DEPLOYING SECURE WIRELESS LANS

Sri Sundaralingam

Technical Marketing Manager
Cisco Systems, Inc.

Agenda

- **Drivers for WLAN Security**
- WLAN Security Vulnerabilities and Threats
- WLAN Security Deployment Criteria
- WLAN Deployment Examples
- WLAN Security Best Practices
- Wireless IDS
- Wireless/Wired Integration Best Practices
- Summary

Why WLAN Security Is important?

VULNERABILITIES:

Hackers

Employees

“War Driving”

THE WALL STREET JOURNAL.

© 2001 Dow Jones & Company, Inc. All Rights Reserved.

VOL. CCXXXVII NO. 25 WE/PA ★★★ MONDAY, FEBRUARY 5, 2001 WSJ.com

Hackers Can Penetrate Wireless Network

By Jared Sandberg
Staff Reporter of The Wall Street Journal

A group of respected security research-

ple, brought to light by network-security specialists around the globe. Mr. Goldberg himself found a significant flaw in the

nel." He adds that the IEEE is working on future versions that won't be vulnerable.

But Mr. Ennis says this type of attack

connect to networks using simple radio antennas in their laptop or desktop PCs. The technology, also called Wi-Fi, is sold by many vendors but was popularized by Apple Computer Inc. under the name AirPort and is quickly being deployed in networks at a growing number of businesses, college campuses, hotels and airports. By the end of 2001, an estimated 10 million Wi-Fi radios will be deployed, according to research firm Cahners In-Stat. Starbucks Corp., for instance, plans to use the technology to allow latte quaffers to noodle around the Internet.

The weakness is another reminder of the difficulty in implementing effective network security.

chief scientist at Zero Knowledge Systems

LESSONS:

- Do not rely on basic WEP encryption; Requirement for Enterprise class Security (WPA, EAP/802.1x protocols, Wireless IDS, VLANs/SSIDs, etc)
- Employees will install WLAN equipment on their own (compromises security of your entire network)
  - –Out of the box configuration of APs: All security features are disabled!
- Business impact due to stolen data: Potential financial and legal consequences (Laws to protect data confidentiality; Example: Healthcare)

HP WORLD 2004
Solutions and Technology Conference & Expo

Requirements for Enterprise Deployments

- Mostly data applications and increasing VoIP deployment rate
  - –Typical Applications—Web/Email access, Wireless VoIP, Instant Messaging, Client/Server Apps
- Homogeneous Environment ➔ Slowly changing to Heterogeneous environment
  - –Most of the Laptop devices standardized (also standardized OS)
  - –VoIP devices impose specific security considerations
  - –Growing Requirement to support multiple Security Types (EAP types as well as Encryption types)
- Employees want wireless
  - –If IT doesn't roll-out wireless, employees will install Rogue APs

Requirements for Vertical Deployments

- Support for active mobile Users
  - –Warehousing: Inventory Tracking (Fork Lift Vehicles)
  - –Healthcare: Patient Monitoring Applications (example: 802.11-enabled Fusion Pumps)
- Legacy Devices
  - –Retail/Warehousing: Legacy barcode scanners, etc (support for static-WEP only)
- Heterogeneous Clients
  - –University: Students can bring any laptop with any vendor NIC card
  - –Retail/Warehousing: Barcode readers, POS terminals, and VoIP handsets very common
- WLAN network is deployed as the primary network for connectivity!
  - –Consider WLAN availability as part of security deployment criteria

Agenda

- Drivers for WLAN Security
- **WLAN Security Vulnerabilities and Threats**
- WLAN Security Deployment Criteria
- WLAN Deployment Examples
- WLAN Security Best Practices
- Wireless IDS
- Wireless/Wired Integration Best Practices
- Summary

WLAN Security Vulnerabilities and Threats

Different Forms of Vulnerabilities and Threats Exist

- Encryption Vulnerabilities: WEP
- Authentication vulnerabilities: shared-key authentication, dictionary attacks, and MITM attacks
- Disable or enable SSID broadcast?
- Address spoofing: mac-address spoofing and ip address spoofing (both hostile/outsider attacks as well as insider attacks)
- Misconfigured APs and clients
- Denial of Service (DoS) attacks: using 802.11 deauthentication/ disassociation frames, RF jamming, etc.

WEP Vulnerabilities

- 802.11 Static-WEP is flawed: passive attacks
  - RC4 Key Scheduling algorithm uses 24-bit Initialization Vector (IV) and does not rotate encryption keys
  - Practical tools that have implemented FMS attack (Example: AirSnort) can uncover the WEP key after capturing 1,000,000 packets
  - This is about ~17 minutes to compromise the WEP key in a busy network!
  - This attack is passive and all the attack tool needs to do is “listen” to the WLAN network (i.e. sniff WLAN packets)
- 802.11 Static-WEP is flawed: active attacks
  - Does not protect the WLAN user data integrity
  - Several Forms of Attacks possible: Replay Attacks, Bit-Flipping attacks, etc.

Authentication Vulnerabilities

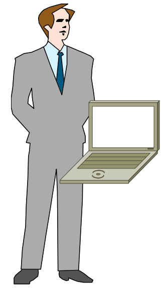
- Shared key authentication is flawed!
  - –AP challenges (plaintext challenge) the WLAN user to ensure possession of valid encryption key
  - –Attacker can obtain key stream ➔ plaintext challenge XOR ciphertext = Key Stream
  - –Not recommended for deployment!
- Dictionary attacks
  - –On-line (active) attacks: Active attack to compromise passwords or pass-phrases
  - –Off-line attacks: Passive attack to compromise passwords or pass-phrases
- MITM attacks
  - –Active attacks where the attacker inserts himself in the middle of authentication sequence

Who Installs Rogue APs?:
“Focus on the Frustrated Insider”

FRUSTRATED INSIDER

>99.9% of Rogue APs

- User that installs wireless AP in order to benefit from increased efficiency and convenience it offers
- Common because of wide availability of low cost APs
- Usually ignorant of AP security configuration, default configuration most common



Jones from Accounting

MALICIOUS HACKER

<.1% of Rogue APs

- Penetrates physical security specifically to install a rogue AP
- Can customize AP to hide it from detection tools
- Hard to detect—more effective to prevent via 802.1x and physical security
- More likely to install LINUX box than an AP

HP WORLD 2004
Solutions and Technology Conference & Expo

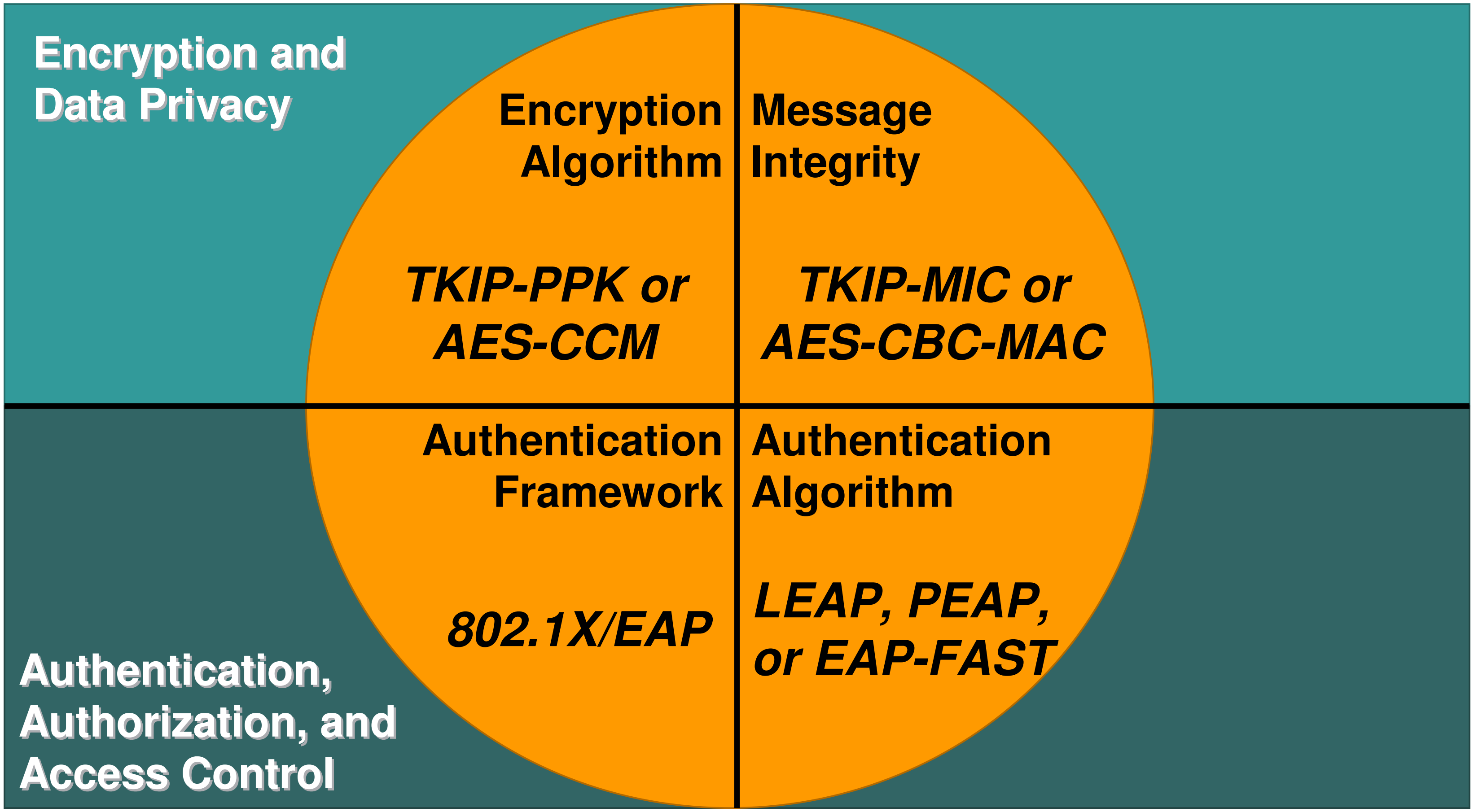
Agenda

- Drivers for WLAN Security
- WLAN Security Vulnerabilities and Threats
- **WLAN Security Deployment Criteria**
- WLAN Deployment Examples
- WLAN Security Best Practices
- Wireless IDS
- Wireless/Wired Integration Best Practices
- Summary

Basic Requirements to Secure Wireless LANs

- Encryption algorithm
  - Mechanism to provide data privacy
- Message integrity
  - Ensures data frames are tamper free and truly from the source address
- Authentication framework
  - Framework to facilitate authentication messages between clients, access point, and AAA server
- Authentication algorithm
  - Mechanism to validate client credentials

