Wireshark Developer and User Conference

Mobile Application Analysis with Wireshark
June 14, 2011

Joe Bardwell
President and Chief Scientist | Connect802 Corporation
joe@Connect802.com - www.Connect802.com

SHARKFEST ‘11
Stanford University
June 13-16, 2011

About Connect802 Corporation

• Founded in 1994 with headquarters in the San Francisco Bay area and East Coast engineering out of Atlanta, Georgia
• 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
Overview

- Wireshark provides you with a microscope to examine the detailed behavior on the network
- The behavior you observe makes sense only in the context of the applicable networking standards
- First you must know what is supposed to be happening – then you analyze what is actually happening – then you discern the differences

802.11 Architecture (Basic)

- The Access Point (AP) provides access to the network
- Client devices are Associated to one and only one AP
- All traffic to/from the client device goes through the AP
**AP Discovery**

- **Passive Discovery**
  - Client devices listen for *Beacon* frames sent by APs
- **Active Discovery**
  - Client devices send *Probe Request* frames
  - APs hear the Probe Requests
  - APs respond with *Probe Response* frames

**Authentication**

- Authentication between client and AP must succeed before the AP will pass data frames
- 802.11 defines two forms of authentication
  - Open System (always successful—equivalent to no authentication at all)
  - Shared Key (hash-based challenge/response using WEP key as a token)
**Association**

- Client device decides which AP it wants to associate with
- *Authentication* packets are exchanged
- *Association Request / Response* is exchanged

**A Conundrum**

- Previously, we said that:
  - Authentication between client and AP must succeed before the AP will pass data frames
  - 802.11 defines two forms of authentication
    - Open System (always successful) - equivalent to no authentication at all
    - Shared Key (hash-based challenge/response using WEP key as a token)
- What about 802.1x (WPA)?
Which Came First...

- 802.1x (WPA) authentication uses the EAPOL protocol
- Only 802.11 packets can be Management or Control frames; EAPOL packets must be sent as Data frames
- Data frames can only be sent after authentication
- But EAPOL is used to accomplish authentication!

802.1x (WPA) Authentication

- When a client and AP wish to perform WPA authentication, the client uses Open System authentication (which is always successful)
- Once this “authentication” is complete, the client can send Data frames, but...
- The AP only lets the client send EAPOL data frames until WPA authentication is successful
Disassociation / Deauthentication

- When the client device wants to leave the network, it can send Disassociation and/or Deauthentication frames to the AP
  - Disassociation terminates the association, but leaves the authentication present
  - If the client later wants to come back, it can associate without going through the authentication process
  - Deauthentication terminates the authentication and, hence, the association, since association requires authentication to be present

Roaming

- Roaming: To move an Association from one AP to another
- Roaming is completely controlled by the client
- APs cannot force a client to roam or control which AP a client roams to
  - Makes implementing load-balancing tricky
Roaming Issues

• Thrashing
  – STA rapidly bounces back and forth between two or more APs
  – Can be caused by excessive AP density or cell overlap

• Sticky
  – STA stays associated with a weak AP when much stronger APs are readily available
  – This is 100% a driver issue; some drivers have adjustable stickiness, others don’t

Reassociation

• When a station wants to roam from one AP to another, it sends a Reassociation frame to the new AP
• If the new AP sends back a successful Reassociation Response, the station has roamed
• The roaming is instantaneous, so at no point does the station lose its link
• If the reassociation fails, the station remains associated with its old AP
Reassociation In Wireshark

- Probes are used to find potential new APs
  - This usually happens continuously
  - Some devices will only start probing when they want to roam
- Authentication must precede Reassociation
  - Some devices will pre-authenticate with multiple nearby APs to speed up roaming

### A Real-World Example

- Customer reported that client devices would go offline periodically
- Incidents were not localized to any particular time or place
- Survey of the environment with spectrum analyzer showed excellent signal strength and no interference (always check for this!)
Clean Spectrum

“Dirty” Spectrum (FHSS)
“Dirty” Spectrum (FHSS)

Frequency-Hopping Interferer seen across the spectrum.

“Dirty” Spectrum (Jammer)

Wideband signal across the entire frequency range (no 802.11 is visible above the jammer’s peak power).
"Dirty" Spectrum (Microwave)

Peak power in channel 11, decreasing in 1 and 6 shape.

A Distributed Problem

- The problem did not happen in any predictable location
- Multiple Wireshark laptops (with multi-channel adapters) were set up throughout the site so that when the problem happened, we would catch it
Long-Term Capturing

- Incidents were not predictable, therefore Wireshark was set up to capture for a very long time (overnight)
- Wireshark config was as shown to the right

What We Found: Retries

<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>Duration</th>
<th>Error Code</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>04:00</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:01</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:02</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:03</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:04</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:05</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:06</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:07</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:08</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:09</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:10</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:11</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:12</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:13</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:14</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:15</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:16</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:17</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:18</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
<tr>
<td>04:19</td>
<td>Data</td>
<td>04:00</td>
<td>00000000</td>
<td>10000</td>
</tr>
</tbody>
</table>

