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

Connect802
Wireless Data Solutions

SHARKFEST '11
Stanford University
June 13-16, 2011

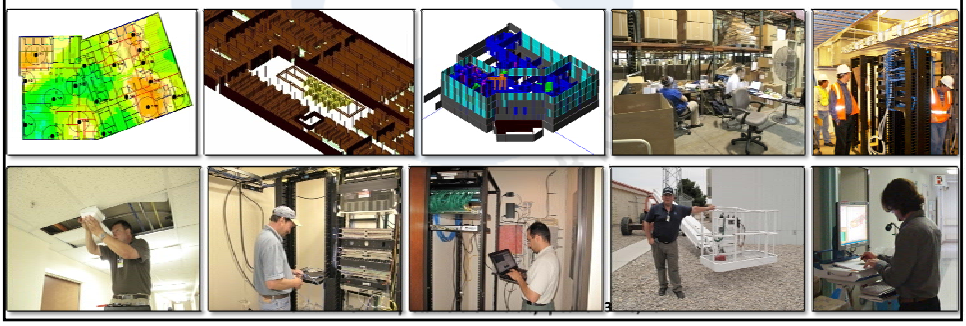
Connect802
follow us on
twitter

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

Connect802
Wireless Data Solutions

www.Connect802.com

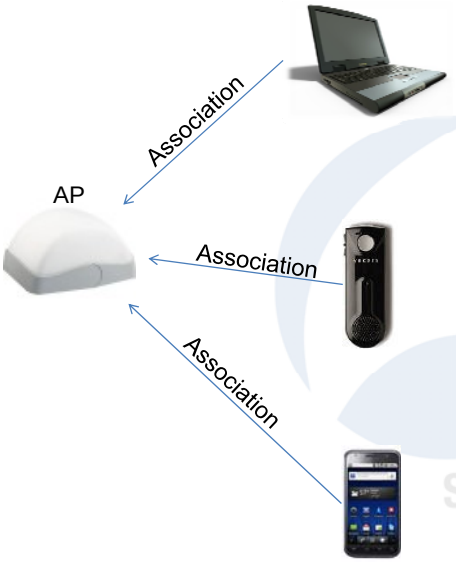


Overview

- 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

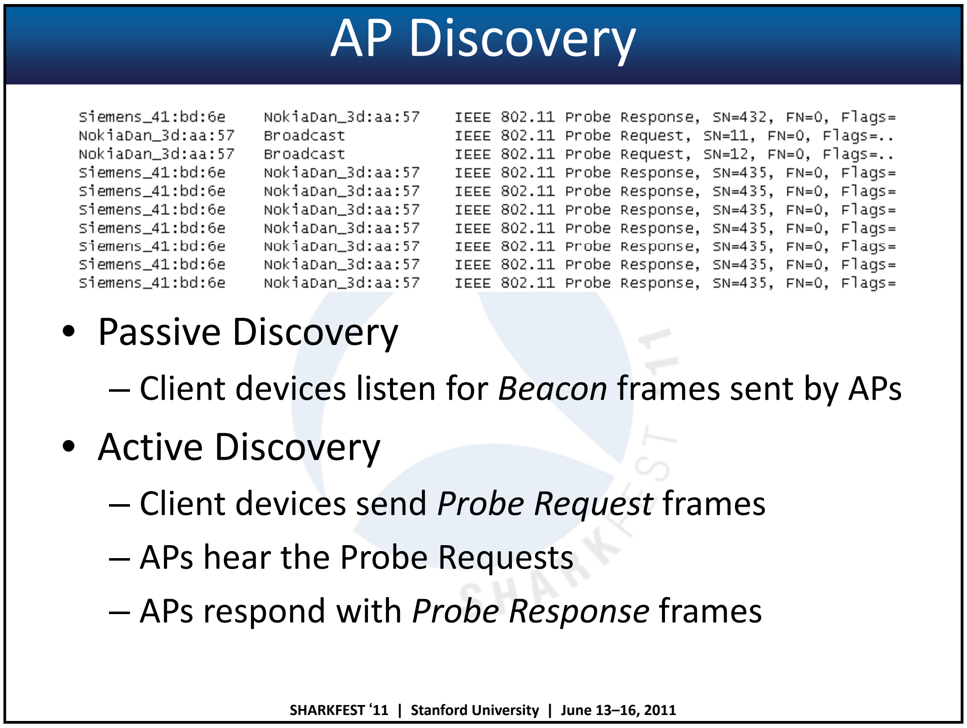
SHARKFEST '11 | Stanford University | June 13–16, 2011

