - Transmit
  - Store: cardholder data
- Developed by MasterCard and Visa, endorsed by other brands
- Global reach (AIS* regulation outside of US)



*Account Information Security
http://www.cisco.com/go/compliance

Mapping Wireless Security to PCI

Wireless Security Tools for PCI Compliance	
Build and Maintain a Secure Network	• Change default settings Best Practice: No default SSIDs, disable broadcast No default login passwords for wireless management
Protect Cardholder Data	• Encrypt wireless data in transit Best Practice: WPA or WPA2 (uses TKIP and AES) VPNs for remote access, host intrusion prevention
Maintain a Vulnerability Management Program	• Deploy wireless Network Admission Control for client posture • Use CSA for host based intrusion detection • Integrate wired and wireless IPS/IDS
Implement Strong Access Control Measures	• Authenticate wireless users and devices—802.1X • Deploy wireless NAC for client posture assessment Best Practice: NAC with 802.1X for Single Sign On
Regularly Monitor and Test Networks	• Deploy monitoring to secure and control the wireless domain Best Practice: Integrated 24/7 RF monitoring
Maintain an Information Security Policy	• Ensure wireless LANs are included in security policy • Enforce consistent information security policy using NAC

Recommended Architectures for PCI

- Cisco worked with PCI auditors to develop architectures that address the requirements of PCI compliance
- Lab tested and audited architectures maximize integration with various technology partners
- Reduce the complexity of designing a secure network
- Mapping of Cisco products directly to PCI requirements

http://www.cisco.com/go/compliance

Summary

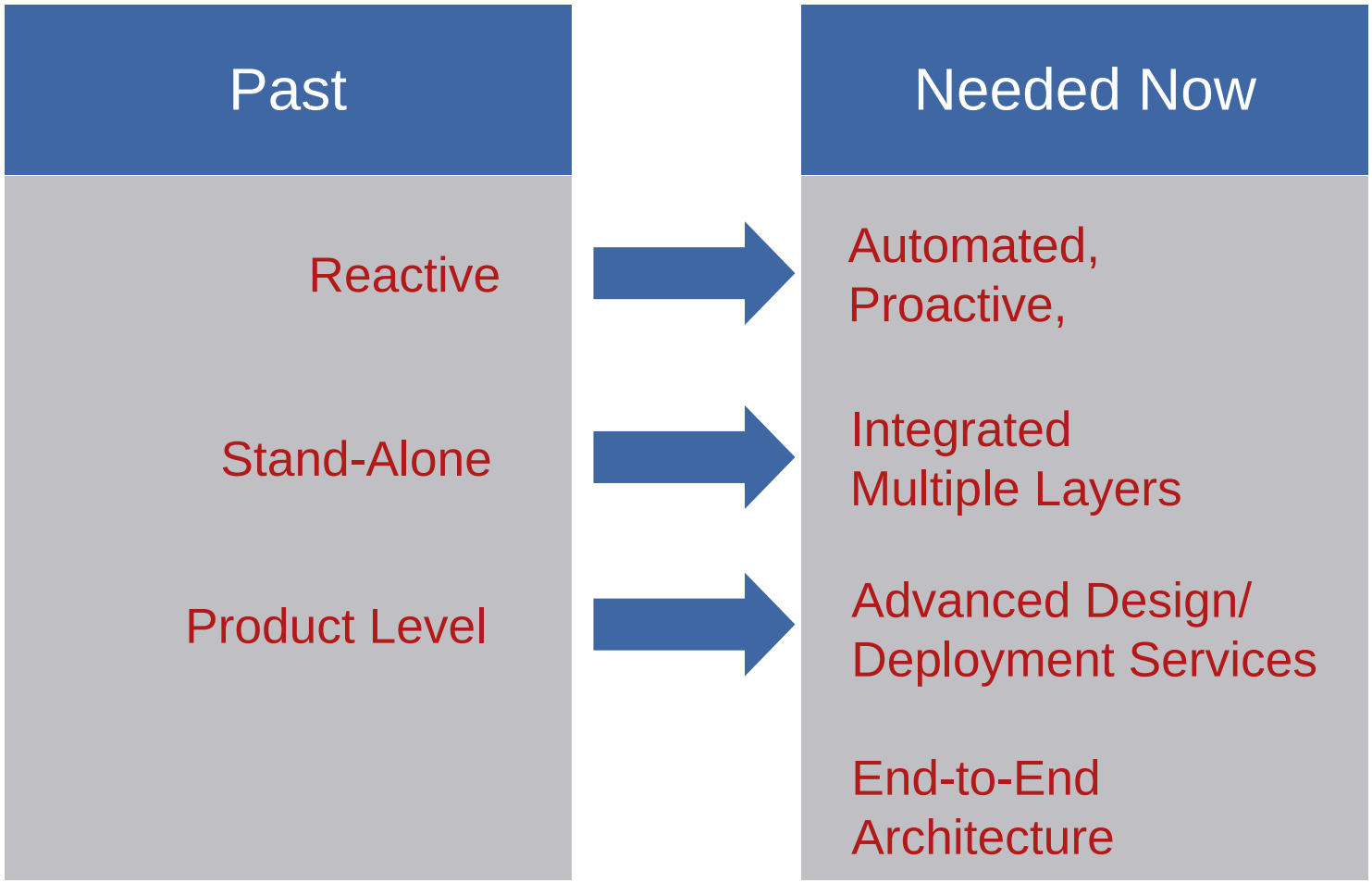
- Businesses are impacted by non-compliance, as evidenced by fines, lawsuits, and breaches
- The wireless network plays a critical role in addressing PCI compliance
- The Cisco Secure Wireless Solution delivers integrated security, including RF monitoring, for robust protection of credit card data
- Cisco delivers a framework for addressing PCI compliance—companies still must certify their compliance through a third party compliance review



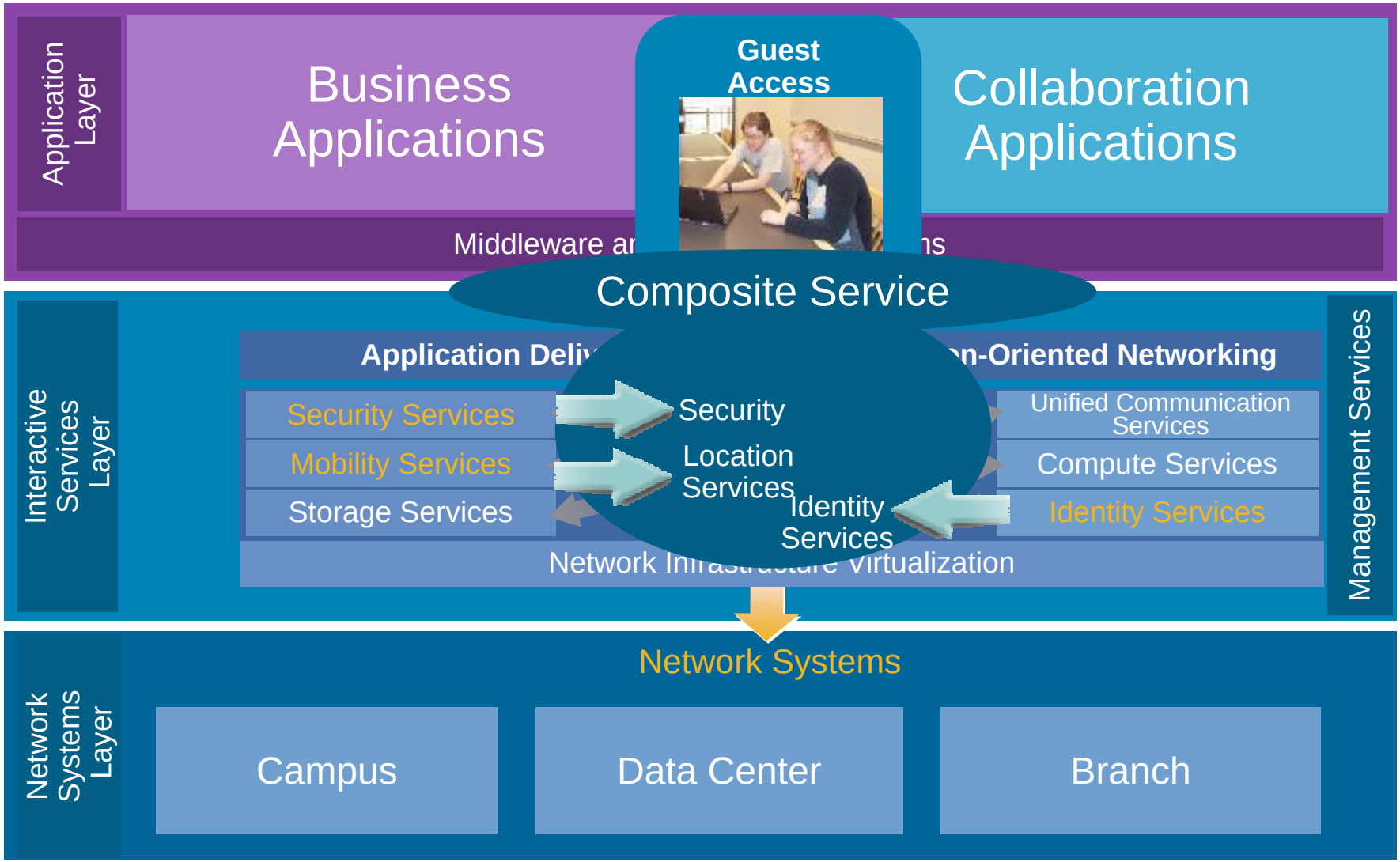
Contents

- 1 Wireless Overview: Drivers and Security Risks
- 2 Secure Wireless for Regulatory Compliance
- 3 Cisco Secure Wireless Solution
- 4 Wireless Security Planning: Benchmark Analysis
- 5 Architectures and Design Principles

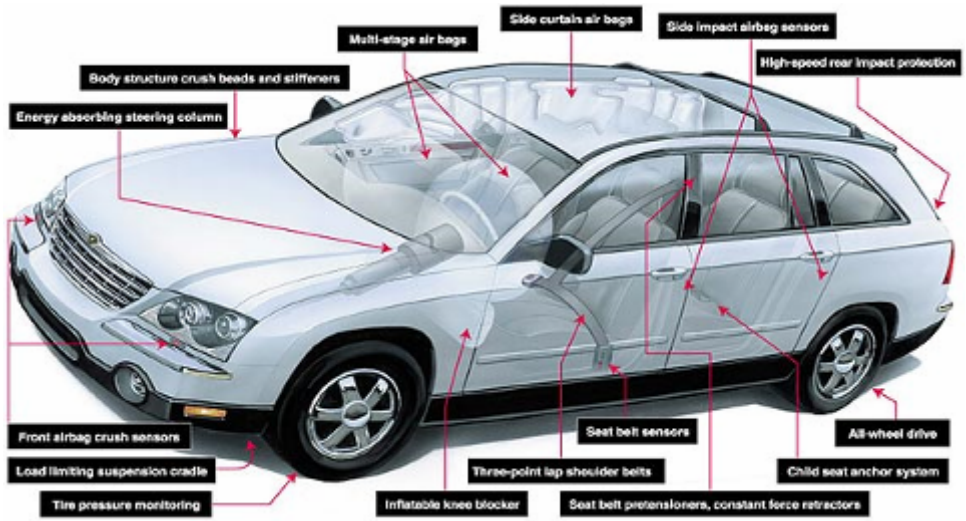
Evolution of Security Requirements



Service-Oriented Network Architecture (SONA)
Composite Services: Guest Access



Benefits of a Systems Approach



- Complex environment
- Gaps and inconsistency
- Lower visibility
- More difficult to manage
- Higher TCO

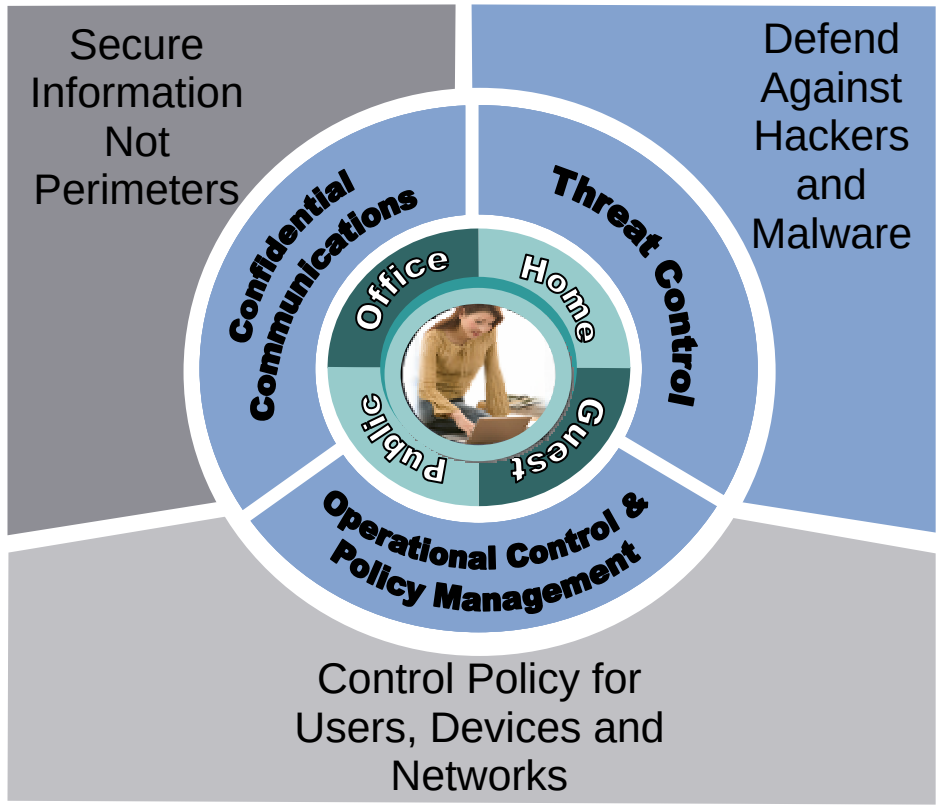
- Simplified environment
- Tighter integration = tighter security
- Greater visibility
- Easier to deploy and manage
- Lower TCO

Protecting Assets and Limiting Exposure

Cisco Vision

- The Self Defending Network protects businesses from IT related security threats
- Cisco delivers SDN through a series of architectures
- The Cisco Secure Wireless Solution delivers
  - Integrity
  - Confidentiality
  - Availability

Cisco Self Defending Network
Secure Wireless Solution



Cisco Secure Wireless Solution

An Architecture that Builds on the Inherent Security of the Cisco Unified Wireless Network to Combine Best of Breed Security Services for Unparalleled Control of Business Resources to Meet Compliance Needs

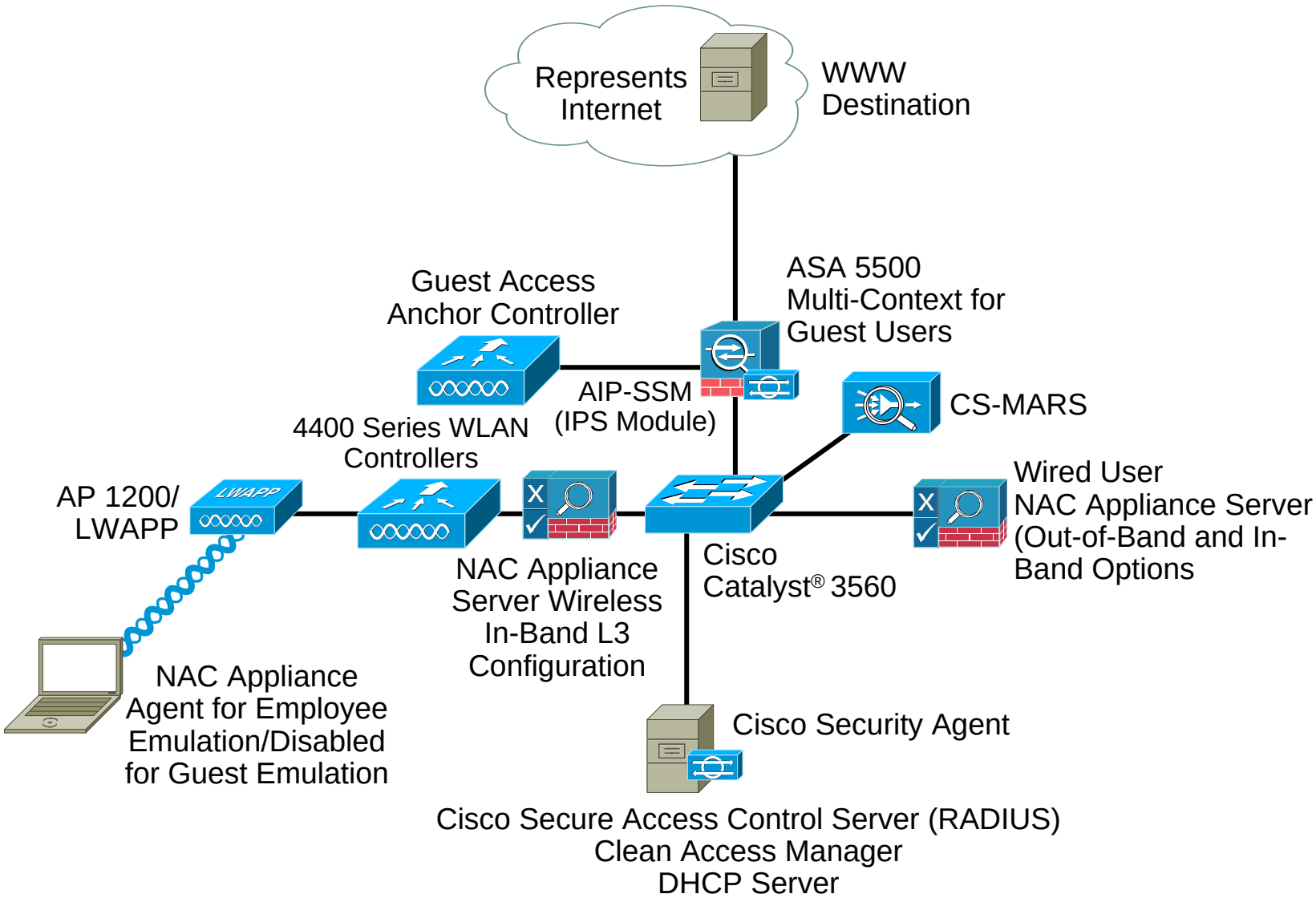
What's New?

- An end-to-end architecture
- Integration of wireless and security
- Industry-leading security services

Key Features

- Unified wired and wireless IPS/IDS
- Client validation, posture assessment and remediation
- Wireless single sign on and 802.1X integration
- Integrated firewall for secure guest access
- Host intrusion prevention
- Rogue detection via automatic RF monitoring

Secure Wireless Solution Architecture

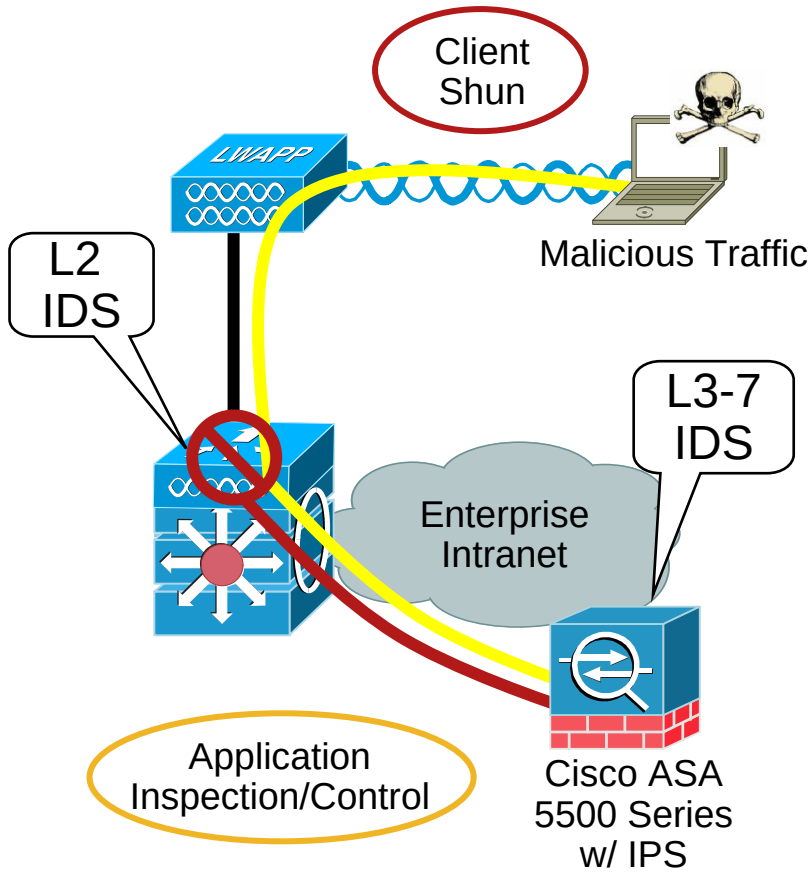


Unified Intrusion Prevention

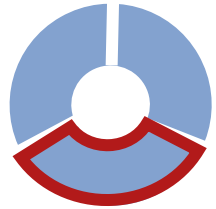
Business Challenge

Mitigate Network Misuse, Hacking and Malware from WLAN Clients

- Inspects traffic flow for harmful applications and blocks wireless client connections
- Eliminates risk of contamination from wireless clients
- Zero-day response to viruses, malware and suspect signatures
- Products:
  - Cisco IPS Software (AIP-SSM w/ ASA 5500)
  - Wireless LAN Controller



Client Validation and Posture Assessment



Business Challenge

Identify Who Is on the Network and Enforce Granular Policies to Prevent Exposure to Viruses and "Malware"