Confirm that you have sufficient hard drive space before doing this. 20 meg per file * 1000 files = 20 gig of data total.
802.11 Reliability

- 802.11 Data must be acknowledged by the recipient
- If an ACK is not received, the source station retransmits
- Note the Retry bit and the repeated Sequence Number in the packets below

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Frame Type</th>
<th>Length</th>
<th>Frame Check</th>
<th>Priority</th>
<th>but Rate</th>
<th>Sequence Number</th>
<th>ACK Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>123</td>
<td>12:45</td>
<td>intel_eei1710f</td>
<td>Data</td>
<td>1234</td>
<td></td>
<td>0</td>
<td>1000</td>
<td>0001</td>
<td></td>
</tr>
<tr>
<td>127</td>
<td>12:45</td>
<td>intel_eei1710f</td>
<td>Data</td>
<td>1234</td>
<td></td>
<td>0</td>
<td>1000</td>
<td>0001</td>
<td></td>
</tr>
<tr>
<td>139</td>
<td>12:45</td>
<td>intel_eei1710f</td>
<td>Data</td>
<td>1234</td>
<td></td>
<td>0</td>
<td>1000</td>
<td>0001</td>
<td></td>
</tr>
<tr>
<td>140</td>
<td>12:45</td>
<td>intel_eei1710f</td>
<td>Data</td>
<td>1234</td>
<td></td>
<td>0</td>
<td>1000</td>
<td>0001</td>
<td></td>
</tr>
</tbody>
</table>

How Many Retries?

- We see over 60 retries from the AP
- 802.11 defines two Retry thresholds, which default to 7 and 4
- This can be overridden by the administrator
- This is a good example of why this defaults to a LOW number!
Dynamic Rate Shifting

- When retries occur, a station will decrease the data rate used to increase the packet’s resistance to corruption
- This is known as Dynamic Rate Shifting (DRS)

What’s Happening: Retries

- Packets from the AP to the STA are being retransmitted
- Four possibilities:
  - STA did not get the data frame, hence no ACK
  - STA got the data but did not send an ACK
  - STA sent an ACK, but it didn’t get to the AP
  - ACK got to the AP, and the AP incorrectly retransmitted anyway
Is It The AP or the STA?

- Graph below is filtered on only traffic going to/from the AP in question and not the STA in question
- Orange line indicates the anomalous event
- Does anything seem to change before/after?

---

It’s the Station

- AP’s behavior is consistent before/after the anomalous event
  - Data (green line) continues to flow
  - No increase in retries to stations other than the one in question
- What could cause this behavior?
  - STA is receiving data frames and not sending ACKs, in violation of 802.11 standard (unlikely)
  - STA is not receiving data frames for some reason (more likely)
### What We Found: Association

