



Wireless in Manufacturing

Tatjana Boskovic, Channel SE

tboskovi@cisco.com

Manufacturing event, 20/03/2009

Agenda

- Introduction
- Cisco Unified Wireless Network Fundamentals
- Wireless for Manufacturing
 - H-REAP
 - VoWLAN
 - Context-aware mobile services
- Q&A

Expansion of Mobile Clients and Services

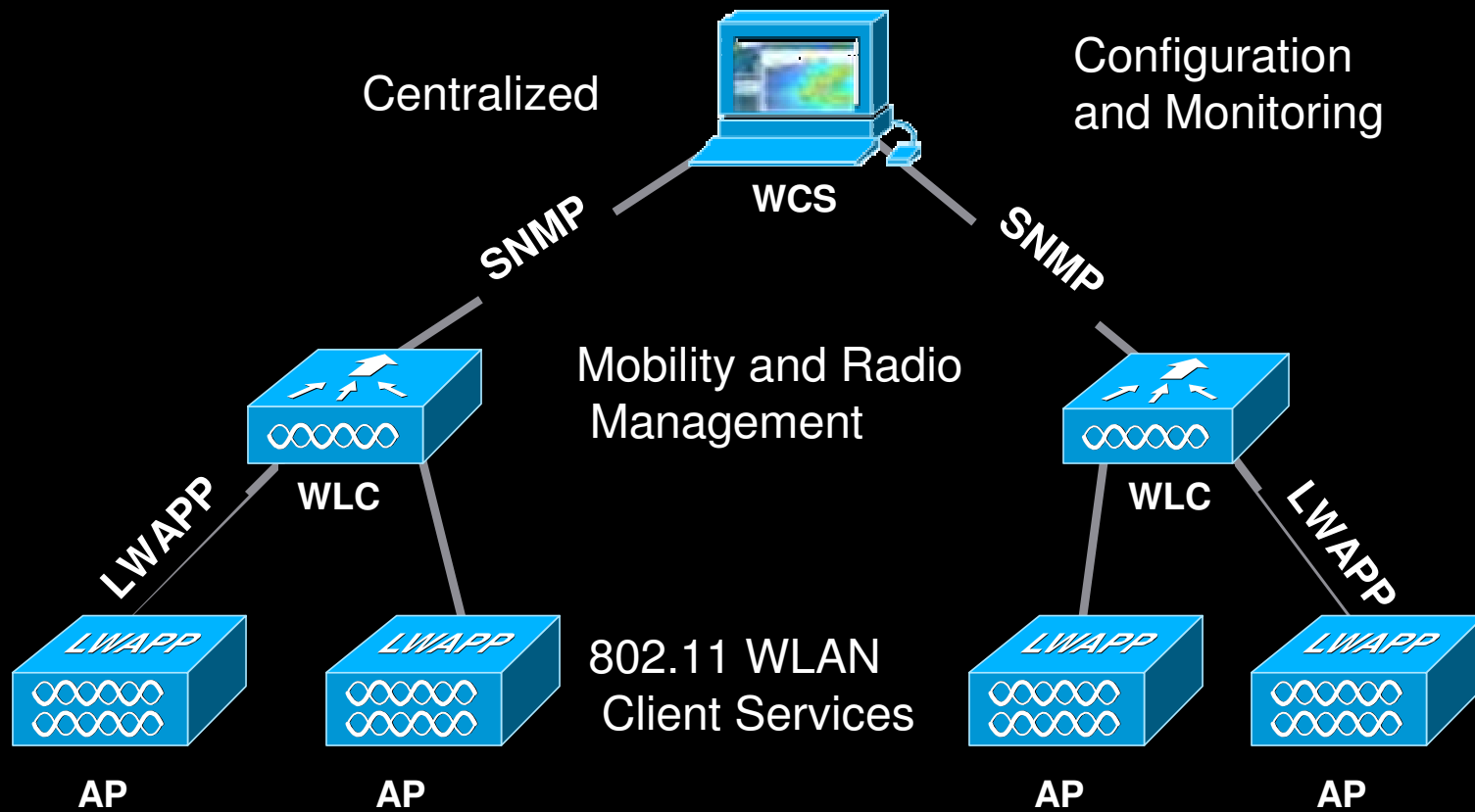


WLAN needs to be ready for new applications

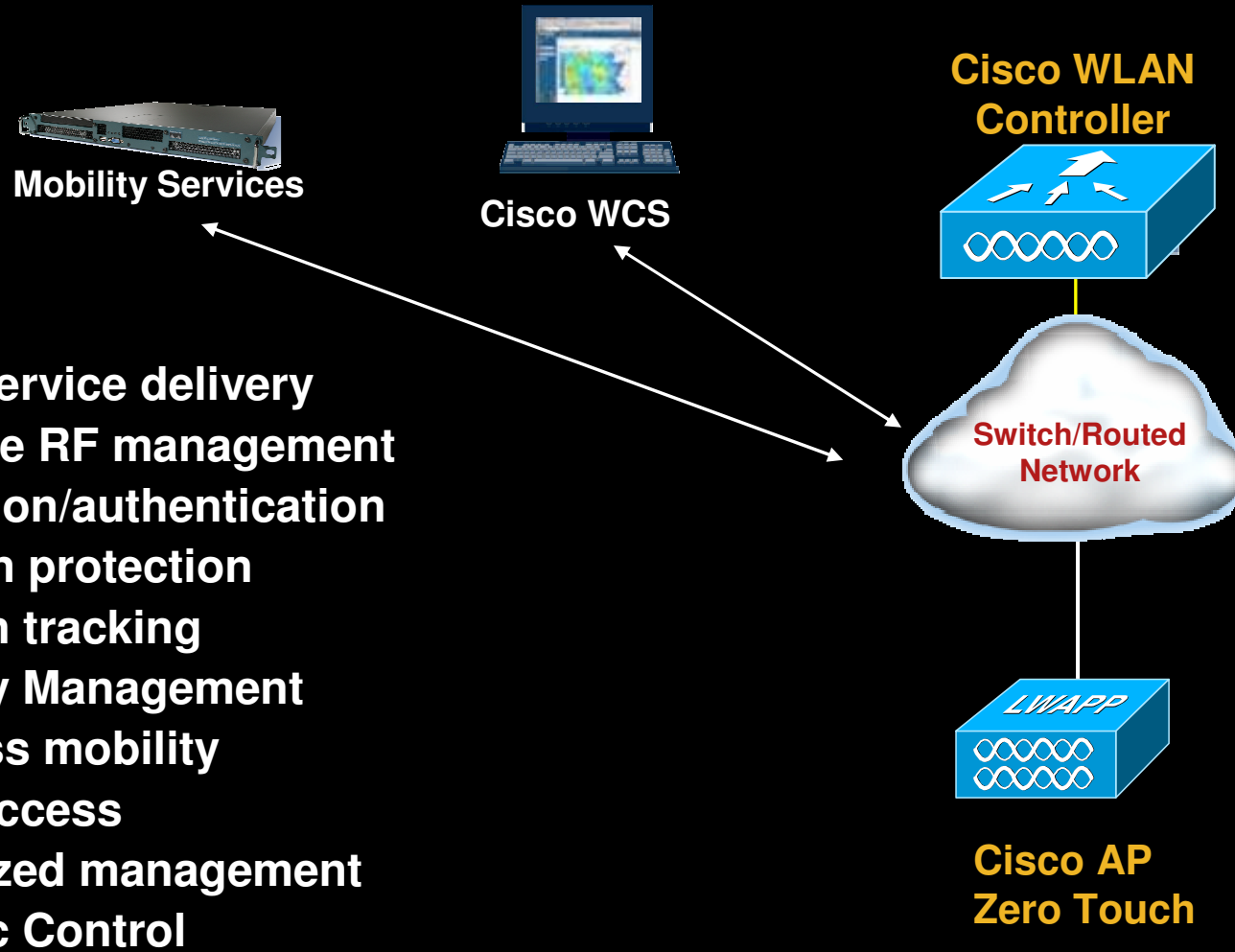
CUWN Fundamentals



CUWN Components and Hierarchy



Unification of Applications

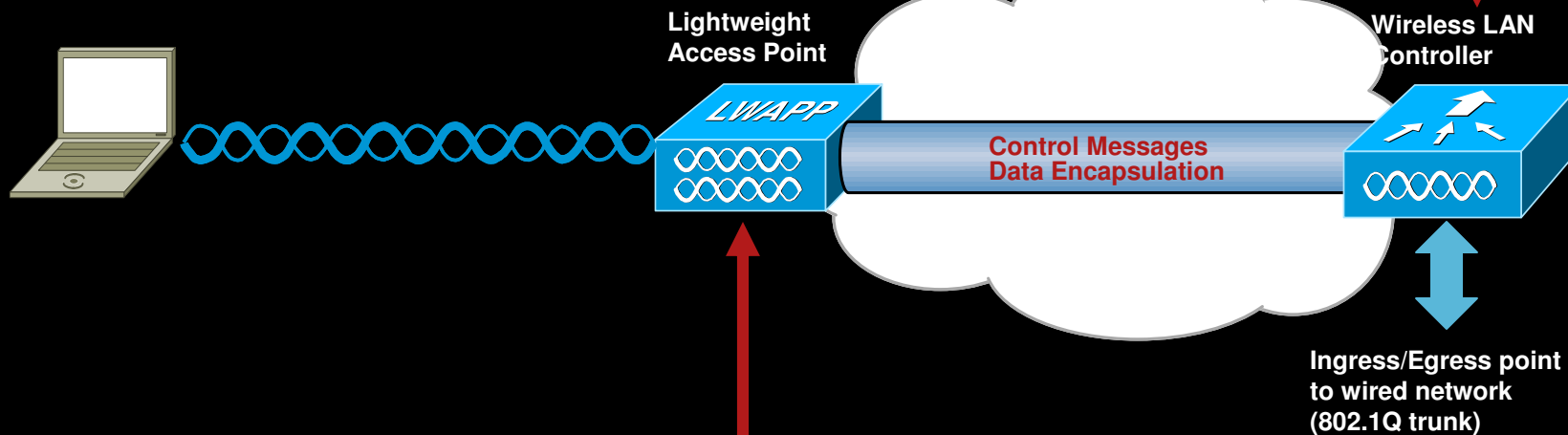


Cisco:

