Wireshark Developer and User Conference

Wireshark and 802.11ac Wireless Evolution
Joe Bardwell – Connect802 Corporation

How do you "THINK" my first day of kindergarten went?!?
They didn't even have Wi-Fi..

SHARKFEST '12 | UC Berkeley | June 24–27, 2012

Wireshark Developer and User Conference

Wireshark and 802.11ac Wireless Evolution

June 24 and 25, 2012

Joe Bardwell
Chief Scientist | Connect802 Corporation

SHARKFEST '12
UC Berkeley
June 24-27, 2012

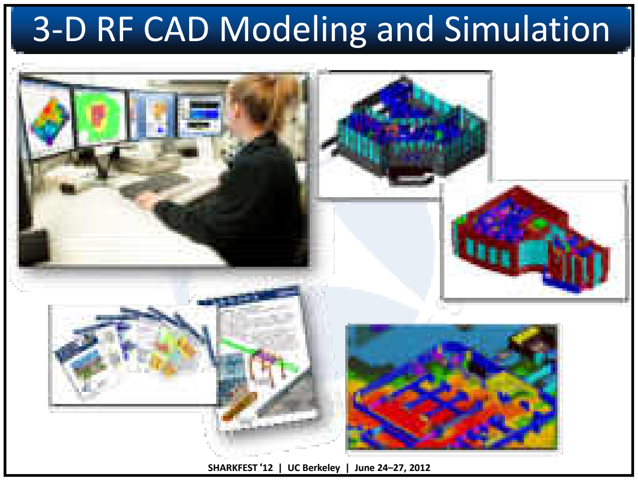
www.Connect802.com
@Connect802
follow us on twitter

SHARKFEST '12 | UC Berkeley | June 24–27, 2012

About Connect802 Corporation

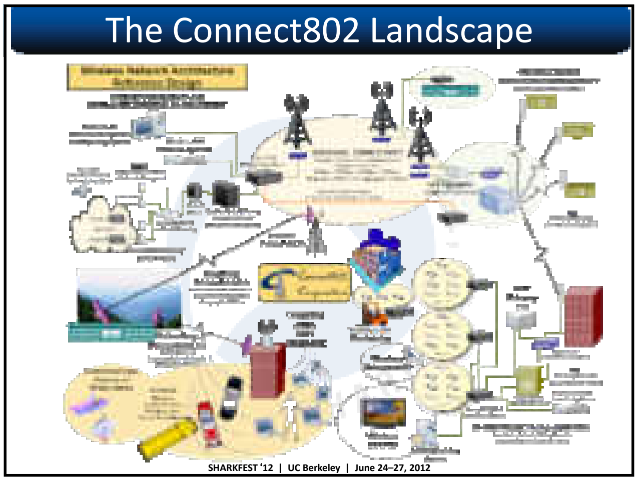
- Founded in 1994 with headquarters in the San Francisco Bay area and East Coast engineering out of Knoxville, Tennessee
- Providing nationwide Wi-Fi, WiMAX, cellular and other wireless solutions
- Applying 3-dimensional RF CAD modeling and simulation to the design process
- Equipment sales, installation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

www.Connect802.com



3-D RF CAD Modeling and Simulation

SHARKFEST '12 | UC Berkeley | June 24–27, 2012



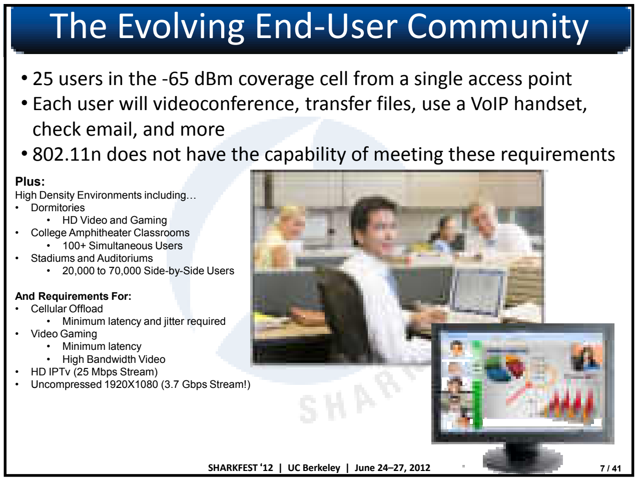
The Connect802 Landscape

SHARKFEST '12 | UC Berkeley | June 24–27, 2012

Here it comes: 802.11ac

"What?? ...I just got my arms around 11n... now there's another standard to figure out?"

- Early consumer products are shipping today
- Commerical-grade access points are expected in 2013
- Client-side 11ac may begin to appear in mid-to-late 2013 or early 2014
  - Apple may even have 11ac support in products by the end of this year!
- Infonetics Research expects the 11ac market to have a spike in growth in 2015



The Evolving End-User Community

- 25 users in the -65 dBm coverage cell from a single access point
- Each user will videoconference, transfer files, use a VoIP handset, check email, and more
- 802.11n does not have the capability of meeting these requirements

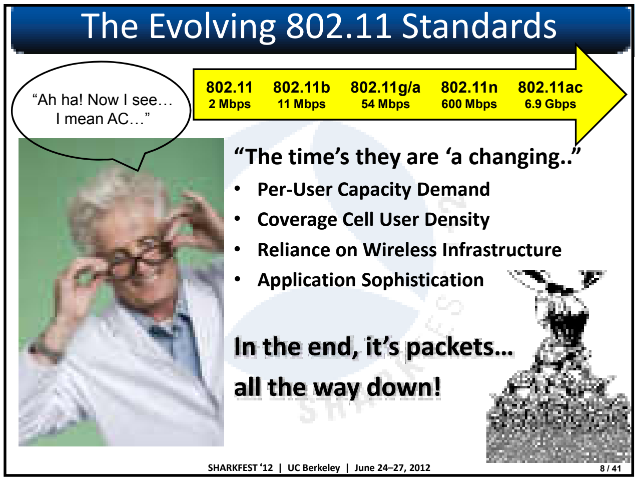
Plus:
High Density Environments including…

- Dormitories
  - HD Video and Gaming
- College Amphitheater Classrooms
  - 100+ Simultaneous Users
- Stadiums and Auditoriums
  - 20,000 to 70,000 Side-by-Side Users

And Requirements For:

- Cellular Offload
  - Minimum latency and jitter required
- Video Gaming
  - Minimum latency
  - High Bandwidth Video
- HD IPTv (25 Mbps Stream)
- Uncompressed 1920X1080 (3.7 Gbps Stream!)