- Ensures wireless client is 'up-to-date' with latest security policies
- Quarantines and fixes any wireless client that is non-compliant
- Enforces differentiated policies and network services based on user role
- Products:
  - NAC Appliance
  - WLAN Controller

Authenticate and Authorize

- Enforces authorization policies and privileges

Scan and Evaluate

- Agent and network scan for required versions and infections

Quarantine and Enforce

- Isolate non-compliant devices from rest of network

Update and Remediate

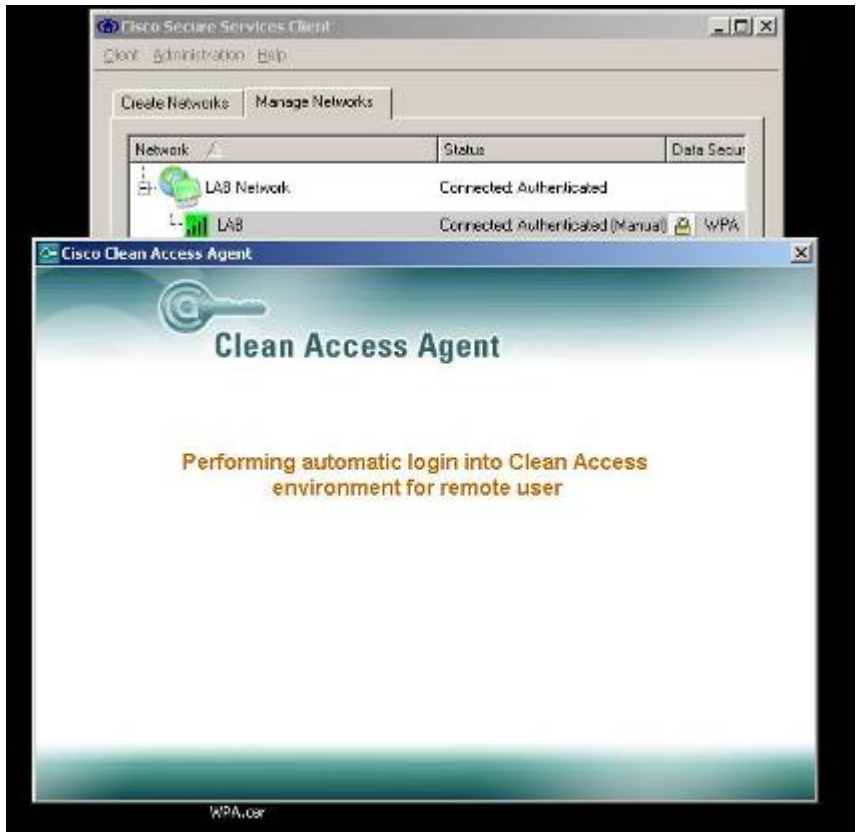
- Network-based tools for remediation of threats and vulnerabilities

Wireless Single Sign on and 802.1X

Business Challenge

Streamline User Experience, Consolidate Accounting, and Improve Password Management

- Integrated user authentication and posture assessment
- Protects the network from malicious code while being noninvasive to the user
- Products:
  - NAC Appliance
  - Cisco Secure ACS
  - Cisco Secure Services Client



Wireless NAC Leadership

Only Cisco Has an Integrated Wireless NAC Solution; All Others Need to Partner to Provide the Same Functionality

2007 GOLD AWARD for Endpoint Security

Scope

- Single NAC solution for both wireless and wired network
  - Apply consistent policy regardless of access method (LAN, WLAN, VPN, etc.)
- Accommodates guest users, unmanaged PCs, and networked devices, such as printers and game consoles

Ease of Use

- Seamless, proven integration with WLC
  - Single sign-on support for 802.1X, AD, MAC address
- Lightweight agent (if required) for optimal user experience
- No changes to infrastructure required

Enterprise-Ready

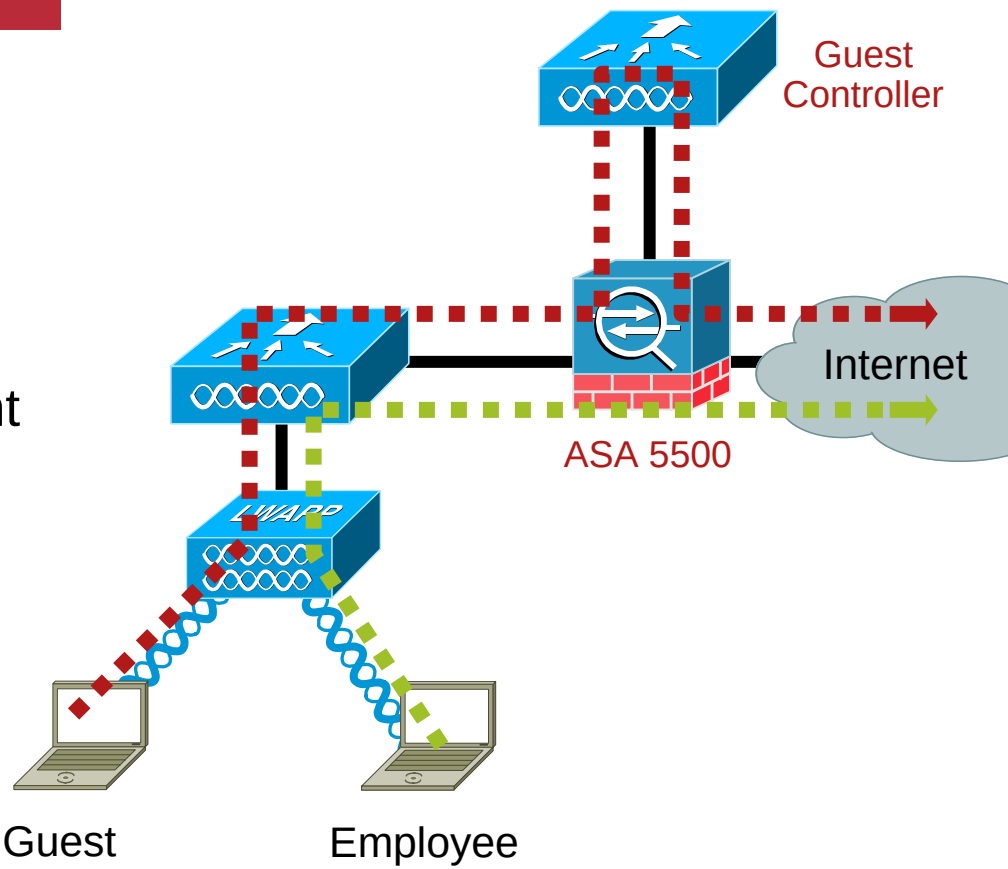
- Over 1,500 customers using Cisco NAC
- Highly scalable
- Fast deployment: fewer than two days for most
- Leverages existing investment in infrastructure and security applications
  - Does not require Cisco infrastructure

Secure Wireless Guest Access

Business Challenge

Offer Secure, Controlled Access to Network Services for Non Employees and Contractors

- Zero touch wireless guest services with integrated stateful firewall for application level control of wireless traffic
- Control or block prohibited traffic patterns at a single point (e.g. P2P, IM, FTP)
- Products:
  - ASA 5500 Firewall
  - WLAN Controller
  - NAC Appliance (Optional)



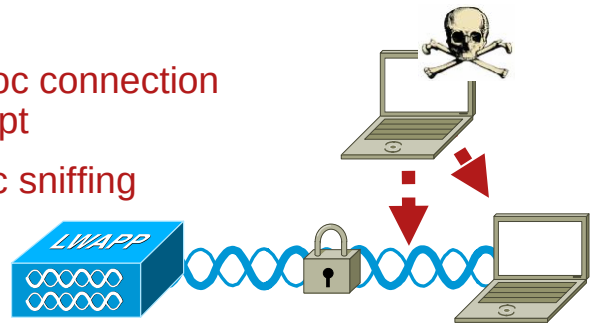
Host Intrusion Prevention

Business Challenge

Standardize on Wireless Client Connection Policies While Protecting Them from Suspect Content and Potential Hackers

- Enforcement of client connection policies:
  - Ad-hoc, SSIDs, VPNs at hotspots
- Restrict wireless access when the device is connected to wired
- Prevents wireless client from exploitation as a bridge into the wired network
- Wireless bandwidth optimization (QoS-WMM)
- Products:
  - CSA v. 5.2

- Ad-Hoc connection attempt
- Traffic sniffing

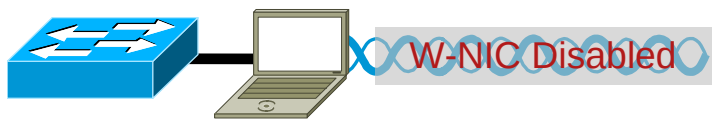


✓Wireless Ad-Hoc restricted

✓SSID allowed

✓VPN enforced

✓Malware disabled and contained



✓Wireless NIC disabled

✓Malware disabled and contained

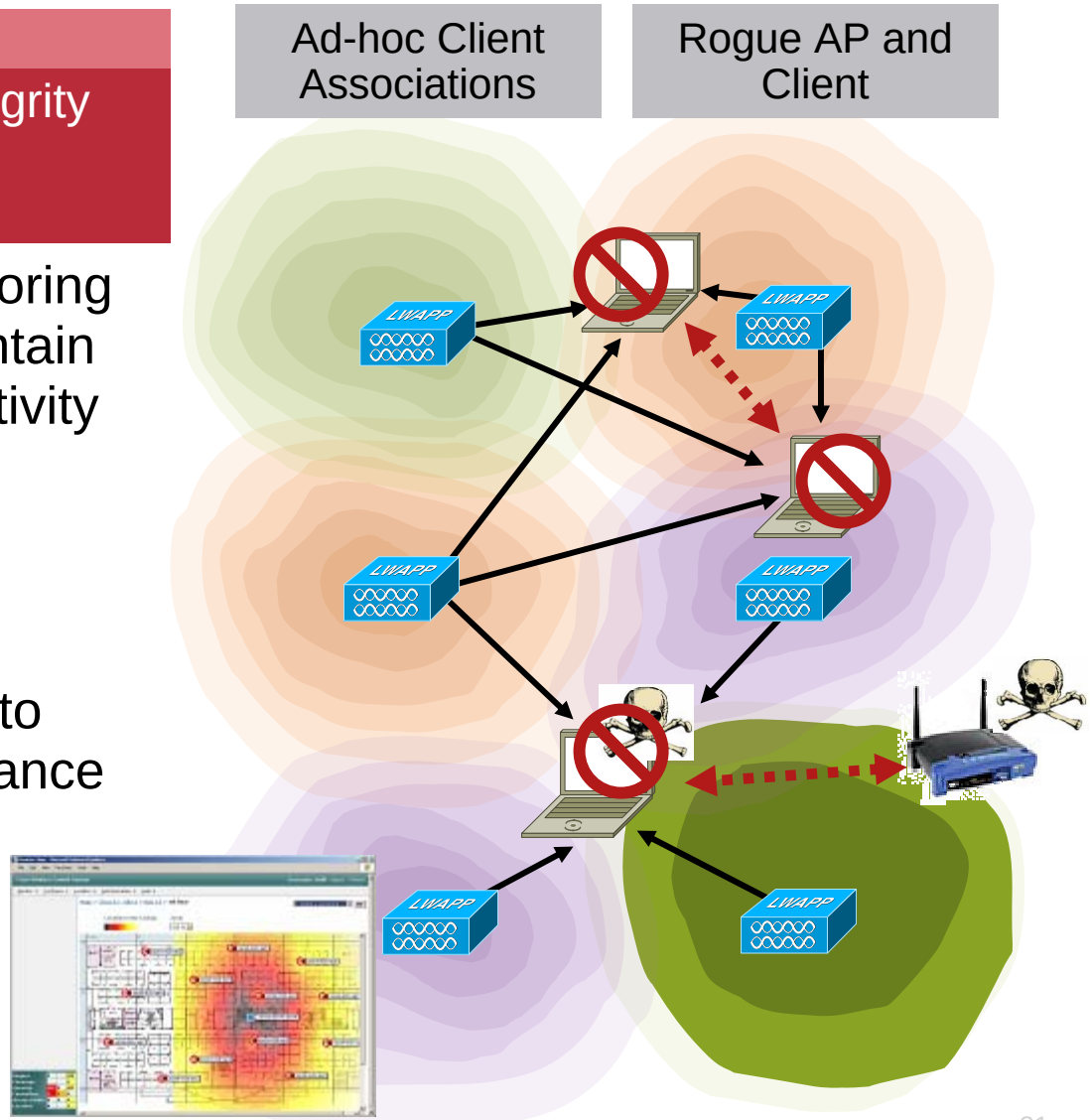
Rogue Detection and Containment

Business Challenge

Protect Network and Information Integrity from Compromise by RF Attacks

- Integrated 24/7 RF monitoring to identify, locate and contain unauthorized wireless activity
- Interfaces into WCS for a single network management view
- Proactive threat defense to ensure regulatory compliance
- Products:

  WLAN Controller + WCS



Rogue Detection Leadership

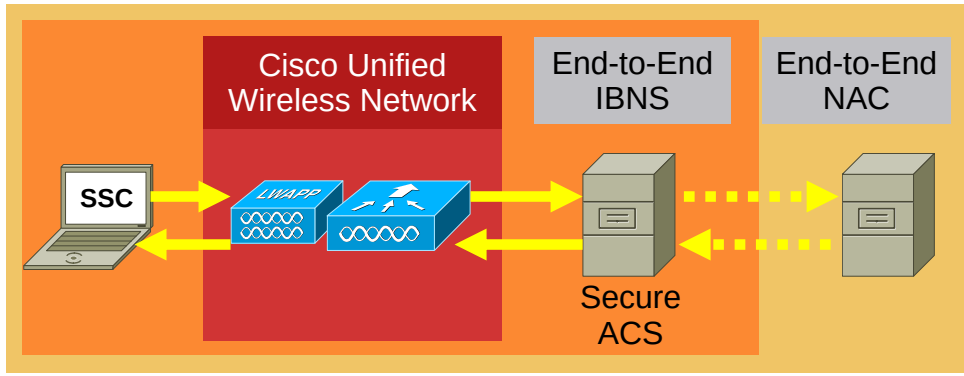
Overlay	Vs.	Cisco
Stand Alone IDS Application		Single WLAN Security Platform
Monitors Policy		Monitors and Enforces Policy
Requires Overlay Sensors, Cabling and Servers		Integrated Directly into WLAN Infrastructure
No Location Capability		Integrated Location Tracking
Typically Deployed at a Ratio of One Overlay Sensor for Every 5–10 APs		All AP's Within the WLAN Perform IDS/IPS Functionality
Separate NMS—No Policy Synchronization		Single NMS Interface for Entire WLAN Configuration, Monitoring and Enforcement
No Support for Custom Signatures		Custom Signatures Supported
Additional CAPEX		Standard Feature

Simple, Secure Client Connectivity

Business Challenge

Deploying and Managing a Common Security Profile Across an Increasingly Diverse Array of Wireless Clients

- A single 802.1X authentication supplicant for wired and wireless devices
  - Simplified management
  - Improved security
  - Lower total cost of ownership (TCO)
- Encryption of management frames
- Products:
  - Cisco Secure Services Client
  - Cisco Secure ACS
  - Cisco Compatible Extensions



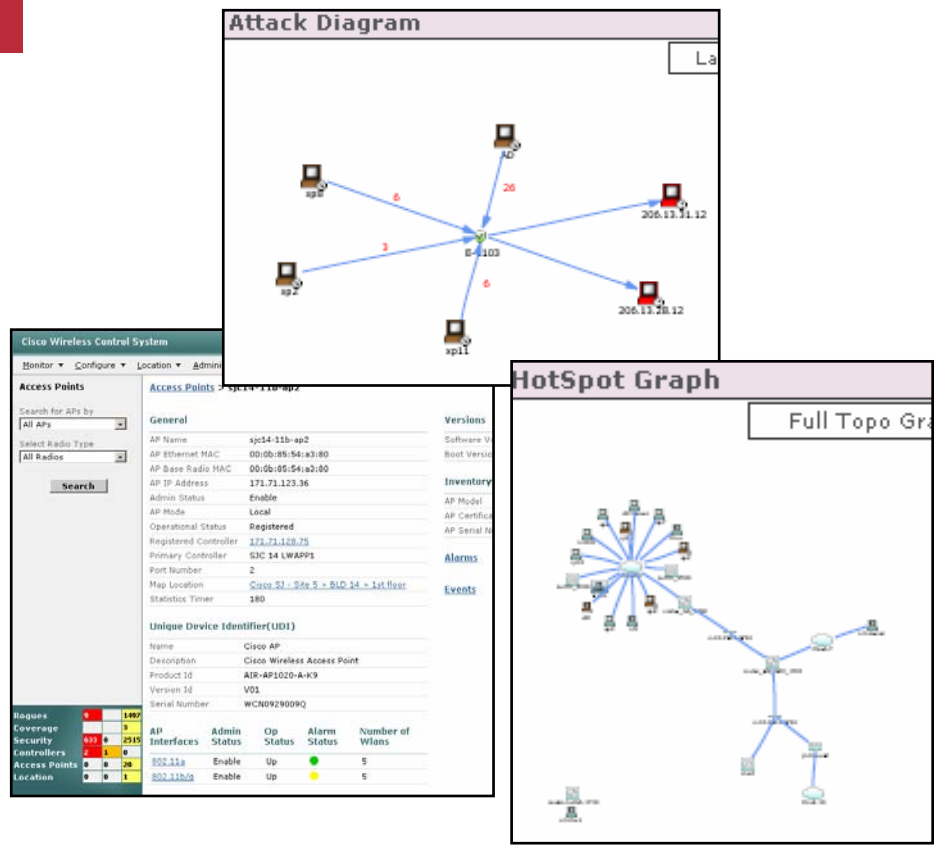
- ✓ Management Frame Protection
- ✓ Fast Secure Roaming
- ✓ LEAP and EAP-FAST

Wireless Security Management

Business Challenge

Supporting and Maintaining a Diverse Range of Security Products, Correlating Events and Delivering Concise Reporting

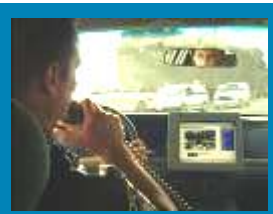
- WCS offers central, one-touch configuration and management of wireless security profiles
- Security alerts are located and viewed graphically
- CS-MARS allows quick response with incident capture and event correlation for security alarms
- Products:
  - CS-MARS
  - WCS



Case Study: Major Financial Institution

- Challenge
  - Lack of visibility into events and vulnerabilities associated with the RF environment
  - Distinct need for rogue access points and device detection
  - Need secure, scalable wireless system that meets business compliance requirements
- Solution
  - Cisco Unified Wireless Network with integrated wireless IDS
  - The Cisco 2710 Wireless Location Appliance
- Business Results
  - Increased productivity—rogue access point detection has eliminated the need for IT staff to manually walk through the building scanning for rogues
  - Lower operational cost due to single management interface for wireless and security management (no need for an overlay system)





Case Study: University of Portland

THE UNIVERSITY OF PORTLAND
OREGON'S CATHOLIC UNIVERSITY

- Challenge
  - Fear of network disruption due to viruses or “malware” from students and visitors
  - Difficult to upgrade security policies due to lack of centralized management
- Solution
  - Cisco Unified Wireless Network with integrated Security and Guest Services
  - Cisco Network Admission Control solution
- Business Results
  - Ability to offer guest services with confidence that security policies will be maintained on all devices
  - Faster response times to new security vulnerabilities or wireless upgrades through centralized management

Secure Wireless Solution Summary

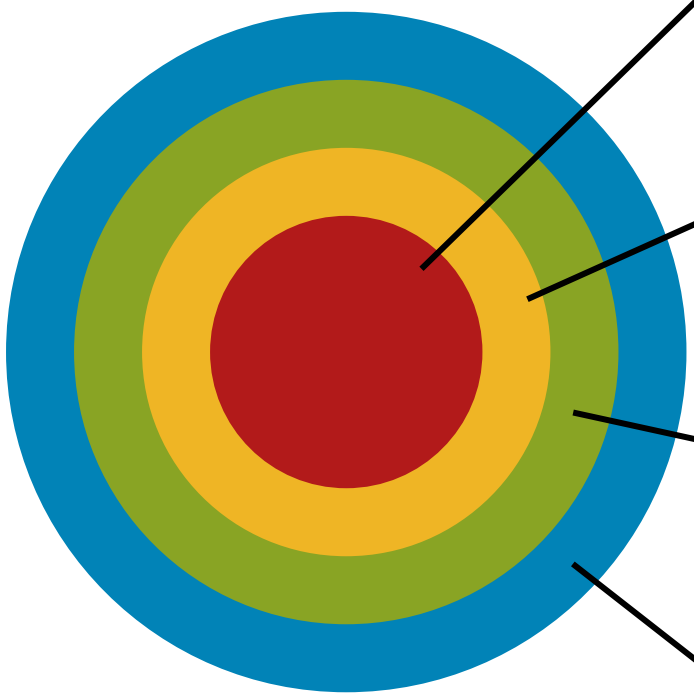
- The Secure Wireless Solution builds on the robust security of the Unified Wireless Network
  - The solution is designed to be modular and flexible
  - Not all or nothing
- The Cisco Unified Wireless Network is equipped with industry leading security standards “out of the box”
  - WPA and WPA2
  - 802.1X support
- Broadest level of integrated security features
  - Unified wired and wireless IPS/IDS
  - Management Frame Protection
  - Wireless posture assessment and role based access

Contents

- 1 Wireless Overview: Drivers and Security Risks
- 2 Secure Wireless for Regulatory Compliance
- 3 Cisco Secure Wireless Solution
- 4 Wireless Security Planning: Benchmark Analysis
- 5 Architectures and Design Principles

Wireless Security Phases

Benchmark Preparedness



Phase 1: Critical
WLAN Security Fundamentals

Phase 2: Urgent
Traffic and Information Integrity

Phase 3: Recommended
Endpoint Control and Protection

Phase 4: Best Practice
Network Visibility and Policy

Critical: WLAN Security Fundamentals

Deployment of Baseline Security for a Safe Wireless LAN

- Strong user authentication

  (802.1X, EAP/EAP-Fast, ACS for AAA)

- Strong transport encryption

  (802.11i, AES, TKIP, MFP, WPA/WPA-2)

- Protect network broadcasts

  (Disable SSID broadcast)

- Detect and prevent rogue APs, clients, ad-hoc networks, DoS, etc.

