



Cisco Unified Mobility for the Enterprise



Nassim Ait Youcef – Systems Engineer nyoucef@cisco.com

22nd of April 2008

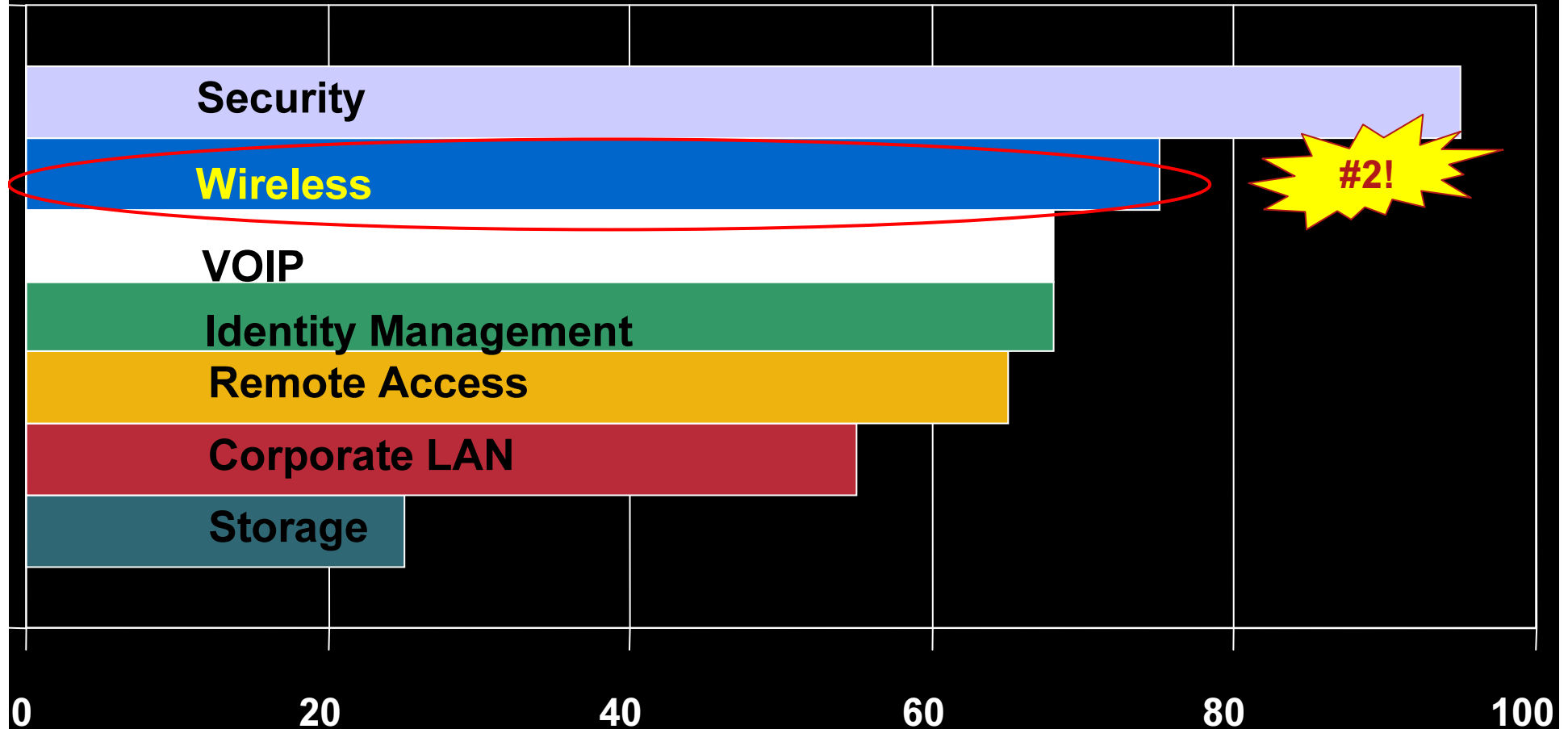
Agenda

- **Wireless Trends**
- **Cisco Wireless Networks**
- **Top Reasons to Deploy Wireless**
- **Other Benefits of the Unified Approach**
- **Summary**
- **Q&A**

Where is the CIO Spending in the Next Year?

Security, Wireless and VoIP are top 3 Networking Priorities

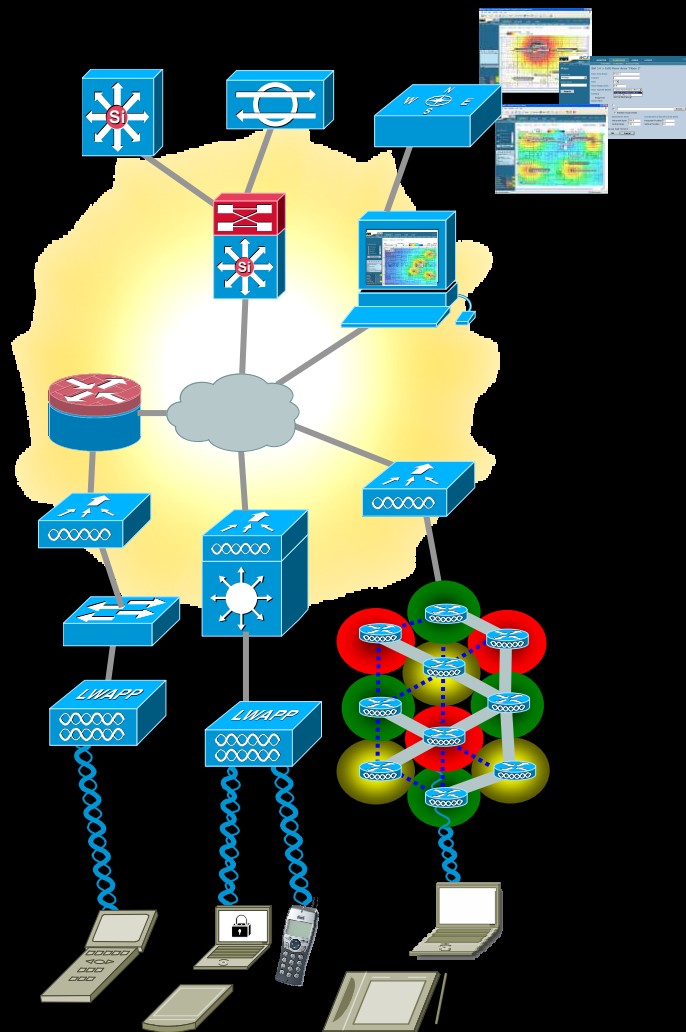
Goldman Sachs FY 06 IT Survey:
Medium and High Priorities



Source: Goldman Sachs IT Spending Report, July 2006

Cisco Unified Wireless Network

End-to-End, Unified – Only Cisco



Unified Advanced Services

Unified cellular and Wi-Fi VoIP. Advanced threat detection, identity networking, location-based security, asset tracking and guest access.

World-Class Network Management

Same level of security, scalability, reliability, ease of deployment, and management for wireless LANs as wired LANs.

Network Unification

Integration into all major switching and routing platforms. Secure innovative WLAN controllers.

Mobility Platform

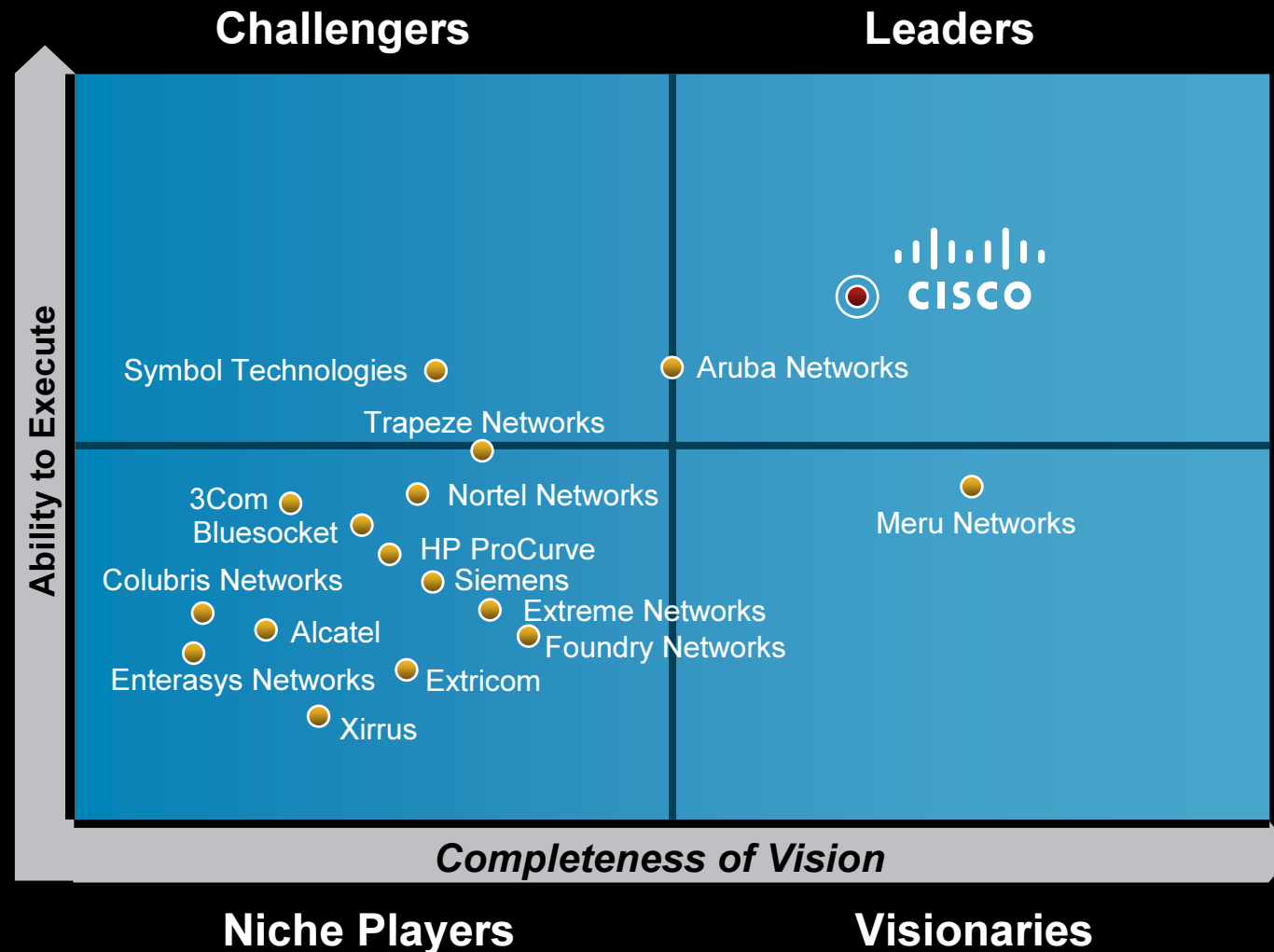
Ubiquitous network access in all environments. Enhanced productivity. Proven platform with large install base and 61% market share. Plug and play.

Client Devices

90% of Wi-Fi silicon is Cisco Compatible Certified. "Out-of-the-Box" wireless security.

Gartner Magic Quadrant

Cisco is the only clear vendor in the Leader Quadrant



Forrester Wave: Q2Y07

Cisco is clearly distinguished as the market leader



A Business Class Wireless Experience

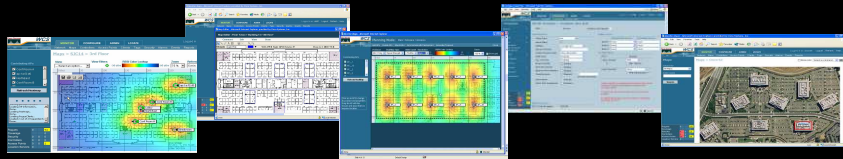
Why Settle for Anything Less?



**Cisco
Self-Defending
Network**

Unified Advanced Services

Unified built-in support of leading edge applications - not an after thought. Cisco Wireless Location Appliance, Cisco WCS, SDN, NAC, Wi-Fi phones, and RF firewalls.



World-Class Network Management

World Class NMS that visualizes and helps secure your air space. Cisco Wireless Control System (WCS)



Network Unification

Seamless network infrastructure across a range of platforms. Cisco 4400, 2000 Wireless LAN Controllers and Cisco Catalyst 6500 Series WiSM. ISR integration.



Mobility Platform

APs dynamically configured and managed through LWAPP. Cisco Aironet Access Points: 1500, 1300, 1240AG, 1230AG, 1130AG, 1000 and the new 1252.

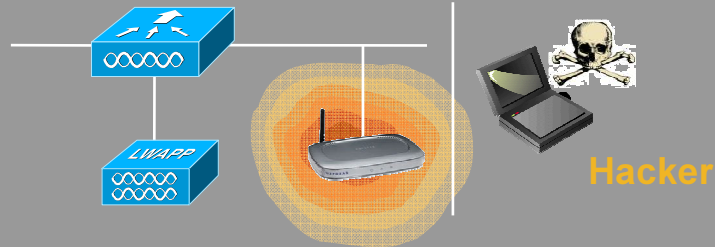


Client Devices

Secure clients that work out of the box. Cisco Compatible Client Devices & Cisco Aironet clients.

Top 4 Reasons Every CXO Needs a Pervasively Deployed Wireless System

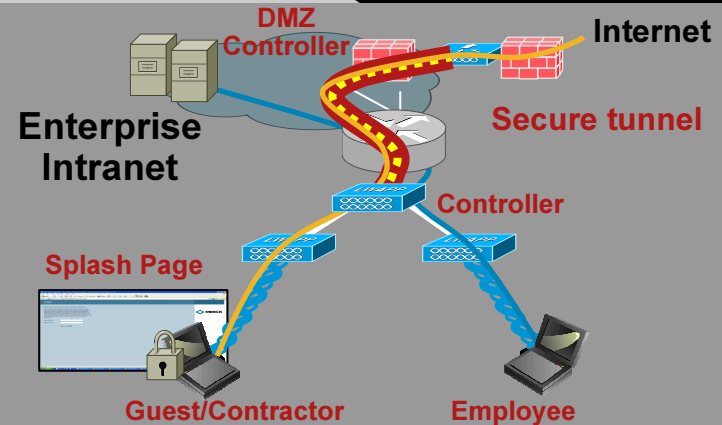
Security



Rogue APs—Employees create opening to enterprise network unknowingly

FTC FINES

Guest Access



Voice

- WiFi enabled voice
- 7921G, Blackberry, Treo
- Better coverage
- Reduced Cost
- Integrated with IP PBX



Location

Active IP Monitoring

Retail



Healthcare



Financial



Multi-Service Location

Voice Services



Compliance



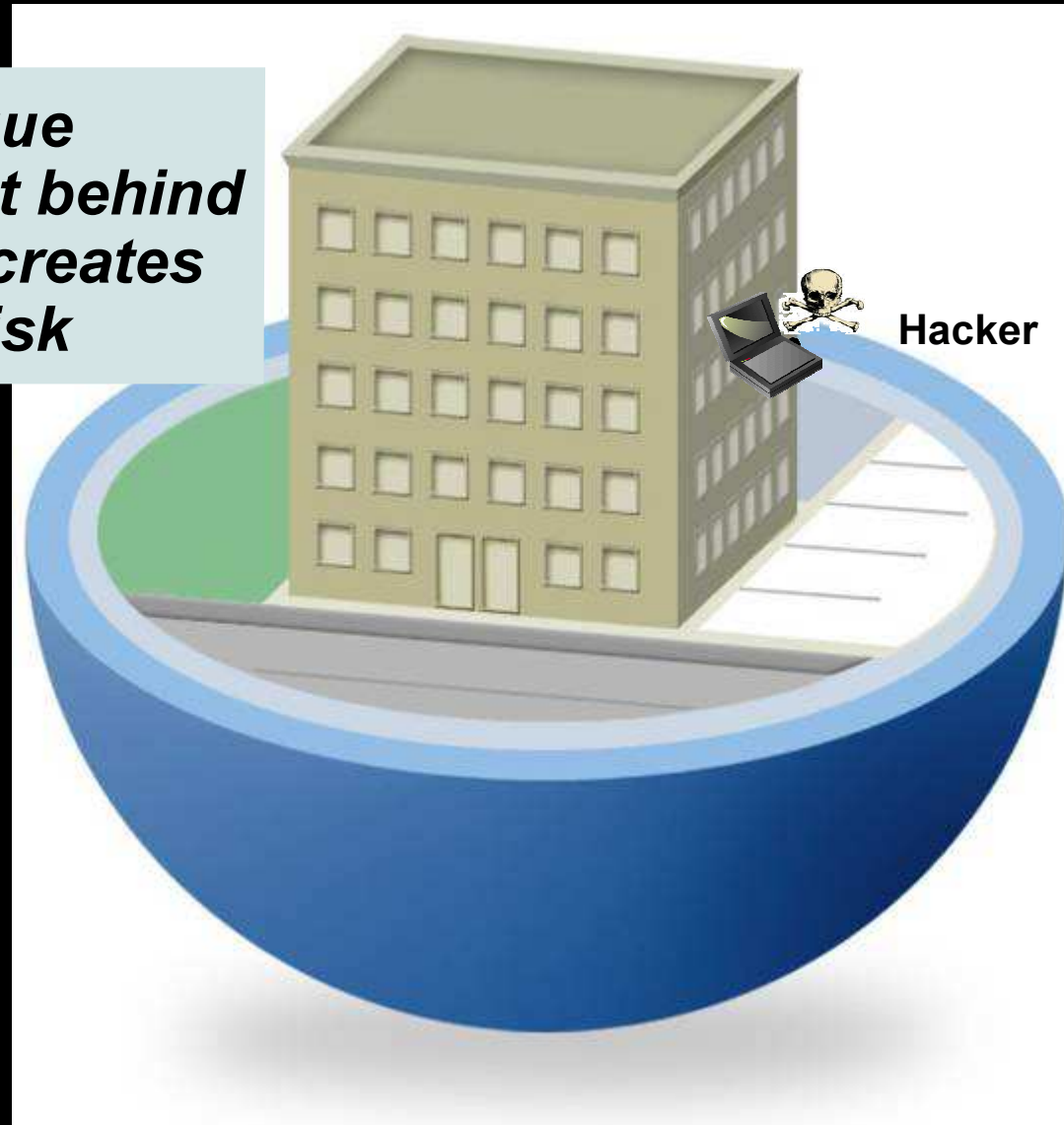
Sensor Networks



#1 Security

The Wireless Enterprise Has No Walls

A single rogue access point behind the firewall creates enormous risk



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 **by your own employees**

*A handheld walk-around
survey is sufficient
(i.e. AirMagnet)*

WRONG!

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

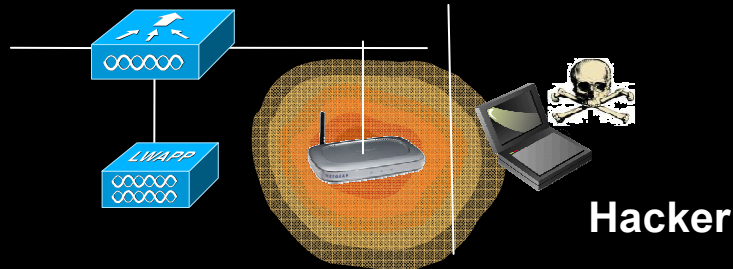
*I use 802.11i, WPA or
VPN, so my network is
secure*

WRONG!

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

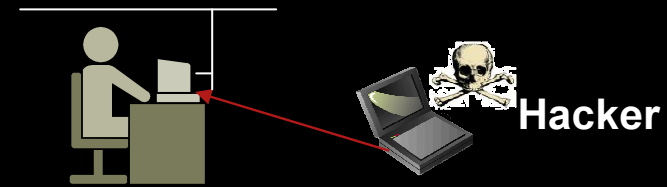
Top Wireless Threats

Rogue AP



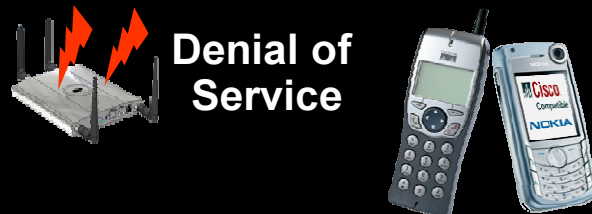
- Employees create opening to enterprise network unknowingly

Ad Hoc



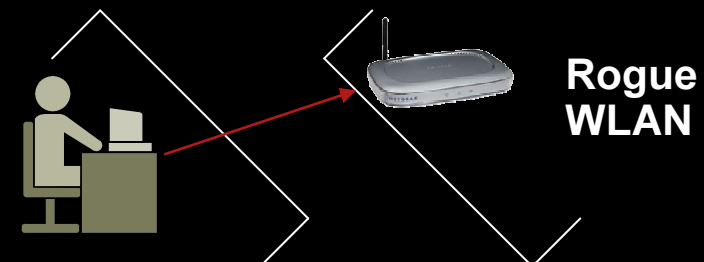
- Client-to-client connections, bypassing infrastructure security checkpoints

DoS Attacks



- Malicious hackers disrupt critical business services

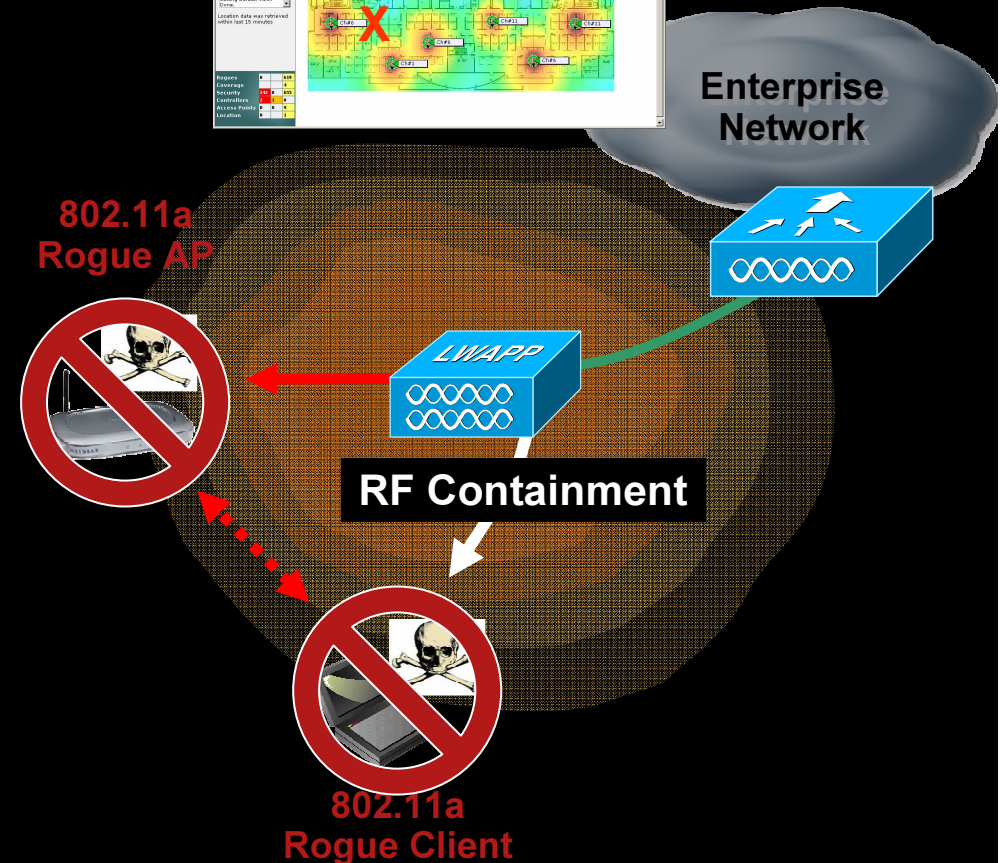
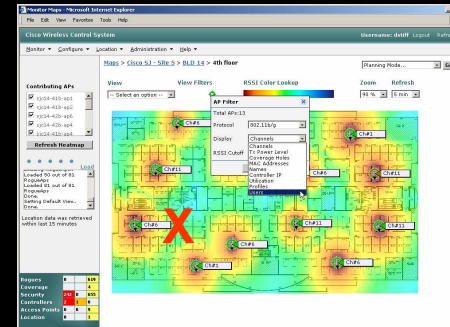
Client Mis-association



- Employees connect to an external WLAN, creating portal to enterprise wired network

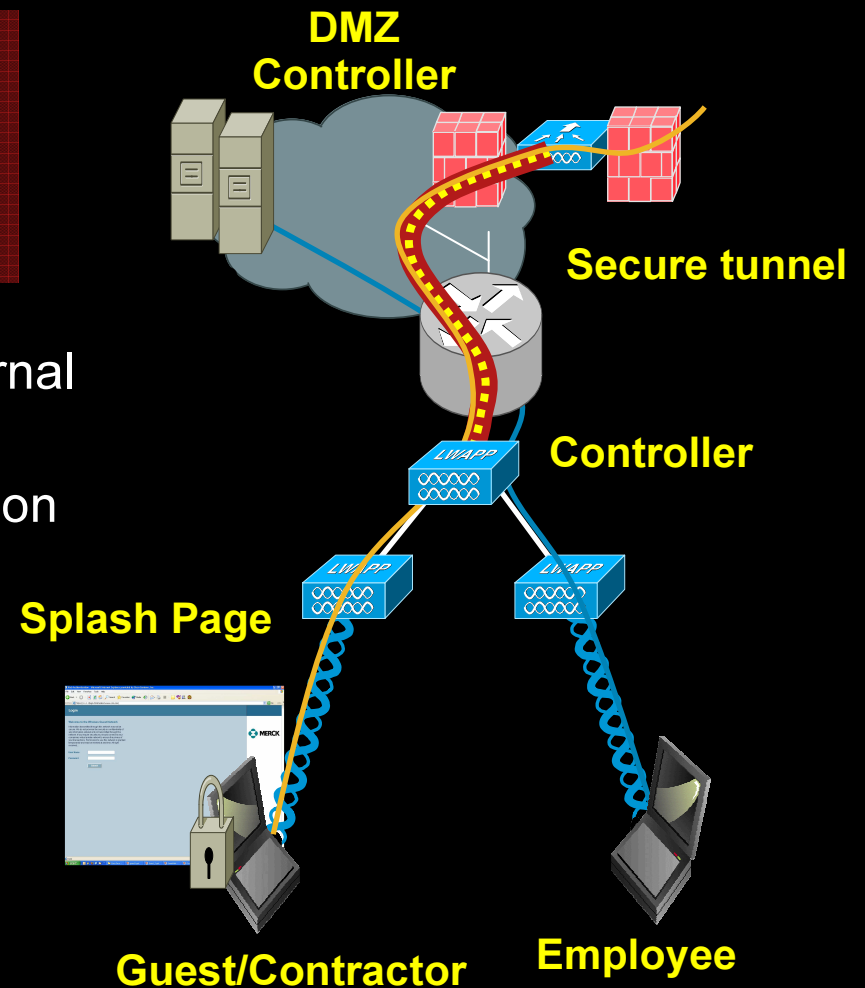
Cisco Unified Wireless Network Integrated Wireless IDS/IPS Protects Your Business

- Automatically detects:
 - Rogue access points and clients
 - Ad hoc networks
 - Denial of service attacks
 - Client mis-associations
- Intelligent RF scanning = cost effective solution
- Intrusion prevention under IT control
- Location appliance provides precision mapping for physical removal



#2 Secure, Controlled Guest Access

- Business Need: Provide access to networked resources for visiting customers, partners and contractors
- But, how to do so without exposing internal resources?
- Cisco's wireless guest networking solution provides:
 - Secure, controlled network access
 - Pervasive, managed coverage
 - Lower costs for support and moves/adds/changes
 - Quick and easy access for extended workforce.



#3 Mobile Voice & Data Services

- Business Need: Augment network coverage for mobile email and telephony while lowering cellular charges
- Challenges:
 - Poor in-building cellular coverage
 - No access to enterprise voice apps
 - Multiple numbers / mailboxes drain productivity
- Benefits of mobile voice & data:
 - Positively impact productivity
 - Real-time communications accelerates decision making
 - Reduced cellular, paging, SMS charges
 - Leverage corporate dialing plans, least cost routing



Voice over WLAN

Requires end-to-end intelligence



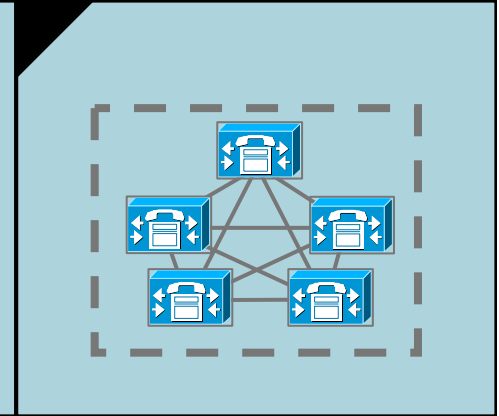
VoWLAN Clients



Voice Ready WLAN Infrastructure



Unified Wired/Wireless LAN Infrastructure



Cisco CallManager & Mobility Applications

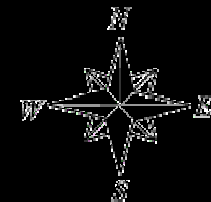
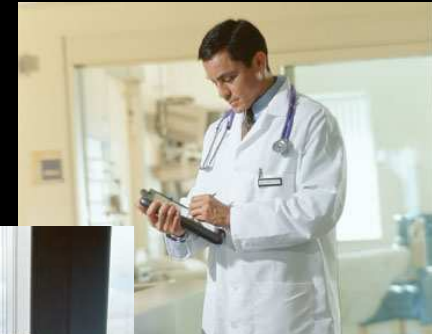
- Comprehensive on campus solution
- Dedicated clients, soft phones
- CCX enables QoS, Fast Secure Roaming
- IEEE 802.11b easy to use wireless IP phone
- Pixel display provides intuitive access to features and applications
- Mobility on / off campus
- Dual 802.11 and cellular phone
- Partners: Nokia, RIM
- Additional voice clients

#4 Location Services

- Business Need: Decrease cost of locating and replacing assets. Improve security and effectiveness of communications

Location Services Benefits:

- Real-time Network Visibility—**Manage assets and streamline workflows**
- Asset Tracking—**View Wi-Fi devices and people as they physically move**
- Security—**Quickly locate security threats such as rogue access points and devices**
- Location Trending—**Find out where devices and people have been and when**



WCS with Location Appliance

Cisco Wireless Control System Username: sedemo Logout Refresh

Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾

Maps > Cisco SJ - Site 5 > BLD 14 > 3rd floor

Contributing APs

- sjc14-31b-ap3
- sjc14-32b-ap3
- sjc14-31b-ap4
- sjc14-32b-ap5
- sjc14-31b-ap1

Refresh Heatmap

Load

Done, but with errors on page.