SHARKFEST '12 | UC Berkeley | June 24–27, 2012 7 / 41



The Evolving 802.11 Standards

802.11	802.11b	802.11g/a	802.11n	802.11ac
2 Mbps	11 Mbps	54 Mbps	600 Mbps	6.9 Gbps

"The time's they are 'a changing.."

- **Per-User Capacity Demand**
- **Coverage Cell User Density**
- **Reliance on Wireless Infrastructure**
- **Application Sophistication**

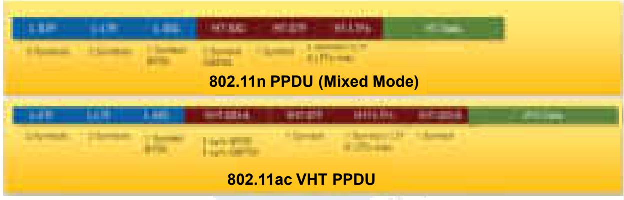
In the end, it's packets…

all the way down!

SHARKFEST '12 | UC Berkeley | June 24–27, 2012 8 / 41

The PLCP Protocol Data Unit (PPDU)

- Physical Layer Convergence Procedure
- Symbol duration: 4 microseconds (Optional 3.6 µs symbol with short guard interval)



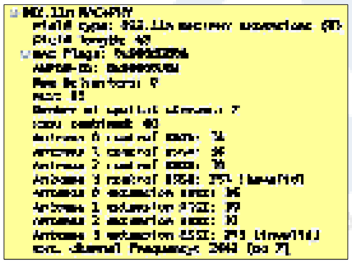
1 Symbol = 4µs

L: Indicates Legacy (802.11abgn) Field
VHT: Indicates 802.11ac Very High Throughput
VHT-SIG-A: Number of Streams, MCS, Beamforming Matrix
STF: Short Training Field
LTF: Long Training Field (Mapping Matrix)

HT: Indicates 802.11n High Throughput
SIG: Protection Mechanism Signal Field
VHT-SIG-B: Length of Data and MCS for MU Mode
VHT-STF: Improves AGC Estimations for MIMO

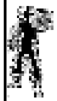
The Evolution of Wireshark

"Appear... Oh mystical Wireshark decodes..."

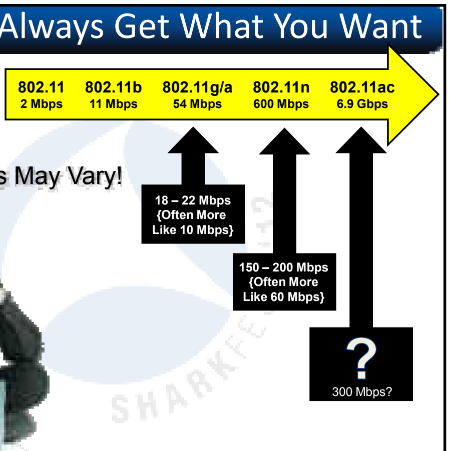


```
⊟ 802.11n MAC+PHY
    Field type: 802.11n MAC+PHY extension (3)
    Field length: 48
  ⊞ MAC Flags: 0x00000000
    A-MPDU-ID: 0x00000000
    Num Delimiters: 0
    MCS: 15
    Number of spatial streams: 2
    RSSI combined: 40
    Antenna 0 control RSSI: 36
    Antenna 1 control RSSI: 36
    Antenna 2 control RSSI: 36
    Antenna 3 control RSSI: 255 (invalid)
    Antenna 0 extension RSSI: 36
    Antenna 1 extension RSSI: 37
    Antenna 2 extension RSSI: 33
    Antenna 3 extension RSSI: 255 (invalid)
    Ext. Channel Frequency: 2442 [BG 7]
```

You Can't Always Get What You Want



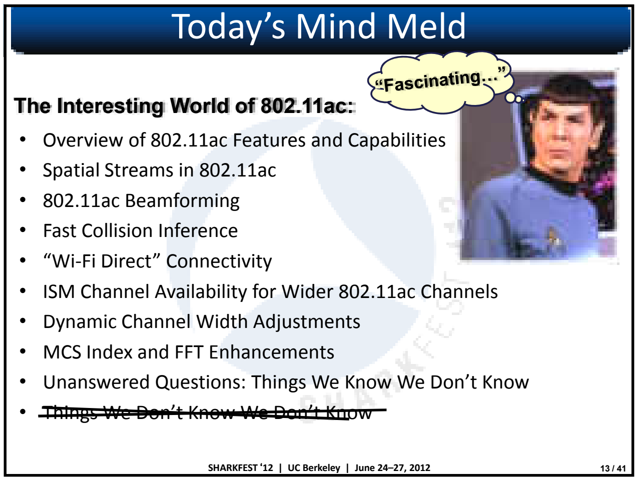
Big News:
Your Results May Vary!



802.11ac is NOT 802.11ad

- Don't confuse 802.11ac with 802.11ad
  - WiGig Alliance initiated the standard
    - Confirmed in May 2010 as the basis for the 802.11ad draft standard
  - Operates in the 60 GHz Band
  - 4 X 2.16 GHz wide channels delivering up to 7 Gbps
  - Single carrier radio (allows 2.4 and 5 GHz Wi-Fi plus 60 GHz 11ad)
  - Very limited range at 60 GHz (HDMI Cable Replacement)
  - Up to 32 spatial streams with refined beamforming
- Oh – and there's also 802.11ah coming down the pike…
  - Sub-1GHz frequencies
    - US 902-928 MHz ISM Band
    - Does not include TV white space (802.11af)
  - Ultra low-power Wi-Fi
  - Targeted for product-to-market in 2014

In case you wondered:
802.11ae is a standard for prioritization of management frames when exchanged between LAN and WAN



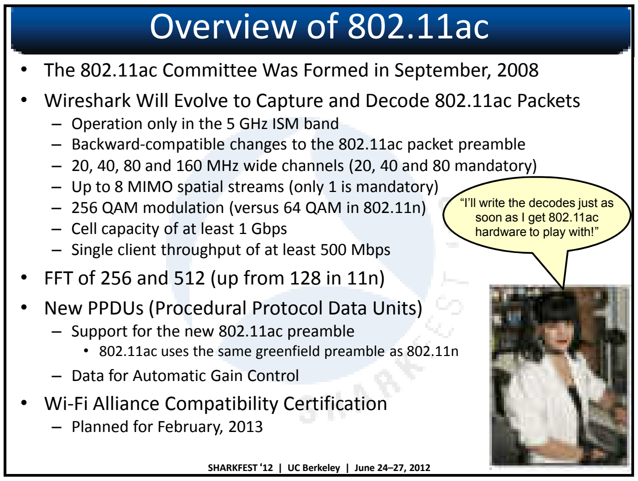
Today’s Mind Meld

“Fascinating…”

