

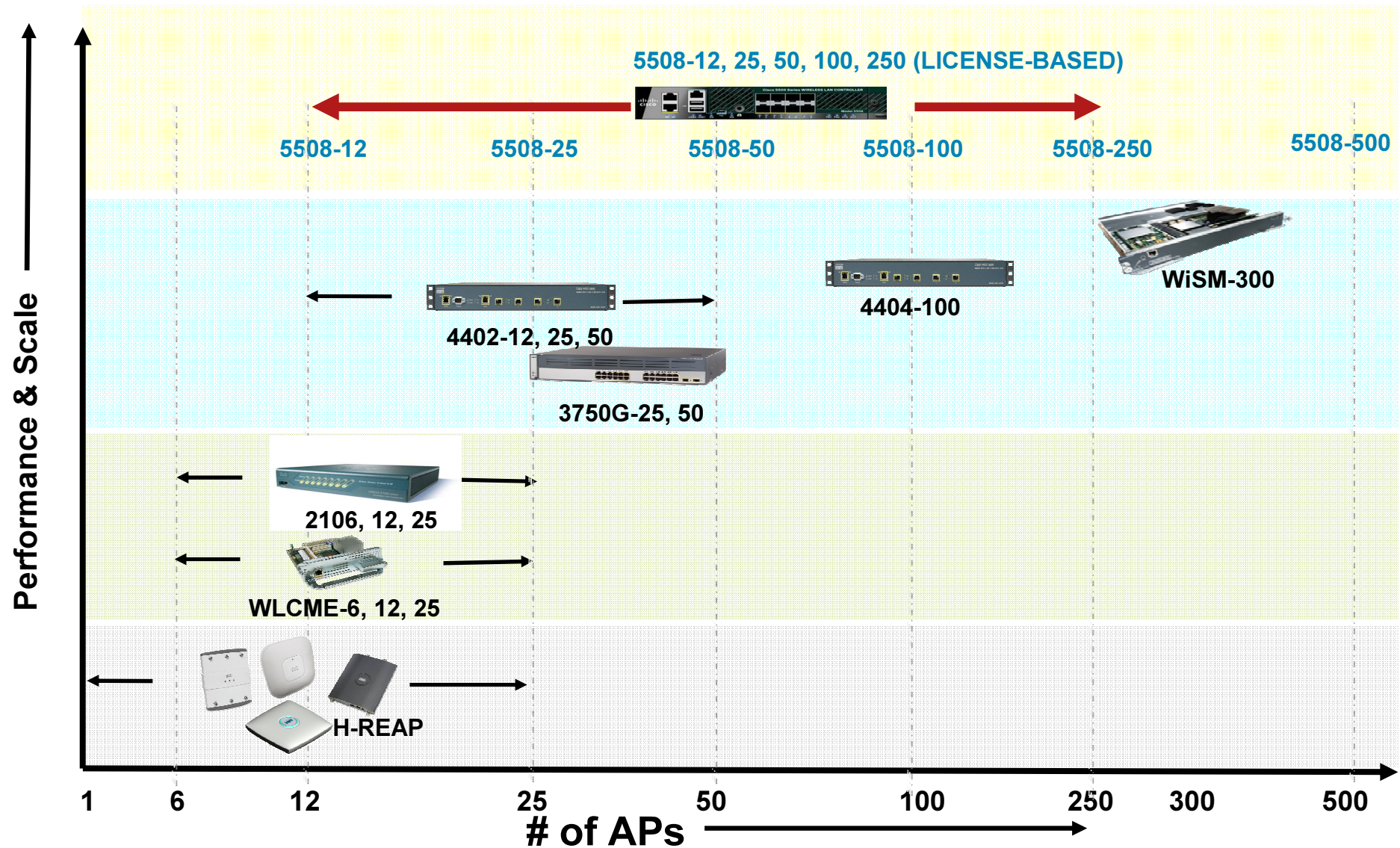


Wireless update



Dragan Novaković
dnovakov@cisco.com

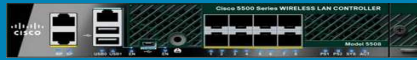

Wireless Controller Product Portfolio



Cisco 5500 Wireless Controller Features

	Scalability / Performance	Enhanced Mobility	Pay as you grow
Features	<ul style="list-style-type: none">▪ 8GB throughput – cleartext and encrypted▪ Up to 250 APs▪ 50 AP concurrent upgrade / join	<ul style="list-style-type: none">▪ 36,000 AP large mobility domain▪ Cisco M-Drive Technology with ClientLink▪ BandSelect▪ VLANSelect	<ul style="list-style-type: none">▪ AP count upgrade▪ Plus feature package▪ Demo license
Benefits	<ul style="list-style-type: none">▪ Wire-like performance for bandwidth intensive apps▪ <i>Reduced down-time</i>▪ Improved manageability – fewer controllers to manage	<ul style="list-style-type: none">▪ Fast mobility handoffs▪ Improved performance for 802.11a/g▪ Optimal RF and wired resource utilization▪ Extensive client compatibility and predictable roaming	<ul style="list-style-type: none">▪ Flexibility to invest as business needs grow▪ Investment protection▪ Lower entry level cost▪ Try and buy

Controller Comparison

	5500	4400
		
# of Access Points	Up to 250	12, 25, 50, 100
Throughput	Up to 8 Gbps	Up to 4 Gbps
Clients	Up to 7,000	Up to 5,000
Concurrent AP upgrades/joins	Up to 50	Up to 10
Network I/O	Up to 8, 1 Gbps SFPs	Up to 4, 1 Gbps SFPs
High speed I/O slot for future functionality	Yes	No
AP count upgrade via licensing	Yes	No
Functionality upgrade via licensing	Yes	No
Encrypted data link between AP and controller	Yes	No
OfficeExtend AP	Yes	No

Industry's Broadest Access Point Portfolio

Cisco Next Generation Wireless Portfolio

Cisco Aironet 1140 Series

Carpeted environment
1:1 AP1130 replacement
Performance under standard
802.3af power



Cisco Aironet 1250 Series

Challenging environment
Versatile RF coverage with
external antennas
Flexible power options for
optimal RF coverage



Indoor and Outdoor

Diverse Deployment Options



Cisco M-Drive Technology

1250 Power Options

Aironet® 1250



**Full 802.11n
Requires More
Than Standard
802.3af Power
over Ethernet**

Standard 802.3af PoE

Less Than Full Performance with Two Modules

Cisco Enhanced PoE

Full Performance

Power Injector

Full Performance

Local AC Power

Full Performance

Three PoE Modes Supported with 1250 AP

- Enhanced mode use ~18.5 Watts config port for 20 Watt

3560-E Cisco IOS Version 12.2(44)SE

3750-E Cisco IOS Version 12.2(44)SE

4500E—X4648E , X4648+E Cisco IOS Version 12.2(44)SG

1250 injector

- Optimized mode 16.8 Watts

6500—X6148, X6148A , X6548 Cisco IOS Version 12.2(33)SXH2

PoE daughter cards: WS-F6K-48-AF, WS-F6K-GE48-AF

- 802.3 af mode 15.4 Watts

Any 802.3af switch

Maximum Data Link Speed for Three PoE Modes

	2.4 GHz Mbps	5 GHz Mbps	Spatial Streams
Enhanced (18.5 Watts)	144	300	2
Optimized (16.8 Watts)	144	300	2
AF (15.4 Watts)	72	150	1

- Enhanced and optimized power mode deliver the same performance in 5 GHz because uses two spatial streams
- Enhanced and optimized power mode deliver same performance in 2.4 GHz for dense deployments

The difference is Optimized Max TX drops from 20 dBm with EPoE to 14dBm with Optimized

Access Point EOL Topics

- **AP112x/121x/123x Series**

EoS date: Jun 18th, 2009

EoSM date: Jun, 2011

Enhanced CTMP Program to migrate

Inter-release controller mobility in H-MR1

Trade-In Product Families	Trade-To	Previous Std CTMP %	New CTMP %
10x0, AS-1200%, 112x, 1230	1130/1240	10%	15%
10x0, AS-1200%, 112x, 1230	1250/1140	10%	25%

Cisco 890 Integrated Services Routers



For Small Office, Small Business, or Enterprise Teleworker

Autonomous SW - 12.4(10)JDA3

Unified Image 5.2 (Grgich Hills)

- 2.4 and 5 GHz 802.11n wireless with captive 2.4 & 5 GHz Omni dipole antenna based on AIR-ANT4941
- Dedicated AP processor, memory, and Cisco IOS image
- Default Autonomous Mode, upgradeable to Unified mode (LWAPP)

Full compatibility with CUWN using WLC & WCS

Feature & roadmap parity with AP1250

H-REAP mode support for Branch Office and Teleworker Solutions

- **Combines Internet access, security and wireless services onto a single device**
- **WAN/LAN Technologies**
 - Fast Ethernet, Gig Ethernet
 - ISDN for Primary or Backup
 - 802.11n WLAN and Unified Management
- **Comprehensive Routing & Security**
 - Included as default Advanced IP Services
 - IPSec acceleration: DMVPN, GET VPN,
 - Easy VPN
 - Firewall, IPS, SSL-VPN
 - Content Filtering (Licensed-based)
- **Comprehensive Cisco IOS Routing, QoS and network management**
- **Ease of Management**
 - Cisco Configuration Professional
 - Cisco Works
 - Unified Wireless Management

CISCO 890 Series

Memory

Flash
Default: 128 MB
Max: 256 MB

DRAM
Default: 512 MB
Max: 768 MB

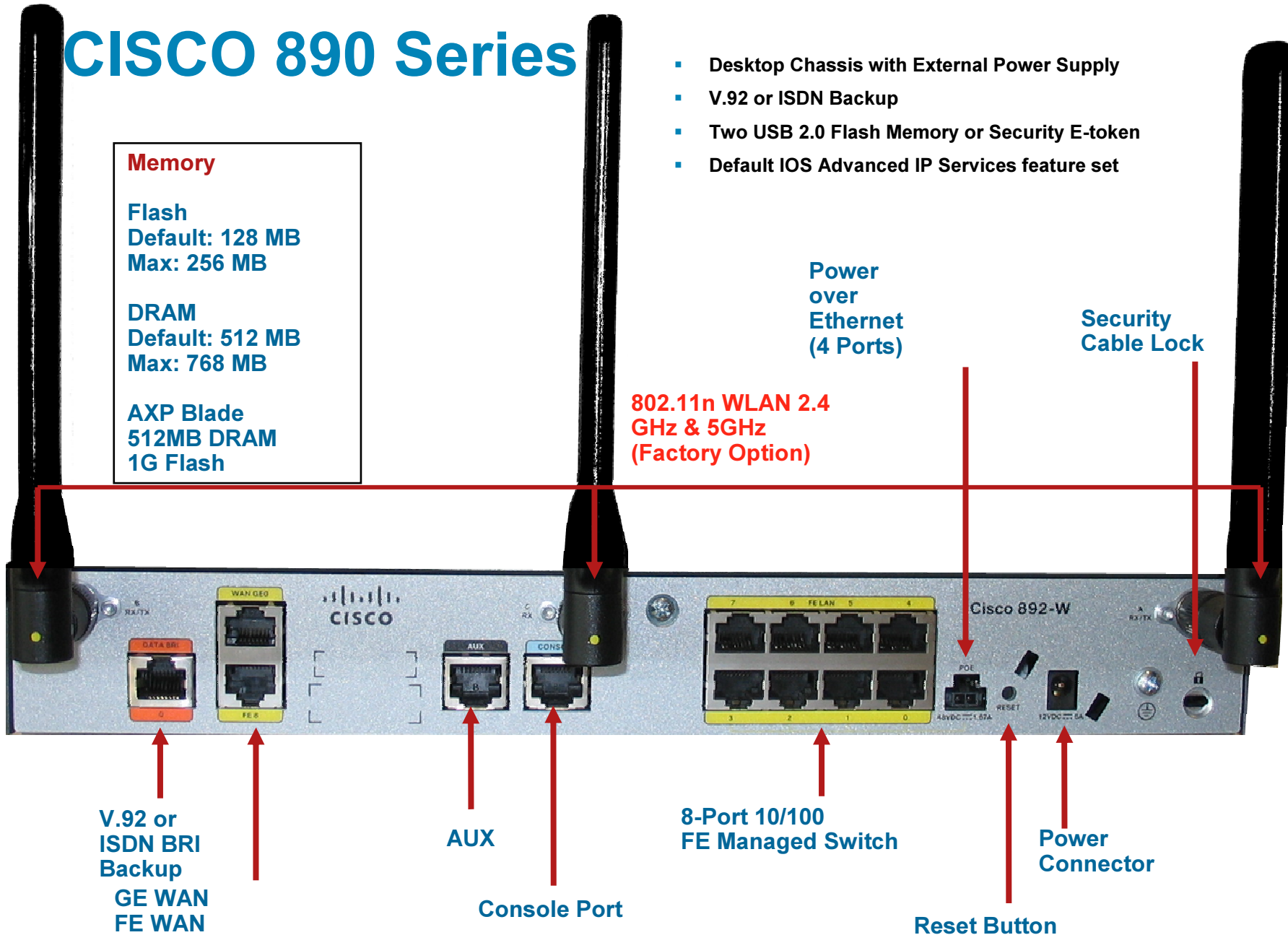
AXP Blade
512MB DRAM
1G Flash

- Desktop Chassis with External Power Supply
- V.92 or ISDN Backup
- Two USB 2.0 Flash Memory or Security E-token
- Default IOS Advanced IP Services feature set