- WLAN service delivery
- Real-time RF management
- Encryption/authentication
- Intrusion protection
- Location tracking
- Capacity Management
- Seamless mobility
- Guest Access
- Centralized management
- Dynamic Control

AP/Controller Division of Labor

Mutual Authentication (X.509 Certificate)
LWAPP Control is AES Encrypted
LWAPP Data is Encapsulated



Real-time 802.11/MAC functionality
Remote RF interface
Data Encryption/Decryption
WLAN IDS Signature analysis

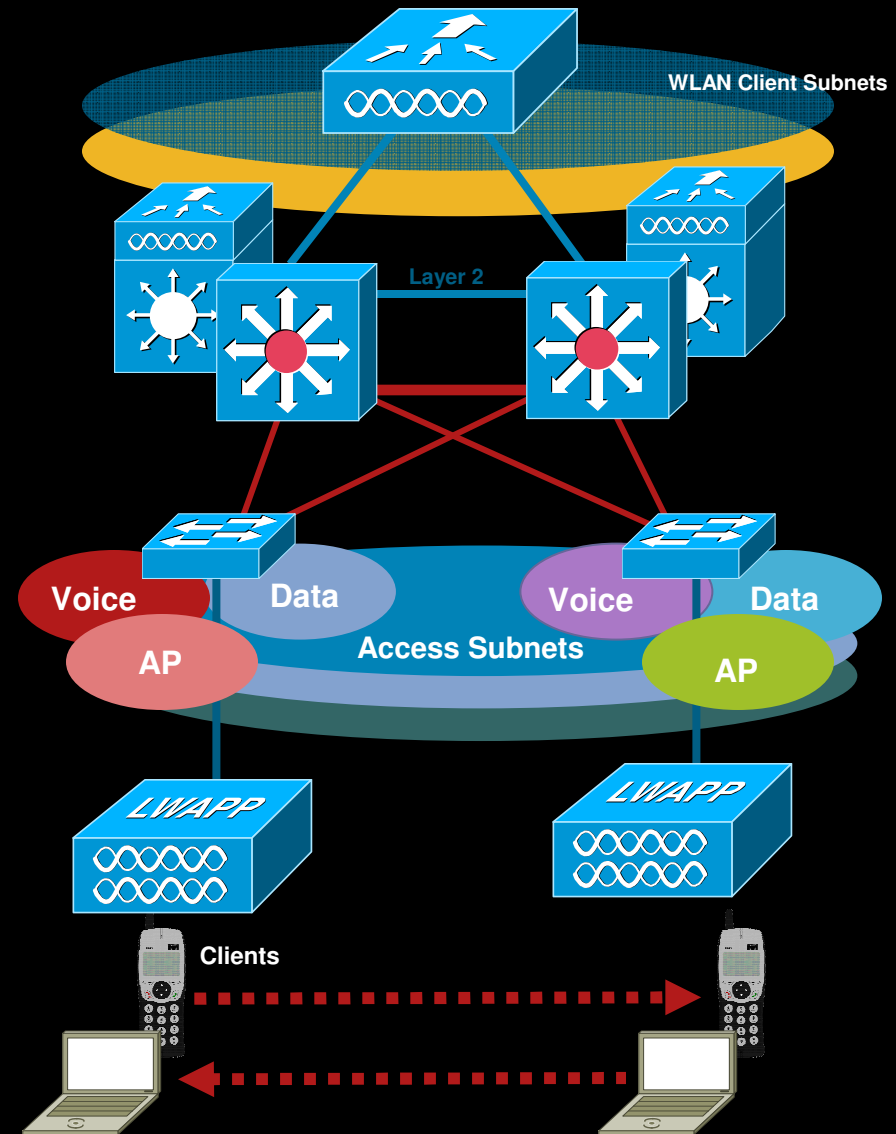
Non real-time 802.11/MAC functionality
Security management
QoS policies enforcement
Firmware management
Northbound management interfaces

Where to Place a WLAN Controller?

Distributed Designs

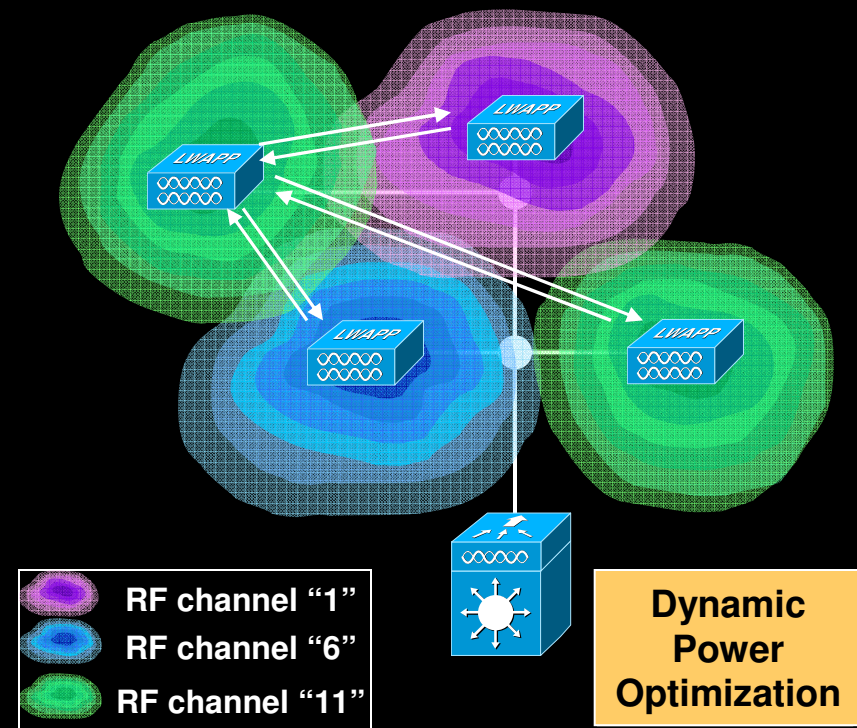
- WiSM(s) or 440x WLAN controller(s) connected at distribution layer
- Controller redundancy
- Key design considerations:
 - Spanning tree
 - HSRP/GLBP
 - Traffic flow
 - Load balancing
 - Resiliency
 - Access layer “collapsed” into distribution layer
 - Access layer IP addressing
 - Access layer features need to be implemented in the distribution layer

–Mobility!