The Interesting World of 802.11ac:

- Overview of 802.11ac Features and Capabilities
- Spatial Streams in 802.11ac
- 802.11ac Beamforming
- Fast Collision Inference
- “Wi-Fi Direct” Connectivity
- ISM Channel Availability for Wider 802.11ac Channels
- Dynamic Channel Width Adjustments
- MCS Index and FFT Enhancements
- Unanswered Questions: Things We Know We Don’t Know
- ~~Things We Don’t Know We Don’t Know~~

SHARKFEST ‘12 | UC Berkeley | June 24–27, 2012 13 / 41

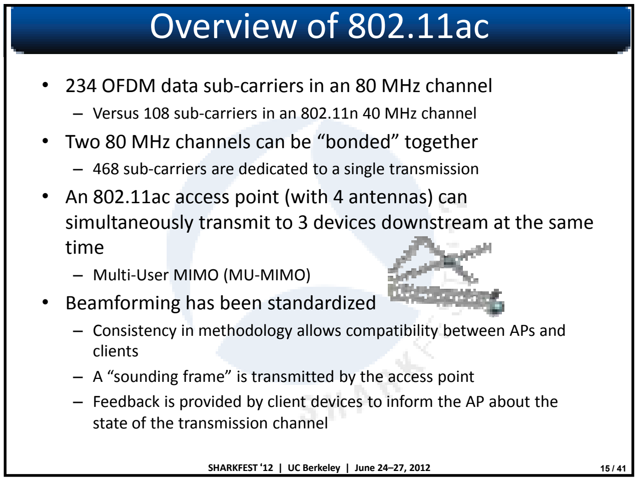


Overview of 802.11ac

- The 802.11ac Committee Was Formed in September, 2008
- Wireshark Will Evolve to Capture and Decode 802.11ac Packets
  - Operation only in the 5 GHz ISM band
  - Backward-compatible changes to the 802.11ac packet preamble
  - 20, 40, 80 and 160 MHz wide channels (20, 40 and 80 mandatory)
  - Up to 8 MIMO spatial streams (only 1 is mandatory)
  - 256 QAM modulation (versus 64 QAM in 802.11n)
  - Cell capacity of at least 1 Gbps
  - Single client throughput of at least 500 Mbps
- FFT of 256 and 512 (up from 128 in 11n)
- New PPDUs (Procedural Protocol Data Units)
  - Support for the new 802.11ac preamble
    - 802.11ac uses the same greenfield preamble as 802.11n
  - Data for Automatic Gain Control
- Wi-Fi Alliance Compatibility Certification
  - Planned for February, 2013

“I’ll write the decodes just as soon as I get 802.11ac hardware to play with!”

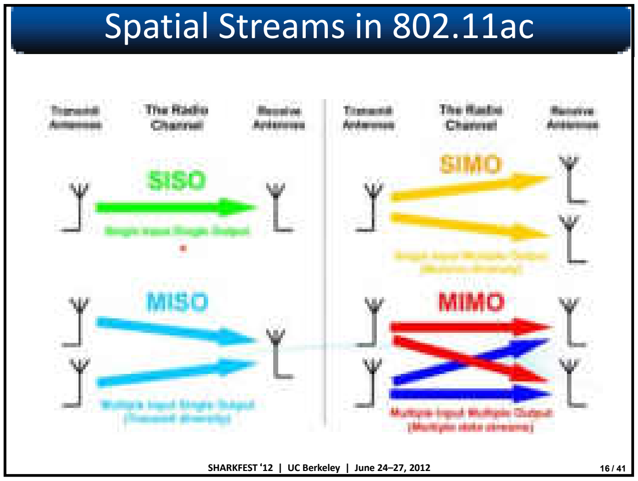
SHARKFEST ‘12 | UC Berkeley | June 24–27, 2012



Overview of 802.11ac

- 234 OFDM data sub-carriers in an 80 MHz channel
  - Versus 108 sub-carriers in an 802.11n 40 MHz channel
- Two 80 MHz channels can be “bonded” together
  - 468 sub-carriers are dedicated to a single transmission
- An 802.11ac access point (with 4 antennas) can simultaneously transmit to 3 devices downstream at the same time
  - Multi-User MIMO (MU-MIMO)
- Beamforming has been standardized
  - Consistency in methodology allows compatibility between APs and clients
  - A “sounding frame” is transmitted by the access point
  - Feedback is provided by client devices to inform the AP about the state of the transmission channel

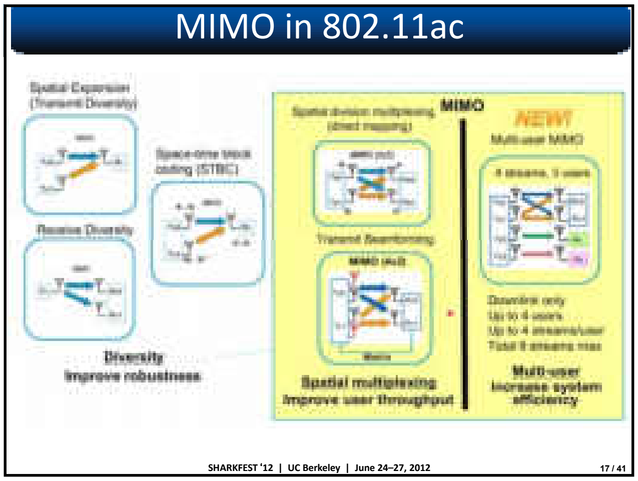
SHARKFEST ‘12 | UC Berkeley | June 24–27, 2012 15 / 41



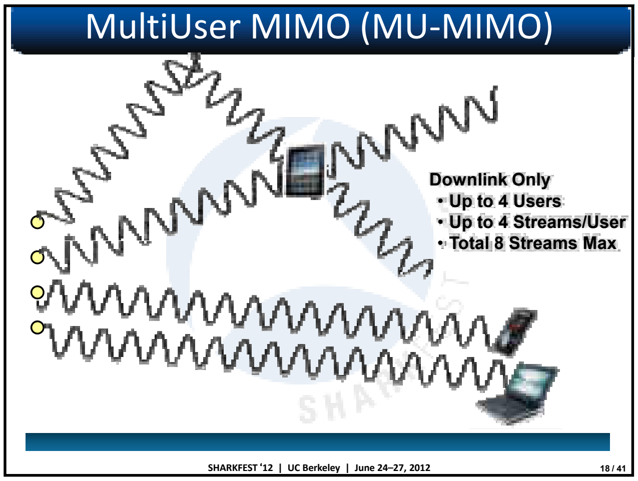
Spatial Streams in 802.11ac

Transmit Antennas
The Radio Channel
Receive Antennas
Transmit Antennas
The Radio Channel
Receive Antennas
SISO
Single Input Single Output
SIMO
Single Input Multiple Output (Receive diversity)
MISO
Multiple Input Single Output (Transmit diversity)
MIMO
Multiple Input Multiple Output (Multiple data streams)