  (Audits, RF scanning, wireless IPS)

- Strong passwords if using LEAP

  (Pre-configured clients and tokens)

Urgent: Traffic and Access Control

Tight Control of WLAN Traffic, Including Information Integrity and Network Access

- Device posture assessment

  (NAC for client/clientless connections)

- Dynamic, role-based network access and managed connectivity

  (NAC, CSSC, VLANs)

- WLAN threat mitigation

  (Unified wired and wireless IPS)

- Perimeter Control

  (ASA—L2-7 firewall, stateful inspection, app inspection)

Recommended: Endpoint Protection

Endpoint Inspection, Hardening, and Control

- Endpoint connection policy/status

  (WLAN Controller, NAC, MFP)

- Endpoint malware mitigation

  (CSA)

- Threat alert distribution

  (CSA + IPS + MARS)

Best Practice: Network Visibility

Network-Wide Visibility for Event Reporting and Correlation

- Comprehensive WLAN security management, rogue location prediction, client troubleshooting

  (Wireless Control System)

- Security event analysis and correlation

  (CS-MARS)

- Spectrum analysis

  (Cognio for 2.4GHz and 5GHz spectrum analysis—delineates Wi-Fi, Bluetooth, microwaves, etc.)

Wireless Security Policy Concepts

1. Objective:

   Clearly define policy goals, and what it is expected to achieve or prevent

2. Ownership and authority:

   Identify policy owners and specify intervention authority and contingencies

3. Scope:

   Users, groups, guests, contractors, visitors, and devices that must comply

4. Risk assessment:

   Potential threats, affected assets, and potential business impact

5. Security practices:

   Authentication, access control, authorization, confidentiality, integrity, availability, ad-hoc devices, firewall, traffic inspection

6. Acceptable usage:

   Client distribution, clientless access, device posture assessment, acceptable behavior, network segmentation and assignment

7. Deployment:

   Trial WLAN and production implementation, testing and verification, policy refinement, training administrators, educating end-users

8. Auditing and enforcement:

   Monitoring, identification, investigation, and permanent resolution of events, consequences of non-compliance, internal and/or third-party auditing, identification of regulatory compliance requirements

15 Minute Break

Contents

WLAN Security Fundamentals

- Wi-Fi Protected Access
- IEEE 802.1X—authentication
- IEEE 802.11i—link encryption
- Management Frame Protection
- Cisco Compatible Extensions
- Fast Secure Roaming

Wi Fi™ Protected Access

All Wireless Traffic **Must Be Authenticated and Encrypted** Between the Client and the Access Point to Ensure Information Integrity

What are WPA and WPA2?

- Authentication and Encryption standards for Wi-Fi clients and APs
- 802.1X authentication
- WPA uses TKIP encryption
- WPA2 uses AES block cipher encryption

Which should I use?

- Gold, for supporting NIC/OS'es
- Silver, if you have legacy clients
- Lead, if you absolutely have no other choice (i.e. ASDs)

Gold

WPA2/802.11i
- EAP-FAST
- AES

Silver

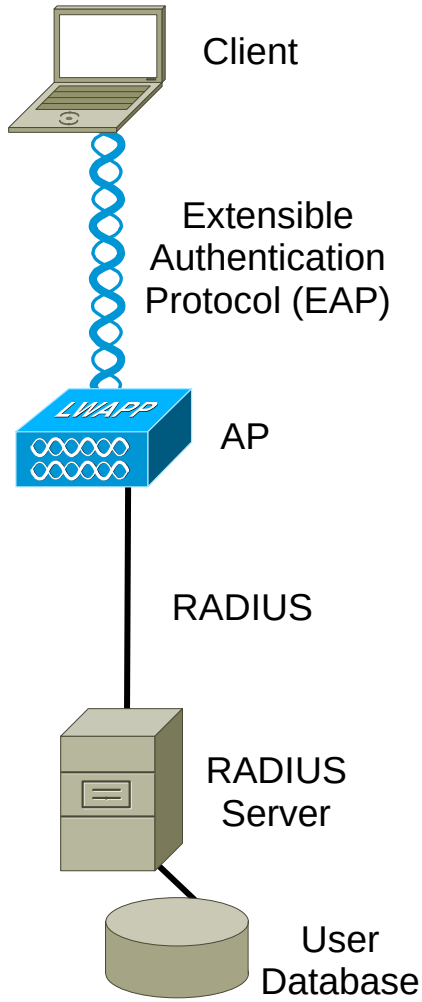
WPA
- EAP
- TKIP

Lead

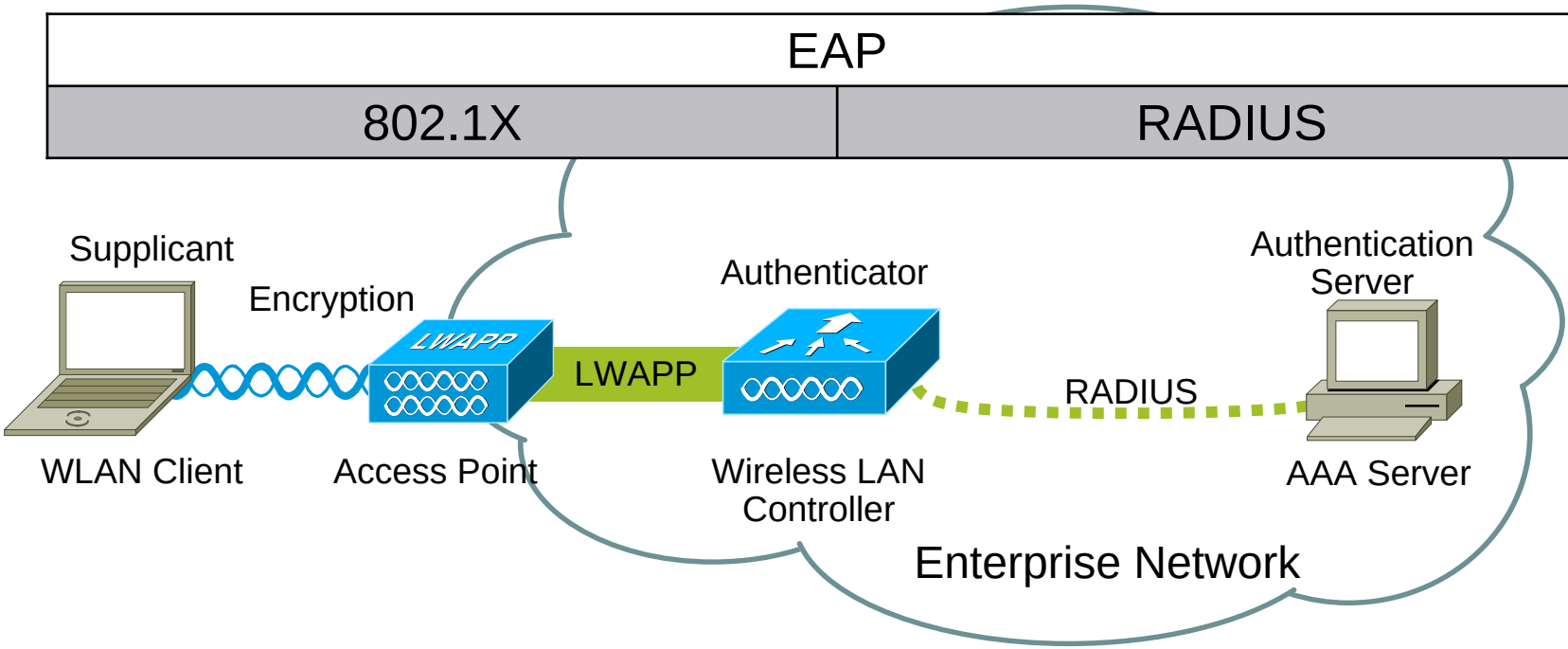
Dynamic WEP
- EAP/LEAP
- VLANs + ACLs

802.1X Authentication Overview

- IEEE 802.11 Task group i recommendation for WLAN authentication
- Supported by Cisco since December 2000
- Extensible and interoperable—supports:
  - Different EAP authentication methods or types
  - New encryption algorithms, including AES as a replacement for RC4
- Key benefits
  - Mutual authentication between client and authentication (RADIUS) server- Mitigation for unauthorized clients/ rogue AP
  - Encryption keys derived after authentication — No requirement to manually manage keys
  - Centralized policy control — Automated encryption policy/ user access to authorized resources



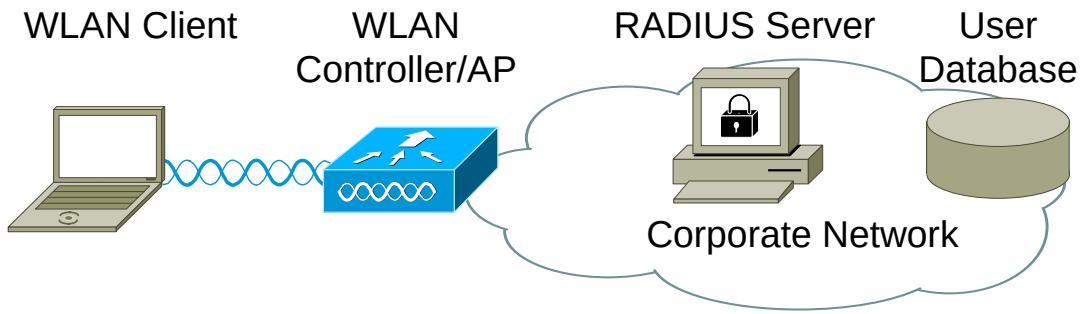
Overview of 802.1X/EAP



- **Enterprise WLAN Security relies upon 802.1X authentication**
- **802.1X is port based security**
  - The association process establishes a virtual port
  - Encryption protects that virtual port

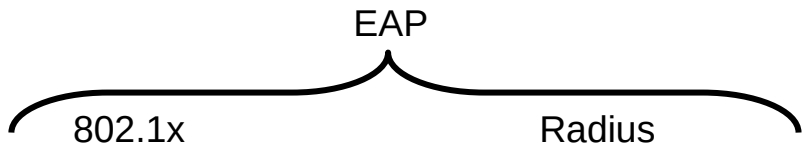
How Does Extensible Authentication Protocol (EAP) Authenticate Clients?

Client Associates



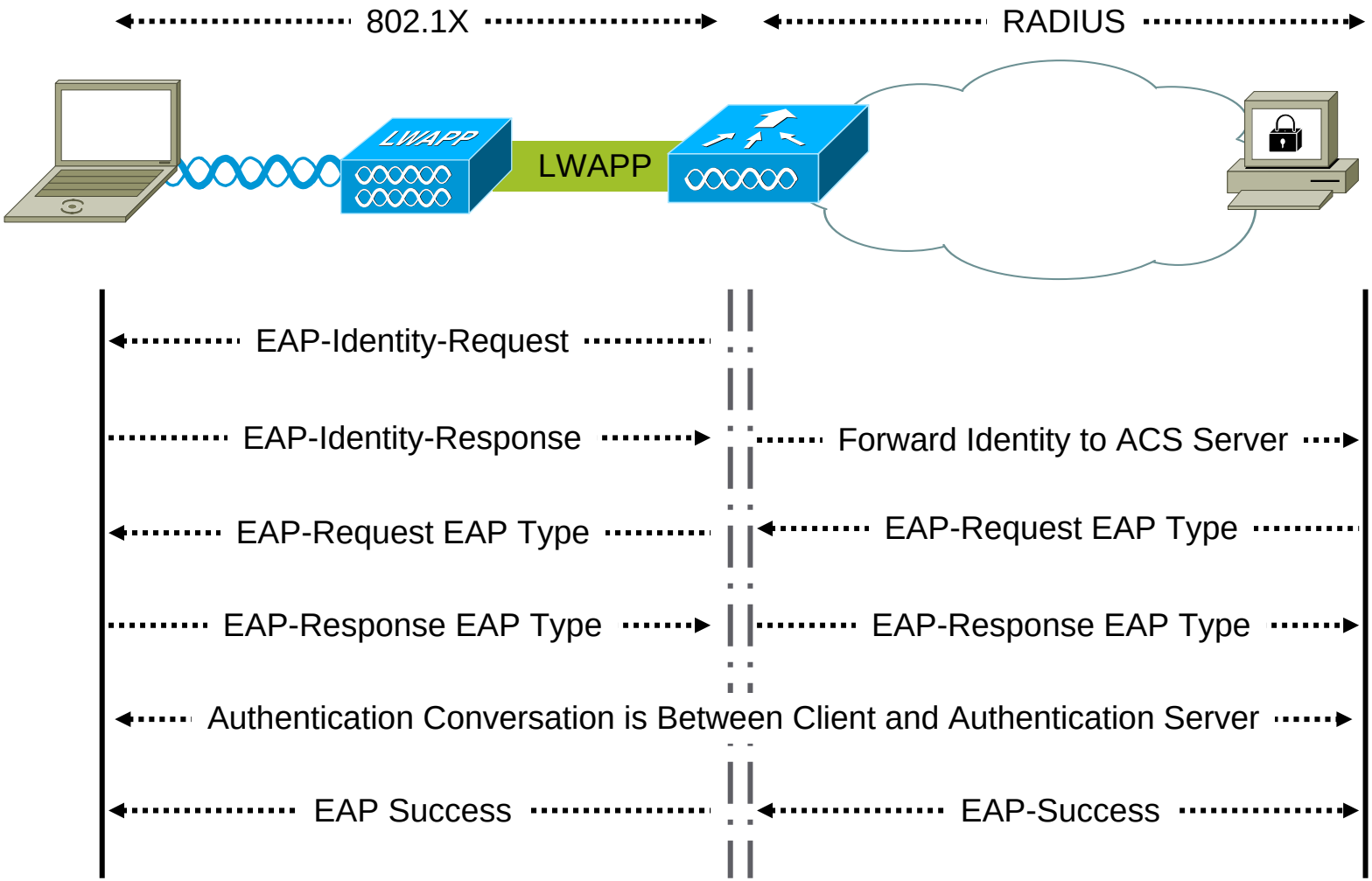
Cannot Send Data Until…

…EAP Authentication Complete



Client Sends Data

EAP Authentication

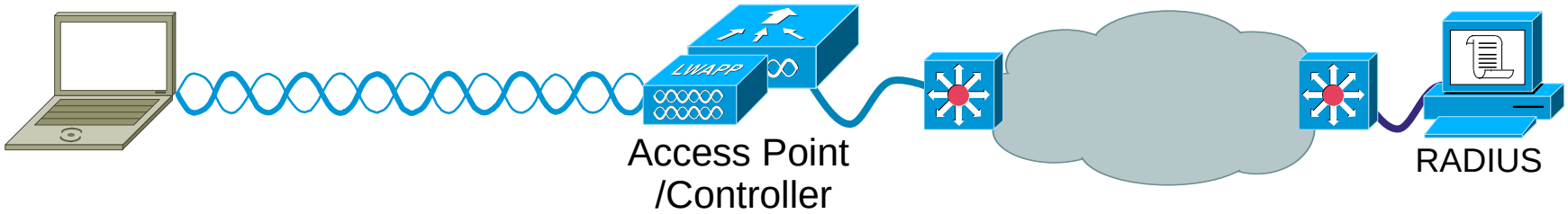


EAP Protocols: Feature Support

	EAP-TLS	PEAP	LEAP	EAP-FAST
WPA Support	Yes	Yes	Yes	Yes
Client Certificates	Yes	No	No	No
Server Certificates	Yes	Yes	No	No
Application Specific Device (ASD) Support	No	No	Yes	Yes
Fast Secure Roaming (CCKM)	No	No	Yes	Yes
Local Authentication	No	No	Yes	Yes
Deployment Complexity	High	Medium	Low	Low
RADIUS Server Scalability Impact	High	High	Low	Low/ Medium
Off-Line Dictionary Attacks	No	No	Yes[1]	No

[1]Strong Password Policy Recommended. Please Refer to:
http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html

802.11i/WPA Authentication and Key Management Overview



Capabilities Discovery

802.1X Authentication

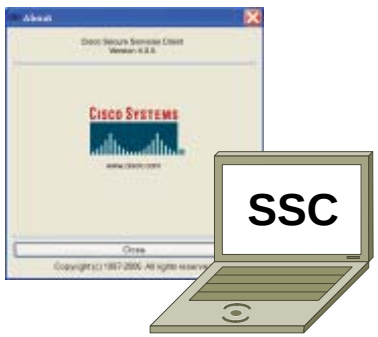
Key Management

Key Distribution

Data Protection

Introducing: Cisco Secure Services Client

- Cisco Solution Support:
  - Network Admission Control
  - Cisco Secure ACS
  - Identity Based Network Security for Catalyst switches
  - Cisco Unified Wireless Network

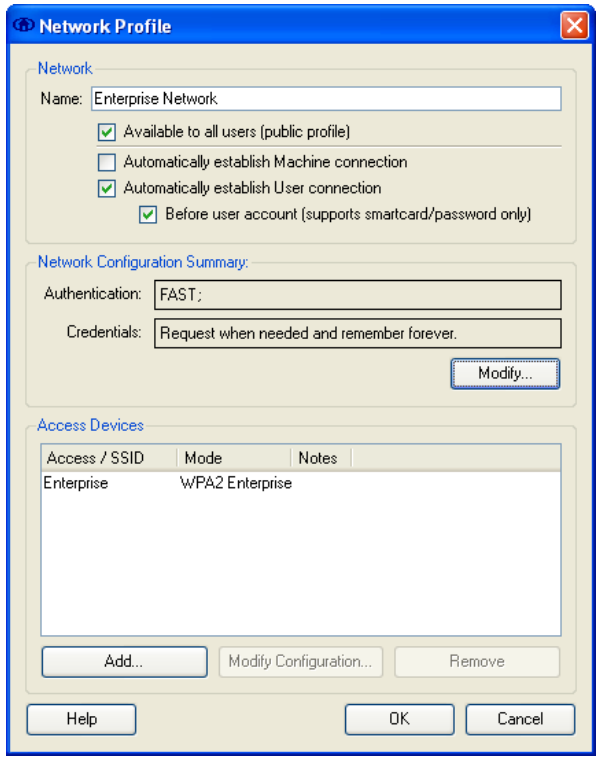


Cisco Secure Services Client

- Features
  - Unified wired and wireless client
  - Support for industry standards
  - Endpoint integrity
  - Single sign-on capable
  - Enabling of group policies
  - Administrative control
- Benefits
  - Reduces client software
  - Simple, secure device connectivity
  - Minimizes chances of network compromise from infected devices
  - Reduces complexity
  - Restricts unauthorized network access
  - Centralized provisioning

CSSC Configuration

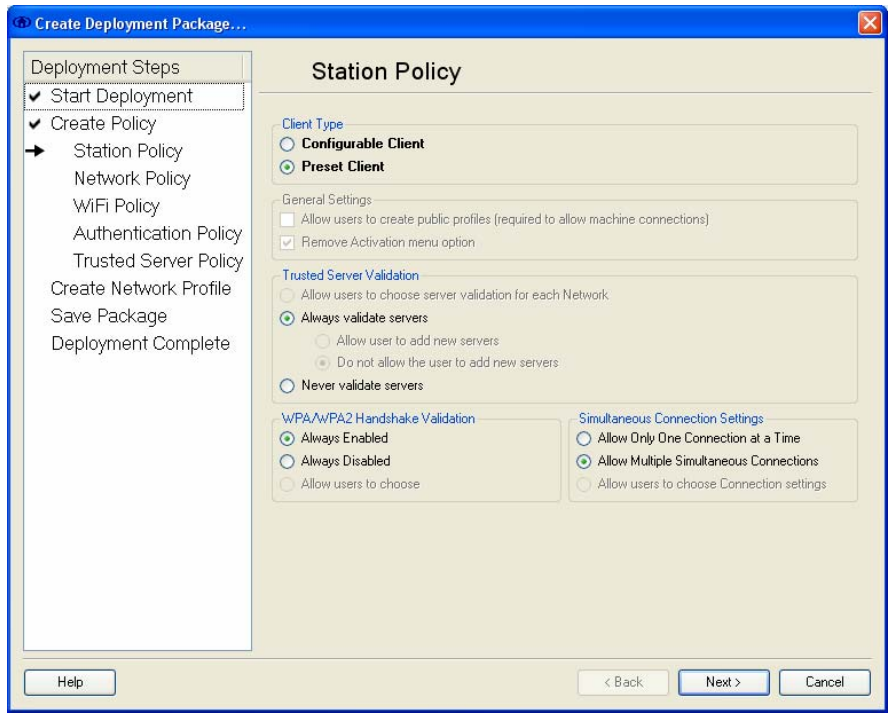
- Network Profile
- Profile restriction
- Authentication configuration
- Access devices—WLAN SSID, Ethernet interface
- Configurable for auto/manual establish
- Machine/user authentication



Flexible Credential Selection and Logon Integration Allows the CSSC Solution to Work for Many, Varied Customer Use Scenarios