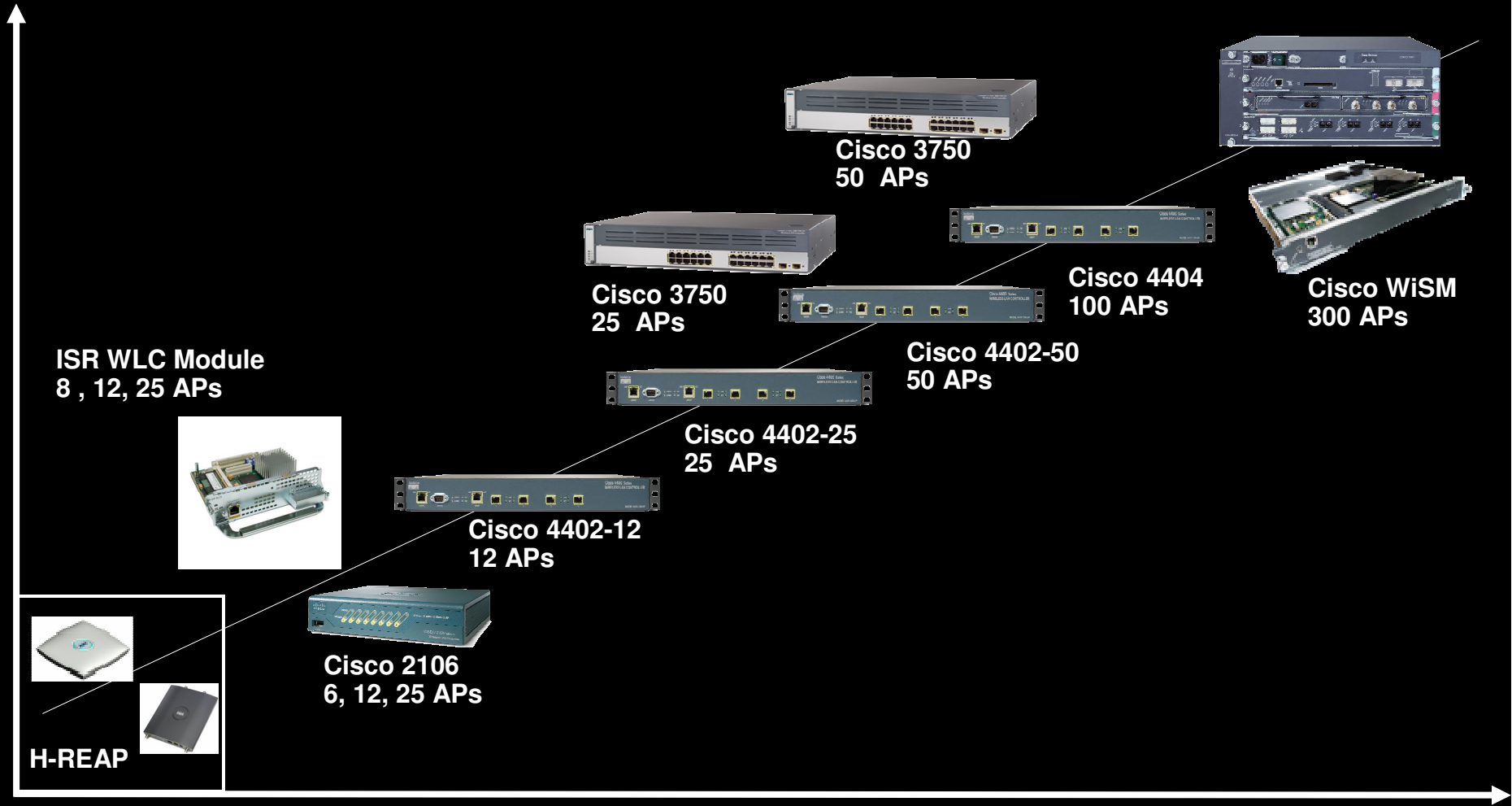


RRM – Radio Resource Management

- The RF domain is an ever changing environment
- The controller has a system level view
- Transmit Power Control
- Dynamic Channel Assignment
- Coverage Hole







Cisco Wireless Controller Family



Deployment Size

Cisco Access Points

	AP 1130 	AP 1240 	AP 1250 	AP 1520 
Modular Platform	No	No	Yes	Yes
Data Uplink (Mbps)	10/100	10/100	10/100/1000	10/100/1000
Power Requirement	802.3af	802.3af	802.3af* 802.3at	AC/12VDC
Installation	Standard	Rugged	Rugged	Outdoor
Antennas	Internal	External	External	External
Wi-Fi 802.11n draft 2.0 Certified	No	No	Yes	No

The Aironet 1140 Series Access Point

- Integrated Radios
 - 2.4 GHz (b/g/n)
 - 5 GHz (a/n)
- 10/100/1000 Ethernet Port
- Console port
- Security lock
- Plastic over metal design
- Powered via 802.3af PoE
- Retrofit Mounting Kit allows the AP1140 to slide into existing AP1130 mounting brackets (ordered separately)



1140 vs 1250 Positioning



1140



1250



Deployment	Indoor	Ruggedized
Antennas	Integrated	External (RP-TNC)
Wired Uplink	Gigabit	Gigabit
Power Options	PoE, AC, Pwr Inj	PoE*, ePoE, AC, Pwr Inj

* 1250 runs on PoE with reduced performance

Cisco Wireless Control System (WCS)



World-Class Network Management

Features

- Client troubleshooting (via CCX)
- Planning, configuration, monitoring, location, IDS/IPS, and troubleshooting
- Hierarchical maps
- Intuitive GUI and templates
- Policy based networking (QoS, security, RRM, etc.)

Benefits

- Lower OPEX and CAPEX
- Better visibility and control of the air space
- Consolidate functionality into a single management system
- Determines location and voice readiness

System Monitoring – Network Summary



Wireless Control System

User: root | Virtual Domain: root
[Refresh](#) | [Print View](#) | [Logout](#)

Quick Search

Search Controllers

Saved Searches

--Select Search--

WCS Home
Customize
[Edit Tabs](#) [Edit Contents](#)

General
Client
Security
Mesh

Inventory Detail Status

Controllers: 4 Radios: 34 Location Servers: 0




Client Count

6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y | Custom



Coverage Areas

Name	Total APs	a/n Radios	b/g/n Radios	OOS Radios	Clients
BLDG14	0	0	0	0	0

[View All Maps](#)

Total APs not yet assigned to Maps : 17

LWAPP Uptime

AP Name	LWAPP Uptime
Cisco1242	38 d 22 h 9 m 27 s
AP0019.2fa6.beb0	38 d 22 h 9 m 24 s
Ciscolln	31 d 2 h 58 m 32 s
AP001d.4591.25e8	24 d 20 h 59 m 46 s
AP0019.3076.3272	23 d 5 h 34 m 3 s

Recent Coverage Holes (0)

No Coverage Holes found

Controller Memory Utilization (%)

6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y | Custom



Min Max Avg

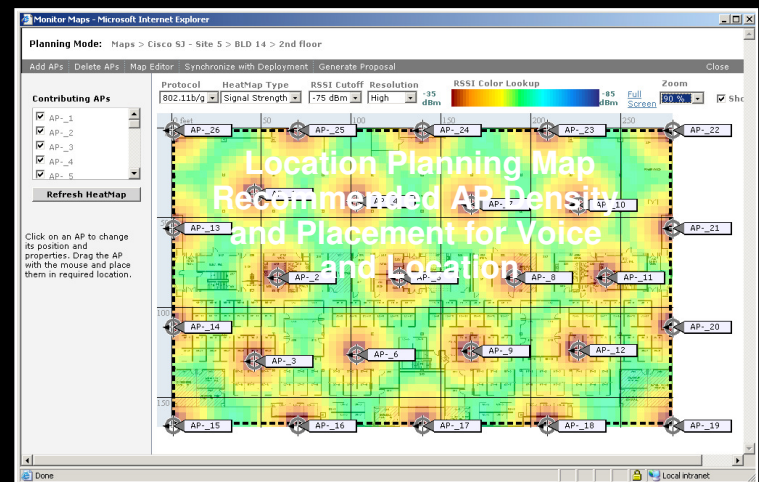
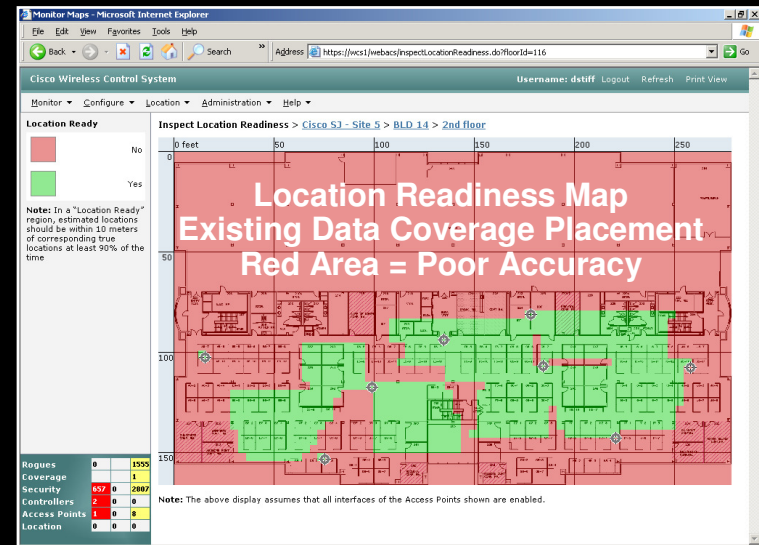
Alarm Summary

Malicious AP	0	0	0
Coverage Hole	0	0	0
Security	4	0	7
Controllers	10	2	0
Access Points	31	0	10
Location	0	0	0
Mesh Links	0	0	0

WCS Location Service Planning



- **Location readiness**
Assess location accuracy for existing deployments
- **Location planning mode**
Suggests AP density and placement based on data, voice, or location services
- **Location inspector**
Post deployment and calibration tool for location quality verification
- **Accuracy improvements**
Smoothing, additional antennas, faster calibration, enhanced algorithms—minimum variance estimation



Integrated Wireless Intrusion Protection

- Detect common RF-related attacks
 - Netstumbler, wellenreiter, void11, FakeAP, address spoofing, DoS, etc.
- Customizable attack signatures
- Real-time 24x7 monitoring and alarming
- Rogue AP/client detection, location, and containment
 - Identify known (i.e. “trusted”) rogues
- Manually disable clients
- View dynamically excluded clients
- Rogue AP switchport tracing

Cisco Wireless Control System

Monitor | Configure | Location | Administration | Help

Security

Security Summary

Rogue AP Details			Signature Attacks			AP Threats/Attacks					
	Last 24 Hours	Total Active		Last 24 Hours	Total Active		Last 24 Hours	Total Active			
Alert	174	2089	1612	Disassoc flood	2	34	1	Fake AP Attack	1	7	15
Contained	0	0	0	Assoc flood	0	0	0	AP Missing	0	0	0
Threat	0	1	0	Beast death	0	0	0	AP Impersonation	0	0	0
Contained Pending	0	0	0	Broadcast Probe floo	0	0	0	AP Invalid SSID	0	0	0
Known Contained	0	0	0	Death flood	1	7	0	AP Invalid Preamble	0	0	0
Trusted Missing	0	0	0	Custom	0	0	0	AP Invalid Encryption	0	0	0
802.11a	76	562	503	EAPOL flood	0	16	0	AP Invalid Radio Policy	0	0	0
802.11b/g	126	942	597	NULL probe resp 1	0	0	0	Denial of Service (NAV related)	0	0	0
On Network	0	5	1	NULL probe resp 2	0	0	0				
Off Network	202	2229	1611	NetStumbler 3.2.0	0	0	0	Client Security Related	Last 24 Hours	Total Active	
Adhoc	0	0	0	NetStumbler 3.2.3	0	0	0	Excluded Client Events	0	1	203
				NetStumbler 3.3.0	0	0	0	WEP Decrypt Errors	0	60	526
				NetStumbler generic	0	0	0	WPA MIC Errors	0	2	112
				Reassoc flood	0	4	0	Shunned Clients	0	2	112
				Res mgmt 6 & 7	0	0	0	IPSEC Failures	0	0	0
				Res mgmt D	0	0	0				
				Res mgmt E & F	0	0	0				
				Wellenreiter	0	0	0				