SHARKFEST ‘12 | UC Berkeley | June 24–27, 2012 16 / 41

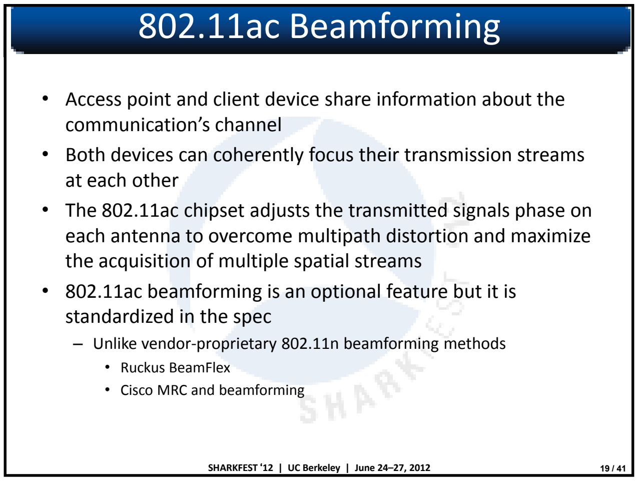


MIMO in 802.11ac



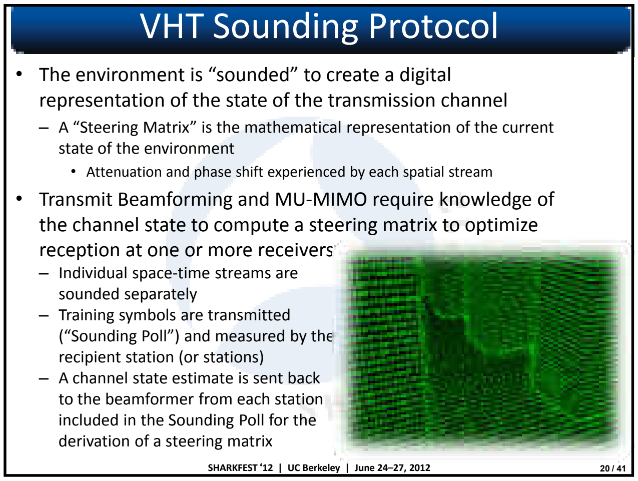
MultiUser MIMO (MU-MIMO)

Downlink Only
- **Up to 4 Users**
- **Up to 4 Streams/User**
- **Total 8 Streams Max**



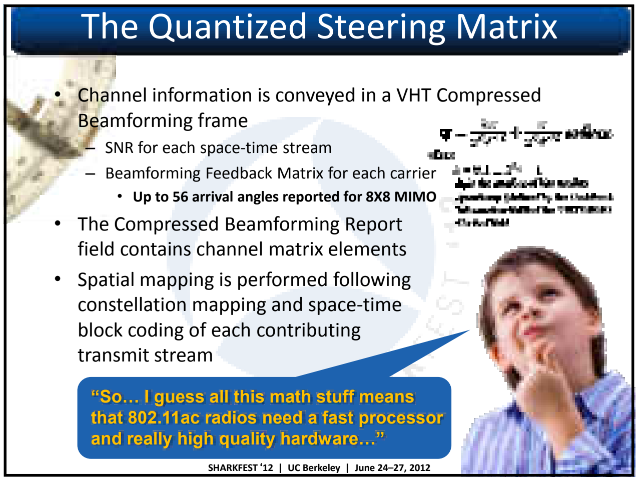
802.11ac Beamforming

- Access point and client device share information about the communication's channel
- Both devices can coherently focus their transmission streams at each other
- The 802.11ac chipset adjusts the transmitted signals phase on each antenna to overcome multipath distortion and maximize the acquisition of multiple spatial streams
- 802.11ac beamforming is an optional feature but it is standardized in the spec
  - Unlike vendor-proprietary 802.11n beamforming methods
    - Ruckus BeamFlex
    - Cisco MRC and beamforming



VHT Sounding Protocol

- The environment is "sounded" to create a digital representation of the state of the transmission channel
  - A "Steering Matrix" is the mathematical representation of the current state of the environment
    - Attenuation and phase shift experienced by each spatial stream
- Transmit Beamforming and MU-MIMO require knowledge of the channel state to compute a steering matrix to optimize reception at one or more receivers
  - Individual space-time streams are sounded separately
  - Training symbols are transmitted ("Sounding Poll") and measured by the recipient station (or stations)
  - A channel state estimate is sent back to the beamformer from each station included in the Sounding Poll for the derivation of a steering matrix

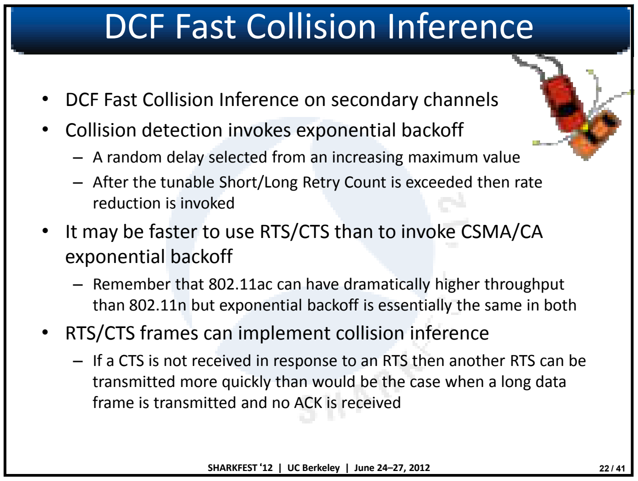


The Quantized Steering Matrix

- Channel information is conveyed in a VHT Compressed Beamforming frame
  - SNR for each space-time stream
  - Beamforming Feedback Matrix for each carrier
    - **Up to 56 arrival angles reported for 8X8 MIMO**
- The Compressed Beamforming Report field contains channel matrix elements
- Spatial mapping is performed following constellation mapping and space-time block coding of each contributing transmit stream

"So… I guess all this math stuff means that 802.11ac radios need a fast processor and really high quality hardware…"

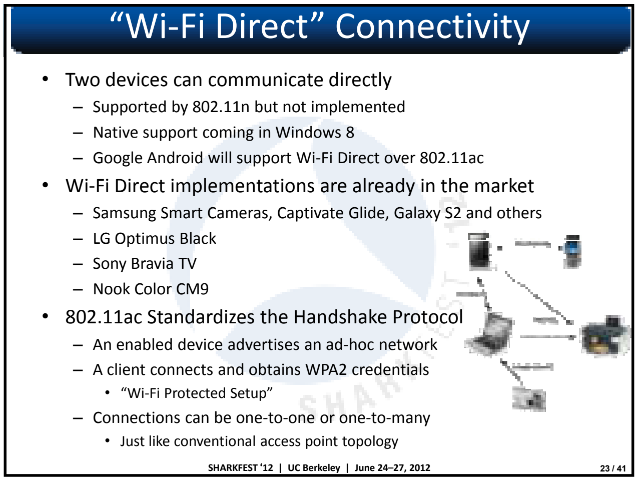
SHARKFEST '12 | UC Berkeley | June 24–27, 2012



DCF Fast Collision Inference

- DCF Fast Collision Inference on secondary channels
- Collision detection invokes exponential backoff
  - A random delay selected from an increasing maximum value
  - After the tunable Short/Long Retry Count is exceeded then rate reduction is invoked
- It may be faster to use RTS/CTS than to invoke CSMA/CA exponential backoff
  - Remember that 802.11ac can have dramatically higher throughput than 802.11n but exponential backoff is essentially the same in both
- RTS/CTS frames can implement collision inference
  - If a CTS is not received in response to an RTS then another RTS can be transmitted more quickly than would be the case when a long data frame is transmitted and no ACK is received

SHARKFEST '12 | UC Berkeley | June 24–27, 2012 22 / 41



"Wi-Fi Direct" Connectivity

- Two devices can communicate directly
  - Supported by 802.11n but not implemented
  - Native support coming in Windows 8
  - Google Android will support Wi-Fi Direct over 802.11ac
- Wi-Fi Direct implementations are already in the market
  - Samsung Smart Cameras, Captivate Glide, Galaxy S2 and others
  - LG Optimus Black
  - Sony Bravia TV
  - Nook Color CM9
- 802.11ac Standardizes the Handshake Protocol
  - An enabled device advertises an ad-hoc network
  - A client connects and obtains WPA2 credentials
    - "Wi-Fi Protected Setup"
  - Connections can be one-to-one or one-to-many
    - Just like conventional access point topology

SHARKFEST '12 | UC Berkeley | June 24–27, 2012 23 / 41

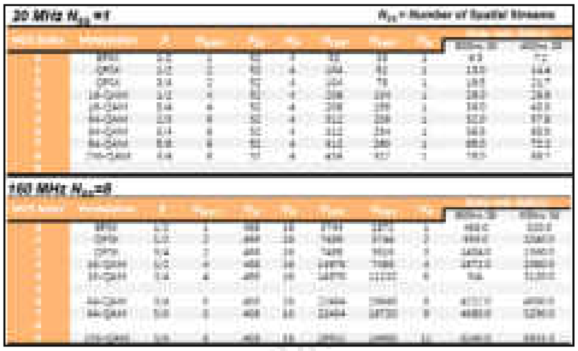
Wi-Fi Direct

- **Wi-Fi Direct Provides Capabilities Similar to Bluetooth But At Wi-Fi Speeds and Ranges**
  - Support for Wi-Fi Direct is included in 1st Generation 802.11ac chipsets

From YouTube by the WiFi Alliance
"Wi-Fi Direct^{TM}: Connect with the possibilities"

SHARKFEST '12 | UC Berkeley | June 24–27, 2012 24 / 41

Connection Rates by MCS Index



20 MHz N_{SS} =1 — N_{SS} = Number of Spatial Streams

MCS Index	Modulation	R	N_{BPSCS}	N_{SD}	N_{SP}	N_{CBPS}	N_{DBPS}	N_{ES}	Data Rate (Mb/s) 800ns GI	Data Rate (Mb/s) 400ns GI
0	BPSK	1/2	1	52	4	52	26	1	6.5	7.2
1	QPSK	1/2	2	52	4	104	52	1	13.0	14.4
2	QPSK	3/4	2	52	4	104	78	1	19.5	21.7
3	16-QAM	1/2	4	52	4	208	104	1	26.0	28.9
4	16-QAM	3/4	4	52	4	208	156	1	39.0	43.3
5	64-QAM	2/3	6	52	4	312	208	1	52.0	57.8
6	64-QAM	3/4	6	52	4	312	234	1	58.5	65.0
7	64-QAM	5/6	6	52	4	312	260	1	65.0	72.2
8	256-QAM	3/4	8	52	4	416	312	1	78.0	86.7

160 MHz N_{SS}=8

MCS Index	Modulation	R	N_{BPSCS}	N_{SD}	N_{SP}	N_{CBPS}	N_{DBPS}	N_{ES}	Data Rate (Mb/s) 800ns GI	Data Rate (Mb/s) 400ns GI
0	BPSK	1/2	1	468	16	3744	1872	1	468.0	520.0
1	QPSK	1/2	2	468	16	7488	3744	2	936.0	1040.0
2	QPSK	3/4	2	468	16	7488	5616	3	1404.0	1560.0
3	16-QAM	1/2	4	468	16	14976	7488	4	1872.0	2080.0
4	16-QAM	3/4	4	468	16	14976	11232	6	N/A	3120.0
5										
6	64-QAM	3/4	6	468	16	22464	16848	8	4212.0	4680.0
7	64-QAM	5/6	6	468	16	22464	18720	9	4680.0	5200.0
8										
9	256-QAM	5/6	8	468	16	29952	24960	12	6240.0	6933.3

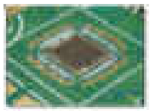
R – Coding Rate
N_{BPSCS} – Bits/Subcarrier (per Spatial Stream)
N_{SD} –Modulated Data Symbols
N_{SP} –Pilot Symbols
N_{CBPS} –Coded Bits / Symbol
N_{DBPS} –Data Bits / Symbol
N_{ES} –Data Field BCC Encoders

