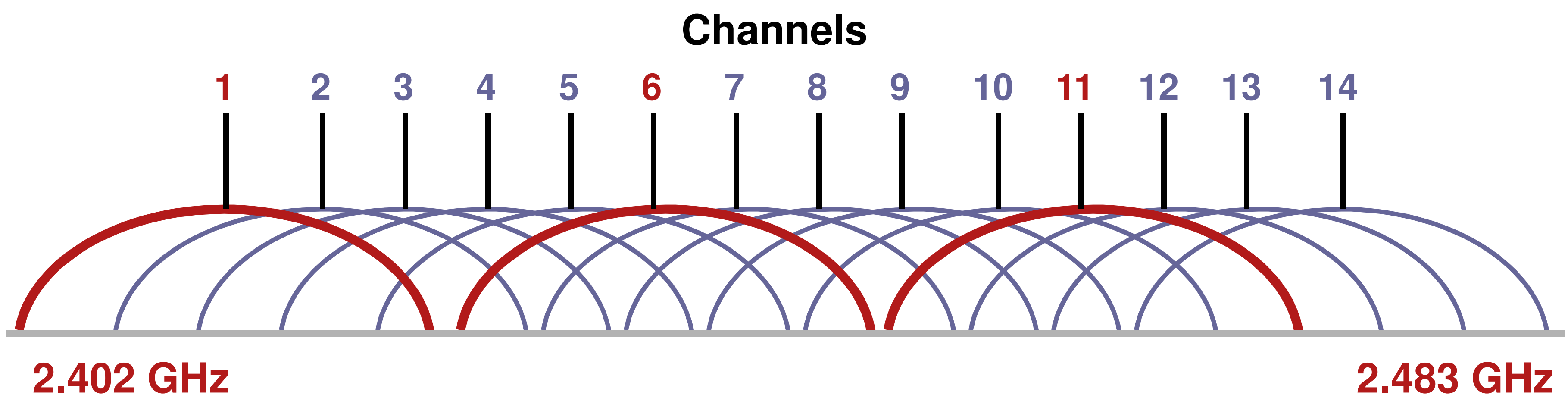
Wireless LAN Fundamental

IEEE 802.11 Radio Summary
Properties

	802.11	802.11b	802.11g	802.11a
Ratified	1999	1999	2003	1999
Data Rates (Mbps)	1,2	1,2,5.5,11	1,2,5.5,11 and 6,9,12,18,24, 36,48,54	6,9,12,18,24, 36,48,54
Number of Non-Overlapping Channels	Frequency Hopping	3	3	8 Indoors/ 11 Outdoors
Frequency Range (GHz)	2.402–2.483			5.15–5.35, 5.47–5.725*
Status	Obsolete	Worldwide Available		Limited Worldwide Availability

IEEE 802.11b
Direct Sequence @ 2.4 GHz

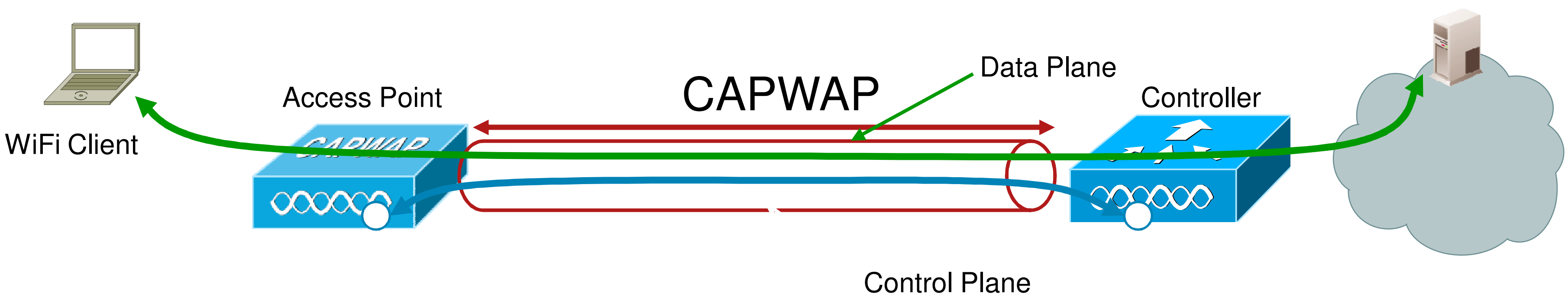


- Up to (14) 22 MHz wide channels
- 3 non-overlapping channels (1, 6, 11)
- Up to 11 Mbps data rate
- 3 access points can occupy the same space for a total of 33 Mbps aggregate throughput, but not on same radio card

LWAPP/CAPWAP Protocol Overview

Centralized Wireless LAN Architecture
What is CAPWAP ?

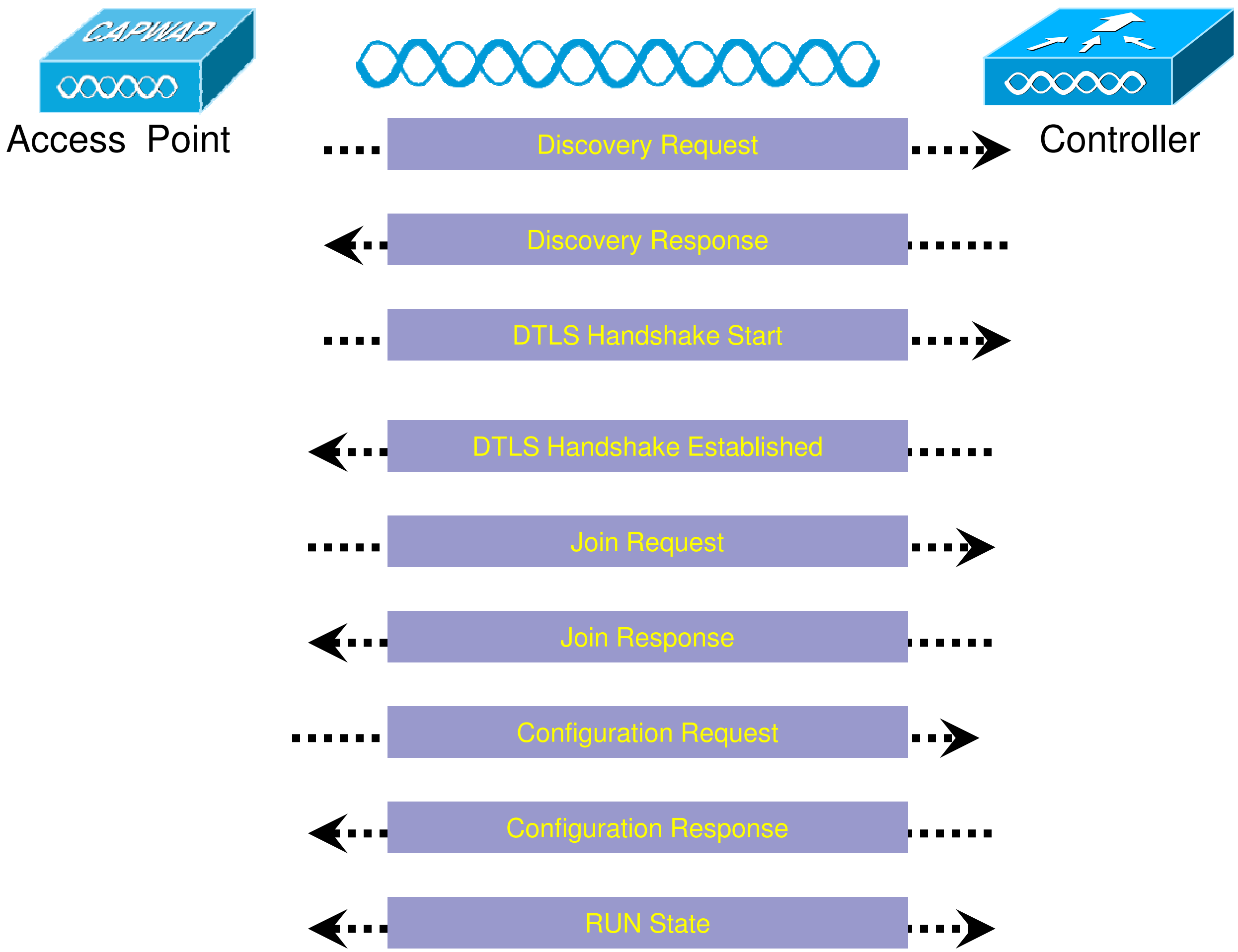
- CAPWAP - Control And Provisioning of Wireless Access Points is used between APs and WLAN Controller and based on LWAPP
- CAPWAP carries control and data traffic between the two
  - Control plane is DTLS encrypted
  - Data plane is DTLS encrypted (Optional)
- LWAPP-enabled access points can discover and join a CAPWAP controller, and conversion to a CAPWAP controller is seamless
- CAPWAP is not supported on Layer-2 mode deployment



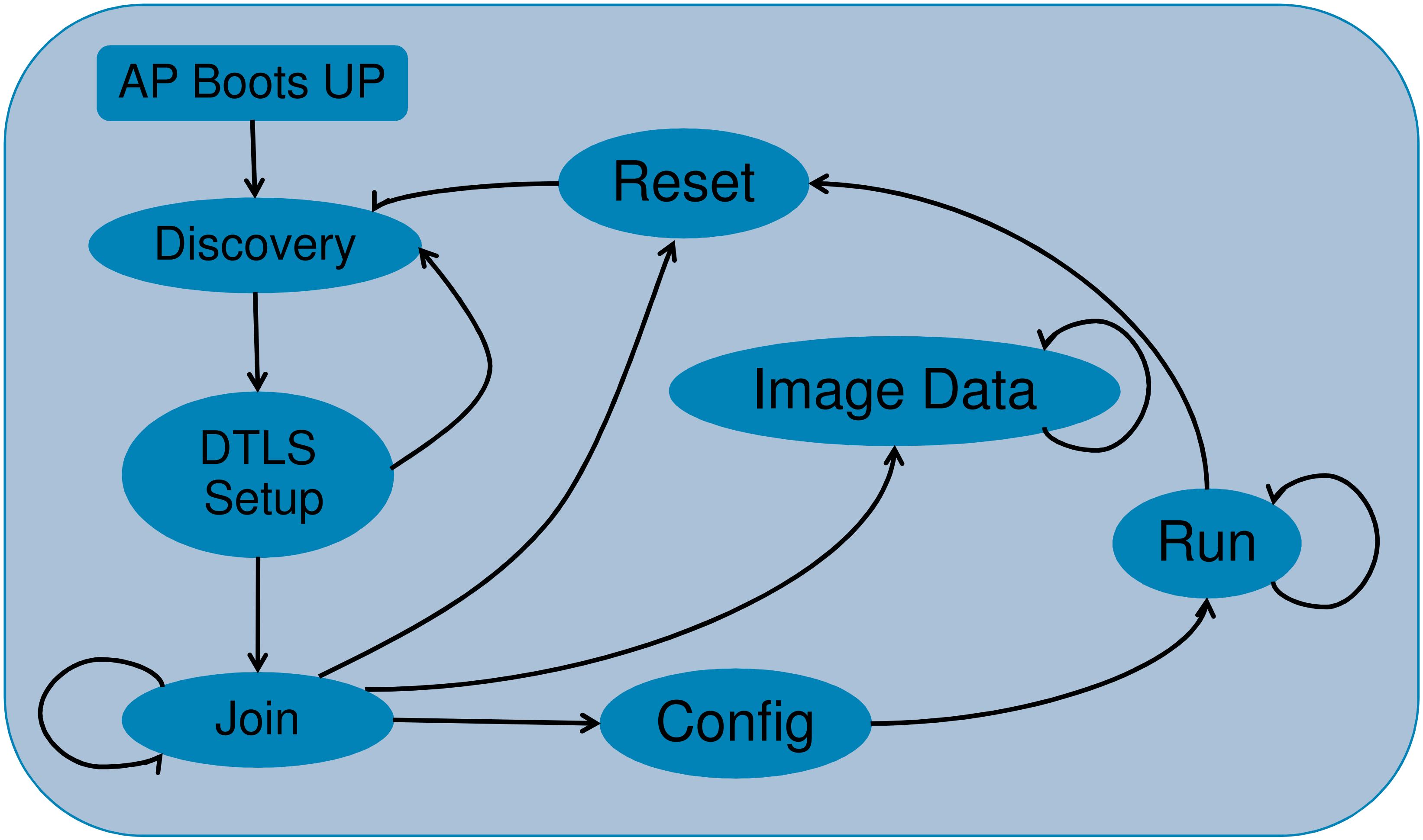
What is DTLS ?

- Datagram Transport Layer Security (DTLS) protocol provides communications privacy for datagram protocols
- The DTLS protocol is based on the stream-oriented TLS protocol
- DTLS is defined in RFC 4347 for use with UDP encapsulation

CAPWAP AP Discover / Join Process



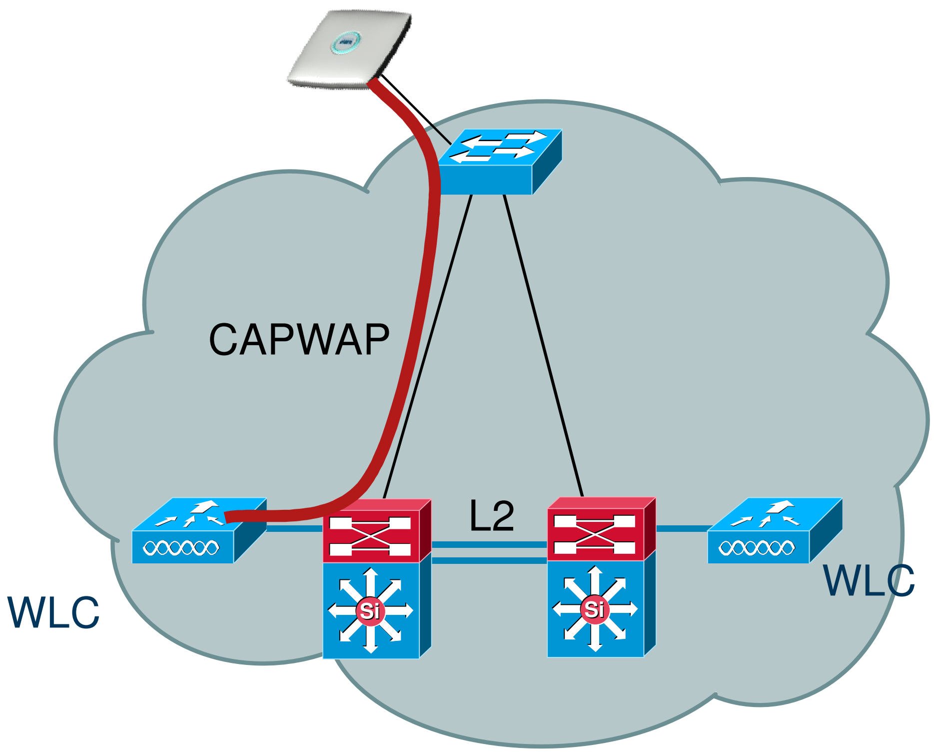
CAPWAP State Machine



Where to Place a Controller ?

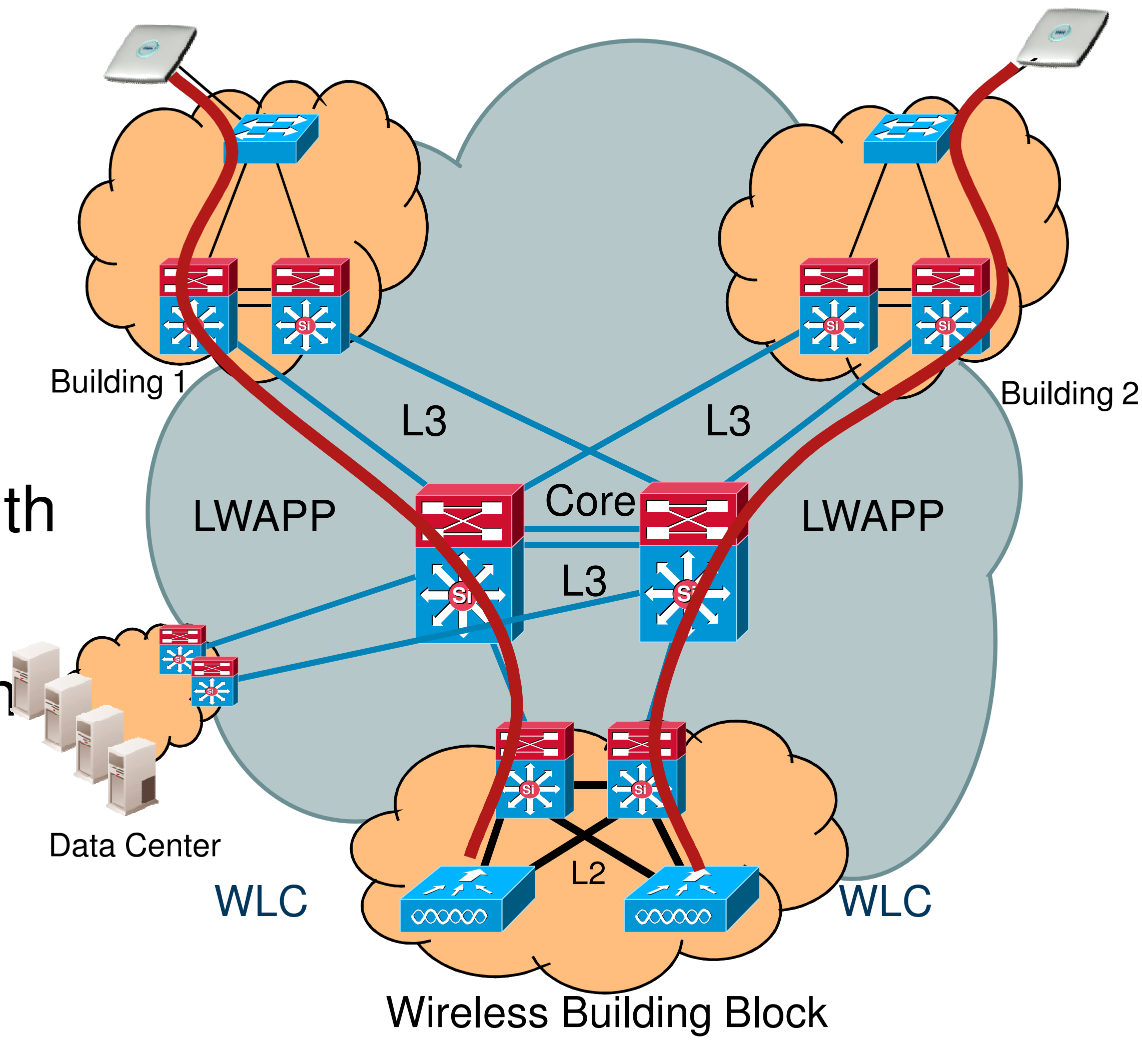
Single Building – Distribution/Core

- WLC in distribution/core
- Most of the time : L2 Roaming



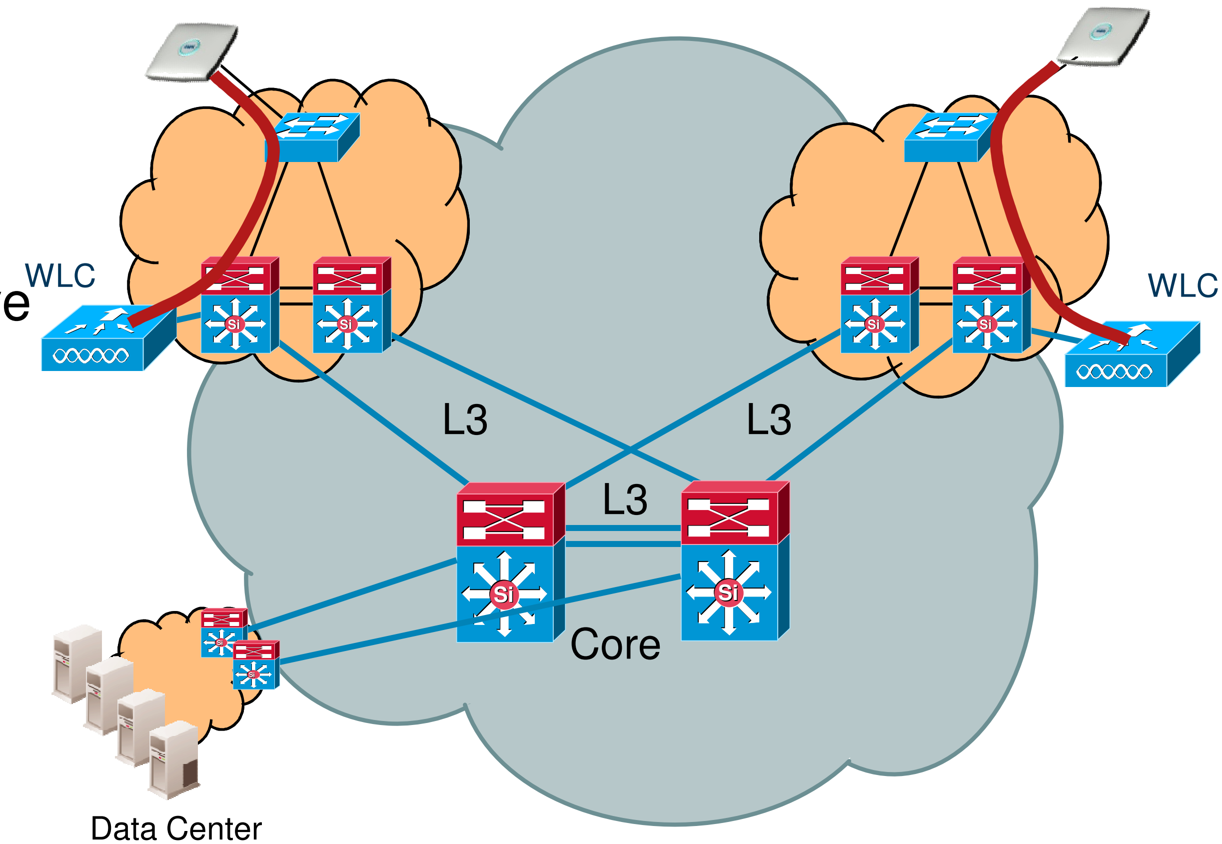
Campus – Centralized WLC
Overview

- Centralized WLC
- Concept of Wireless Building Block
- No Wireless VLANs everywhere
- Better performance with L2 Mobility
- Recommended design