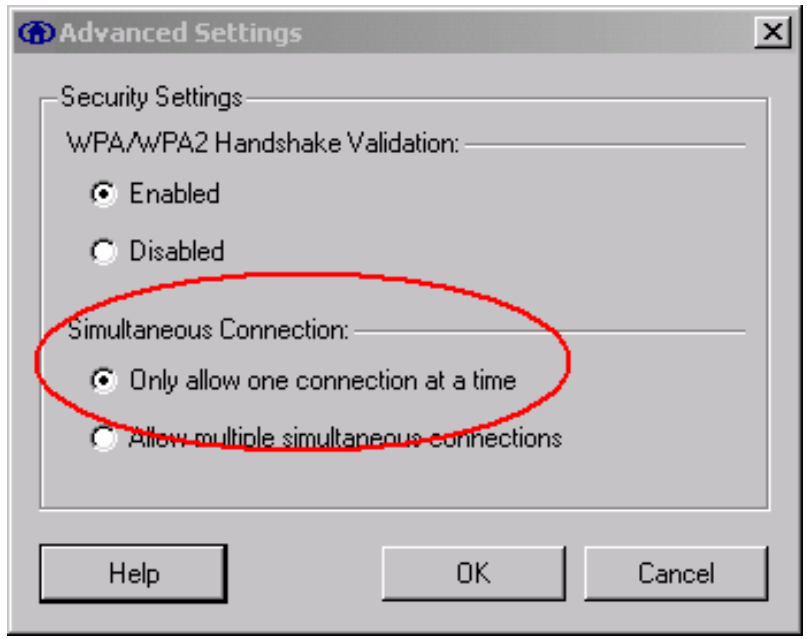
CSSC Deployment Mechanism

- Administrator tool to create profiles
- "Policy" deployment restricts user control of CSSC
  - Server validation
  - EAP type
  - WLAN encryption
- Server trust requirement
  - Per PAC authority
  - Per RADIUS server certificate

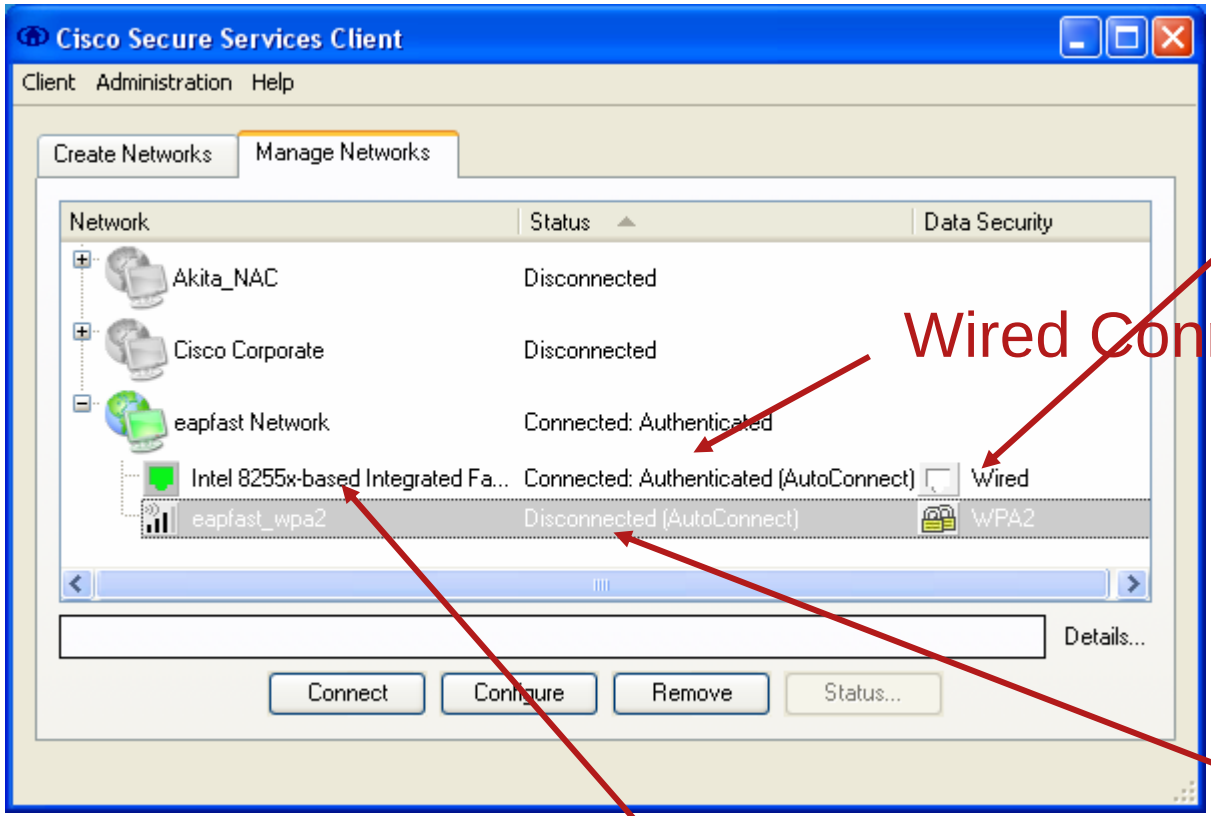


CSSC “No Wireless when Wired” Feature

- Enables wireless interface to be disabled when a wired connection is present
- Note that this feature requires that both 802.11 and Ethernet connection are included under network profiles
- Port control is activated for a single 802.1X session
- Prevents unwanted wireless bridging to wired network



Demo—Disabling Wireless when Wired



Connect Wired Ethernet

Wired Connection Established

Wireless Disabled

Initially Connected Using Wireless Adapter

Cisco Compatible Extensions
The Standard for Client Advancement

Over 90% of Client Devices Cisco Compatible

Client Devices

Features

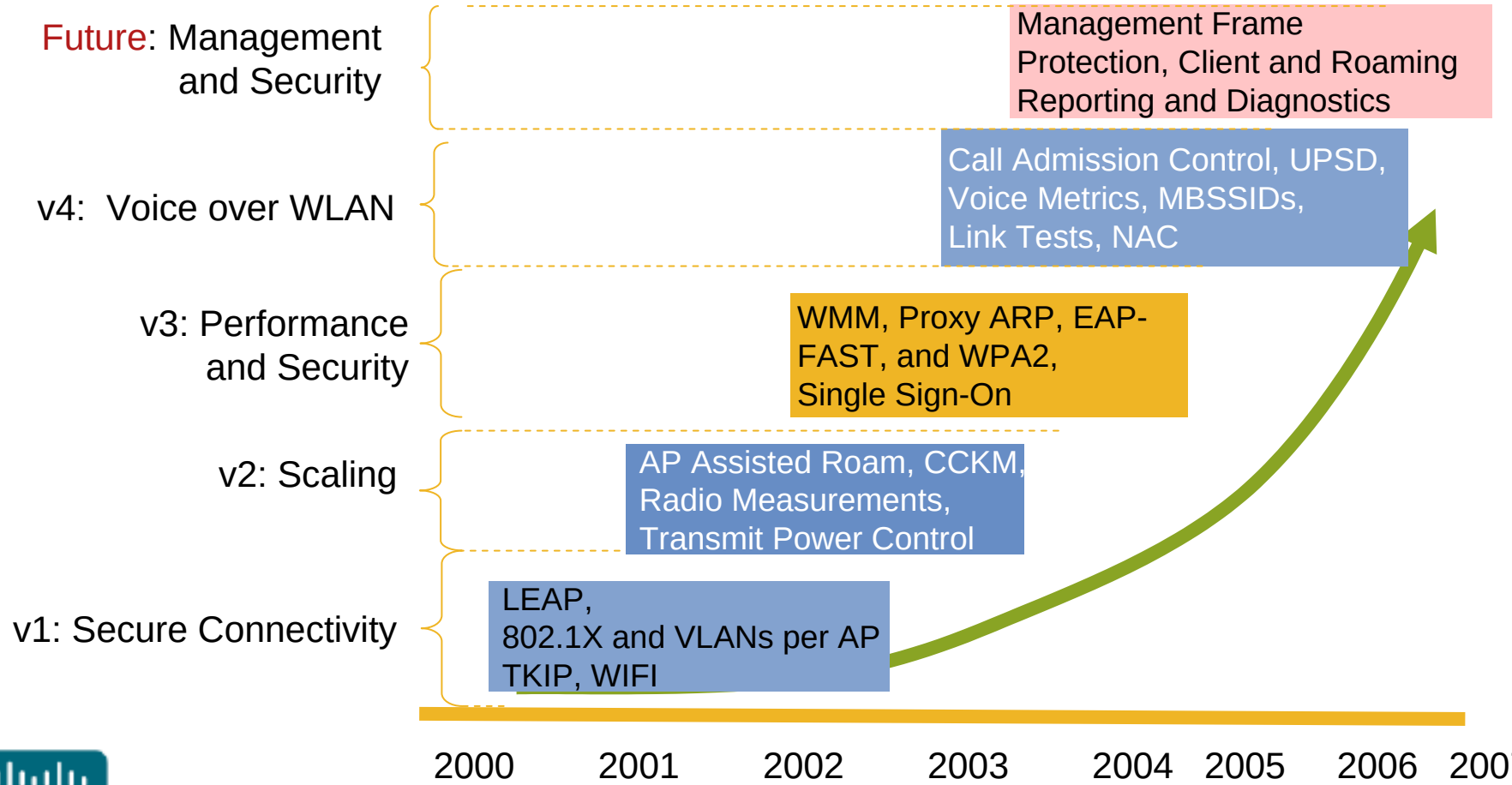
- Assured compatibility with 400+ devices
- Standards-based
- Enhanced security, mobility, and performance
- Supports Mobility Services i.e.. Location, voice

Benefits

- Accelerates innovation
- Supports diverse enterprise applications
- Ensures multi-vendor interoperability
- Enables simplified deployment of mobile WLAN clients

http://www.cisco.com/go/cicsocomipatible/wireless

Cisco Client Extensions (CCX) Roadmap

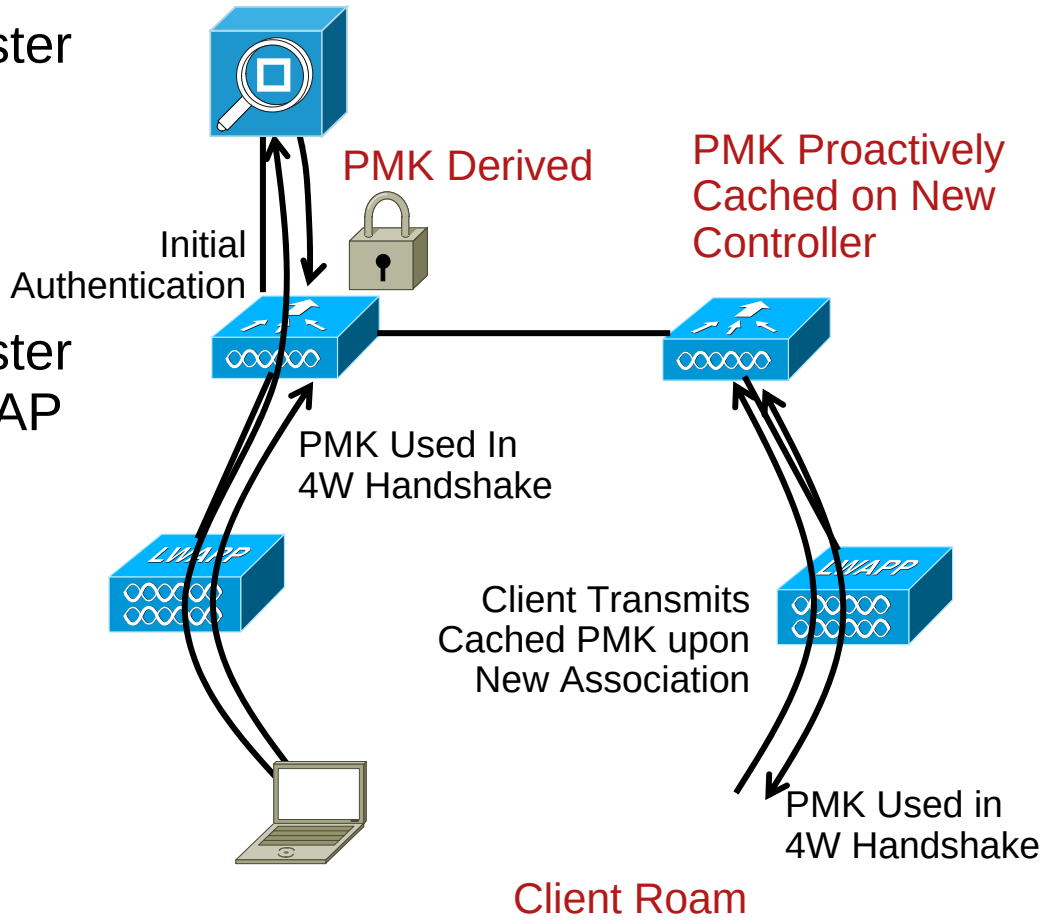


Fast Secure Roaming—Wireless Voice

- Fast secure roaming is required:
  - For latency sensitive applications (e.g. voice)
  - To avoid application disruption due to lengthy (re) authentication times as a client roams between access points
- Cisco implements fast secure roaming via key caching:
  - Handled by the controller for the Unified Wireless Network
- Requires WPA2 client authentication
  - Implemented with Microsoft WPA2 client
  - Other WPA2 clients also support PMK caching
- Cisco delivers CCKM (802.11r) for fast secure roaming

Fast Secure Roaming for Secure Voice Proactive Key Caching (PKC)

- Extension of Pairwise Master Key caching
- Leverages client use of Master Key caching
- Permits knowledge of Master Key before client roam to AP on new controller
- Controller mobility group automatically exchanges the key



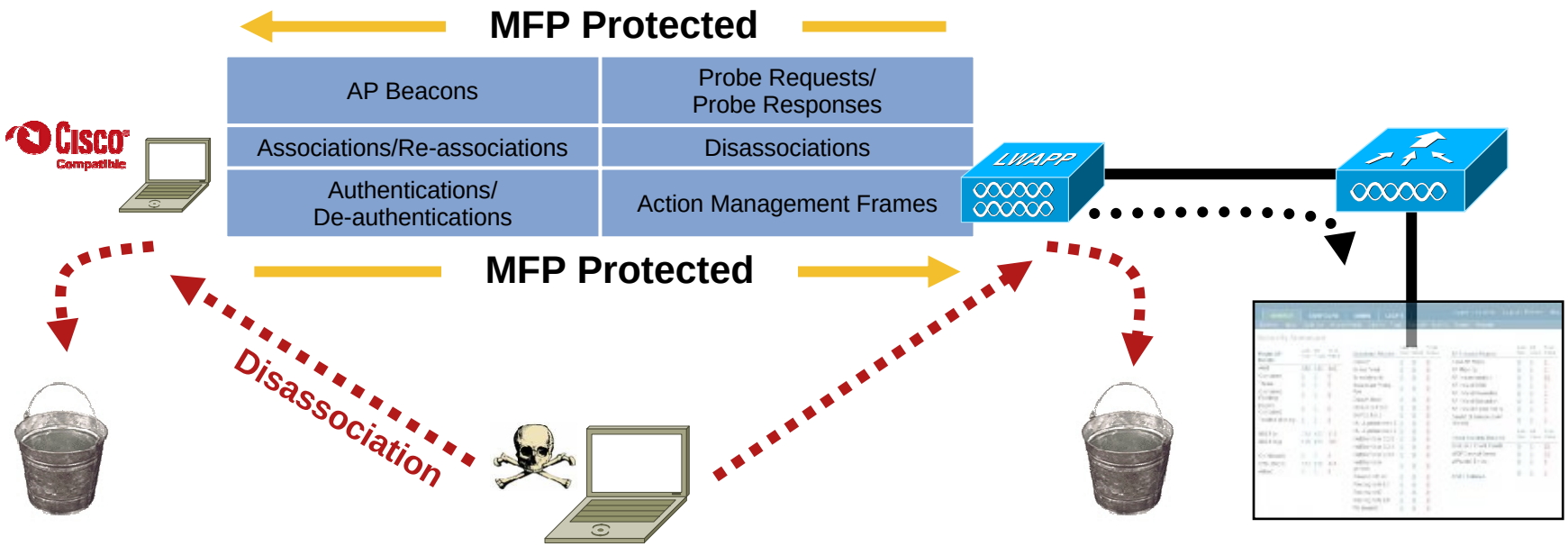
Management Frame Protection

Problem

- Wireless management frames are not authenticated, encrypted, or signed
- A common vector for exploits

Solution

- 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



Benefits of MFP

- Protection: For rogue AP, man-in-the-middle exploits, other management frame attacks
- Prevention: Will be supported in clients capable of decrypting the signature
- Increases the fidelity of rogue AP and WLAN IDS signature detection
- Cisco security leadership and innovation
- Proposed standard—IEEE 802.11w

WLAN Security Fundamentals Summary

- WLAN Security encompasses both authentication and encryption; both components are encompassed with standards bodies and industry consortiums
- There are a number of EAP types available; be ascertain that the chosen EAP authentication type employed is compatible with authentication database and client devices
- WPA provides both dynamic, per-packet keying in addition to key authentication/message integrity
- Cisco Secure Services Client and Cisco Compatible Extensions improve client security and management
- Management Frame Protection encrypts the management frames to mitigate the risk of common wireless LAN security attacks
- Fast secure roaming improves security for latency sensitive applications including voice over wireless

Posture and Remediation

- NAC Appliance Business Case
- NAC Deployment Options

Wireless Network Admission Control

Network Admission Control Uses the Network Infrastructure to Enforce Security Policies on Devices Seeking to Access Network Resources

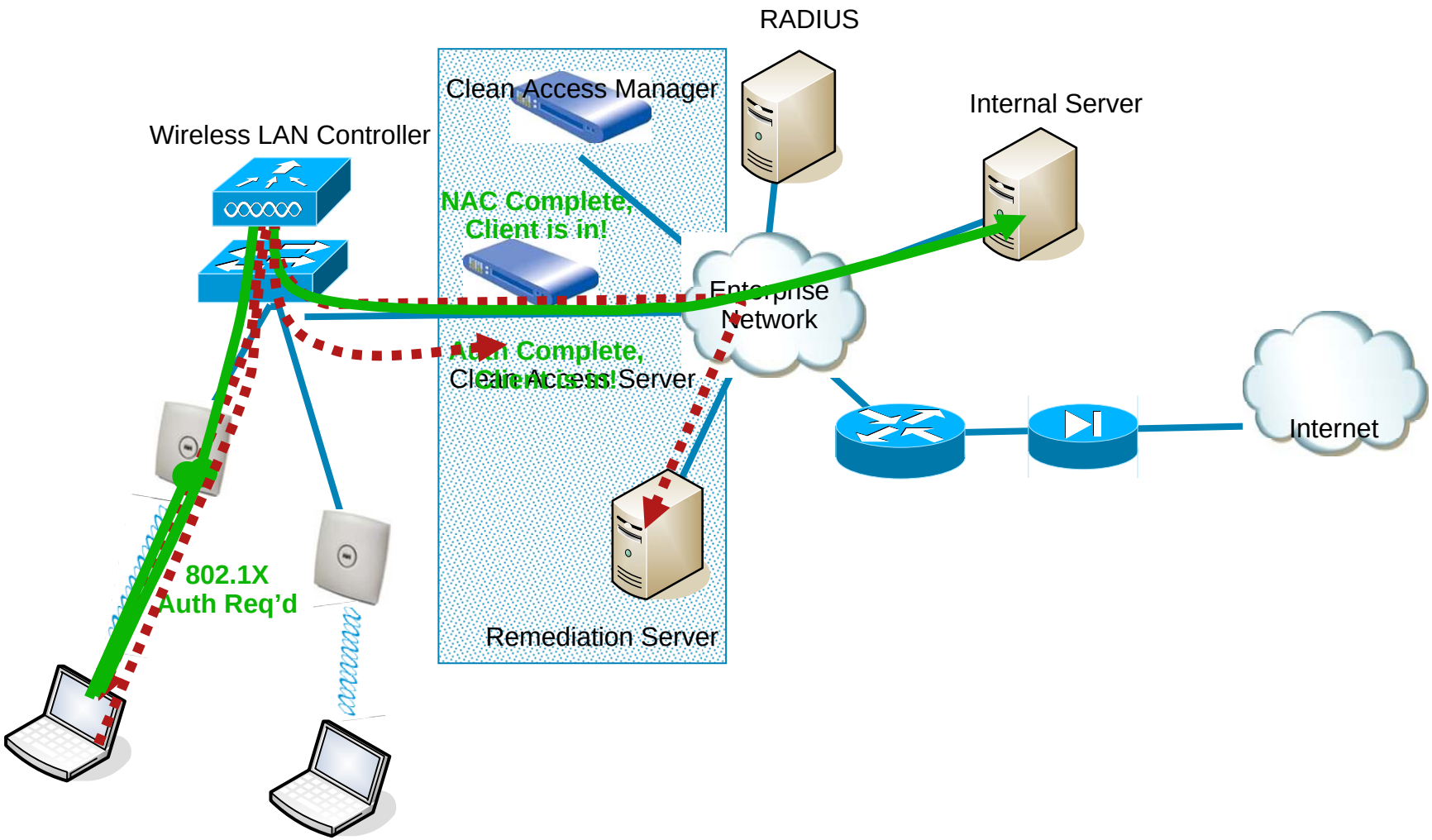
- Mobile/wireless clients are obvious platform for spreading contamination
  - Users on managed devices may be in public locations
  - Users are often guests and contractors — on unmanaged devices
- IT Managers primarily concerned with controlling network access and threats to network availability
- Ensuring devices accessing the network comply with policy (security tools installed, enabled, and current) is difficult and expensive without NAC

"Gartner believes that NAC is too valuable a capability to ignore . . ."