Error Correction With BCC

- Binary Convolutional Codes
  - A quantifiable number of errors can be guaranteed to be corrected
    - The “Correcting Capability” (t) can be calculated based on the complexity of the encoding scheme
    - The “Hamming Distance” (d) is the number of bits that are different in two strings of equal length

$$t = \frac{d-1}{2}$$

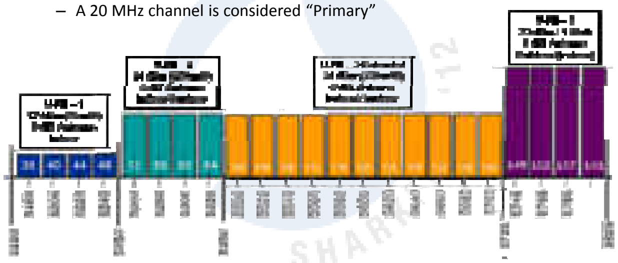
- Used In All 802.11 Implementations
  - The encoder(s) must be capable of processing the transmitted bit stream
    - 802.11n implements a single BCC encoder
    - 802.11ac can implement up to 12 separate encoders
- A Typical Encoding Process
  - A binary convolutional code is denoted by a three-tuple (n, k,m).
  - n output bits are generated whenever k input bits are received.
  - The current n outputs are linear combinations of the present k Input bits and the previous m × k input bits.
  - m designates the number of previous k-bit input blocks that must be memorized in the encoder.
  - m is called the memory order of the convolutional code



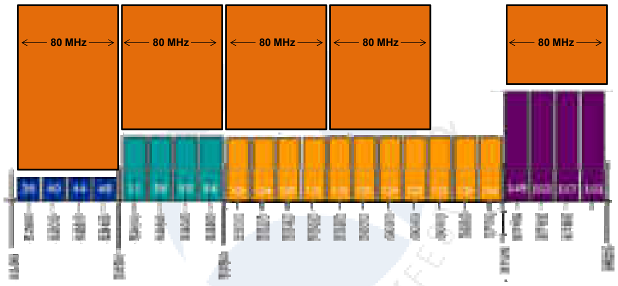
Multiple BCC Encoders Implies High Processing Capabilities

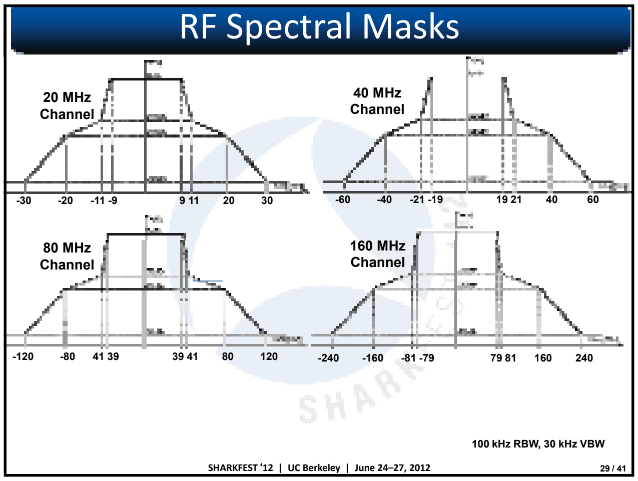
ISM Channel Availability

- 802.11ac Channel Configuration Options
  - 20, 40, 80 and 160 Mbps
  - DFS is still required in U-NII-2 Extended (Channel 100 – 140)
  - A 20 MHz channel is considered “Primary”



ISM Channel Availability

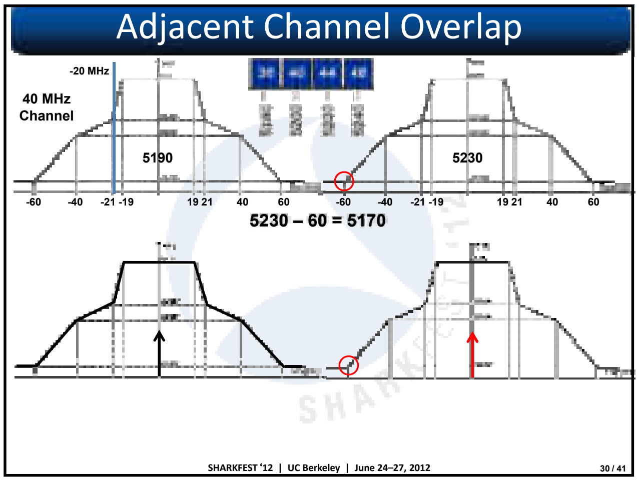




RF Spectral Masks

100 kHz RBW, 30 kHz VBW

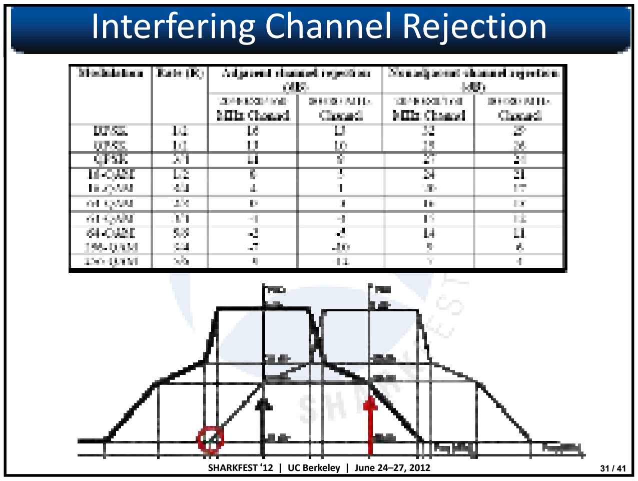
SHARKFEST '12 | UC Berkeley | June 24–27, 2012 29 / 41



Adjacent Channel Overlap

5230 – 60 = 5170

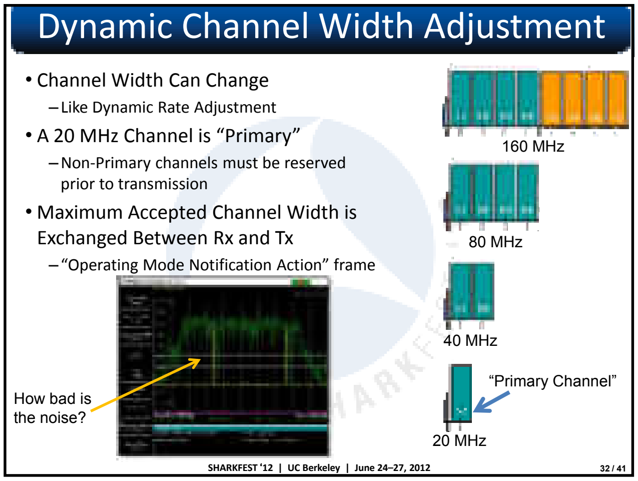
SHARKFEST '12 | UC Berkeley | June 24–27, 2012 30 / 41