Most Recent Security Alerts

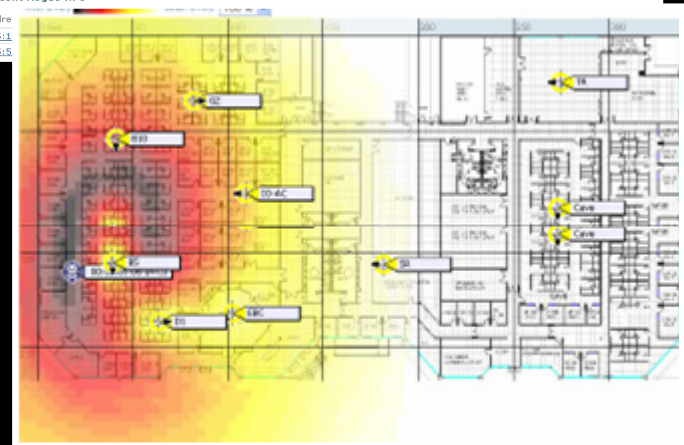
Failure Object	Date/Time	Message
Switch_S1C_1d_1WAPP2/171.71.128.78	5/19/06 9:40 AM	IDS 'Disassoc flood' Signature attack detected on AP 'sjc14-41b-ap2...
Client 00:02:8a:ba:70:c2	5/19/06 7:06 AM	The WEP Key configured at the station may be wrong. Station MAC Add...
Client 00:0e:9b:1f:b3:0c	5/19/06 6:23 AM	The WEP Key configured at the station may be wrong. Station MAC Add...
Client 00:02:8a:ed:04:71	5/19/06 6:11 AM	The WEP Key configured at the station may be wrong. Station MAC Add...
Client 00:14:ad:0e:91:05	5/19/06 6:09 AM	The WEP Key configured at the station may be wrong. Station MAC Add...

Most Recent Rogue APs

MAC Address	Location
00:0b:85:1	
00:0b:85:5	

Summary Metrics:

- Rogues: 1
- Coverage: 78
- Security: 127
- Controllers: 1
- Access Points: 5
- Location: 0



Scheduled Shut off of WLAN and Access Point Radios

Feature

- Scheduled configuration change of the operational mode (on/off) of access points can be set by Cisco WCS

The screenshot shows the 'AP Schedule Details' page in the Cisco WCS interface. The page includes a search bar for AP names, a table of selected APs, and configuration options for the schedule. The 'Admin Status' is set to 'Enable'. The 'Schedule Time' is set to 15:59 on 12/11/2007. The 'Recurrence' is set to 'Weekly' with checkboxes for Sunday through Saturday, where Friday and Saturday are checked. A 'Submit' button is visible at the bottom.

Selected AP Name(s)	
Deepak.89a8	802.11 a
Deepak.1242	802.11 a
Deepak.1242	802.11 b/g
Deepak.89a8	802.11 b/g

Benefit

- Supports deactivation of WLAN to meet security requirements during business or non-business hours

The screenshot shows the 'WLANs' configuration page in the Cisco WCS interface. The page is for a WLAN named 'Guest' with SSID 'Guest'. The 'Status' is 'Enabled' and 'Schedule Status' is checked. The 'Start Time' is set to 15:57 on 12/11/2007. The 'Security Policies' are set to 'WEB-Auth'. The 'Radio Policy' is 'All' and the 'Interface' is 'management'. The 'BroadCast SSID' is checked to be 'Enable'.

Cisco Compatible Extensions

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/ciscocompatible/wireless>

Cisco Secure Services Client

- **Key Features:**

- 802.1X authentication for wired and wireless devices**

- Windows XP/2000 support**

- **EAP:**

- EAP-FAST, EAP-MD5, PEAP-MSCHAP, PEAP-GTC, EAP-TLS, EAP-TTLS, Cisco LEAP**

- **Encryption:**

- WEP, Dynamic WEP, TKIP, AES**

- **Standards:**

- WPA and WPA2**



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

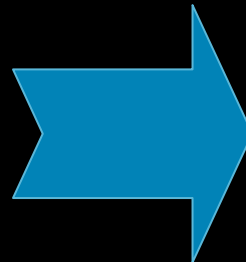
Cisco Context Aware Mobility Solution

Moving from Cisco 2710 to Cisco MSE Platform

Cisco 2700 Series Wireless Location Appliance



- Indoor only
- 2500 tags and clients
- RSSI only
- Industry's first location solution integrated into the WLAN infrastructure
- Location only
- Open API
- WCS management



Cisco 3300 Series Mobility Services Engine



- Indoor, outdoor, high ceilings
- 18,000 tags and clients
- RSSI and TDOA
- Next-generation
- Open API
- WCS management
- Robust architecture for adding other technologies (UWB, passive)
- Shared platform for other mobility services (incl. future)

Wireless for Manufacturing



Branch Office Deployment— Hybrid REAP

Design Considerations:

- Allows bridging/tagging of traffic locally (local switching) by WLAN
- Allows simultaneous tunneling of traffic to WLC (central switching) by WLAN
- “Connected Mode”—LWAPP control centralized
- “Standalone Mode” (WAN outage)
 - Locally switched WLANs stay up
 - Some lost functionality
- ← 100 msec latency between APs and WLC
- H-REAP APs should be connected to trunk ports—allow only the relevant, locally switched VLANs
- No optimization for:
 - Fast, secure roaming (CCKM, PKC)
 - Voice (no CAC or TSPEC support in standalone mode)

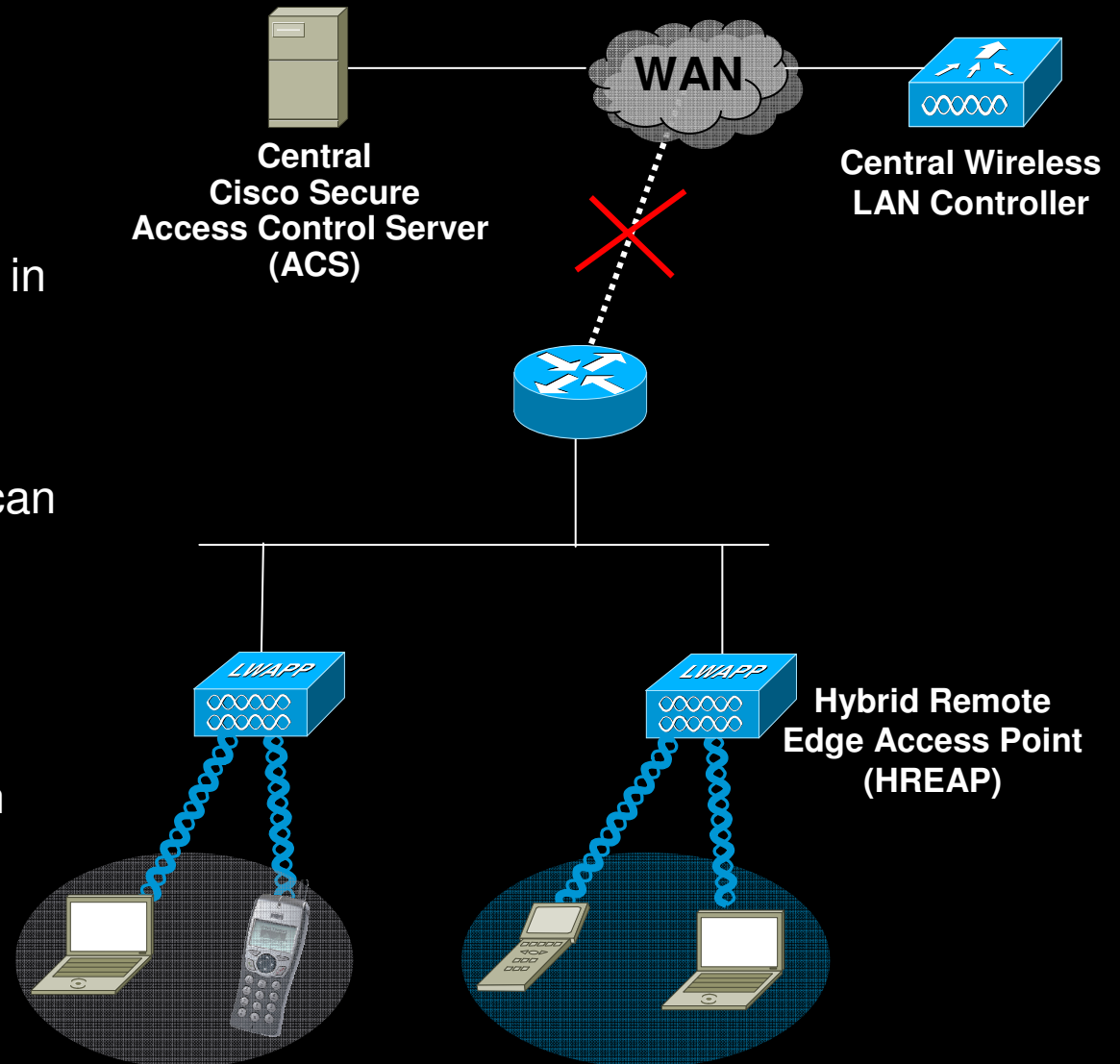
HREAP – 802.1x Auth on the AP

Features

- Allows HREAP to do 802.1x authentication on the AP itself in standalone mode
- Uses a pre-configured list of usernames and passwords
- During WAN outage HREAP can authenticate users using the HREAP's RADIUS server