Basic Requirements to Secure Wireless LANs



Encryption and Data Privacy

Encryption Algorithm

TKIP-PPK or AES-CCM

Message Integrity

TKIP-MIC or AES-CBC-MAC

Authentication Framework

802.1X/EAP

Authentication Algorithm

LEAP, PEAP, or EAP-FAST

Authentication, Authorization, and Access Control

Advanced Requirements to Secure Wireless LANs

- Secure management policies
  - Secure Telnet, SSH, SNMP, FTP, TFTP, RADIUS, and WLCCP traffic to the APs and Bridges
- Wireless IDS
  - Provide capability to detect and suppress unauthorized APs, detect active attacks, and enhance Layer-2 Security
- Wired/Wireless Integration best practices
  - Mapping wireless security policies to the wired network
  - Use of multiple user/device groups (via SSIDs/VLANs/mGRE tunnels)
  - Use of wired security features for wireless lan deployment

Agenda

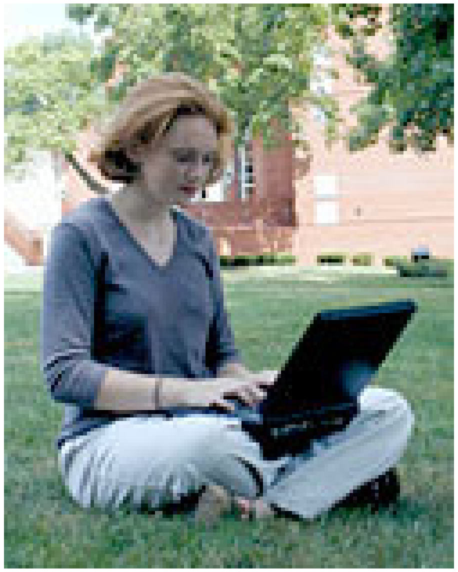
- Drivers for WLAN Security
- WLAN Security Vulnerabilities and Threats
- WLAN Security Deployment Criteria
- **WLAN Deployment Examples**
- WLAN Security Best Practices
- Wireless IDS
- Wireless/Wired Integration Best Practices
- Summary

Enterprise Deployment Example

- WLAN deployment scenario
  - –Typical Applications: Web/Email access, Instant Messaging, Client/Server Applications, and VoIP over WLAN
  - –Coverage provided across all floors including meeting rooms
- Specific deployment goals
  - –Authenticate and authorize each user
  - –Protect user data confidentiality and integrity
  - –Standardized client Environment
  - –Scalability and manageability
  - –Guest access
  - –HQ as well as remote office deployment
  - –Wireless LAN is deployed as an additional medium (i.e. Wired LAN is considered as the primary network connectivity medium)

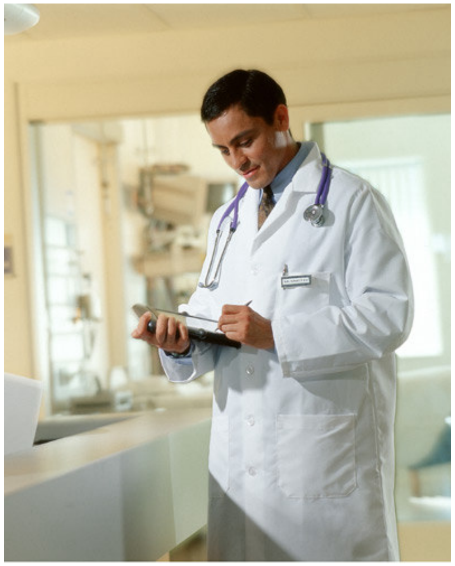
Education Deployment Example

- Collaborative learning applications aid students and teachers
- Staff: Requirement to access student records and other sensitive data over WLAN
- Deployment goals:
  - –Non-standardized client environment for students
  - –Students: user authentication only
  - –Staff: user authentication and data confidentiality
- Non-standardized client environment for students means:
  - –Students are allowed to bring any device
  - –Students could be using any OS
  - –Students could be using any vendor WLAN NIC
- Standardized device (OS and WLAN NIC) for staff



Healthcare Deployment Example

- WLAN deployment across multiple clinics and hospitals
  - –Mobile real-time patient information
  - –Wireless LAN provides access to image-rich applications
  - –Patient care, patient monitoring applications
- Deployment criteria
  - –Strive to standardize on client environment
  - –De-centralized WLAN deployment: Multiple sites (small, medium, and Large); Multiple deployment models
  - –A must requirement to protect patient related data information
  - –WLAN network is the primary network, so Availability matters!



HP WORLD 2004
Solutions and Technology Conference & Expo

Agenda

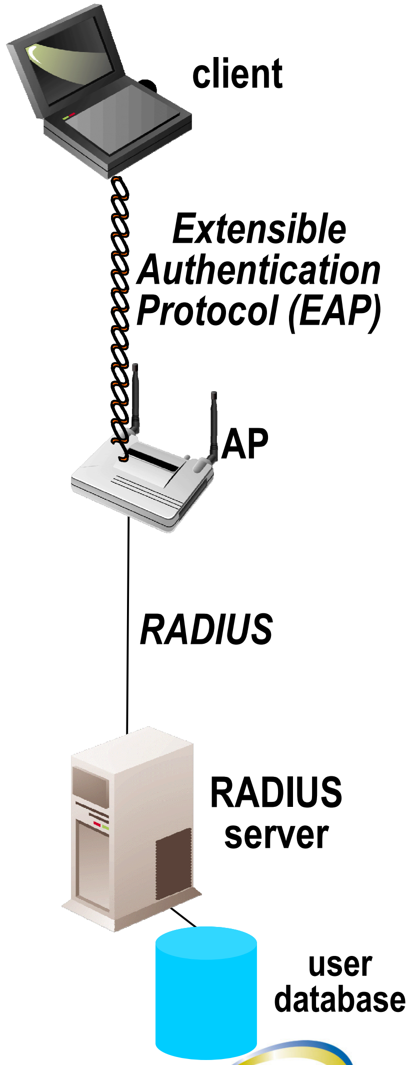
- Drivers for WLAN Security
- WLAN Security Vulnerabilities and Threats
- WLAN Security Deployment Criteria
- WLAN Deployment Examples
- **WLAN Security Best Practices**
- Wireless IDS
- Wireless/Wired Integration Best Practices
- Summary

Wireless LAN Security Best Practices

- **Technologies to Secure Wireless LANs**
  - EAP/802.1x Authentication Protocols
  - Data Encryption and Message Integrity: WPA, CKIP, WPAv2
- EAP/802.1x with WPA/WPAv2 Deployment Considerations
  - EAP Supplicant Availability
  - RADIUS Server Scalability And Availability

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
  - Encryption keys derived after authentication
  - Centralized policy control, where session timeout triggers reauthentication and new key

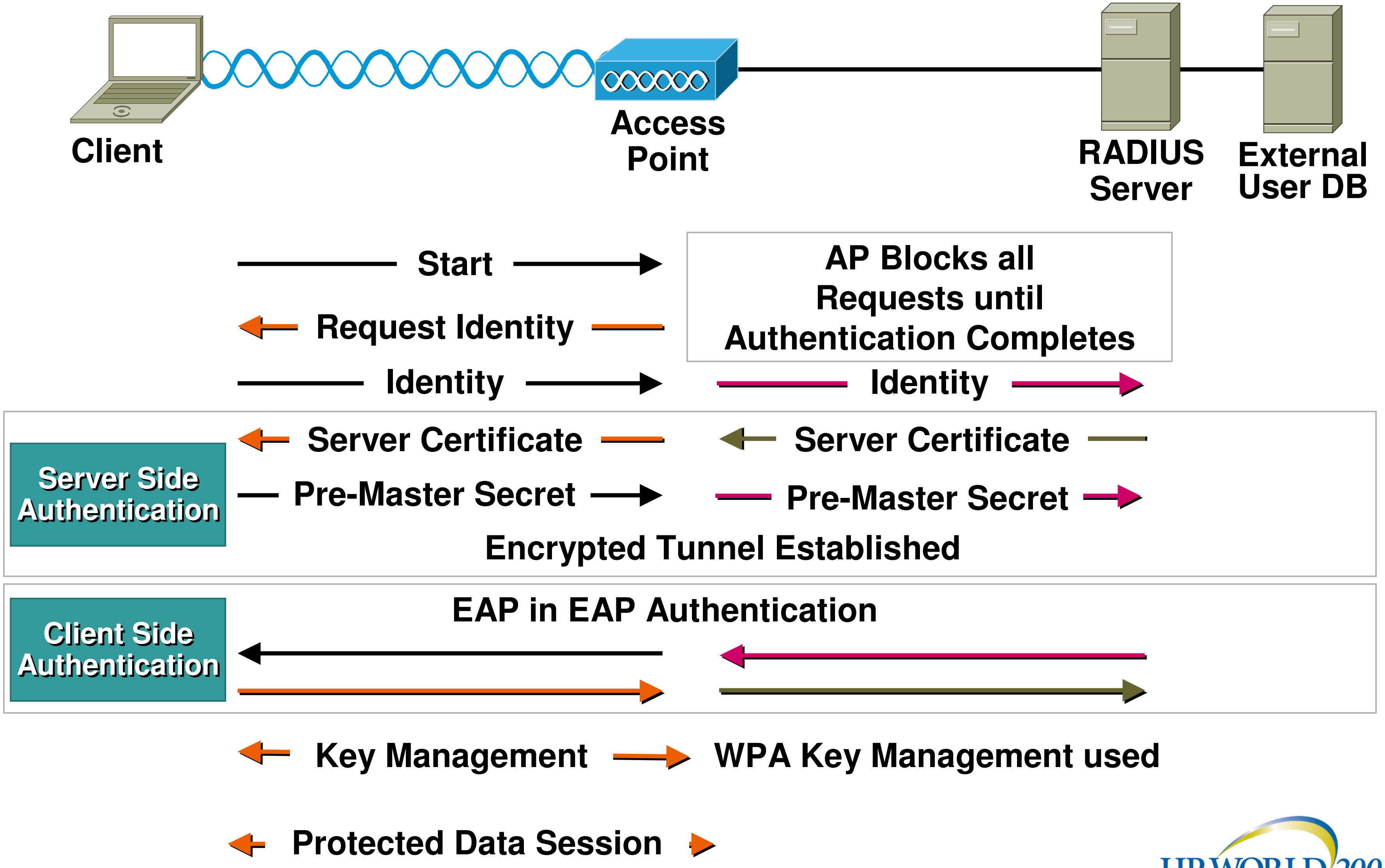


HP WORLD 2004
Solutions and Technology Conference & Expo

EAP-PEAP

- Hybrid Authentication Method
  - Server side authentication with TLS
  - Client side authentication with EAP authentication types (EAP-GTC, EAP-MSCHAPv2, etc.)
- Clients do not require certificates
  - Simplifies end user/device management
- RADIUS server requires a server certificate
  - RADIUS server self-issuing certificate capability
  - Purchase a server certificate per server from public PKI entity
  - Setup a simple PKI server to issue server certificates
- Allows for one way authentication types to be used
  - One-time-passwords
  - Proxy to LDAP, Unix, NT/AD, Kerberos, etc.