Interfering Channel Rejection

Modulation	Rate (R)	Adjacent channel rejection (dB)		Nonadjacent channel rejection (dB)	
		20/40/80/160 MHz Channel	80+80 MHz Channel	20/40/80/160 MHz Channel	80+80 MHz Channel
BPSK	1/2	16	13	32	29
QPSK	1/2	13	10	29	26
QPSK	3/4	11	8	27	24
16-QAM	1/2	8	5	24	21
16-QAM	3/4	4	1	20	17
64-QAM	2/3	0	-3	16	13
64-QAM	3/4	-1	-4	15	12
64-QAM	5/6	-2	-5	14	11
256-QAM	3/4	-7	-10	9	6
256-QAM	5/6	-9	-12	7	4

SHARKFEST '12 | UC Berkeley | June 24–27, 2012 31 / 41

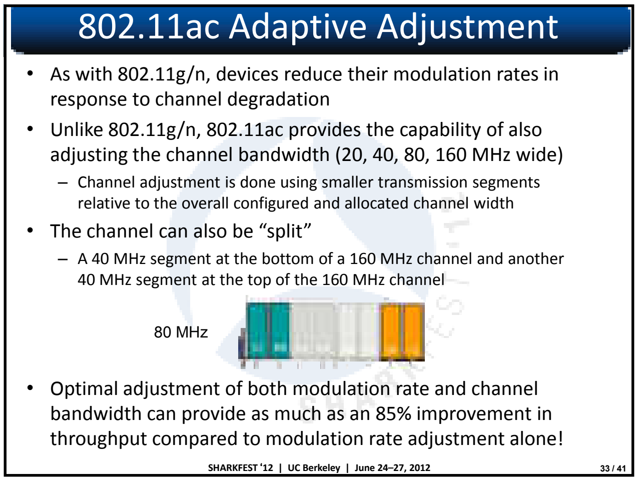


Dynamic Channel Width Adjustment

- Channel Width Can Change
  - Like Dynamic Rate Adjustment
- A 20 MHz Channel is "Primary"
  - Non-Primary channels must be reserved prior to transmission
- Maximum Accepted Channel Width is Exchanged Between Rx and Tx
  - "Operating Mode Notification Action" frame

How bad is the noise?

SHARKFEST '12 | UC Berkeley | June 24–27, 2012 32 / 41

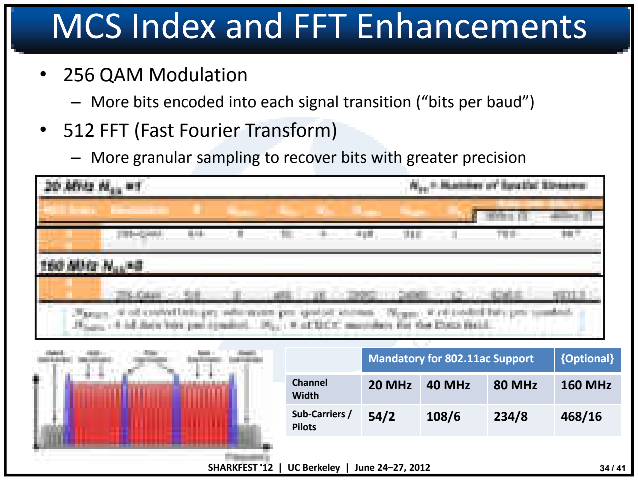


802.11ac Adaptive Adjustment

- As with 802.11g/n, devices reduce their modulation rates in response to channel degradation
- Unlike 802.11g/n, 802.11ac provides the capability of also adjusting the channel bandwidth (20, 40, 80, 160 MHz wide)
  - Channel adjustment is done using smaller transmission segments relative to the overall configured and allocated channel width
- The channel can also be "split"
  - A 40 MHz segment at the bottom of a 160 MHz channel and another 40 MHz segment at the top of the 160 MHz channel

- Optimal adjustment of both modulation rate and channel bandwidth can provide as much as an 85% improvement in throughput compared to modulation rate adjustment alone!

SHARKFEST '12 | UC Berkeley | June 24–27, 2012 33 / 41



MCS Index and FFT Enhancements

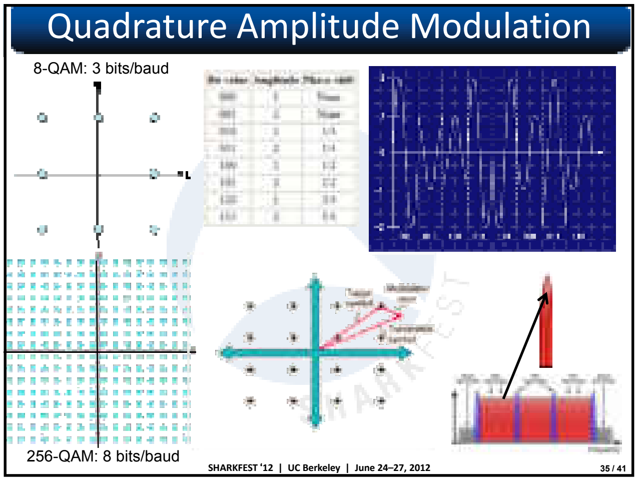
- 256 QAM Modulation
  - More bits encoded into each signal transition ("bits per baud")
- 512 FFT (Fast Fourier Transform)
  - More granular sampling to recover bits with greater precision

20 MHz N_{SS} =1 — N_{SS} = Number of Spatial Streams

160 MHz N_{SS} =8

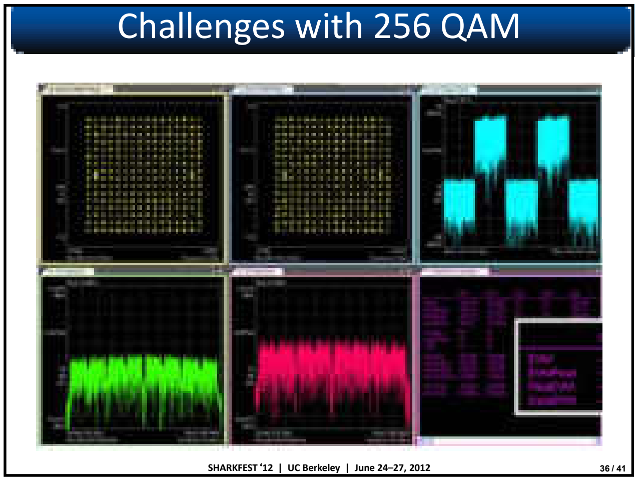
	Mandatory for 802.11ac Support			{Optional}
Channel Width	20 MHz	40 MHz	80 MHz	160 MHz
Sub-Carriers / Pilots	54/2	108/6	234/8	468/16