Power
over
Ethernet
(4 Ports)

Security
Cable Lock

802.11n WLAN 2.4
GHz & 5GHz
(Factory Option)



V.92 or
ISDN BRI
Backup
GE WAN
FE WAN

AUX




Console Port

8-Port 10/100
FE Managed Switch

Reset Button

Power
Connector

Cisco Integrated APs in Next Gen ISR - Comparison

Product	 Cisco 860	 Cisco 880	 Cisco 890
802.11 modes supported	802.11b/g/n	802.11b/g/n	802.11a/b/g/n (Dual Mode)
Antennas	MIMO	MIMO	MIMO
Dual-mode antennas	No	No	Yes
Removable antennas	No	No	Yes
AZR support	Yes	Yes	Yes
Number of SSIDs and wireless VLANs	10/2	16/8	16/8
LEAP, PEAP, EAP-TLS, 802.1x, static and dynamic WEP, PSK, WPA, TKIP/SSN, MAC auth, survivable local auth, RADIUS	Yes	Yes	Yes
WiFi and WMM Certifications	Yes	Yes	Yes
Universal Client Mode	No (Workgroup Bridge)	No (Workgroup Bridge)	No (Workgroup Bridge)
802.11 Bridging	Yes	Yes (autonomous)	Yes (autonomous)
Autonomous/Unified Support	Autonomous only	Autonomous and Unified	Autonomous and Unified
WAN options	FE	ADSL/G.SHDSL/FE/3G	FE/GE
Management	CCP, SDM, CLI, WCS	CCP, SDM, CLI, WLC, WCS	CCP, SDM, CLI, WLC, WCS
Availability	Available today	Available today	Available today



802.11n

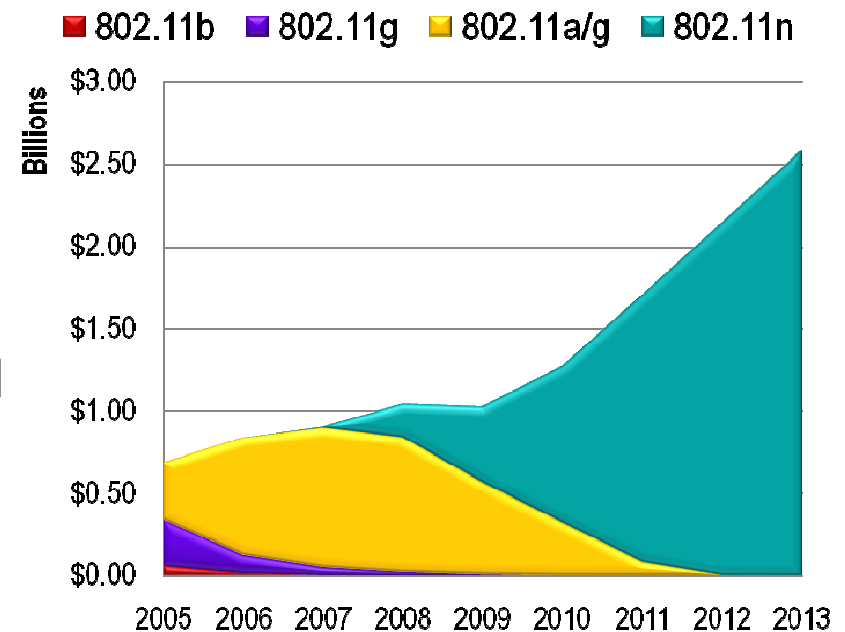


802.11n Ratification



- Sept 11, 2009 final ratification
- Cisco helped standardization and rapid adoption of 802.11n
- 500K Cisco draft 2.0 802.11n enterprise-grade APs
- 800+ devices certified with draft 2.0 against AP1250 in the WFA test-bed
- Enhanced enterprise-specific scenarios tested with Intel, Apple, Nokia and others in Assurewave

WW – Enterprise AP Revenues



Source: Dell'Oro Group, Q1CY'09

Goals of the IEEE 802.11n Standard

Performance

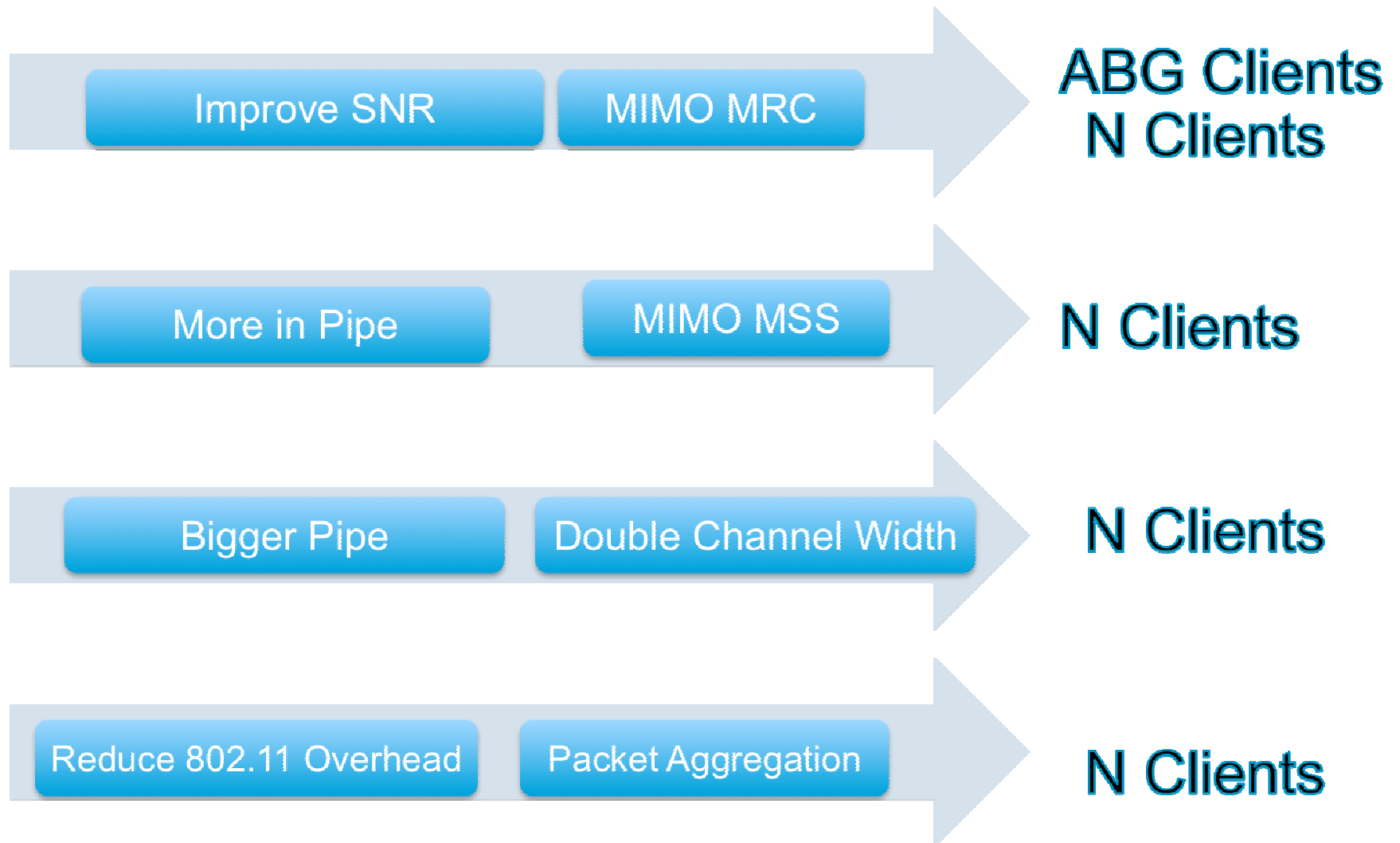
- Performance parity with 100 Mbps fast Ethernet
- Improved reliability
- Backward compatibility with A/B/G
- Improved immunity to noise

What Does the 11n Ratification Mean?

- Barrier to adoption has been removed
- Final 802.11n is backward compatible with a/b/g and Draft 2.0
- WFA Grand-fathering existing products
 - Draft 2.0 products are eligible to use the 802.11n logo without retesting
 - No hardware or software changes required for Cisco Aironet 1140 and 1250 Series Access Points
- Zero mandatory features beyond draft 2.0



Key Approaches 802.11n Uses to Improve Performance



MIMO (Multiple Inputs Multiple Outputs)

- 802.11n it is mandatory requirement to have at least two receivers and one transmit per band

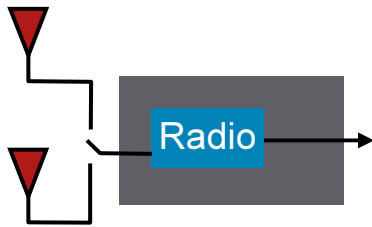
Optional to support up to four TXs and four RXs

- MRC—Maximum ratio combining
- MSS—Multiple spatial streams—spatial multiplexing
- BF—Beam forming

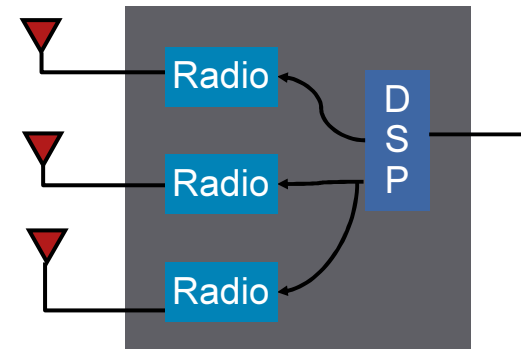
Note: MIMO provides improvements for non-n802.11 clients

*

Comparing SISO and MIMO Signal Reception

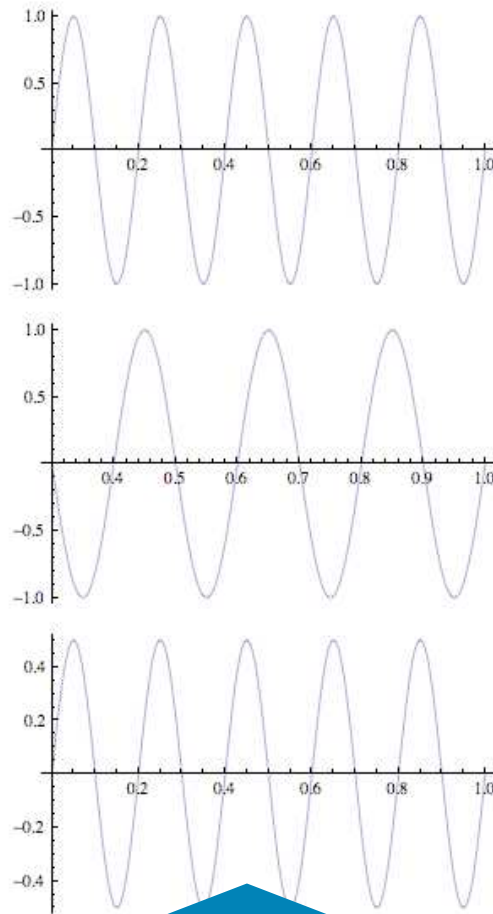


- One radio chain
- Multipath degrades

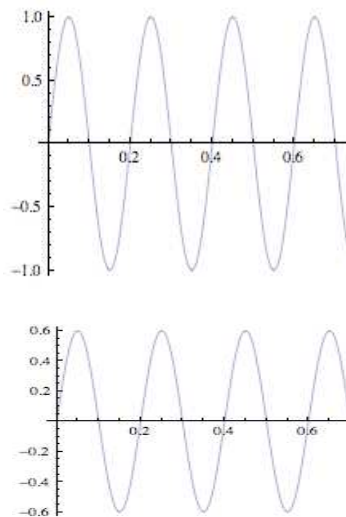


- Three radio chains
- Multipath improves
- Better immunity to noise
- Better SNR than SISO

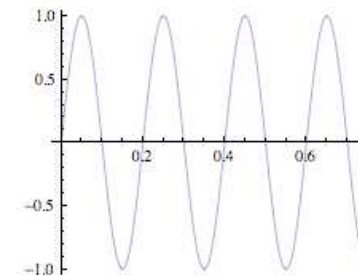
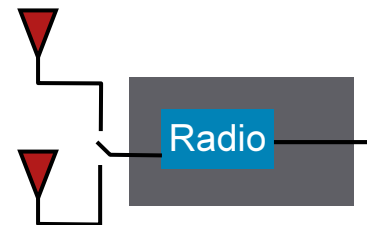
Illustration of Three Multipath Reflections to SISO AP



**Multipath
Reflections of
Original Signal**

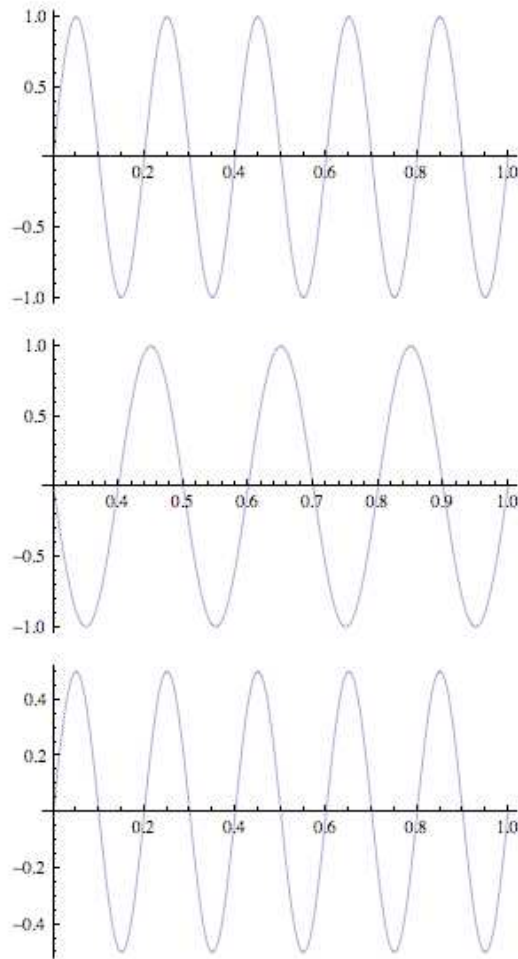


**Signal Each
Antenna Sees
Due to
Multipath Effect**

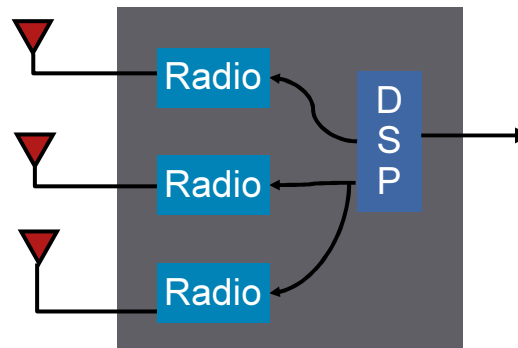


**Radio Switches
to Best Signal
with Least
Multipath Effect**

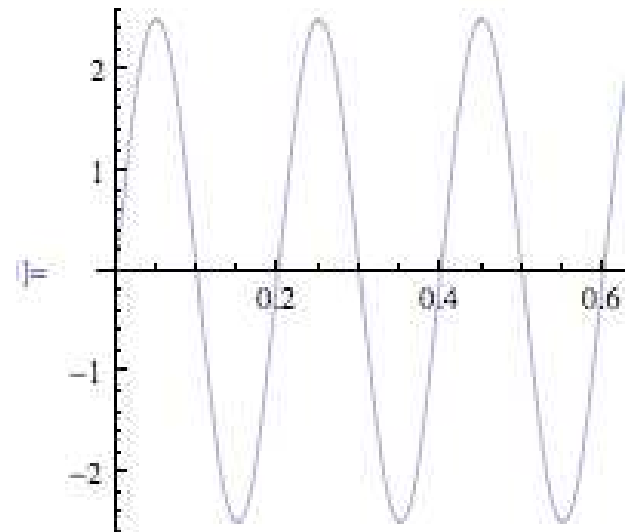
Illustration of Three Multipath Reflections to MIMO AP with MRC



**Multipath Reflections
of Original Signal**



**The DSP Adjusts
the Received Signal
Phase So They Can
Be Added Together**



**The Resulting Signal
Is Addition of
Adjusted Receive
Signals**

Introducing M-Drive with ClientLink

Beam Forming enhances mixed mode client performance

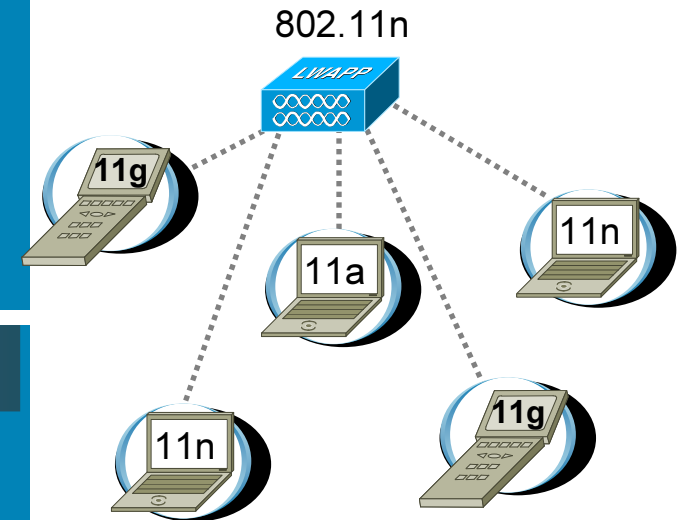


Challenge

- 11ag clients consume valuable “airtime”, limiting performance in mixed mode client environments
- Client refresh cycles over 3-5 years
- MIMO inherently only improves uplink performance

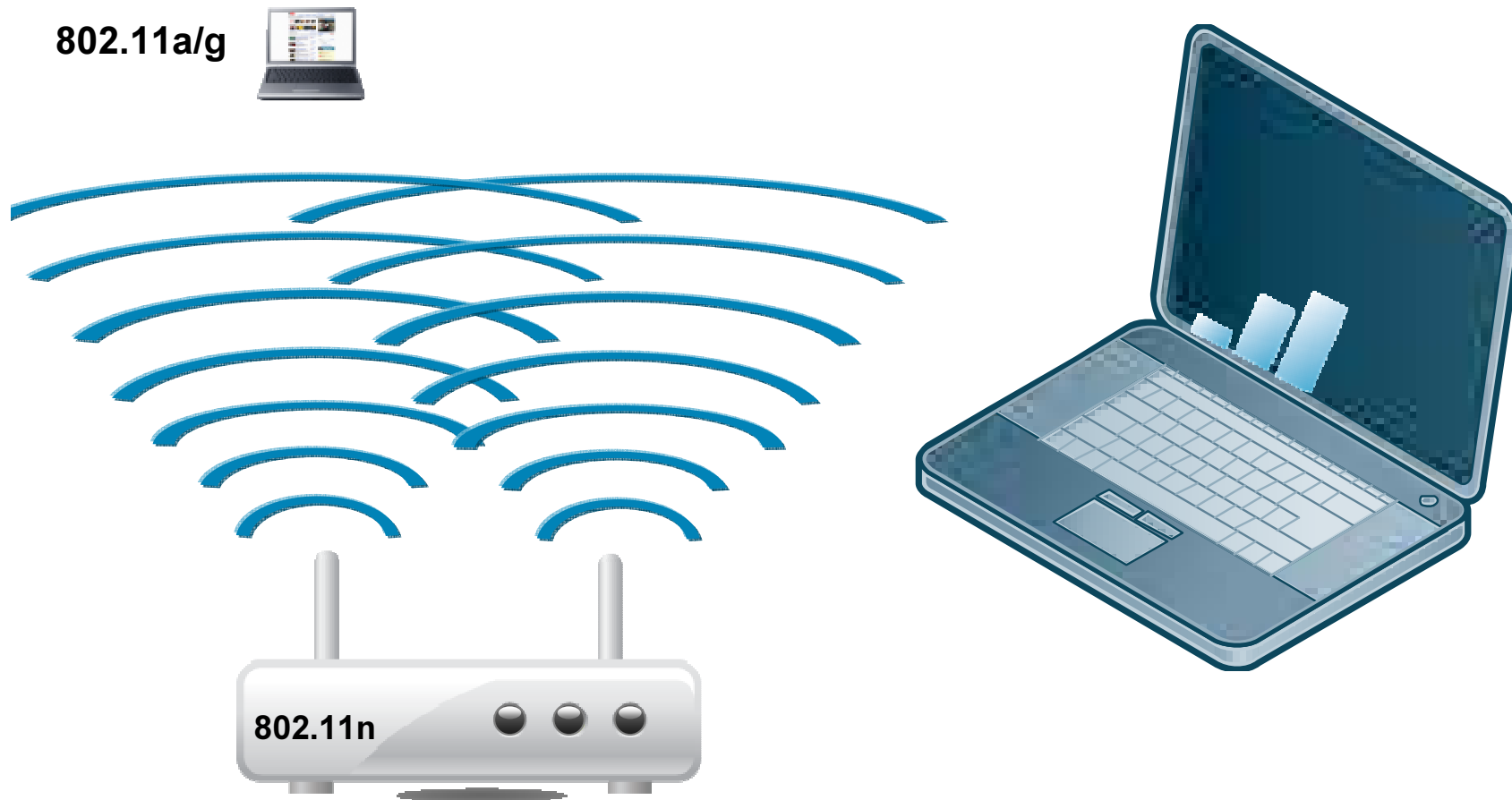
Solution

- Beam forming focuses signal exclusively to each standards based 11ag client
 - Up to 65% higher throughput for 802.11a/g clients
 - 27% higher overall system capacity
 - Reduces coverage holes in challenging RF environments



The Problem

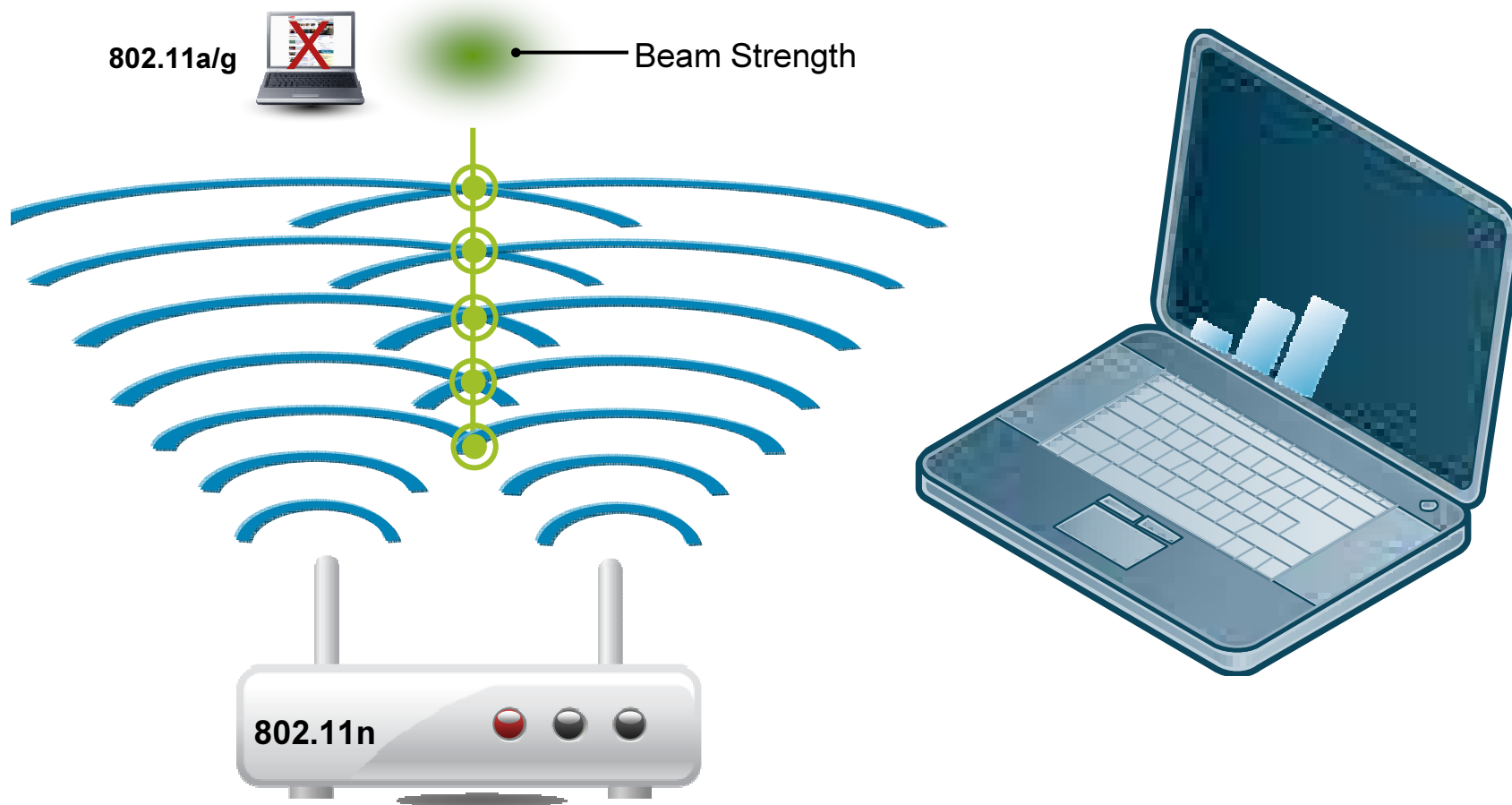
Beam Strength Not Directed to Client



**802.11a/g Client Connection Not Optimized,
Creates Coverage Hole**

The Problem

Beam Strength Not Directed to Client

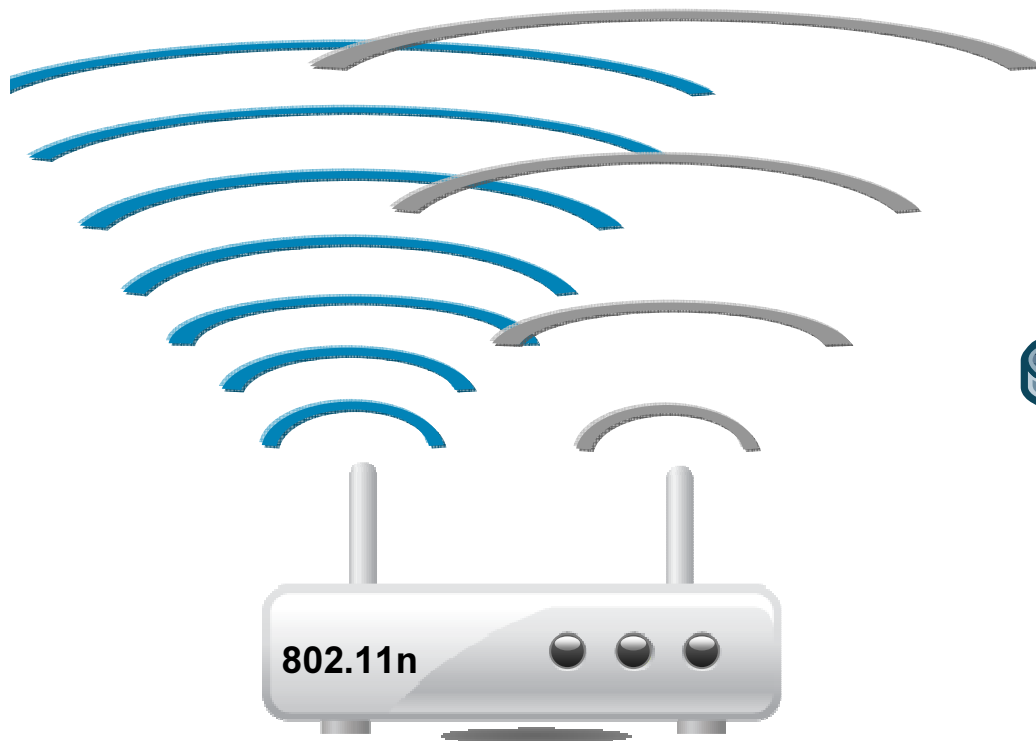


**802.11a/g Client Connection Not Optimized,
Creates Coverage Hole**

The Solution

Cisco Innovation: ClientLink

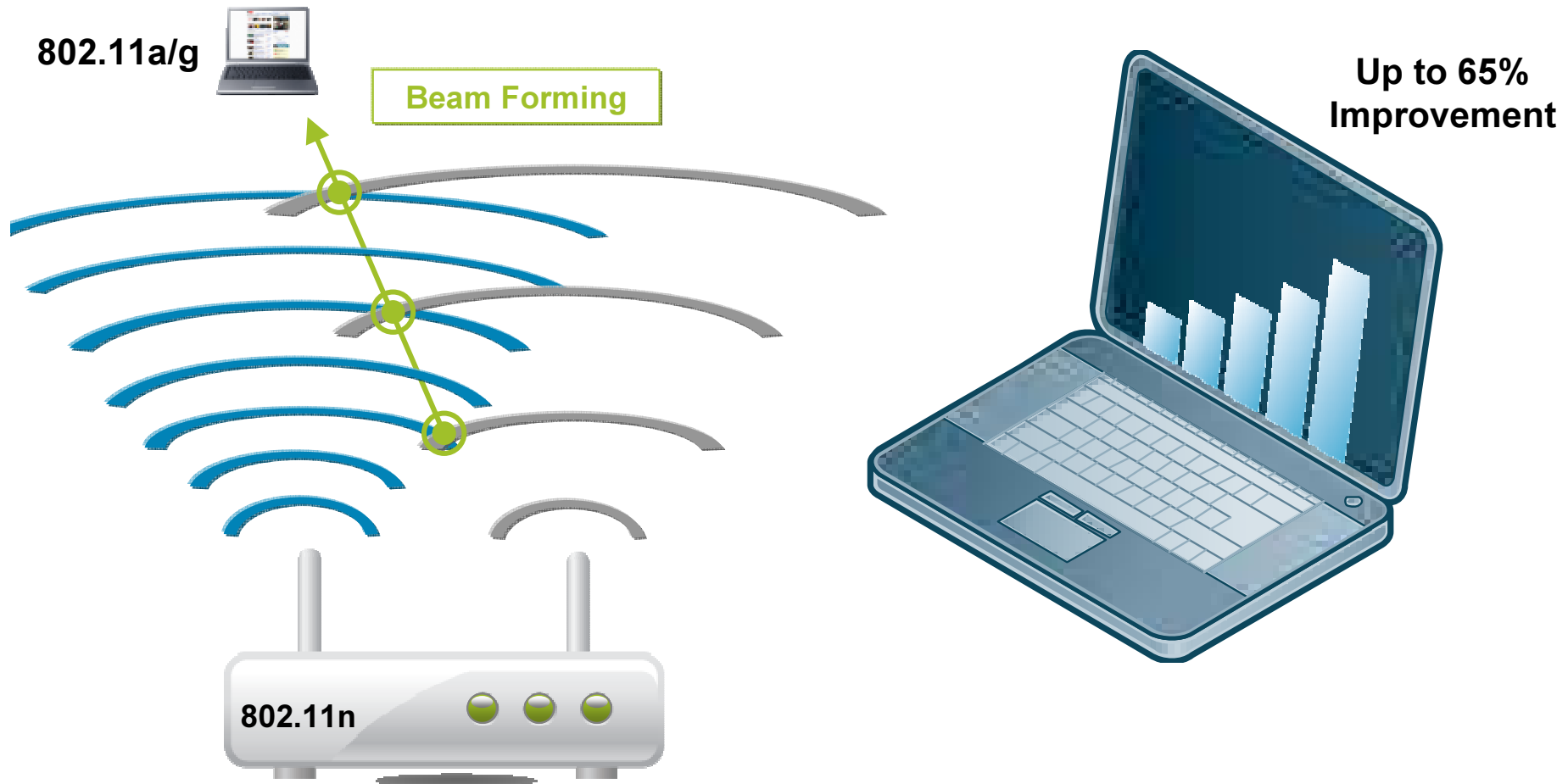
802.11a/g



**Intelligent Beam Forming Directs Signal to
Improve Performance and Coverage for 802.11a/g Devices**

The Solution

Cisco Innovation: ClientLink



Intelligent Beam Forming Directs Signal to Improve Performance and Coverage for 802.11a/g Devices

Benefit #1: Higher Throughput per 11a/g Device

Miercom

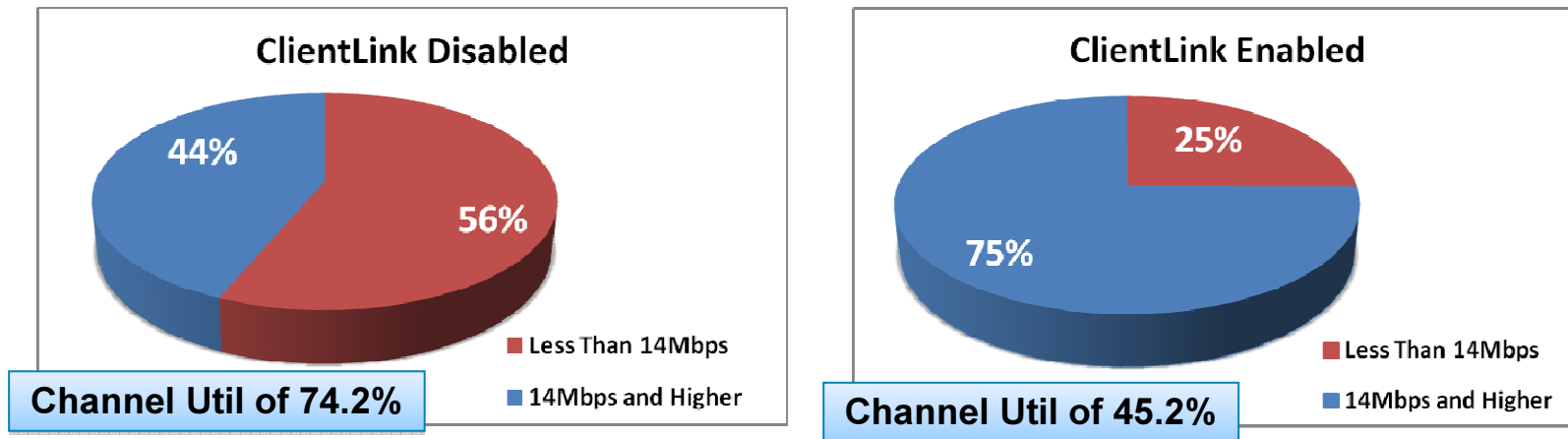
Up to **65%** Increase in Throughput



Test: 802.11a/g device with 802.11n network
Source: Miercom

Benefit #2: Higher System Capacity

Up to **27%** Improvement in Channel Capacity **Miercom**



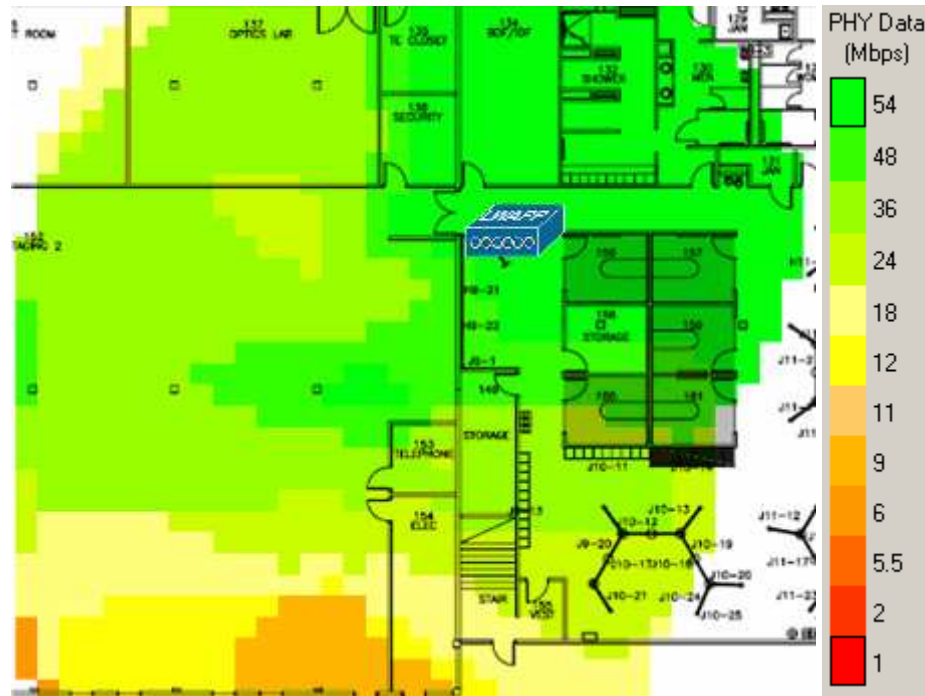
- Faster data transmission, less retries = more efficient use of RF channel.
- Faster 11a/g transactions opens airtime for 11n devices, providing them improved experience

Test: 802.11a/g device measured at 16 antenna orientations w/ 802.11n network
Source: Miercom

Benefit #3: Reduced Coverage Holes

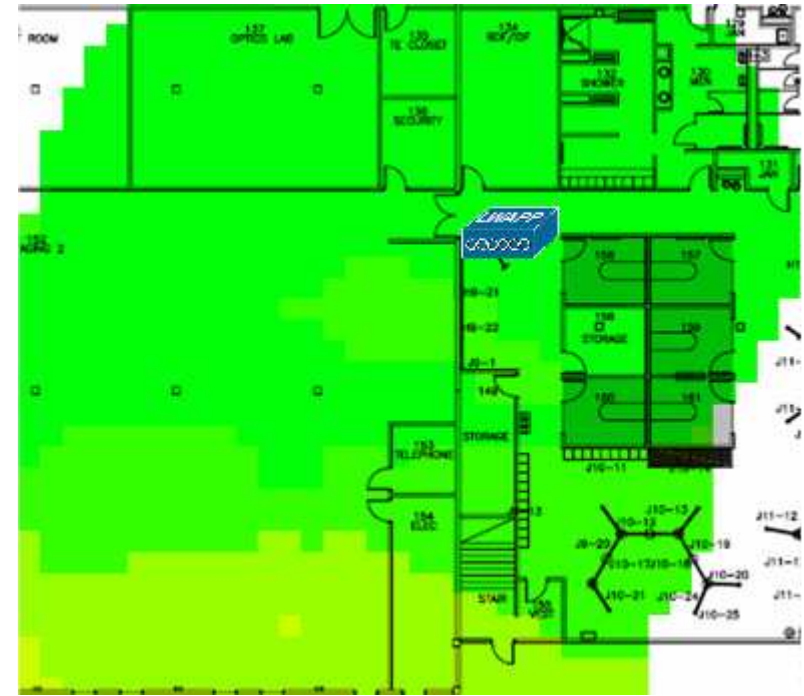
Miercom

ClientLink Disabled



Lower Data Rates

ClientLink Enabled



Higher Data Rates

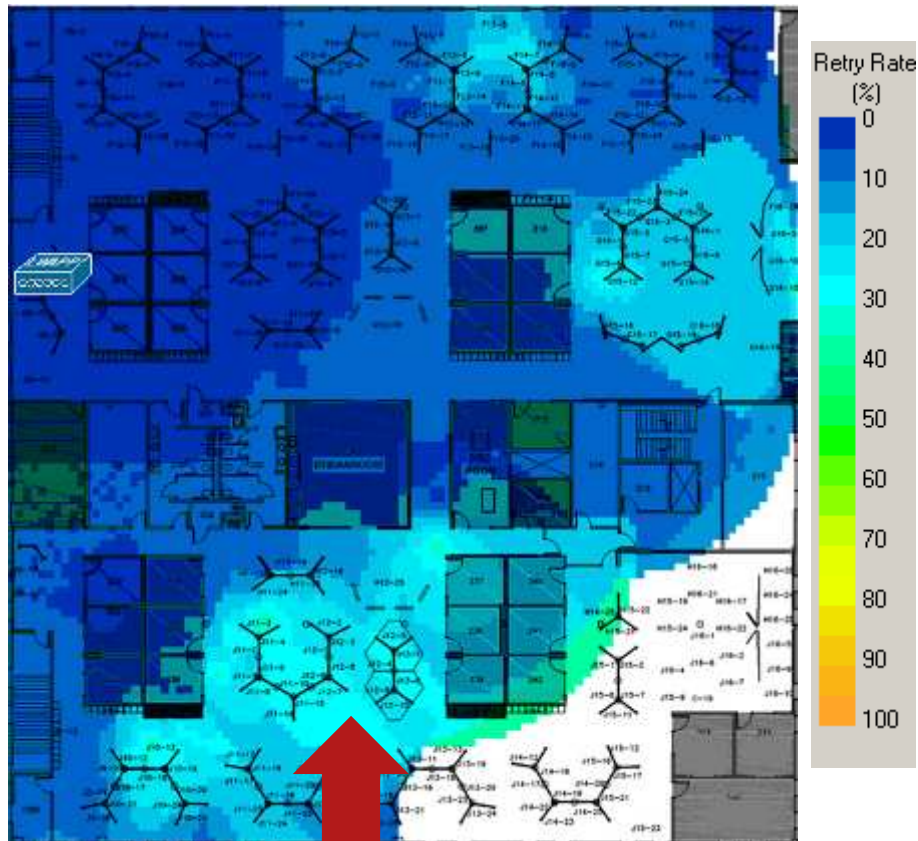
Source: Miercom; AirMagnet 6.0 Iperf Survey

Benefit #3: Reduce Coverage Holes (Cont.)

Lower retry rates

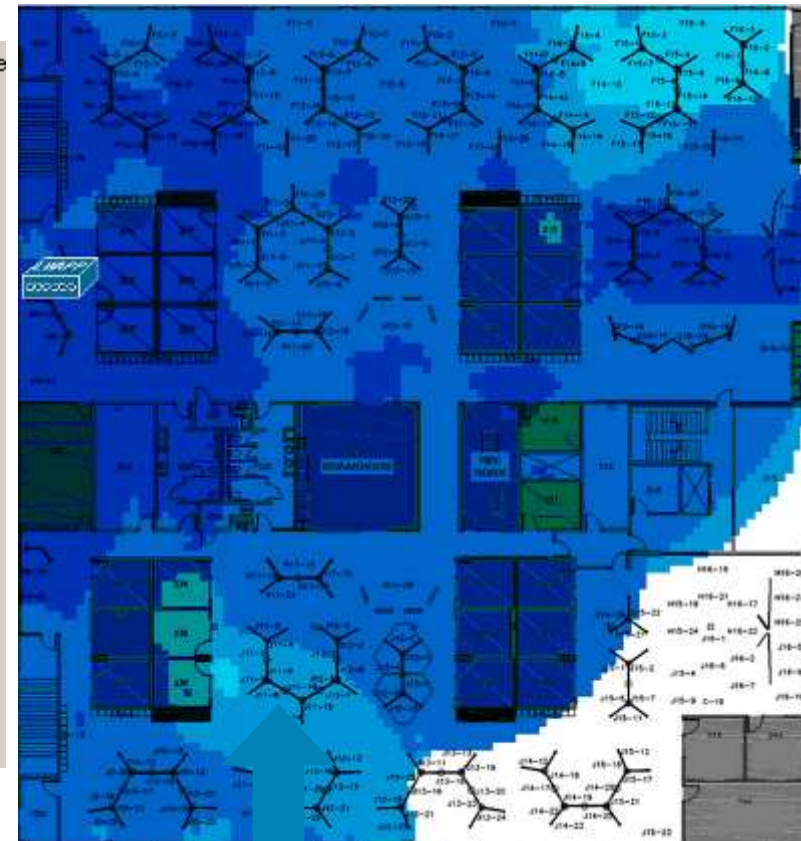
Miercom

ClientLink Disabled



High Retry Rates

ClientLink Enabled



Low Retry Rates

Source: Miercom; AirMagnet 6.0 Iperf Survey

Beam Forming Enhancements

- Beam Forming will improve performance **only when data rates begin to fall**
 - Translation: **If the connection is already good (i.e. data rate of 54Mbps) there is no improvement**
- Measureable advantages:

- Increased **SNR** at cell edges

Provides

- Increased downstream **data rates** at cell edges

Provides

- Increased downstream **throughput** at cell edges

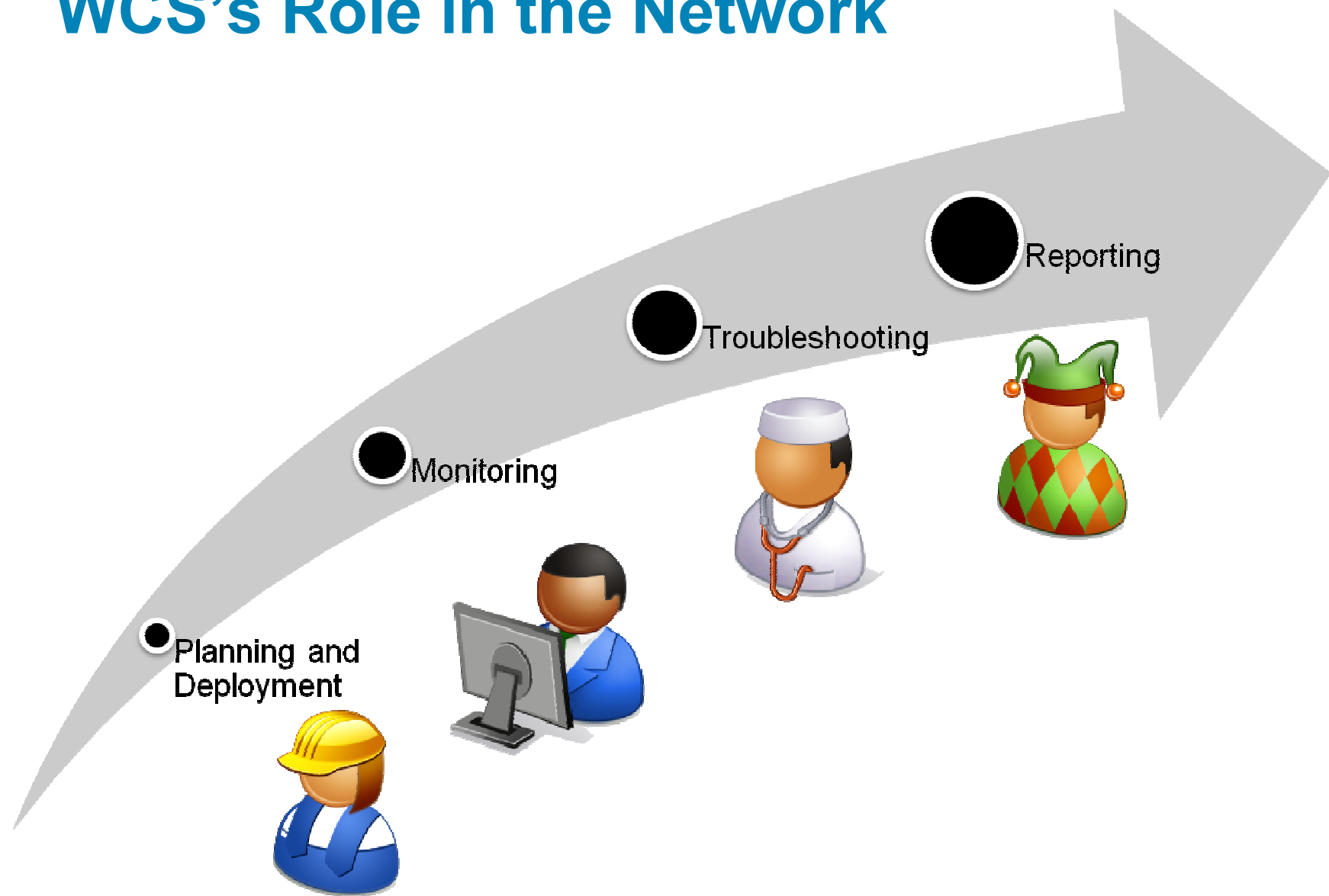
Essential Facts

- ClientLink only kicks in after the client's RSSI falls below a certain threshold.
 - For 802.11a, this is **-60dBm or weaker**
 - For 802.11g, this is **-50dBm or weaker**
- Most benefits will occur when the client is ~40ft or more from the AP
- ClientLink can beam form to **up to 15 clients per radio**
 - Thus for a dual-band AP – up to 30 clients per AP
 - When the beam forming table is full, the oldest client is aged out and replaced
 - This is not the maximum number of clients per radio – that does not change**

WCS Update



WCS's Role in the Network



Planning and Deployment

- Using WCS Planning Tool
- Setting up Network Elements via WCS
 - Controller Configuration Groups
 - Configuration Template LaunchPad
 - Controller Auto-Provisioning
 - Configuration Auditing Methods
- Provisioning Maps and Context-Aware Service

Planning Tool—Customize Plan

Planning Mode: Maps > SJ-14 > 4th Floor

Add APs Delete APs Map Editor Synchronize with Deployment Generate Proposal

Contributing APs

- ☒ AP_1
- ☒ AP_2
- ☒ AP_3

Refresh HeatMap

Click on an AP to change its position and properties. Drag the AP with the mouse and place them in required location.

Protocol: 802.11b/g/n HeatMap Type: Signal Strength RSSI Cutoff: -75 dBm Resolution: High RSSI Color Lookup: -35 dBm to -90 dBm Full Screen Zoom: 100 %

Planning Mode: Maps > SJ-14 > 4th Floor

Add APs Delete APs Map Editor Synchronize with Deployment Generate Proposal

Contributing APs

- ☒ AP_1
- ☒ AP_2
- ☒ AP_3

Refresh HeatMap

AP Name: AP_5 Ap Type: AP 1130 Ap Mode: Local

802.11a/n Interface

Tx Power: 15 dBm Antenna Name: AJAX-OMNI Ant. Mode: Omni Angle: 180 degrees

802.11b/g/n Interface

Tx Power: 18 dBm Antenna Name: AJAX-OMNI Diversity: Enabled Angle: 180 degrees

Default suggestions after running the planning tool present AP deployment choices and ability to switch between data and signal strength heatmap

Clicking an AP in the plan allows customization (added, deleted or simply modify properties) before a proposal may be generated

Maps Layout

Maps Tree View

- Maps (Root Area)
 - StandAlone Buildings
 - Juribe Building
 - SJ-14
 - 3rd Floor
 - 4th Floor
 - Campus 1
 - Building 3
 - 2nd Floor
 - campus bld01

Maps (Edit View)

Monitor > Maps

Show: Type: All Status: All Go

Name	Type	Status	a/n Radio
<input type="checkbox"/> Campus 1			
<input type="checkbox"/> Campus 1 > Building 3	Building	0	0
<input type="checkbox"/> Campus 1 > campus bld01	Building	0	0
<input type="checkbox"/> Juribe Building	Building	0	0
<input type="checkbox"/> SJ-14	Building	37	37
	Floor Area		

Default View of Campus, Buildings, and Floors can be easily changed with the "Quick Filters"

-- Select a command --

-- Select a command --

- New Campus
- New Building
- Delete Maps
- Move Buildings
- Copy Maps
- Properties
- Import AP/WiFi TDOA Receiver/Chokepoint Placement...
- Export AP/WiFi TDOA Receiver/Chokepoint Placement...
- Import WLSE Map and AP Location Data...
- RF Calibration Models
- Location Presence

Hierarchical Layout for easy navigation

Adding Campus or Buildings are made easy with the drop-down menu actions through an easy wizard that walks you through provisioning floor plans and APs

Maps Tree View

- Maps (Root Area)
 - StandAlone Buildings
 - Juribe Building
 - SJ-14
 - 3rd Floor
 - 4th Floor
 - Campus 1

Floor	Map	Details																				
4		<table border="0"> <tr> <td>Floor Area</td> <td>4th Floor</td> <td>Total APs</td> <td>18</td> </tr> <tr> <td>Floor Index</td> <td>4</td> <td>a/n Radios</td> <td>18</td> </tr> <tr> <td>Contact</td> <td>Saurabh Bhasin</td> <td>b/g/n Radios</td> <td>18</td> </tr> <tr> <td>Status</td> <td></td> <td>Out of Service Radios</td> <td>0</td> </tr> <tr> <td></td> <td></td> <td>Clients</td> <td>44</td> </tr> </table>	Floor Area	4th Floor	Total APs	18	Floor Index	4	a/n Radios	18	Contact	Saurabh Bhasin	b/g/n Radios	18	Status		Out of Service Radios	0			Clients	44
Floor Area	4th Floor	Total APs	18																			
Floor Index	4	a/n Radios	18																			
Contact	Saurabh Bhasin	b/g/n Radios	18																			
Status		Out of Service Radios	0																			
		Clients	44																			
3		<table border="0"> <tr> <td>Floor Area</td> <td>3rd Floor</td> <td>Total APs</td> <td>19</td> </tr> <tr> <td>Floor Index</td> <td>3</td> <td>a/n Radios</td> <td>19</td> </tr> <tr> <td>Contact</td> <td>Saurabh Bhasin</td> <td>b/g/n Radios</td> <td>19</td> </tr> <tr> <td>Status</td> <td></td> <td>Out of Service Radios</td> <td>0</td> </tr> <tr> <td></td> <td></td> <td>Clients</td> <td>133</td> </tr> </table>	Floor Area	3rd Floor	Total APs	19	Floor Index	3	a/n Radios	19	Contact	Saurabh Bhasin	b/g/n Radios	19	Status		Out of Service Radios	0			Clients	133
Floor Area	3rd Floor	Total APs	19																			
Floor Index	3	a/n Radios	19																			
Contact	Saurabh Bhasin	b/g/n Radios	19																			
Status		Out of Service Radios	0																			
		Clients	133																			

Building view provides a quick glance in to floors' status and alarm summary for easier troubleshooting

Maps Layout—Floor View

Maps Tree View

- ☒ Access Points
- ☒ AP Heatmaps
- ☒ Clients
- ☐ 802.11 Tags
- ☐ Rogue APs
- ☐ Rogue Adhocs
- ☐ Rogue Clients
- ☐ coverageAreas
- ☐ Location Regions
- ☐ Rails
- ☐ Markers
- ☒ Chokepoints
- ☐ Wifi TDQA Receivers

Display MSE data within last:

15 Minutes

Save Settings

Floor View

Monitor > Maps > WNBH > 4th Floor

Data may be delayed up to 15 minutes or more depending on background polling interval

Auto Refresh: 5 min

Commonly used map actions are ever-present in icon format

Quickly Add/Remove Layers that may be placed on the floor plan and heat maps

Mouse-over on objects on the map provides quick object summaries

Client 00:1b:63:c3:41:e1

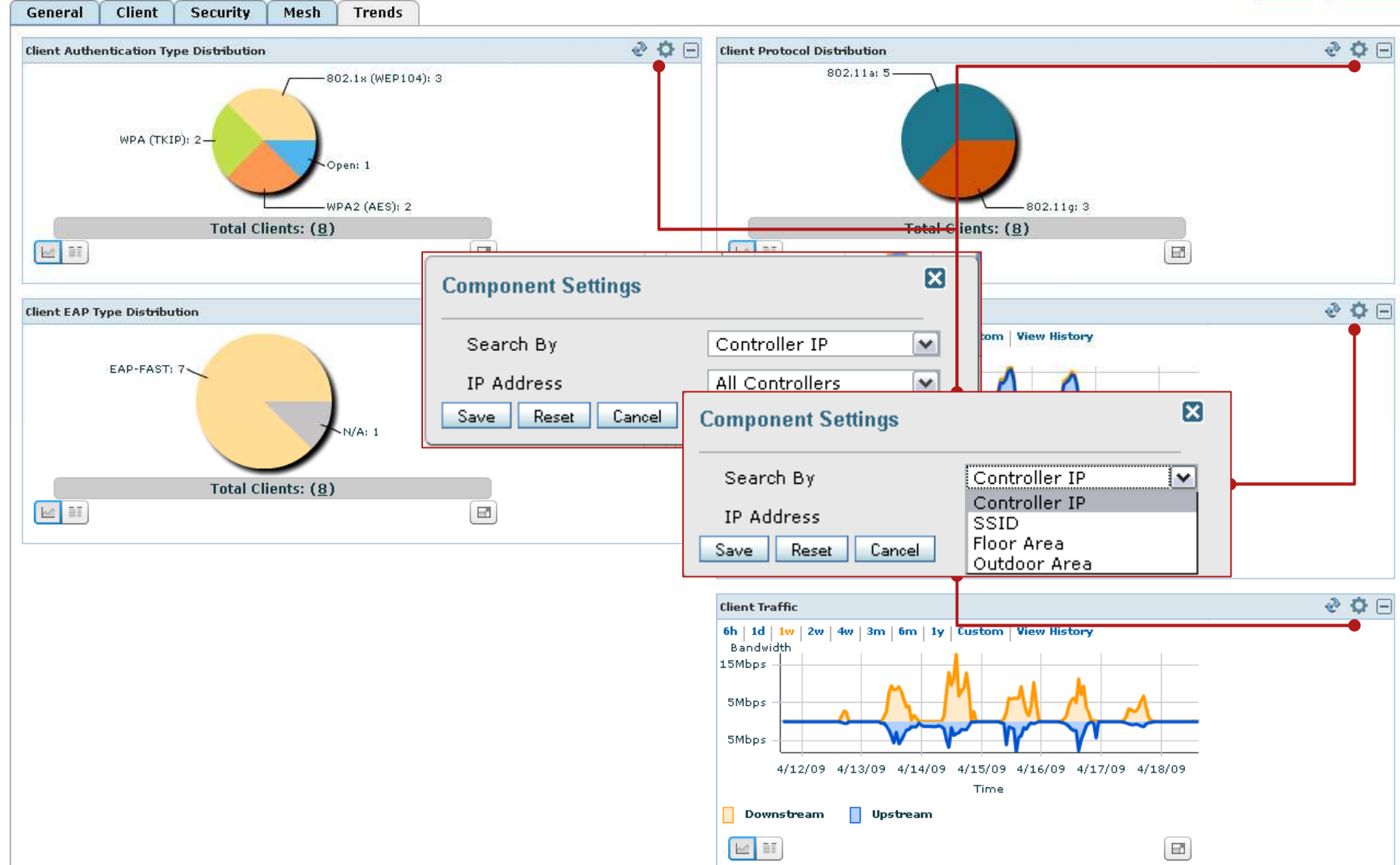
UserName	sabhasin
IP Addr	10.32.32.146
Asset Name	
Asset Group	
Asset Category	
Status	Associated
Auth	Yes
SSID	alpha
AP Name	Cascade-Miami_Beach
Protocol	802.11n(5GHz)
Port No	13
Last Located	4/27/09 11:08 AM

Loaded 143 out of 143 Clients Done.
Loading Tags.. Loaded 9 out of 9 Tags Done.
Loading Chokepoints.. Loaded 2 chokepoints Done.

Customizing WCS Dashboard

WCS Home

[Edit Tabs](#) [Edit Contents](#)



Quick Filters, Custom List Layout

Clients [\(Edit View\)](#)

Monitor > Clients

Show: **Authenticated Clients** [Go](#)

---Select client filter---

- 2.4GHz Clients
- 5GHz Clients
- All Clients
- Associated Clients
- Authenticated Clients
- Clients detected by Location Server
- Clients detected in last 24 hours
- Excluded Clients
- New Clients detected in last 24 hours
- Probing Clients
- Unauthenticated Clients
- WGB Clients

Client U	Client IP Address	Vendor Name	AP Name	Controller Name	SSID	VLAN	Protocol	Association	Association Time	Session Length
<Unkn	19.19.151	Intel	AP1140-2	Talwar-TME	temp-open	19	802.11g	Associated	04/18/2009 17:00:42	43 min 16 sec
<Unkn	8.107.21.126	Intel	sic14-12b-ap4	SJC 14 LWAPP1	guestnet	240	802.11a	Associated	04/18/2009 17:00:42	43 min 16 sec
fpang	1.70.243.104	Intel	sic14-21b-ap2	SJC 14 LWAPP1	blizzard	260	802.11a	Associated	04/18/2009 03:02:48	14 hrs 41 min 10 sec
ianaray	1.70.241.26	Cisco	sic14-12b-ap6	SJC 14 LWAPP1	blizzard	260	802.11g	Associated	04/15/2009 14:11:39	3 days 3 hrs 32 min 19 sec
ianaray	1.70.240.79	Cisco	sic14-12b-ap6	SJC 14 LWAPP1	blizzard	260	802.11a	Associated	04/16/2009 15:11:14	2 days 2 hrs 32 min 44 sec
ianaray	10.16.217.88	Cisco	sic14-12b-ap6	SJC 14 LWAPP1	wipp	251	802.11g	Associated	04/17/2009 15:35:46	1 days 2 hrs 8 min 12 sec
iblandfo	00:1b:d4:54:6f:1c	Cisco	sic14-12b-ap6	SJC 14 LWAPP1	wipp	251	802.11a	Associated	04/14/2009 11:31:47	4 days 6 hrs 12 min 11 sec
lsekha	00:21:5c:85:b7:c7	Intel	sic14-11b-ap2	SJC 14 LWAPP1	blizzard	260	802.11a	Associated	04/18/2009 16:23:58	1 hrs 20 min 0 sec
sabhasin	00:1f:6c:7a:16:7e	Cisco	sic14-41b-ap1	SJC 14 LWAPP2	wipp	251	802.11a	Associated	04/14/2009 11:31:47	4 days 6 hrs 12 min 11 sec

Use Quick Filters or Column Sorting to arrange information relevant to the task

Edit View

Use the **Show/Hide** buttons to specify the information to display in this view for this user. To set to the default view and order click reset. [Reset](#)

Hide Information

AP MAC Address
Anchor Controller
Authenticated
Automated Test Ran
CCX
Client Host Name
Controller IP Address
Controller Port
E2E
Encryption Cipher
Link Test
MSE
Map Location
Profile Name
RSSI

Show >
< Hide

View Information

Client IP Address
Vendor Name
AP Name
Controller Name
SSID
VLAN
Protocol
Association
Association Time
Session Length
Authentication Type
Traffic (MB)
Throughput (kbps)

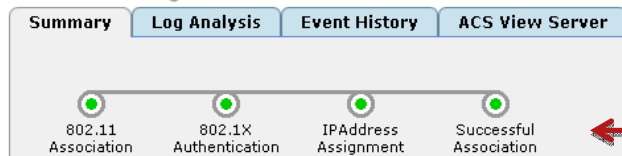
Up
Down

Submit Cancel

Edit List Pages for content relevant to you

Client Troubleshooting—Examples

Troubleshooting Client '00:21:5c:6b:83:1f'



Identify whether the problem occurs at 802.11 or higher layers

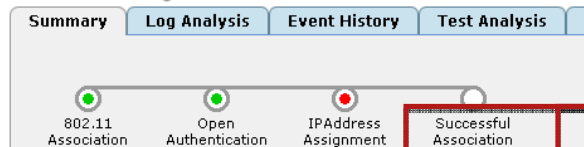
Problem

None

Suggested Action

None

Troubleshooting Client '00:40:96:a3:64:c0'



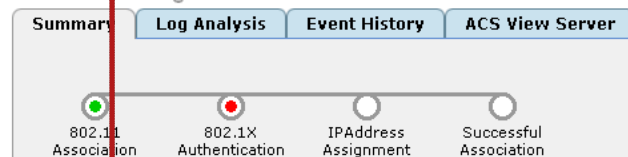
Problem

Client could not complete the dhcp interaction.

Suggested Action

Check whether the DHCP server is reachable.
Check whether dhcp server is configured to serve the wlan.
Check whether dhcp scope is exhausted.
Check whether multiple dhcp servers are configured with
Check local dhcp server is present if dhcp bridging mode
client is configured to get address from dhcp server.
Check if client has static ip configured and ensure client g
wlan, ensure that client is configured to do dhcp exchange
default config does not include it).

Troubleshooting Client '00:16:6f:22:de:b4'



Problem

802.1X Authentication Failure

Suggested Action

Check whether Radius server(s) is reachable
Check whether client's choice of EAP method is supported by radius server
Check Clients username/password/cert is valid
Check to see if the certificates used by the Authentication server are accepted by the client.

Client Troubleshooting—Examples

Troubleshooting Client '00:1d:e0:09:ad:6b'

Summary Log Analysis Event History ACS View Server

☒ Last 5 Minutes
☐ Between Hour Min
And Hour Min

Authentication Records

Troubleshooting Client '00:12:80:ad:7c:0a'

Summary Log Analysis Event History Test Analysis Messaging

Event History Summary

Recent 10 Client Events

Message

Client '00:12:80:ad:7c:0a' completed security policy with AP 'req01-31l-ap4', interface '802.11b/g'.

Client '00:12:80:ad:7c:0a (birds, 0.0.0.0)' is deauthenticated from AP 'req01-31l-ap4', interface '802.11b/g' with reason code '1'.

Client '00:12:80:ad:7c:0a' completed security policy with AP 'req01-31l-ap4', interface '802.11b/g'. 4/23/09 11:49

Client '00:12:80:ad:7c:0a (birds, 0.0.0.0)' is deauthenticated from AP 'req01-31l-ap4', interface '802.11b/g' with reason code '1'. 4/23/09 11:49

Recent 10 AP Events

Message

Message	Date / Time
AP 'req01-21l-ap4', interface '802.11b/g/n'. Interference threshold violated.	4/23/09 11:52
AP 'req01-32l-ap2', interface '802.11b/g'. Interference threshold violated.	4/23/09 11:52
AP 'req01-22l-ap7', interface '802.11b/g/n'. Interference threshold violated.	4/23/09 11:51
AP 'req01-21l-ap9', interface '802.11b/g/n'. Interference changed to acceptable.	4/23/09 11:51
AP 'req01-31l-ap9', interface '802.11b/g'. Interference threshold violated.	4/23/09 11:51

Analyzing logs from ACS and viewing latest client and AP events

Troubleshooting Client '00:12:80:ad:7c:0a'

Summary Log Analysis Event History Test Analysis Messaging Event Log ACS View Server

Use this tab to send an instant text message to the user of this client. Select a message from the list. Then click **Send**.

Message Category

The SSID is invalid.
The SSID is invalid.
The network settings are invalid.
There is a WLAN capability mismatch.
The user credentials are incorrect.
Please call support.
The problem is resolved.
The problem has not been resolved.
Please try again later.
Please correct the indicated problem.
Troubleshooting is refused by the network.
Retrieving client reports.
Retrieving client logs.
Retrieval complete.
Beginning association test.
Beginning DHCP test.
Beginning network connectivity test.
Beginning DNS
Beginning name
Beginning 802.1
Redirecting client

Advance options are enabled in presence of CCXv5 clients. Additional analysis and messaging is possible provided client diagnostics is enabled on the WLAN

Troubleshooting Client '00:12:80:ad:7c:0a'

Summary Log Analysis Event History Test Analysis Messaging Event Log ACS View Server

The following tests are available for clients. Use the checkboxes to select the test(s) you would like to perform, then click **Start**. Click **Stop** to halt the tests. When a test is completed, click on the test status to view the results.

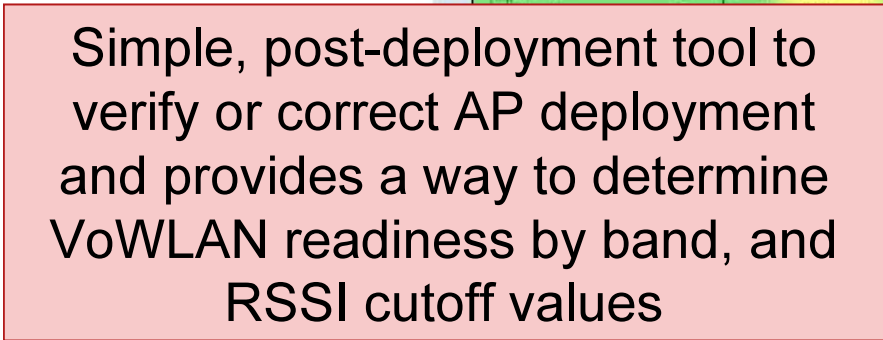
Select	Diagnostic Test	Input	Status	Results
<input type="checkbox"/>	DHCP		Not initiated	None
<input type="checkbox"/>	IP Connectivity		Not initiated	None
<input type="checkbox"/>	DNS Ping		Not initiated	None
<input type="checkbox"/>	DNS Resolution	Name to resolve: <input type="text"/>	Not initiated	None
<input type="checkbox"/>	802.11 Association	AP name: <input type="text"/> Profile: <input type="text"/>	Not initiated	None
<input type="checkbox"/>	802.1x Authentication		Not initiated	None
<input type="checkbox"/>	Profile Redirect	Client Profile Number: <input type="text"/>	Not initiated	None

Results:

Voice Audit Tool

- Allows auditing current network configuration from a VoWLAN deployment perspective
- Use default rules and thresholds based on Cisco best practices
- Ability to customize the rules to match your network and requirements
- Provides a simple report with a list of configuration gaps

© 2011 Pearson Education, Inc. All rights reserved. Printed in the United States of America. This publication is protected by copyright. Any unauthorized reproduction or distribution, in any form or by any means, without written permission from Pearson Education, Inc., is prohibited.



*Accuracy of the Red,Yellow,Green region may vary depending on the RF environment and quality of Calibration(if Calibrated).

Location Accuracy Tool—Example

Position Test Point on Floor '4th Floor'
New Scheduled Accuracy > New Scheduled Accuracy > New On Demand Accuracy > Position Test Point on Floor '4th Floor'

Select a client/tag/interferer:

--Client List--

X Y
81.0 26.8

Start Stop Analyze Results

0 feet 50 100

SONOMA COAST OLLIVIER BEACH SANTA CRUZ

Test with Clients, Tags, Exciters

Schedule Accuracy Tests

Accuracy Tests

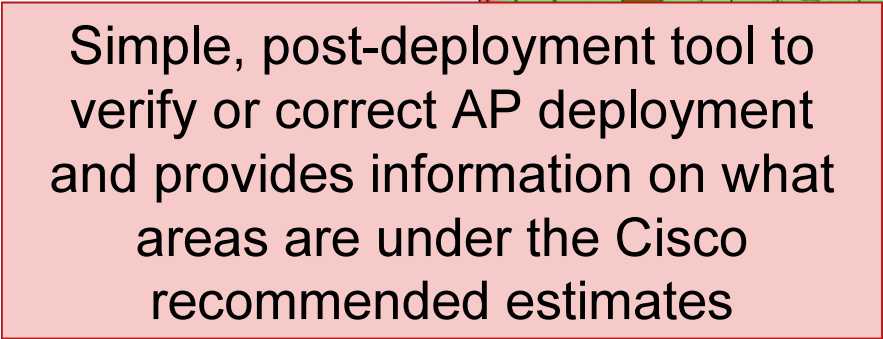
<input type="checkbox"/>	Name	Test Type	Floor	Status
<input type="checkbox"/>	TEST-1	On demand Accuracy Test	SJ-14 > 4th Floor	Idle

-- Select a command --

- New Scheduled Accuracy Test...
- New On-demand Accuracy Test...
- Download Logs For Last Run...
- Download Logs..
- Delete

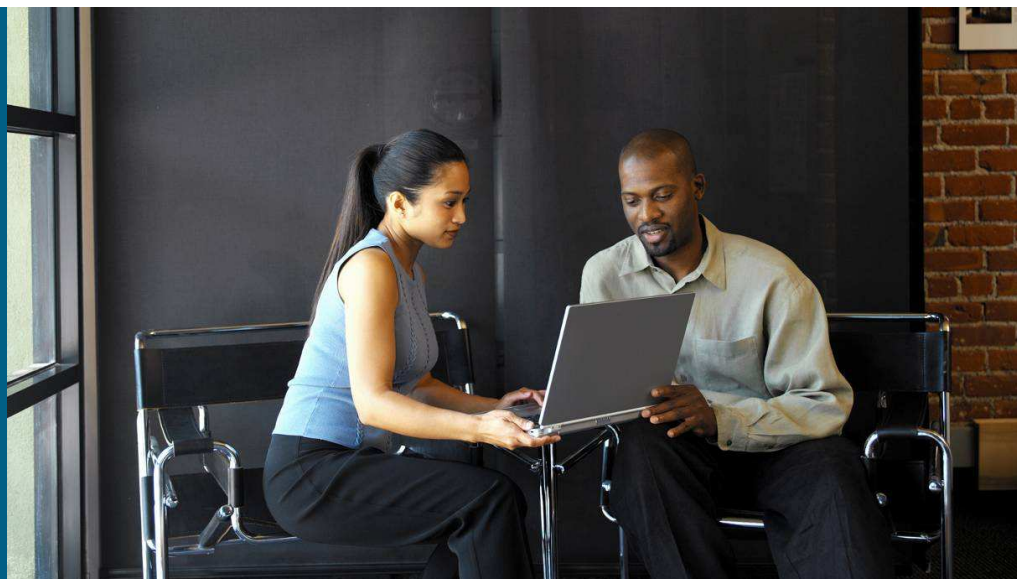
Determine Accuracy Probability, Correct Deployment

Position the Test Point on the floor and click on 'Start'. Click 'Stop' after few minutes and proceed to the next location. Please wait for 2 minutes at the new location before clicking on 'Start'. When done with all locations, click on 'Analyze Results'.





Mobility Services



Wireless LAN Mobility Services

Security



- Automatic, 24 x 7 security and compliance monitoring for breaches via wireless medium
- Network access control based on user location

Guest



- Guest networks for customers, partners and auditors
- Vendor replenishment networks
- Public access networks

Voice



- Real-time mobile voice communications
- Improved collaboration via mobile unified communications
- Faster customer service response

Location



- Asset management
- Location-based content distribution
- Streamlined workflow using historical location data

Pervasive Wireless Network

Services on MSE

- CAS, wIPS & MIR can run concurrently on MSE 3310
- CAS & wIPS can run concurrently on MSE 3350
- Scalability varies based on platform and services deployed

MSE-3310		
wIPS	CAS	MIR
1,000	1,000	TBD
2,000	0	TBD
0	2,000	TBD
MSE-3350		
wIPS	CAS	MIR
0	18,000	N/A
1,000	12,000	N/A
2,000	6,000	N/A
2,500	3,000	N/A
3,000	0	N/A

MSE Services SKU Calculator				
			Enter Values	
	Service Name	Units	Requirements	Available
	Context-Aware for Clients	Clients Tracked	1,000	10,000
	Context-Aware for Tags	Tags Tracked	1,000	10,000
	Mobile Intelligent Roaming	Mobile Users	500	1,100
	Wireless Intrusion Prevention	Monitor Mode AP's	200	1,715
Quantity	SKU		Valid Config	
			Create SKU List	
			Clear	

Cisco 2710 vs. MSE

	Cisco 2710	Cisco MSE
Max. number of tracked devices	2500 (combination of tags and clients)	3310: 2,000 (up to 1K clients, up to 1K tags) 3350: 18,000
Client tracking engine	Cisco	Cisco
Tag tracking engine	Cisco	Partner (AeroScout)
Other services	None	wIPS, MIR, future (concurrent service support in v6.0)
Location tracking technology	RSSI only	RSSI, TDOA, wired, future technologies

Hardware: Cisco 2710 vs. MSE

- In both cases, 1U Linux-based appliance
- MSE based on multicore processors with additional memory to support multiple concurrent services (requires software release v6)
 - MSE 3350: RAID 1 (in hardware)
 - MSE 3310: RAID 1 (in software)

Receive Signal Strength Indication (RSSI) Overview

- Cisco RSSI-based location tracking solution based on “network-side” RSSI measurements
- Requires min. of three AP's; optimal accuracy requires more than 3 AP's
- Best suited for indoor office-like environments (carpeted, low ceiling, i.e. < 20 feet)
- Main factors affecting accuracy:
 - AP density
 - AP placement
 - RF environment

Time Difference of Arrival (TDoA) Overview

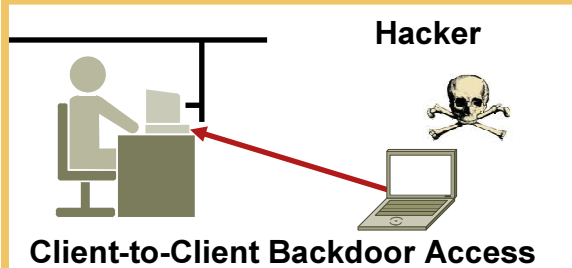
- Based upon relative differences in time measurement
- Requires clock synchronization at receivers, but not the mobile device
- Requires min. of three time-synchronized TDoA receivers
- Time for message to be received at different receivers is proportional to length of transmission path between the mobile device and each receiver

The Wireless Threat Landscape

Attacks Across Multiple Vectors

On-Wire Attacks

Ad Hoc Wireless Bridge

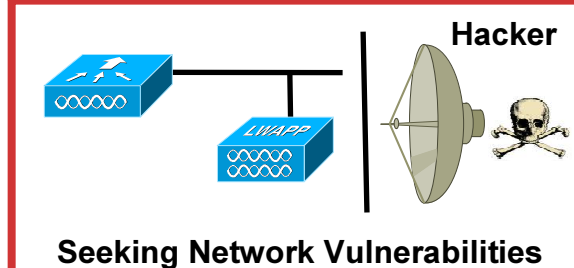


Over-the-Air Attacks

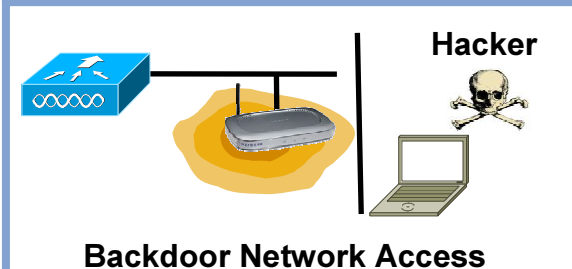
MiTM/Honeypot AP



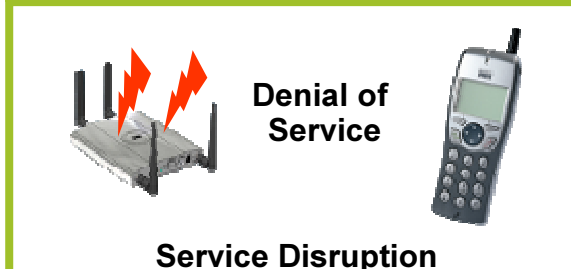
Reconnaissance



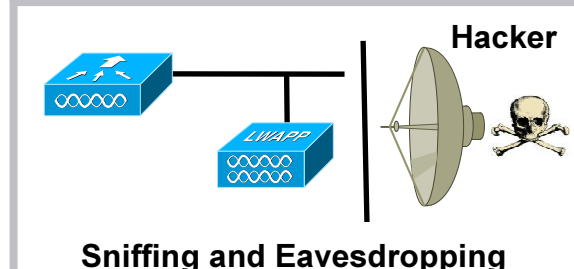
Rogue Access Points



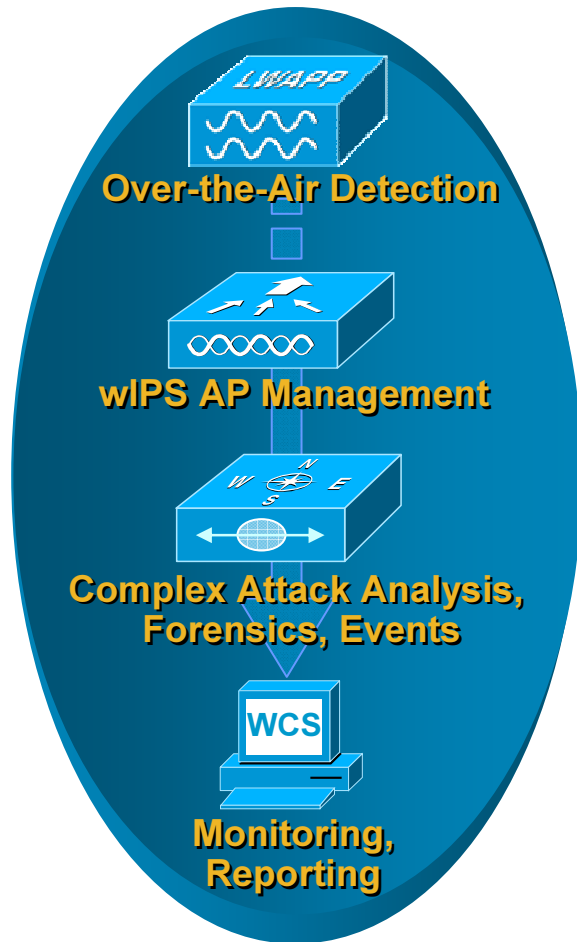
Denial of Service



Cracking Tools

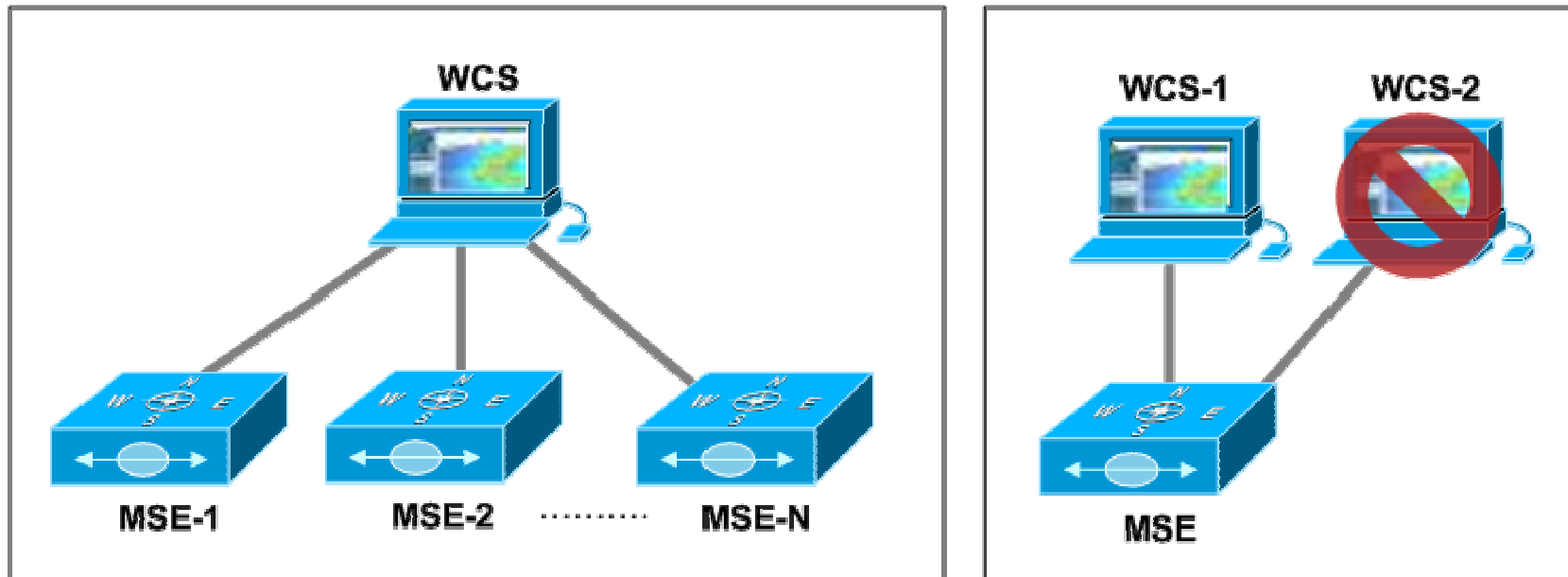


wIPS Component Functions



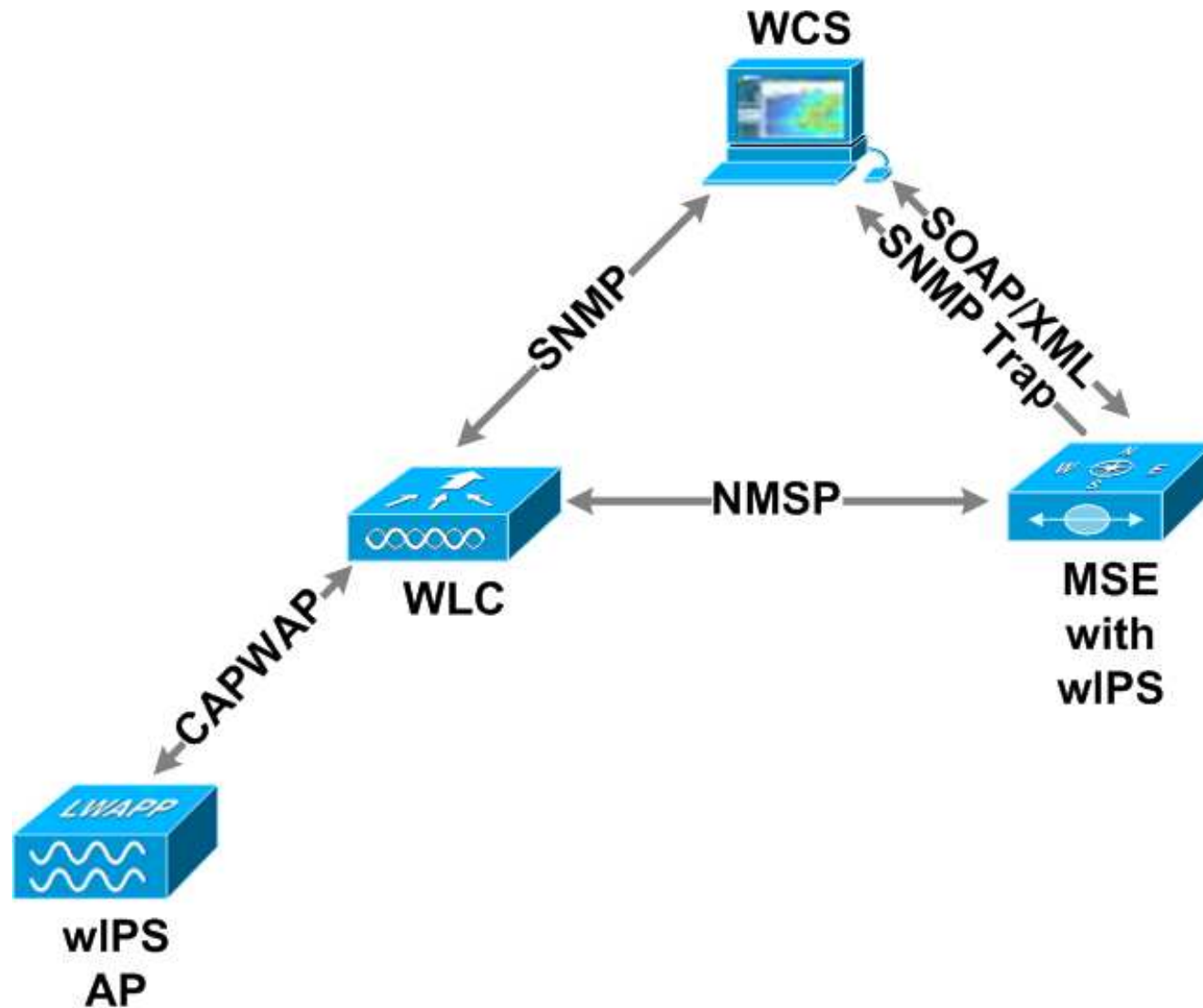
- wIPS Monitor Mode AP – attack detection (scanning at 250ms per channel)
- Controller – manages wIPS APs, forwards wIPS data to MSE
- MSE with wIPS Service – anomaly detection, attack archival and alarm aggregation
- WCS – centralized configuration and monitoring, viewing of wIPS alarms

System Scalability

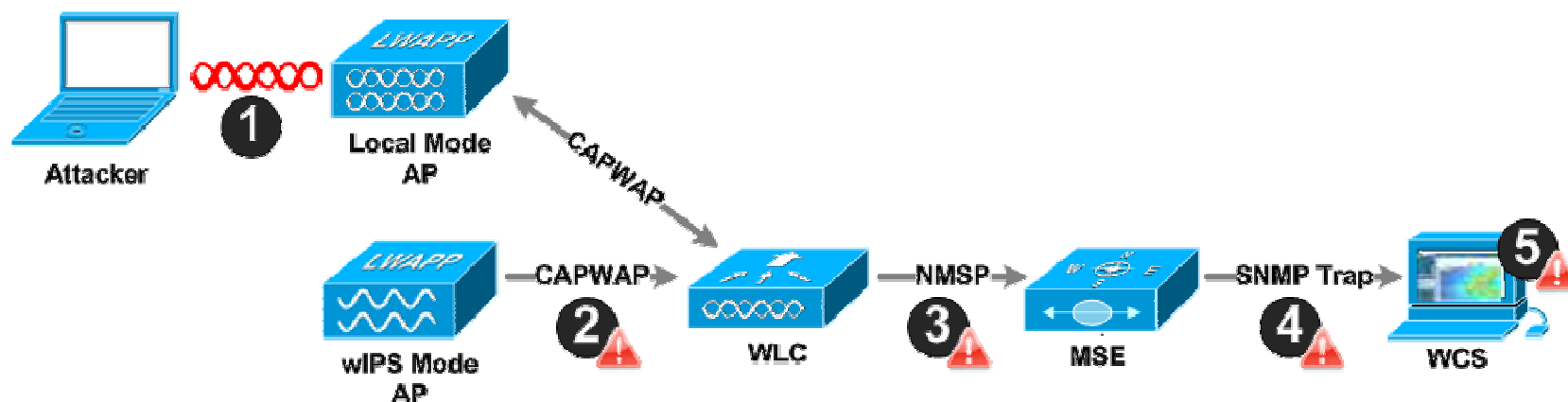


- Only one WCS can manage an MSE
- WCS can support a maximum of 3000 Access Points on a high-end server.
- An MSE 3310 running the wIPS Service can support an upper limit of 2000 wIPS Access Points.

wIPS System Communications



wIPS Alarm Flow



1. Attack Launched against 'infrastructure device'
2. Detected on AP
 - Communicated via CAPWAP to WLC
3. Passed transparently to MSE via NMSP
4. Logged into wIPS Database on MSE
 - Sent to WCS via SNMP trap
5. Displayed on WCS


wIPS—Example Alarm

General		Message
Detected By WIPS AP	1250-ap	Spoofed MAC address detected
WIPS AP IP Address	172.20.226.235	
WIPS AP MAC	00:1b:d5:13:15:e2	Description A device spoofing the MAC address of Corp [Channel: 1, SSID: Corp] was detected. Please power off Corp [Channel: 1, SSID: Corp] to see if 802.11 frames transmitted from the same MAC address still exist. The spoofed MAC Address may not have contained a valid OUI assigned by the IEEE and could have been randomly generated by a potential attacker probing for SSIDs in use.
Owner		
Acknowledged	No	Help
Category	Security	
Created	Oct 2, 2008 11:12:59 AM	Event History
Modified	Oct 2, 2008 11:12:59 AM	
Severity	Major	Annotations
Previous Severity	Clear	
First Seen	Oct 2, 2008 11:12:04 AM	
Last Seen	Oct 2, 2008 11:12:04 AM	
Last Disappeared	-	
Channel	1	
Attacker Client/AP MAC	00:21:1b:fd:a6:81	
Controller IP Address	172.20.226.197	
MSE	172.20.226.201	
Controller MAC	00:21:55:06:f2:80	

- Click 'Help' for more info on the attack

wIPS—Integrated Encyclopedia

- Available for each alarm
- Provides text and visual description of attack
- Provides potential remediation steps

**Man-in-the-Middle Attack Detected**

Alarm Description & Possible Causes

Man-in-the-Middle (MITM) attack is one of the most common 802.11 attacks that can lead to confidential corporate and private information being leaked to hackers. In a MITM attack, the hacker can use a 802.11 wireless analyzer and monitor 802.11 frames sent over the WLAN. By capturing the wireless frames during the association phase, the hacker gets IP and MAC address information about the wireless client card and access point, association ID for the client, and the SSID of the wireless network.

Man-in-the-Middle Attack