EAP-PEAP Authentication



Client

Access Point

RADIUS Server

External User DB

Start

AP Blocks all Requests until Authentication Completes

Request Identity

Identity

Identity

Server Side Authentication

Server Certificate

Server Certificate

Pre-Master Secret

Pre-Master Secret

Encrypted Tunnel Established

Client Side Authentication

EAP in EAP Authentication

Key Management

WPA Key Management used

Protected Data Session

HP WORLD 2004
Solutions and Technology Conference & Expo

EAP Protocols: Feature Support

	EAP-TLS	PEAP	LEAP	EAP-FAST
Single sign-on	Yes	Yes	Yes	Yes
Login scripts (MS DB)	Yes[1]	Yes[1]	Yes	Yes
Password expiration (MS DB)	N/A	Yes	No	Yes
Client and OS availability	XP, 2000, CE, and others[2]	XP, 2000, CE, CCXv2 clients[3], and others[2]	Cisco/CCXv1 or above clients and others[2]	Cisco/CCXv 3 clients[4] and others[2]
MS DB support	Yes	Yes	Yes	Yes
LDAP DB support	Yes	Yes[5]	No	Yes
OTP support	No	Yes[5]	No	No

[1] Windows OS supplicant requires machine authentication (machine accounts on Microsoft AD)

[2] Greater Operating System coverage is available from Meetinghouse and Funk supplicants

[3] PEAP/GTC is supported on CCXv2 clients and above

[4] Cisco 350/CB20A clients support EAP-FAST on MSFT XP, 2000, and CE operating systems. EAP-FAST to be supported on CB21AG/PI21AG clients in 4QCY2004 and CCXv3 clients in 1QCY2005

[5] Supported by PEAP/GTC only

HP WORLD 2004
Solutions and Technology Conference & Expo

EAP Protocols: Feature Support

	EAP-TLS	PEAP	LEAP	EAP-FAST
Off-line Dictionary attacks?	No	No	Yes[1]	No
Fast Secure Roaming (CCKM)	No	No	Yes	Yes
Local authentication	No	No	Yes	Yes[2]
WPA support	Yes	Yes	Yes	Yes
Application Specific Device (ASD) support	No	No	Yes	Yes
Server certificates?	Yes	Yes	No	No
Client certificates?	Yes	No	No	No
Deployment complexity	High	Medium	Low	Low
RADIUS server scalability Impact	High	High	Low	Low/Medium

[1] Strong Password Policy recommended; Please refer to --- http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html

[2] Local Authentication support is planned for 4QCY2004

HP WORLD 2004
Solutions and Technology Conference & Expo

IEEE 802.11i (WLAN Security) Improvements

- 802.11i is an IEEE 802.11 subcommittee responsible for WLAN Security Improvements
- Key Components of IEEE 802.11i standard are:
  - EAP/802.1x framework based User Authentication
  - TKIP: Mitigate RC4 key scheduling vulnerability and active attack vulnerabilities
  - IV Expansion: 48-bit IVs
  - Key Management: Isolate Encryption key management from user authentication
  - AES: Long term replacement protocol for RC4 (WEP)
- WPA is the Wi-Fi Alliance (WFA) inclusion of 802.11i Security Recommendations

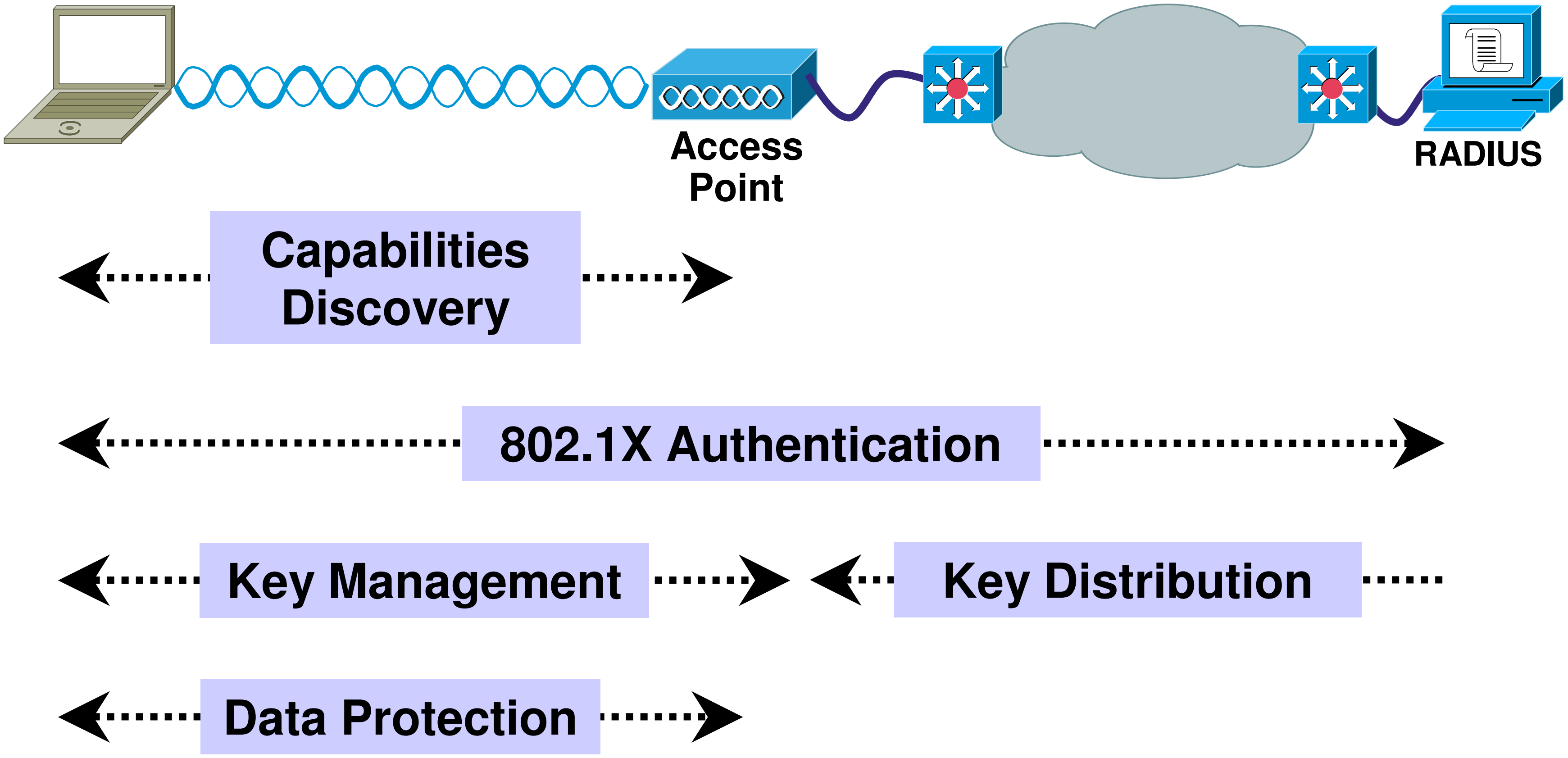
Cisco TKIP (CKIP)

- Cisco TKIP is a pre-WPA implementation of 802.11i security recommendations
- Available on Cisco/CCX clients only
- Cisco TKIP components
  - –TKIP: Per-Packet Keying and Message Integrity Check (MIC)
  - –Broadcast Key Rotation
  - –Note: Per-Packet Keying and MIC can be independently enabled
  - –Cisco TKIP is advertised (by Cisco APs) using Aironet Extensions
- Cisco TKIP was implemented for historical reasons
  - –CY ’01: Cisco TKIP was implemented and made available due to lack of standardized enhanced/strong encryption

Wi-Fi Protected Access (WPA)

- Components of WPA:
  - Authenticated key management using 802.1X:
    - EAP authentication and Pre-Shared Key (PSK) authentication
  - TKIP: Per-Packet Keying and Message Integrity Check (MIC)
  - Unicast and broadcast key management
  - IV expansion: 48-bit IVs
- Cisco's support for WPA:
  - AP1200 and AP350 (IOS only) and AP1100
  - Cisco 350, CB20A, CB21AG/PI21AG, CCXv2 Clients
- Client support for WPA requires Host-level supplicant
  - Note: Host-level supplicant is required for key management function whereas TKIP functionality is implemented at the NIC driver/firmware level

802.11i/WPA Authentication and Key Management Overview



Capabilities Discovery

802.1X Authentication

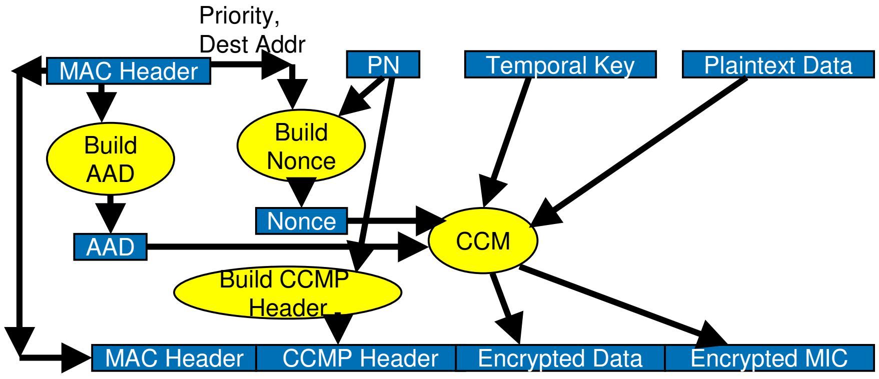
Key Management

Key Distribution

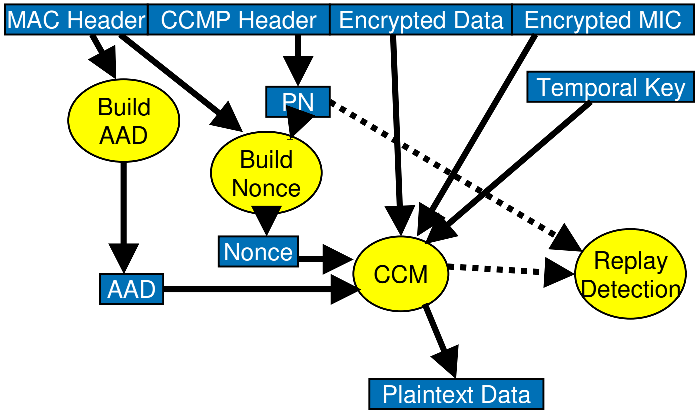
Data Protection

WPAv2 Description

- A Key component of WPAv2 is Advanced Encryption Standard (AES) support
  - 128-bit AES-CCM (CCM is Counter Mode for confidentiality and CBC-MAC mode for integrity) to be supported in WPA2
- Optimized 4-way handshake to establish PTK and distribute GTK