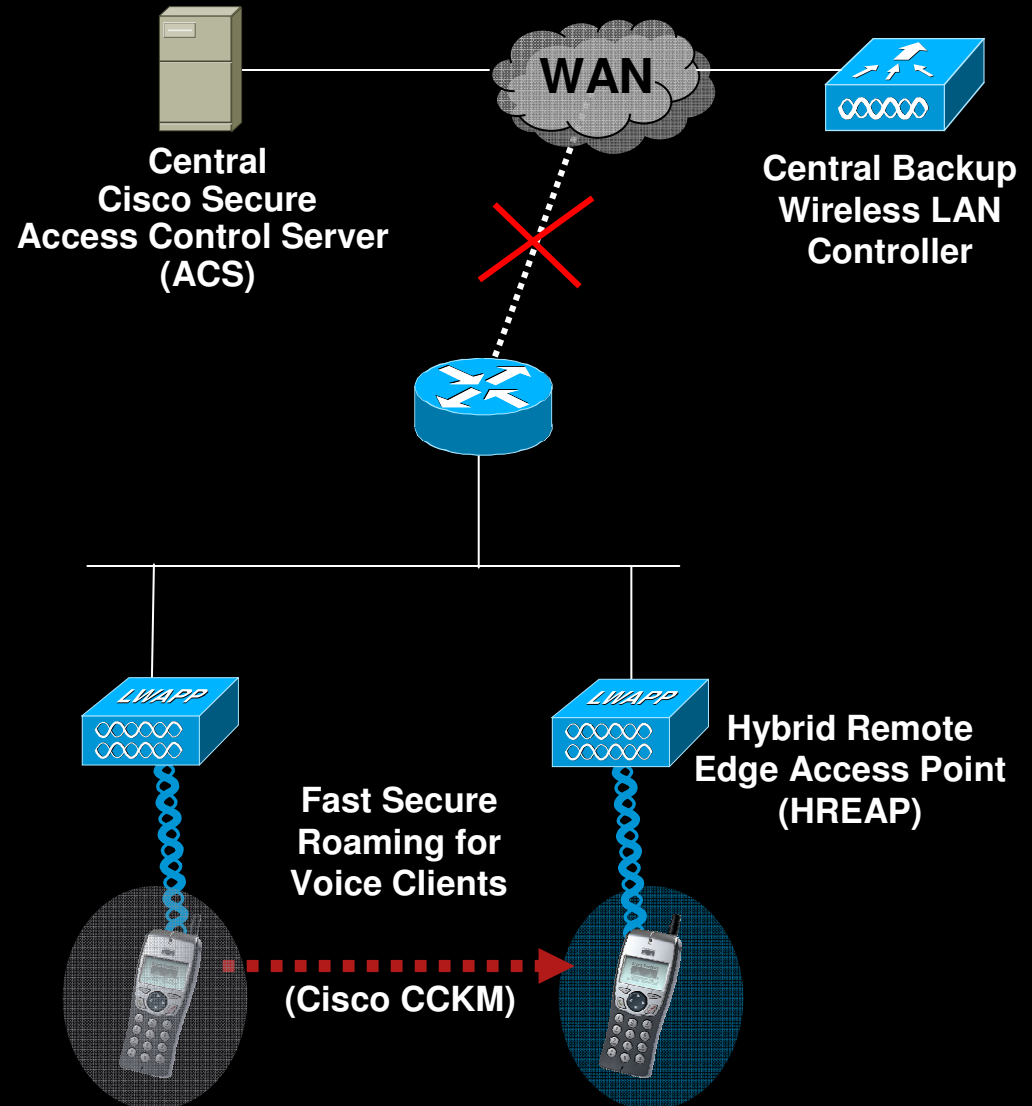
Benefits

- Ensure minimum service even during WAN outage
- No additional HW required for 802.1x authentication



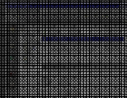
HREAP – CCKM

- **HREAP supports Layer 2 fast secure roaming**
 - Cisco Centralized Key Management (CCKM) roaming on local controller if the WAN link connection is lost
- **Benefit**
 - Roaming voice clients in remote locations and branch offices will stay connected even when the WAN link to the wireless LAN controller is lost

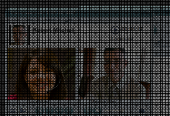


Plant Voice over WLAN Solution

Applications



Data Warehouse Voice Picking




Unified Personal Communicator




Intermec


UC Network Elements




Cisco Unified Communications Manager



Messaging Gateway




Cisco Unified Presence

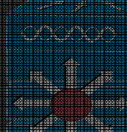


Voice Gateway

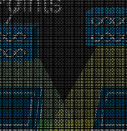




Cisco Wireless Control System

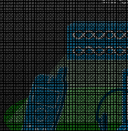


Cisco WLAN Controller



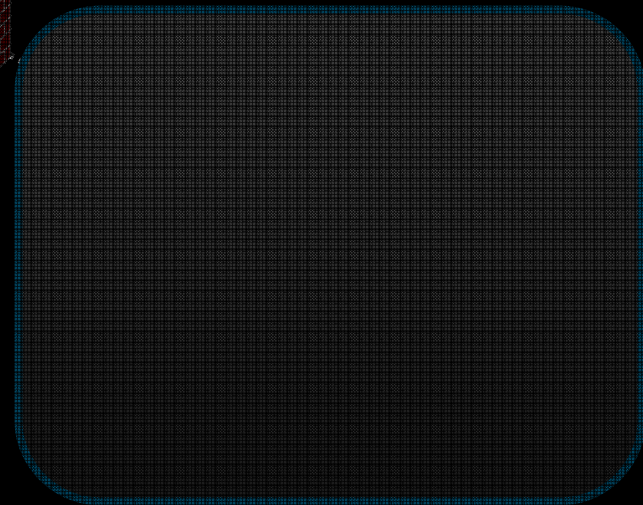
Cisco Airone Access Points

Warehouse



Hybrid Remote Edge Access Point

Remote Worker



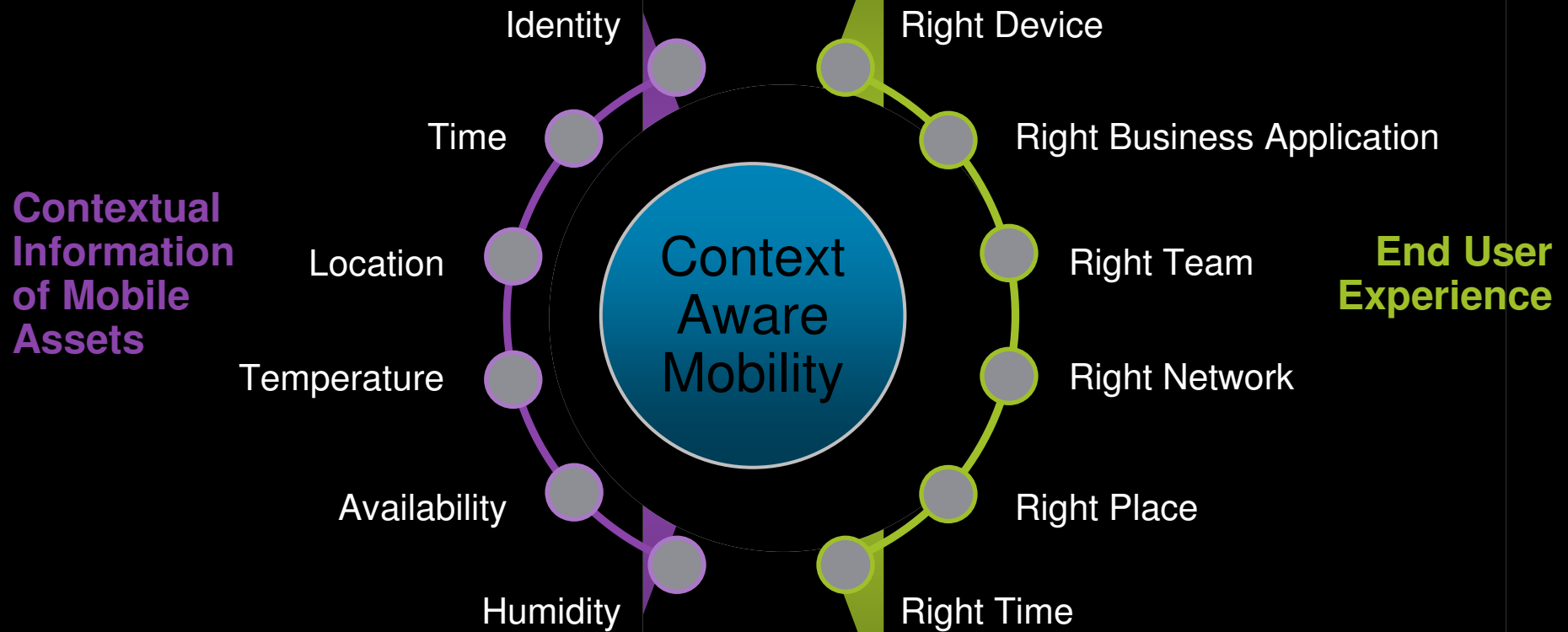
Plant

7921G Overview

- 802.11a/b/g
- 2 in (5 cm) color display with 176 x 220 pixel resolution
- Dedicated Volume and Mute buttons
- Application button supports PTT via XML
- Two softkey buttons
- Speakerphone
- Diversity antenna (5GHz band only)
- Ringing, message waiting, and charging LED
- 5-way navigation key
- Separate ringer and speaker
 - Louder ring volume
- Vibrate alert
- Backlit keypad and display
- Headset connector 2.5mm (4-conductor/tri-band)
- USB 1.1 connector