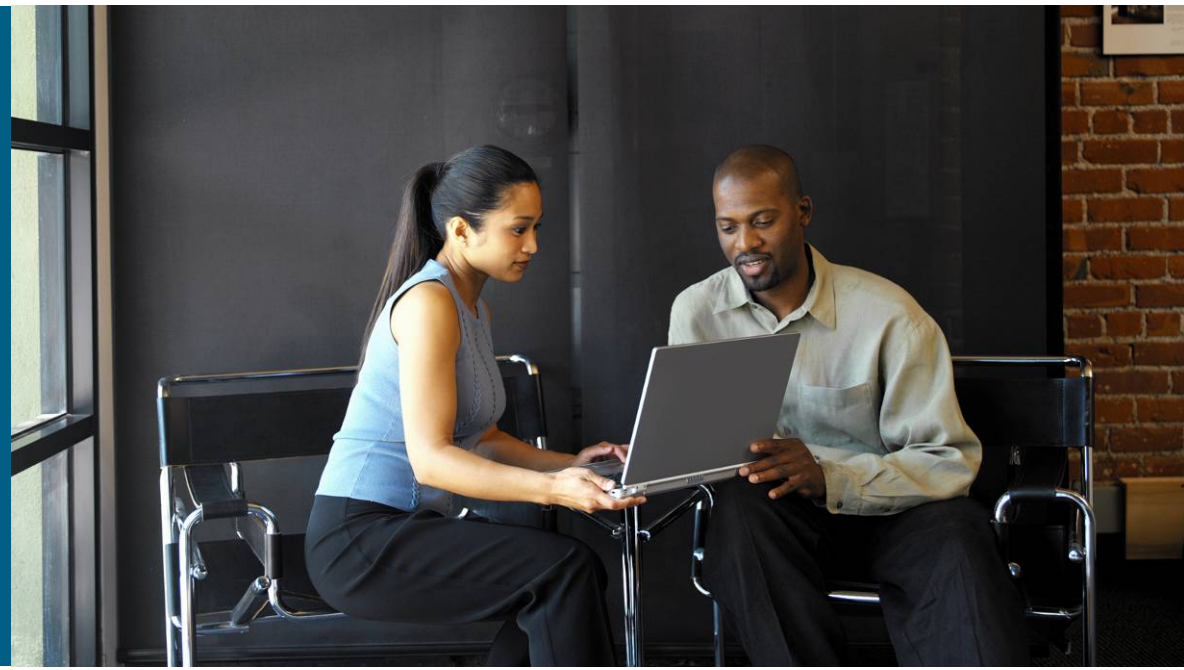
Gartner Research Note G00143551, October 5, 2006

Source: Network Computing Reader Poll and Current Analysis
Network Computing July 2006, 303 Respondents

Wireless Network Admission Control

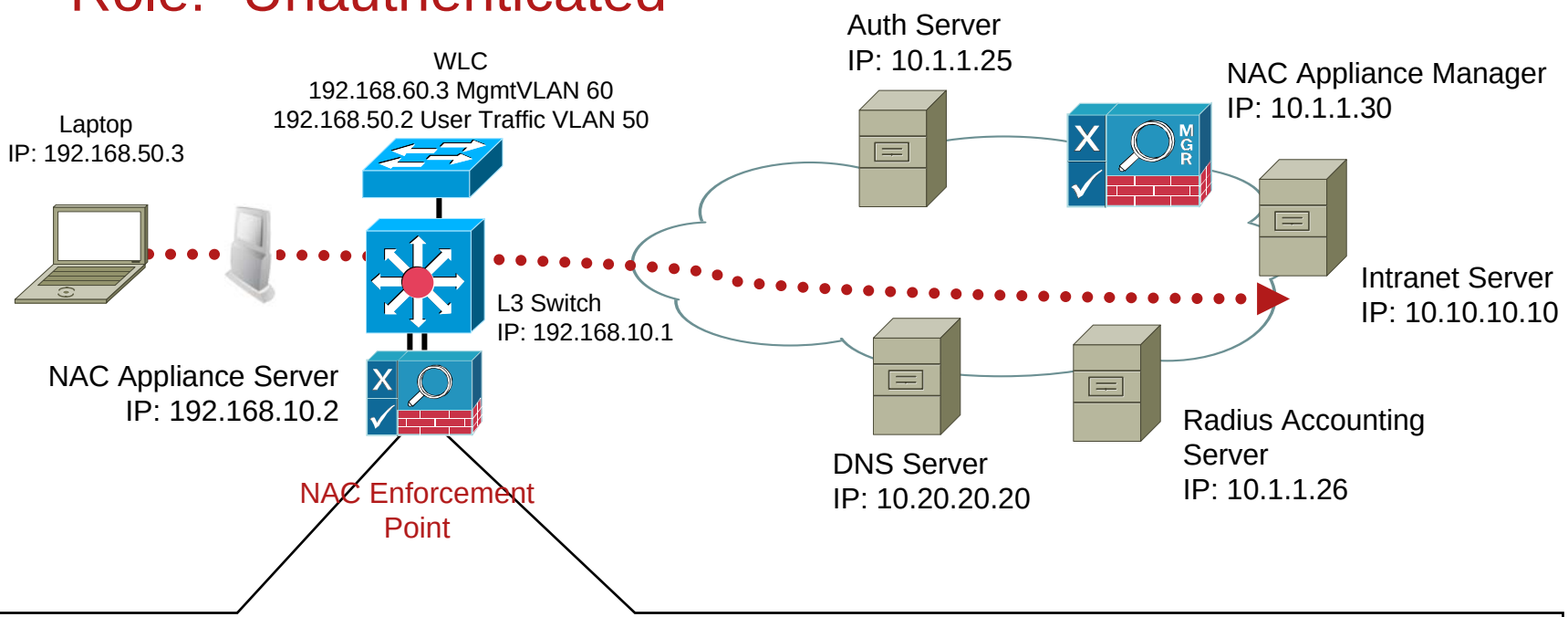


Demo:
Wireless NAC



NAC Appliance Process Flow Wireless Access

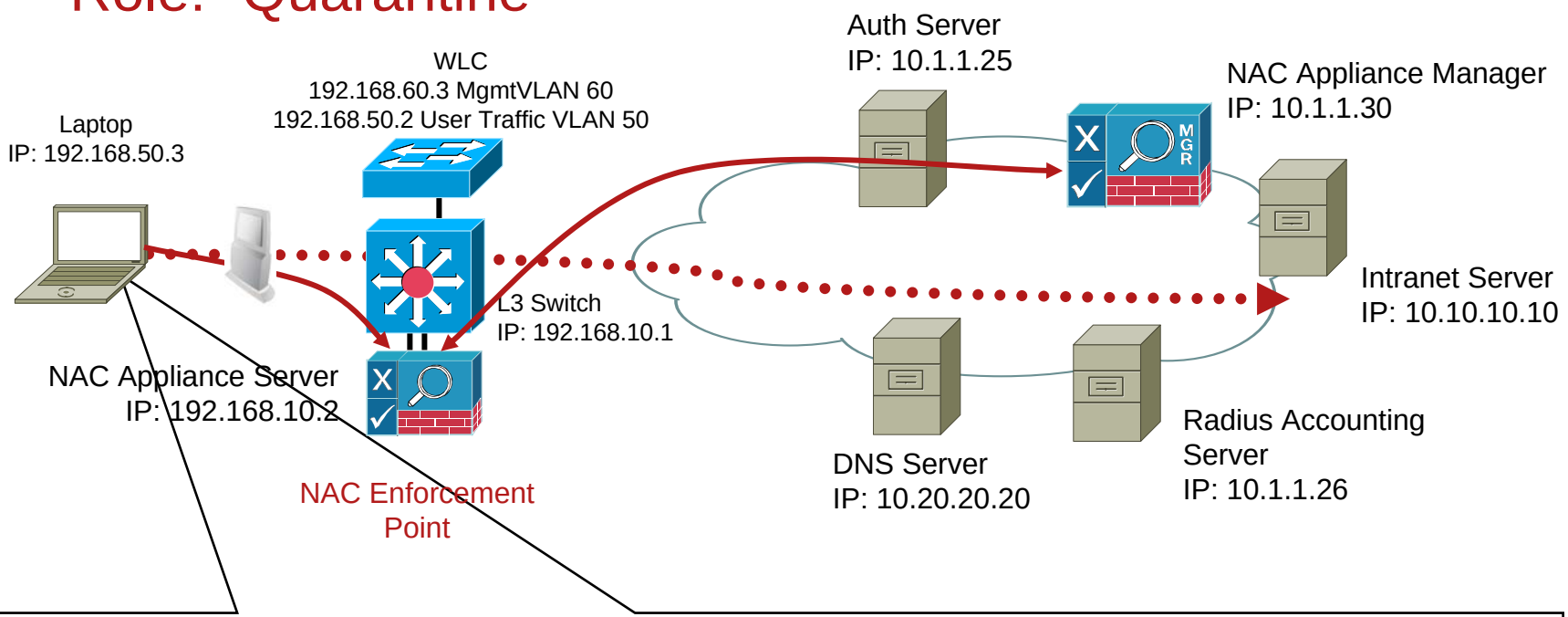
Role: “Unauthenticated”



1. Wireless user connects to WLC via LWAPP and authenticates to Auth Server (any auth methods including 802.1X)
2. Wireless user obtains IP address from Auth Server
3. WLC forwards Radius accounting login info to CAS
4. Wireless user opens a browser and is redirected to download the NAC Agent (if they don’t already have it loaded)

NAC Appliance Process Flow Wireless Access

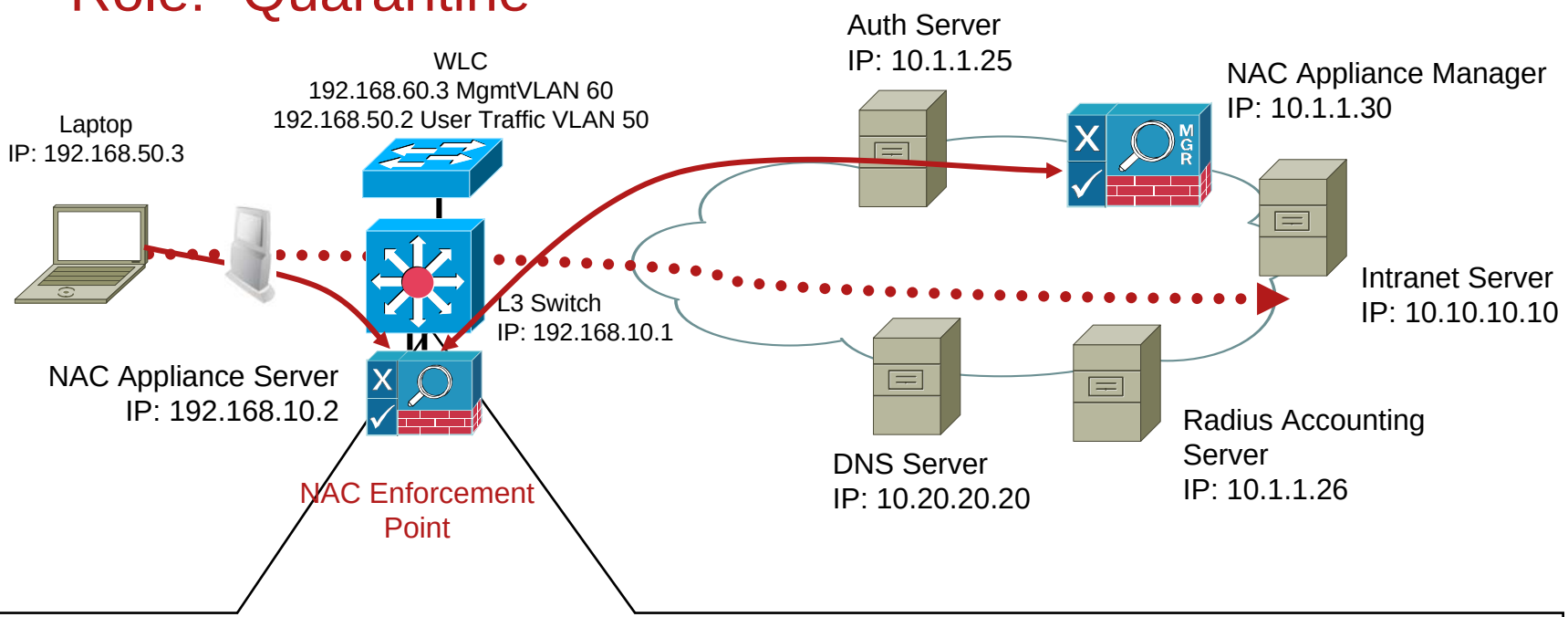
Role: “Quarantine”



5. The Agent queries the NAC Appliance Server to discover if the wireless user is authenticated (which it will be by the radius accounting previously sent)
6. The Agent performs posture assessment and forwards results to the Server to make the network admission decision

NAC Appliance Process Flow Wireless Access

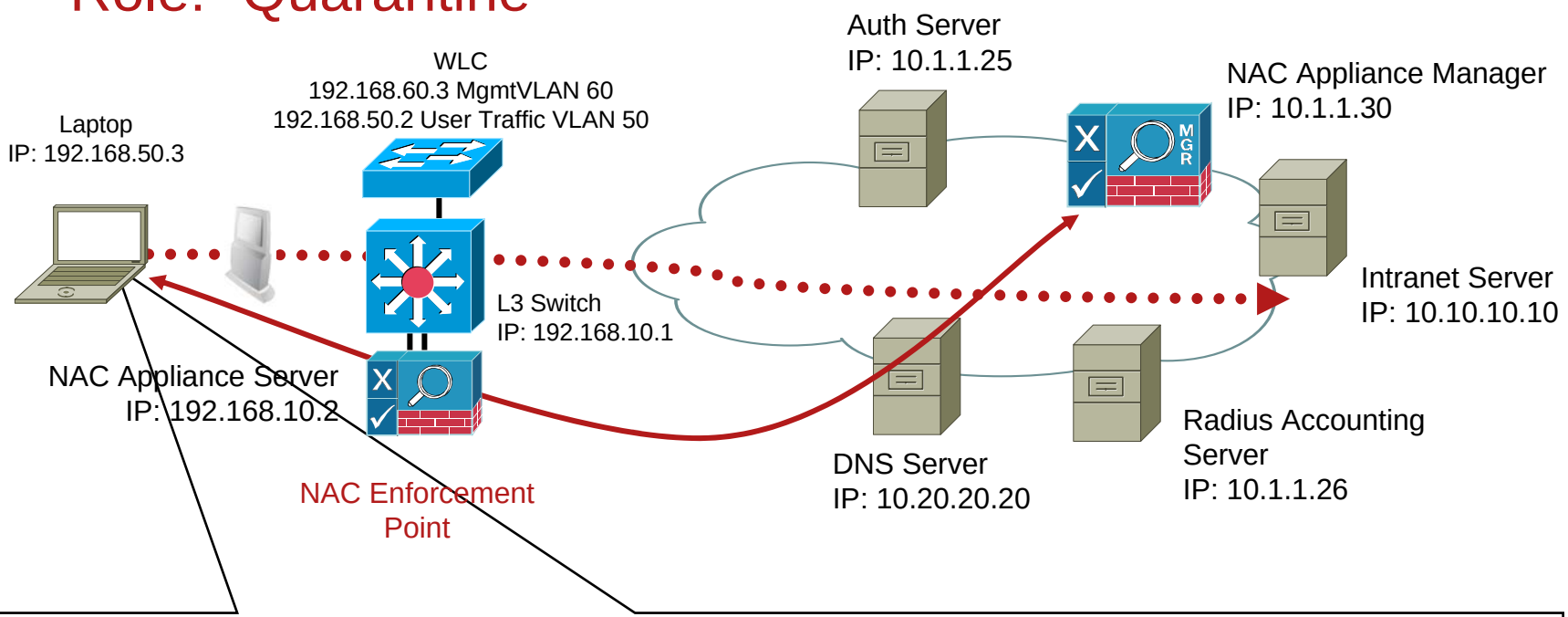
Role: “Quarantine”



8. NAC Server forwards posture report to NAC Manager
9. Manager determines that the user is NOT in compliance and instructs the Server to put the laptop into the “Quarantine Role”
10. NAC Manager sends remediation steps to NAC Agent

NAC Appliance Process Flow Wireless Access

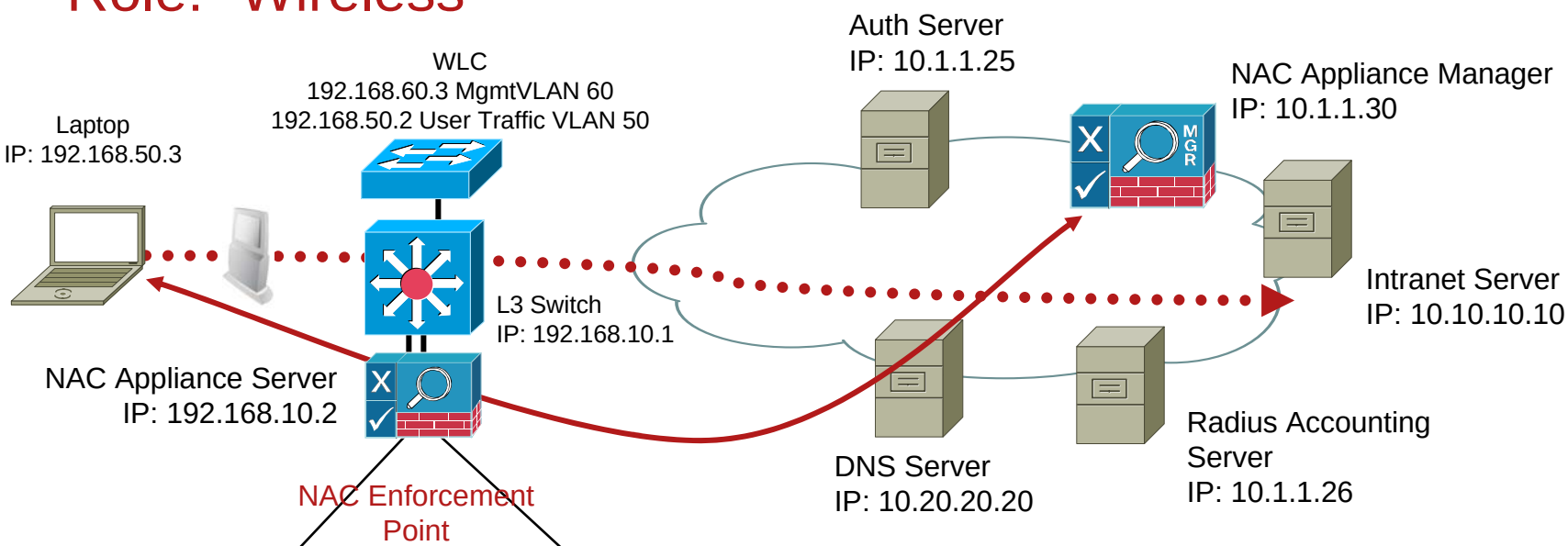
Role: “Quarantine”



11. NAC Agent displays access time remaining in “Quarantine Role” for remote user
12. The Agent guides remote user through step-by-step remediation with one-click update for remediation
13. The Agent informs the NAC server that the wireless user has been successfully remediated
14. The NAC Server provides the user with an Acceptable User Policy (AUP) agreement

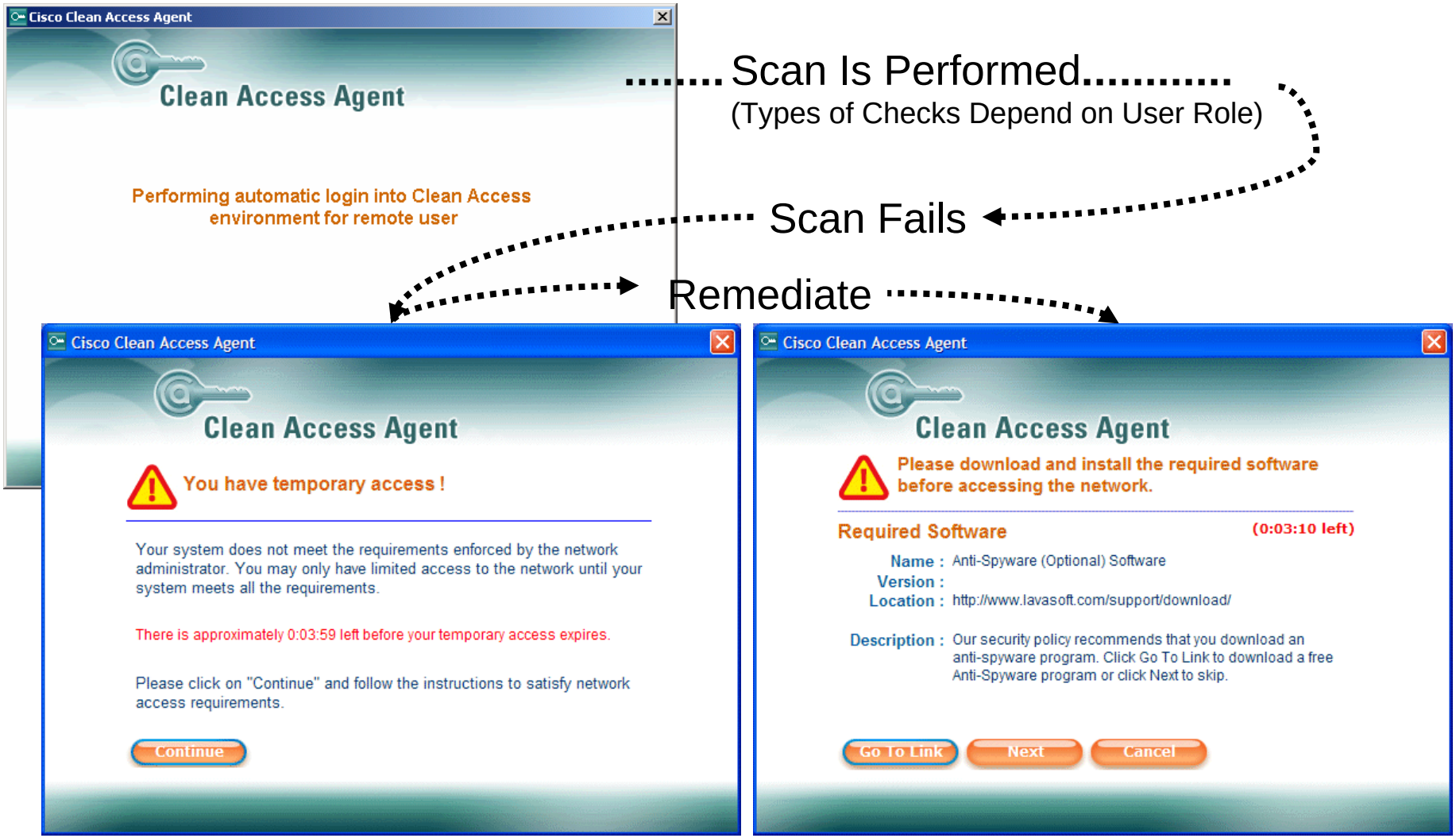
NAC Appliance Process Flow Wireless Access