CCMP Encapsulation



CCMP Decapsulation

HP WORLD 2004
Solutions and Technology Conference & Expo

Cisco TKIP vs. WPA vs. WPAv2

	Cisco TKIP	WPA	WPAv2
TKIP (PPK and MIC)	Yes	Yes	Yes
AES (128-bit)	No	No	Yes
48-bit IVs supported?	No	Yes	Yes
Per-User session key refresh (i.e. session key rotation)	Every 4 HR and 40 minutes	Not Required	Not Required
Broadcast Key rotation supported?	Yes	Yes	Yes
FMS Attack Mitigation	Yes	Yes	Yes
Data Integrity protection	Yes	Yes	Yes
Replay Attack Detection	Yes	Yes	Yes

Wireless LAN Security Best Practices

- Technologies to Secure Wireless LANs
  - EAP/802.1x Authentication Protocols
  - Data Encryption and Message Integrity: WPA, CKIP, WPAv2
- **EAP/802.1x with WPA/WPAv2 Deployment Considerations**
  - EAP Supplicant Availability
  - RADIUS Server Scalability and Availability

EAP and WPA Supplicant Availability

- Native Windows Supplicant
  - –Windows XP: Both EAP and WPA supplicants available
  - –Windows 2000 and older: EAP supplicant available
  - –This is available for Cisco and non-Cisco clients
- Cisco 350 and CB20A Client
  - –LEAP: Windows, Linux, Mac OS, and DOS
  - –PEAP: Windows XP, Windows 2000, and Windows CE
  - –EAP-FAST: Windows XP, Windows 2000, and Windows CE
  - –WPA: Windows XP and Windows 2000
  - –Note: WPA support for PEAP on Windows 2000 for 350/CB20A client adapters requires third-party supplicant due to lack of native OS support for WPA
- CB21AG and PI21AG Clients
  - –Supported on Windows XP and Windows 2000
  - –LEAP, EAP-TLS, PEAP/MS-CHAPv2, and PEAP-GTC
  - –WPA supported for all EAP types on both Windows 2000 and XP platforms
  - –EAP-FAST (4QCY2004)

EAP and WPA Supplicant Availability

- CCX client
  - –LEAP: CCXv1 and above
  - –EAP-FAST: CCxv3.0 (Target: 1QCY2005)
  - –PEAP-GTC: CCXv2 and above
  - –WPA: CCXv2 and above
- Third-party supplicants (for both EAP and WPA)
  - –Funk
  - –Meetinghouse Data Communications
- Using Cisco/CCX supplicant vs. native OS supplicant
  - –Client management functions
  - –Vendor specific configurations: RF Management, Roaming, etc.
- Bridges
  - –Cisco LEAP supported on BR1400, BR1300, BR350, WGB350, etc.

Cisco Compatible Extensions (CCX)

- 69 CCX partners to date
  - –20 silicon vendors
- >130 products have passed CCX v1 Testing
  - –Including laptops from HP, IBM, Dell, and Toshiba
  - –Many more products in the pipeline
- CCX v2 products
  - –Security
    - •WPA
    - •Interoperability testing for three 802.1X authentication types (LEAP, PEAP, EAP-TLS)
  - –Mobility (Fast Secure Layer 2 Roaming)
  - –Voice over WLAN
  - –Rogue AP detection
  - –Site survey assist

http://www.cisco.com/en/US/partners/pr46/pr147/partners_pgm_partners_0900aecd800a7907.html

RADIUS Server Scalability and Availability

- Why RADIUS scalability and availability matters?
  - This will affect your WLAN network availability
- Factors determining RADIUS server scalability:
  - EAP Protocol (LEAP vs. EAP-FAST vs. PEAP/EAP-TLS)
  - Total number of EAP users as well as APs
  - Authentication time-out
  - Reference: http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_white_paper09186a00801495a1.shtml
- RADIUS server availability considerations
  - Dependency on a WAN link to reach the RADIUS server
  - Location of primary vs. secondary RADIUS servers

RADIUS Server Availability

- Large campus design (as part of metro area network)
  - Locate primary and redundancy servers in different data centers (i.e.. Separate physical locations)
- Large enterprise global deployment
  - Provide primary and redundancy servers locally for large campuses
  - Deploy RADIUS servers in regional network operational centers (NOCs) for branch/remote offices
  - Note: assumption made here is remote/branch offices have reliable redundancy for WAN links
- Distributed retail stores or healthcare clinics
  - Use regional NOC or HQ NOC as the primary RADIUS server
  - Use a localized RADIUS server as the redundant server
    - Local RADIUS server OR
    - Local authentication service available on the AP

WLAN Deployment Examples (Cont.)

Enterprise Deployment Example

- Clients standardized on CCX laptops with Windows 2000 and XP operating systems
- PEAP/MS-CHAPv2 with WPA deployed as the security mechanism for laptop users
- LEAP with dynamic WEP deployed as the security mechanism for Cisco 7920 devices (to be migrated to LEAP/with CCKM and WPA)
- Separate user accounts with strong password policy used for VoIP users (i.e. LEAP users)
- Web-based user authentication implemented for guest access
- Primary/Redundant RADIUS servers located locally for HQ campus
- RADIUS servers deployed at regional NOCs for remote/branch offices

WLAN Deployment Examples (Cont.)

Education Deployment Example

- Open with Mac Address authentication along with web-based authentication deployed for students
- Data confidentiality not provided to students due to non standardized client environment
- Client devices for staff standardized on Windows XP and 2000 with Cisco 350 client adapters
- EAP-FAST with WPA deployed for staff to provide user-based authentication and data confidentiality

WLAN Deployment Examples (Cont.)

Healthcare Deployment Example

- Windows 2000/XP and Windows CE standardized for mobile client devices (with Cisco and non-Cisco WLAN adapters)
- Cisco LEAP selected as the EAP authentication protocol
- Third-party supplicant used to enable LEAP on non-Cisco clients
- Fast Secure Roaming is a requirement for patient monitoring systems (example: Fusion pump monitors) and VoIP devices
- Strong password policy (15-character password) used for LEAP deployment
- RADIUS servers deployed locally for large hospitals
- RADIUS servers deployed at regional NOCs for distributed small/medium clinics
- Local authentication service used at small/remote clients where WAN link stability is questionable

Agenda

- Drivers for WLAN Security
- WLAN Security Vulnerabilities and Threats
- WLAN Security Deployment Criteria
- WLAN Deployment Examples
- WLAN Security Best Practices
- **Wireless IDS**
- Wireless/Wired Integration Best Practices
- Summary

Why Wireless IDS Matters?

- Ongoing monitoring of 802.11 network to detect
  - Unauthorized Access Points
  - Active attacks
  - Incorrectly configured Access Points and Clients
- Wireless IDS has become an evolving technology area (compared to old days of wired IDS)
  - Requirement to monitor for attack tools (NetStumbler, etc)
  - Requirement to monitor specific types of attacks (mostly active attacks)
  - Manual containment (alert the administrator and let him choose a course of action) vs. Auto containment

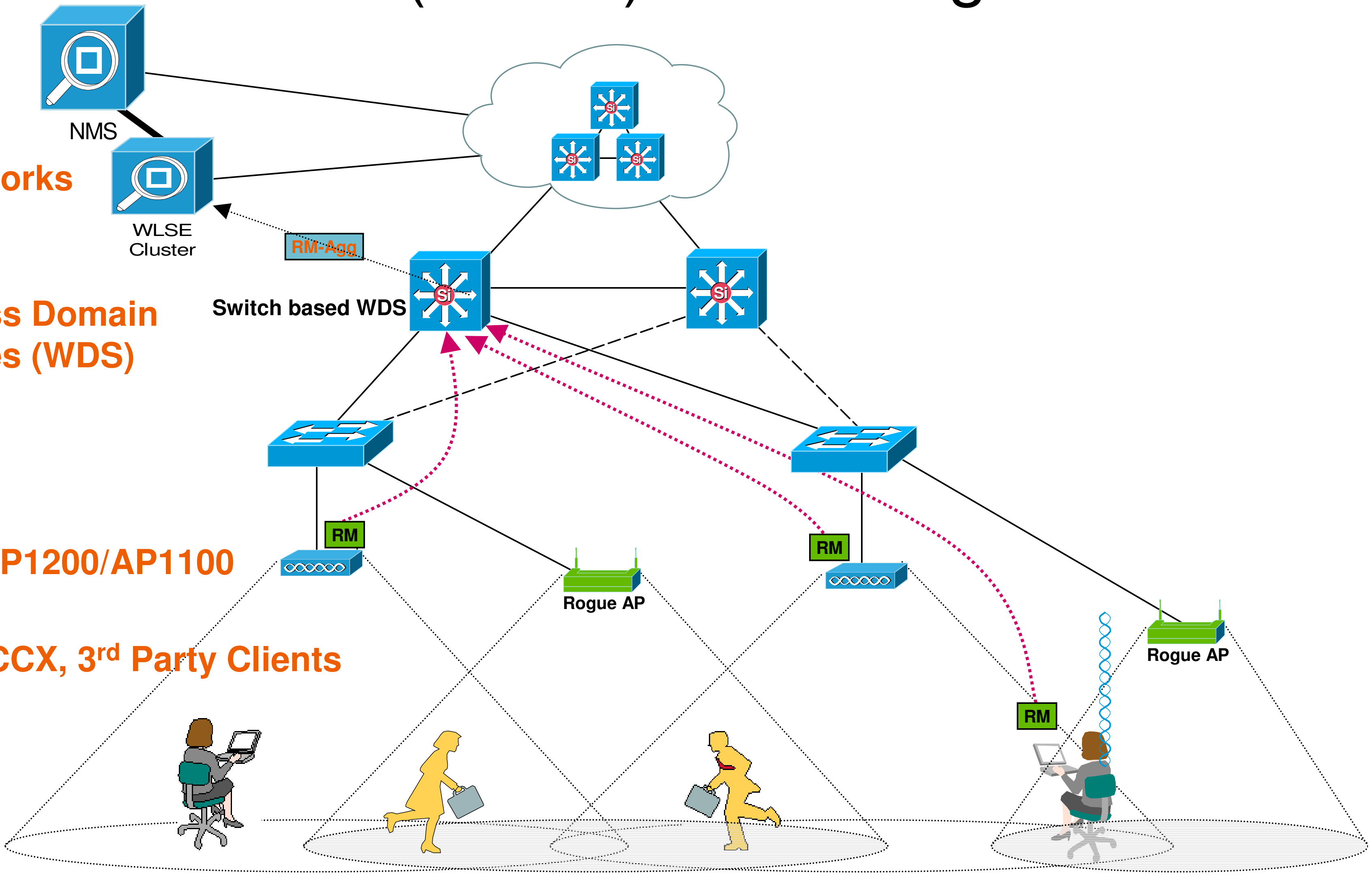
Cisco SWAN Solution: Radio (Air/RF) Monitoring