- After a short time, STA is seen associating to a different AP
- Most likely scenario: STA went offline (hence, retries from the AP) then came back

```
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00</td>
<td>STA1 ASSOCIATION-REQ (A)</td>
</tr>
<tr>
<td>00:01</td>
<td>STA1 ASSOCIATION-ACK</td>
</tr>
<tr>
<td>00:02</td>
<td>STA1 ASSOCIATION-REQ (B)</td>
</tr>
<tr>
<td>00:03</td>
<td>STA1 ASSOCIATION-ACK</td>
</tr>
</tbody>
</table>

---

### “Optional”?

- 802.11 does not require Disassociate or Deauthenticate frames when a station goes offline
  - What if a station had its battery pulled or suddenly went out of range?
  - 802.11 must allow for situations where the station unexpectedly goes offline
- If STA doesn’t send Disassociate or Deauthenticate, this scenario can arise
  - AP doesn’t know the STA is gone!
What We Found: More Retries!

• The Association is interrupted during WPA authentication

When analyzing repeated packets, examine sequence numbers at various layers of the OSI model to determine where the retransmission is coming from

– Repeated 802.11 sequence number indicates wireless ACK was not received
Retry Analysis

- 1\textsuperscript{st} Packet has SEQ 167
- 2\textsuperscript{nd} and subsequent packets have SEQ 219
- 1\textsuperscript{st} Packet must have been ACK’ed by the STA
- STA failed to send the appropriate EAPOL response
- AP’s operating system timed out and tried again

---

Retry Analysis

- This same process can be applied going up the layers of the OSI model
  - 802.11 retries indicate no ACK from recipient
    - Noise/interference corrupting packet
      - Remove the source of interference
      - Shield the source of interference
      - Move to a different channel than the interference
    - Insufficient signal strength/client is out of range
      - Assess network design to determine if AP placement is correct
      - Assess AP output power (dynamic power setting sometimes turns output power down too low)
Retry Analysis

• This same process can be applied going up the layers of the OSI model
  – TCP retransmissions with 802.11 retries on the same packet indicate extreme interference
    • Normally, 802.11 retries would get the data through before TCP timed out
    • If TCP is timing out, the wireless network must be nearly totally congested

<table>
<thead>
<tr>
<th>TCP Retransmission</th>
<th>ismaeasdaqtest &gt; 43120 [PSH, ACK] Seq=1 Ack=0</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP DU0 ACK 18232</td>
<td>43120 &gt; ismaeasdaqtest [ACK] Seq=5 Ack=5921</td>
</tr>
<tr>
<td>b1menu &gt; 30019 [ack] Seq=1 Ack=2481 Win=45535 Len=0</td>
<td></td>
</tr>
<tr>
<td>TCP Retransmission</td>
<td>ismaeasdaqtest &gt; 43120 [PSH, ACK] Seq=1461</td>
</tr>
<tr>
<td>TCP DU0 ACK 18232</td>
<td>43120 &gt; ismaeasdaqtest [ACK] Seq=5 Ack=5921</td>
</tr>
</tbody>
</table>

Who is 00:30:64:04:28:ab? Tell 00:30:64:04:28:ad

Retry Analysis

• This same process can be applied going up the layers of the OSI model
  – TCP retransmissions without 802.11 retries on the same packet usually indicates corruption or congestion on the wired network
    • Corruption is rare in today's wired networks
    • Congestion (possibly due to QoS rules?) is more likely
  – The lack of 802.11 retries indicates that the packet got from the wireless station to the AP successfully
Retry Analysis

• This same process can be applied going up the layers of the OSI model
  – Repeated packets or packet sequences without either TCP or 802.11 retransmissions indicate an app or user is the cause
  – App with server polling interval too low
  – Very impatient user!

What We Found: Deauthenticate
What We Found: Deauthenticate

AP finally times out on the absent STA. Sends Deauth just to make sure the STA knows the transaction is off.

Oh look! There's the STA again, trying to find an AP to associate to!

STA begins association again.

This time it succeeds and data begins to flow.

... And they all lived happily ever after?
What We Found: Disassociate

• After some time, the station disassociates
  – Is it going offline (correctly this time?)
  – What happens next?

Disassociate. STA is leaving the AP.

Probes. STA is trying to find an AP to associate with.

STA begins association again.

Success! What was all that about? The STA is just roaming, but it’s using Disassociate instead of Reassociate.
What Do We Know?

• Station sometimes drops offline without sending a Disassociate or Deauthenticate frame, causing the AP to retransmit packets 50-70 times before giving up
• Station uses Disassociate frame when roaming, resulting in loss of connectivity until roaming succeeds
• Who is at fault here? AP? STA? Network?

Analysis With I/O Graphs

• When combined with filters, Wireshark's I/O graphs can help with visualization of a network issue

![Graph showing network traffic and client behavior]
Graph 1 – No filter. Total packets-per-second for the network/trace
Graph 2 – wlan.fc.retry==1 shows 802.11 retries

Graph 4 – shows roaming-related packets: Probe Request, Authentication, Association Request, Association Response, 802.1x Authentication (see below for filter). If desired, also filter on a specific station’s MAC address. Alternatively pre-filter the trace and save out only packets that pass the filter.
Tick Interval at 1 sec ensures that Y-axis is showing packets per second (vs. packets per 5 seconds etc...)

Adjust pixels per tick to stretch the X axis to the most useful value for your troubleshooting
A Visual Guide

- Client is roaming. Some data gets through.
- Flurry of retries from AP
- Client goes silent
- Client returns to normal operation. "Burst" of backlogged data.

Using I/O Graphs To Compare

- These two graphs compare the wireless and the wired side of the same conversation
- Red lines indicate retries (wireless) or TCP retransmissions (wired)
These two graphs compare the wireless and the wired side of the same conversation.

- Wireshark was capturing on both sides and timestamps were cross-correlated.
- Red lines indicate retries (wireless) or TCP retransmissions (wired).
Clock Synchronization

- When analyzing roaming, it is sometimes necessary to compare traces taken from different laptops.
- Clocks on the laptops are seldom perfectly synchronized, so comparing the traces can be difficult.
- Record time offset of each laptop relative to a “master” clock like a cell phone or one laptop.
- Calculate delta between each laptop and each other laptop to allow trace comparison.

“Normal” Roaming

- Same device, slightly different behavior.
- Just based on the graph, how does this compare?
“Normal” Roaming

No flurry of retries. STA did go “radio silent” before roaming

Roaming completes quickly

Conclusion

“When you have eliminated the impossible, whatever remains, however improbable, must be the truth.” — Sir Arthur Conan Doyle
Conclusion

• We must hold the observed behavior up against the standards that define what the device and protocol should do
  – 802.11 (Wi-Fi), 802.3 (Ethernet), and so forth: http://standards.ieee.org/about/get/
  – Vendor-specific items like Cisco’s CCX (Cisco Certified Extensions): getting protocol-level documentation for vendor-specific items is often difficult—usually requires a call to the vendor’s engineer

Conclusion

• The problem is with the STA
• Even if you could blame the excessive roaming on the network or the air, the use of Disassociate instead of Reassociate when roaming is definitively incorrect
• No explanation for why the device sometimes goes “radio silent” before roaming
• This was a specialized appliance with custom drivers written by the vendor (as opposed to the chipset manufacturer): talk to the vendor!
Joe Bardwell
Connect802 Corporation
San Ramon, CA
(925) 552-0802
joe@Connect802.com