Role: “Wireless”

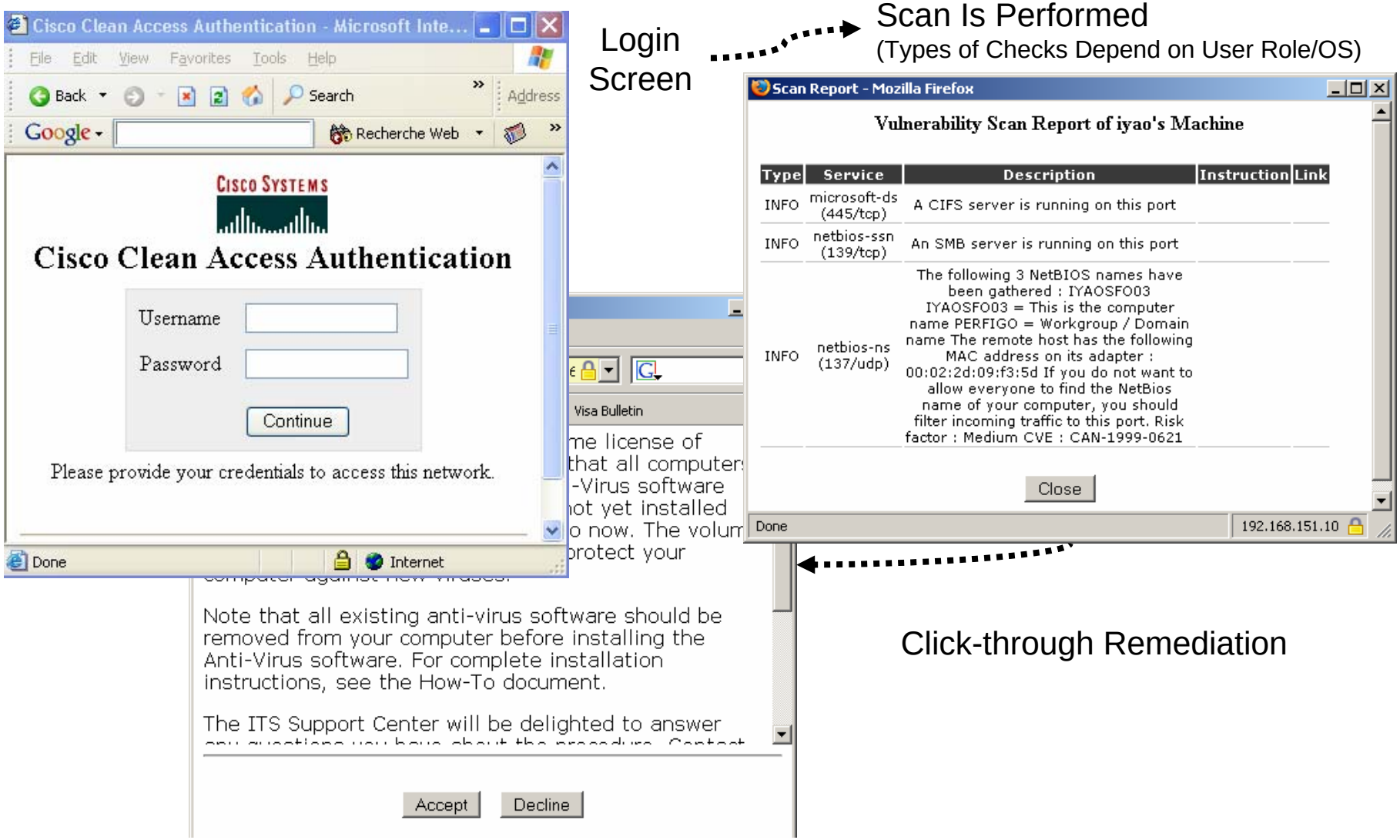


15. Upon AUP acceptance, the NAC Appliance Server assigns remote user to the “Wireless” role
16. NAC Appliance Server puts IP address of remote user into “Online User” list
17. Wireless user is now allowed to access to the Intranet server

End User Experience: With Agent



NAC Appliance Overview: Web Login



Wired and Wireless IPS/IDS

- Spectrum Analysis
- RF Monitoring
- Unified Wired and Wireless IPS/IDS

Securing Against RF Interference

WiFi Devices

+

Other Devices:
2.4/5GHz Products that Interfere

=

Bad Experiences

- Performance degradation
- Low data rates
- Lack of coverage
- Poor voice quality
- Support calls
- Increased cost of operations
- Poor user satisfaction

Security Breaches

- RF jamming and denial of service
- Non-WiFi rogues

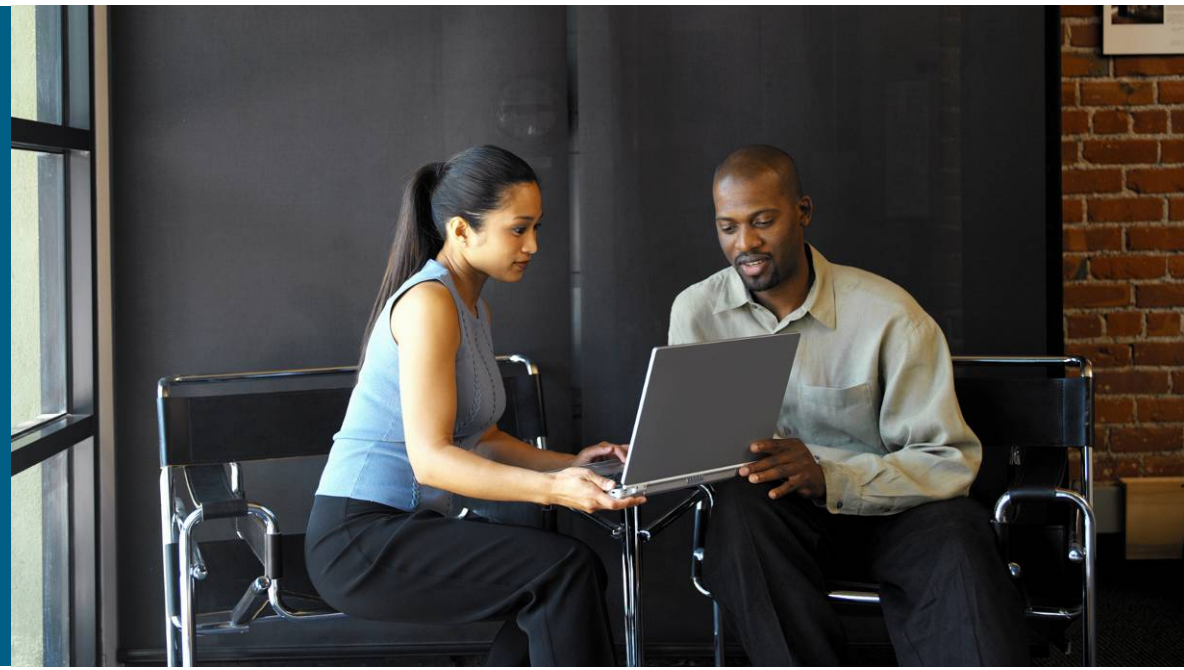
Wi-Fi Competes for RF Spectrum

RF Interference: Cognio Spectrum Expert

- What is it?
  - Interference detector
  - “Smart” physical layer analyzer
  - Complements packet/integrated tools
- What does it do?
  - Finds interference sources by name
  - Analyzes and determines “what’s wrong”
  - Device finding
  - Baseline and alert on air quality
- Unique advantages
  - List interference devices by name
  - Lock onto and find individual devices
  - Baseline and trend the “air”
  - Work inside your existing laptop
  - Many others

Cisco Solutions Plus Offering to Solve Interference and Other Layer 1 (RF) Issues

Demo:
Cognio



Rogue AP Detection

- Rogue AP detection has multiple facets:

  Air/RF detection—detection of rogue devices by observing/sniffing beacons and 802.11 probe responses

  Rogue AP location—use of the detected RF characteristics and known properties of the managed RF network to locate the rogue device

  Wire detection—a mechanism for tracking/correlating the rogue device to the wired network

- A wireless IDS may require different deployments to effectively address all of these facets

  For example, it is typically required to use a scanning-mode AP as a “rogue traffic injector” to attempt to trace the rogue’s connected port

Wireless Rogue Mitigation Overview

Proactive RF Defense Integrated into the Cisco Unified Wireless Network

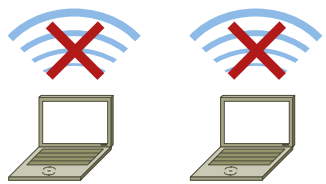
1. Detect Rogue AP (Generate Alarm)

2. Assess Rogue AP (Identity, Location)

3. Contain Rogue AP

4. View Historical Report

Rogues



- Manual mitigation
- Multiple rogues contained simultaneously

Rogue AP Detection and Suppression

- Rogue AP detection methodology

  WLAN system collects (via beacons and probe responses) and reports BSSID information

  System compares collected BSSID information versus authorized (i.e., managed AP) BSSID information

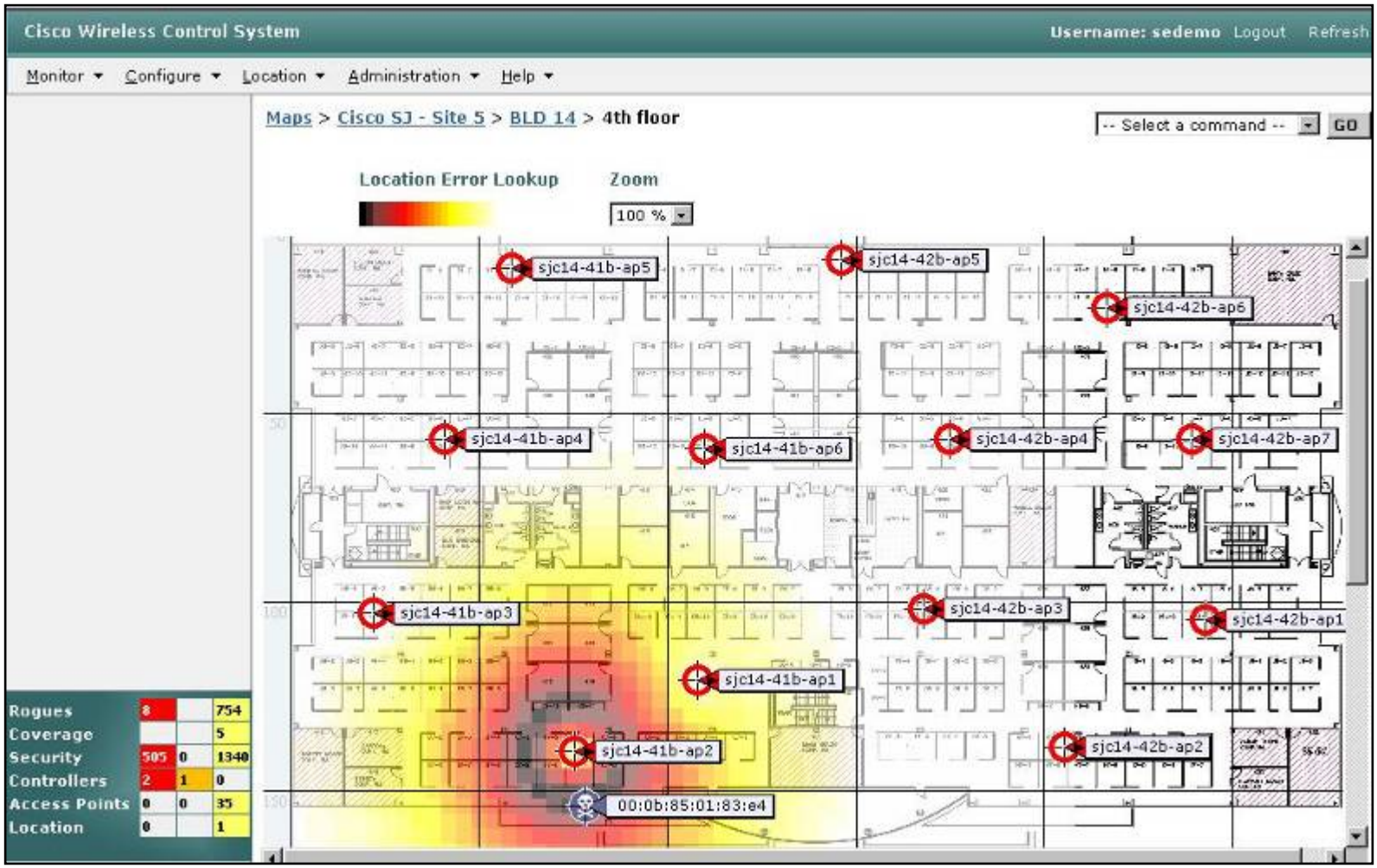
  Unauthorized APs are flagged and reported via fault monitoring functionality

- Rogue AP suppression techniques

  Trace the rogue AP over the wired network to verify that the rogue is internal and should be contained

  Use of managed devices to disassociate clients from unauthorized AP and prevent further associations via 802.11 de-association frames

Cisco Unified Wireless: Locate Rogue AP (High Resolution)

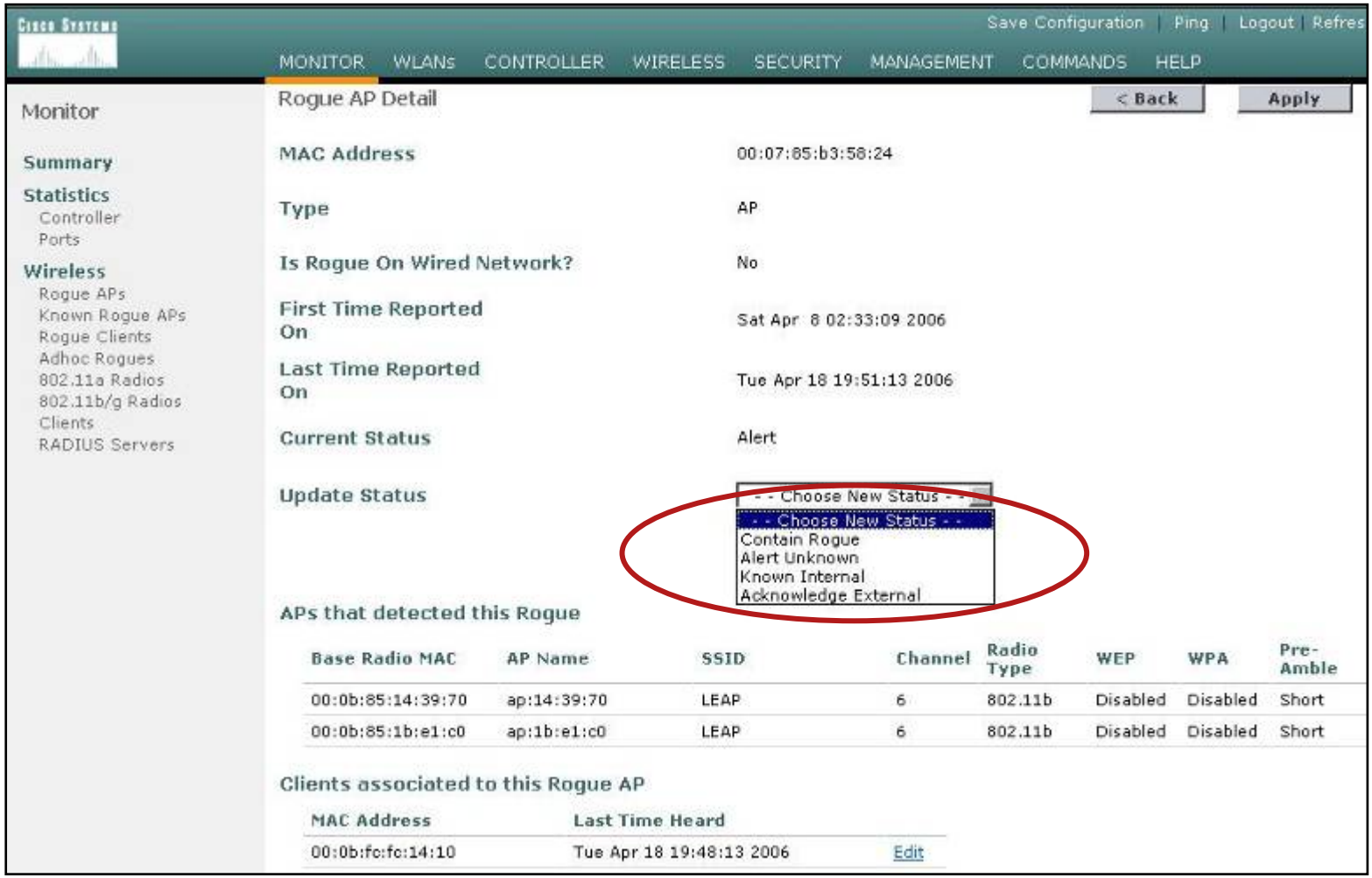


Cisco Unified Wireless: Rogue Containment

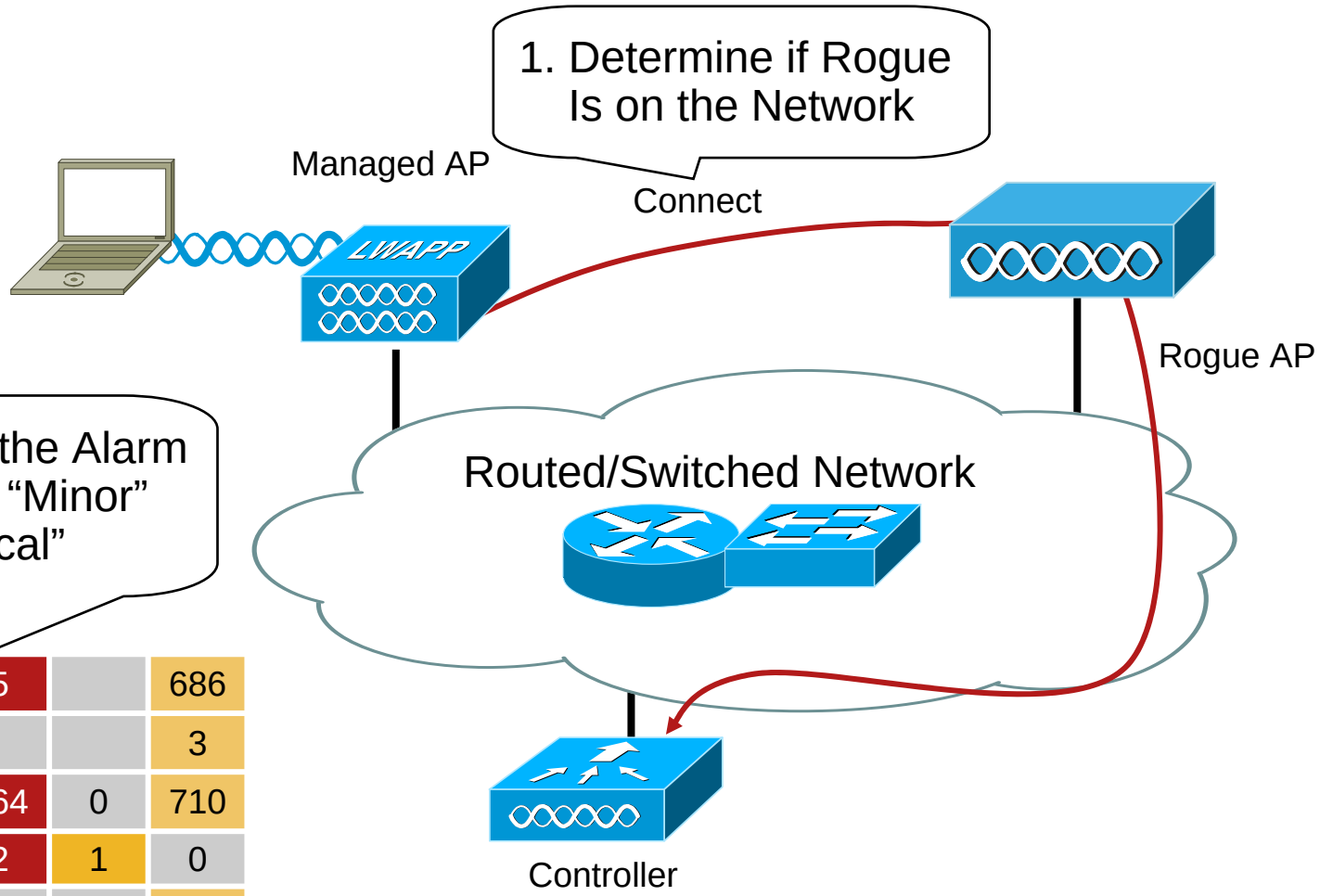
Rogue AP, Rogue-Connected Client, or Ad-hoc Client May Be Contained by Controller Issuing Unicast De-Association Packets