CiscoWorks WLSE

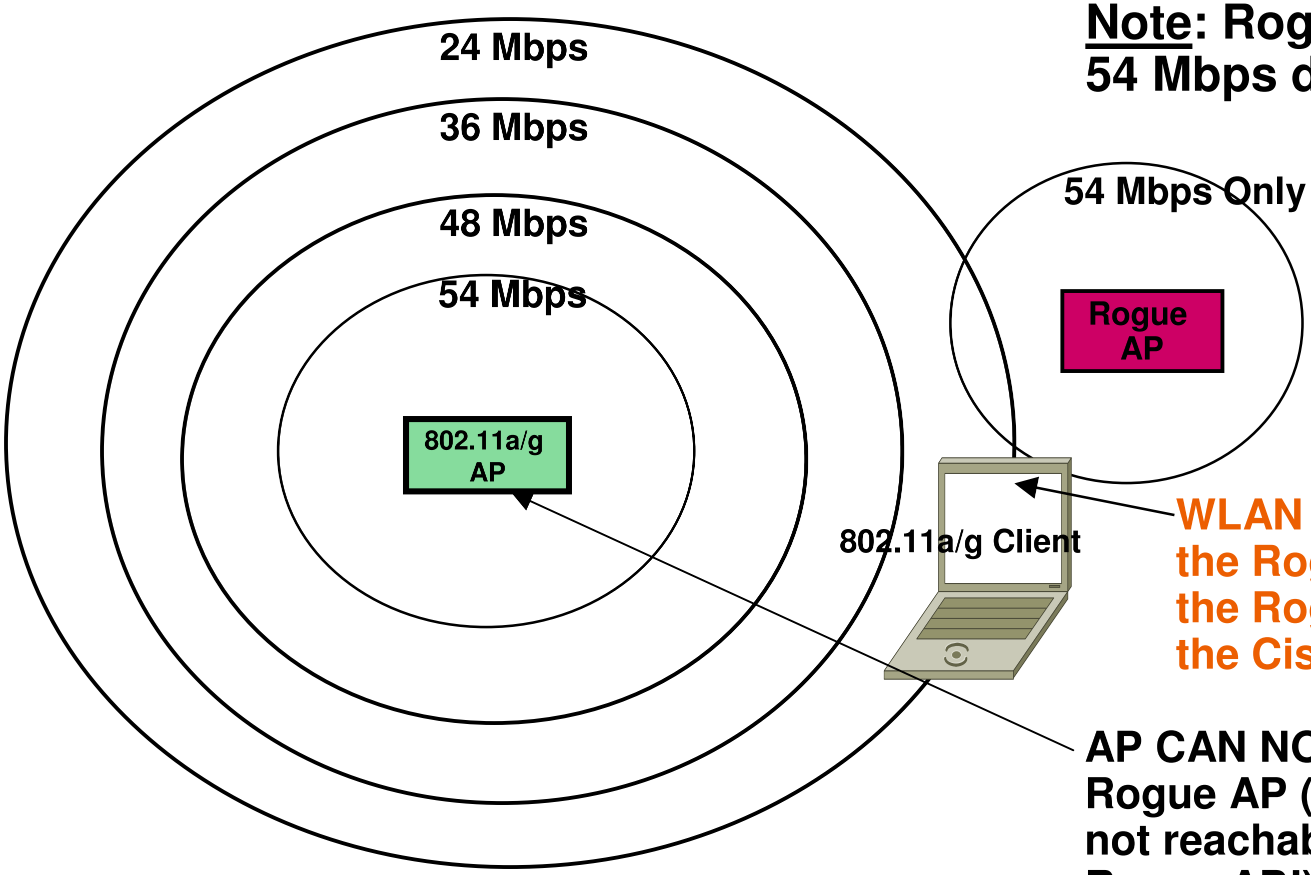
Wireless Domain Services (WDS)

Cisco AP1200/AP1100

Cisco, CCX, 3rd Party Clients



Why Client-Based Scanning?



Note: Rogue AP only has 54 Mbps data rate enabled!

WLAN Client does detects the Rogue AP and reports the Rogue AP information to the Cisco AP!

AP CAN NOT detect the Rogue AP (54 Mbps coverage not reachable as far as the Rogue AP!)

Cisco's WLAN Solution leverages multi-vendor clients from CCX partners as well as Cisco Clients!

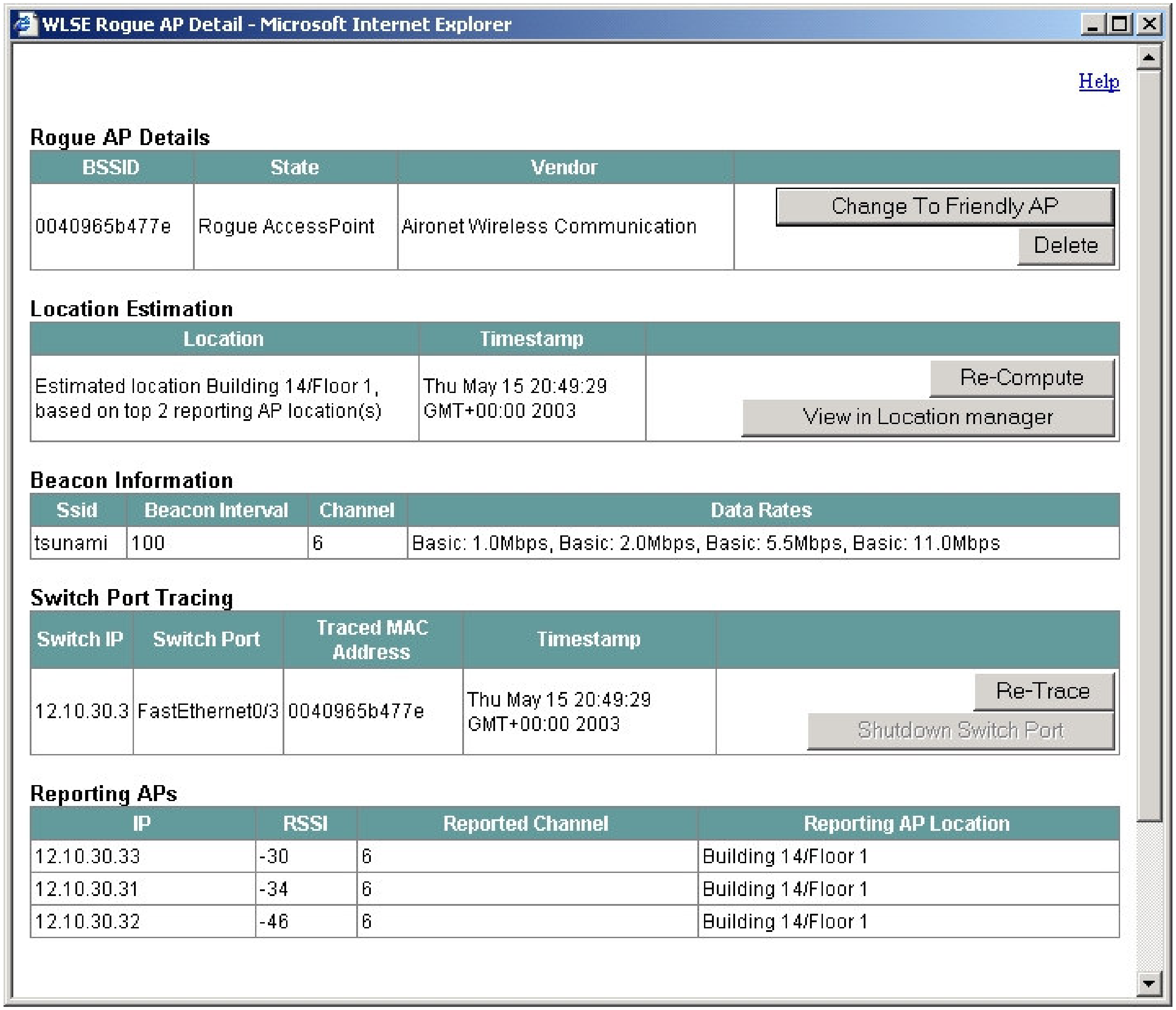
Integrated vs. Dedicated IDS Deployment

- Integrated Wireless IDS deployment (supported since WLSE 2.5 and 12.2(13) JA)
  - –Active 802.11 Access Points collect RF data while servicing 802.11 clients
  - –AP would be configured for a specific channel and can collect data for that channel while servicing clients
  - –AP would jump to an other channel (i.e. non-servicing channel) while idle to collect RF information
- Dedicated Wireless IDS deployment (supported with WLSE 2.7 and 12.2(15)JA release and above)
  - –AP functions as a dedicated sensor to scan all channels for 802.11b/g and/or 802.11a
  - –Specialized IDS functions available via dedicated mode
- Combined deployment modes possible
  - –Example: AP's 802.11g radio deployed in integrated mode whereas 802.11a radio deployed in dedicated mode

Rogue AP Detection and Suppression

- Rogue AP detection methodology
  - APs and clients collect and report BSSID information via beacons and probe responses
  - WLSE compares collected BSSID information versus authorized (i.e. managed APs) BSSID information
  - Unauthorized APs are flagged and reported via faults monitoring functionality
- Rogue AP suppression techniques
  - Administrator is notified location of the rogue AP via location manager; locate the rogue AP and physically remove it!
  - Trace the rogue AP over the wired network and shut-down the switch port
    - CDP Needs to be enabled on the switches
    - CAM table lookup is used to locate the rogue AP

Cisco Works WLSE:
Rogue AP Details Screen



Rogue AP Details

BSSID	State	Vendor	
0040965b477e	Rogue AccessPoint	Aironet Wireless Communication	Change To Friendly AP Delete

Location Estimation

Location	Timestamp	
Estimated location Building 14/Floor 1, based on top 2 reporting AP location(s)	Thu May 15 20:49:29 GMT+00:00 2003	Re-Compute View in Location manager

Beacon Information

Ssid	Beacon Interval	Channel	Data Rates
tsunami	100	6	Basic: 1.0Mbps, Basic: 2.0Mbps, Basic: 5.5Mbps, Basic: 11.0Mbps