Context Aware Mobility Solution



Ability to Dynamically Capture and Use Contextual Information of Mobile Assets to Optimize, Change or Create Communications Flow and Business Processes

Challenges of Today's Solutions

In close proximity
Passive RFID



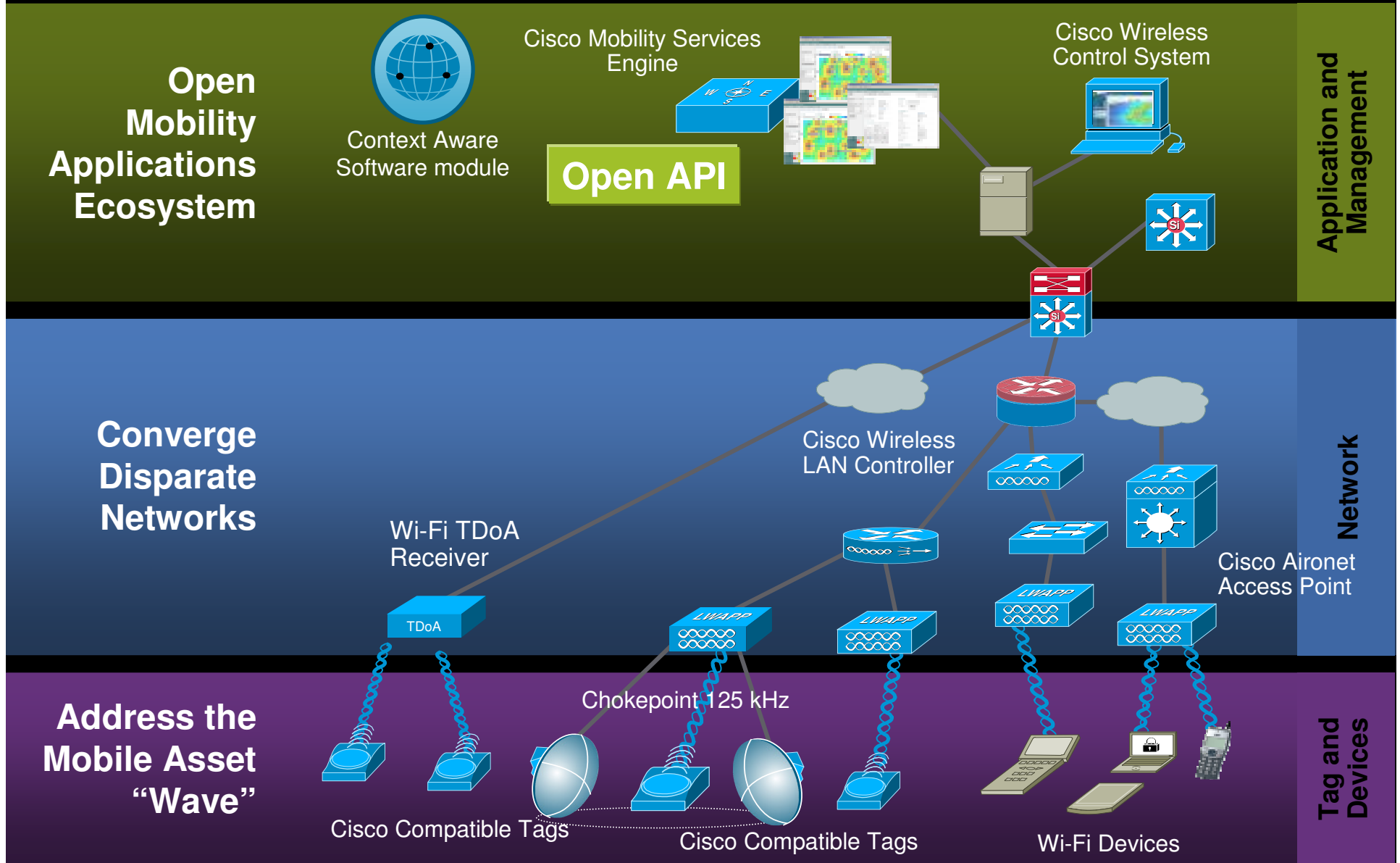
Campus
Wi-Fi (TDoA,
Chokepoint)

Building
Wi-Fi (RSSI, Chokepoint)

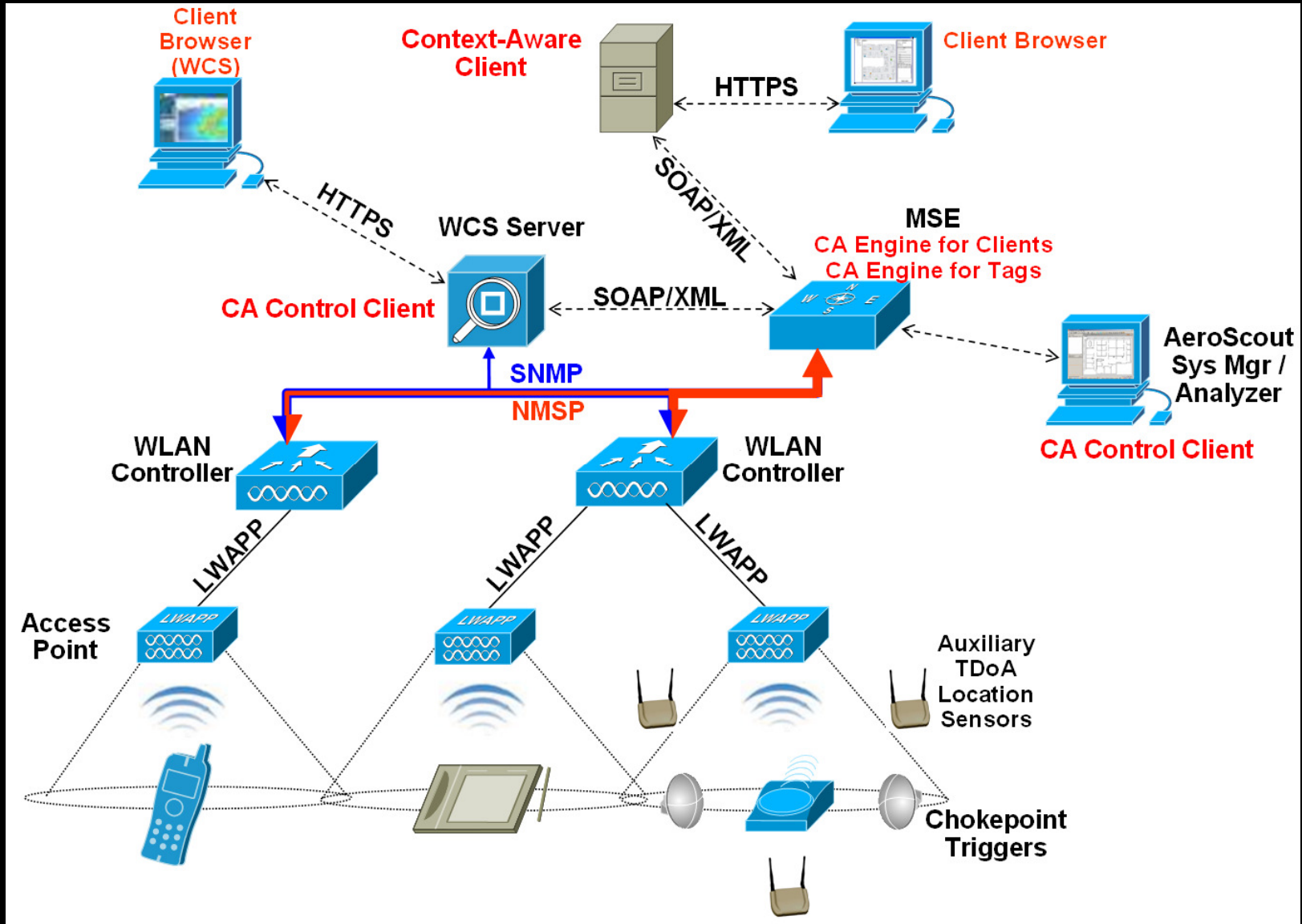
Nationwide
Cellular, GPS

Different Devices, Networks and Applications to Manage for Each
Workspace Involved in the Business Process