Rogues	0	620
Coverage		2
Security	173 0	342
Controllers	2 1	0
Access Points	0 0	4
Location	0	0

View **View Filters** **RSSI Color Lookup**

-- Select an option --

-- Select a command --

GO

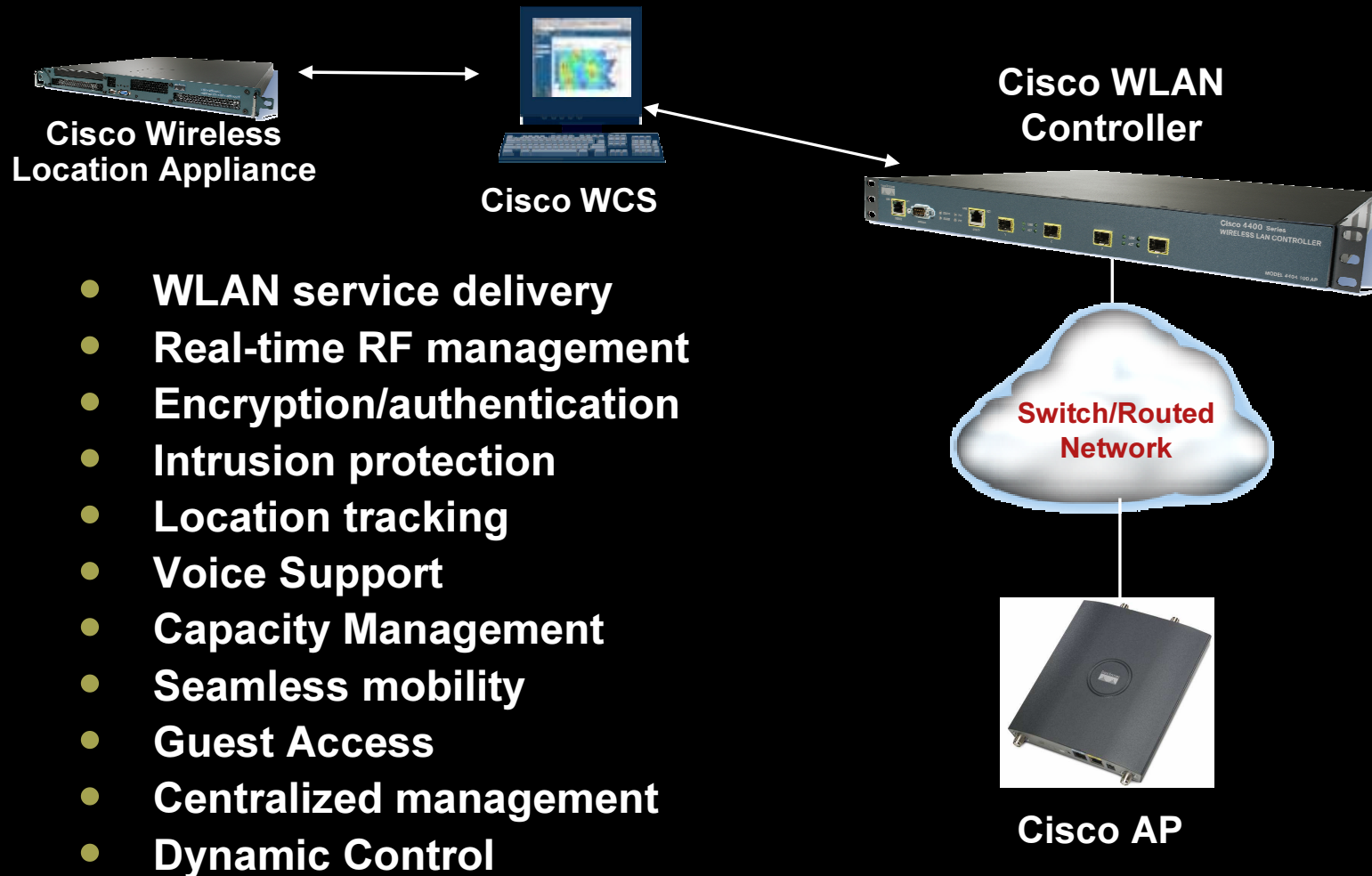
- Select a command --
- Add Access Points...
- Position APs...
- Remove Access Points...
-
- Edit Floor Area...
- Delete Floor Area...
-
- Recompute RF Prediction...
- Refresh from Network...
-
- Map Editor
-
- Planning Mode...

Location data was retrieved within last 15 minutes

Local intranet

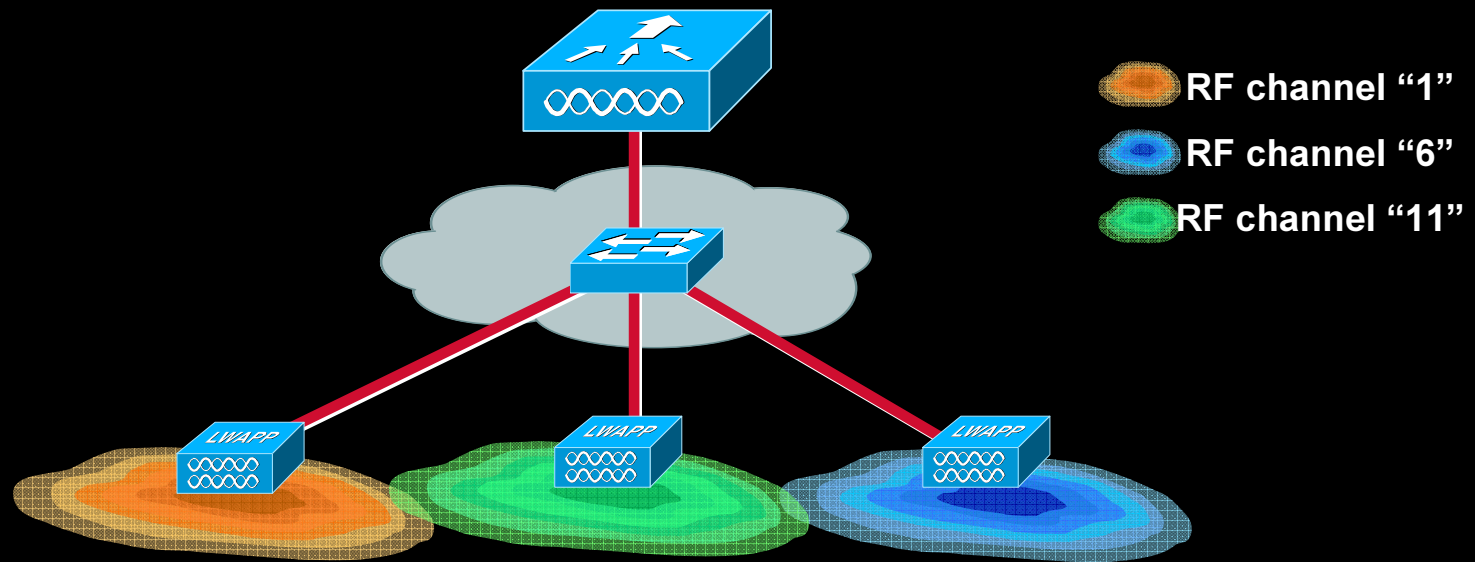
Other Benefits of the Unified Approach

A Single Unified WLAN System



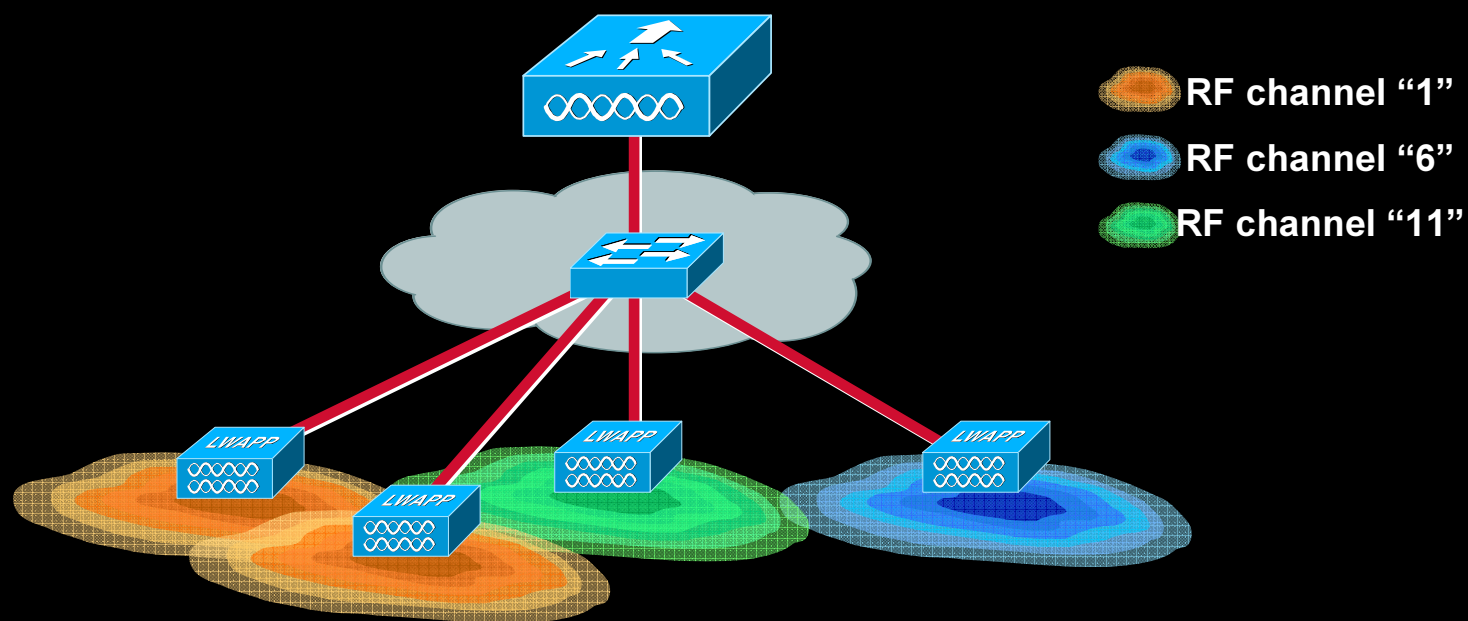
- **WLAN service delivery**
- **Real-time RF management**
- **Encryption/authentication**
- **Intrusion protection**
- **Location tracking**
- **Voice Support**
- **Capacity Management**
- **Seamless mobility**
- **Guest Access**
- **Centralized management**
- **Dynamic Control**

Dynamic Channel & Power Assignment



System is running normally in a stable state

Dynamic Channel & Power Assignment

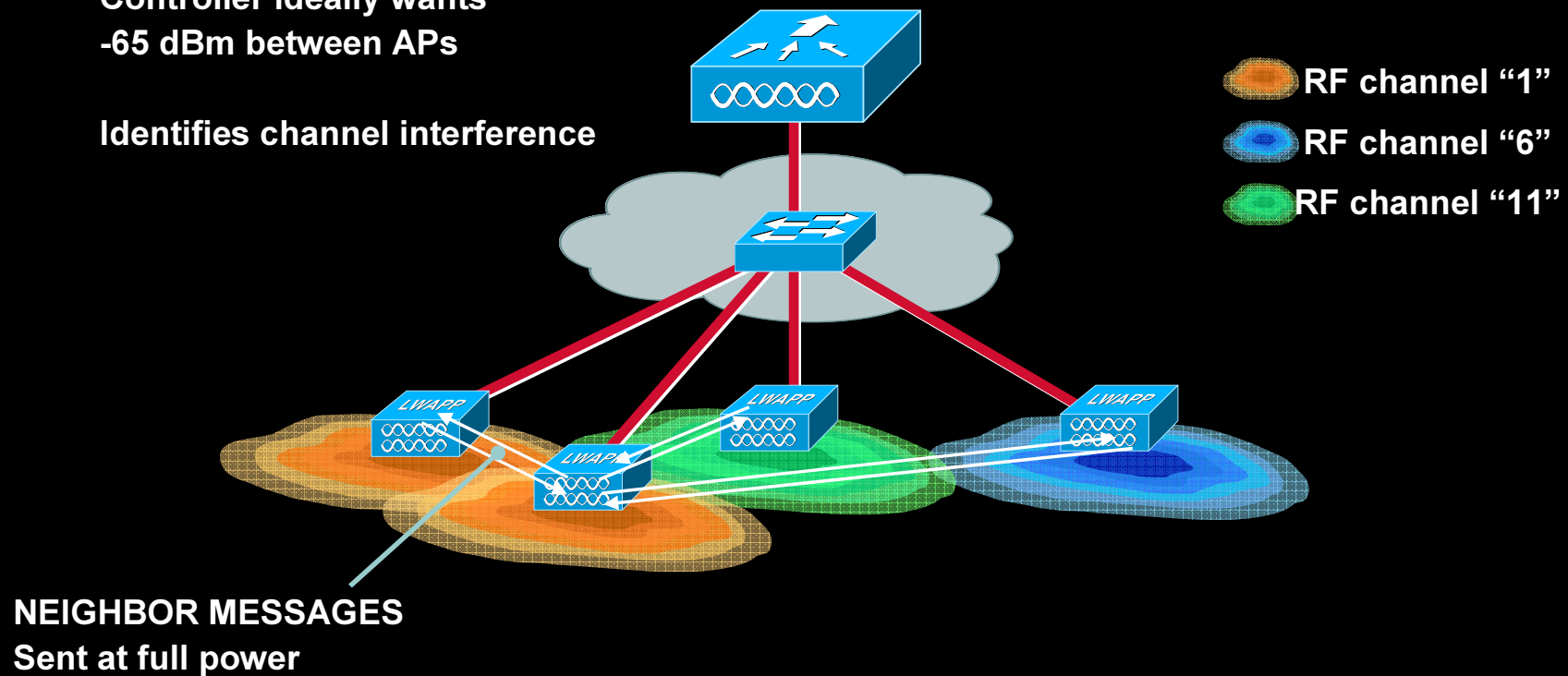


New AP is added to the system on channel 1

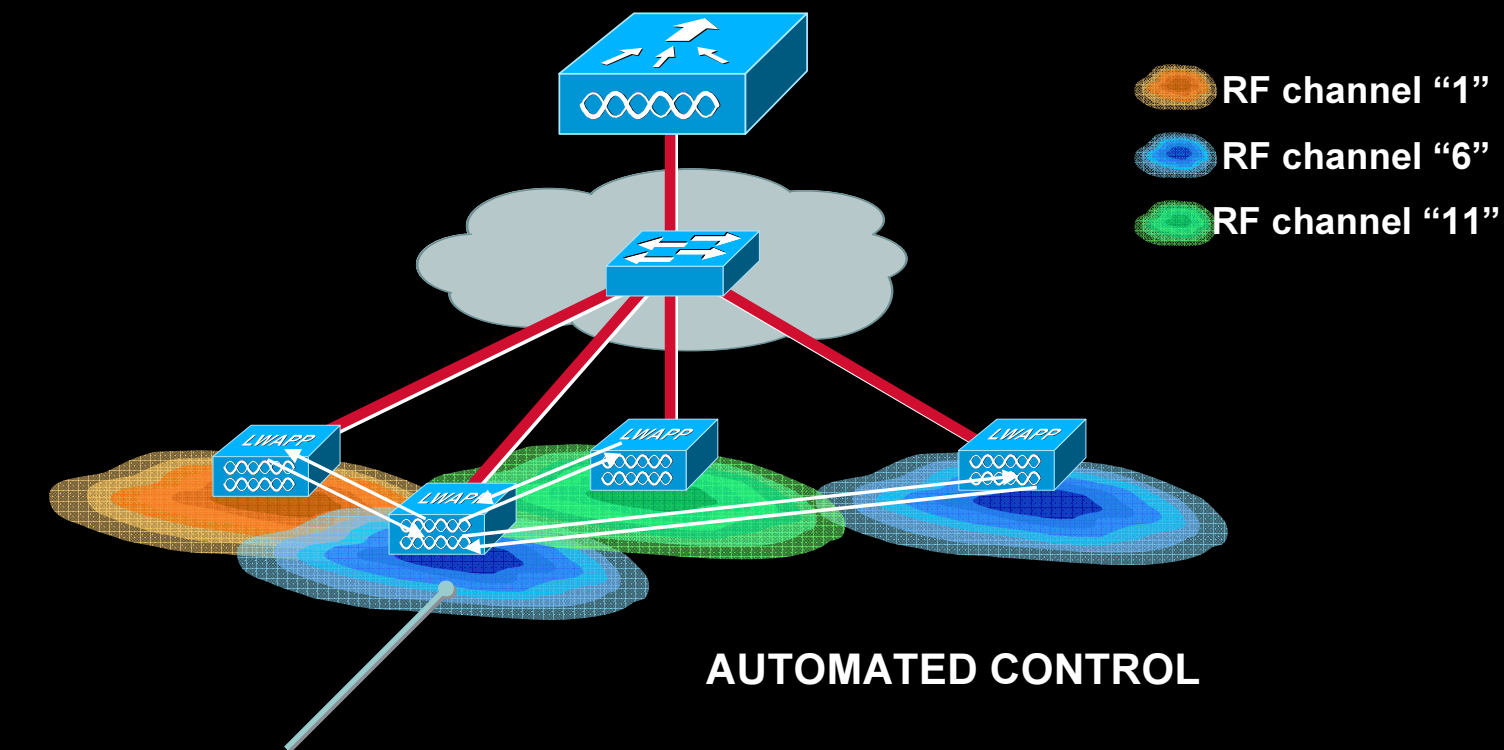
Dynamic Channel & Power Assignment

Controller ideally wants
-65 dBm between APs

Identifies channel interference



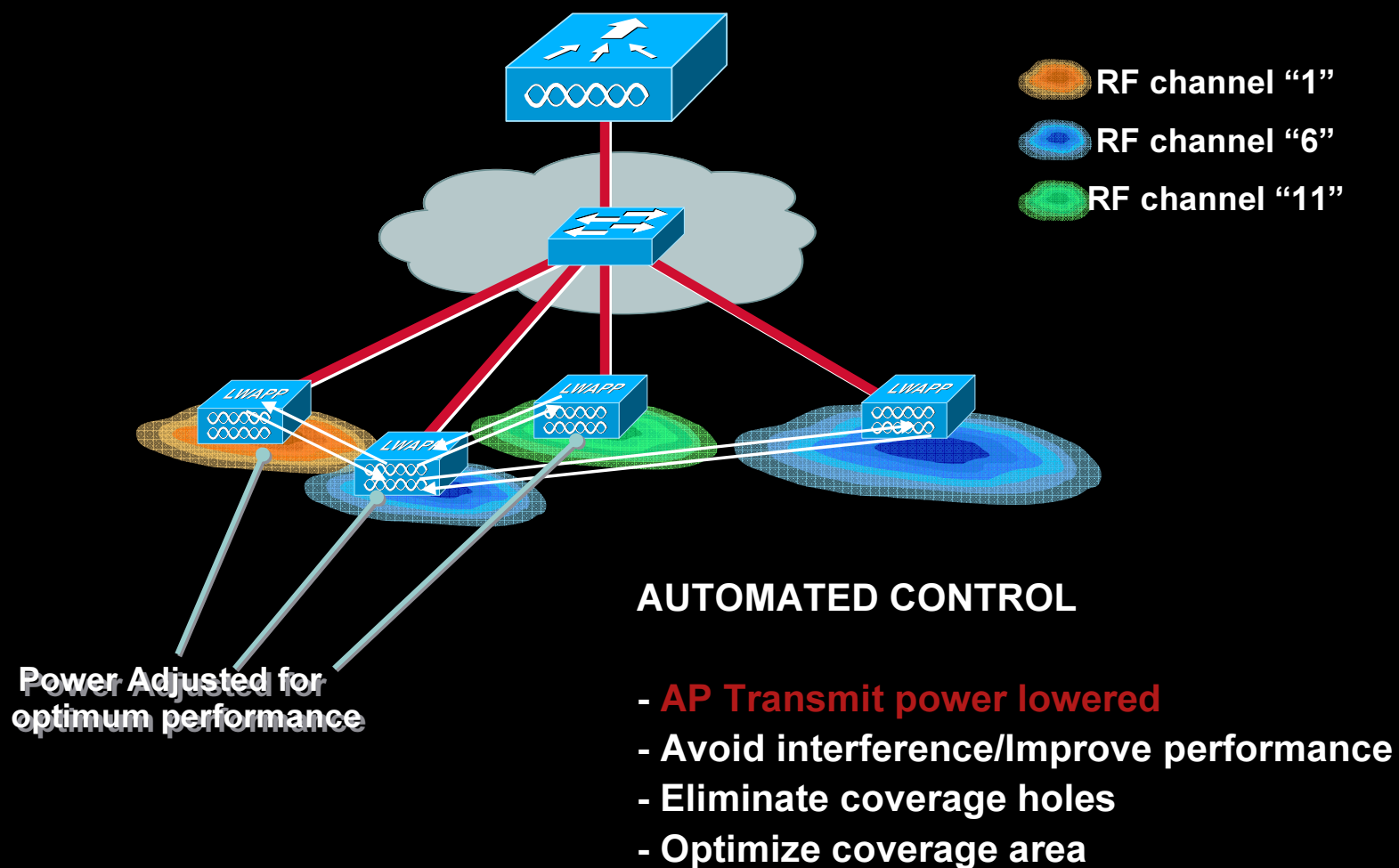
Dynamic Channel & Power Assignment



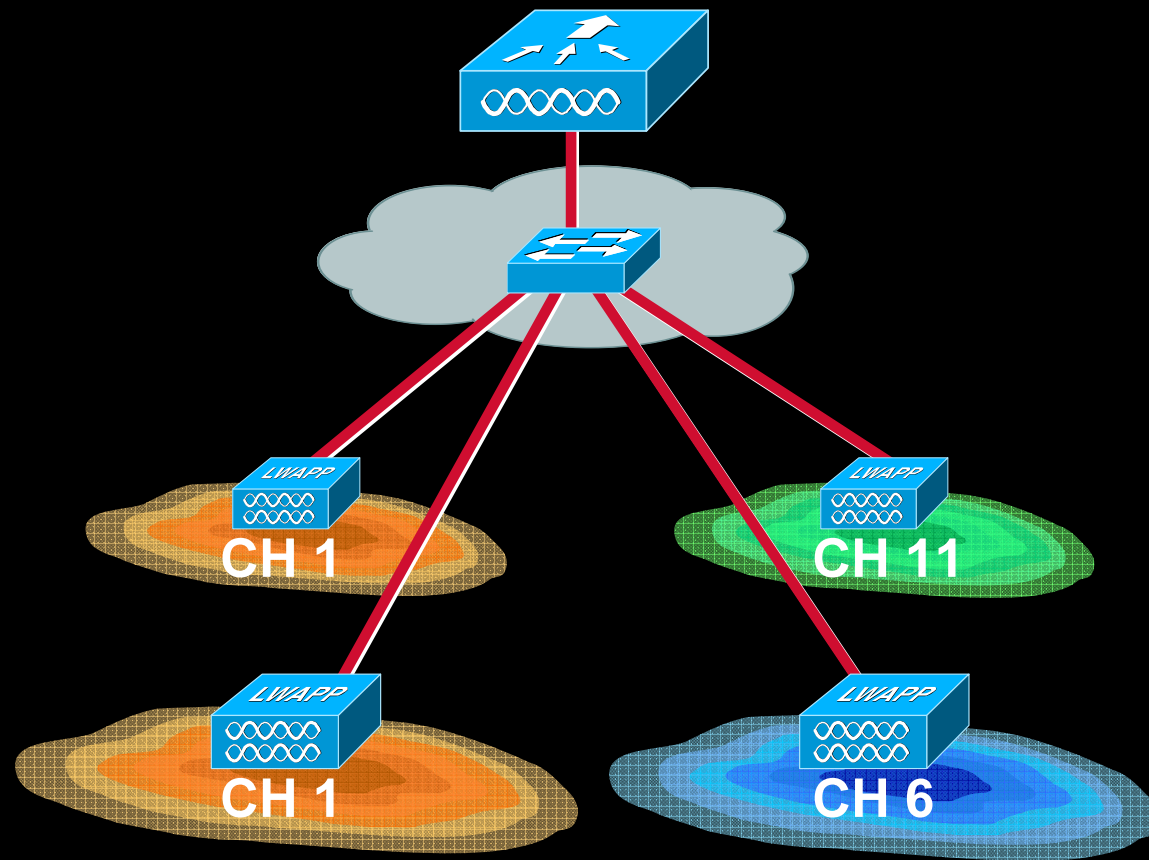
Channel changed to 6

- AP RF channel changed
- Avoid interference/Improve performance
- Eliminate coverage holes
- Optimize coverage area

Dynamic Channel & Power Assignment

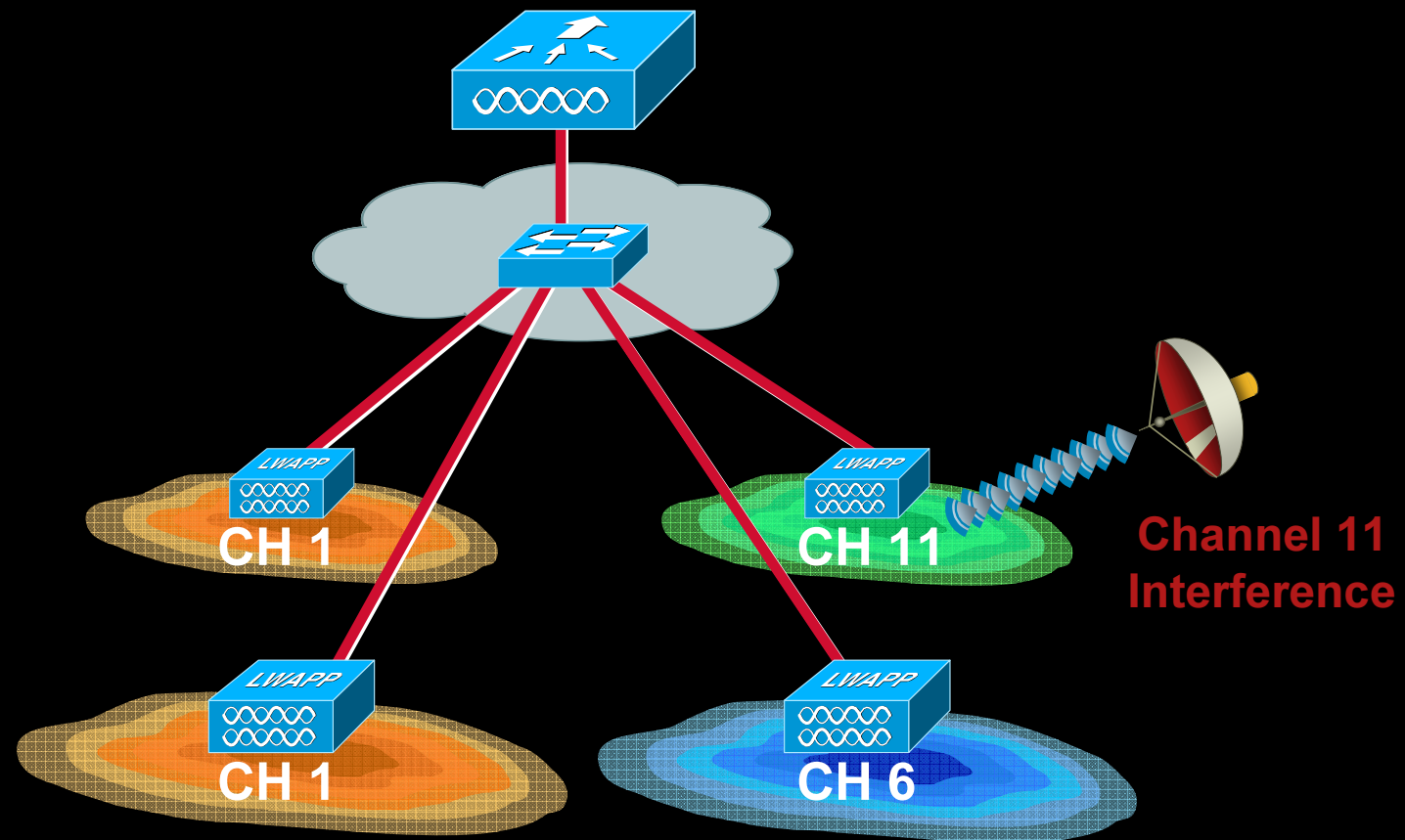


Interference Detection & Avoidance



System is running normally in a stable state

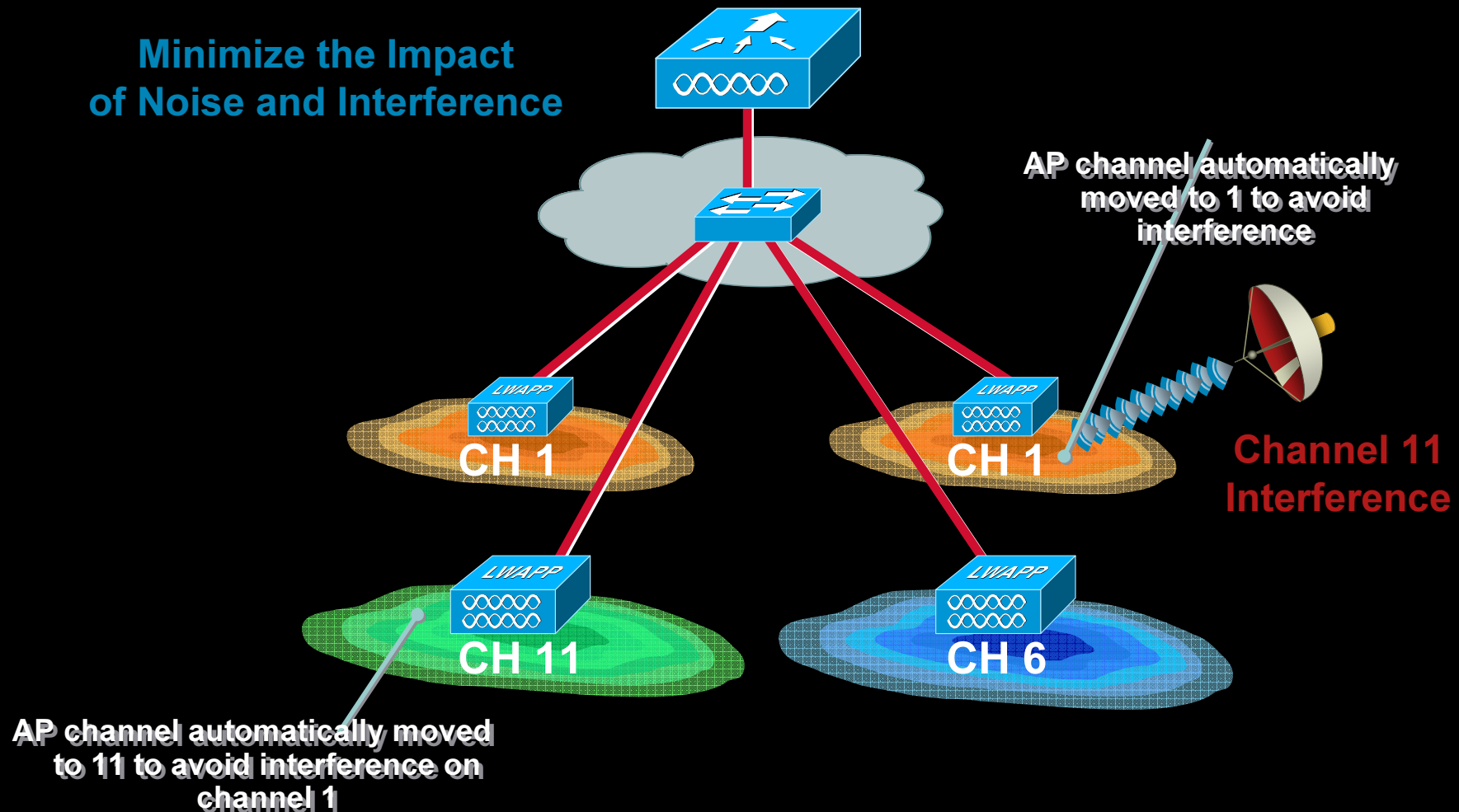
Interference Detection & Avoidance



Interference source on channel 11

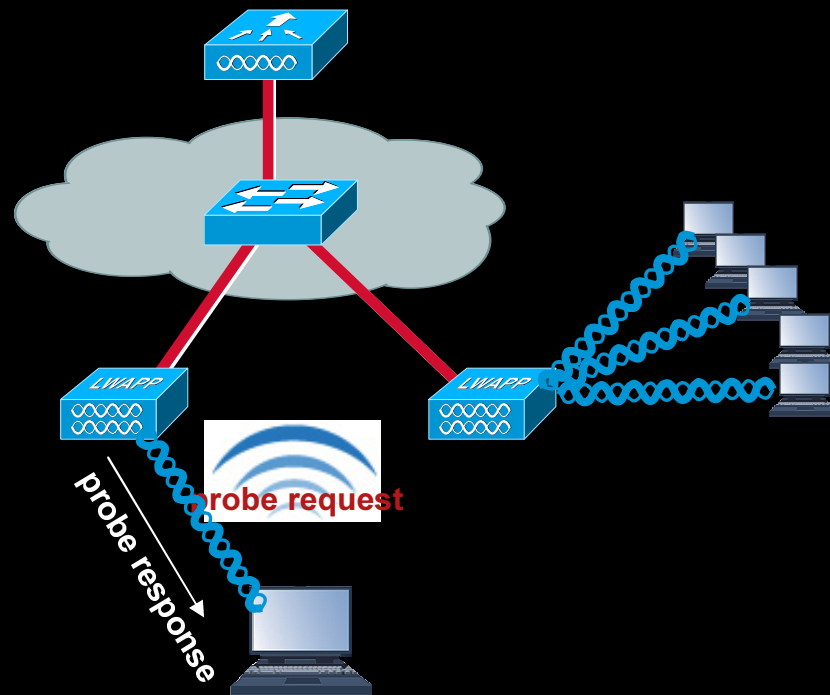
Interference Detection & Avoidance

Minimize the Impact
of Noise and Interference



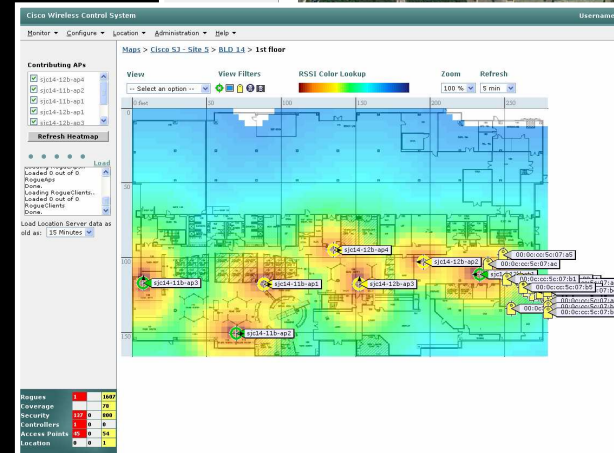
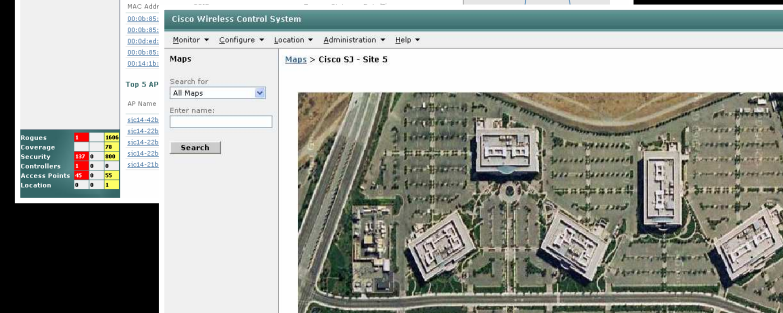
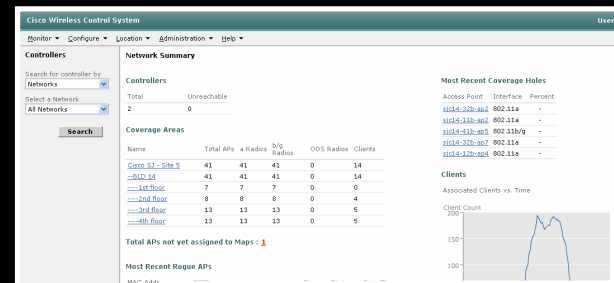
Client Load Balancing

- Client sends probe
- Controller determines best AP and ONLY IT sends probe response
- Client connects to AP



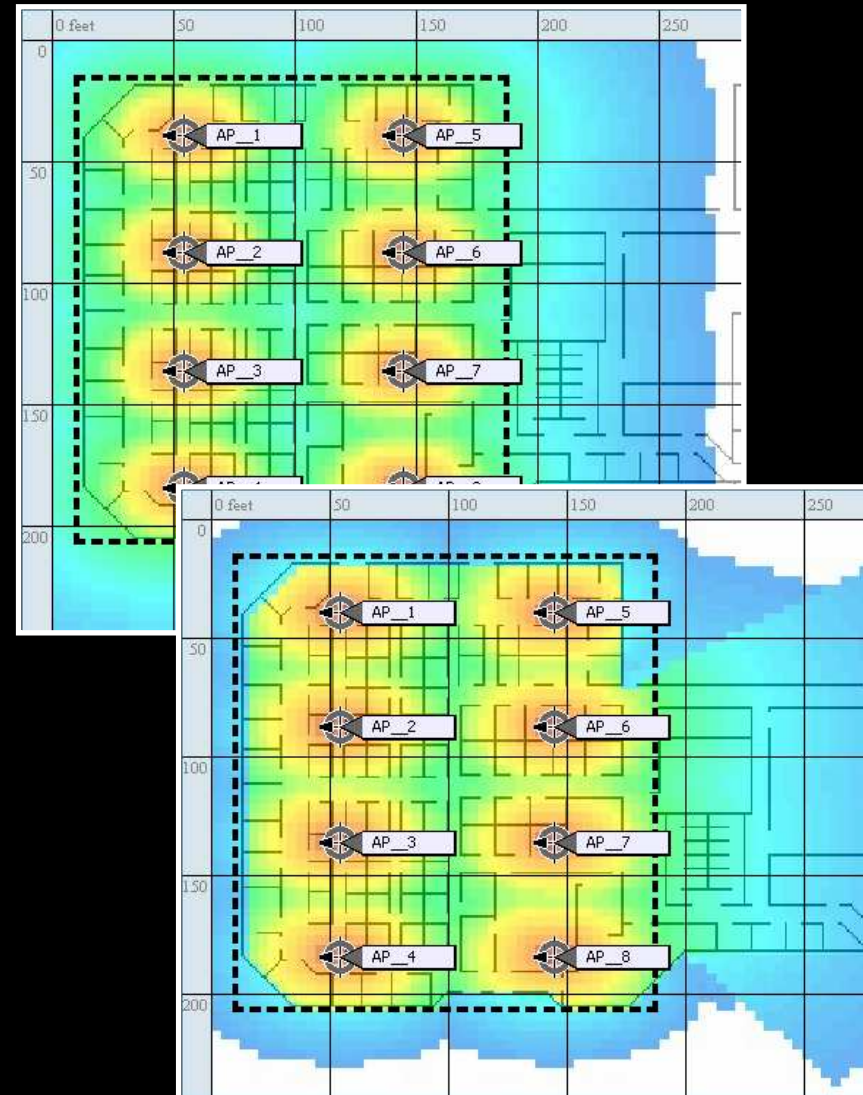
Cisco Wireless Control System (WCS)

- WCS is the management platform for Cisco's controller-based solution
- WCS is used for:
 - Network planning and ongoing monitoring
 - Real-time visibility and control of the air space
 - Unified policies that are centrally managed and enforced
 - Management of Cisco controllers and lightweight APs
- WCS is optional, but highly recommended when:
 - Multiple controllers are deployed, supporting numerous APs
 - Advanced WLAN services are deployed (IDS, location, voice, ...)



WLAN Planning Tool

- Optimize WLAN design for coverage or performance
- Assign RF characteristics to building material
 - Integrated floor plan editor
- WCS suggests optimal AP placement and graphically displays expected coverage area
- Printable reports
- Minimize the need for manual site survey



System Monitoring—Network Summary

Quick snapshot of all relevant system events

Administration Help
Username

Controllers

Search for controller by
Networks

Select a Network
All Networks

Search

Network Summary

Controllers

Total Unreachable
2 0

Controller Status

Coverage Areas

Name	Total APs	a Radios	b/g Radios	OOS Radios	Clients
Cisco SJ - Site 5	41	41	41	0	9
--BLD 14	41	41	41	0	9
---1st floor	7	7	7	0	0
---2nd floor	8	8	8	0	3
---3rd floor	13	13	13	0	2
---4th floor	13	13	13	0	4

Coverage Concerns

Rogue APs

Most Recent Rogue APs

MAC Address	SSID	Type	State	Date/Time
00:14:1c:83:6c:81	gueswlan	AP	Alert	5/19/06 9:28 AM
00:13:5f:55:f2:f1	d21peap	AP	Alert	5/19/06 9:28 AM
00:13:19:7b:d2:c1	orange12	AP	Alert	5/19/06 9:28 AM
00:13:5f:55:f2:f0	123	AP	Alert	5/19/06 9:28 AM
00:0b:85:09:93:3c	MibChangedTemplate	AP	Alert	5/19/06 9:28 AM

Top 5 APs

AP Name	Map Location	a Clients	b/g Clients	Total
sic14-22b-ap1	Cisco SJ - Site 5 > BLD 14 > 2nd floor	0	1	0
sic14-22b-ap4	Cisco SJ - Site 5 > BLD 14 > 2nd floor	0	1	0
sic14-21b-ap2	Cisco SJ - Site 5 > BLD 14 > 2nd floor	0	1	0
sic14-41b-ap6	Cisco SJ - Site 5 > BLD 14 > 2nd floor	0	1	0

Coverage Holes

Most Recent Coverage Holes

Access Point	Interface	Percent
sic14-32b-ap2	802.11a	-
sic14-11b-ap2	802.11a	-
sic14-41b-ap5	802.11b/g	-
sic14-32b-ap7	802.11a	-
sic14-12b-ap4	802.11a	-

Clients

Associated Clients vs. Time

Dashboard provides key alarms & events status display.

Current and historical client activity

Rogues	1	1609
Coverage	0	78
Security	138	800
Controllers	1	0
Access Points	45	53
Location	0	1

RF Monitoring—Floor Activity

Cisco Wireless Control System Username: s

Monitor > Configure > Location > Administration > Help >

Maps > Cisco SJ - Site 5 > BLD 14 > 1st floor

Contributing APs

- sjc14-12b-ap4
- sjc14-11b-ap2
- sjc14-11b-ap1
- sjc14-12b-ap1
- sjc14-12b-ap3

Refresh Heatmap

Load

Loaded 0 out of 0 RogueAps Done.

Loading RogueClients.. Loaded 0 out of 0 RogueClients Done.

Load Location Server data as old as: 15 Minutes

View: -- Select an option --

View Filters: RSSI Color Lookup

Zoom: 100 %

AP Filter

Total APs: 7

Protocol: 802.11b/g

Display:

- Names
- Channels
- Tx Power Level**
- Coverage Holes
- MAC Addresses
- Names
- Controller IP
- Utilization
- Profiles
- Users

Access Points > SJC14-42A-e330-MIAMI_BEACH-EAST > 802.11b/g

Access Point Details

General

AP Name: SJC14-42A-e330-MIAMI_BEACH-EAST-802.11b/g

AP MAC Address: 00:0b:85:1b:e3:30

Radio: 802.11b/g

Admin Status: Enable

Operational Status: Up

Power Level: 1

Controller: 10.32.30.4

Port: 1

Map Location: Cisco SJ > Building 14 > 14 - Floor 4

Profile Information

Noise Profile: Okay

Interference Profile: Issue

Load Profile: Okay

Coverage Profile: Okay

Noise by Channel (dBm)

Interference by Channel (% busy)

Load Statistics

Rx Utilization: 0%

Tx Utilization: 0%

Channel Utilization: 30%

Attached Client Count: 0

% Client Count vs RSSI

% Client Count vs SNR

Individual Client Usage Details

Client RSSI History (dBm)

Client CPU History

Rx Neighbors

MAC Address

- 00:0b:85:04:3c:a0
- 00:0b:85:1a:f2:a0
- 00:0b:85:23:2b:60
- 00:0b:85:23:36:a0
- 00:0b:85:23:37:80
- 00:0b:85:23:37:a0

Bytes Sent and Received (Kbps)

Packets Sent and Received (per sec)

AP status indicated by icon color.

APs and many fields are links to provide drill down details

Access Points	45	0	52
Location	0	0	1

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

Cisco Wireless Control System

Monitor | Configure | Location | Administration | Help

Security

Summary

Rogue APs

Rogue Clients

Shunned Clients

Security Summary

Rogue AP Details			Signature Attacks			AP Threats/Attacks					
Alert	Last Hour	24 Hours	Total Active	Last Hour	24 Hours	Total Active	Last Hour	24 Hours	Total Active		
Contained	0	0	0	Disassoc flood	2	34	1	Fake AP Attack	1	7	15
Threat	0	1	0	Assoc flood	0	0	0	AP Missing	0	0	0
Contained Pending	0	0	0	Bcast deauth	0	0	0	AP Impersonation	0	0	0
Known Contained	0	0	0	Broadcast Probe floo	0	0	0	AP Invalid SSID	0	0	0
Trusted Missing	0	0	0	Death flood	1	7	0	AP Invalid Preamble	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 Hour	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	596
				NetStumbler generic	0	0	0	WPA MIC Errors	0	2	119
				Reassoc flood	0	4	0	Shunned Clients	0	2	119
				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_S3C_14_LWAPP2/171.71.128.78	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:be: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:85:1
00:0b:85:5	00:0b:85:5

Rogues: 1
 Coverage: 78
 Security: 137
 Controllers: 1
 Access Points: 45
 Location: 0

Security Monitoring

Quick snapshot of all relevant security events

Rogue Detection

Alert Logs

Cisco Wireless Control System

Administration Help

Summary

Summary	Last Hour	24 Hours	Total Active
Rogue APs			
Rogue Clients			
Shunned Clients			

Rogue AP Details	Last Hour	24 Hours	Total Active
Alert	173	2084	1610
Contained	0	0	0
Threat	0	1	0
Contained Pending	0	0	0
Known Contained	0	0	0
Trusted Missing	0	0	0
802.11a	75	562	502
802.11b/g	128	940	596
On Network	0	5	1
Off Network	203	2227	1609
Adhoc	0	0	0

Signature Attacks	Last Hour	24 Hours	Total Active
Disassoc flood	2	34	1
Assoc flood	0	0	0
Boast deauth	0	0	0
Broadcast Probe floo	0	0	0
Deauth flood	1	7	0
Custom	0	0	0
EAPOL flood	0	16	0
NULL probe resp 1	0	0	0
NULL probe resp 2	0	0	0
NetStumbler 3.2.0	0	0	0
NetStumbler 3.2.3	0	0	0
NetStumbler 3.3.0	0	0	0
NetStumbler generic	0	0	0
Reassoc flood	0	4	0
Res mgmt 6 & 7	0	0	0
Res mgmt D	0	0	0
Res mgmt E & F	0	0	0
Wellenreiter	0	0	0

AP Threats/Attacks	Last Hour	24 Hours	Total Active
Fake AP Attack	1	7	15
AP Missing	0	0	0
AP Impersonation	0	0	0
AP Invalid SSID	0	0	0
AP Invalid Preamble	0	0	0
AP Invalid Encryption	0	0	0

Client Security	Last Hour	24 Hours	Total Active
Client Security Related			
Excluded Client Events	0	1	203
WEP Decrypt Errors	0	60	596
WPA MIC Errors	0	2	119
Shunned Clients	0	2	119
IPSEC Failures	0	0	0

Most Recent Security Alerts	Failure Object	Date/Time	Message
	Switch SJC 14 LWAPP2/171.71.128.78	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:bc: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:a4:0e: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	SSID	Type	State	Date/Time
	00:14:1b:5a:41:1f	secure-6	AP	Alert	5/19/06 9:46 AM
	00:14:1b:b6:7f:2e		AP	Alert	5/19/06 9:46 AM

Rogues	1		1609
Coverage			78
Security	137	0	800
Controllers	1	0	0
Access Points	45	0	57
Location	0	0	1

Dealing with Rogue APs

1. Review Rogue Alarm log
2. Assign alarm
3. Locate Rogue
4. Determine state of Rogue
5. Contain Rogue if a threat
6. Clear alarm

The screenshot displays the Cisco Wireless Control System interface. On the left, there are filters for Alarms, including Severity (All Severities), Alarm Category (Rogue AP), and Rogue AP State (Threat). A search bar is available for finding Rogue APs. The main panel shows details for a specific Rogue AP with MAC address 00:12:f0:56:a9:1d, including its vendor (Unknown), type (AP), and state (Threat). A summary table at the bottom left shows various metrics like Rogues (1), Coverage (1609), Security (136), etc. On the right, a floor plan map shows the location of the rogue AP, with RF fingerprinting data overlaid. A legend indicates that a Rogue's state can be Unknown - Alert, Known - Internal, or Unknown - External.

Alarms can be assigned for tracking.

A Rogue's state can be:
 Unknown - Alert
 Known - Internal
 Unknown - External

Annotation area to track resolution

RF Fingerprinting places rogue on map to 10 meter resolution

Rogues	1	1609
Coverage	0	78
Security	136	800
Controllers	1	0
Access Points	45	59
Location	0	1

Summary

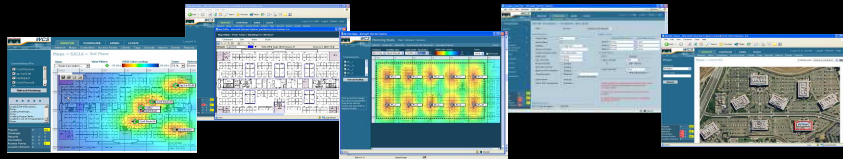
A Business Class Wireless Experience



**Cisco
Self-Defending
Network**

Unified Advanced Services

Unified built-in support of leading edge applications - not an after thought. Cisco Wireless Location Appliance, Cisco WCS, SDN, NAC, Wi-Fi phones, and RF firewalls.



World-Class Network Management

World Class NMS that visualizes and helps secure your air space. Cisco Wireless Control System (WCS)



Network Unification

Seamless network infrastructure across a range of platforms. Cisco 4400, 2000 Wireless LAN Controllers and Cisco Catalyst 6500 Series WiSM. ISR integration.



Mobility Platform

APs dynamically configured and managed through LWAPP. Cisco Aironet Access Points: 1500, 1300, 1240AG, 1230AG, 1130AG, 1000.



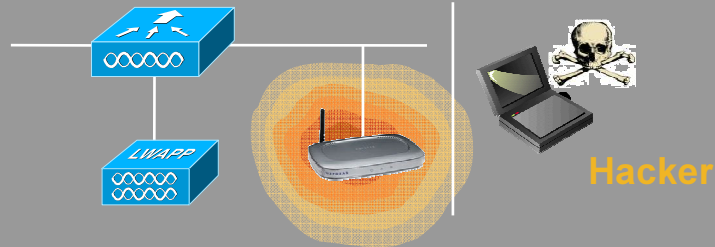
Client Devices

Secure clients that work out of the box. Cisco Compatible Client Devices & Cisco Aironet clients.

Summary

Top 4 Reasons for Deploying Wireless

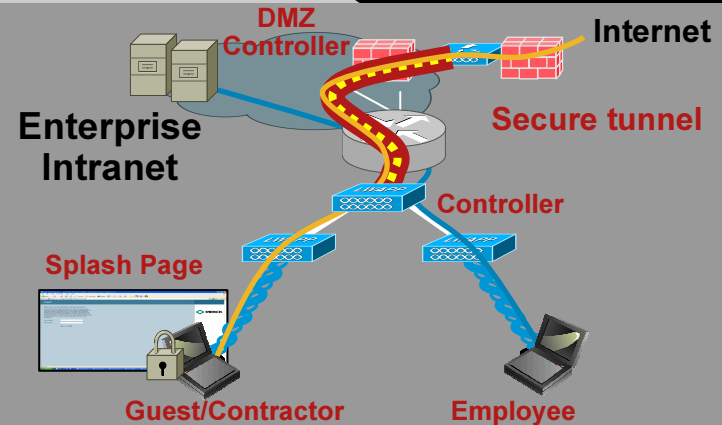
Security



Rogue APs—Employees create opening to enterprise network unknowingly

FTC FINES

Guest Access



Voice

- WiFi enabled voice
- 7921G, Blackberry, Treo
- Better coverage
- Reduced Cost
- Integrated with IP PBX



Location

Active IP Monitoring

Retail



Healthcare



Financial



Multi-Service Location

Voice Services



Compliance



Sensor Networks



www.cisco.com/go/wireless

Q&A