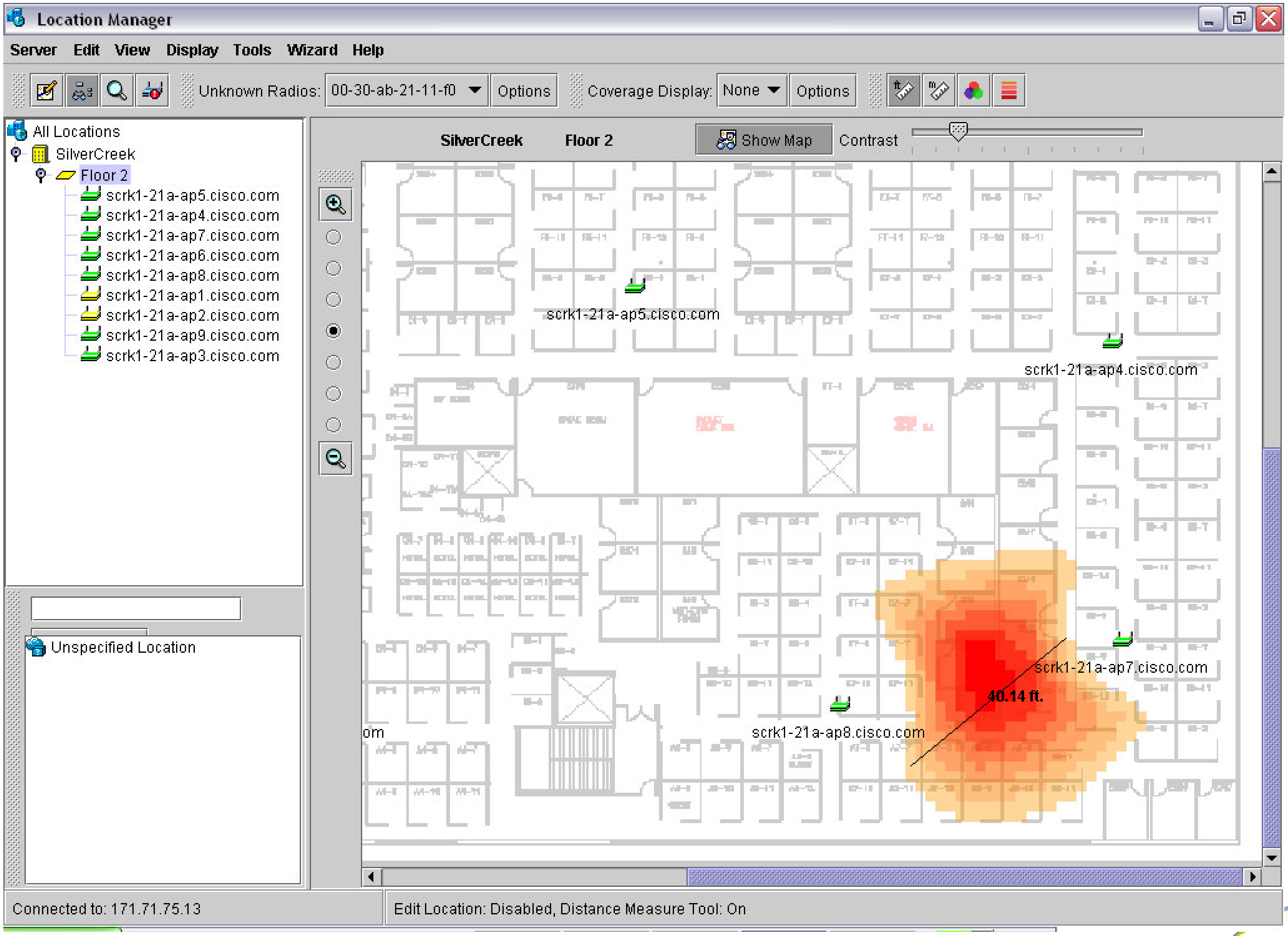
Switch Port Tracing

Switch IP	Switch Port	Traced MAC Address	Timestamp	
12.10.30.3	FastEthernet0/3	0040965b477e	Thu May 15 20:49:29 GMT+00:00 2003	Re-Trace Shutdown Switch Port

Reporting APs

IP	RSSI	Reported Channel	Reporting AP Location
12.10.30.33	-30	6	Building 14/Floor 1
12.10.30.31	-34	6	Building 14/Floor 1
12.10.30.32	-46	6	Building 14/Floor 1

CiscoWorks WLSE: Location Manager



Location Manager

Unknown Radios: 00-30-ab-21-11-f0

Coverage Display: None

SilverCreek Floor 2

- All Locations
  - SilverCreek
    - Floor 2
      - scrk1-21a-ap5.cisco.com
      - scrk1-21a-ap4.cisco.com
      - scrk1-21a-ap7.cisco.com
      - scrk1-21a-ap6.cisco.com
      - scrk1-21a-ap8.cisco.com
      - scrk1-21a-ap1.cisco.com
      - scrk1-21a-ap2.cisco.com
      - scrk1-21a-ap9.cisco.com
      - scrk1-21a-ap3.cisco.com

Unspecified Location

Connected to: 171.71.75.13

Edit Location: Disabled, Distance Measure Tool: On

WLAN Deployment Examples (Cont.)

- RF Monitoring is recommended for all deployments
  - Enable Radio (RF) Monitoring functions using the latest WLSE, Switch, and AP IOS releases
  - Enable RF scanning using the APs and if possible enable client based scanning using Cisco/CCX clients
  - Make sure to investigate and identify “friendly” APs in multi-tenant environment
- Enable security policy monitoring via WLSE
  - Define standardized security policy via WLSE and monitor for any discrepancy in AP configuration
  - Monitor the availability of the RADIUS servers for EAP authentication

Agenda

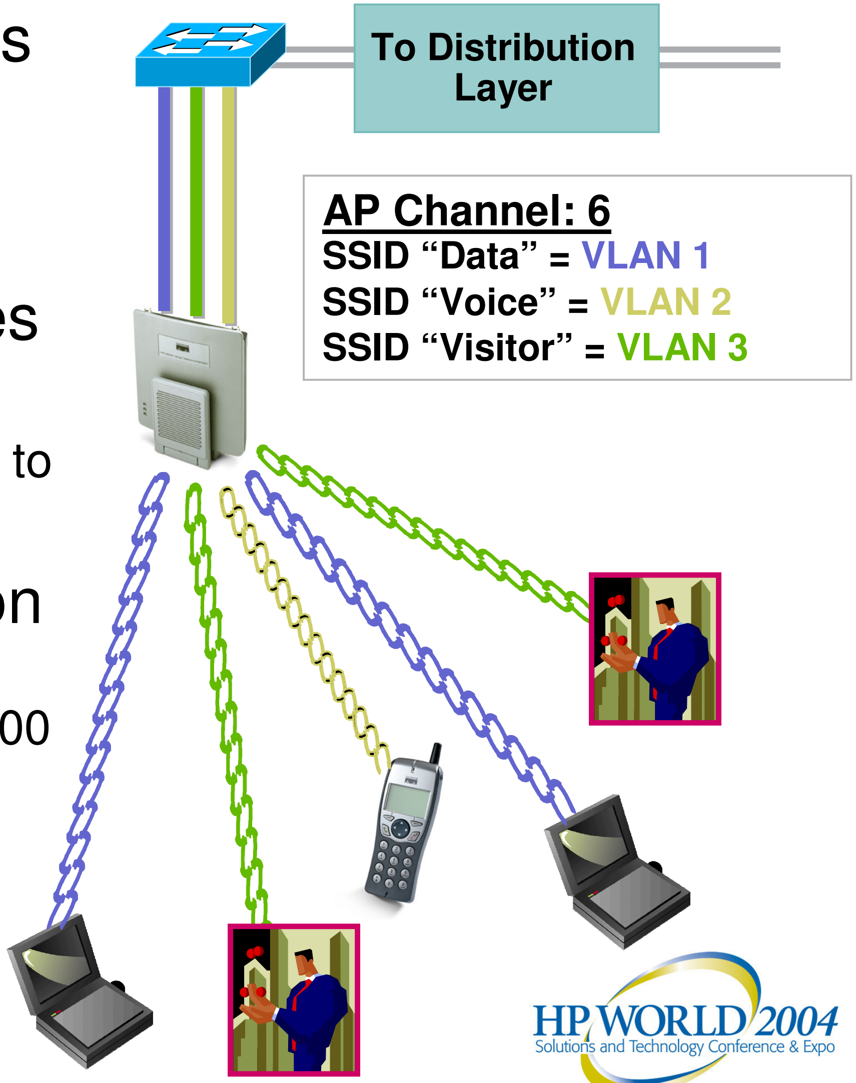
- Drivers for WLAN Security
- WLAN Security Vulnerabilities and Threats
- WLAN Security Deployment Criteria
- WLAN Deployment Examples
- WLAN Security Best Practices
- Wireless IDS
- **Wireless/Wired Integration Best Practices**
- Summary

Wired/Wireless Integration Best Practices

- Mapping wireless security policies to the wired network
  - Use of multiple user/device groups (via SSIDs/VLANs/mGRE tunnels)
- Use of wired security features for wireless LAN deployment
- Fast secure roaming (CCKM)
- Catalyst 6500 switch integration
  - Central point of ingress for control and data traffic
  - End-to-end integrated security
  - Fast secure Layer-3 roaming

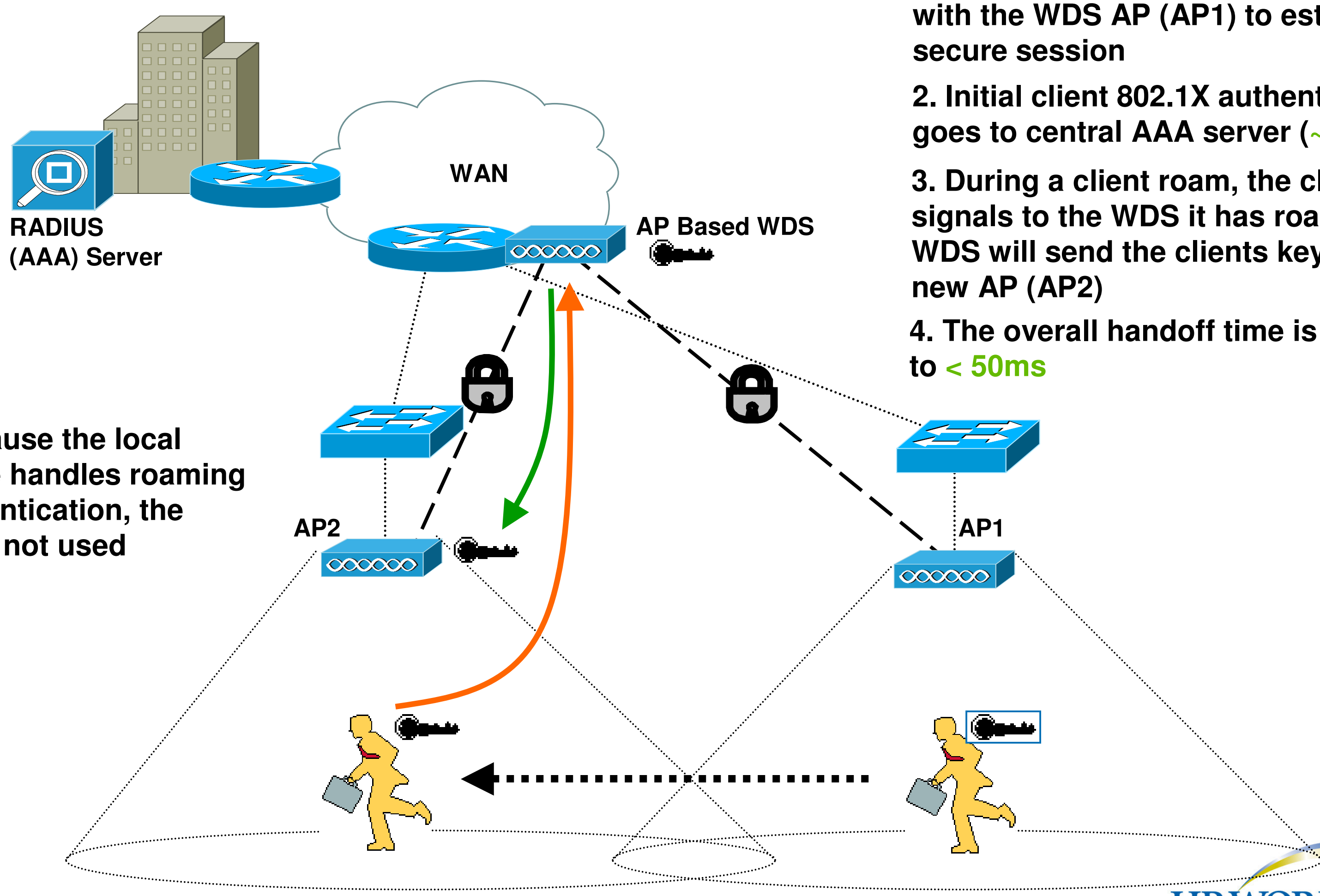
Mapping Wireless Security Policies to the Wired Network

