# Enterprise Wireless Networking

## Session ID #: 2498


## Abbas Masnavi

## Cisco Systems, Inc.


CISCO SYSTEMS

HP WORLD 2003
Solutions and Technology Conference & Expo

# Agenda


- Introduction
- Mobility
- WLAN Security
- Quality of Service
- Closing Remarks/Q&A

# Momentum is Building in Wireless LANs



- Wireless LANs are an “addictive” technology
- Strong commitment to Wireless LANs by technology heavy-weights
  - –Cisco, IBM, Intel, Microsoft
- Embedded market is growing
  - –Laptops & PDA’s with “wireless inside”
  - –Phones are next
- The WLAN market is expanding from Industry-Specific Applications to Universities, Municipalities, Homes, & Offices

# Evolution of the WLAN Business



***Early Adopters***

**Specific Industries**

Hotels Hospitals
Retail Manufacturing

**Education**

Universities
K1-12 Libraries

***Mainstream***

**Home Networking**

**Office WLANs**

**Outdoor Wireless Bridging**

***Next Wave***

**Public Access "Hotspots"**

Airports Restaurants
Hotels Coffee Shops
Entire Towns Convention Centers

**New Applications**

Phones, PDA's, Printers
Buses, Sports Events, Construction Sites
Public Safety (Police, Ambulances)

# Enterprise-Class WLAN Solutions


- **Security**
  - 802.1X: LEAP, PEAP
  - TKIP, WPA
- **Cost of ownership**
  - In-line power
  - Software upgradeability
  - Hardware upgradeability
- **Performance**
  - Throughput
  - Load balancing
  - 100 mW radios (802.11b)
- **Product line diversity**
  - Variety of antennas
  - Interoperable client solutions
  - Partnerships

# WLAN Product Line

HP WORLD 2003
Solutions and Technology Conference & Expo

## In-building Infrastructure

1200 Series
1100 Series

## Clients

350 Series 2.4 GHz
5 GHz client adapter
Wireless IP Phone

## Antennas

## Bridges

350 and
1400
Series

CISCO SYSTEMS

# Outdoor Wireless Bridges: Applications



- **Government Buildings**
  - Connect buildings' data networks
  - Cheaper than T1 (fast ROI)
  - Cheaper than trenching fiber
  - Backup system for when cables get cut
- **Education**
  - Public school system sharing WAN link
  - Colleges expanding into leased facilities
  - Connecting classroom trailers to main bldg.
- **Municipal Applications**
  - Emergency response (police, fire, city hall)
  - Public transportation (buses)
  - Courthouse
- **Temporary Broadband Link**
  - Construction sites
  - Sporting events
  - County Fairs

**16+ miles**
**11 Mbps**

# WLAN "Alphabet Soup": IEEE 802.11 Standards Activities


- **802.11a:** 5GHz, 54Mbps
- **802.11b:** 2.4GHz, 11Mbps
- **802.11d:** Multiple regulatory domains
- **802.11e:** Quality of Service (QoS)
- **802.11F:** Inter-Access Point Protocol (IAPP)
  *Recommended Practice (this is not a standard)*
- **802.11g:** 2.4GHz, 54Mbps
- **802.11h:** Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC)
- **802.11i:** Security *(currently at Draft 3.0)*
- **802.11j:** Japan 5GHz Channels (4.9-5.1 GHz)
- **802.11k:** Measurement

# 5 GHz vs. 2.4 GHz Comparison


## 5 GHz—802.11a

- Maximum WLAN data rate: 54 Mbps
- 12 channels available (4 for outdoor only)
- Initially approved for use in only certain countries (including U.S.)
- Less interference

## 2.4 GHz—802.11b and g

- 11Mbps → 54Mbps
- 3 channels
- Worldwide compatibility
- Compatibility with installed base of 802.11b products
- Easy upgrade path to high-speed 802.11g
- Wide selection of client devices
- Lower cost products
- Lower power requirements (important for handhelds)

# Agenda


- Introduction
- ***Mobility***
  - Dynamic Coverage
  - L2/L3 Roaming
  - Wireless Mobility
- WLAN Security
- Quality of Service
- Closing Remarks/Q&A

# Dynamic/Complete Coverage

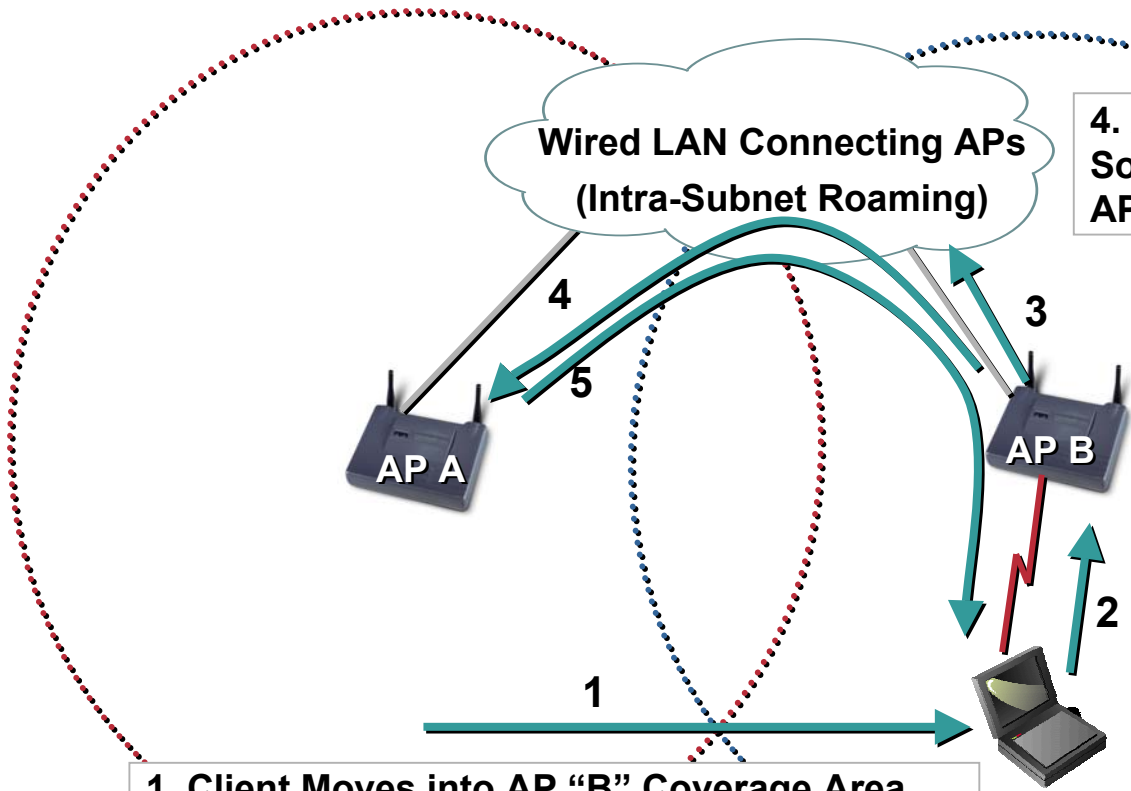


## Dynamic Coverage = Complete Coverage

- Site surveys can be expensive and are a snapshot in time
- The WLAN needs to be able to detect RF environment changes and automatically adjust power, frequency, and bit rate