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

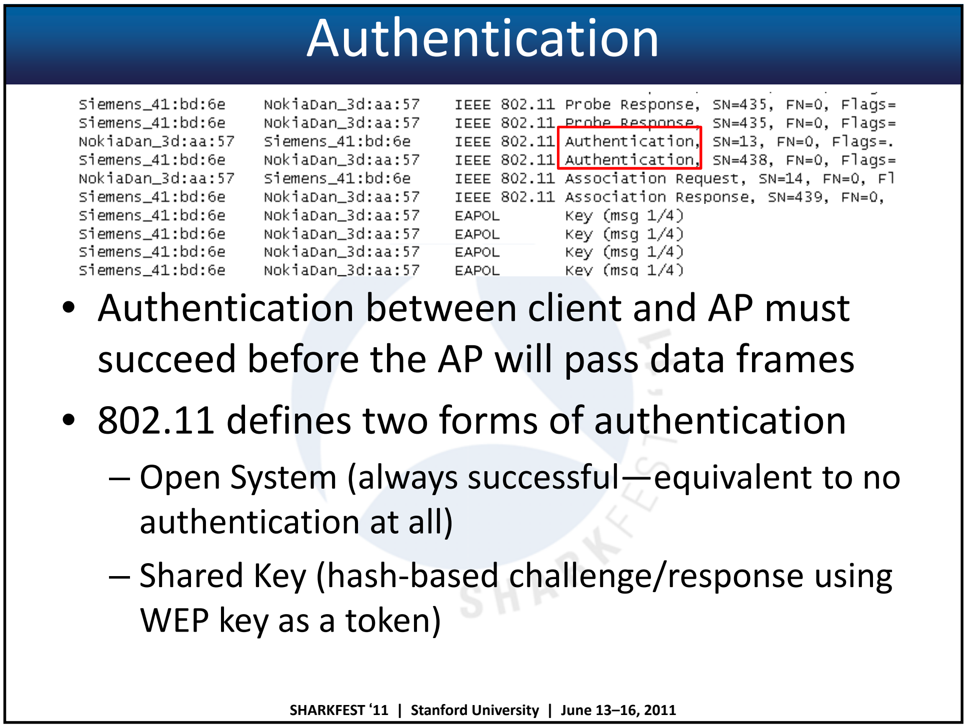
SHARKFEST '11 | Stanford University | June 13–16, 2011



AP Discovery

```
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Probe Response, SN=432, FN=0, Flags=
NokiaDan_3d:aa:57   Broadcast            IEEE 802.11 Probe Request, SN=11, FN=0, Flags=..
NokiaDan_3d:aa:57   Broadcast            IEEE 802.11 Probe Request, SN=12, FN=0, Flags=..
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Probe Response, SN=435, FN=0, Flags=
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Probe Response, SN=435, FN=0, Flags=
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Probe Response, SN=435, FN=0, Flags=
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Probe Response, SN=435, FN=0, Flags=
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Probe Response, SN=435, FN=0, Flags=
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Probe Response, SN=435, FN=0, Flags=
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Probe Response, SN=435, FN=0, Flags=
```

- 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

```
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Probe Response, SN=435, FN=0, Flags=
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Probe Response, SN=435, FN=0, Flags=
NokiaDan_3d:aa:57   Siemens_41:bd:6e     IEEE 802.11 Authentication, SN=13, FN=0, Flags=.
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Authentication, SN=438, FN=0, Flags=
NokiaDan_3d:aa:57   Siemens_41:bd:6e     IEEE 802.11 Association Request, SN=14, FN=0, Fl
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Association Response, SN=439, FN=0,
Siemens_41:bd:6e    NokiaDan_3d:aa:57    EAPOL       Key (msg 1/4)
Siemens_41:bd:6e    NokiaDan_3d:aa:57    EAPOL       Key (msg 1/4)
Siemens_41:bd:6e    NokiaDan_3d:aa:57    EAPOL       Key (msg 1/4)
Siemens_41:bd:6e    NokiaDan_3d:aa:57    EAPOL       Key (msg 1/4)
```

- 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

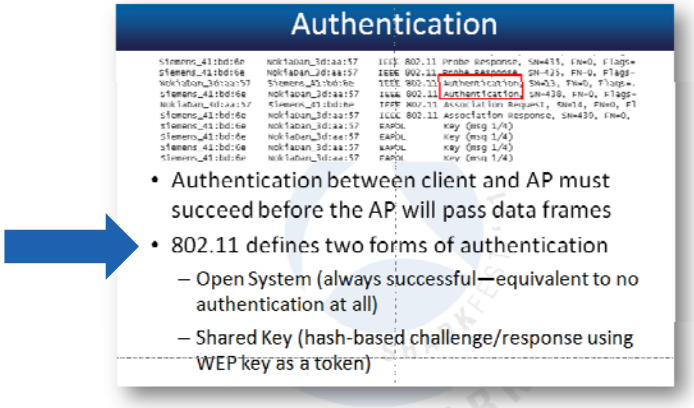
```
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Probe Response, SN=435, FN=0, Flags=
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Probe Response, SN=435, FN=0, Flags=
NokiaDan_3d:aa:57   Siemens_41:bd:6e     IEEE 802.11 Authentication, SN=13, FN=0, Flags=.
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Authentication, SN=438, FN=0, Flags=
NokiaDan_3d:aa:57   Siemens_41:bd:6e     IEEE 802.11 Association Request, SN=14, FN=0, Fl
Siemens_41:bd:6e    NokiaDan_3d:aa:57    IEEE 802.11 Association Response, SN=439, FN=0,
Siemens_41:bd:6e    NokiaDan_3d:aa:57    EAPOL       Key (msg 1/4)
Siemens_41:bd:6e    NokiaDan_3d:aa:57    EAPOL       Key (msg 1/4)
Siemens_41:bd:6e    NokiaDan_3d:aa:57    EAPOL       Key (msg 1/4)
Siemens_41:bd:6e    NokiaDan_3d:aa:57    EAPOL       Key (msg 1/4)
```

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

SHARKFEST '11 | Stanford University | June 13–16, 2011

A Conundrum

- Previously, we said that:

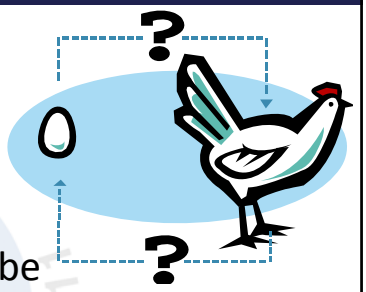


- What about 802.1x (WPA)?

SHARKFEST '11 | Stanford University | June 13–16, 2011

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!



SHARKFEST '11 | Stanford University | June 13–16, 2011

802.1x (WPA) Authentication

Siemens_41:bd:6e	NokiaDan_3d:aa:57	IEEE 802.11	Probe Response, SN=435, FN=0, Flags=
Siemens_41:bd:6e	NokiaDan_3d:aa:57	IEEE 802.11	Probe Response, SN=435, FN=0, Flags=
NokiaDan_3d:aa:57	Siemens_41:bd:6e	IEEE 802.11	Authentication, SN=13, FN=0, Flags=.
Siemens_41:bd:6e	NokiaDan_3d:aa:57	IEEE 802.11	Authentication, SN=438, FN=0, Flags=
NokiaDan_3d:aa:57	Siemens_41:bd:6e	IEEE 802.11	Association Request, SN=14, FN=0, Fl
Siemens_41:bd:6e	NokiaDan_3d:aa:57	IEEE 802.11	Association Response, SN=439, FN=0,
Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	Key (msg 1/4)
Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	Key (msg 1/4)
Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	Key (msg 1/4)
Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	Key (msg 1/4)