- Multiple WLAN Security Policies
  - –Data vs. voice vs. legacy devices vs. guest access
  - –VLAN to SSID mapping
- Mapping WLAN security policies to wired security policies
  - –Use L2 to L4 ACLs on the wired side to reinforce WLAN security policies
- Catalyst 6500 WLSM Integration
  - –Use 6500 security features on the mGRE interface terminating on the 6500



AP Channel: 6
SSID “Data” = VLAN 1
SSID “Voice” = VLAN 2
SSID “Visitor” = VLAN 3

Cisco SWAN: Fast Secure Roaming



NOTE: Because the local WDS device handles roaming and reauthentication, the WAN link is not used

1. AP must now 802.1X authenticate with the WDS AP (AP1) to establish a secure session

2. Initial client 802.1X authentication goes to central AAA server (~500ms)

3. During a client roam, the client signals to the WDS it has roamed and WDS will send the clients key to the new AP (AP2)

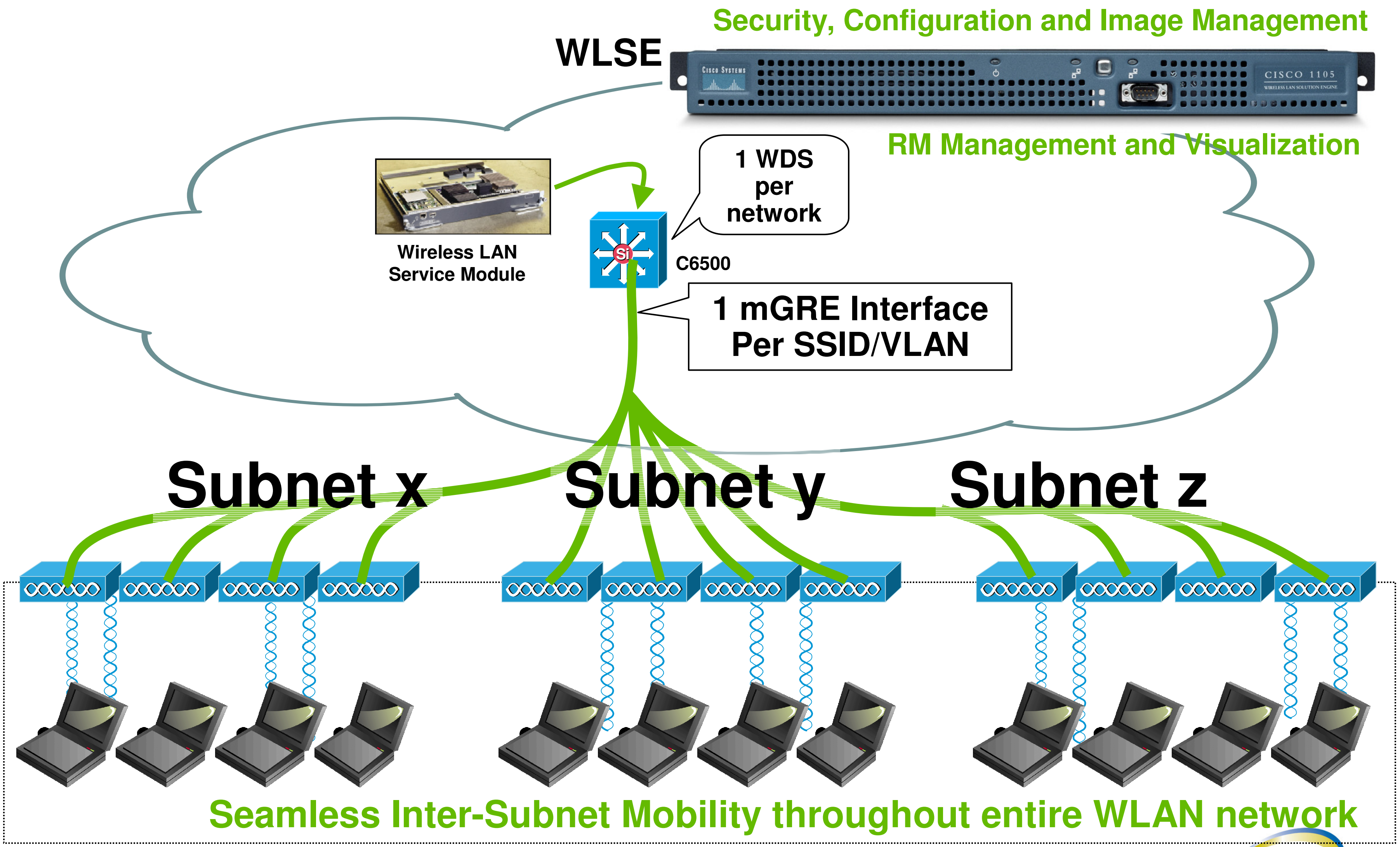
4. The overall handoff time is reduced to < 50ms

HP WORLD 2004
Solutions and Technology Conference & Expo

Catalyst 6500 Switch Integration

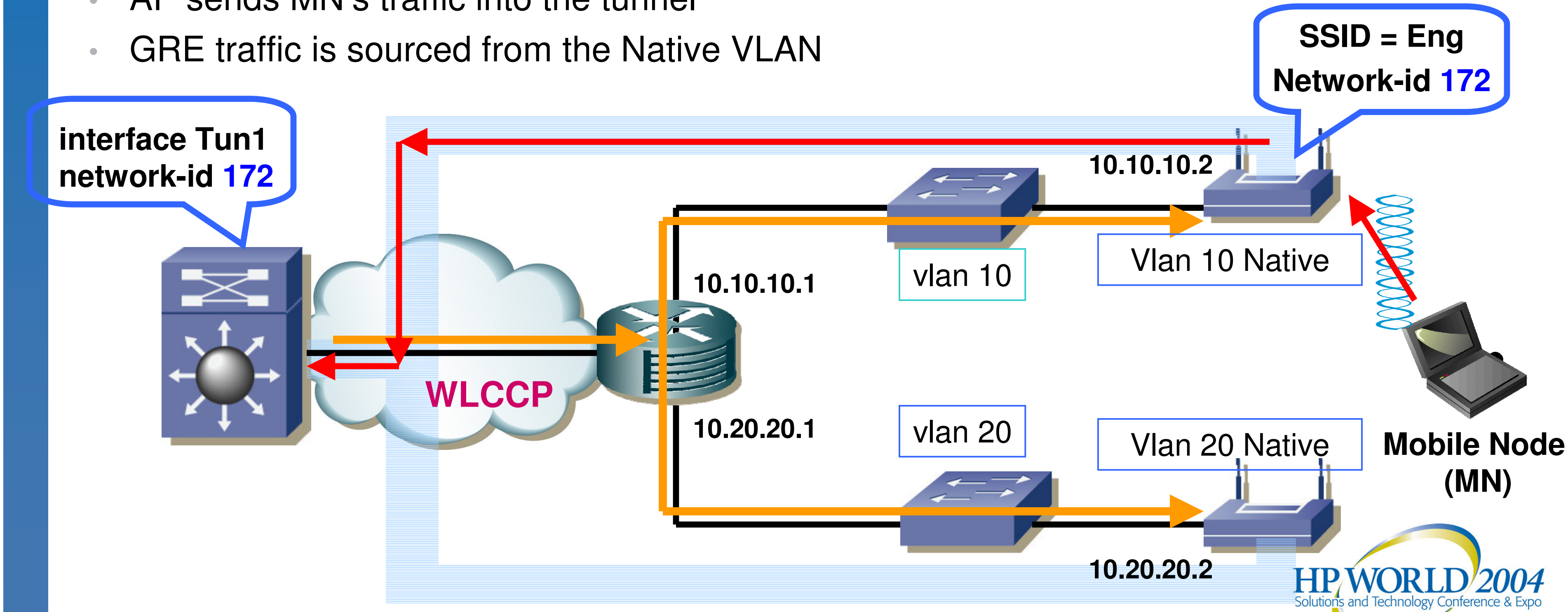
- Wired/wireless integration enabled with Wireless LAN Service Module (WLSM)
  - –One pair of Catalyst 6500 (equipped with WLSMs and Supervisor 720 modules) to enable wireless traffic aggregation
  - –NOTE: WLAN traffic aggregation can be enabled at distribution or data-center layer levels
  - –Increased WDS scalability for roaming and RF management services
  - –Layer-3 Roaming supported
- Central point of ingress for control and data traffic
  - –Data traffic is aggregated at the 6500 switch using mGRE tunnels from the APs
to the Switch
  - –mGRE tunnels terminate on the 6500 supervisor (hardware based GRE encapsulation is supported using the Supervisor 720)
  - –Control traffic (WLCCP traffic) terminates on the WLSM
- End-to-end integrated security
  - –Ability to leverage existing 6500 security features for WLAN user traffic aggregation