Campus – Distributed WLC
Overview

- Distributed WLC or WiSM
- Each building as its own WLC
- Each building can have its own Mobility group
- Wireless insertion at distribution layer
- Several distributed Wireless VLANs across the Campus

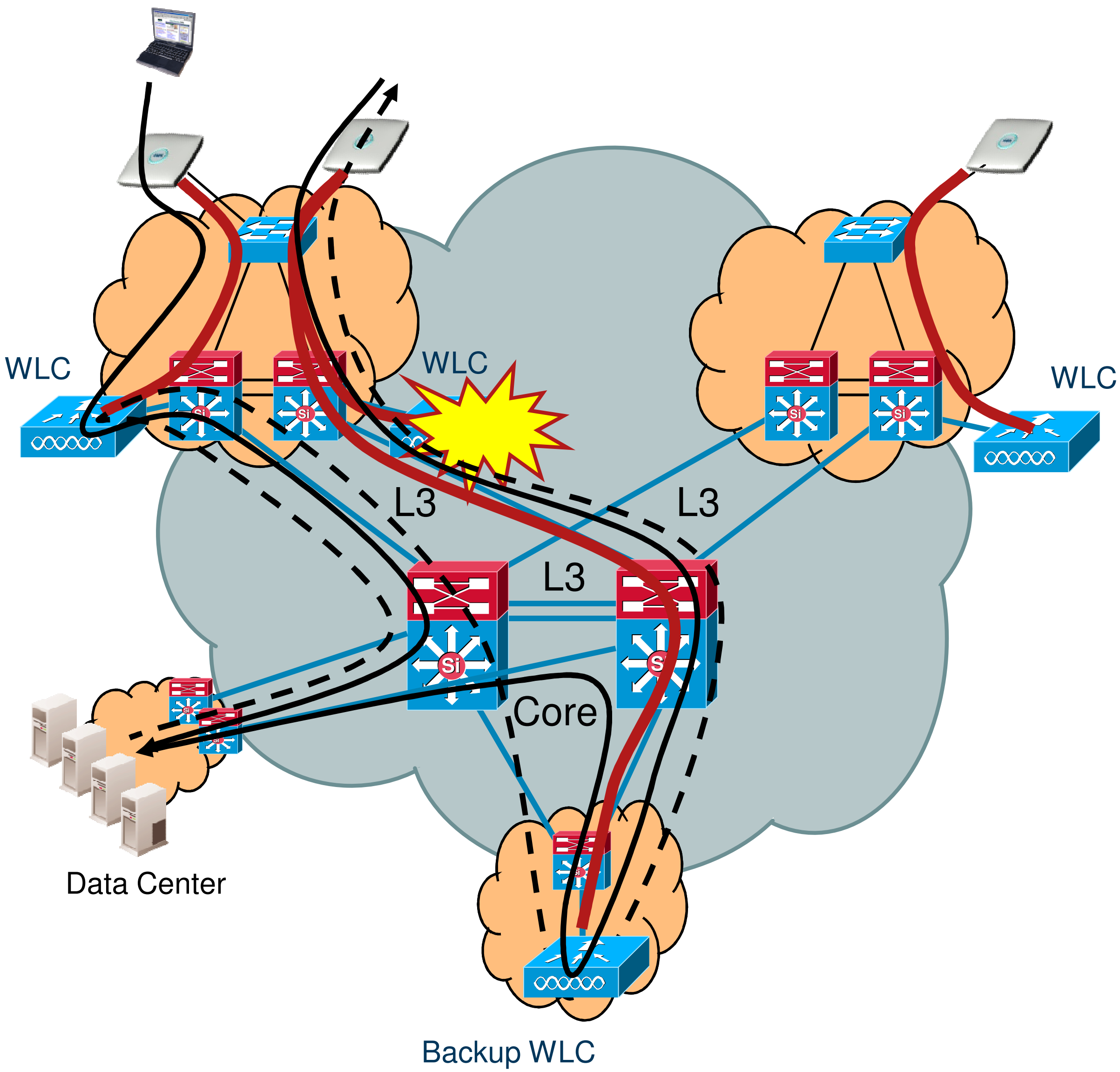


Campus – Distributed WLC

Scalability & Failover

- Using a Central Backup WLC
- Need for L3 roaming and same Mobility group across the Campus

⇨ Seems to be like a … Wireless Building Block …



Campus – Distributed WLC

Pros / Cons

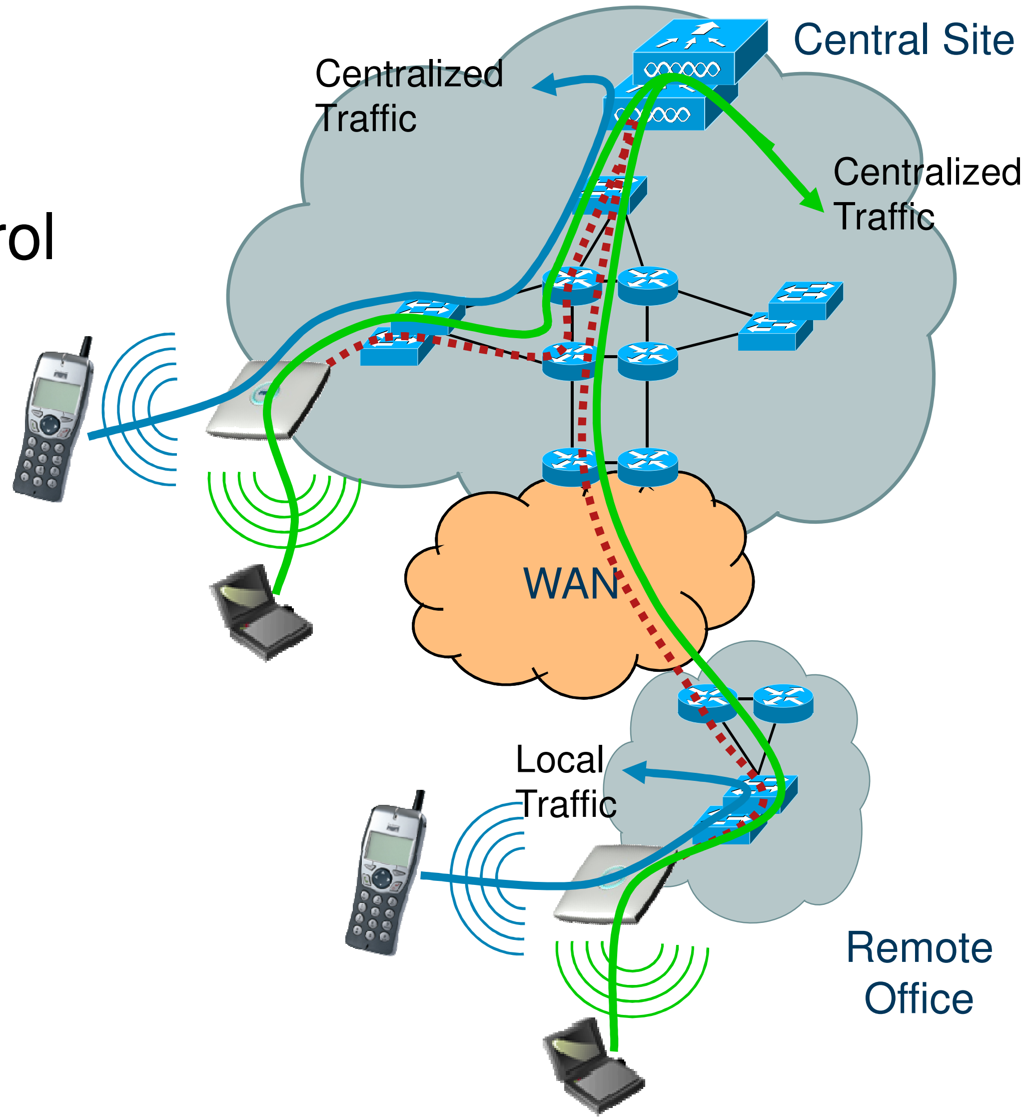
- Pros
  - No need for a wireless building block (cost ?)
  - No LWAPP traffic in core network in normal operation
- Cons
  - If radio continuity between buildings, all WLC need to be in a single mobility group
  - L3 roaming inside the building (less performance versus L2 roaming)
  - Control features (ACL, FW, NAC, …) need to be distributed in each building
  - More complex Failover strategies, more complex to troubleshoot

Understanding H-REAP

- Hybrid Architecture
- Single Management & Control point
    - –Centralized Traffic (Split MAC)

      Or

    - –Local Traffic (Local MAC)
- HA will preserve local traffic only



Deploying with RRM in Mind

RRM—Radio Resource Management

- What are RRM's objectives?
  - To dynamically balance the infrastructure and mitigate changes
  - Monitor and maintain coverage for all clients
  - Manage Spectrum Efficiency so as to provide the optimal throughput under changing conditions
- What RRM does not do
  - Substitute for a site survey
  - Correct an incorrectly architected network
  - Manufacture spectrum

How Does RRM Do This?

- **DCA**—Dynamic Channel Assignment

  Each AP radio gets a transmit channel assigned to it

  Changes in “air quality” are monitored, AP channel assignment changed when deemed appropriate (based on DCA cost function)

- **TPC**—Transmit Power Control

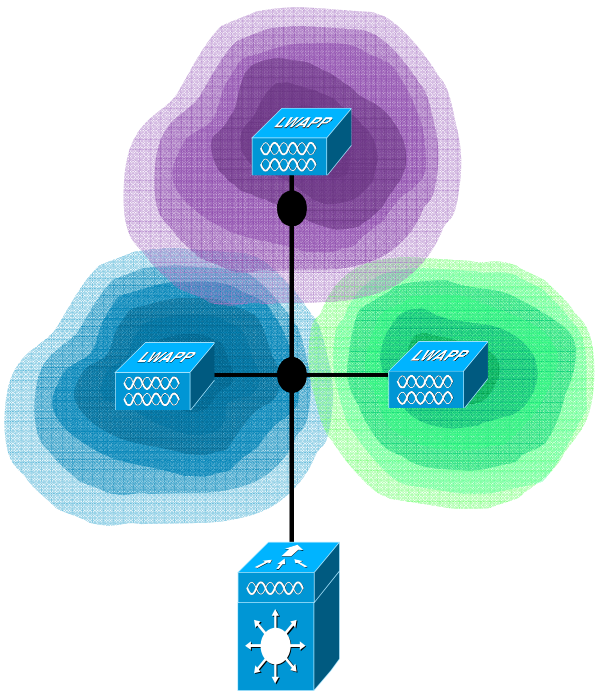
  Tx Power assignment based on radio to radio pathloss

  TPC is in charge of reducing Tx on some APs—but may also increase Tx by defaulting back to power level higher than the current Tx level

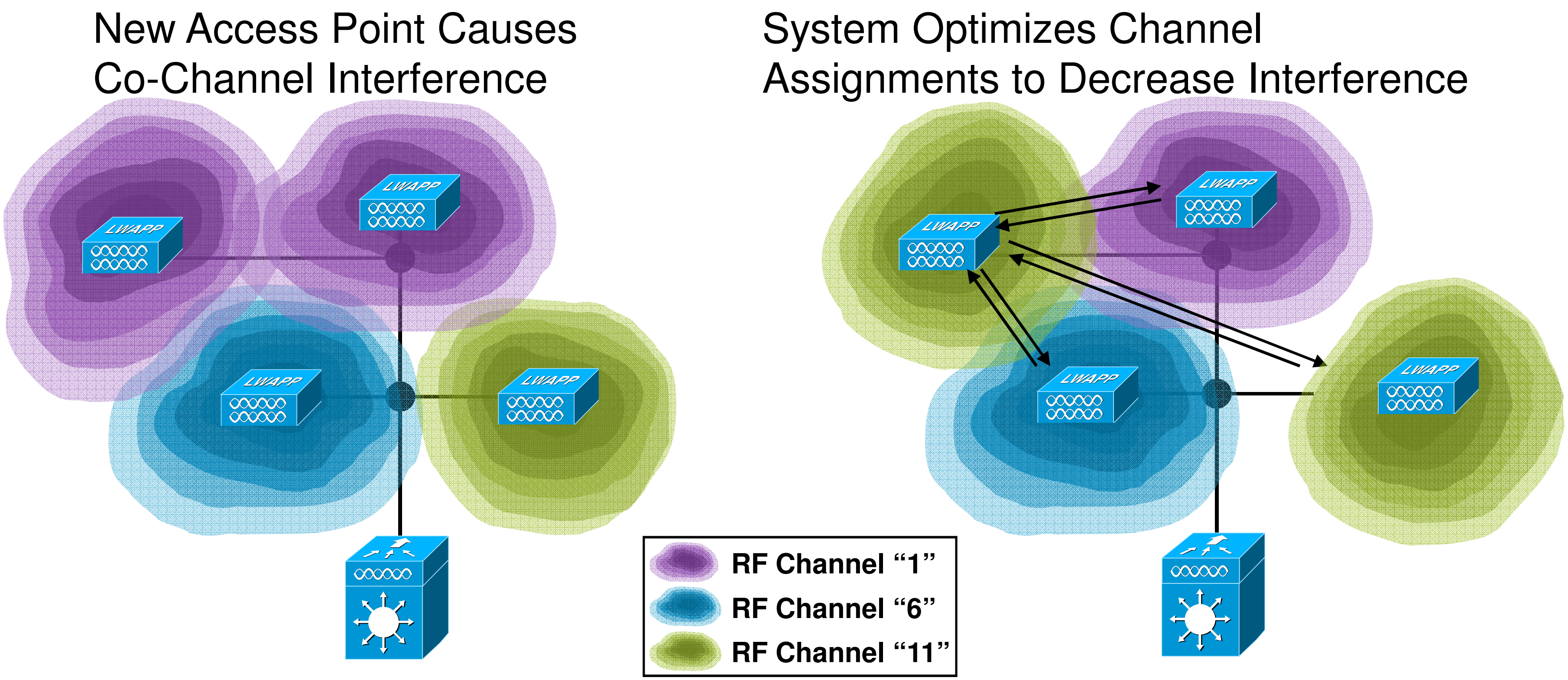
- **CHDM**—Coverage Hole Detection and Mitigation

  Detecting clients in coverage holes

  Deciding on Tx adjustment (typically Tx increase) on certain APs based on (in)adequacy of estimated downlink client coverage



RRM—DCA—
Dynamic Channel Assignment



What It Does

- Ensures that available RF spectrum is utilized well across frequencies/channels

  Best network throughput is achieved without sacrificing stability or AP availability to clients

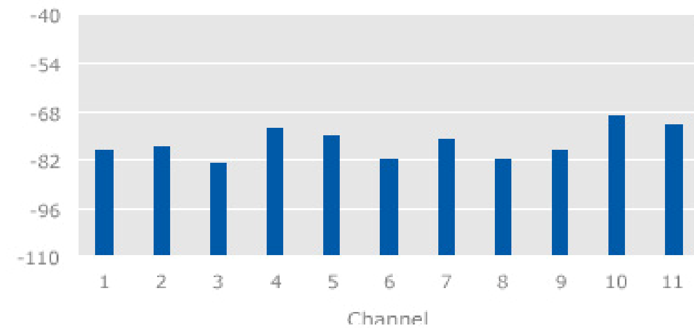
DCA in a Nutshell

- Who calculates DCA
  - It runs on the RF Group Leader WLC
  - Decisions on channel assignment change made on a per AP, per radio basis
- DCA manages channel assignments to each AP
  - Assigns channels to radios
  - Changes the existing assignment on some radios, if appropriate
- What criterion is evaluated:
  - RSSI-based Cost Function that captures overall interference (including non-802.11 noise) on a channel

Profile Information

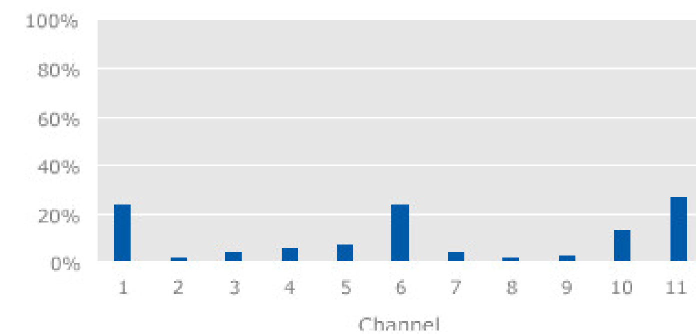
Noise Profile	Okay
Interference Profile	Issue

Noise by Channel (dBm)

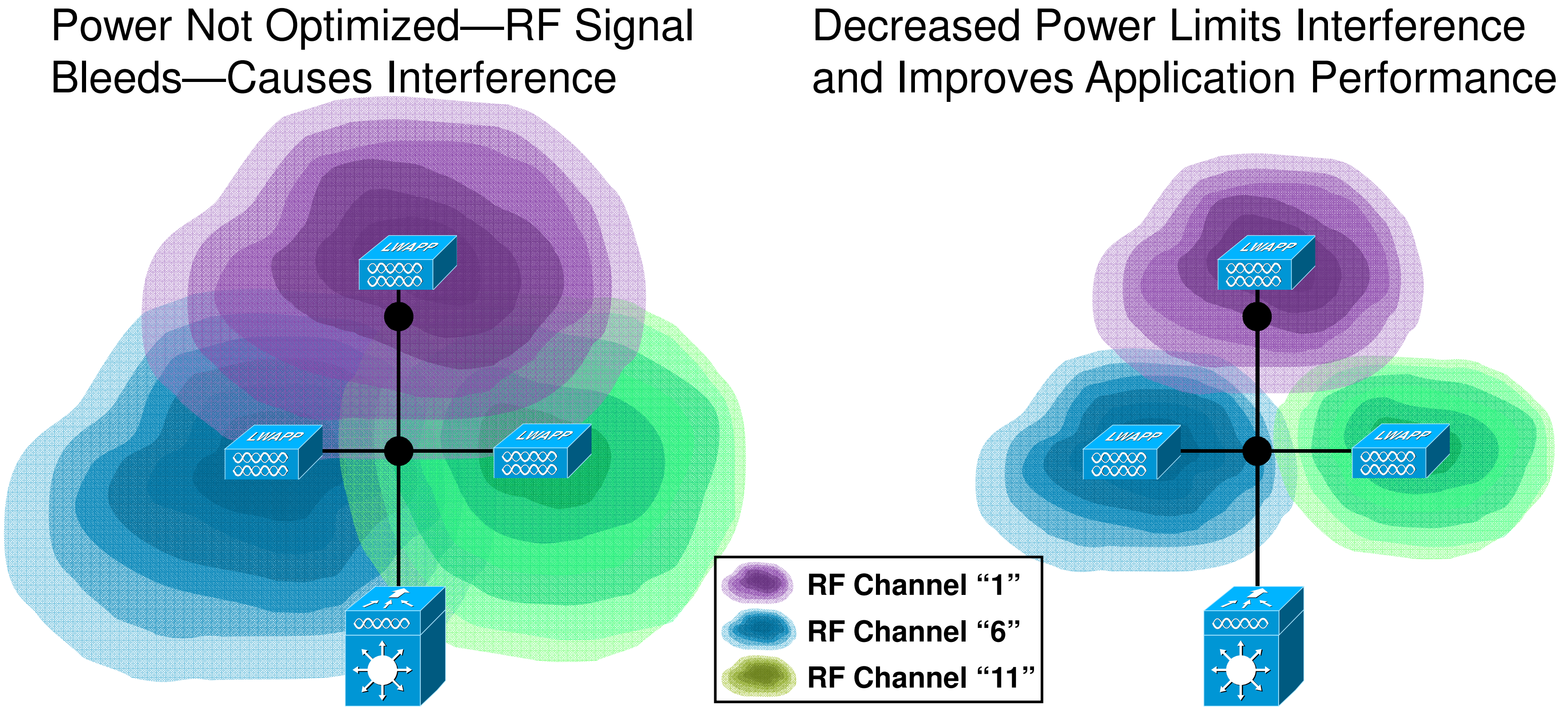


Load Profile	Okay
Coverage Profile	Okay

Interference by Channel (% busy)



RRM-Transmit Power Control



What It Does

- TX power assignment based on radio to radio pathloss
- TPC is in charge of reducing Tx on some APs—but it can also increase Tx by defaulting back to power level higher than the current Tx level (under appropriate circumstances)

TPC in a Nutshell

- Who calculates TPC

  It runs on the RF Group Leader WLC

  Decisions on TX power assignment change made on a per AP, per radio basis

- TPC viewed as a two-stage process

  Determining the ideal Tx for a radio given neighboring AP info

  Deciding if making the change from Tx_current to Tx_ideal is actually worth one's while

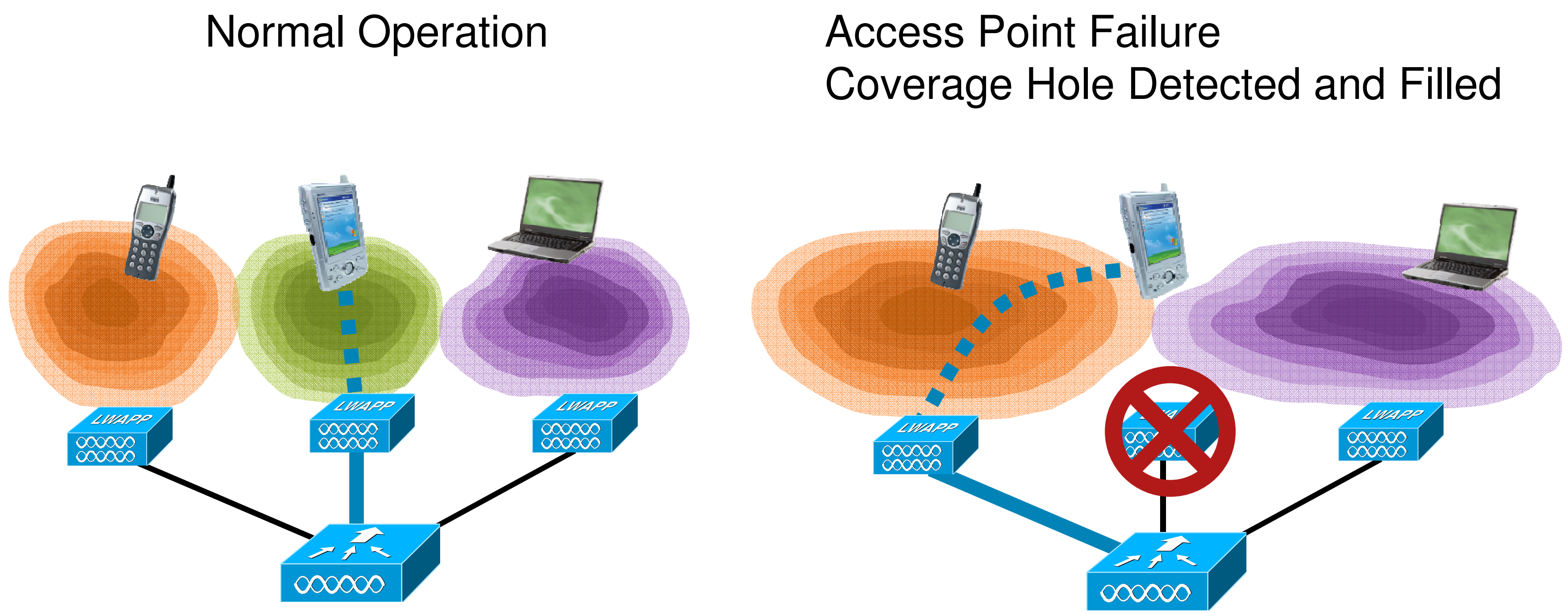
- Determining Tx_ideal for a radio

  Tx_ideal = Tx_max + (TPC_Threshold – RSSI_3rd)

- Comparing the tentative improvement vs. the hysteresis

  If change from Tx_current to Tx_ideal is small, since Tx changes can be disruptive, it may be better to leave AP's Tx as is

Radio Resource Management
Coverage Hole Detection and Mitigation



What It Does

- No single point of failure
- Automated network failover decreases support and downtime costs
- Wireless network reliability approaches wired

RRM—CHDM

- Runs on every controller independently from the RF Group Leader
- Detection—WLC
  - Determines for each client of an AP if that client is in a CH (coverage hole)
  - Keeps the count of how many of a given AP's clients are in a coverage hole
- Mitigation is dependant upon
  - CH detection—and NumFailedClients threshold
  - Decides if an AP's TX needs to be increased
  - Decides on the rate/amount of increase

Operations Are Completely Independent of TPC, but Will Affect TPC and DCA

802.11n

Agenda

- 802.11n Technology Fundamentals
- 802.11n Access Points
- Design and Deployment
  - Planning and Design for 802.11n in Unified Environment
  - Key Steps for Configuration of 11n in a Unified Environment
  - 11n Client Adapters

802.11n Advantages

Throughput	Reliability	Predictability
Increased Bandwidth for emerging and existing applications	Reduced Retries permitting low latency and delay sensitive applications such as voice	Reduced dead spots permitting consistent connectivity for every application

Technical Elements of 802.11n

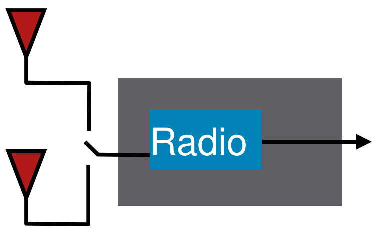
MIMO	40Mhz Channels	Packet Aggregation	Backward Compatibility

MIMO (Multiple Inputs Multiple Outputs)

- MIMO is pronounced mee-moh or my-moh
- 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
- SM—Spatial multiplexing

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

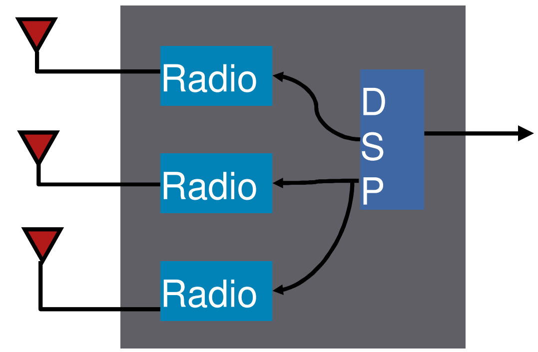
Comparing SISO and MIMO Signal Reception



- One radio chain
- Switches between antennas

  Either A or B

- Multipath degrades



- Three radio chains
- Aggregates all antennas

  A and B and C

- Multipath improves
- Better immunity to noise
- Better SNR than SISO

MIMO Radio Terminology

- TxR:S

  Transmit Antennas x Receive Antennas : Spatial Streams

- T – Transmit Antennas
- R – Receive Antennas
- S – Spatial Streams (1 = 150Mbps, 2 = 300Mbps)
- The 1250 and 1140 are 2x3:2

  Two Transmit, Three Receive, Two Spatial Streams

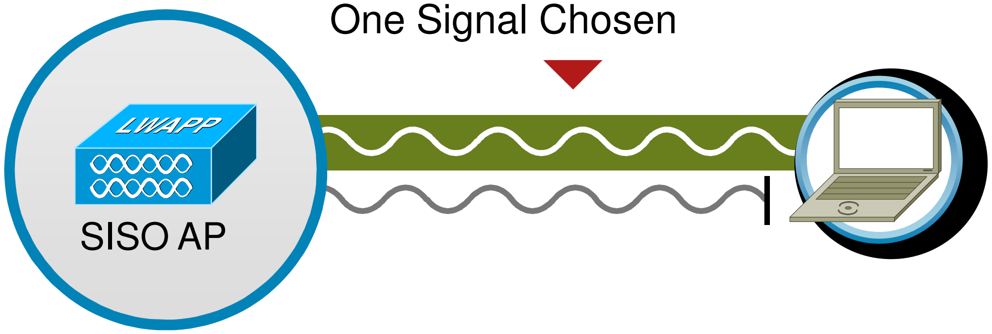
Maximum Ratio Combining

MIMO | 40Mhz Channels | Packet Aggregation | Backward Compatibility

MIMO (Multiple Input, Multiple Output)

Without MRC

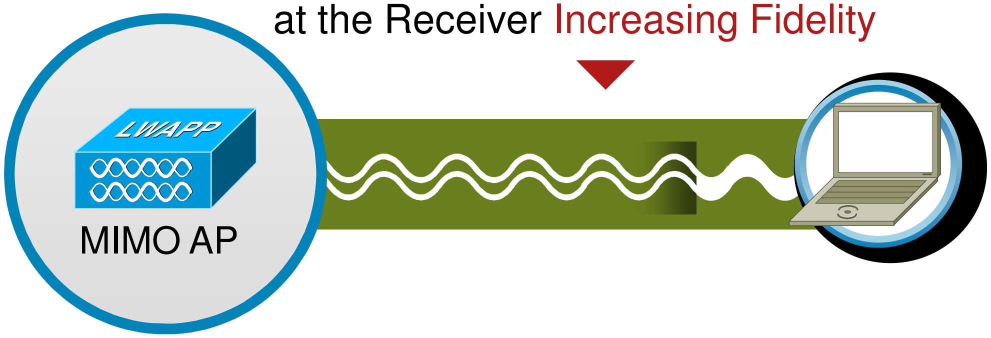
Multiple Signals Sent;
One Signal Chosen



Performance

With MRC

Multiple Signals Sent and Combined
at the Receiver Increasing Fidelity



Performance

Maximum Ratio Combining

- Performed at receiver (either AP or client)
- Combines multiple received signals
- Increases receive sensitivity
- Works with both 11n and non-11n clients
- MRC is like having multiple ears to receive the signal

Illustration of Three Multipath Reflections to SISO AP

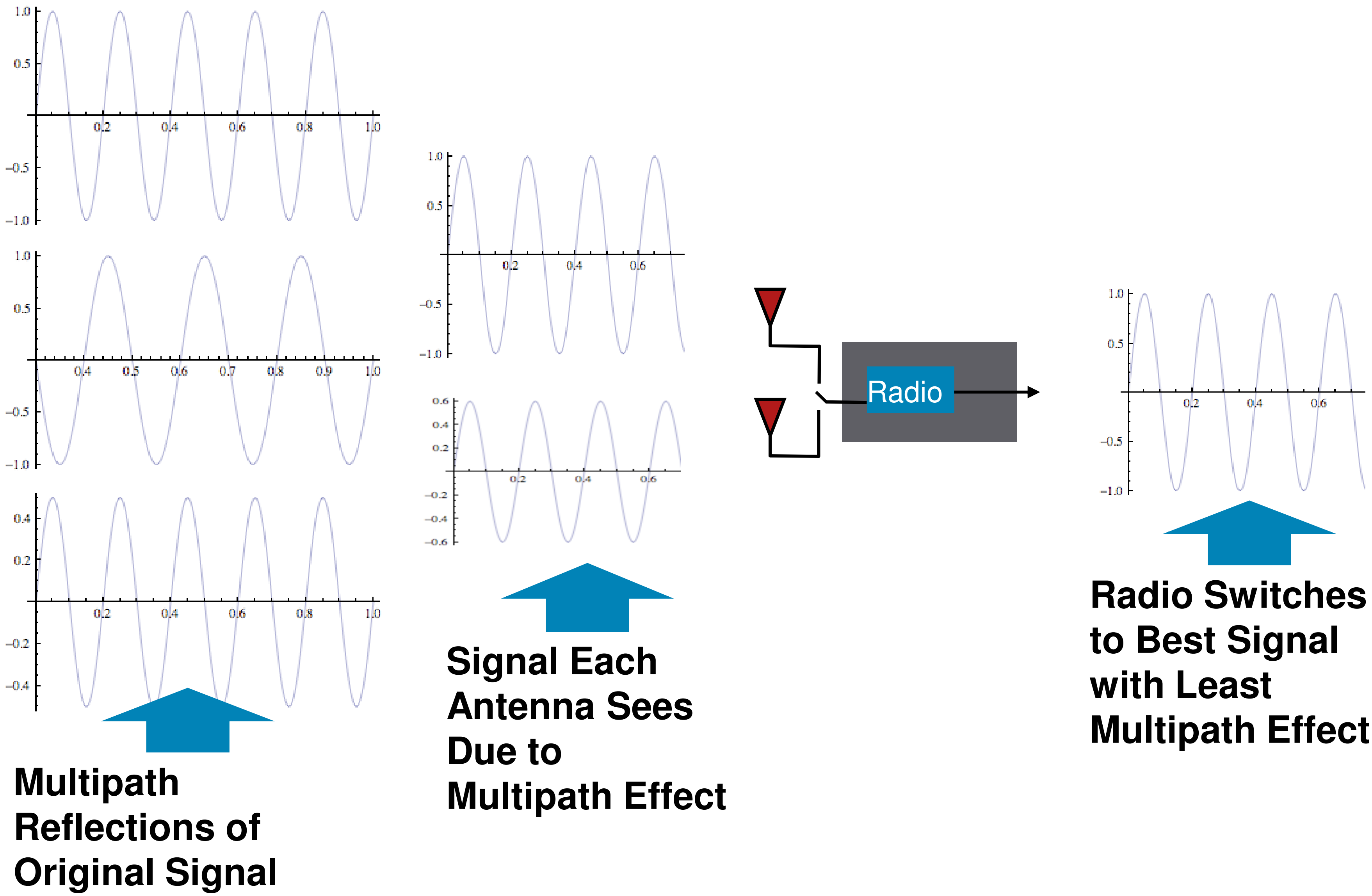
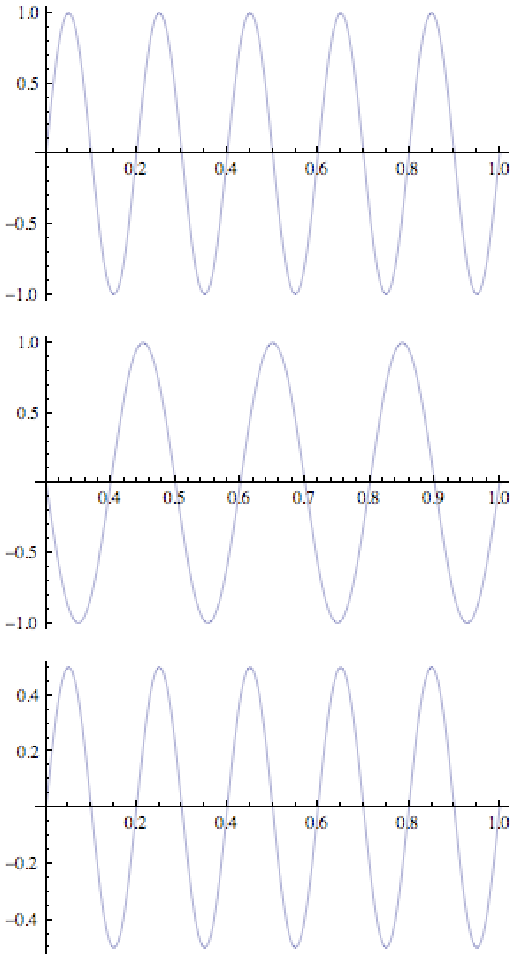
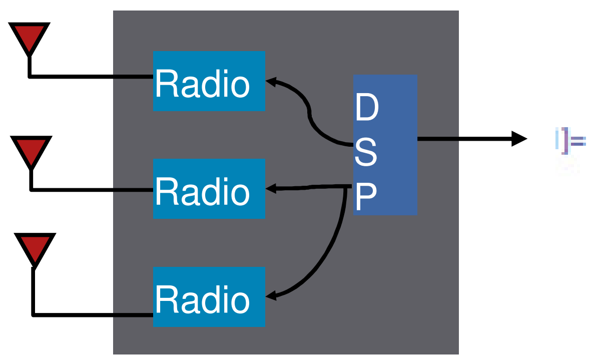


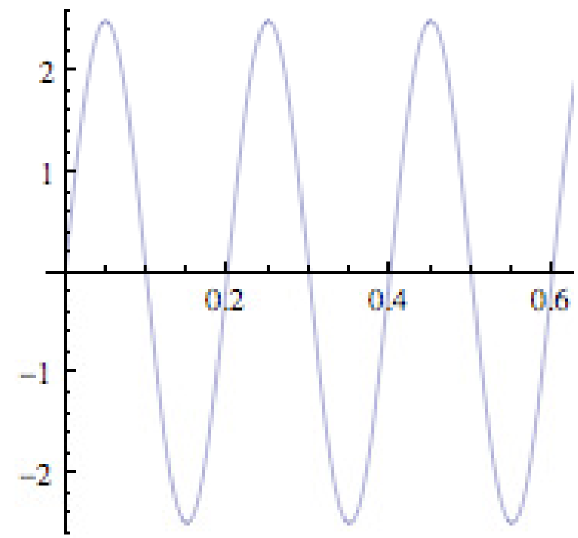
Illustration of Three Multipath Reflections to MIMO AP with MRC



Multipath Reflections of Original Signal



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



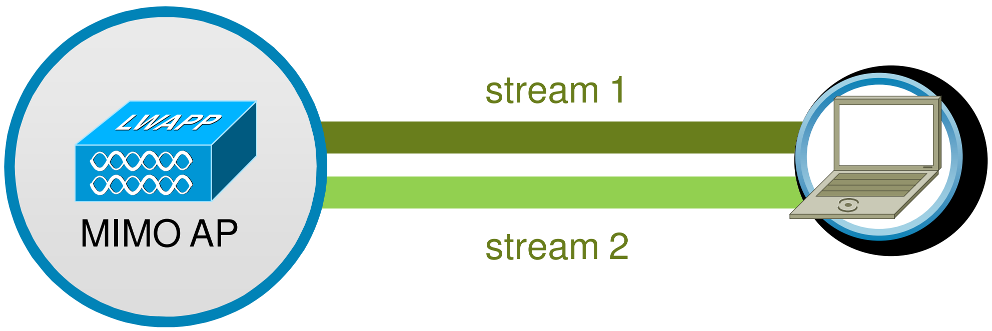
The Resulting Signal Is Addition of Adjusted Receive Signals

Spatial Multiplexing

	40Mhz Channels	Packet Aggregation	Backward Compatibility

MIMO (Multiple Input, Multiple Output)

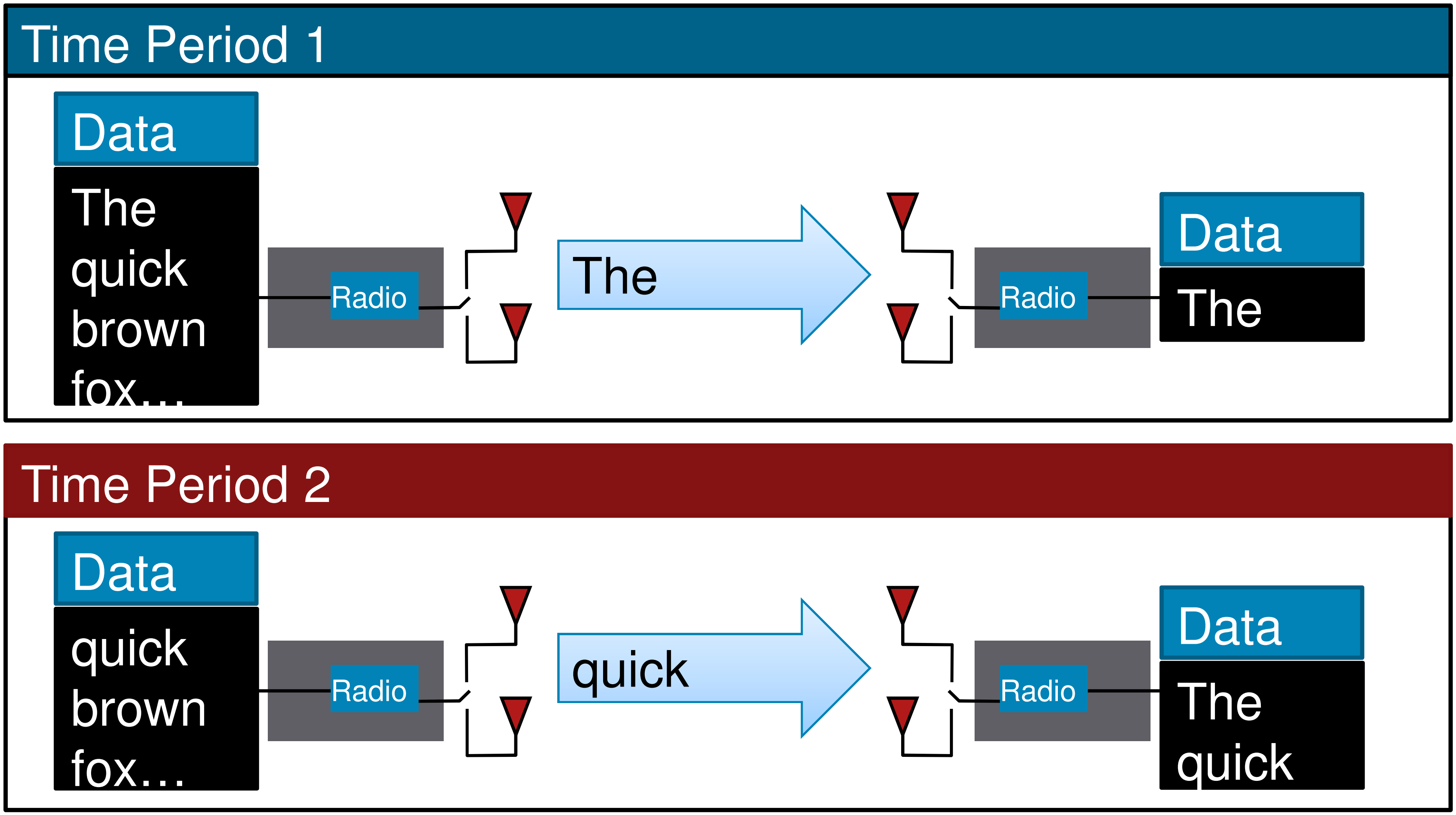
Information Is Split and Transmitted on Multiple Streams



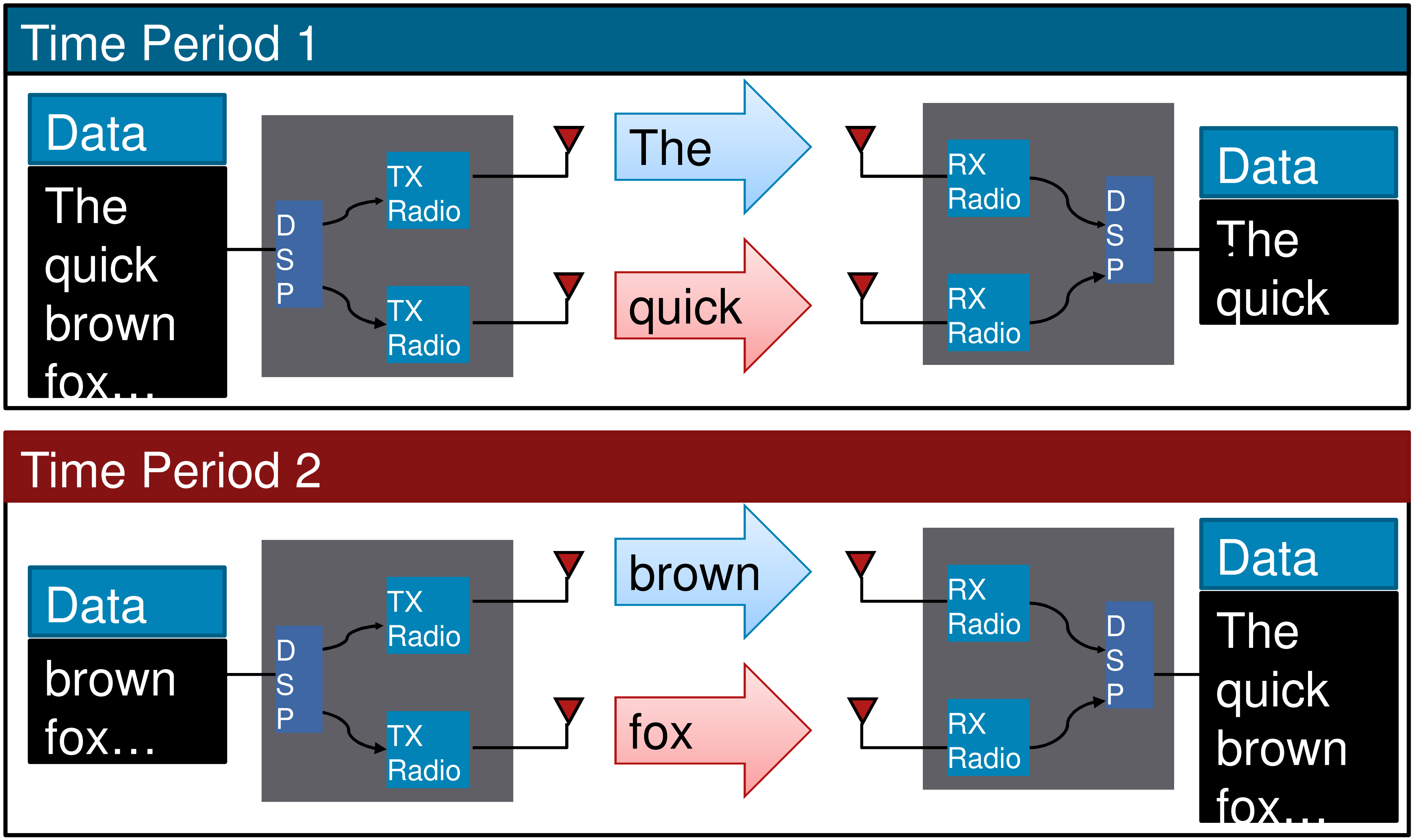
Performance

Transmitter and Receiver Participate	Concurrent Transmission on Same Channel	Increases Bandwidth	Requires 11n Client

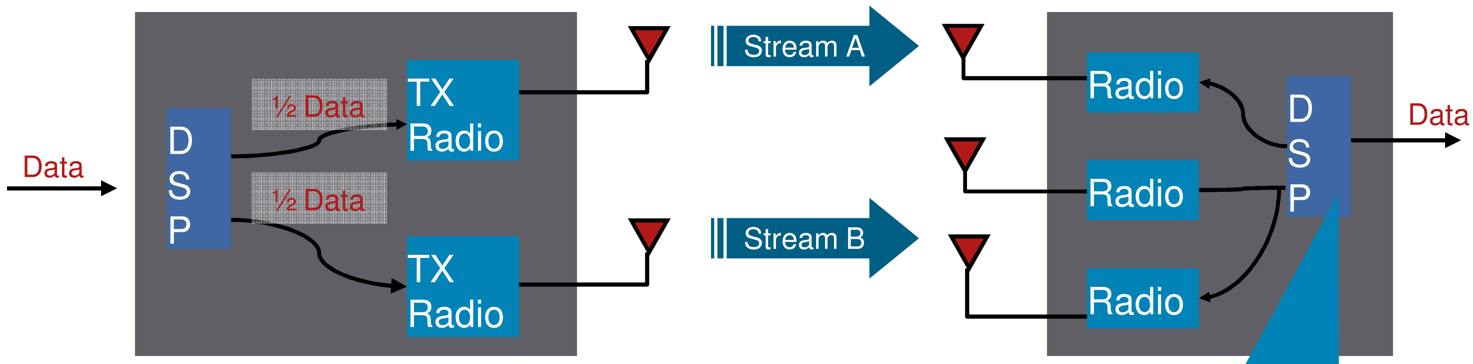
SISO Data Transmission



MIMO Spatial Multiplexing Data Transmission



More Efficient Spectrum Utilization with MIMO Spatial Multiplexing



- The data is broken into two streams transmitted by two transmitters at the same frequency

I Can Recognize the Two Streams Transmitted at the Same Frequency Since the Transmitters Have Spatial Separation Using My Three RX Antennas with My Multipath and Math Skills

Technical Elements of 802.11n

MIMO	40Mhz Channels	Packet Aggregation	Backward Compatibility

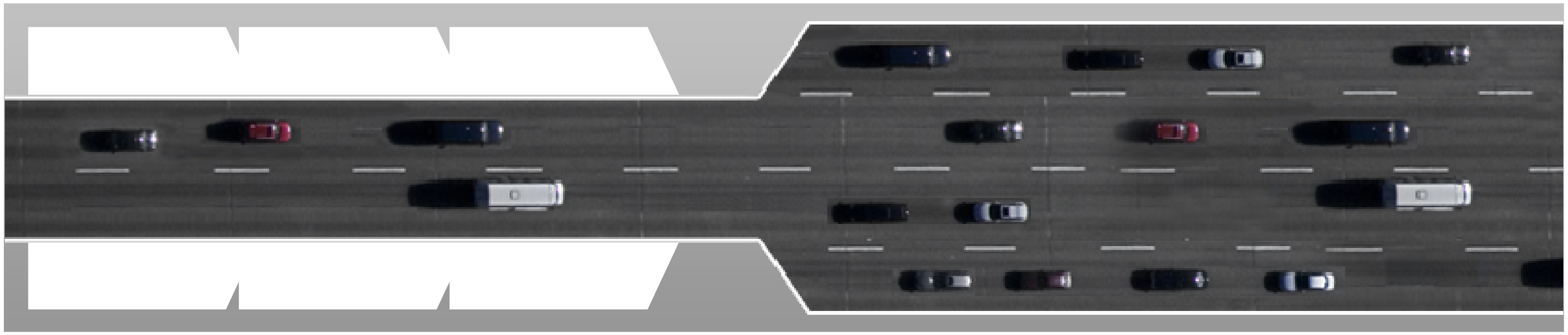
MIMO	40Mhz Channels	Packet Aggregation	Backward Compatibility

40-MHz Channels

MIMO | 40Mhz Channels | Packet Aggregation | Backward Compatibility

40Mhz Channels

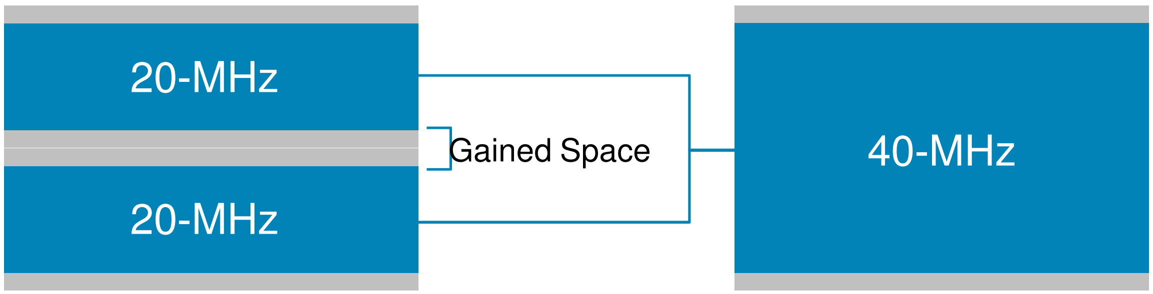
Moving from 2 to 4 Lanes



- 40-MHz = 2 aggregated 20-MHz channels—takes advantage of the reserved channel space through bonding to gain more than double the data rate of 2 20-MHz channels

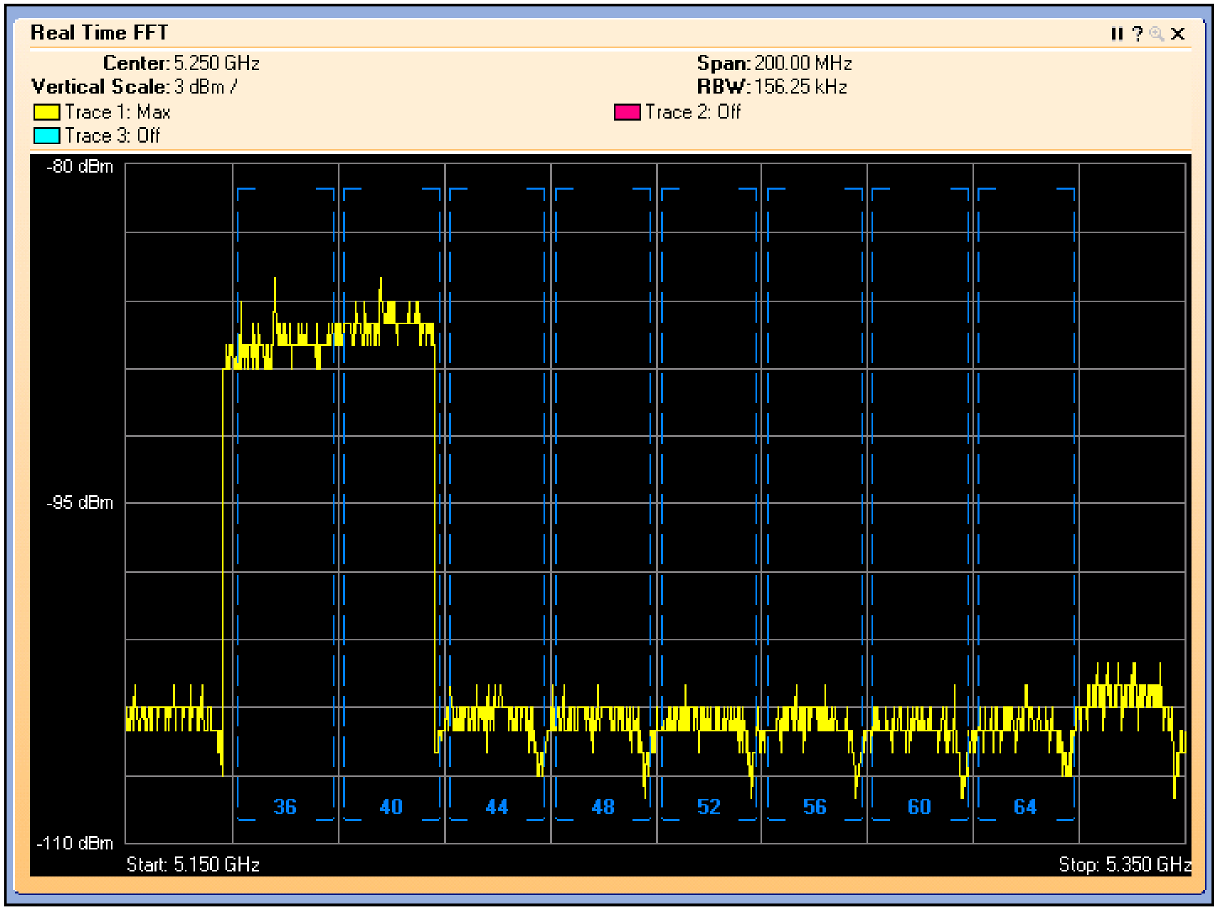
Double Wide Channel

40-MHz Wide Channel Support



- 802.11n supports 20 or 40 MHz wide channels
  - 40 MHz wide channels recommended only for 5 GHz
- Consists of a primary channel and a secondary channel also referred to as extension channel
  - Second channel must be adjacent
  - Can be above or below primary
  - Protection provided for 20 MHz wide client use

40 MHz-Wide Channel



- Spectrum Expert Trace for 40 MHz-wide channel channel 36 primary and channel 40 extension

Technical Elements of 802.11n

MIMO	40Mhz Channels	Packet Aggregation	Backward Compatibility

Aspects of 802.11n

MIMO | 40Mhz Channels | Packet Aggregation | Backward Compatibility

Packet Aggregation

Carpooling Is More Efficient Than Driving Alone

Without Packet Aggregation

802.11n Overhead | Data Unit: Packet

802.11n Overhead | Data Unit: Packet

802.11n Overhead | Data Unit: Packet

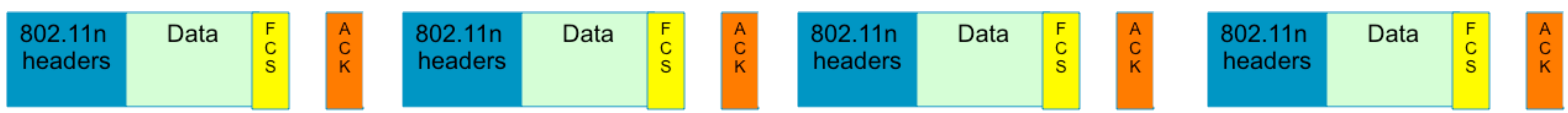
802.11n Overhead | Data Unit: Packet, Packet, Packet

With Packet Aggregation

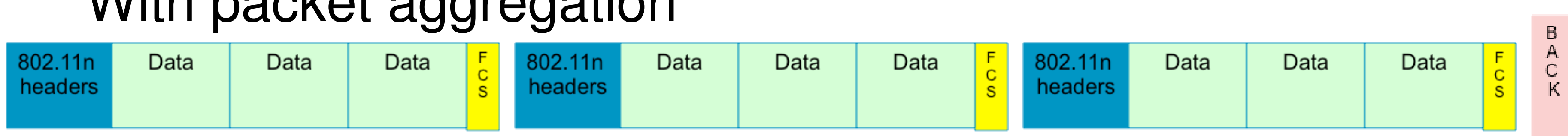
Packet Aggregation

- All 11n devices must support receiving of either packet aggregation method A-MPDU or A-MSDU
- A-MPDU packet aggregation is what 1250 and 1140 will use for packet aggregation with block acknowledge

Without packet aggregation



With packet aggregation



Technical Elements of 802.11n

MIMO | 40Mhz Channels | Packet Aggregation | Backward Compatibility

MIMO

40Mhz Channels

Packet Aggregation

Backward Compatibility

Aspects of 802.11n

MIMO	40Mhz Channels	Packet Aggregation	Backward Compatibility

Backward Compatibility

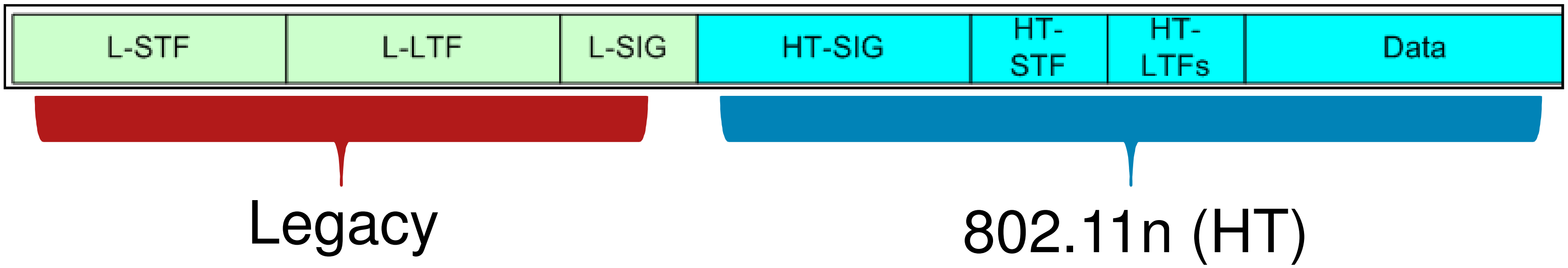
2.4GHz

11n Operates in Both Frequencies

5GHz

802.11ABG Clients Interoperate with 11n AND Experience Performance Improvements

802.11n HT PHY

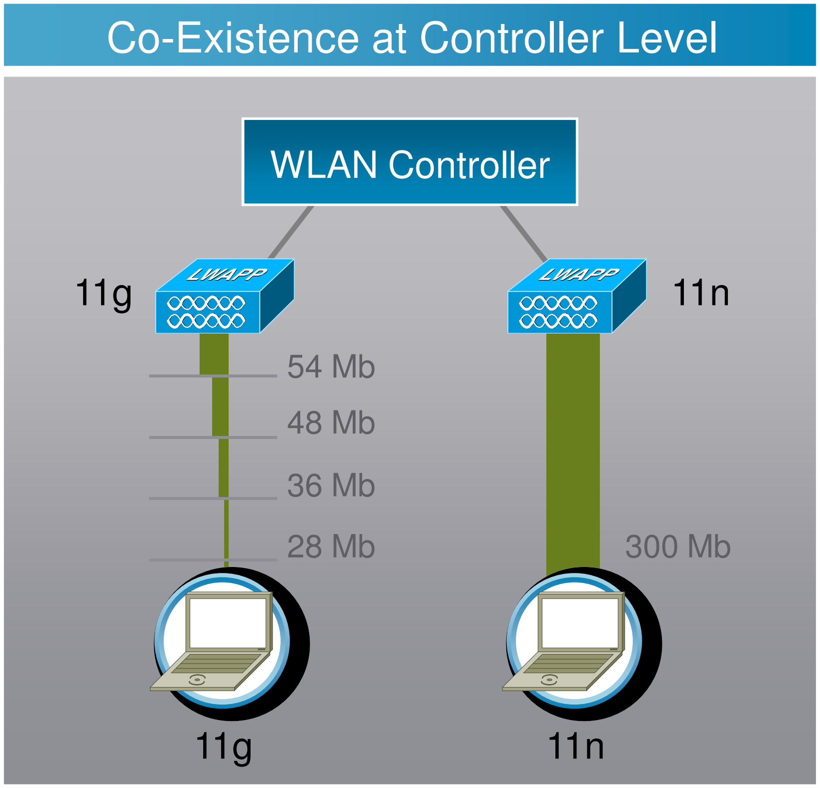


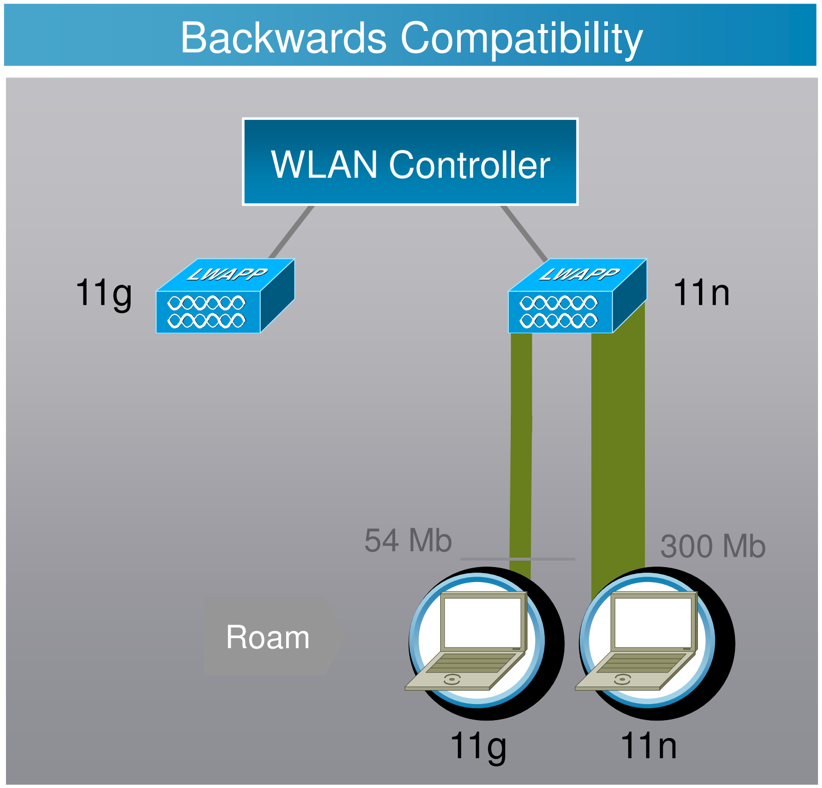
- To provide legacy co-existence all 11n transmissions today use a mixed mode PHY that encapsulates the HT PHY in the Legacy PHY when transmitting at HT rates
- Legacy devices degrade 11n device performance based on duty cycle they use in the spectrum

Backward Compatibility & Co-Existence

- Co-existence of ABG/N APs
- Benefits of 11n accrue to ABG clients

  MIMO benefits ABG clients on the AP receive side from MRC





802.11n Data Rates

MCS—Modulation and Coding Scheme

- 802.11a/b/g used data rates
- 802.11n defines MCS rates
- 77 MCS rates are defined by standard
- 1140 and 1250 support 16 (MCS 0-15)
  - Eight are mandatory
- Best MCS rate is chosen based on channel conditions
- MCS specifies variables such as
  - Number of spatial stream, modulation, coding rate, number of forward error correction encoders, number data subcarriers and pilot carriers, number of code bits per symbol, guard interval

MCS Chart

MCS Index	Modulation	Spatial Streams	802.11n Data Rate			
			20 MHz		40 MHz	
			L-GI	S-GI	L-GI	S-GI
0	BPSK	1	6.5	7.2	13.5	15
1	QPSK	1	13	14.4	27	30
2	QPSK	1	19.5	21.7	40.5	45
3	16-QAM	1	26	28.9	54	60
4	16-QAM	1	39	43.3	81	90
5	64-QAM	1	52	57.8	108	120
6	64-QAM	1	58.5	65	122	135
7	64-QAM	1	**65**	**72.2**	**135**	**150**
8	BPSK	2	13	14.4	27	30
9	QPSK	2	26	28.9	54	60
10	QPSK	2	39	43.3	81	90
11	16-QAM	2	52	57.8	108	120
12	16-QAM	2	78	86.7	162	180
13	64-QAM	2	104	116	216	240
14	64-QAM	2	117	130	243	270
15	64-QAM	2	**130**	**144**	**270**	**300**

Maximum with 1 spatial stream

Maximum with 2 spatial streams

A Few More 802.11n Features Used to Increase Performance

- Beam forming
- Reduced inter-frame spacing
- Reduced guard interval

  From 800ns to 400ns between 'symbols'

- QAM 64

Cisco Next-Generation Wireless Portfolio

- Cisco Aironet 1140 Series
  - Carpeted Indoor Environments
  - Easy to Deploy-Sleek design with integrated antennas
  - 802.11n performance with efficient 802.3af power
  - Blends seamlessly into the environment

- Cisco Aironet 1250 Series
  - Rugged Indoor Environments
  - Versatile RF coverage with external antennas
  - Flexible power options for optimal RF coverage

11a/g to 11n Access Point Migration

Indoor Environments

Integrated Antennas

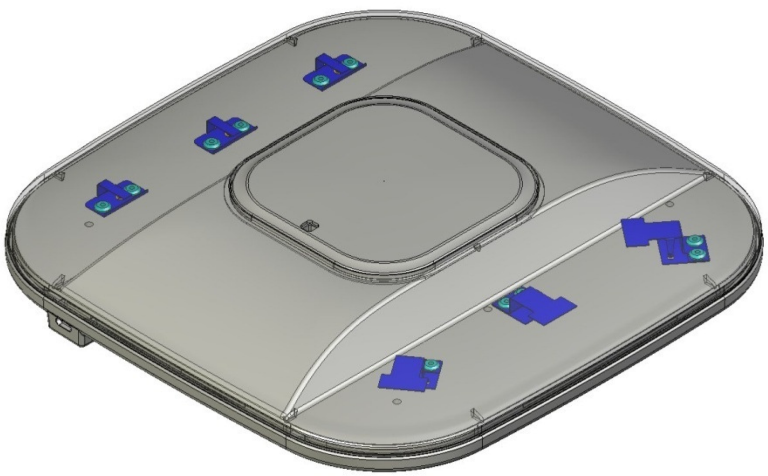
Rugged Environments

Antenna Versatility

Still Three Antennas per Band

1250

1140



2.4GHz – 4dBi

5GHz – 3dBi

Planning and Design for 802.11n

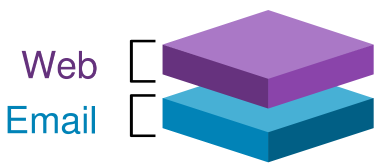
**

Phases of an 11n Deployment

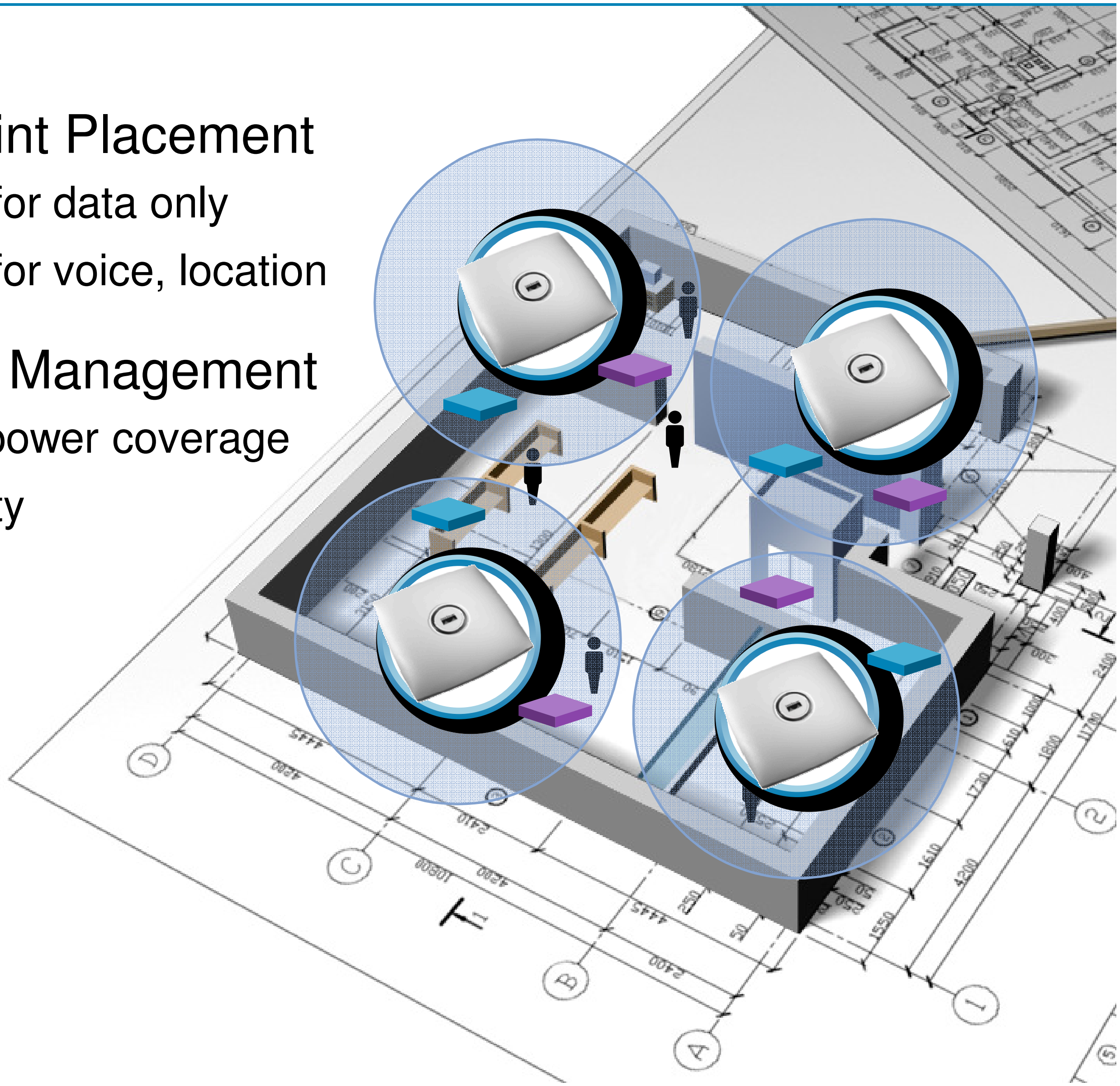
- Design Considerations
  - 1:1 Replacement Strategy for Capacity
  - 5GHz Strategy
- Planning
  - WCS Planning Tool
  - Infrastructure Considerations
- Deployment
  - Site Survey
- Operation
  - Configuration (40MHz RRM, Data Rates, Security, etc.)
  - Tracking and augmenting controller capacity

1130 Access Point Placement

- 1130 Access Point Placement
  - 1 per 5,000 sq feet for data only
  - 1 per 3,000 sq feet for voice, location
- Radio Resource Management
  - Adaptive channel / power coverage
  - Operational simplicity

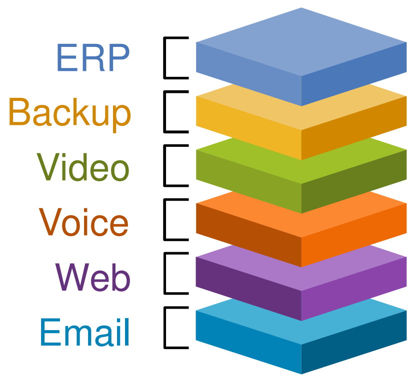


Several Supported Apps

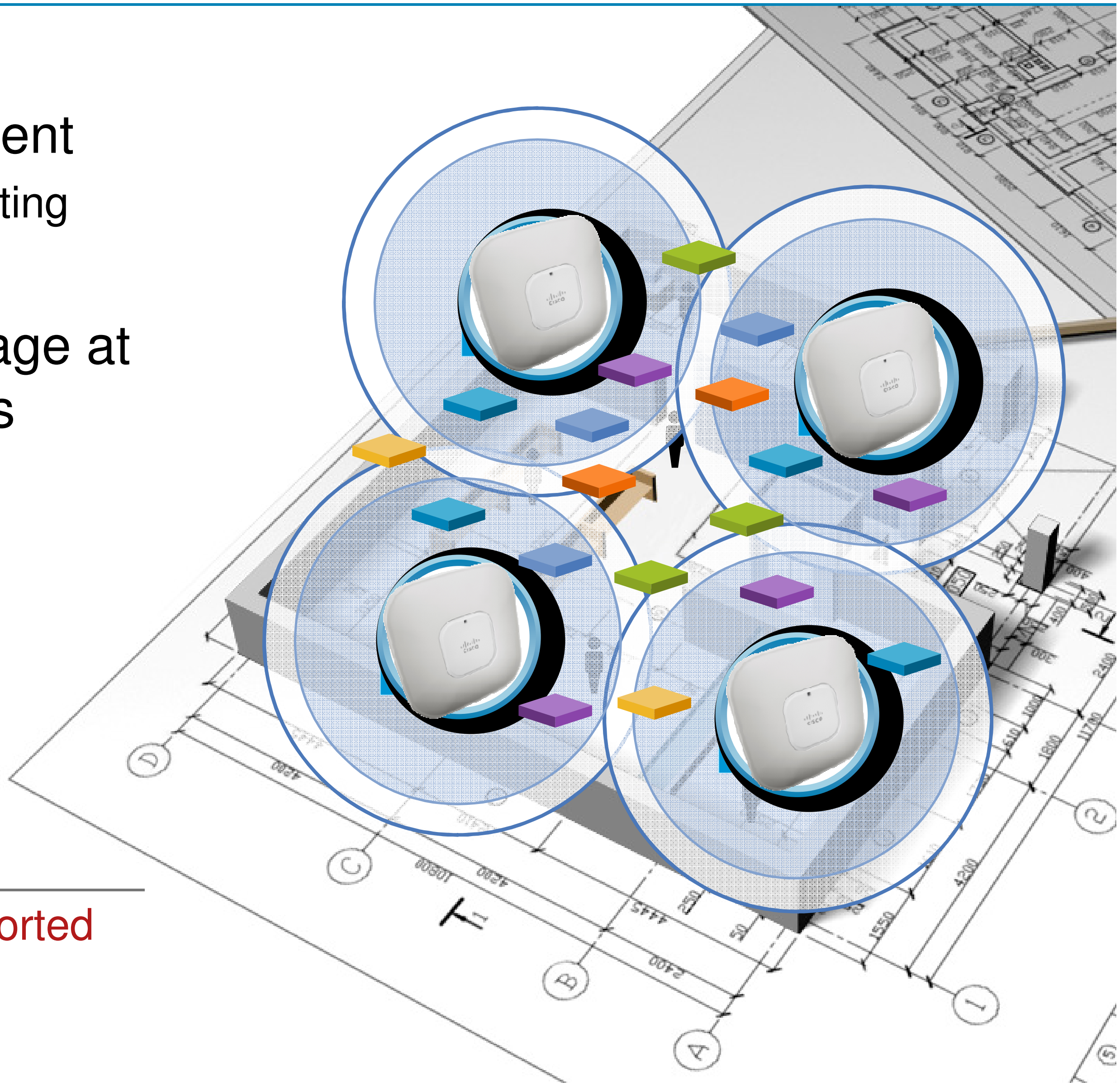


1140 Access Point Placement

- 1 for 1 replacement
  AP1140 reuses existing
  AP1130 T-Rail Clip
- Improved coverage at higher data rates



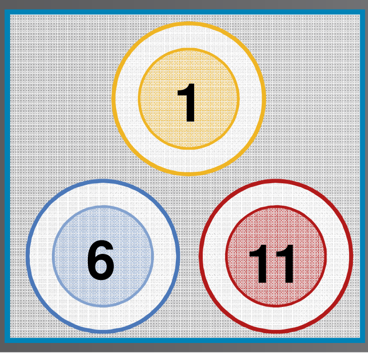
More Applications Supported at Any Given Location

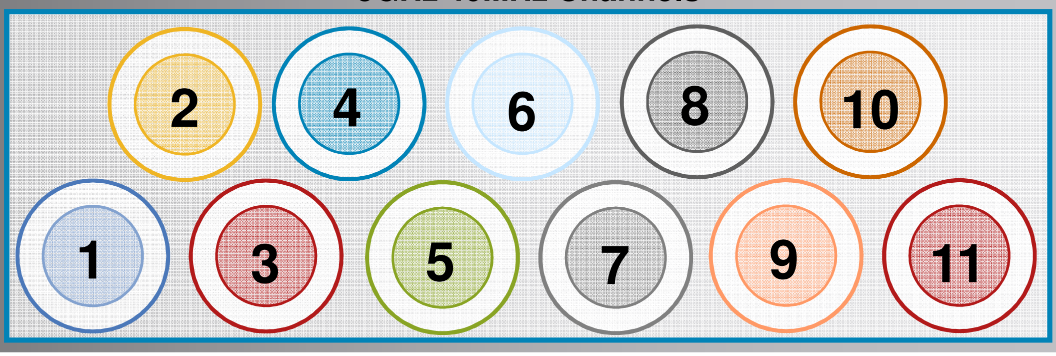


Effective Frequency Use—5GHz and 2.4GHz

Create a 5GHz Strategy

- 5GHz Recommended for 802.11n
  - More available spectrum—greater number of channels
  - Reduced interference (no Bluetooth, Microwave Ovens, etc.)
  - Maximum throughput in a 40MHz channel
  - Many 11n devices only support 40MHz in 5GHz
- 2.4GHz still benefits from MIMO and packet aggregation

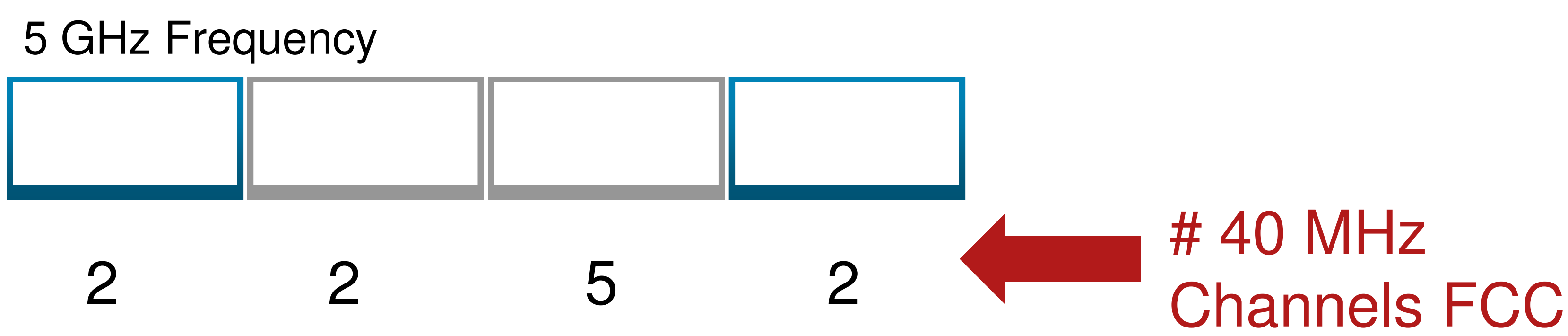




Capacity Principles

Channel Capacity: Use 5 GHz and 2.4 GHz

- 2.4 GHz clients using N will consume less spectrum
- 5 GHz will provide the most capacity for 802.11n clients
  - More available spectrum—greater number of channels
  - Greater speeds dues to 40 MHz channel the fact that many devices will only support 40 MHz channel in 5 GHz
- DFS support allows up to 11–40 MHz wide channels to be used in 5 GHz band
  - If radar is detect in the area some UNI2 and UNI2 channels may disabled



11n Deployment

Site Survey Recommendations

- Use "Active Survey" tools

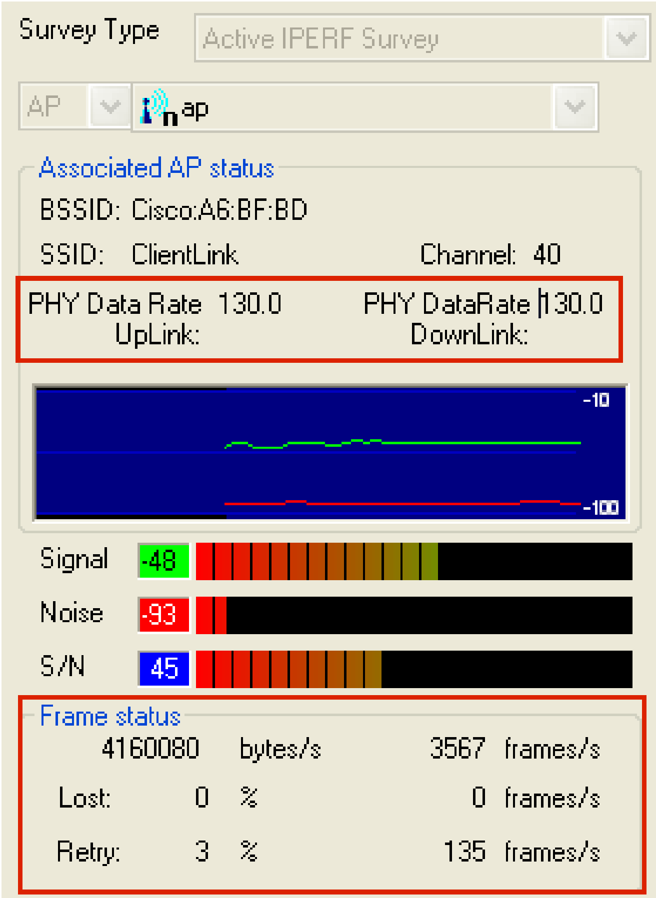
  AirMagnet 6.0 uses Iperf to send traffic when surveying to measure actual data link speeds

- Survey for lowest common client

  Once for 11a/g clients

  Once for 11n clients (optional)

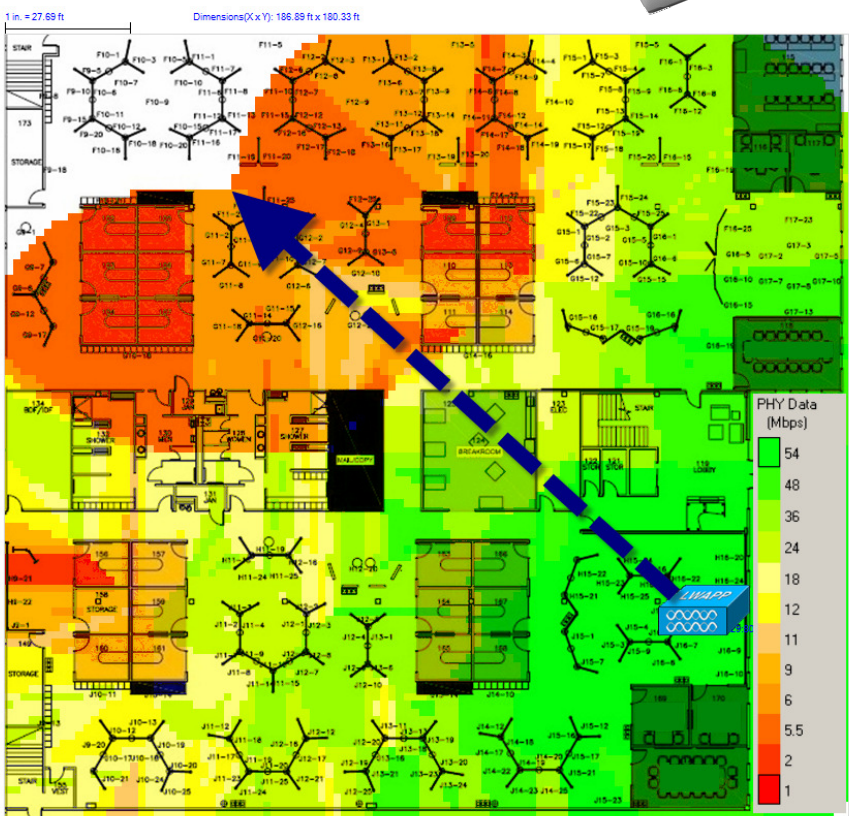
- Survey at intended AP power levels

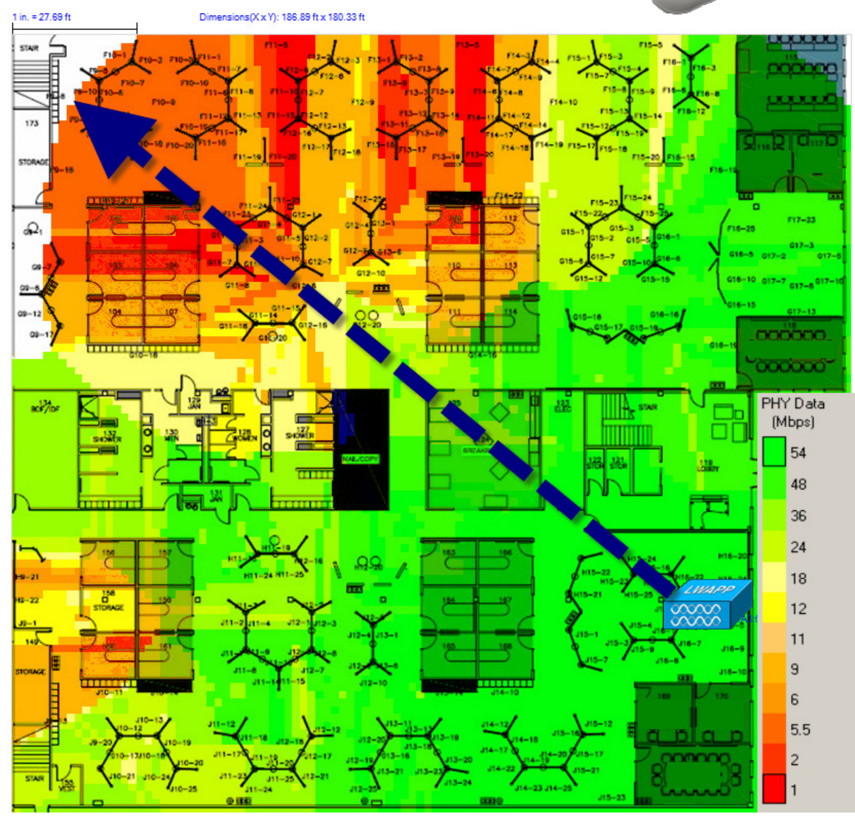


2.4GHz - Maximum Range

AP1130 – 2.4GHz

AP1140 – 2.4GHz

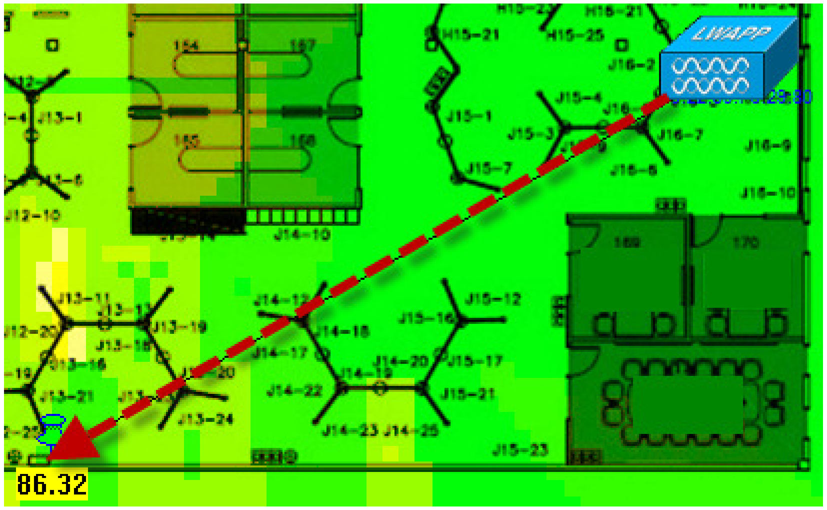


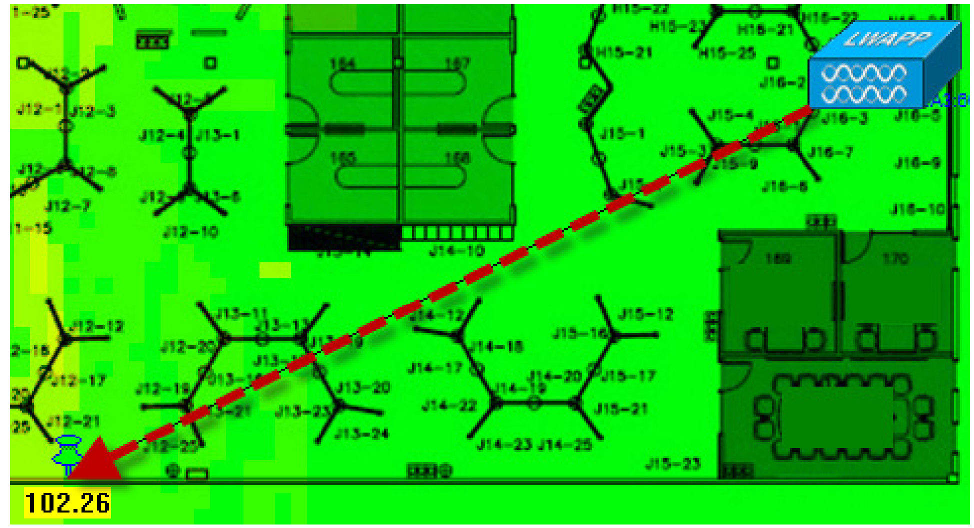


10% Increase in 802.11g Range

Improved 802.11g Coverage

1130 vs. 1140—11G Active Survey





1130 11G Survey

8 Mbps Coverage

86 Feet

0 11G Survey

Mbps Coverage

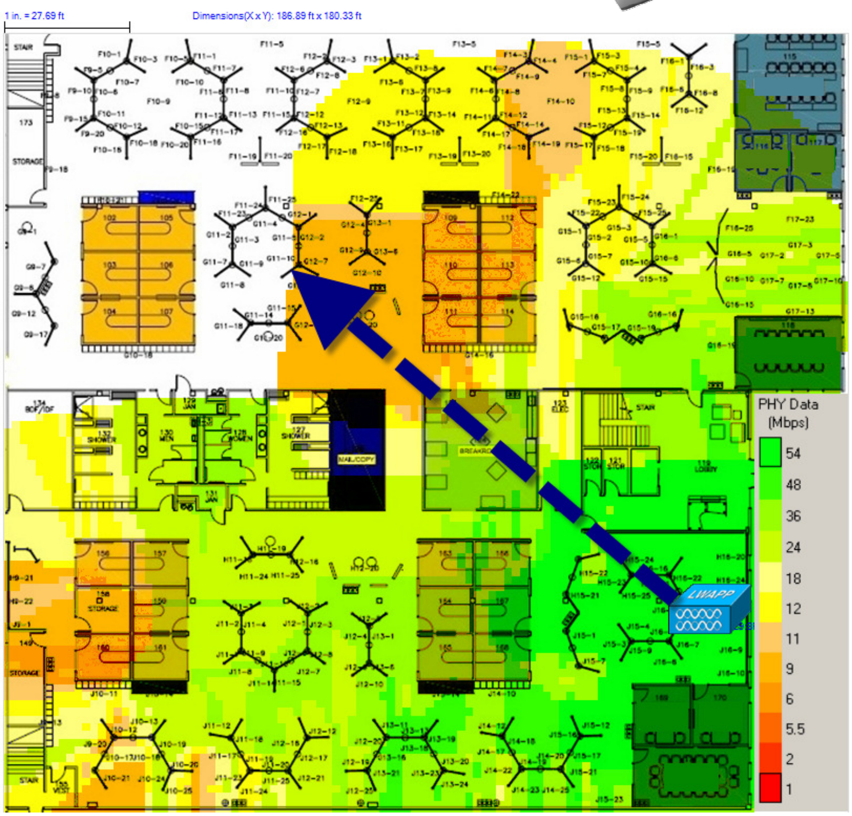
102 Feet

- Note the more uniform coverage of high (green) data rates

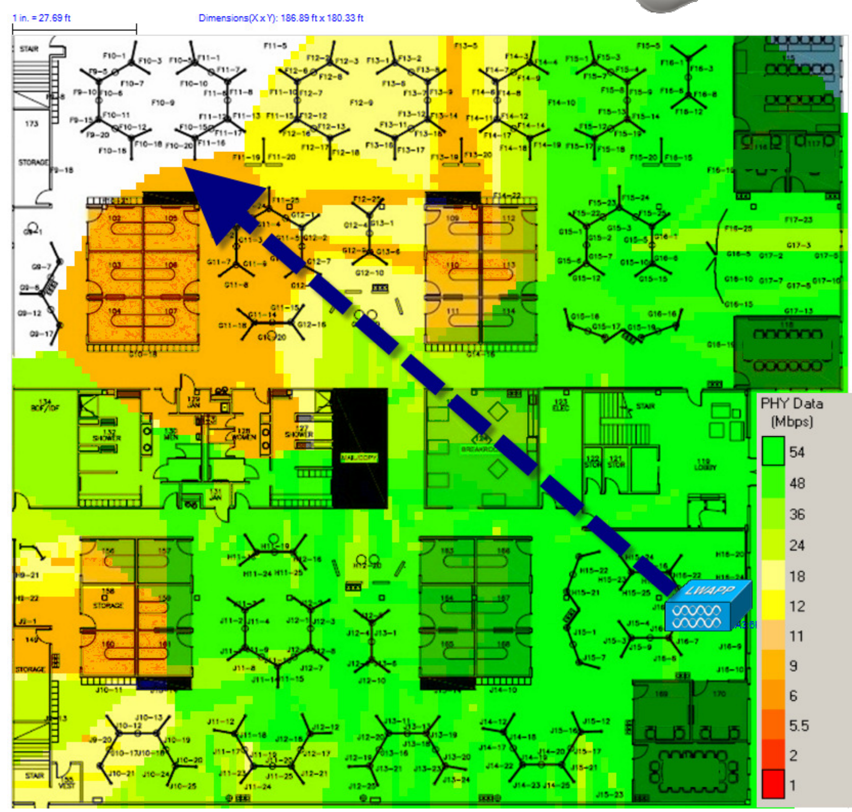
18% Increase in 802.11g Coverage

5GHz - Maximum Range

AP1130 – 5GHz



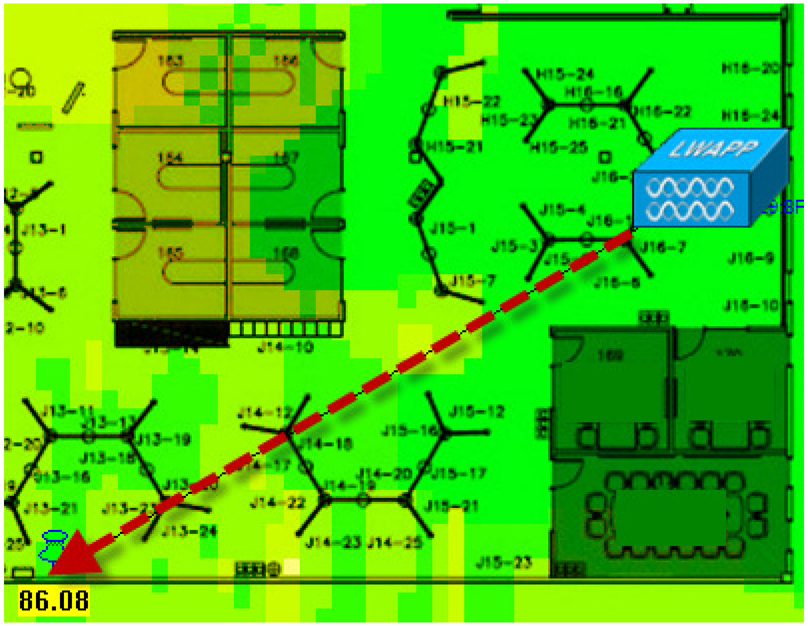
AP1140 – 5GHz

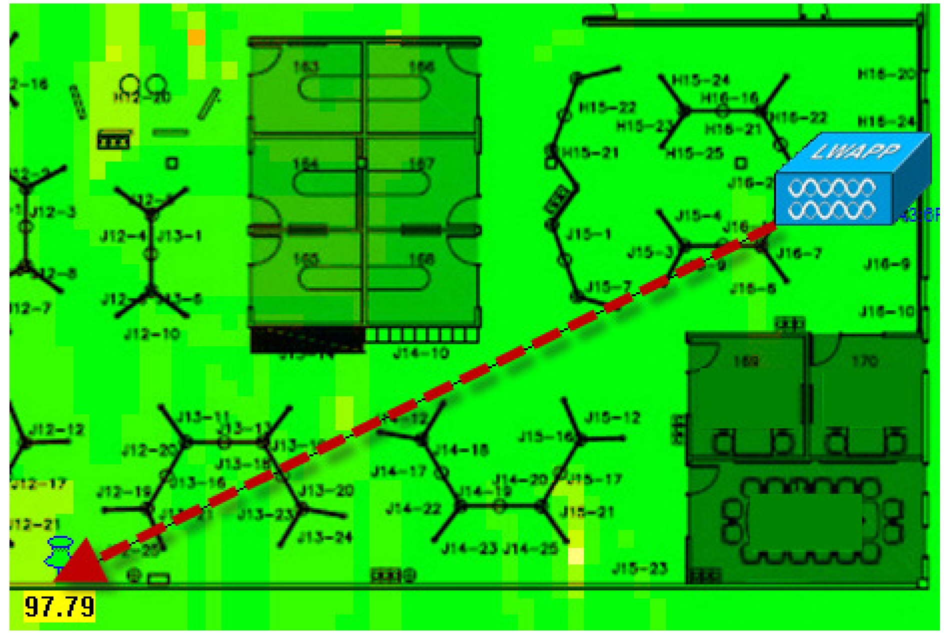


10-15% Increase in 802.11a Range

Improved 802.11a Coverage

1130 vs. 1140—11A Active Survey





1130 11A Survey

48 Mbps Coverage

86 Feet

1140 11A Survey

Mbps Coverage

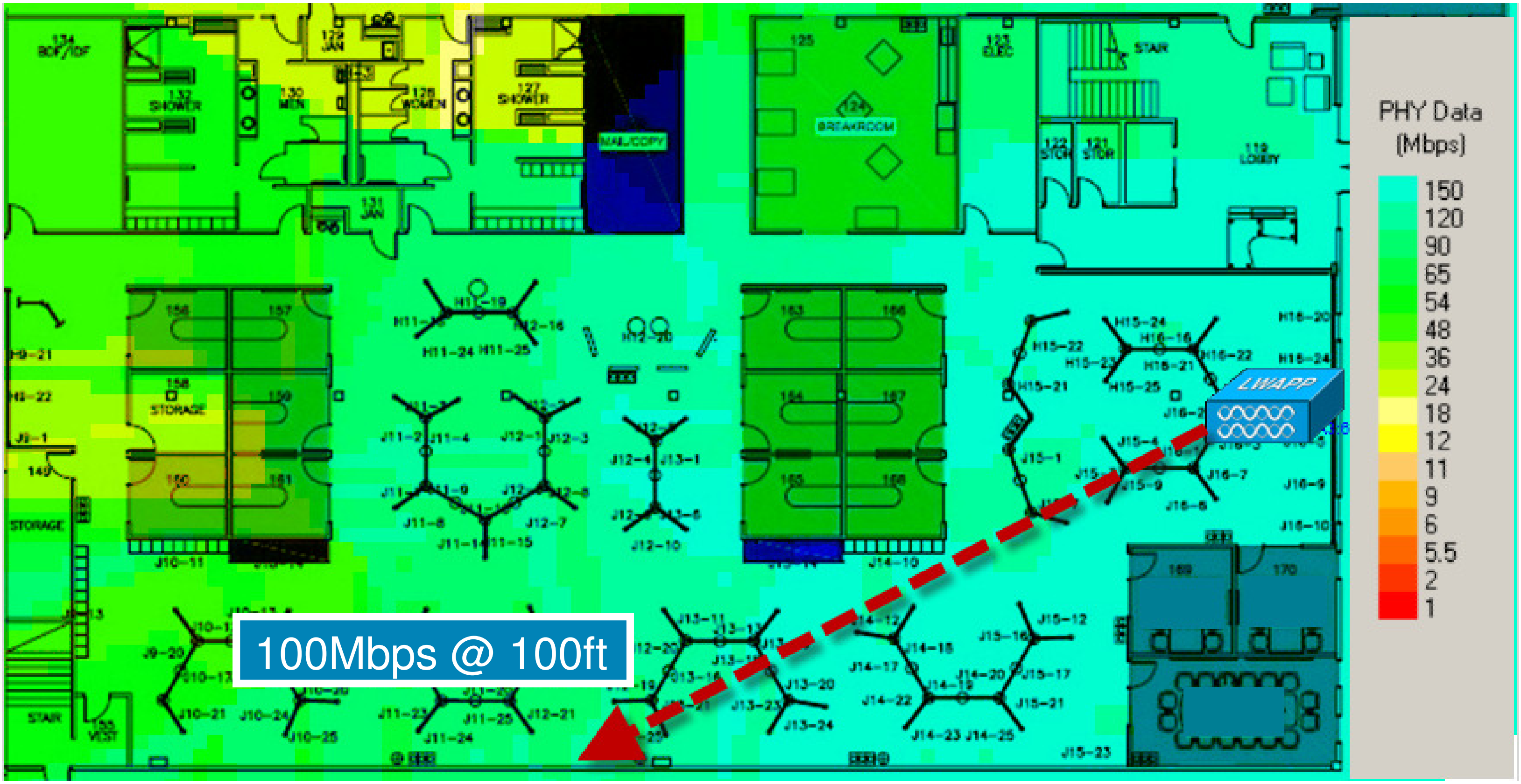
97 Feet

- Note the more uniform coverage of high (green) data rates

12% Increase in 802.11a Coverage

802.11n Coverage

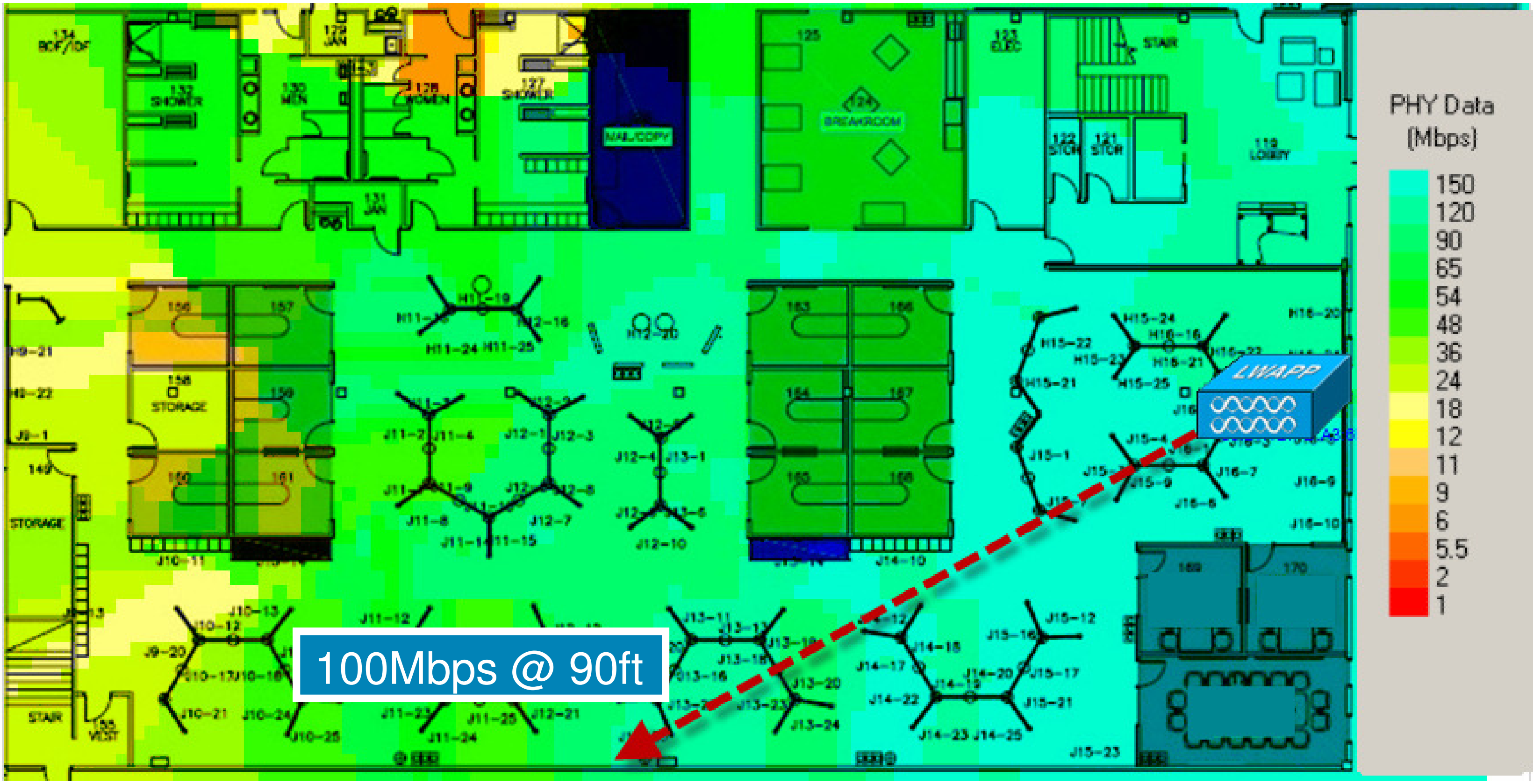
2.4GHz – 20MHz Channel Size



- Maximum of 144Mbps in a 2.4GHz 20MHz channel
- At 100ft average data rate is 100Mbps

802.11n Coverage

5GHz – 20MHz Channel Size

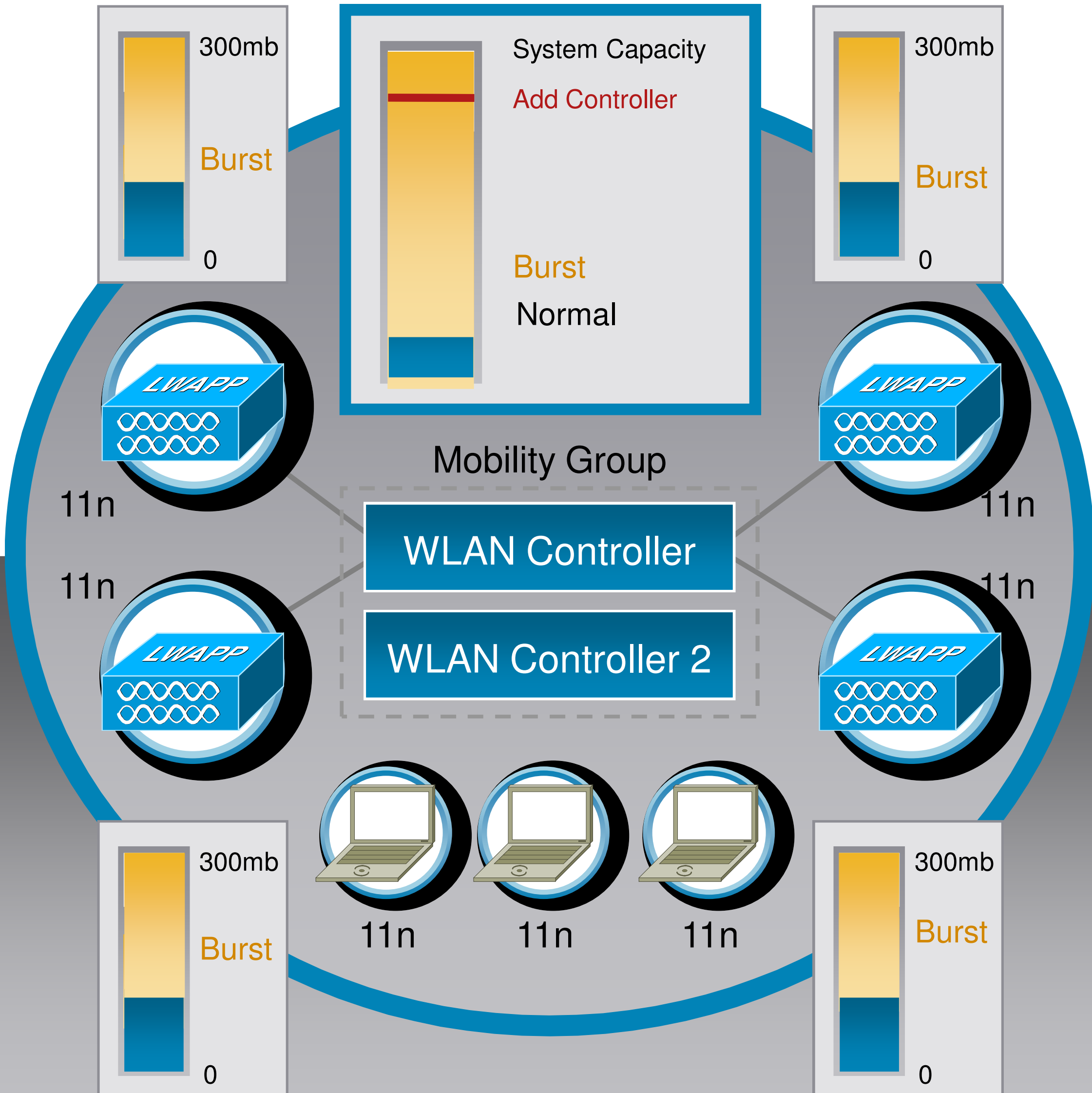


- Maximum of 144Mbps in a 5GHz 20MHz channel
- At 90ft average data rate is 100Mbps

Five Principles for Maximizing Capacity with 802.11n

1. Design for 5 GHz 40 MHz wide channels and increased cell density
2. Design for lowest common denominator legacy clients
   - Plan to migrate client devices to 11n
   - Disable lower legacy rates
3. Minimize noise and interference effects
   - Use RRM for interference avoidance
   - Use Spectrum Expert to find interference source
4. Design for GigE to APs
5. Specify a good 802.11n client adapter

Network Capacity and Scalability



- Plan for system level capacity, not per AP capacity
- Plan for throughput (60% of data rate)
- Additional controller increases capacity and improves availability
- Typical Ethernet network oversubscription is 20:1

Improving Mixed Mode Performance

Disabling Unnecessary Data Rates

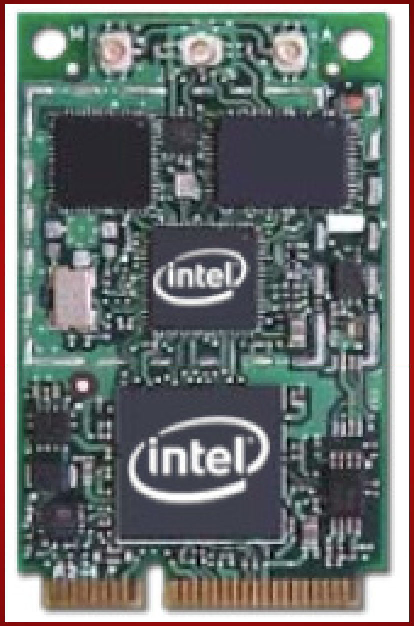
- Benefit: Beacons and Broadcast traffic utilize less “airtime”
- For 802.11b/g deployments
  Disable: 1, 2, 5.5, 6 and 9Mbps
- For 802.11g-only deployments
  Disable: 1, 2, 5.5, 6, 9 and 11Mbps
- For 802.11a deployments
  Disable: 6 and 9 Mbps
- Higher rates can also be disabled (ex. 12, 18Mbps) – <u>dependant on deployment</u>

Tuned 802.11b/g Data Rates:

Data Rates**

1 Mbps	Disabled
2 Mbps	Disabled
5.5 Mbps	Disabled
6 Mbps	Disabled
9 Mbps	Disabled
11 Mbps	Mandatory
12 Mbps	Supported
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

802.11n
Client Adapters



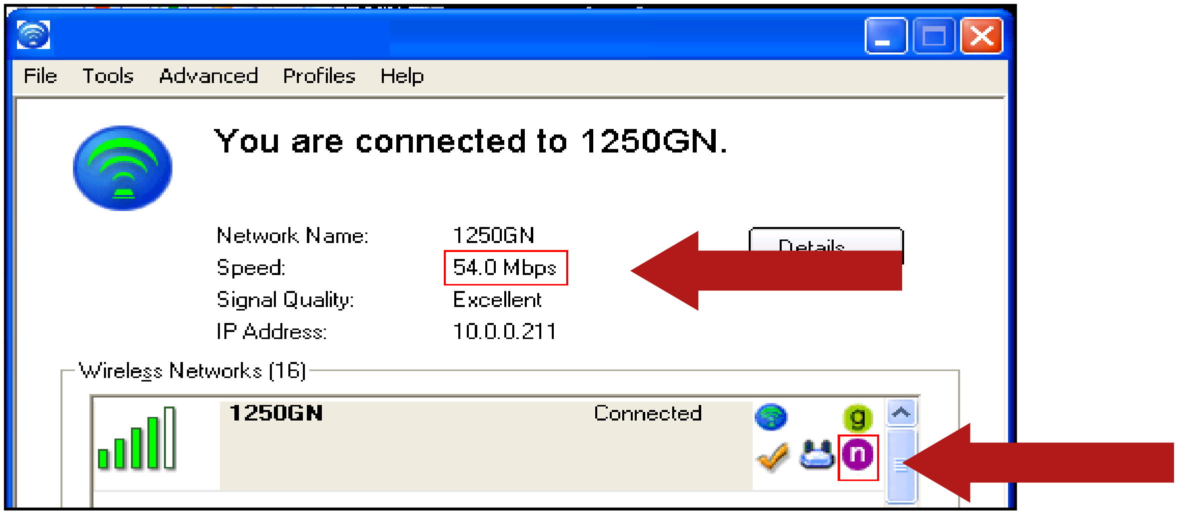
11n Client Adapters

- Make sure adapter is 11n Draft 2.0 certified by WiFi Alliance - http://www.wi-fi.org
- 802.11n adapters have a major influence on performance levels that can be achieved
- Built-in 11n adapters out perform add-on
  - USB and PCMCIA 11n adapters have less than optimal antenna placement
- Not realistic to upgrade most older laptops with internal 11n adapters
  - Need three antennas connectors

11n Client Adapter Recommendations

- Update 802.11n client drivers to the latest revision
- Cisco-Intel relationship means that the Intel 11n adapter with Cisco's APs have had the most test time

Client Shows 11n SSID But Does Not Connect at 11n Data Rates

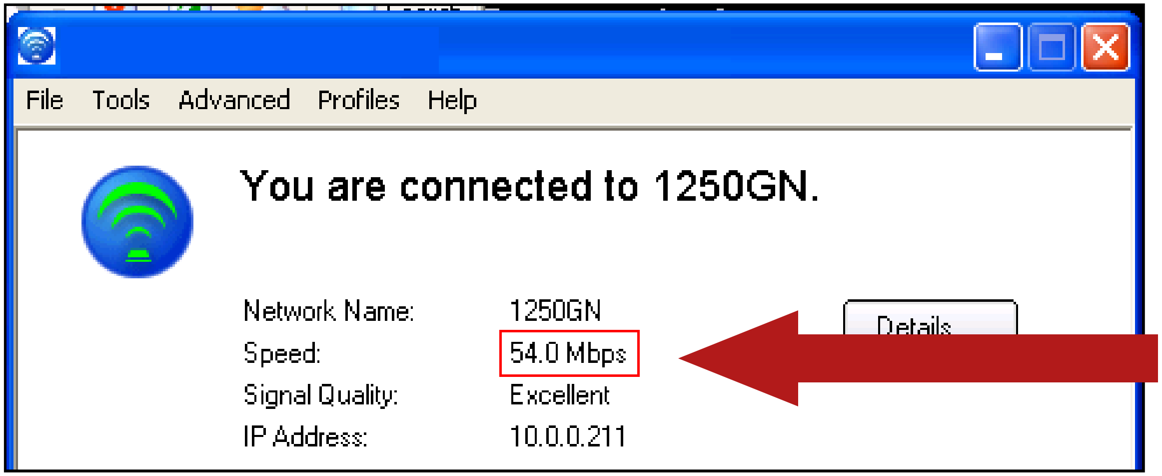


- Does the client have a 11n adapter?

  Some legacy clients will show that the AP support 11n even though the that client does not support 11n

- Is 11n support enabled in adapter driver?

Have 11n Adapter and Still Connecting at A or G Rates



- What type of encryption is allowed for WLAN?

  Must be AES or None

  If WEP or TKIP will not support 11n HT rates

- Is WMM allowed?

  WMM must be Enable or Require

  If WMM disabled will not support 11n HT rates

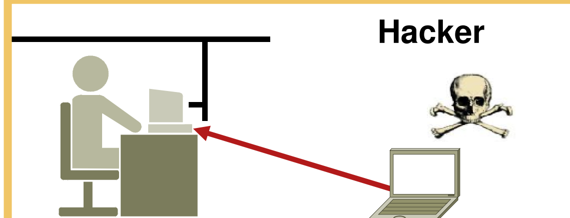
Adaptive Wireless IPS

The Wireless Threat Landscape

Attacks Across Multiple Vectors

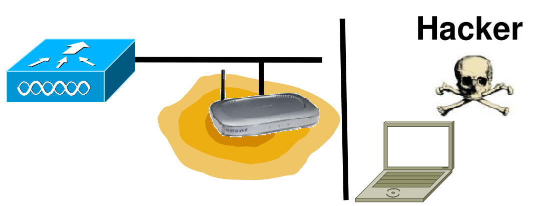
On-Wire Attacks

Ad Hoc Wireless Bridge



Client-to-Client Backdoor Access

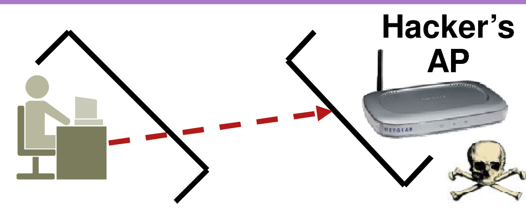
Rogue Access Points



Backdoor Network Access

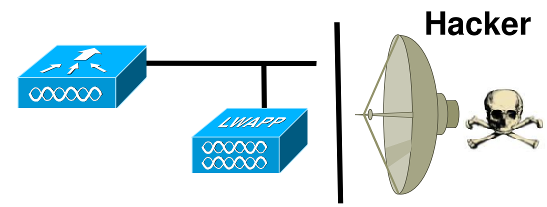
Over-the-Air Attacks

MiTM/Honeypot AP



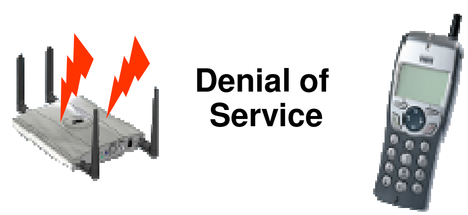
Connection to Malicious AP

Reconnaissance



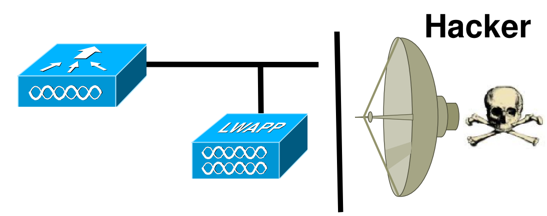
Seeking Network Vulnerabilities

Denial of Service



Service Disruption

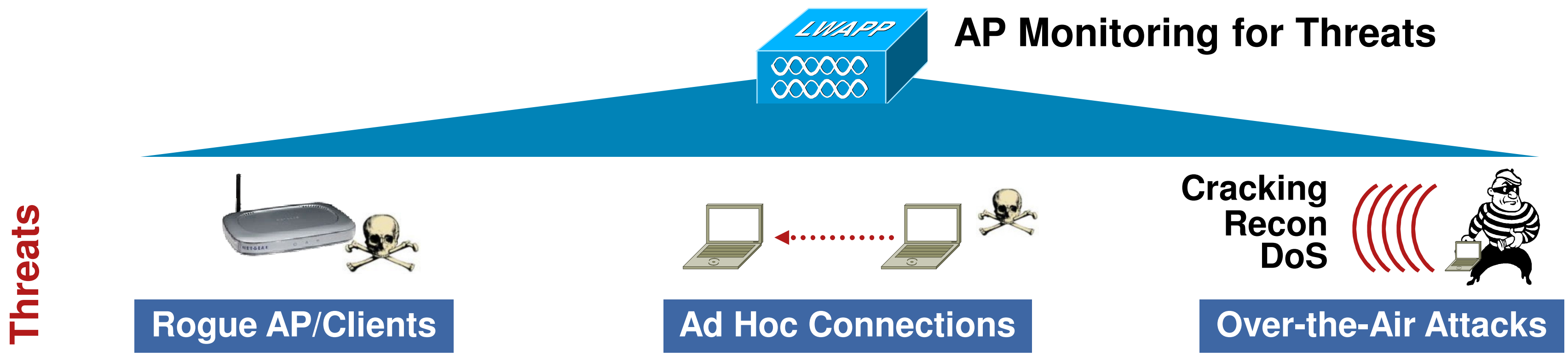
Cracking Tools



Sniffing and Eavesdropping

Wireless Intrusion Prevention

Purpose and Components



Threat Management Workflow

Detect » Classify » Notify / Log » Mitigate » Report / Archive

What Is the Threat?

→ How Severe Is It?

→ Alert Staff, Raise System Alarm, or Just Log?

→ What Action Must Be Taken?

→ End-to-End Record of Event and Actions

What's New in the CUWN Wireless IPS Solution?

New Feature Summary

What Adaptive wIPS adds above the WLC-based WIDS solution…

Expanded Detection

- 6x increase in attack detection capabilities – 17 to 45 signatures
- Detection for "unknown" or "Day Zero" attacks

Ease of Use

- Default configuration templates
- Plain-English attack explanations & step-by-step mitigation

Analysis/Reporting

- Event forensics
- On-board security event archive & reporting
- Attack aggregation

On-Going Protection

- Continually updated wireless threat detection for new attacks
- Dedicated threat research and detection development team

Over-the-Air Attack Techniques and Tools

Examples of Attacks Detected – 100-200 Attacks *(depends how you count them)*

Network Profiling and Reconnaissance

- Honeypot AP
- Netstumbler
- Kismet
- Wellenreiter
- Excessive device error
- Excessive multicast/broadcast

Authentication and Encryption Cracking

- Dictionary attacks
- AirSnarf
- Hotspotter
- WEPCrack
- ASLEAP
- EAP-based attacks
- CoWPAtty
- Chop-Chop
- Airckrack
- Airsnort
- PSPF violation
- WEP Attack
- Illegal frame types
- Excessive association retries
- Excessive auth retries
- LEAPCracker

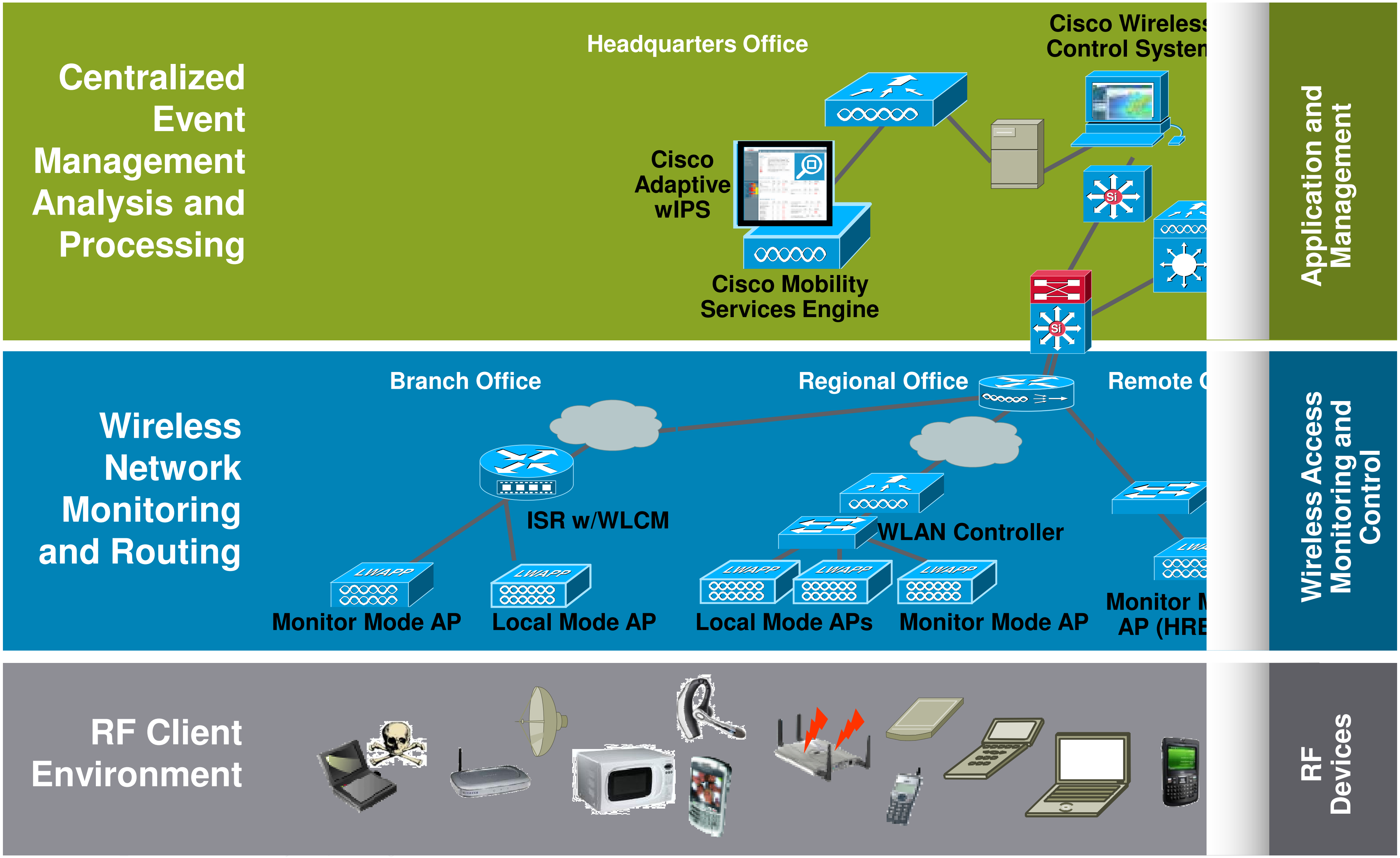
Man-in-the-Middle

- MAC/IP Spoofing
- Fake AP
- Evil Twin AP
- ARP Request Replay Attack
- Fake DHCP server
- Pre-standard APs (a,b,g,n)

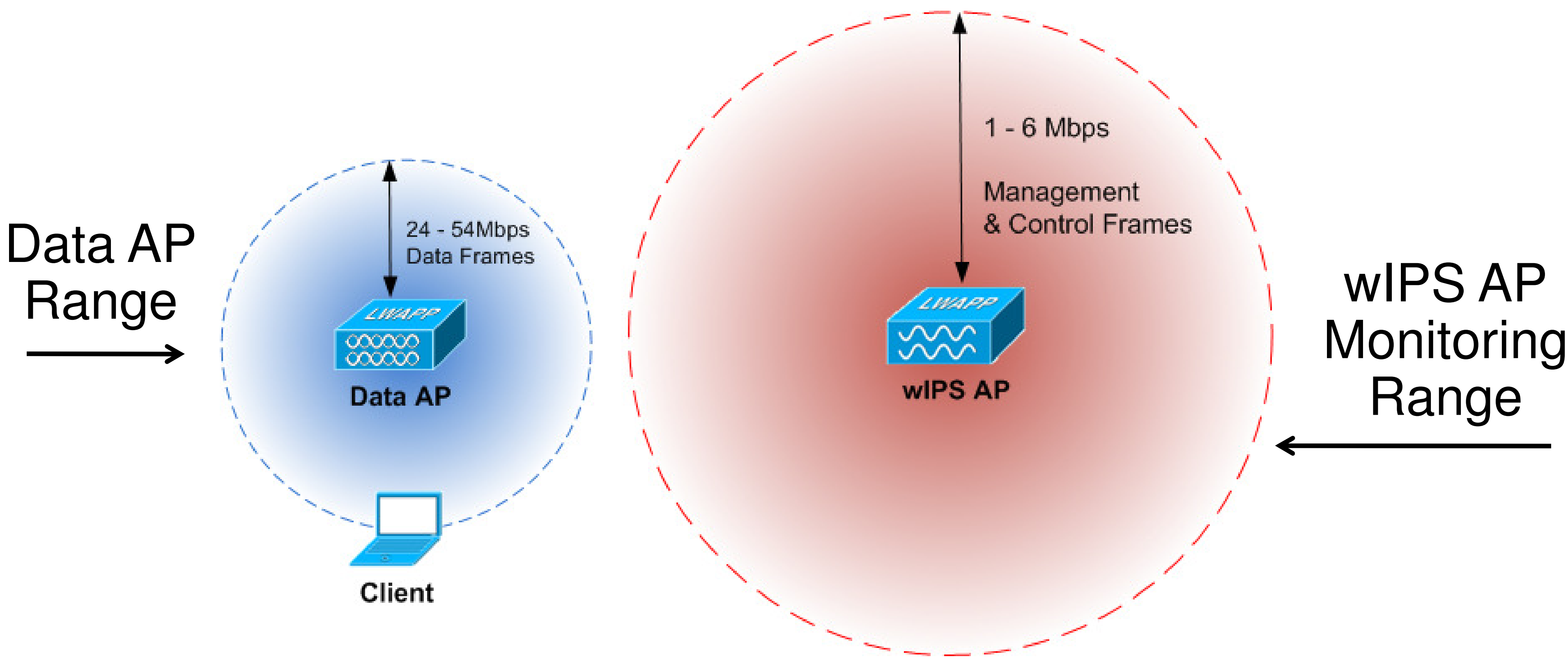
Denial of Service

- Malformed 802.11 frames
- FATA-Jack, AirJack
- Fragmentation attacks
- Excessive authentication
- De-auth attacks
- Association attacks
- CTS attacks
- RTS attacks
- Excessive device bandwidth
- EAPOL attacks
- Probe-response
- Resource management
- RF Jamming
- Michael
- Queensland
- Virtual carrier
- Big NAV
- Power-save attacks
- Microwave interference
- Bluetooth interference
- Radar interference
- Other non-802.11 interference
- Device error-rate exceeded
- Interfering APs
- Co-channel interference
- VoWLAN-based attacks
- Excessive roaming

Adaptive Wireless IPS Solution Overview

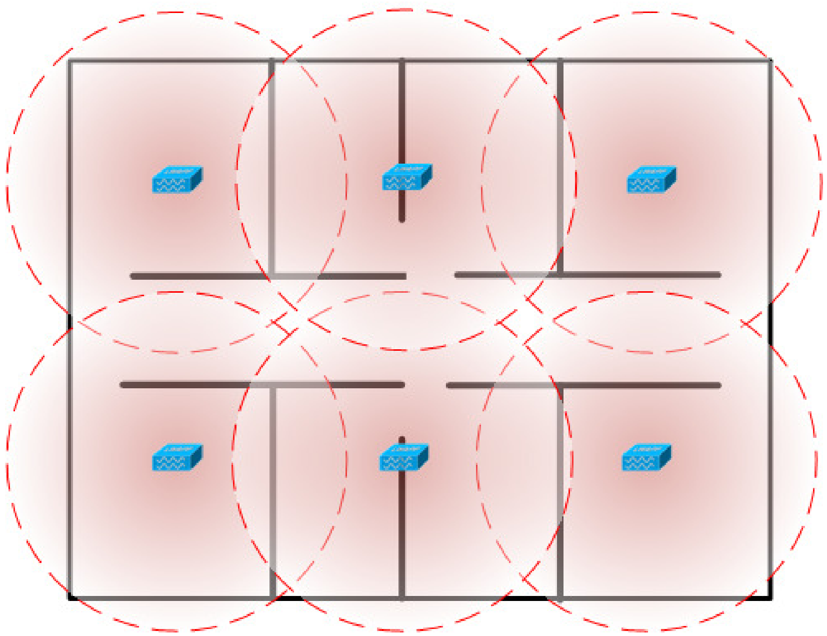


wIPS AP Monitoring Range



- Data APs are deployed for communication with clients
- wIPS APs deployed to capture management and control frames

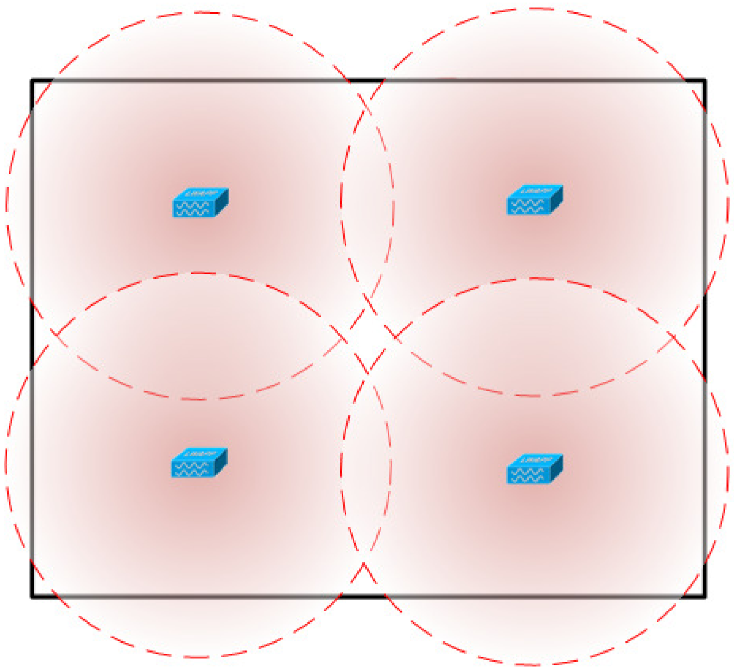
Walled Indoor - Recommendations



- Environments such as healthcare, finance, enterprise and education.
- Deploy 1 AP every XX,000 sqft

Walled Office Indoor Environment			
Confidence Level	Deployment Density	2.4GHz Detection	5GHz Detection
Gold	15,000 sqft	Exhaustive	Comprehensive
Silver	20,000 sqft	Comprehensive	Adequate
Bronze	25,000 sqft	Adequate	Sparse

Open Indoor - Recommendations



- Environments such as warehouses and manufacturing.
- Deploy 1 AP every XX,000 sq ft.

Open Indoor Environment			
Confidence Level	Deployment Density	2.4GHz Detection	5GHz Detection
Gold	30,000 sqft	Exhaustive	Comprehensive
Silver	40,000 sqft	Comprehensive	Adequate
Bronze	50,000 sqft	Adequate	Sparse