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.

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

3-D RF CAD Modeling and Simulation

Copyright by Connect802 Corporation - www.Connect802.com
The Connect802 Landscape

Here it comes: 802.11ac

- Early consumer products are shipping today
- Commercial-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 Lightweight 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
  - 4K UltraHD (25 Mbps Stream)
- Uncompressed 1080P1080 (3.7 Gbps Stream)

The Evolving 802.11 Standards

- 802.11n 600 Mbps
- 802.11ac 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!
The PLCP Protocol Data Unit (PPDU)

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

802.11n PPDU (Mixed Mode)

802.11ac VHT PPDU

L: Indicates Legacy (802.11abgn) Field
HT: Indicates 802.11n High Throughput
VHT: Indicates 802.11ac Very High Throughput
SIG: Protection Mechanism Signal Field
VHT-SIG-A: Number of Streams, MCS, Beamforming Matrix
VHT-SIG-B: Length of Data and MCS for MU Mode
STF: Short Training Field
VHT-STF: Improves AGC Estimations for MIMO
LTF: Long Training Field (Mapping Matrix)

The Evolution of Wireshark

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

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
  - Up to 32 spatial streams with refined beamforming
  - Very limited range at 60 GHz (HDMI Cable Replacement)
  - Sub-1GHz frequencies
  - Ultra low-power Wi-Fi
  - Targeted for product-to-market in 2014

802.11ac VHT PPDU

In case you wondered: 802.11a is a standard for prioritization of management frames when exchanged between LAN and WAN.
Today’s Mind Meld

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

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 PPDU’s (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

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

Spatial Streams in 802.11ac

- SISO (Single Input Single Output)
- MISO (Multiple Input Single Output)
- SIMO (Single Input Multiple Output)
- MIMO (Multiple Input Multiple Output)
MIMO in 802.11ac

- Spatial Expansion (Transmit Diversity)
- Spatial-time block coding (STBC)
- Receive Diversity
- Spatial multiplexing (direct mapping)

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

**“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 advertise 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

**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

**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

**Copyright by Connect802 Corporation - www.Connect802.com**

Stanford University
June 13-16, 2011
### Connection Rates by MCS Index

#### 20 MHz $N_{sb}$ \#1

<table>
<thead>
<tr>
<th>Mode</th>
<th>$K_{ps}$</th>
<th>$N_{ps}$</th>
<th>$K_{ds}$</th>
<th>$N_{ds}$</th>
<th>$K_{好了}$</th>
<th>$N_{好了}$</th>
<th>$K_{好了}$</th>
<th>$N_{好了}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPI</td>
<td>1.2</td>
<td>0.76</td>
<td>1.2</td>
<td>0.76</td>
<td>1.2</td>
<td>0.76</td>
<td>1.2</td>
<td>0.76</td>
</tr>
<tr>
<td>DQPSK</td>
<td>0.75</td>
<td>0.75</td>
<td>0.75</td>
<td>0.75</td>
<td>0.75</td>
<td>0.75</td>
<td>0.75</td>
<td>0.75</td>
</tr>
<tr>
<td>16QAM</td>
<td>3.4</td>
<td>3.4</td>
<td>3.4</td>
<td>3.4</td>
<td>3.4</td>
<td>3.4</td>
<td>3.4</td>
<td>3.4</td>
</tr>
<tr>
<td>64QAM</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
</tr>
<tr>
<td>256QAM</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
</tr>
</tbody>
</table>

#### 160 MHz $N_{sb}$ \#1

<table>
<thead>
<tr>
<th>Mode</th>
<th>$K_{ps}$</th>
<th>$N_{ps}$</th>
<th>$K_{ds}$</th>
<th>$N_{ds}$</th>
<th>$K_{好了}$</th>
<th>$N_{好了}$</th>
<th>$K_{好了}$</th>
<th>$N_{好了}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPI</td>
<td>1.2</td>
<td>0.76</td>
<td>1.2</td>
<td>0.76</td>
<td>1.2</td>
<td>0.76</td>
<td>1.2</td>
<td>0.76</td>
</tr>
<tr>
<td>DQPSK</td>
<td>0.75</td>
<td>0.75</td>
<td>0.75</td>
<td>0.75</td>
<td>0.75</td>
<td>0.75</td>
<td>0.75</td>
<td>0.75</td>
</tr>
<tr>
<td>16QAM</td>
<td>3.4</td>
<td>3.4</td>
<td>3.4</td>
<td>3.4</td>
<td>3.4</td>
<td>3.4</td>
<td>3.4</td>
<td>3.4</td>
</tr>
<tr>
<td>64QAM</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
</tr>
<tr>
<td>256QAM</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
</tr>
</tbody>
</table>

### 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

#### Used In All 802.11 Implementations
- The encoder(s) must be capable of processing the transmitted bit stream
  - 802.11x 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 triple $(n, k, m)$
- $n$ 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

---

### 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”
RF Spectral Masks

20 MHz Channel

40 MHz Channel

80 MHz Channel

160 MHz Channel

Adjacent Channel Overlap

40 MHz Channel

5190

5230

5230 – 60 = 5170

Interfering Channel Rejection

<table>
<thead>
<tr>
<th>Modulation</th>
<th>Rate (Mb/s)</th>
<th>Adjacent channel rejection (dB)</th>
<th>Non-adjacent channel rejection (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPSK</td>
<td>1</td>
<td>11</td>
<td>11 (20 MHz)</td>
</tr>
<tr>
<td>QPSK</td>
<td>1/2</td>
<td>11</td>
<td>11 (20 MHz)</td>
</tr>
<tr>
<td>QPSK</td>
<td>1/4</td>
<td>11</td>
<td>11 (20 MHz)</td>
</tr>
<tr>
<td>QAM</td>
<td>1/2</td>
<td>21</td>
<td>21 (20 MHz)</td>
</tr>
<tr>
<td>QAM</td>
<td>1/4</td>
<td>21</td>
<td>21 (20 MHz)</td>
</tr>
<tr>
<td>QAM</td>
<td>1/8</td>
<td>21</td>
<td>21 (20 MHz)</td>
</tr>
<tr>
<td>QAM</td>
<td>1/16</td>
<td>21</td>
<td>21 (20 MHz)</td>
</tr>
<tr>
<td>QAM</td>
<td>1/32</td>
<td>21</td>
<td>21 (20 MHz)</td>
</tr>
</tbody>
</table>

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?
• 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!

• 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

<table>
<thead>
<tr>
<th>Channel Width</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 MHz</td>
</tr>
<tr>
<td>40 MHz</td>
</tr>
<tr>
<td>80 MHz</td>
</tr>
<tr>
<td>160 MHz</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sub-Carriers / Pilots</th>
</tr>
</thead>
<tbody>
<tr>
<td>54/2</td>
</tr>
<tr>
<td>108/6</td>
</tr>
<tr>
<td>234/8</td>
</tr>
<tr>
<td>468/16</td>
</tr>
</tbody>
</table>

256-QAM: 8 bits/baud
**802.11ac Circuitry EVM**

"Error Vector Magnitude" (-32 dBm required for 256 QAM)

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

<table>
<thead>
<tr>
<th>Measurement Point</th>
<th>802.11g: 16, 64</th>
<th>802.11n: 128</th>
<th>802.11ac: 128, 256, 512</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11ac MIMO Source</td>
<td>Two Channel MIMO RF Transmitter</td>
<td>SAW</td>
<td>EVM</td>
</tr>
</tbody>
</table>

**The Fast Fourier Transform**

- 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).

**FFT Number: 802.11n VS 802.11ac**

- 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?
It's Coming.. Be Ready :-)