# Seamless Layer 2 Roaming






4. AP B Sends MAC Multicast Using Source Address of AP B; AP A Drops Client from Association Table

3. AP B Sends MAC Multicast Using Source Address of the Client; This Updates the CAM Tables in Upstream Switches and Directs Further LAN Traffic for the Client to AP B, and Not AP A

2. Client Re-Authenticates and Re-Associates with AP "B"

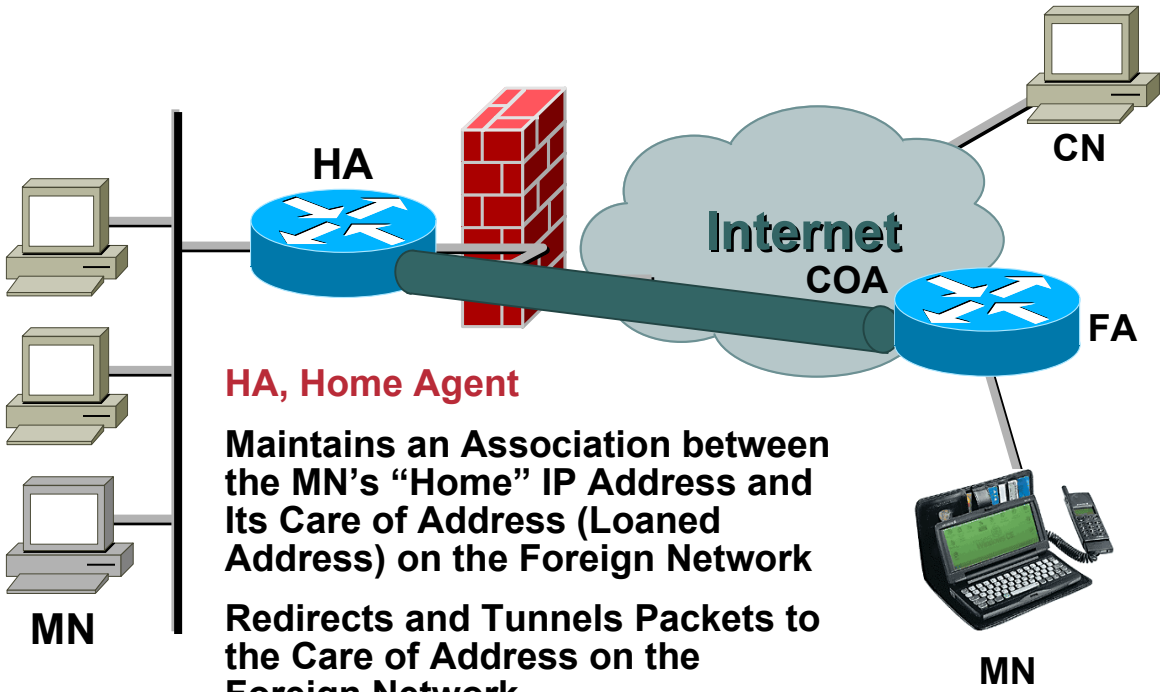
1. Client Moves into AP "B" Coverage Area from AP "A" (Both APs in Same Subnet); Moving from AP A's Coverage Area Will Trigger a "Roaming Event" (e.g. Max Retries Met); the Client Will then Initiate Normal Scanning Process for Available APs

Scanning for APs:
To Associate with AP B (Satisfy One or More Criteria)

- Signal strength 20% better?
- Fewer hops to backbone?
- Assoc(AP B) + 4 < Assoc(AP A)?

# Mobile IP Terminology






**CN, Correspondent Node**

Destination IP Host in Session with a Mobile Node

**HA, Home Agent**

Maintains an Association between the MN's "Home" IP Address and Its Care of Address (Loaned Address) on the Foreign Network

Redirects and Tunnels Packets to the Care of Address on the Foreign Network

**FA, Foreign Agent**

Provides an Addressable Point of Attachment to the MN Called Care of Address (COA)

Maintains an Awareness for All Visiting MNs

Acts as a "Relay" between the MN and Its Home Agent

Receives All Packets for the MN from the MN's Home Agent

**MN, Mobile Node**

An IP Host that Maintains Network Connectivity Using Its "Home" IP Address, Regardless of which Subnet (or Network) It Is Connected to

# Roaming Layer 3



- Without mobile IP, roaming is achieved by extending the Layer 2 network
- Cisco has supported mobile IP for a number of years
- Mobile IP has been waiting on mainstream clients; these are now available
- The easiest first step is the use of collocated CAs, and a central HA (no FA needed)

# Additional WLAN Mobility Issues



- L2 roaming latency
- L3 subnet roaming
- Mobile IP, Proxy Mobile IP, IAPP – which one is best?
- Power saving modes affect multicast (buffering)
- New roaming and power saving technologies being developed (Cisco Fast Secure Roaming)

# Agenda


- Introduction
- Mobility
- ***WLAN Security***
- Quality of Service
- Closing Remarks/Q&A

# Standard Wireless LAN Security

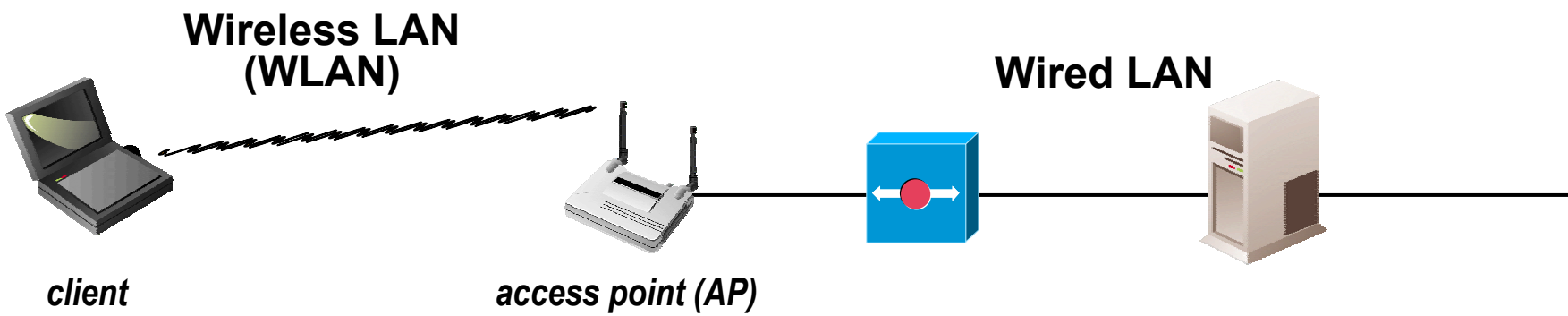


## Issue

- Wireless sniffer can view all WLAN data packets
- Anyone in AP coverage area can get on WLAN