Cisco Context Aware Mobility Solution

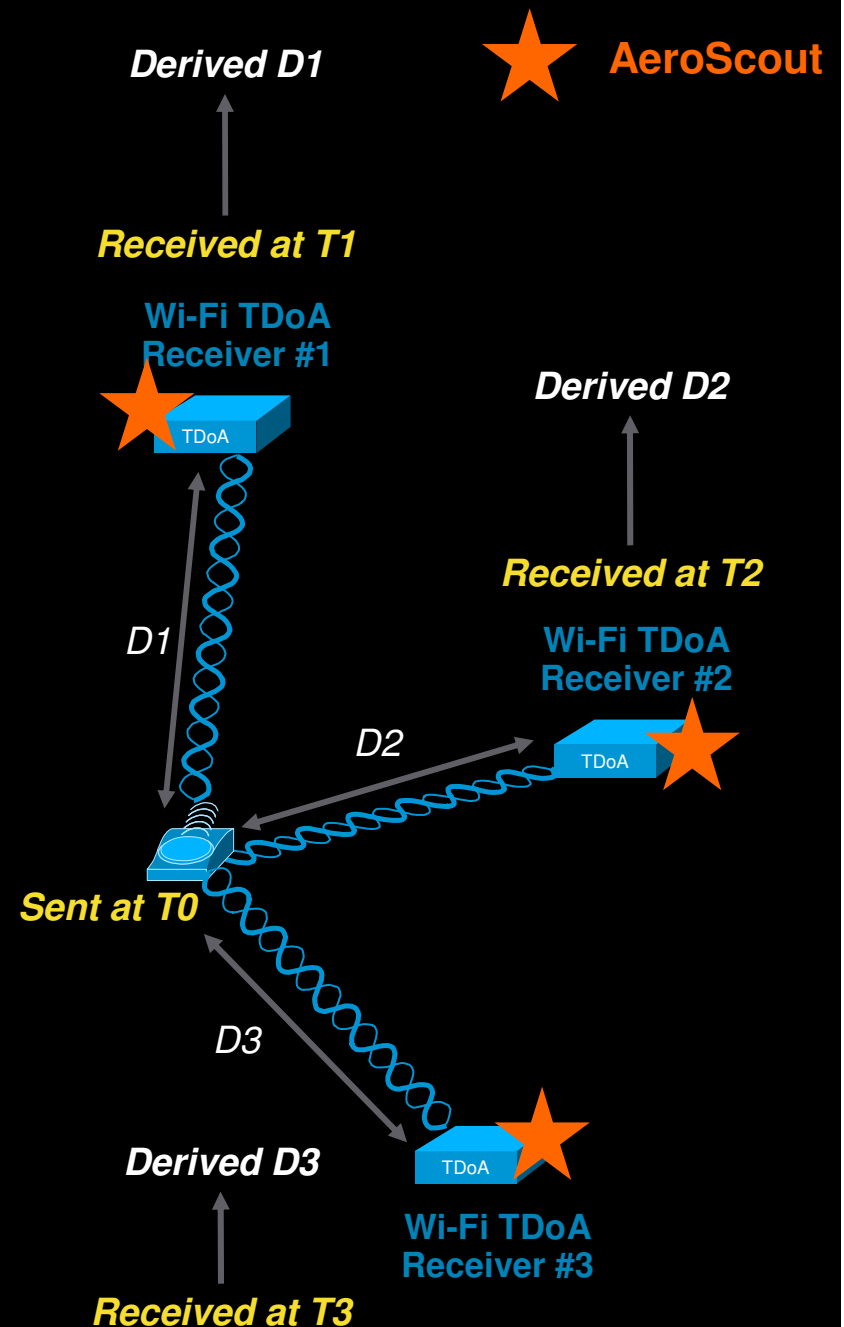


Context-Aware Mobility Schematic



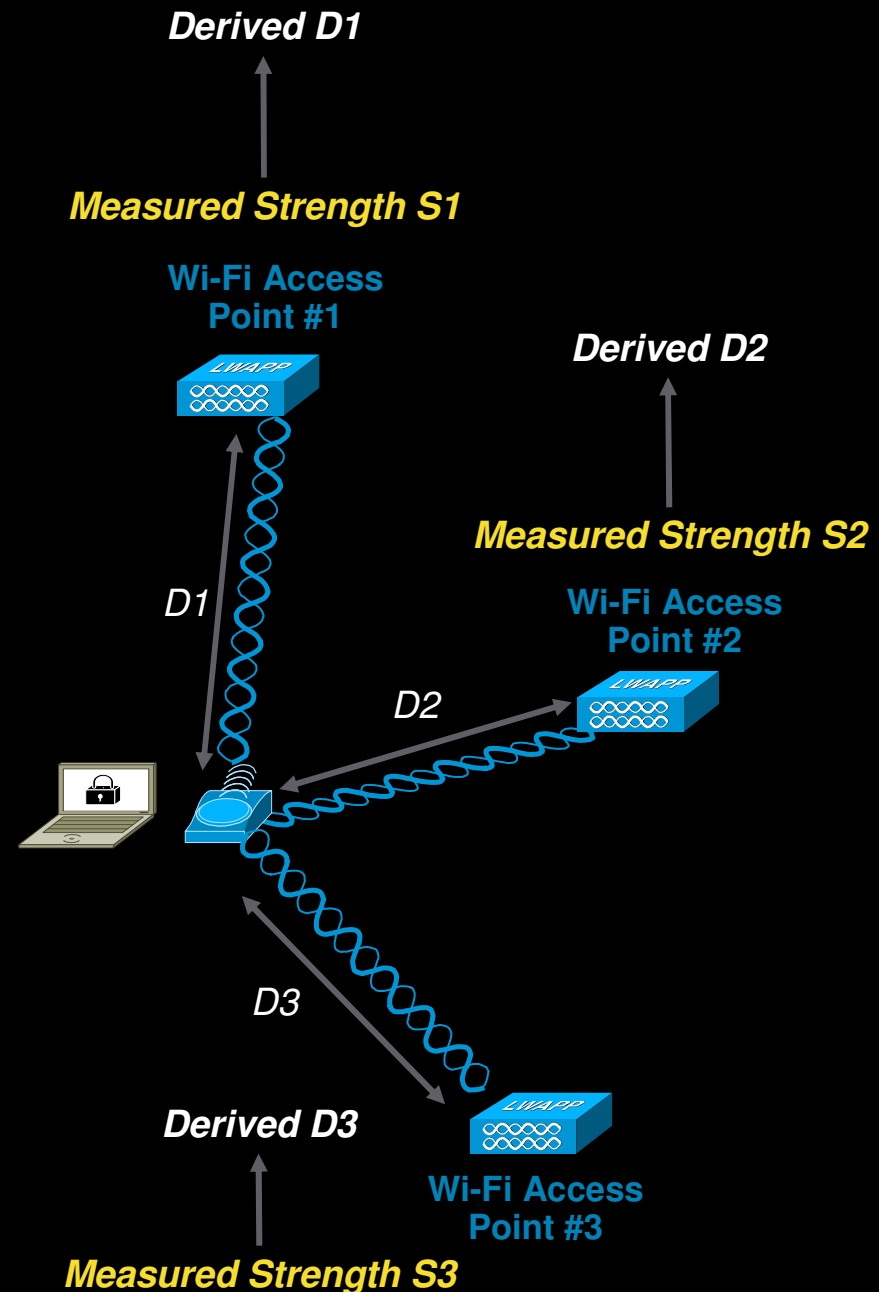
How TDoA works

- Time Difference of Arrival
- Used with any CCX tags (not client)
- Wi-Fi TDoA receivers are synchronized
- Distances between the tag and APs is calculated based on the time difference of arrival
- Requires Line of Sight
- Recommended for high ceilings, outdoors and outdoor like environments (e.g. warehouses, parking lots)



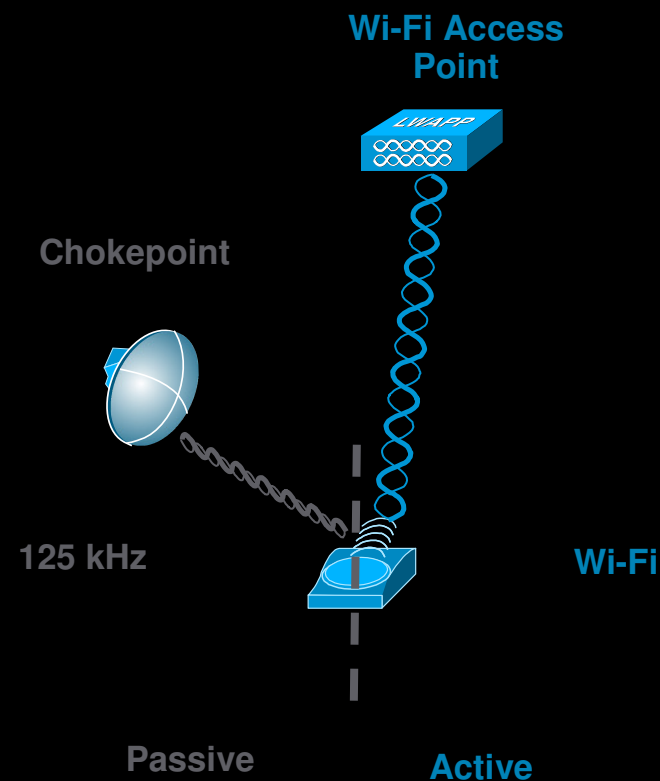
How RSSI works

- Received Signal Strength Indicated
- Used with Tags and Clients
- Receivers are the access points
- Distances between the tag and APs is calculated based on the received signal strength
- Requires medium to short read range for better accuracy
- Recommended for indoors



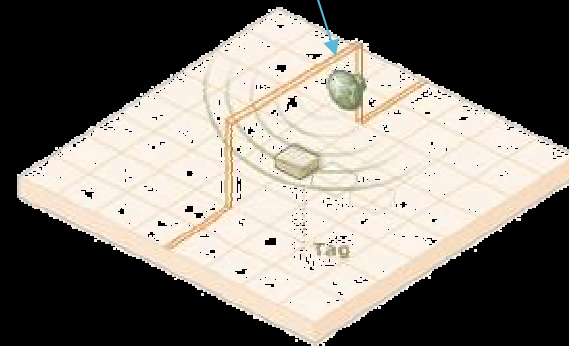
How Chokepoint works

- Hybrid tags with 125 kHz passive and Wi-Fi active sides
- Tags and chokepoints have to be from the same vendor (Aeroscout or WhereNet)
- When the tag is in close proximity of the chokepoint, its passive side gets excited and captures the information (location and sensing) then the active side sends the information over Wi-Fi
- The tag beaconing frequency can be reconfigured by the chokepoint
- Indoor or Outdoor