- Maximum number of APs participating in containment is configurable
- Maximum of three simultaneous containments may operate on a single LWAPP AP
- Rogue client devices may be authenticated to a RADIUS (MAC address) database
- Maximum time for auto-containment is configurable

Cisco Unified Wireless: Rogue AP Detection and Containment

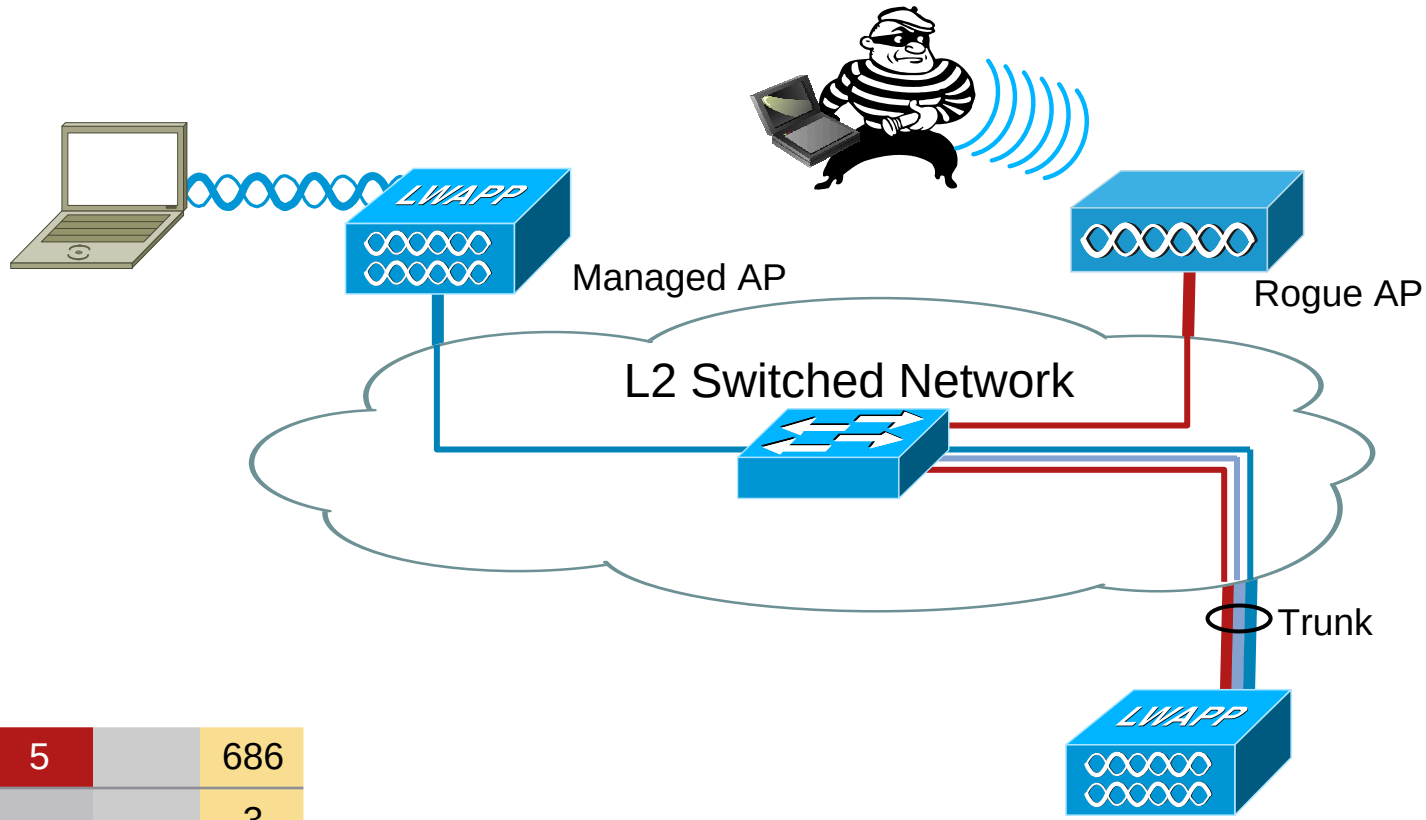


Rogue Location Discovery Protocol (RLDP)



Rogues	5		686
Coverage			3
Security	164	0	710
Controllers	2	1	0
Access Points	0	0	34
Location	0		0

Rogue Detector AP Mode



Rogues	5		686
Coverage			3
Security	164	0	710
Controllers	2	1	0
Access Points	0	0	34
Location	0		0

Dedicated Rogue Detector AP

- Detects all client ARPs
- Controller queries rogue detector to determine if rogue clients are on the network

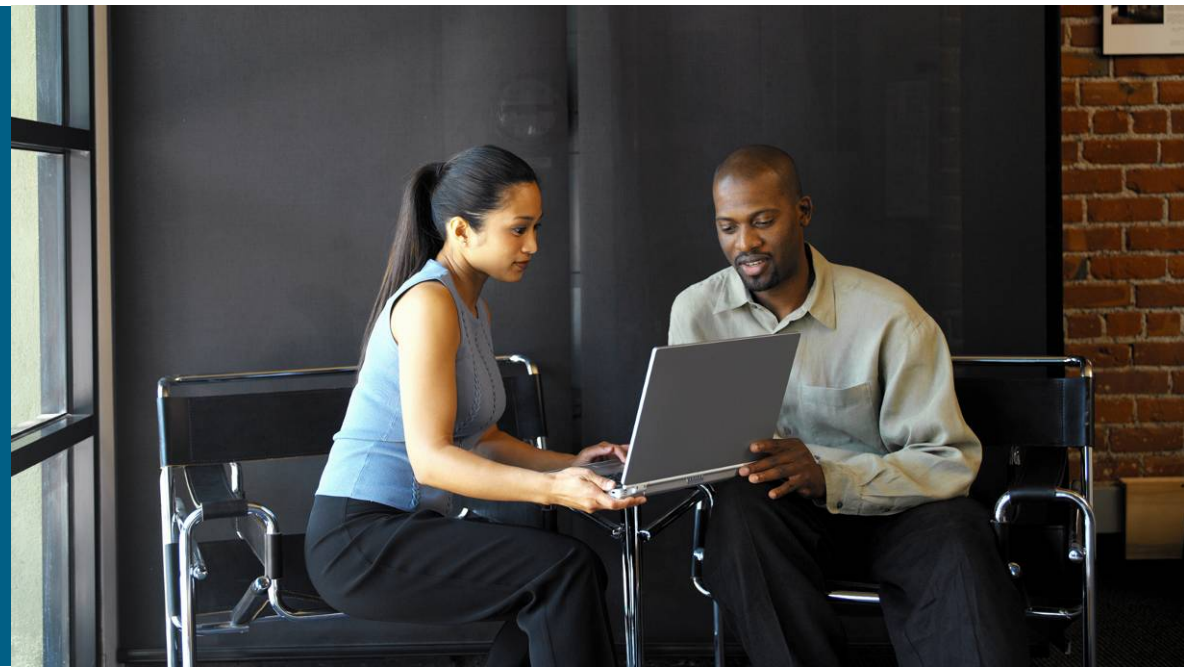
Wireless IDS Signatures

- Default signature file created by Cisco
- Custom signature file created by customer or 3rd party
- Customer can modify, delete, or create signatures via text editor
- Signature files uploaded or downloaded using TFTP
- Can be updated when needed
- Signature file uses a virus definitions file style approach

Signatures

Precedence	Name	Frame Type	Action	State	Description
1	Bcast deauth	Managemen	Report	Enabled	Broadcast Deauthentication Frame
2	NULL probe resp 1	Managemen	Report	Enabled	NULL Probe Response - Zero length
3	NULL probe resp 2	Managemen	Report	Enabled	NULL Probe Response - No SSID ele
4	Assoc flood	Managemen	Report	Enabled	Association Request flood
5	Reassoc flood	Managemen	Report	Enabled	Reassociation Request flood
6	Broadcast Probe floo	Managemen	Report	Enabled	Broadcast Probe Request flood
7	Disassoc flood	Managemen	Report	Enabled	Disassociation flood
8	Deauth flood	Managemen	Report	Enabled	Deauthentication flood
9	Res mgmt 6 & 7	Managemen	Report	Enabled	Reserved management sub-types 6
10	Res mgmt D	Managemen	Report	Enabled	Reserved management sub-type D
11	Res mgmt E & F	Managemen	Report	Enabled	Reserved management sub-types E
12	EAPOL flood	Data	Report	Enabled	EAPOL Flood Attack
13	NetStumbler 3.2.0	Data	Report	Enabled	NetStumbler 3.2.0

Demo:
WCS Security Features and Rogue Detection

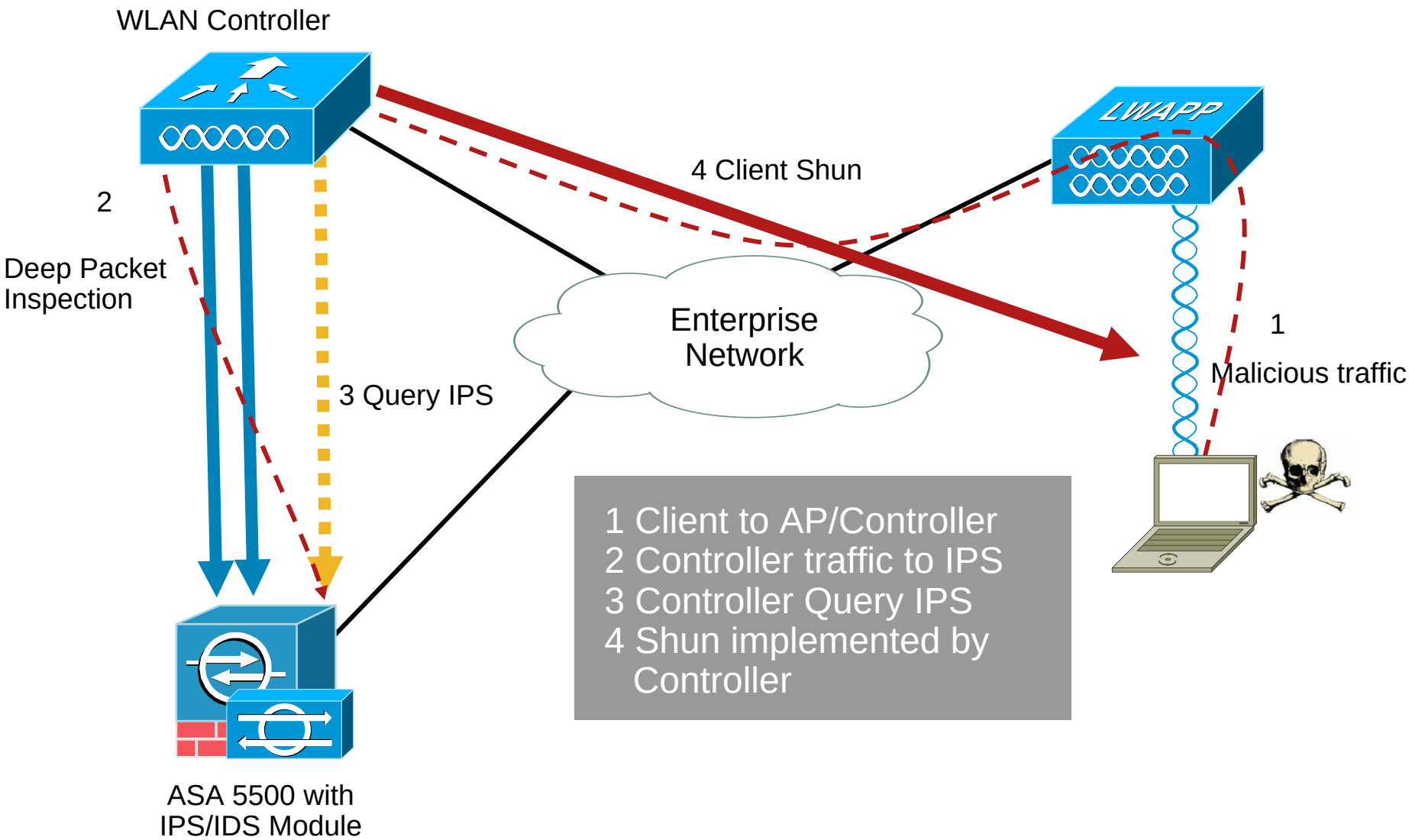


Unified Wired and Wireless IPS Event and Client "Shunning"

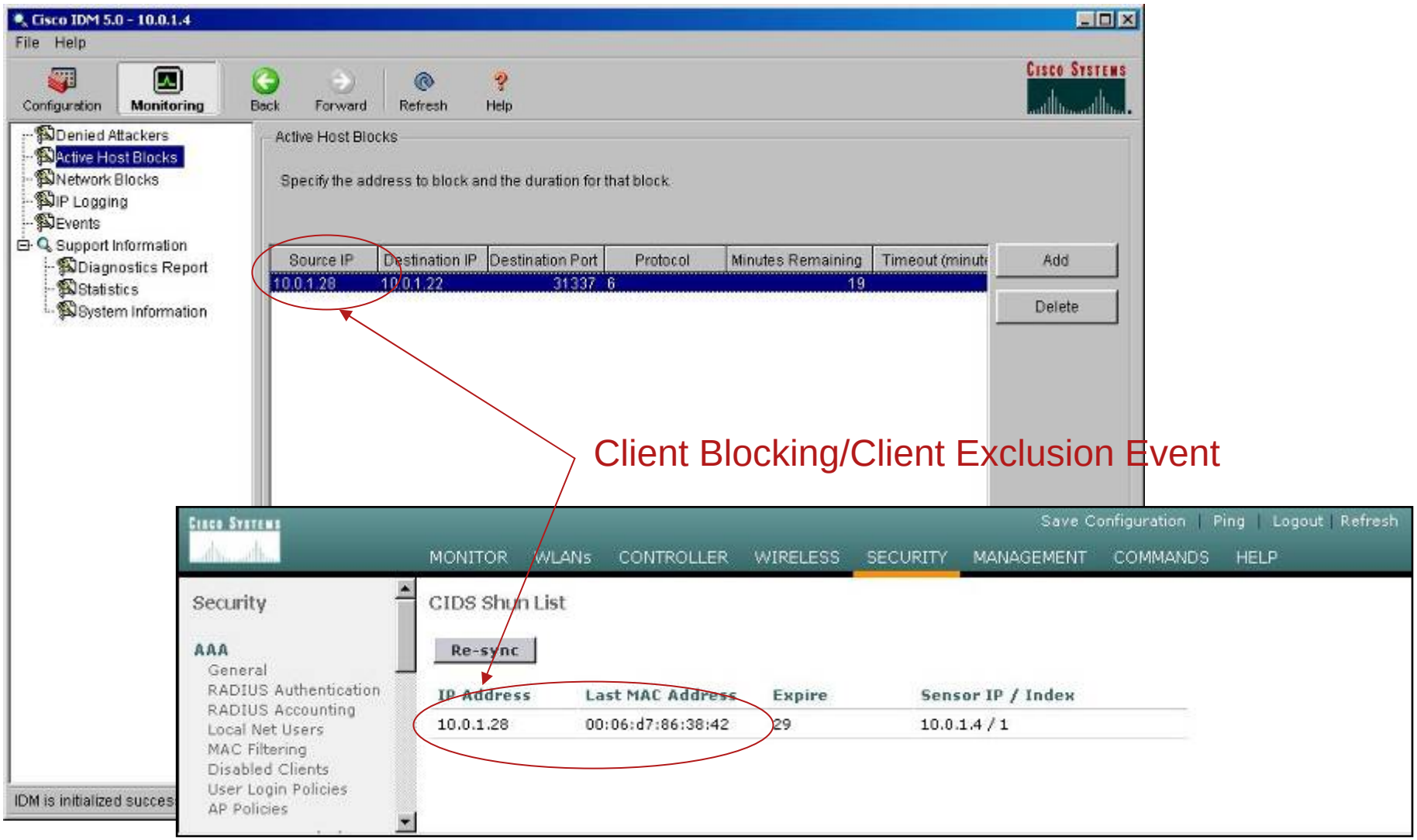
Alerting and Prevention of Application Layer Attacks

- Upon trigger of IPS system, e.g., from a known type of exploit (Nimda, Sasser, TCP stack exploit, etc.), activate a "Shun" or client block event
- A shun event can be invoked either inline or offline
  - Wireless "shun" is invoked at controller via offline mechanism
  - Controller periodically (configurable interval) polls CIDS for client block event
- Invokes client exclusion (blacklisting) at Cisco Controller
  - Client remains in blocked state until CIDS removes block and exclusion times out at controller

IPS Event and Client Shunning



IPS Host Block/Client Shun



Wireless IPS/IDS Summary

- Wired and Wireless IPS are complementary—monitor and control of wireless network should be treated similarly to physical wired network access and switchport security
- Wireless IPS is recommended for all deployments

  Enable RF monitoring via integrated IPS system in order to detect rogue APs, as well as monitor for potential Wireless exploits

  The Cisco Controller solution permits wireless and wired detection of rogue devices, as well as location of potential security breaches
- Wireless access may be employed as an access enforcement point for Cisco's Intrusion Prevention/Detection System Sensor performing L3–L7 security inspection

Mobile Host Intrusion Detection

- Features for Trusted Networks
- Features for Un-trusted Networks

Even Security Professionals Struggle to Secure Wireless Networks

- 2007 RSA Security Conference show network:
  - Half of the wireless devices on conference net vulnerable to two classes of attacks
    - "Evil Twin" attack
    - Various "Zero Day" attacks
    - 30 devices pretended to be access points
  - "Attackers could (and may have) captured the corporate username and authentication hash sent by the users over the airwaves."
- Participants and vendors were security specialists:
  - They had the knowledge to implement best practice
  - They had the motivation to implement best practice
  - Yet, higher priorities left the network vulnerable

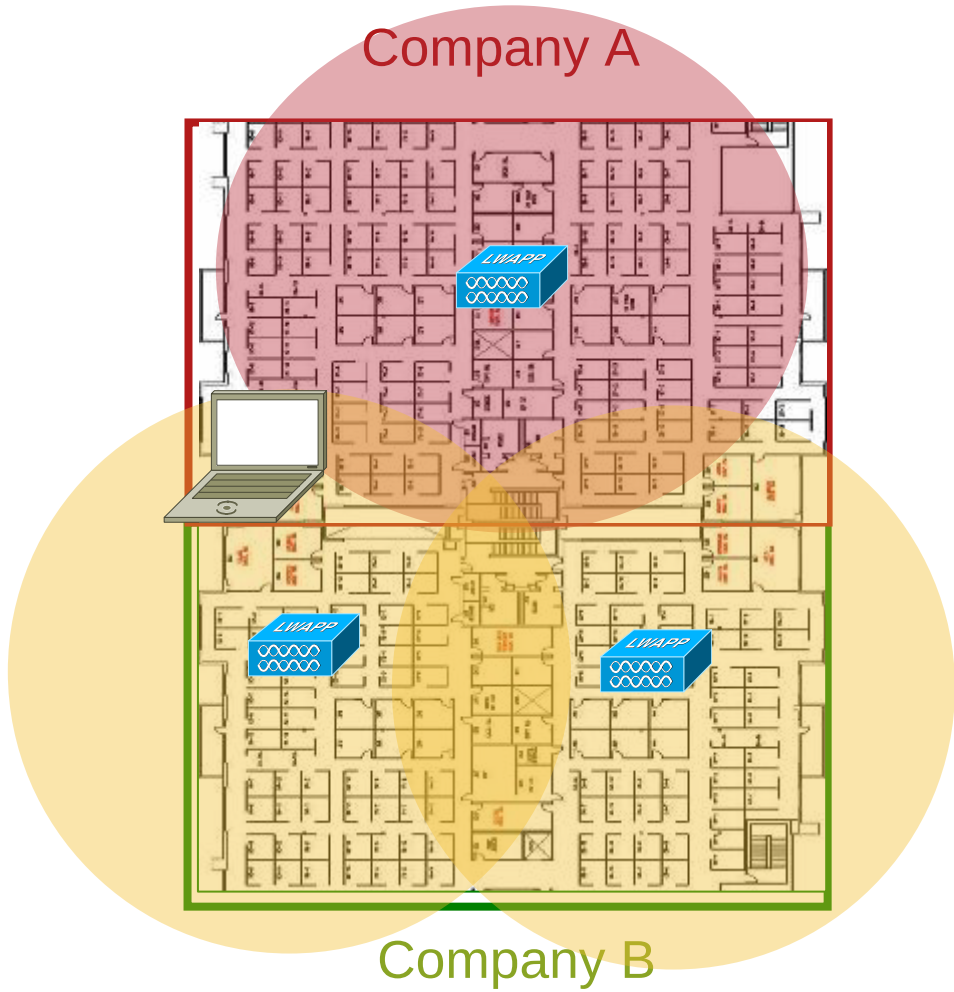
NETWORKWORLD

Source: Network World, 02/07/07
Attendees at RSA Conference Drop Ball on WiFi Security

Wireless Threat Scenario: Multi-Tenant Office Building

In-the-Office Wireless Security

- Two companies in adjacent offices, both use 802.11
- Laptop from company A may find best/only signal is from company B access point
  - Laptop associates with unsecured company B access point
- Laptop is plugged into company A Ethernet
  - Wireless active, associated with company B
  - Whose network is the laptop on?