## Solution

- Encrypt all data transmitted between client and AP
- Without encryption key, user cannot transmit or receive data




**Goal: Make WLAN security equivalent to that of wired LANs (Wired Equivalent Privacy)**

# WEP Encryption



- Wired Equivalent Privacy
- Based on the RC4 symmetric stream cipher
- Requires matching static, pre-shared, 64-bit or 128-bit keys on both the client and access point
- 24-bit Initialization Vector (IV) plus 40- or 104-bit secret key yields 64- or 128-bit data encryption

# Limitations of 802.11 Security



- Shared, static WEP keys
  - No centralized key management
  - Poor protection from variety of security attacks*
- No effective way to deal with lost or stolen adapter
  - Possessor has access to WLAN and any network resource for which no network logon is required
  - Re-keying of all WLAN devices is required
- Lack of integrated user administration
  - Need for separate user databases; no use of RADIUS
  - Potential to identify user by MAC address, not username
  - No usage accounting and auditing; no means to detect unusual activity

* "In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe…"

University of California-Berkeley report on WEP security:
www.isaac.cs.berkeley.edu/isaac/wep-faq.html

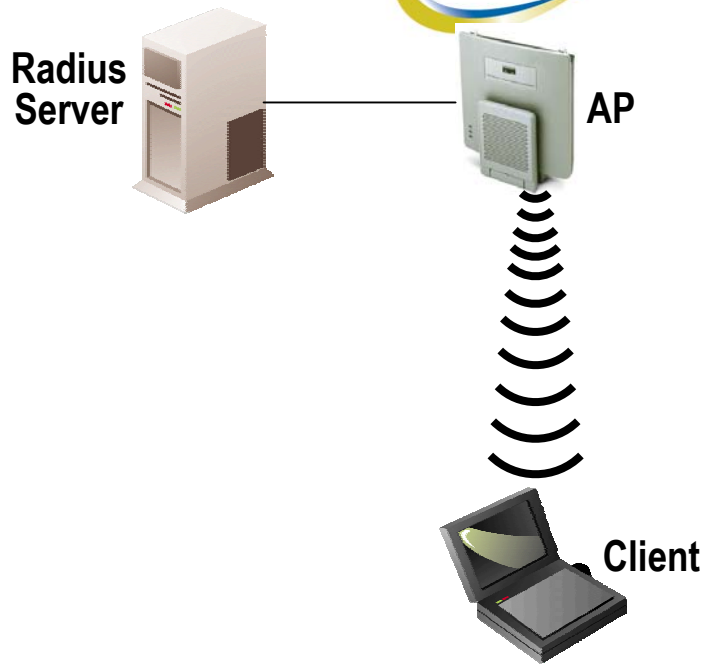
# Key Initiatives


- Continue to enhance enterprise-class WLAN security solutions to extend leadership
- Drive standards efforts
- Develop greater wired/wireless integration since WLANs are an extension of the wired network
- Create partnerships to provide customer solutions for different markets
- Share technology to extend the value of Cisco's advanced features to a variety of client devices

# WLAN Security: 802.1X Authentication



- **LEAP – Cisco Lightweight EAP**
  - Nearly all major OS's supported:
    - WinXP/2K/NT/ME/98/95/CE/CE .NET, Linux, Mac, and DOS
    - CCX program being rolled out now
- **EAP-TLS (Transport Layer Security)**
  - EAP-Transport Layer Security
  - Mutual Authentication implementation
- **EAP-TTLS (Tunneled TLS)**
  - Hybrid—Certificate/password
- **PEAP (Protected EAP)**
  - Establishes secure tunnel (similar to VPN)
  - Co-developed by Cisco, Microsoft, & RSA Security
  - Option: One-Time Passwords ("OTP")

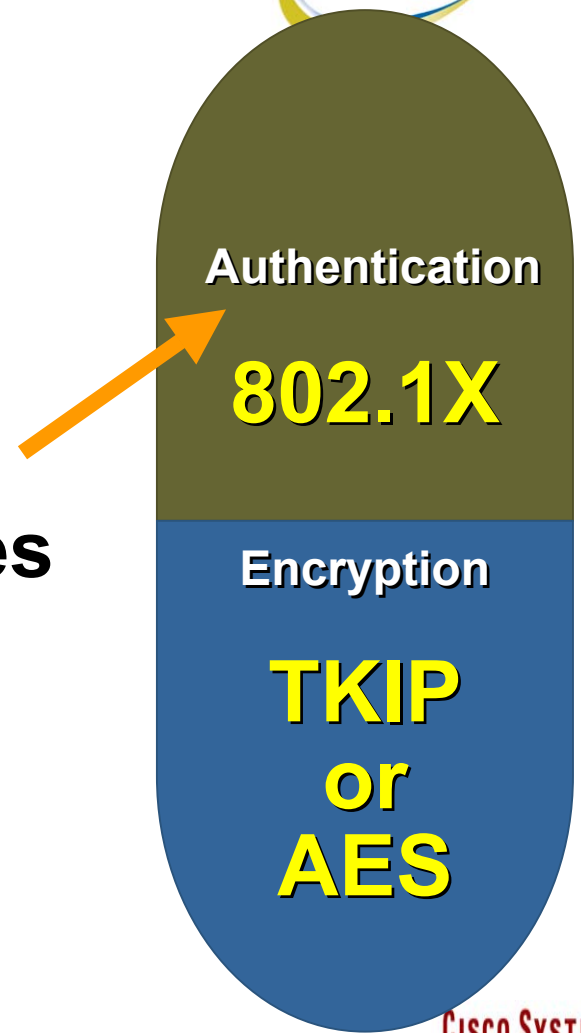



Cisco Systems RSA Security Microsoft

# WLAN Security: 802.1x Authentication

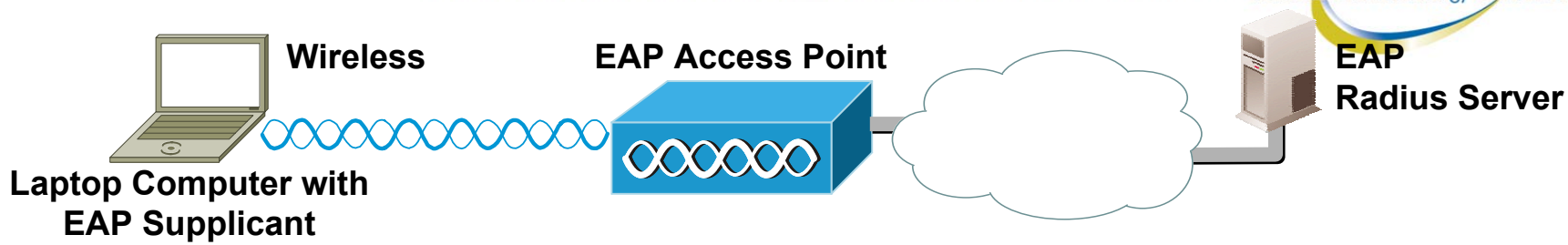


- Centralized, scalable, user-based authentication
- Mutual authentication
- Various authentication types
- Dynamic WEP key support
- WEP key refresh