- 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

SHARKFEST '11 | Stanford University | June 13–16, 2011

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

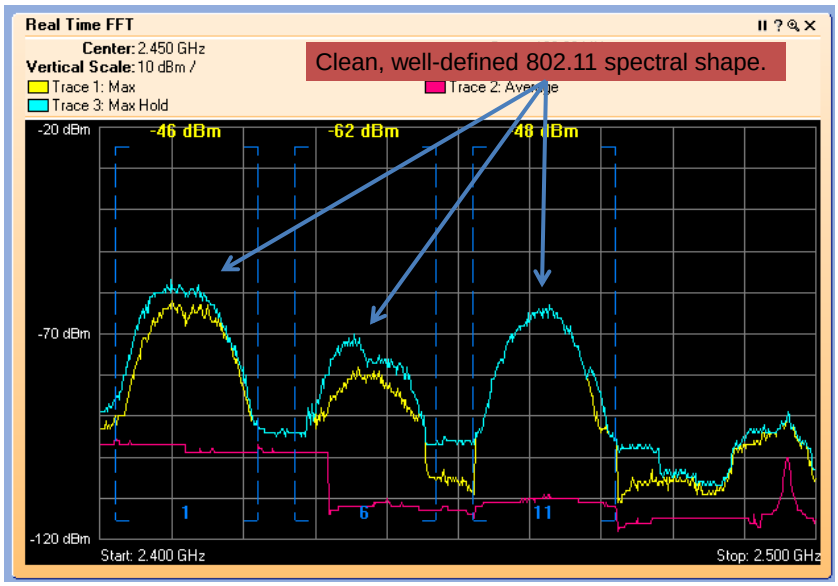
```
Agere_08:12:07      IntelCor_a0:55:c0   IEEE 802.11 Probe Response, SN=2913,
Agere_08:12:07      IntelCor_a0:55:c0   IEEE 802.11 Probe Response, SN=2913,
HewlettP_41:69:e3   Agere_08:09:88      IEEE 802.11 Probe Request, SN=455, FN
Agere_08:09:88      HewlettP_41:69:e3   IEEE 802.11 Probe Response, SN=882, F
HewlettP_41:69:e3   Agere_08:09:88      IEEE 802.11 Authentication, SN=456, F
Agere_08:09:88      HewlettP_41:69:e3   IEEE 802.11 Authentication, SN=883, F
HewlettP_41:69:e3   Agere_08:09:88      IEEE 802.11 Reassociation Request, SN
Agere_08:09:88      HewlettP_41:69:e3   IEEE 802.11 Reassociation Response, S
```

- 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

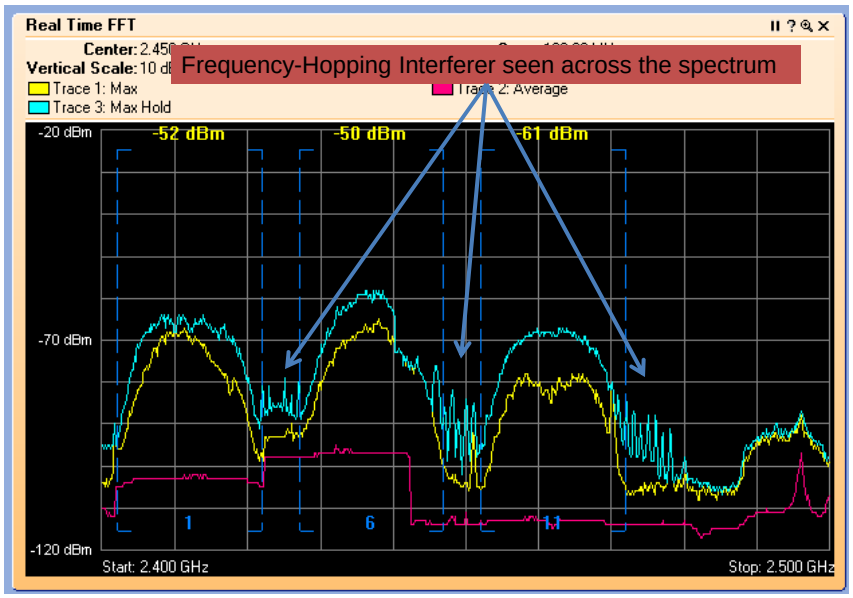
- Customer reported that client devices would go offline periodically
- Incidents were not localized to any particular time or place
- Survey of the environment with spectrum analyzer showed excellent signal strength an no interference (always check for this!)

Clean Spectrum



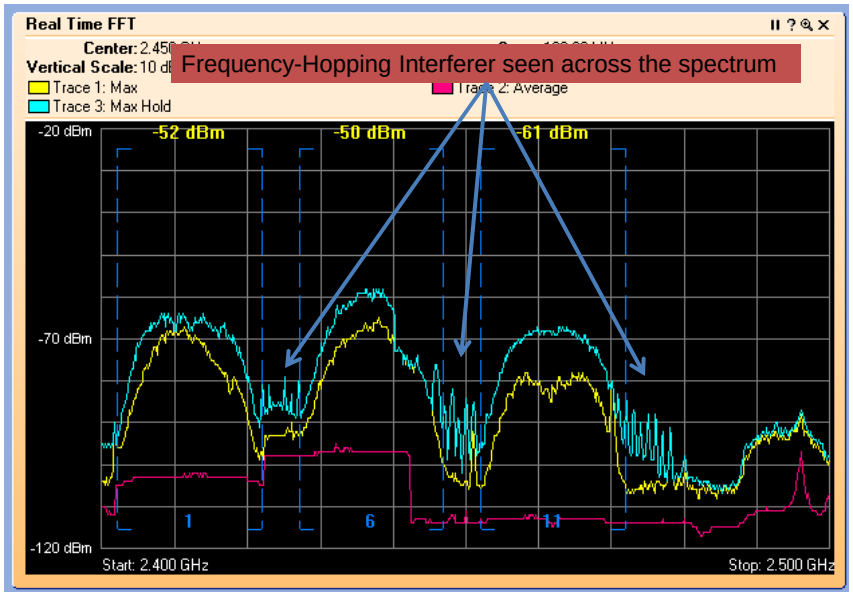
SHARKFEST '11 | Stanford University | June 13–16, 2011