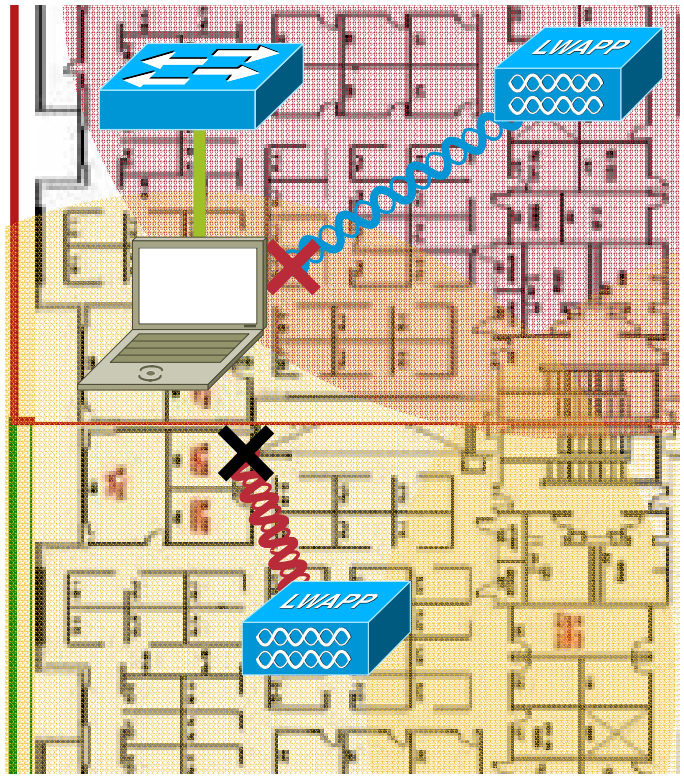
Secure Client Connections in Multi-Tenant Office Buildings

In-the-Office Wireless Security

- CSA blocks wireless to wired bridging

  Wireless restricted if Ethernet port is active

✓ Wireless Restricted if Ethernet active



- CSA forces laptop to associate to access points from company A

  Even if signal is stronger from other AP

✓ Associate with corporate SSID

✓ Use corporate crypto settings (EAP-Fast, etc)

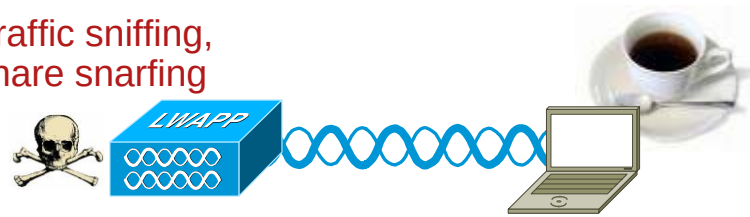
✓ Associate even if stronger signals from other APs

Wireless Client Threat Scenario: Un-Trusted Environments

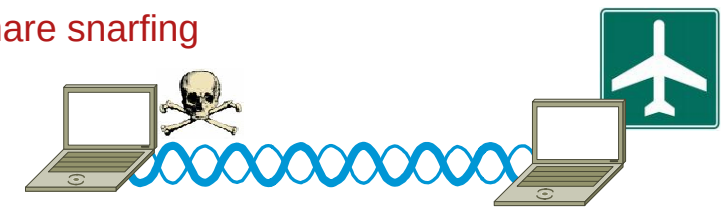
Out-of-the-Office Wireless Security

- Fake “public access” access points
  - Software on laptop masquerades as access point
  - “Evil Twin” looks legitimate to laptop user
  - Attacker targets passwords, wireless/domain credentials, file share access
  - Location-based targeting: airport, multi-tenant office building, cafés
- Direct ad-hoc connection
  - “Promiscuous Client” is similar to “Evil Twin”
  - Direct connect via ad-hoc
  - Very mobile—airplane in flight, visitors to corporate campus

- Attacker masquerades as AP
- Traffic sniffing, share snarfing



- Ad-Hoc connection attempt
- Traffic sniffing
- Share snarfing

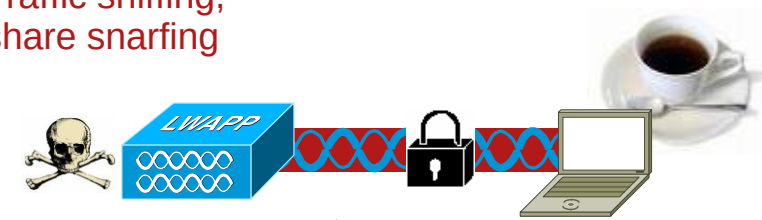


CSA Protects the Mobile Device and User

Out-of-the-Office Wireless Security

- Can you trust a public hotspot?
  - CSA Forces VPN connection to corporate network – ensures data is encrypted
  - VPN encrypts all traffic – defeats sniffing
- CSA prohibits ad-hoc connections
  - Typically no reason for ad hoc mode
  - Protects laptop when no AP is present

- Attacker owns AP
- Traffic sniffing, share snarfing



✓ VPN required

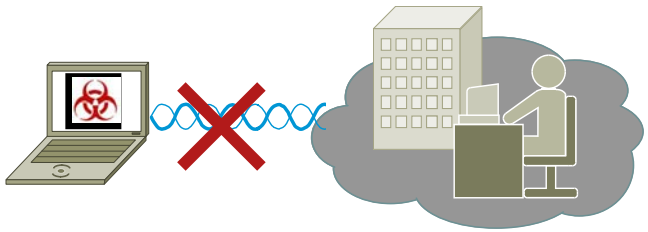
✓ File sharing, null sessions blocked

- Ad-Hoc connection attempt
- Traffic sniffing
- Share snarfing

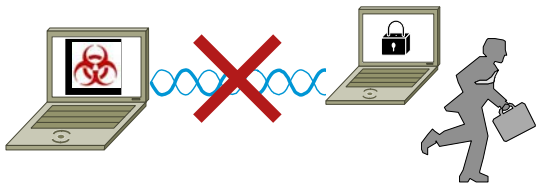
✓ Wireless Ad Hoc restricted

✓ File sharing, null sessions blocked

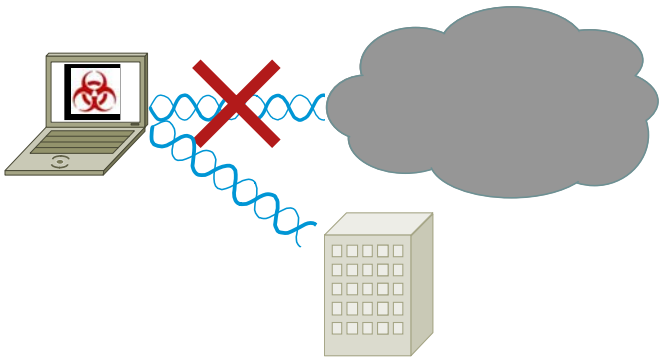
Summary of CSA Wireless Controls



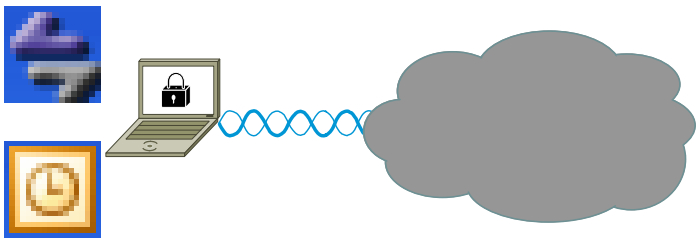
Disable Wireless NIC when Wired Is Active



Connection Restrictions—Certain SSIDs, Encryption, Ad-hoc



Require VPN Connection when out of the Office



Per-Application QoS Prioritization

Guest Access

- Wireless Guest Access
- Enhanced Wired and Wireless Guest Access

Types of Network Users

Corporate Employees	Contractors/ Consultants	Guests Users
• Need internal network access • Can be role based to allow granular access if needs require	• Need restricted internal access • Printers • File shares • Specific applications • Device support	• Internet access only • No need to access internal systems • Segment access completely

Cisco Solutions for Secure Guest Access
Baseline and Enhanced Options

Wireless Guest Access in Cisco Unified Wireless

- Lobby admin portal for user provisioning
- End-user registration page with basic customization
- Network partitioning using tunneling
- User authentication and authorization in local database or AAA server
- Usage logging and reporting

Enhanced Wired and Wireless Guest Access

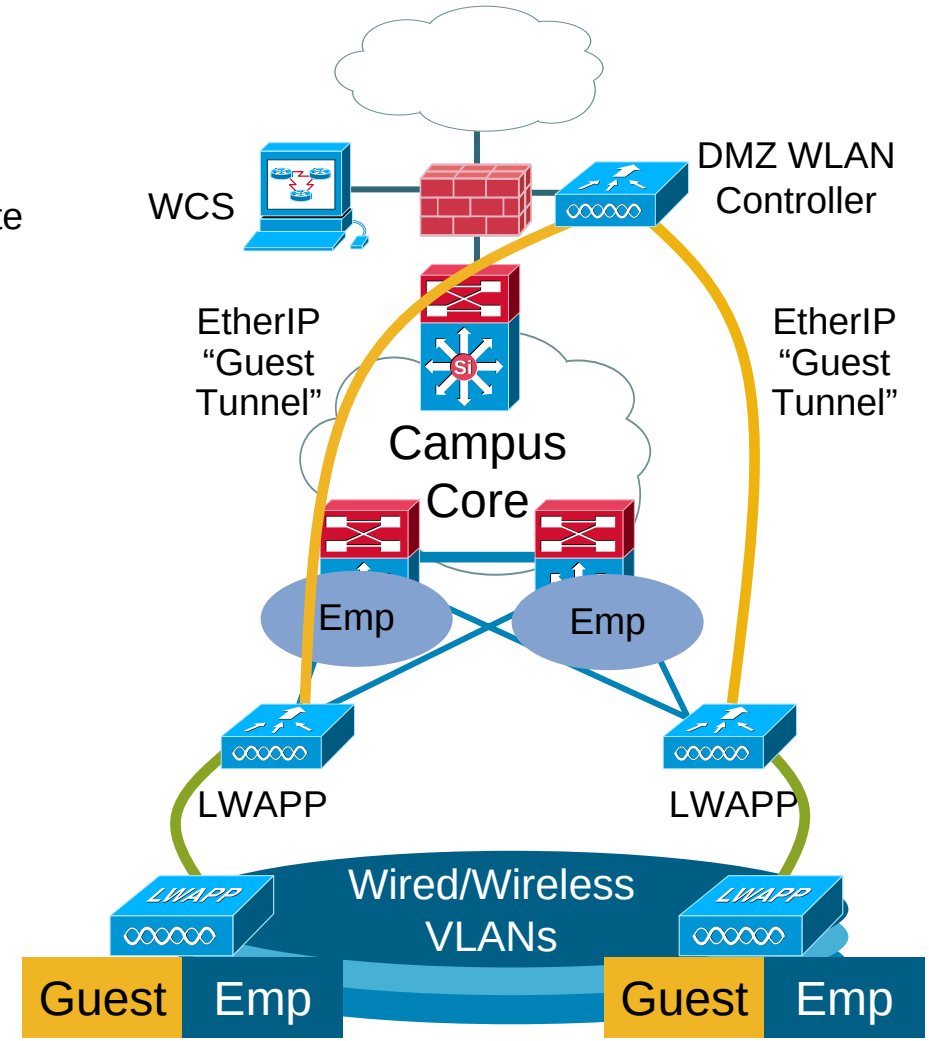
- Baseline, plus…
- Network privileges based on roles
- End-user security posture assessment
- Full policy-based end-user portal customization using partners
- Unification of wireless and wired guest access

Versatile Solutions for Diverse Deployment Environments

Wireless Guest Access

1. Back-end segmentation (mobility anchor)
   - Separate the guest traffic from the corporate internal traffic via EoIP tunnels
2. Lobby ambassador/ host portal
   - Guest user creation and token generation
   - Web portal—internal or external
3. Customizable guest screen
   - Semi-customizable guest login screen
4. Back-end authentication
   - Local user database
   - External AAA authentication capable

Equipment Required:
DMZ WLAN Controller



Enhanced Wired and Wireless Guest Access

Cisco NAC Appliance provides:

- Very granular role-based access
- Endpoint posture assessment and remediation
- OS and posture restrictions
- Integration with broader AAA servers
- Bandwidth policies for guests
- Uniform guest access for wired/wireless

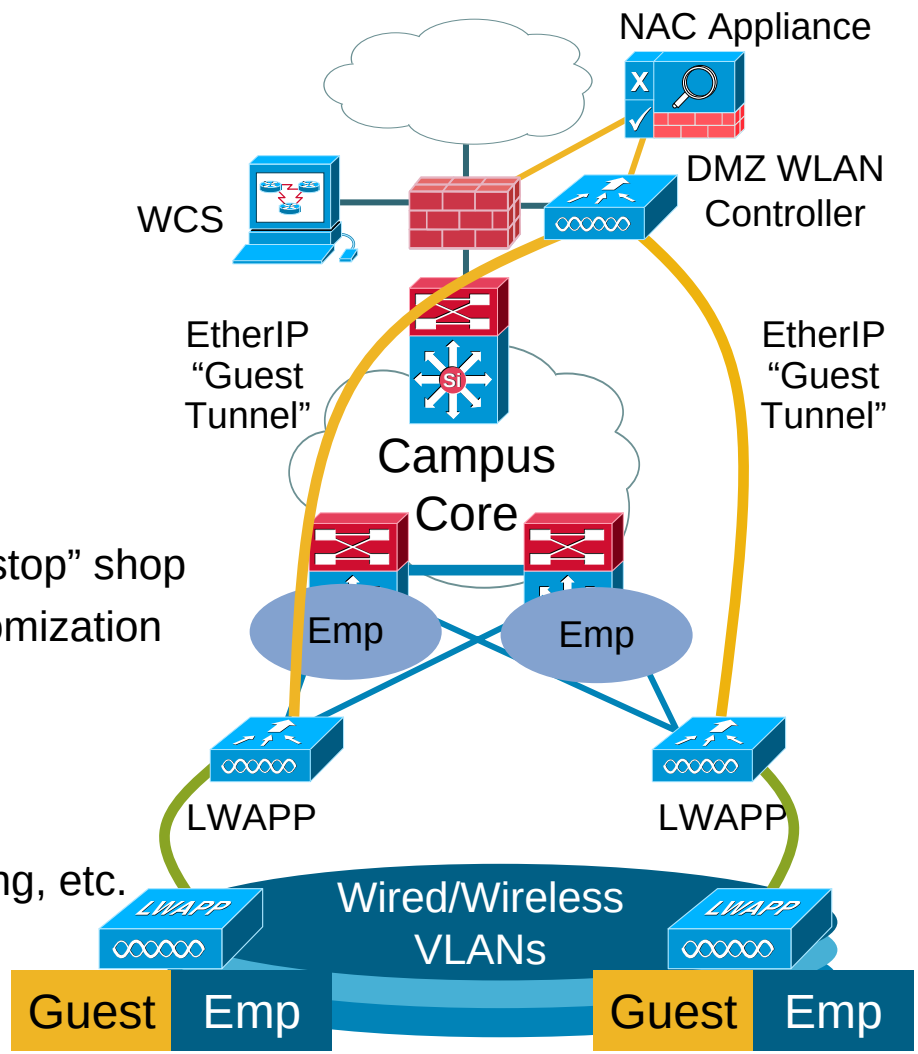
Cisco “GuestNet” Customized Portal:

- Cisco developed portal services for “one-stop” shop
- Basic portal customization, per-user customization

Partner User Portals provide:

- Extensive portal customization
- Customizable logging, reporting, billing
- Temporary user accounts for email, printing, etc.

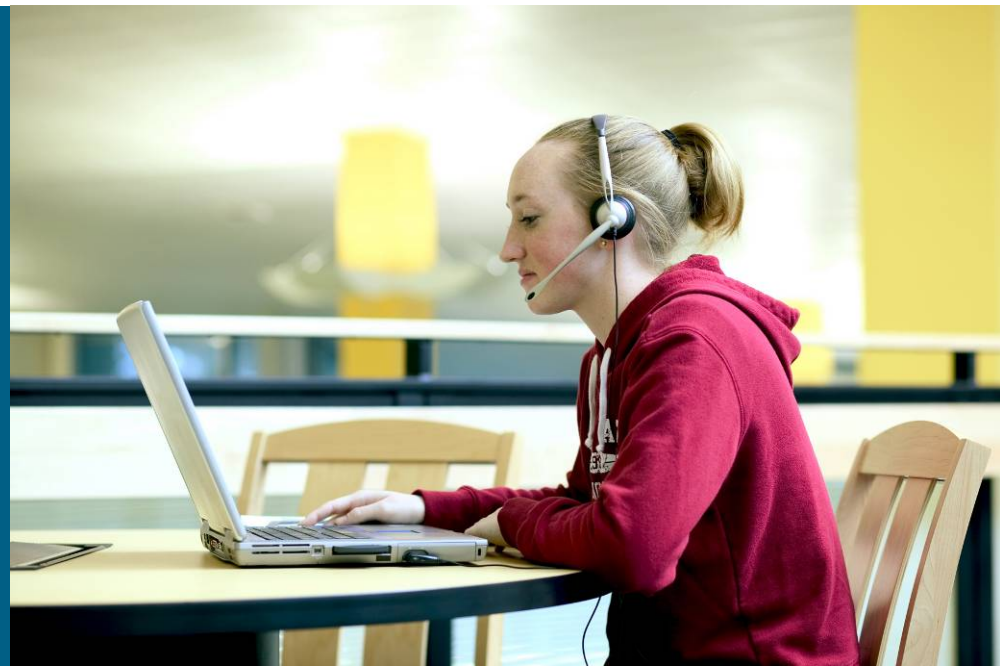
Equipment Required:
DMZ WLAN Controller
NAC Appliance
Advanced Services



Cisco Guest Access Options Summary

	Wireless Guest w/ DMZ WLAN Controller	Enhanced Wired and Wireless with Cisco Advanced Services	Enhanced with Partner Portal Solution
Lobby Admin Portal with End-user Registration	Basic Customization Available	Custom built by Cisco Advanced Services	Fully Customizable “off the Shelf” Product
End-user Authentication	Local Database or AAA Server	Local database or AAA Server	Local Database or AAA Server
Logical Network Separation	EoIP Tunnels	EoIP tunnels and/or VLAN assignment	EoIP Tunnels and/or VLAN Assignment
Roles-based Network Privileges	Not Available	Available	Available
End-user Device Posture Assessment	Not available	Available; with Roles-Based Policy	Available; with Roles-Based Policy
Usage Logging and Reporting	Available	Available	Available
Unified Wireless and Wired Architectures	Currently wireless-specific	Unified	Unified
Unified Guest/Employee NAC Architecture	Not Available	Unified	Unified

Secure Wireless Summary



Summary

Your wireless network is always on. It's an open port anyone can see and use, so it requires 24/7 monitoring and defense-in-depth to keep it safe

1. Create a security policy for your wireless network. Schedule regular audits and policy reviews
2. Enable the baseline security in your wireless devices
3. Control your WLAN traffic, including information integrity and network access
4. Integrate your wireless and wired security solutions for end-to-end protection
5. Apply endpoint inspection, hardening, and control wherever possible
6. Fully integrate your wired and wireless networks for network-wide visibility, event reporting, and correlation

Additional Resources

- For more information about Cisco Secure Wireless Solution, visit:

  http://www.cisco.com/wirelesssecurity

- For more information about Cisco NAC, visit:

  http://www.cisco.com/go/nac

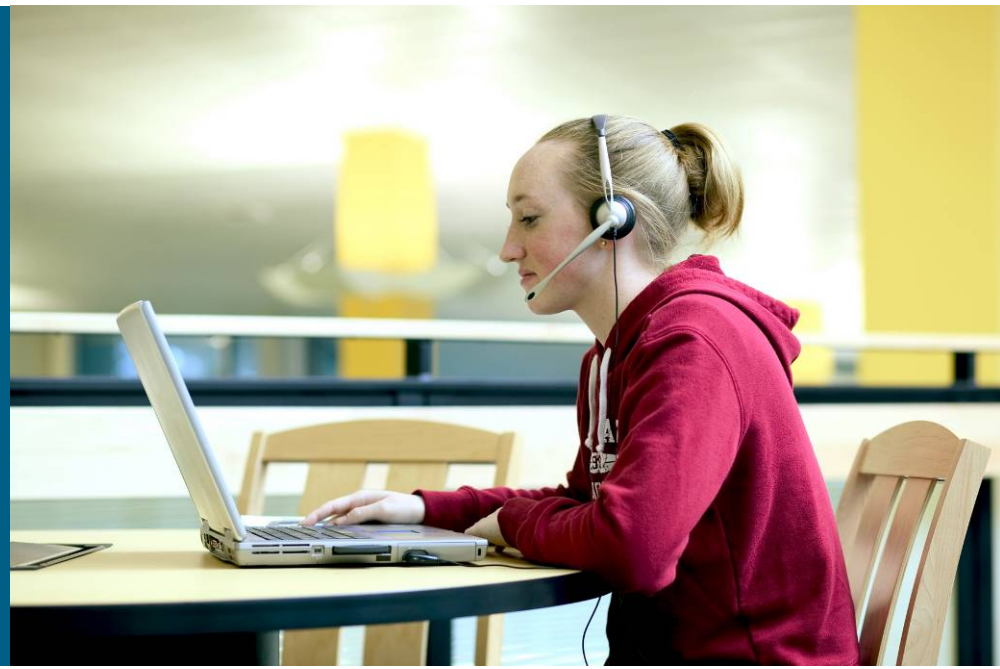
- For more information about Cisco Wireless products, visit:

  http://www.cisco.com/go/wireless

- For more information about the Cisco Unified Wireless Network, visit:

  http://www.cisco.com/go/unifiedwireless

Q and A



Thank You!