# 802.1x/EAP Architecture






**EAP Types:**
- LEAP
- EAP-TLS
- EAP-MD5
- EAP-PEAP
- EAP-TTLS
- Etc.

**Driver for Operating System**
- Support for at least one of the EAP protocols
- Dynamic WEP key support
- Capable of speaking EAP

**Client/Supplicant**

**EAP Authenticator**
- EAP-LEAP
- EAP-TLS and EAP-MD5
- EAP-SIM
- EAP-PEAP and EAP-TTLS

**Authenticator**

**EAP Radius Server**
- Cisco secure ACS, Cisco access register, Funk, Interlink, etc.
- Internal authentication database
- Capability to interoperate with external user Databases (Windows NT/2000 AD, LDAP, etc.)

**EAP Radius DLL**
- Support of mixed EAP protocols deployment
- MS-MPPE-Send-key support
- EAP extensions for Radius

**Backend/RADIUS Server**

# 802.1X for 802.11 – Benefits



- **Scalable, standards-based, Can be used in wired networks as well**
- **Supports a variety of authentication types**
  - **EAP-Cisco Wireless, or LEAP**
  - **EAP-TLS with Windows XP and other Windows versions**
  - **Others, as they are developed**
- **Enables centralized policy control**
  - **Session timeout triggers reauthentication and new WEP key**
- **802.1x in campus prevents *Rogue APs***
  - **Cisco RF monitoring solutions will detect and graphically locate rogue APs**

# Broadening Support for LEAP



**Cisco has licensed LEAP to many companies:**

- **LEAP support: RADIUS servers**
  - **Funk Software:** Steel-Belted Radius Server
  - **Interlink:** Secure.XS Radius Server
- **LEAP support: Client Devices**
  - **Apple:** Powerbooks/iBooks
  - **HP:** Print Servers
  - **Symbol:** Handhelds
  - **Intermec:** Handhelds
- **LEAP support: Client Software**
  - **Funk Software:** Odyssey Client v.1.1
  - **Meetinghouse:** Aegis Client v.1.3.6
- **LEAP support: Chipsets**

| | |
|---|---|
| Intel | TI |
| Intersil | Marvell |
| Atheros | Agere |
| Atmel | Broadcom |

# What is PEAP?



- 802.1X- based authentication protocol
- Based on EAP
- Leverages server-side EAP-TLS using digital certificates
- Supports a variety of different client authentication methods, including log-on passwords and one-time passwords (OTPs)
- Based on a RFC Draft jointly submitted by Cisco Systems, Microsoft and RSA Security to the IETF
- Initial support on Windows XP, now available on Window 2000 SP3

# PEAP Implementation



- PEAP Authentication Mechanisms:
  - One Time Password Server
  - Clear-text password support for LDAP and NDS user databases
  - Support for Password Change (Microsoft)
- Cisco Secure ACS v. 3.1:
  - Database support (including LDAP and NDS)
  - Triggering password change, etc. through tunnel
- Windows XP client software implementation:
  - New supplicant for PEAP
  - User interfaces
  - Updated Aironet Client Utility (v. 5.05.001)

# PEAP Authentication Process



- Two Phase Authentication:
  - Phase 1: Server side TLS authentication is performed to create an encrypted tunnel (similar to SSL)
  - Phase 2: Methods such as Generic Token Card (GTC) are used to authenticate the Client to the Server
- PEAP requires Server-side certificate only (whereas EAP-TLS requires both Server and Client side certificates)

# PEAP Authentication Overview



Supplicant

AP

Enterprise Network

RADIUS Server

EAPOL Start

Start EAP Authentication

EAP—Request/Identity

Ask Client for Identity

EAP—Response/Identity (NAI)

RADIUS Access Request

Access Request with NAI

Server-Side TLS

Client-Side Authentication

Perform Sequence Defined by PEAP

Key

RADIUS Access Success (Pass Session Key to AP)

Key

EAP Success

Client Derives Session Key

EAPOL—Key (Multicast)

EAPOL—Key (Session Parameters)

Deliver Broadcast Key Encrypted with Session Key and Session Parameters

# 802.1X EAP Authentication Comparison



| | LEAP | PEAP | EAP-TLS |
|---|---|---|---|
| Multi-Operating System Support | Yes | No | No |
| Single Sign On For Windows Log-In | Yes | No | Yes |
| Dynamic WEP Key and Mutual Authentication | Yes | Yes | Yes |
| Static Password Support | Yes | Yes | No |
| One Time Password Support | No | Yes | No |
| Server Certificate Required | No | Yes | Yes |
| Client Certificate Required | No | No | Yes |
| Layer 3 Roaming Support | Yes | Yes | Yes |
| MS Windows Password Change | No | Yes | No |
| Microsoft Backend DB Support | Yes | Yes | Yes |
| LDAP/NDS Backend DB Support | No | Yes | Yes |

# Wi-Fi Protected Access (WPA)




- **WPA is the biggest thing to happen to WLAN security since Cisco LEAP**
- **Cisco has supported the base technologies of WPA longer than any other vendor**
- **WPA is being incorporated into Wi-Fi testing by WECA**
  - **Mandatory WPA certification started August, 2003**
  - **Products from ten companies including Cisco's AP1200 and AP1100 have been certified**

# Components of WPA

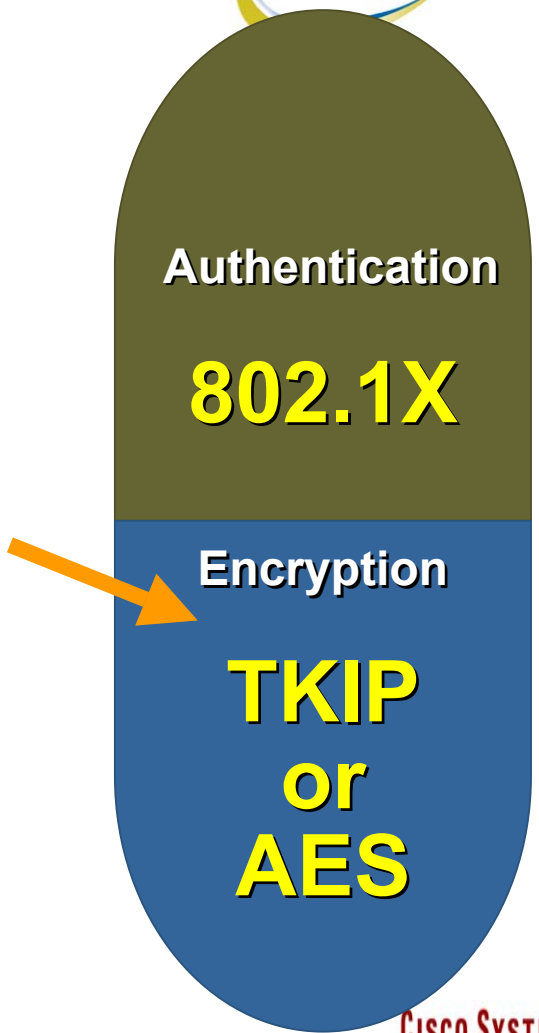



- **Authenticated Key Management using 802.1X:**
  - **EAP Authentication and Pre-Shared Key (PSK) Authentication**
- **Unicast and Broadcast Key Management**
- **TKIP: Per-packet Keying and Message Integrity Check (MIC)**
- **IV-space expansion: 48 bit IVs**
- **Migration Mode – coexistence of WPA and non-WPA devices**

# WLAN Security—Encryption

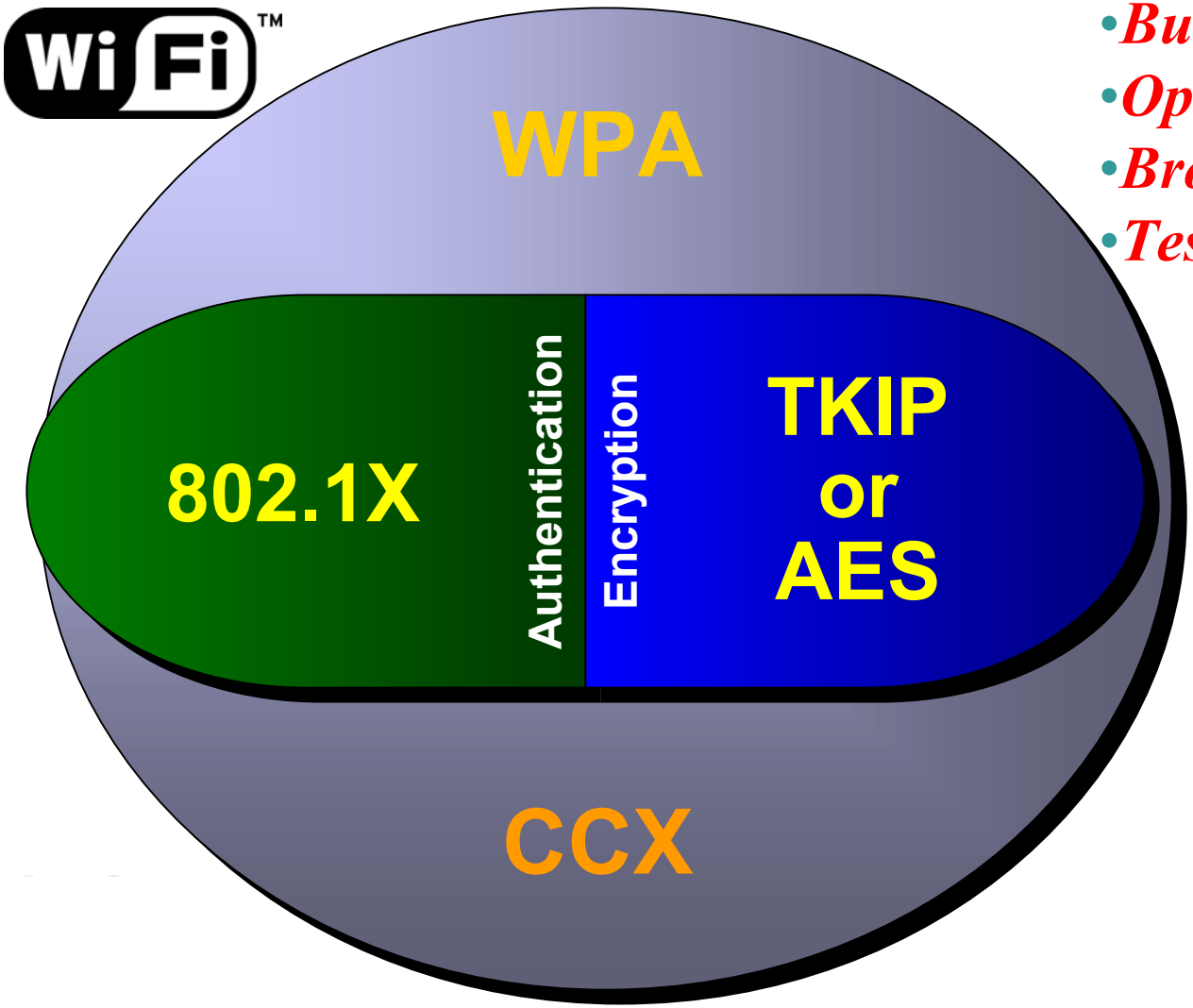


- **TKIP**
  - Temporal Key Integrity Protocol
  - Dec. ’01: Cisco’s pre-standard TKIP
  - Aug. ’03: 802.11i-standard TKIP (part of WPA)
- **AES**
  - Advanced Encryption Standard
  - “The Gold Standard”
  - Optional part of 802.11i spec
  - Hardware encryption vs. software encryption



# Enterprise-Class WLAN Security: The Cisco Wireless Security Suite

HP WORLD 2003




- *Built on Standards*
- *Optimized for Enterprise*
- *Broad Adoption*
- *Tested for Interoperability*

**WPA**
Wi-Fi Protected Access

**TKIP**
Temporal Key Integrity Protocol

**AES**
Advanced Encryption Standard

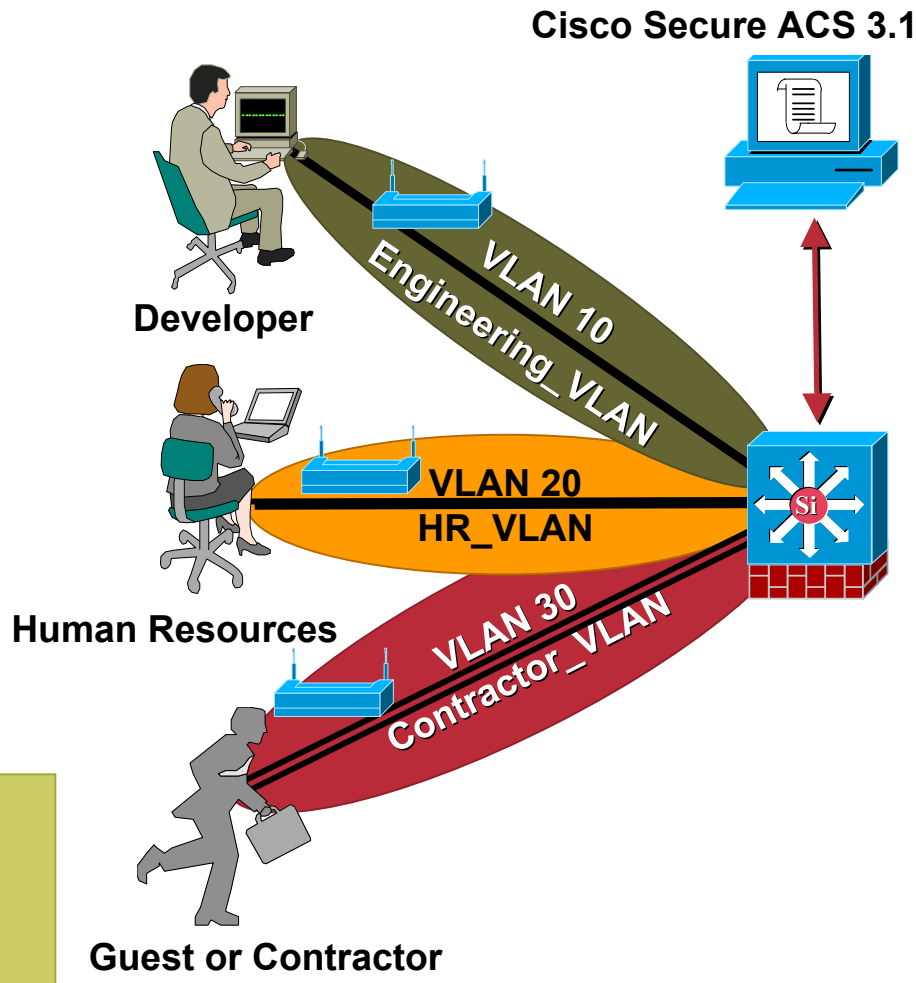
**CCX**
Cisco Compatible eXtensions

Cisco Systems

# Campus WLAN Mobility
## User-Based Network Access



- Based upon user's credentials via 802.1x (User Identity)
- Unauthorized users or those without 802.1x running on their laptop can be denied or placed into a Guest VLAN



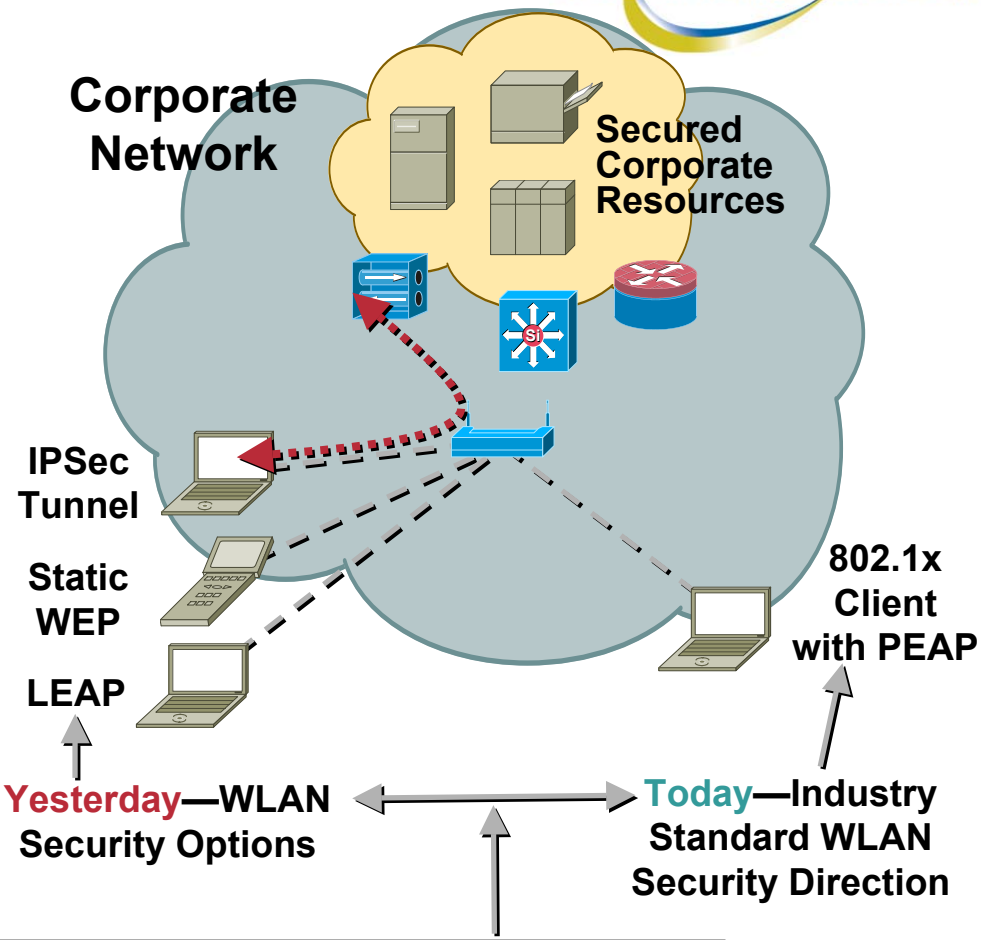

**Authentication-Based Resource Access**

1. Eng Can Only Access Eng Resources
2. HR Only Can Access HR Servers
3. Guest Access for Trusted 3rd Party Contractors

# Campus WLAN Mobility
## Secure WLAN Access

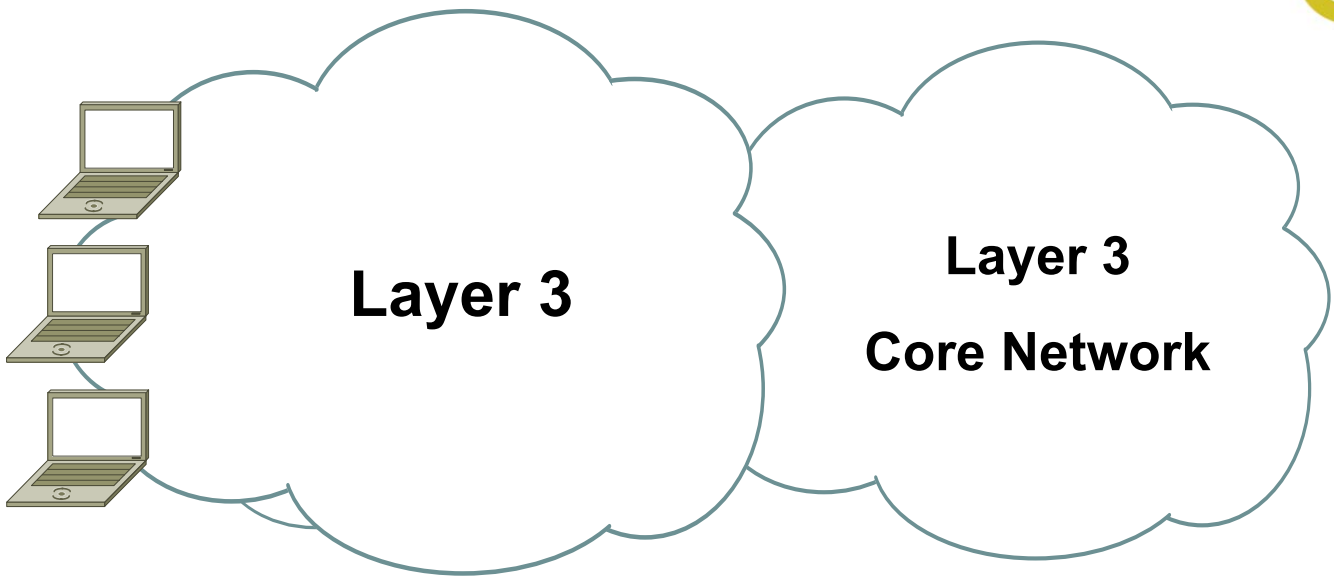


- Several secure deployment options—LEAP, IPSec VPN with Auto Initiation, and dynamic WEP
- 802.1x with PEAP provides industry standard future direction for WLAN security
- VLAN support in AP's provide co-existence and migration from current installed-based security models



# 802.1x/EAP vs. IPSec

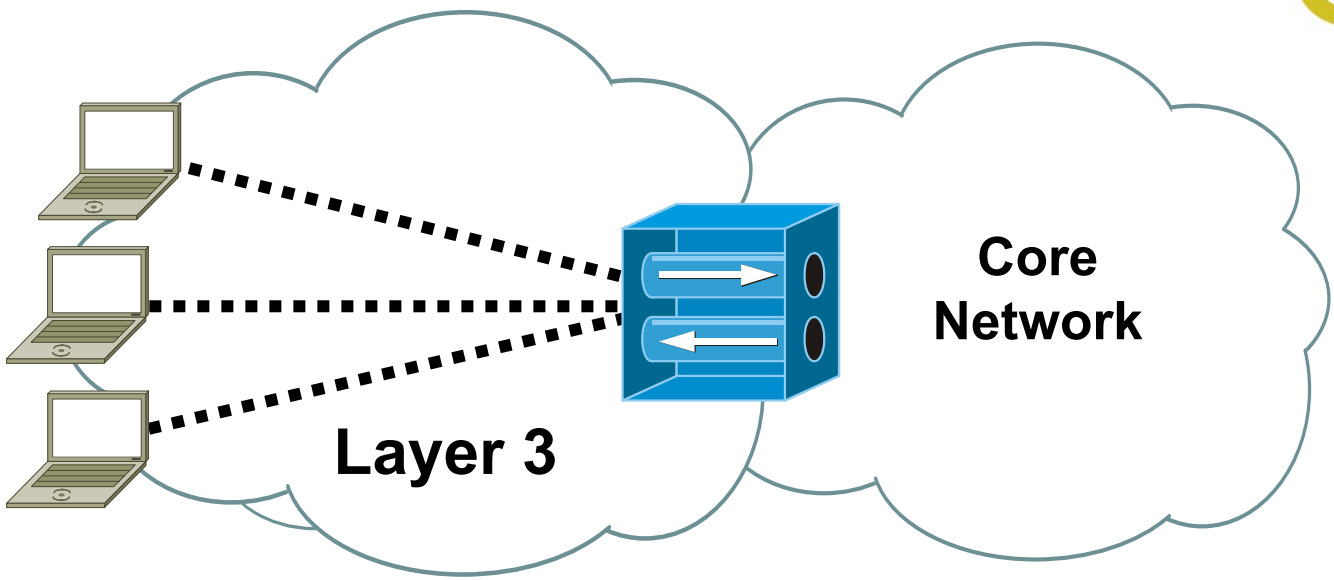





- **802.1x/EAP is architecturally superior**
  - **It is a MAC-layer connection**
  - **Provides LAN functionality**

# 802.1x/EAP vs. IPSec






- **Client VPN is a gateway**
  - **IP only**
  - **Not transparent to IP**
  - **Point to point**

# VPN Security for WLANs



**Remote Access**

**Dialing into Corporate Network from Home, Hotel, Airport, etc.**

**VPN is the Best Solution!**

**On-Campus Access**

**Accessing Corporate Network while inside the Enterprise**

**VPN may not be the Best Answer**

## VPN/WLAN On Campus – Pros

- **Familiar**
  - Is in use at most enterprises
  - Makes user interface consistent for both WLAN & remote access
- **Trusted for authentication & privacy**
  - Supports central security management
  - Ensures 3DES encryption from client to concentrator
- **Compatible with wide range of client devices from multiple vendors**

## VPN/WLAN On Campus – Cons

- **Cost:** Requires VPN concentrators behind APs
- **Performance:** Client software encryption lowers throughput
- **Roaming:** Roaming between VPN concentrators forces application restarts
- **QoS:** All traffic is IPSec traffic; no QoS, multicast, or multiprotocol support
- **Client Devices:** Not supported on phones, scanners, or other specialized devices
- **Convenience:** Additional steps required beyond Windows logon

# Agenda


- Introduction
- Mobility
- WLAN Security
- ***Quality of Service***
- Closing Remarks/Q&A

# 802.11 QoS



- **Quality of Service contends with**
  - **Packet loss**
  - **Delay or latency**
  - **Delay Variance (“jitter”)**
- **Two key issues**
  - **Prioritization**
  - **Service commitment**

# QoS in 802.11e and Wireless Multimedia Extensions (WME)



- To meet service commitments, the AP needs to act as a coordinator
  - Point Coordination Function (PCF) was too restrictive, had scaling issues and required Distributed Coordination Function (DCF), an access contention method using CSMA/CA
  - Enhanced DCF and Hybrid Coordination Function (HCF) are more flexible and are being written into 802.11e and WME to support voice over WLAN

# Agenda


- Introduction
- Mobility
- WLAN Security
- Quality of Service
- *Closing Remarks/*Q&A

# Wireless LAN Direction



- **Ubiquity - Usability + Serviceability**
  - **Integration into devices, and OSs**
  - **Multi-mode radios**
  - **Dynamic coverage**
  - **Transparent roaming**
  - **Transparent mobility**
  - **Transparent security mechanisms**
  - **Management interface for clients**
  - **Transparent QoS**

# Structured Wireless-Aware Network



**"Air"/RF Management**

Rogue AP/Network Detection
Assisted Site Surveys
Performance Optimization

**Secure Mobility**

L2 Mobility
L3 Mobility (Future)

CiscoWorks Mgmt

Cisco IOS Software

Clients

## Management Products

Cisco Secure ACS, CiscoWorks LAN Management Solution and WLSE

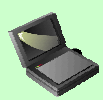
## Multilayer Switching Products

Catalyst 37xx, 4xxx, 65xx

## Wireless APs

AP1200 AP1100

## Cisco & Cisco Compatible Clients



Increase "Air"/RF Measurement effectiveness by 10X to 20X in most cases

# Cisco Compatible Program (CCX) for WLAN Client Cards



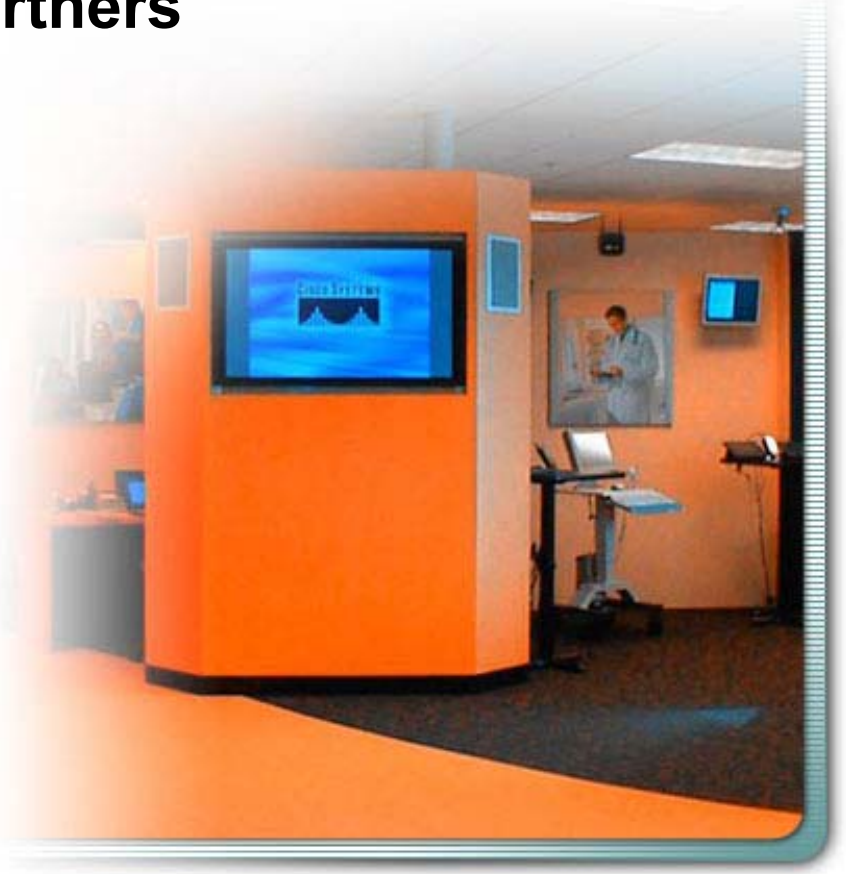
- **No cost licensing of Cisco wireless technology, via Cisco Compatible eXtensions ("CCX") specification for use in non-Cisco wireless client devices**
- **Independent testing to ensure interoperability with Cisco infrastructure**
- **Marketing of these devices by Cisco and the client suppliers under the Cisco Compatible brand**

Cisco® Compatible

# Wireless Integrated Network Solutions (WINS) Lab

HP WORLD 2003
Solutions and Technology Conference & Expo

- Cisco WINS Lab in San Jose
- Showcase for WLAN products and solutions from Cisco and partners
- Exhibits for:
  - Enterprise
  - Healthcare
  - Education
  - Retail/supply chain mgmt.
  - Transportation
  - Bridging
  - Network management
  - Site survey tools



# White Papers and Training

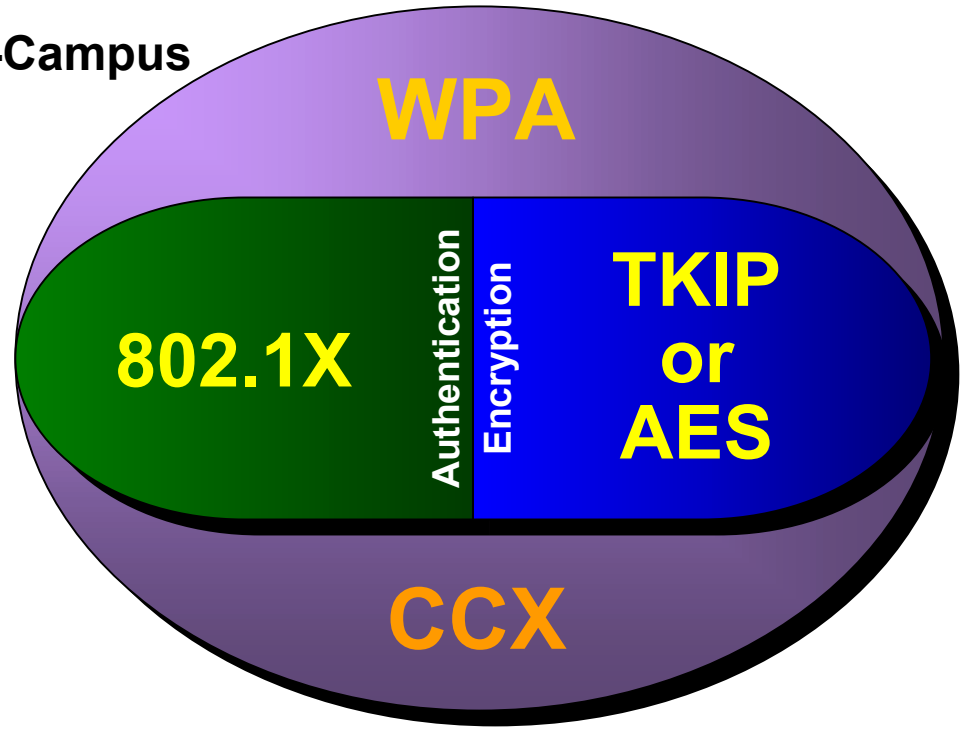


- **Check these sites for excellent technical references:**
  - www.cisco.com/go/safe
  - www.cisco.com/go/aironet
  - www.cisco.com/en/US/products/hw/wireless/ps430/prod_white_papers_list.html
- **Cisco Qualified Specializations (CQS) for Wireless Design and Support**
  - www.cisco.com/go/certifications

# Summary:
# Cisco Wireless Security Suite

HP WORLD 2003
Solutions and Technology Conference & Expo

**On-Campus**




*Strong Security*

*Low Cost*

*Interoperability*

*Mobility*

*Scalability*

**Remote Access**

**VPN is the Best Solution for Remote Access!**

Cisco Systems


HP WORLD 2003
Solutions and Technology Conference & Expo

# Thank You

## Q&A


CISCO SYSTEMS