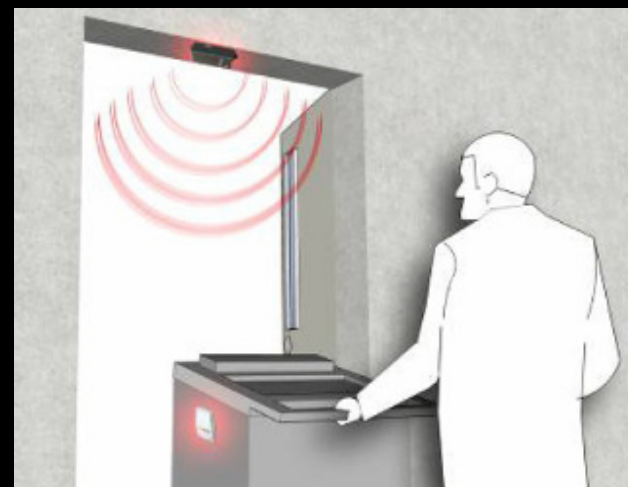
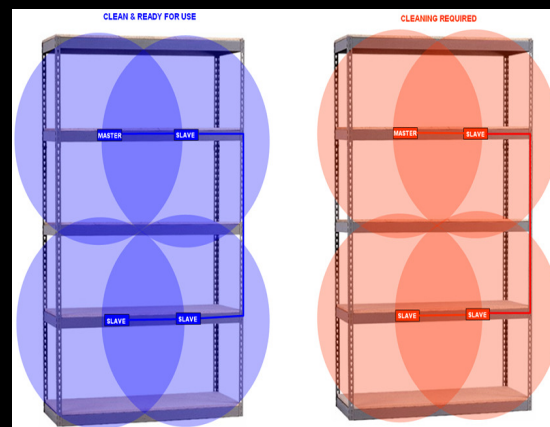
Why Use Chokepoint Triggers?

- Chokepoint triggers cause tagged assets to indicate they are within the confines of a chokepoint or other constricted area.
 - A direct result of the asset tag entering the stimulation zone of the chokepoint trigger.
- Chokepoint triggers can be used to:
 - Trigger tags to transmit stored msgs
 - Provide proximity asset location with granularity dependent on trigger range
 - Determine asset floor location
 - Modify tag state
 - Activate on entry or deactivate on exit
 - Modify tag configuration
 - Trigger tags to initiate data retrieval
- Cisco OEMs Exciters from AeroScout



Use Cases

- Accurate detection in a confined area
 - Asset count in room, on shelf, etc.
- Entrance / Exit detection
 - Indicate unauthorized asset movement or removal
- Trigger status change or other action
 - Auto at entry gate triggers entry procedure
 - Truck at exit gate triggers exit procedure
 - Retrieve vehicle fuel data passing through gate
- Detect direction of movement through gates
 - Distinguish entry from exit at a combined bi-directional gate*
- Find individual asset among many identical
 - Blinking tag LED can identify an individual asset
- Sequence or workflow enforcement
 - Enforce proper workflow progression
- Enforce association between two entities
 - Worker at workstation, patient and room, etc.



* Bidirectional gate requires compatible location client (i.e. MobileView)

Solution Components

Indoor Environments

Function	Component
Wireless Infrastructure	Cisco Unified Wireless infrastructure (Cisco AP's, Cisco WLC) Cisco MSE CCX tags
Location Engine	Context Aware Engine for Tags software (purchased separately), software license (based on tag count)
Network/Device Management	Cisco WCS: manages Cisco wireless infrastructure and Cisco MSE AeroScout System Manager: configuration and management of partner engine, excitors, calibration, displaying tags on floor maps

Solution Components Outdoor/Outdoor-Like

Function	Component
Wireless Infrastructure	<p>Wi-Fi TDOA receivers (does not require Cisco Unified Wireless infrastructure)</p> <p>Cisco MSE</p> <p>CCX tags</p>
Location Engine	<p>Context Aware Engine for Tags software (purchased separately), software license (based on tag count)</p>
Network/Device Management	<p>Cisco WCS: manages Cisco MSE, displaying tags on maps</p> <p>AeroScout System Manager: configuration and administration of partner engine, Wi-Fi TDOA receivers, calibration, displaying tags on maps</p>

RFID Solutions From Cisco and Oat Systems

Oat Systems to Integrate with the Cisco Context Aware Open API to Enable Asset Tracking Solutions in Manufacturing



Context Aware

Why Cisco and Oat Systems

- Market leadership in the enterprise WLAN and RFID space
- Faster implementation by integrating with existing business processes
- Flexible, standards based solution

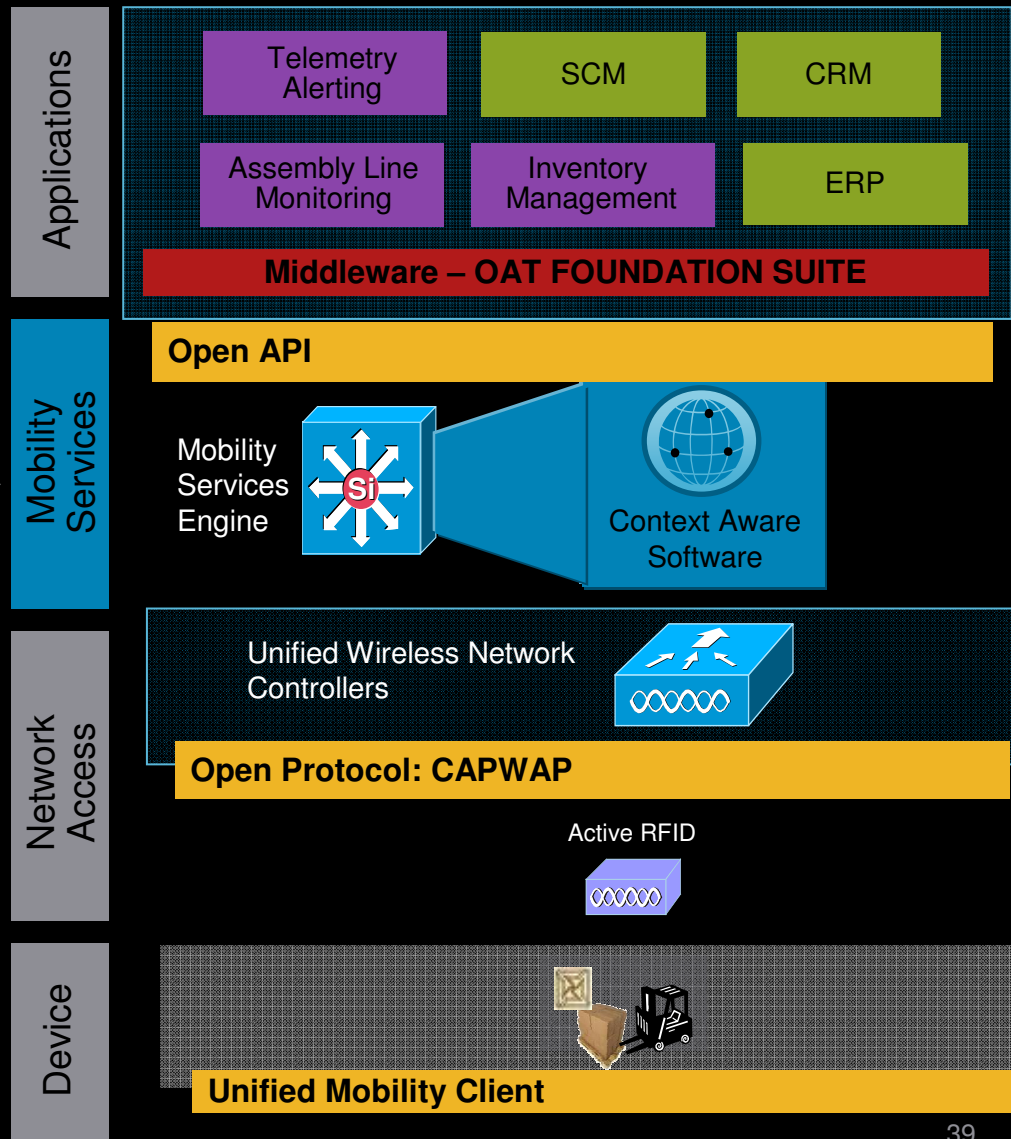


OAT Manufacturing Solutions

- Work In Process (WIP) Tracking
- Asset Tracking

Solution Components:

- OATaxiom™: RFID data management & reporting
- OATdesigner™: RFID scenario builder GUI
- OATexpress™: RFID data capture, filtering and management



Why Cisco for Context Awareness

Breadth and Integration	Beyond regular location	Open Eco-System	Future Extensions
<p>Only industry solution with outdoor and indoor offers</p> <hr/> <p>Choice of techniques (RSSI, TDoA, Chokepoint)</p> <hr/> <p>Central management for both context awareness and WLAN</p> <hr/> <p>Based on existing WLAN infrastructure</p>	<p>Unmatched scalability with up to 18,000 clients and devices</p> <hr/> <p>Telemetry information such as temperature, humidity, motion, pressure...</p>	<p>Integration with business applications via Cisco open API</p> <hr/> <p>Increasing vertical integration for healthcare, manufacturing, retail and education with best-in class partners</p> <hr/> <p>Broad tags choice and application independence with Cisco Compatible Extensions Program</p>	<p>Flexible architecture that allow a fast and seamless integration of a variety of access technologies such as UWB, passive RFID, or GPS</p> <hr/> <p>Integration with other Cisco applications already demonstrated with Unified Communications</p>

Only industry solution that can answer to any of your needs today and evolve as you integrate contextual information more and more into your business processes

Q&A