Cisco SWAN Solution: Switch-Based WDS

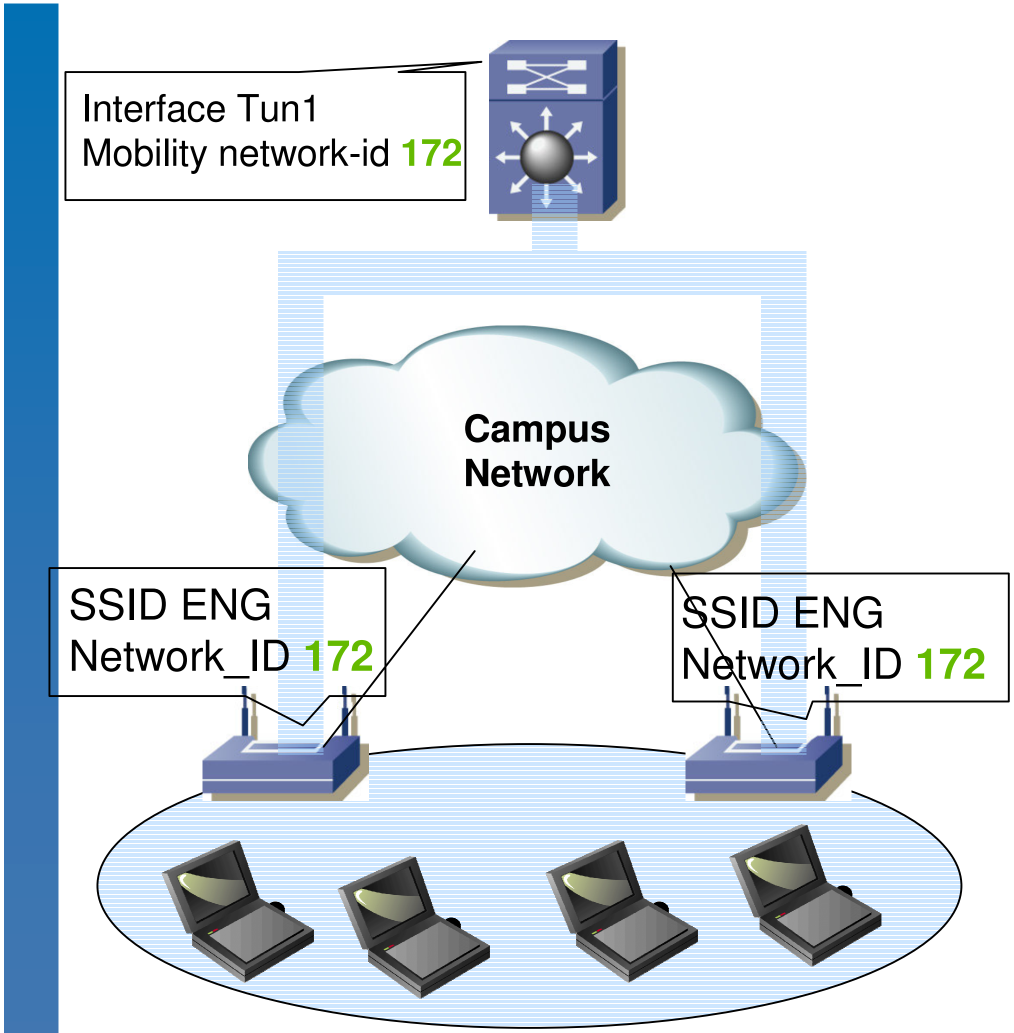

Security, Configuration and Image Management
WLSE
CISCO SYSTEMS
CISCO 1105
RM Management and Visualization
Wireless LAN Service Module
1 WDS per network
C6500
1 mGRE Interface Per SSID/VLAN
Subnet x
Subnet y
Subnet z
Seamless Inter-Subnet Mobility throughout entire WLAN network

Catalyst 6500 WLSM Overview
How Does It Work?

- Define a Native VLAN on the AP's and Access Switches
- Assign IP address to Access Points
- Define Mobility Group on sup720 and Access Points
- AP's learn the mGRE endpoint through WLCCP
- mGRE tunnel is built
- AP sends MN's traffic into the tunnel
- GRE traffic is sourced from the Native VLAN



Catalyst 6500 WLSM Overview
Mobility Group



SSID=ENG/network-ID=172

MOBILITY GROUP:

- Seamless L3 Mobility is enabled within one Mobility Group
- Identified by SSID/network-ID on the AP. Can be specified also as SSID/VLAN-ID/network-ID if multiple VLANs are enabled locally on the AP
- NOTE: If multiple VLANs are enabled on the AP, no need to span VLANs across the campus network to enable L3 mobility!
- Identified by the Tunnel interface on the sup720
- The same SSID/Network-ID on all the AP's where L3 mobility is required
- One network-ID = one wireless subnet
- Limit of 16 SSID/Network-ID

AP-based WDS Vs Switch-Based WDS

	AP-based WDS	Switch-based WDS
WDS Deployment	Maximum of one active WDS per subnet	Multiple WDS allowed per network
Scalability*	Active AP: 30 APs Dedicated AP: 60 APs	WLSM: Up to 300 APs
WDS Discovery	Automatically discovered	Specified on the AP
Fast Secure Roaming	Supported	Supported
RF Data Aggregation	Supported	Supported
Layer-3 Roaming	No	Yes

*** NOTE: Scalability numbers are based on 20 client associations per AP; AP1200 or AP1100 can be used as the AP-based WDS.**

Catalyst 6500 Security Features

Recommended Catalyst 6500 Security Feature Sets to Consider for Wireless/Wired Integration:

- Layer-2/3/4 ACLs (hardware accelerated support) along with various ACL options (standard, extended, reflexive, and time-based)
- Router ACLs (RACLs)
- TCP Intercept: To stop TCP SYN flooding attacks
- Unicast RPF (URPF) Checks: Mitigate problems caused by malformed or spoofed packets
- RP Rate Limiters: Used to prevent DoS attacks using “bogus” traffic (Example: ICMP ping requests from bogus IP addresses)
- IOS Firewall Feature Set: This is a software feature set that provides support for Authentication Proxy; Port to Application Mapping (PAM) and Content Based Access Control (CBAC)
- Service Module Integration (Firewall, IDS, VPN, and NAM service modules are supported with WLSM)

WLAN Deployment Examples (Cont.)

Enterprise Example:

- Catalyst 6500 WLSM integration to provide a scalable WLAN deployment model
- Use separate VLANs/SSIDs/GRE tunnels for Enterprise, VoIP, and Guest access (4 VLANs, 3 SSIDs, 3 GRE tunnels)
- Fast Secure Roaming implemented for VoIP devices
- ACLs were used at the 6500 switch level to limit access to VoIP users (access was only allowed to VoIP gateways, Call Manager, etc)
- Guest User traffic aggregated (on the WLAN aggregation 6500 switch) and tunneled to the DMZ to allow Internet access only
- ACLs were used at the 6500 switch level to limit access to guest users (access was only allowed to DMZ and denied elsewhere)
- BBSM like device was used to authenticate Guest users via Internet browser (https-based user authentication)

WLAN Deployment Examples (Cont.)

Education Deployment Example

- Catalyst 6500 WLSM integration to provide a scalable WLAN deployment model
- Use separate VLANs/SSIDs/GRE tunnels for student and staff WLAN access (3 VLANs, 2 SSIDs, 2 GRE tunnels)
- 6500 security features were leveraged to mitigate various DoS attacks originating via the WLAN network

WLAN Deployment Examples (Cont.)

Healthcare Deployment Example

- Use separate VLANs/SSIDs for Doctors, Nurses, and patient monitoring applications
  - Restrict access for each user-group/application via wired security policies (Layer2/3/4 ACLs, etc)
- Multiple WLAN deployment models: Large Hospital installation to remote clinic environment
  - Layer-3 WDS (Catalyst 6500 Integration) for large (> 100 APs) hospital deployments
  - Layer-2 WDS (AP-based) for small/remote clinics (<20 APs)
- Fast Secure Roaming implemented for active mobile users (Example: Patients equipped with 802.11-enabled fusion pump monitoring devices)

Summary

- WPA, WPAv2, or Cisco TKIP along an EAP protocol solution is recommended for WLAN security deployment
  - Choose the best EAP protocol the suits your deployment environment
  - Consider making a trade-off between security strength vs. ease of deployment
  - RADIUS (i.e. EAP) server availability and scalability MUST be considered as part of your design/implementation process
- Implement advanced security features such as Wireless IDS as well as Wired/Wireless best practices
- Enable Security Policy Monitoring via WLSE
  - Enable RF scanning using the APs and if possible enable client based scanning using Cisco/CCX clients
  - Proactively monitor and respond to security threats

Reference URLs

- Cisco Aironet Security Web site

  http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_package.html

- WEP Vulnerabilities

  http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps

  http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

  http://airsnort.sourceforge.net/

- Cisco Response to Dictionary attacks on Cisco LEAP

  http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml

  http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html

- Latest CCX Information

  http://www.cisco.com/en/US/partners/pr46/pr147/partners_pgm_partners_0900aecd800a7907.html

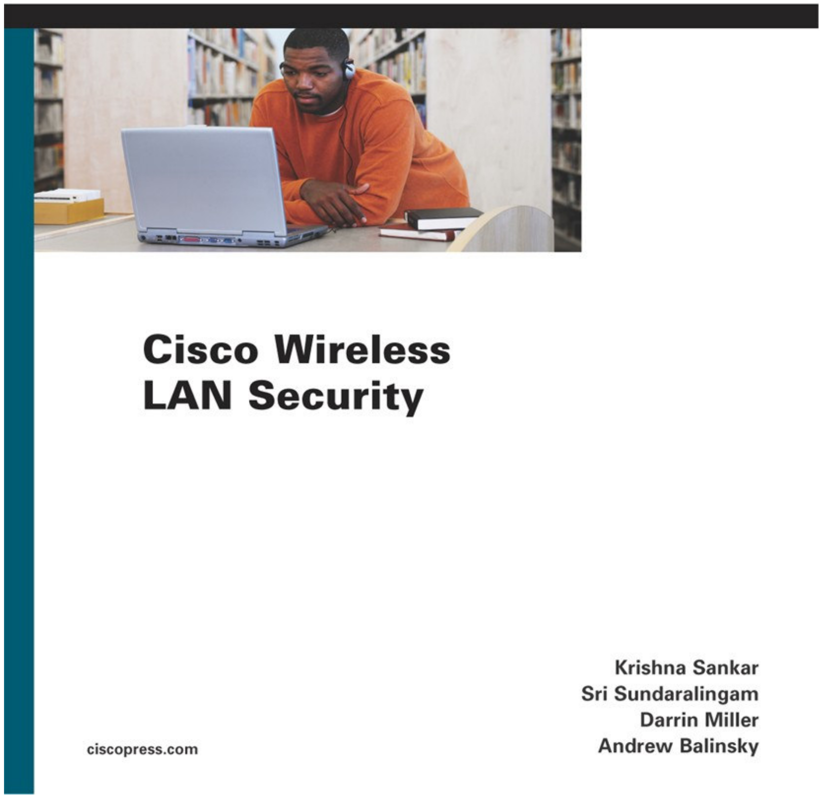
- Cisco ACS deployment guide for WLAN networks

  http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_white_paper09186a00801495a1.shtml

Coming Soon …

Cisco Systems

ISBN: 1587051540



Cisco Wireless LAN Security

Krishna Sankar
Sri Sundaralingam
Darrin Miller
Andrew Balinsky

ciscopress.com

http://ciscopress.com/title/1587051540

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP