

802.11 Secrets Revealed – Part 2 Bit Transmission and Channel Capacity

June 17, 2010

Joe Bardwell

President / Chief Scientist - Connect802 Corporation
www.Connect802.com - joe@Connect802.com

SHARKFEST '10

Stanford University
June 14-17, 2010




SHARKFEST '10 | Stanford University | June 14-17, 2010

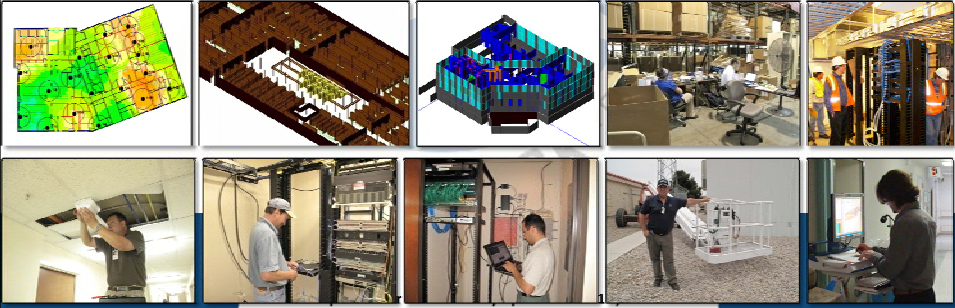


About Connect802 Corporation

- Founded in 1994 with headquarters in the San Francisco Bay area and East Coast engineering out of Knoxville, Tennessee
- Providing nationwide Wi-Fi, WiMAX, cellular and other wireless solutions
- Applying 3-dimensional RF CAD modeling and simulation to the design process
- Equipment sales, installation and support



www.Connect802.com



Your Wireshark Support Resource...

- Connect802 is your authorized AirPcap reseller
- Specialty Dual-Band (2.4 + 5 GHz) antennas for your AirPcap dual-band adapter
- 10/100 and GigE In-Line Port-Mirror Capture Switches with PoE Passthrough

Check out the Connect802 Wireshark enhancement products at:
www.Connect802.com/wireshark











SHARKFEST '10 | Stanford University | June 14-17, 2010




802.11 Header Information

The "Supported Rate" provides a basis for understanding a significant amount of information regarding the 802.11 connection

- ▣ Tagged parameters (58 bytes)
 - ▣ SSID parameter set: "CONNECT802 RF SURVEY"
 - ▣ Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B)
 - Tag Number: 1 (Supported Rates)
 - Tag length: 4
 - Tag Interpretation: Supported rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) [Mbit/sec]
 - ▣ DS Parameter set: Current Channel: 8
 - ▣ ERP Information: no Non-ERP STAs, use protection, short or long preambles
 - ▣ Extended Supported Rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
 - Tag Number: 50 (Extended Supported Rates)
 - Tag length: 8
 - Tag Interpretation: Supported rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0 [Mbit/sec]

Rate	Rate	Rate
1.0(M) @ 1 MHz	2.0(M) @ 2 MHz	5.5(M) @ 5.5 MHz
11.0(M) @ 11 MHz	6.0(M) @ 6 MHz	9.0(M) @ 9 MHz
12.0(M) @ 12 MHz	18.0(M) @ 18 MHz	24.0(M) @ 24 MHz
36.0(M) @ 36 MHz	48.0(M) @ 48 MHz	54.0(M) @ 54 MHz

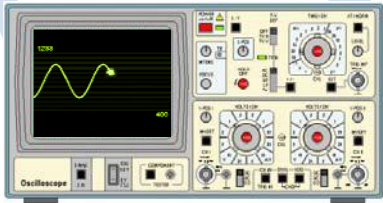
Rate	Rate	Rate
1.0(M) @ 1 MHz	2.0(M) @ 2 MHz	5.5(M) @ 5.5 MHz
11.0(M) @ 11 MHz	6.0(M) @ 6 MHz	9.0(M) @ 9 MHz
12.0(M) @ 12 MHz	18.0(M) @ 18 MHz	24.0(M) @ 24 MHz
36.0(M) @ 36 MHz	48.0(M) @ 48 MHz	54.0(M) @ 54 MHz








SHARKFEST '10 | Stanford University | June 14-17, 2010

Representing Bits with Electromagnetic Signals

- A sine wave carrier signal is generated
- The phase (and possibly the amplitude) of the signal is changed in a pattern that represents bits
- The more complex the pattern, the more bits per second
- The more complex the pattern, the greater the chance that noise or interference will disrupt it



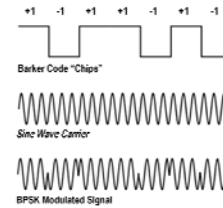
SHARKFEST '10 | Stanford University | June 14-17, 2010

Representing Bits With Electromagnetic Signals

1 Mbps Binary Phase Shift Keying (BPSK)

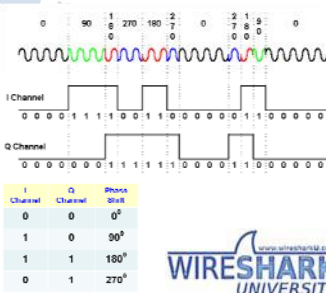
- The phase of a sine wave carrier is shifted by 180 degrees to represent a binary 0 or left unchanged to represent a binary 1
- Barker bit encoding (autocorrelation = 1) is used as a spreading code

Binary 1 = +1 +1 +1 -1 -1 -1 +1 -1 -1 +1 -1
 Binary 0 = -1 -1 -1 +1 +1 +1 -1 +1 +1 -1 +1



2 Mbps Quadrature Phase Shift Keying

- A sine ("In phase") and cosine ("Quadrature wave are transmitted simultaneously and are separated mathematically by the receiver
- Barker bit encoding operates separately on the I and Q components



SHARKFEST '10 | Stanford University | June 14-17, 2010

Improving On Barker Bit Encoding

- Complimentary Code Keying (CCK) with QPSK
 - A pair of 8-bit code sequences have a definable mathematical relationship to each other related to the number of occurrences of +1 and -1 symbols
 - 64 separate eight chip codes represent data bit sequences 000000 through 111111 (i.e. a 6 bit code)

5.5 Mbps

- 802.11b 5.5 Mbps encodes 4 bits per carrier
 - 11 Mega-chips per second, 8 chips per symbol, 4 bits per symbol
 - $11/8 = 1.475 * 4 = 5.5$

11 Mbps

- 802.11b 11 Mbps encodes 8 bits per carrier

$$c = \left[\begin{matrix} j\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 & j\epsilon_1 + \epsilon_3 + \epsilon_4 & j\epsilon_1 + \epsilon_2 + \epsilon_4 & -\epsilon_1 + \epsilon_2 + \epsilon_4 & j\epsilon_1 + \epsilon_2 & j\epsilon_1 + \epsilon_3 & -\epsilon_1 + \epsilon_2 & j\epsilon_1 + \epsilon_2 + \epsilon_3 \end{matrix} \right]$$

$$c = \left[\cos 2\pi - j \sin 2\pi, \cos \pi - j \sin \pi, \cos \frac{5\pi}{2} - j \sin \frac{5\pi}{2}, \cos \frac{3\pi}{2} - j \sin \frac{3\pi}{2}, \cos \frac{3\pi}{2} - j \sin \frac{3\pi}{2}, \cos \frac{5\pi}{2} - j \sin \frac{5\pi}{2}, \cos 2\pi - j \sin 2\pi, \cos \pi - j \sin \pi \right]$$

Encoding and Decoding CCK chip streams involves algorithms that evaluate and compare the phase of the QPSK I and Q channels

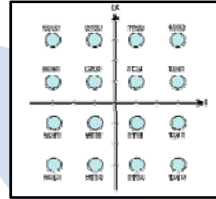
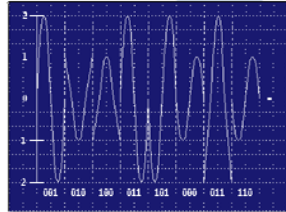
DIBIT	Phase Shift
00	0°
01	90°
10	180°
11	270°



SHARKFEST '10 | Stanford University | June 14-17, 2010

Quadrature Amplitude Modulation (QAM)

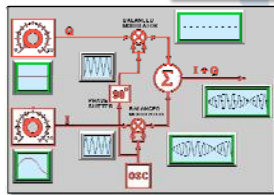
- Phase Shift Keying combined with Amplitude Modulation



16-QAM

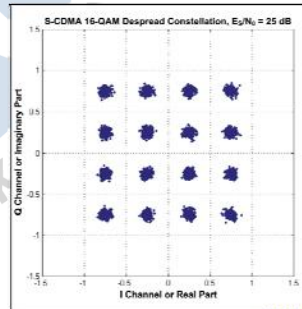


64-QAM



$$s(t) = \sum_{n=-\infty}^{\infty} [v_i[n] \cdot h_i(t - nT_s) \cos(2\pi f_c t) - v_q[n] \cdot h_q(t - nT_s) \sin(2\pi f_c t)]$$

A QAM transmission can be expressed with this formula

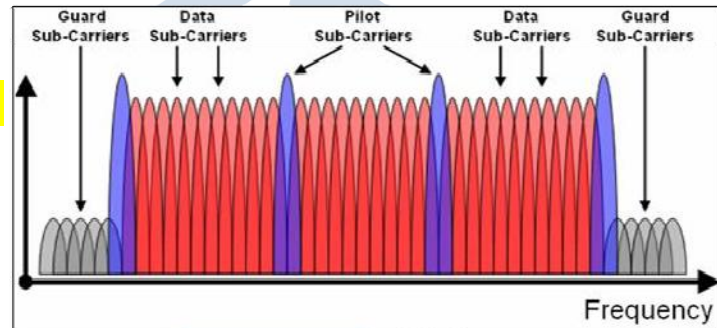


SHARKFEST '10 | Stanford University | June 14-17, 2010

Orthogonal Frequency Division Multiplexing (OFDM)

- 802.11a/g uses 48 sub-carriers
- 802.11n uses 52 sub-carriers

802.11a/g 6 – 54 Mbps
802.11n 6 – 58.5 Mbps



$$\sum_{k=0}^{N-1} |X_k| \cos(2\pi[f_c + k/T]t + \arg[X_k])$$

Algorithmic representation of the transmitted OFDM signal



SHARKFEST '10 | Stanford University | June 14-17, 2010



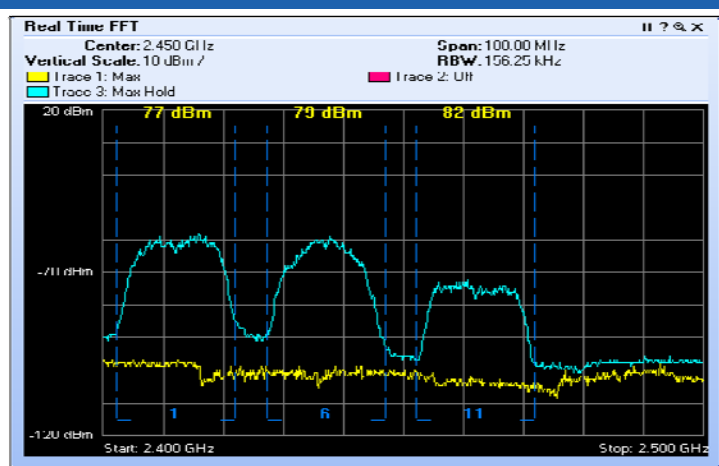
802.11n Modulation Coding Schemes

Bits 0-6 in HT MCS (MCS Index)	Number of spatial streams	Modulation	Coding rate	N _{SS}		N _{SD}		N _{CSFS}		GI = 800ns				GI = 400ns			
				20	40	20	40	20MHz	40MHz	Rate in 20MHz	Rate in 40MHz	Rate in 20MHz	Rate in 40MHz				
0	1	BPSK	1/2	1	1	52	106	52	106	20.5	41.0	10.25	20.5				
1	1	QPSK	1/2	1	1	52	106	104	216	41.0	82.0	20.5	41.0				
2	1	QPSK	3/4	1	1	52	106	104	216	61.5	123.0	30.75	61.5				
3	1	16-QAM	1/2	1	1	52	106	104	216	20.5	41.0	10.25	20.5				
4	1	16-QAM	3/4	1	1	52	106	104	216	30.75	61.5	15.375	30.75				
5	1	64-QAM	1/2	1	1	52	106	104	216	10.25	20.5	2.5625	5.125				
6	1	64-QAM	3/4	1	1	52	106	104	216	15.375	30.75	3.84375	7.6875				
7	1	64-QAM	5/6	1	1	52	106	104	216	17.0	34.0	4.25	8.5				
8	2	BPSK	1/2	1	1	52	106	104	216	41.0	82.0	10.25	20.5				
9	2	QPSK	1/2	1	1	52	106	104	216	20.5	41.0	5.125	10.25				
10	2	QPSK	3/4	1	1	52	106	104	216	30.75	61.5	7.6875	15.375				
11	2	16-QAM	1/2	1	1	52	106	104	216	10.25	20.5	2.5625	5.125				
12	2	16-QAM	3/4	1	1	52	106	104	216	15.375	30.75	3.84375	7.6875				
13	2	64-QAM	1/2	1	1	52	106	104	216	5.125	10.25	1.28125	2.5625				
14	2	64-QAM	3/4	1	1	52	106	104	216	7.6875	15.375	1.921875	3.84375				
15	2	64-QAM	5/6	1	1	52	106	104	216	8.5	17.0	2.125	4.25				
16	2	BPSK	1/2	2	2	104	212	208	432	41.0	82.0	10.25	20.5				
17	2	QPSK	1/2	2	2	104	212	208	432	20.5	41.0	5.125	10.25				
18	2	QPSK	3/4	2	2	104	212	208	432	30.75	61.5	7.6875	15.375				
19	2	16-QAM	1/2	2	2	104	212	208	432	10.25	20.5	2.5625	5.125				
20	2	16-QAM	3/4	2	2	104	212	208	432	15.375	30.75	3.84375	7.6875				
21	2	64-QAM	1/2	2	2	104	212	208	432	5.125	10.25	1.28125	2.5625				
22	2	64-QAM	3/4	2	2	104	212	208	432	7.6875	15.375	1.921875	3.84375				
23	2	64-QAM	5/6	2	2	104	212	208	432	8.5	17.0	2.125	4.25				
24	4	BPSK	1/2	2	2	52	106	936	1944	20.5	41.0	10.25	20.5				
25	4	QPSK	1/2	2	2	52	106	936	1944	10.25	20.5	5.125	10.25				
26	4	QPSK	3/4	2	2	52	106	936	1944	15.375	30.75	7.6875	15.375				
27	4	16-QAM	1/2	2	2	52	106	832	1728	10.25	20.5	2.5625	5.125				
28	4	16-QAM	3/4	2	2	52	106	832	1728	15.375	30.75	3.84375	7.6875				
29	4	64-QAM	1/2	2	2	52	106	1248	2592	5.125	10.25	1.28125	2.5625				
30	4	64-QAM	3/4	2	2	52	106	1248	2592	7.6875	15.375	1.921875	3.84375				
31	4	64-QAM	5/6	2	2	52	106	1248	2592	8.5	17.0	2.125	4.25				

MCS 32 – 77 Provide Legacy 48 Sub-Carrier OFDM And Are Unused

SHARKFEST '10 | Stanford University | June 14–17, 2010

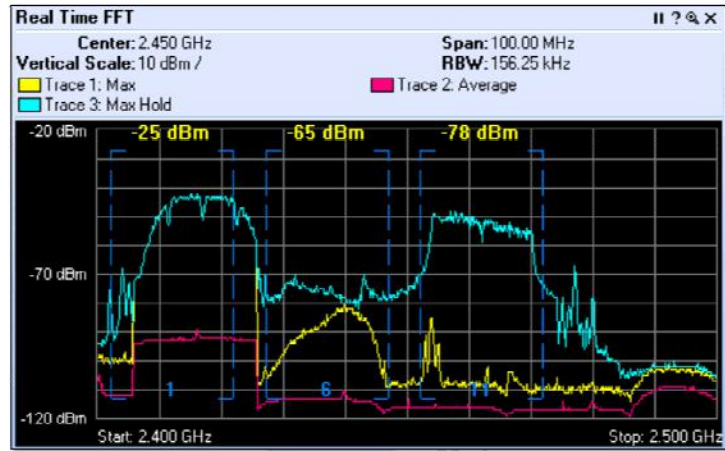
802.11g BPSK and OFDM



802.11 Beacon packets are always transmitted using BPSK modulation (the lowest common denominator)

SHARKFEST '10 | Stanford University | June 14–17, 2010

A Cordless Phone In the Background



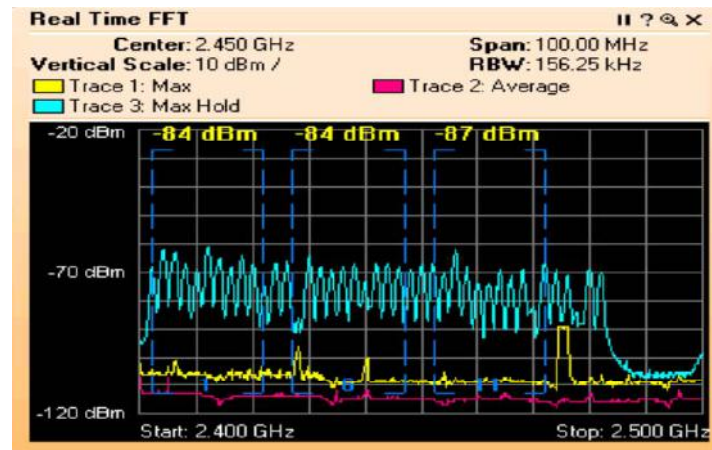
802.11b/g
2.4 GHz Spectrum
(North American Channels 1 through 11)



SHARKFEST '10 | Stanford University | June 14-17, 2010



The Cordless Phone Exposed



- RF spectrum analysis identifies energy signatures in the environment
- Packet level protocol analysis depends on the recovery of bits from the received signal



SHARKFEST '10 | Stanford University | June 14-17, 2010



Why Does 802.11n Have Greater Capacity?

It seems like all you hear about is
"MIMO" (Multiple-Input / Multiple-
Output)



| Stanford University | June 14–17, 2010



Why Does 802.11n Have Greater Capacity?

- Modified OFDM
 - Subcarriers increased from 48 to 52
 - This increases connection rate from 54 Mbps to 58.5 Mbps
- Forward Error Correction (FEC)
 - Sender adds redundant data to allow receiver to detect and correct errors
 - 802.11a/g 3/4 coding rate is increased to 5/6
 - This increases connection rate from 58.5 Mbps to 65 Mbps
- Shorter Guard Interval (GI)
 - OFDM inter-symbol guard interval reduced from 800ns to 400ns
 - This increases connection rate from 65 Mbps to 72.2 Mbps



SHARKFEST '10 | Stanford University | June 14–17, 2010



Why Does 802.11n Have Greater Capacity?

- Channel Bonding
 - Channel bandwidth is increased from 20 MHz to 40 MHz
 - This increases connection rate from 72.2 Mbps to 150 Mbps
 - Better than twice because there is no guard band between adjacent channel space
- Spatial Multiplexing
 - Support for up to four spatial streams (MIMO)
 - This increases bandwidth up to four times
 - Approximately 150 Mbps, 300 Mbps, 450 Mbps, 600 Mbps



SHARKFEST '10 | Stanford University



Additional Performance Enhancements

- Lower MAC Overhead
 - 802.11a/g 54 Mbps yields 26 Mbps throughput (50%)
 - 802.11n 65 Mbps yields 50 Mbps (75%)
- Fast MCS Feedback Rate Selection
 - 802.11a/g rate adaptation is based on transmit errors demanding a conservative approach (“when in doubt, drop the rate”)
 - 802.11n adds explicit per-packet feedback recommending the transmission speed for the next packet
- Low Density Parity Check (LDPC) Coding
 - Enhanced FEC possible because of increased hardware capabilities and faster CPU processors
- Frame Aggregation
 - Transmit multiple data blocks in a single frame
 - Acknowledge multiple data blocks with a single ACK

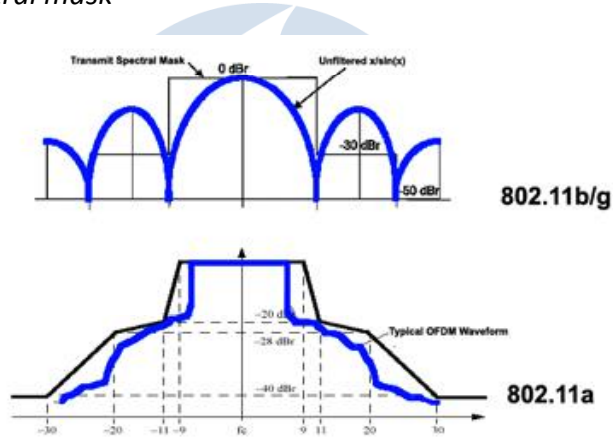


SHARKFEST '10 | Stanford University | June 14–17, 2010



Understanding “Channel Bonding”

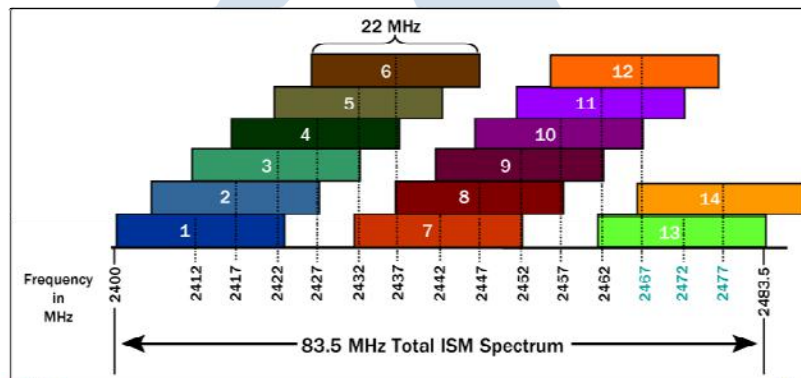
- 802.11 channels are defined by their center frequency and by a *spectral mask*



SHARKFEST '10 | Stanford University | June 14–17, 2010

2.4 GHz ISM Channels

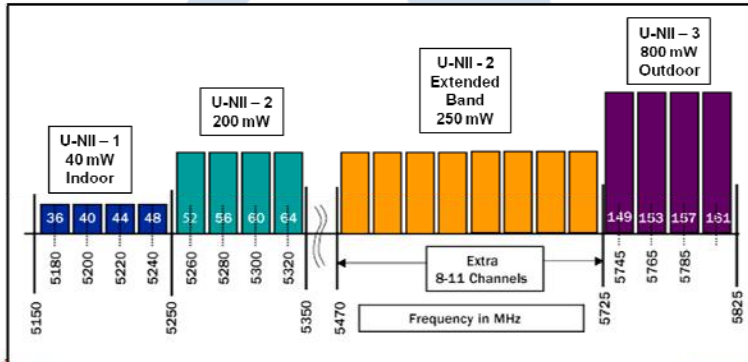
- 83.5 MHz wide 2.4 GHz ISM band
 - 14 channels, each 22 MHz wide, spaced 5 MHz apart
 - Channels 1-11 used in North America
 - 3 non-overlapping channels (1, 6, 11)



SHARKFEST '10 | Stanford University | June 14–17, 2010

5 GHz U-NII Band Channels

- 300 MHz wide 5.8 GHz U-NII band
 - “Unlicensed National Information Infrastructure”
 - 12 channels, each 20 MHz wide, no appreciable overlap
 - Some manufacturer’s don’t use the U-NII-2 band
 - U-NII-2 Extended Band is not used for 802.11



SHARKFEST '10 | Stanford University | June 14-17, 2010

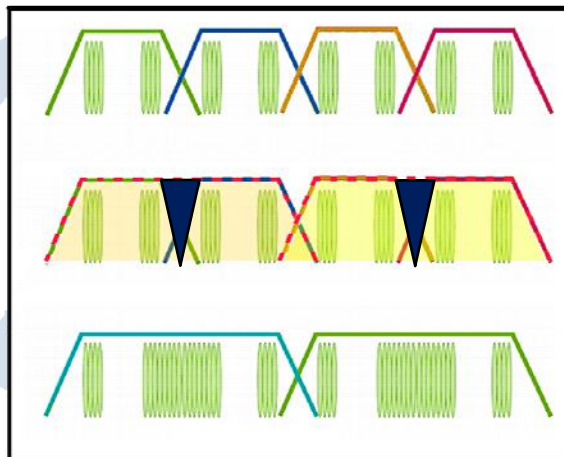


802.11a Versus 802.11n Channel Bonding

Standard 802.11 5.8 GHz
20 MHz Channels

“Bonded”
20 MHz Channels
In 802.11a

40 MHz Channels
In 802.11n

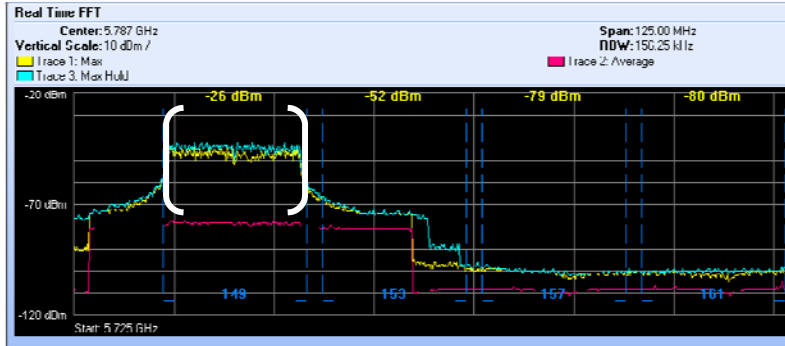


150 Mbps

SHARKFEST '10 | Stanford University | June 14-17, 2010



Channel 149 – 20 MHz Channel

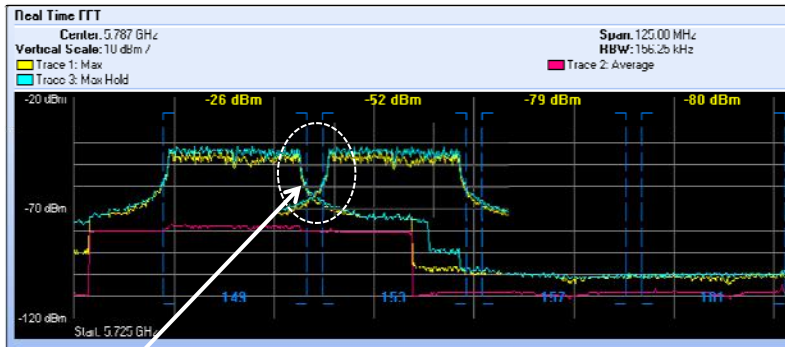


802.11a / 802.11n
5 GHz Spectrum
20 MHz Channels (149)



SHARKFEST '10 | Stanford University | June 14-17, 2010

Two Adjacent 20 MHz Channels (149 and 153)



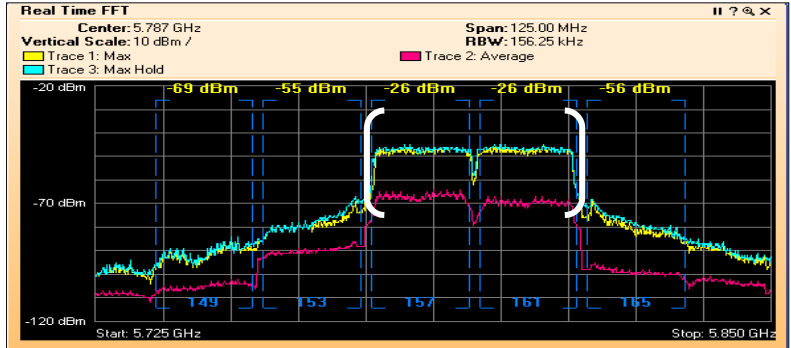
Adjacent 20 MHz channels have a guard band between them

802.11n
5 GHz Spectrum
20 MHz Channels (149 and 153)



SHARKFEST '10 | Stanford University | June 14-17, 2010

A 40 MHz Channel (157+)

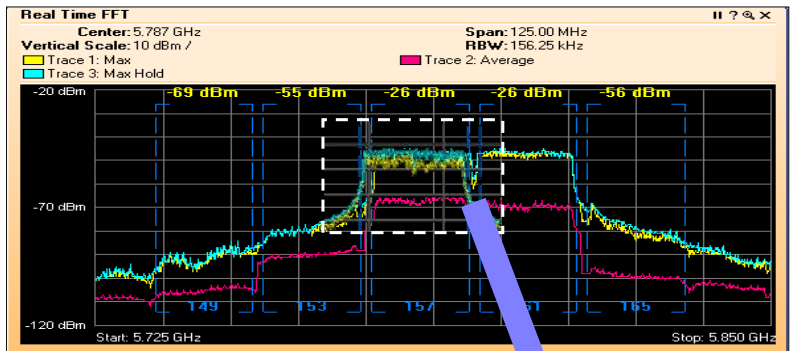


The OFDM sub-carriers in a 40 MHz channel span the entire 40 MHz width, occupying what would have been the spacing between adjacent 20 MHz channels

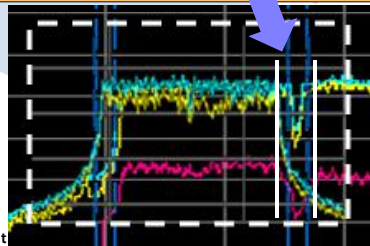


SHARKFEST '10 | Stanford University | June 14-17, 2010

Comparing 20 MHz to 40 MHz Channels



This picture shows the 20 MHz OFDM signature overlaid on the 40 MHz signature

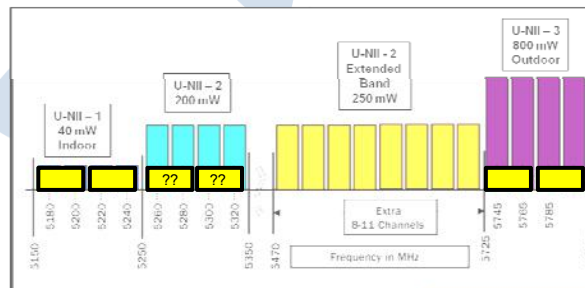
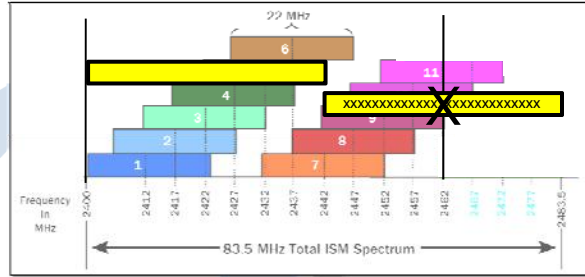


SHARKFEST '10 | St

Important Considerations for 40 MHz Channels

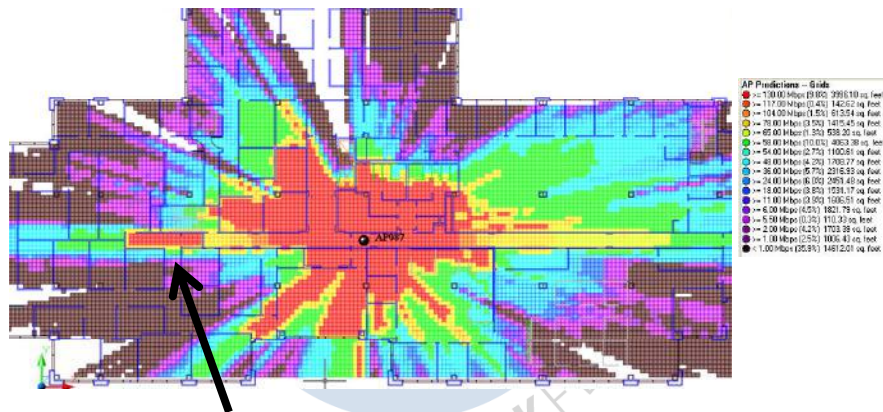
1 Channel
in 2.4 GHz

You need
U-NII-2
support
In 5.8 GHz



SHARKFEST '10 | Stanford University | June 14-17, 2010

802.11n Predictive CAD Coverage Model



Unlike 802.11abg, performance does not consistently decrease with distance from an 802.11n access point

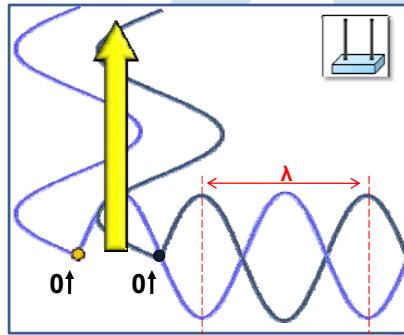


SHARKFEST '10 | Stanford University | June 14-17, 2010



Beamforming 101

Beamforming, also called Beamsteering, allows electronic aiming of the strongest signal from (and the best reception angle to) an antenna array



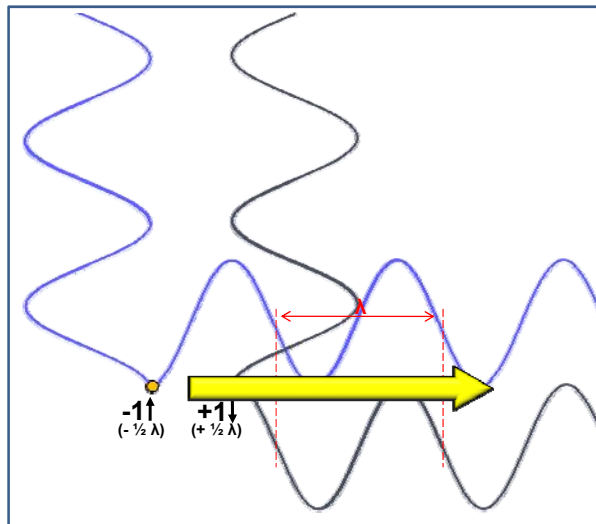
Two antennas, transmitting the same signal, with both antennas transmitting in-phase

Note that the signal starts at 0-degrees and is rising



SHARKFEST '10 | Stanford University | June 14-17, 2010

Beamforming 101



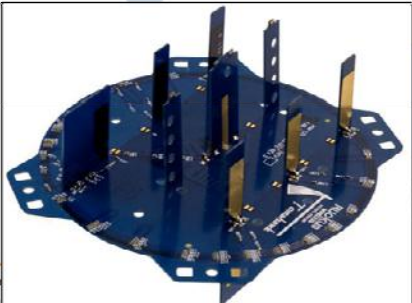
Now the two signals are 180-degrees out of phase but the $\frac{1}{2}$ wavelength separation between the antennas makes the signal in-phase in one direction



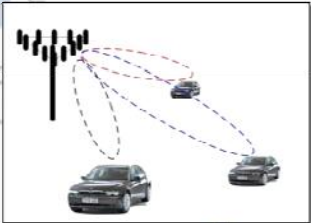
SHARKFEST '10 | Stanford University | June 14-17, 2010

A Beamforming / Beamsteering Antenna

- Beamforming is a commercially available feature
 - Commonplace in cellular communications
 - Part of the final 802.11n standard (Not specified in Draft 2)
 - Used by some manufacturers in WiMAX and Wi-Fi radios
- You may realize as much as 9 dB of directional gain



CACE
TECHNOLOGIES



WIRESHARK
UNIVERSITY

SHARKFEST '10 | Stanford University | June 14-17, 2010

Design of a Commercial 802.11 Network

The application of predictive RF CAD modeling and simulation provides the optimal preliminary design before any on-site work is performed

Design should not start with someone walking the site plan where to put radios

Design begins with the site plan where to put radios

- Construction characteristics
- Wiring closet locations

A 3-Dimensional RF CAD

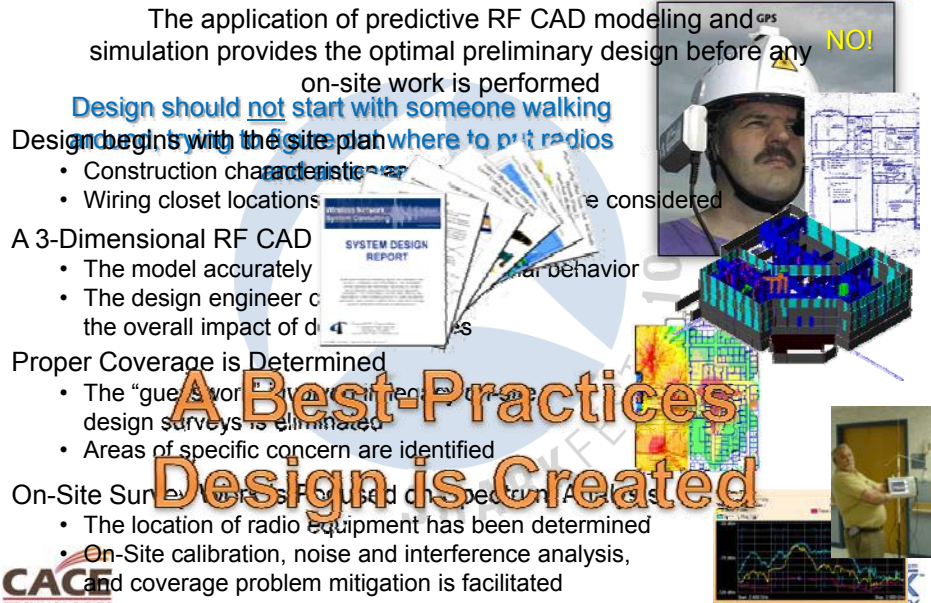
- The model accurately
- The design engineer can see the overall impact of design changes

Proper Coverage is Determined

- The "guess and check" method of design surveys is eliminated
- Areas of specific concern are identified

On-Site Surveys are used for spectrum analysis

- The location of radio equipment has been determined
- On-Site calibration, noise and interference analysis, and coverage problem mitigation is facilitated



A Best-Practices Design is Created

CACE
TECHNOLOGIES

SHARKFEST '10 | Stanford University | June 14-17, 2010

You provide the floor plans.
We create the system design.

Suite Spot Predictive Site Survey

Complete RF Design and Installer's Working Plans

RAWING FILES

ISOMETRIC MODELS

Predictive RF CAD Modeling and Simulation

SHARKFEST '10 | Stanford University | June

RF Characteristics Are Carefully Analyzed

FLOORPLAN INCONSISTENCIES

Collecting Connected Point Coverage

Final Point Coverage (Floor and Ceiling) - Note

Final Point Coverage (Light to Dark Blue)

BEST-PRACTICE DESIGN

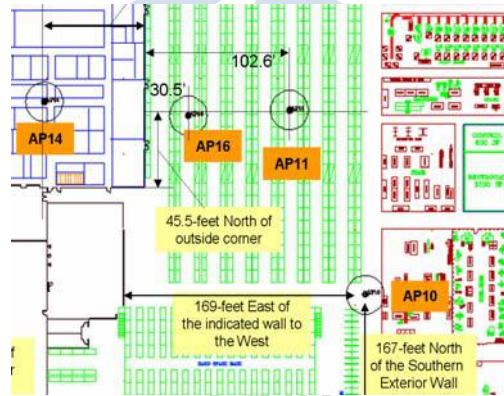
Design	Coverage greater than 45 dBm	Coverage greater than 40 dBm	Coverage greater than 35 dBm
Current Design with Floor at level 0	55.3%	54.2%	33.3%
Current Design with Floor at level 1	54.4%	53.3%	33.3%
Current Design with Floor at level 2	54.4%	53.3%	33.3%

Predictive RF CAD Modeling Allows More Detailed Analysis Than an On-Site Survey

SHARKFEST '10 | Stanford University | June

Your Accurate Installation Plans

- Installation of a commercial 802.11 network adheres to professional standards in the construction industry



SHARKFEST '10 | Stanford University | June 14-17, 2010

These are part of the 802.11 Secrets Revealed!

Thank You!

Joe Bardwell - Connect802 Corporation
joe@connect802.com
www.Connect802.com - (925) 552-0802

The collage includes a spectrum chart with labels for Guard Sub-Carriers, Data Sub-Carriers, and Pilot Sub-Carriers. It also features isometric models of network equipment racks and various technical diagrams. A young boy is shown looking thoughtful, resting his chin on his hand. The text 'Thank You!' is prominently displayed in the center.



SHARKFEST '10 | Stanford University | June 14-17, 2010