SHARKFEST '12 | UC Berkeley | June 24–27, 2012 34 / 41



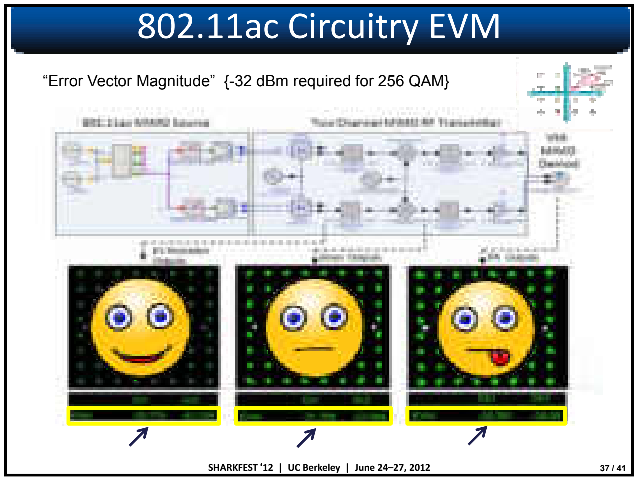
Quadrature Amplitude Modulation

SHARKFEST '12 | UC Berkeley | June 24–27, 2012 35 / 41



Challenges with 256 QAM

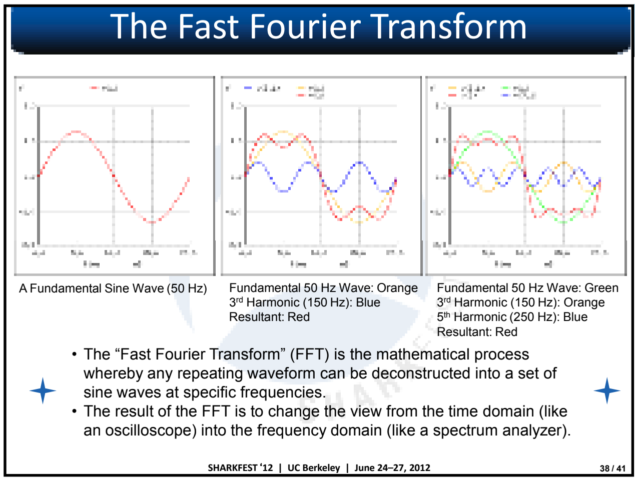
SHARKFEST '12 | UC Berkeley | June 24–27, 2012 36 / 41



802.11ac Circuitry EVM

"Error Vector Magnitude" {-32 dBm required for 256 QAM}

SHARKFEST '12 | UC Berkeley | June 24–27, 2012 37 / 41



The Fast Fourier Transform

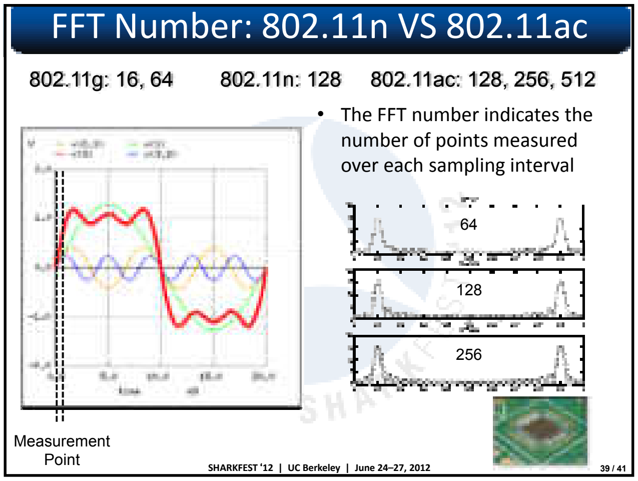
A Fundamental Sine Wave (50 Hz)

Fundamental 50 Hz Wave: Orange
3rd Harmonic (150 Hz): Blue
Resultant: Red

Fundamental 50 Hz Wave: Green
3rd Harmonic (150 Hz): Orange
5th Harmonic (250 Hz): Blue
Resultant: Red

- The "Fast Fourier Transform" (FFT) is the mathematical process whereby any repeating waveform can be deconstructed into a set of sine waves at specific frequencies.
- The result of the FFT is to change the view from the time domain (like an oscilloscope) into the frequency domain (like a spectrum analyzer).

SHARKFEST '12 | UC Berkeley | June 24–27, 2012 38 / 41

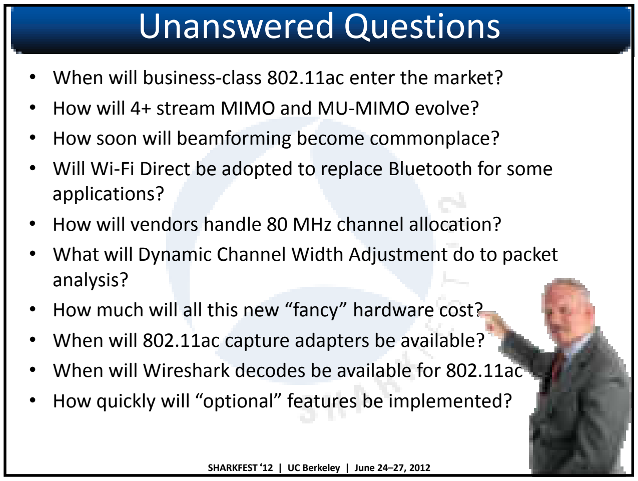


FFT Number: 802.11n VS 802.11ac

802.11g: 16, 64 802.11n: 128 802.11ac: 128, 256, 512

- The FFT number indicates the number of points measured over each sampling interval

SHARKFEST '12 | UC Berkeley | June 24–27, 2012 39 / 41



Unanswered Questions

- When will business-class 802.11ac enter the market?
- How will 4+ stream MIMO and MU-MIMO evolve?
- How soon will beamforming become commonplace?
- Will Wi-Fi Direct be adopted to replace Bluetooth for some applications?
- How will vendors handle 80 MHz channel allocation?
- What will Dynamic Channel Width Adjustment do to packet analysis?
- How much will all this new "fancy" hardware cost?
- When will 802.11ac capture adapters be available?
- When will Wireshark decodes be available for 802.11ac
- How quickly will "optional" features be implemented?

SHARKFEST '12 | UC Berkeley | June 24–27, 2012

It's Coming.. Be Ready :-)

June 5-9, 2012

The ASUS G75VW with Broadcom 802.11ac WiFi

SHARKFEST '12 | UC Berkeley | June 24–27, 2012

41 / 41

Thank You!

@Connect802
follow us on
twitter

www.Connect802.com
joe@connect802.com