"Dirty" Spectrum (FHSS)



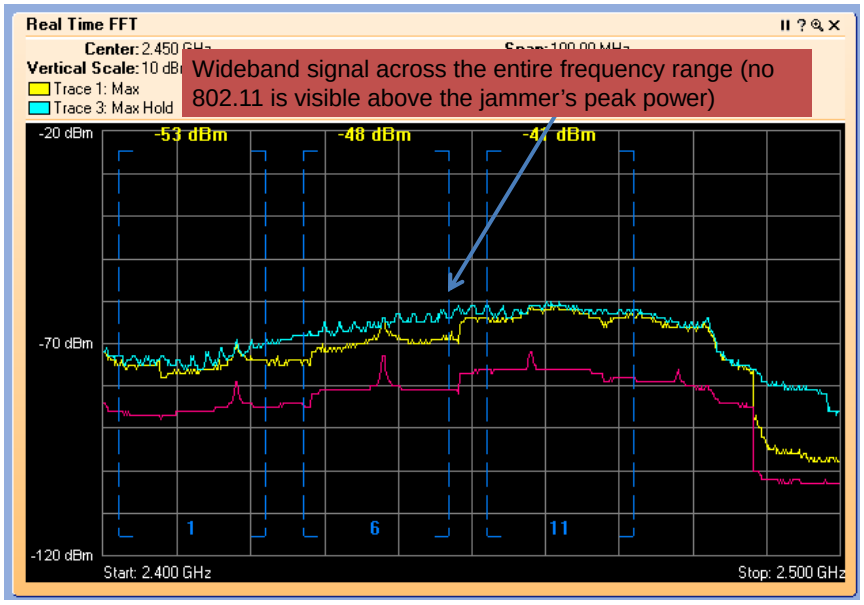
SHARKFEST '11 | Stanford University | June 13–16, 2011

"Dirty" Spectrum (FHSS)



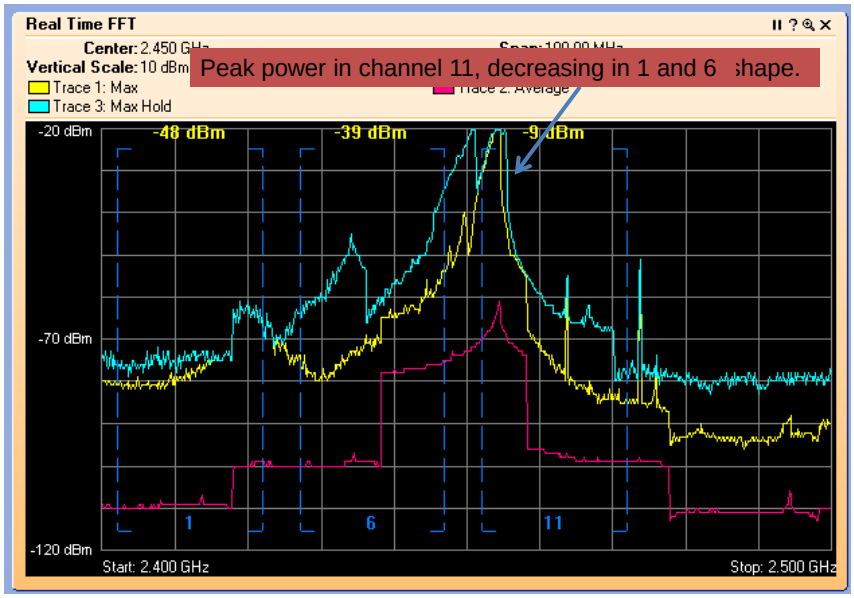
SHARKFEST '11 | Stanford University | June 13–16, 2011

"Dirty" Spectrum (Jammer)



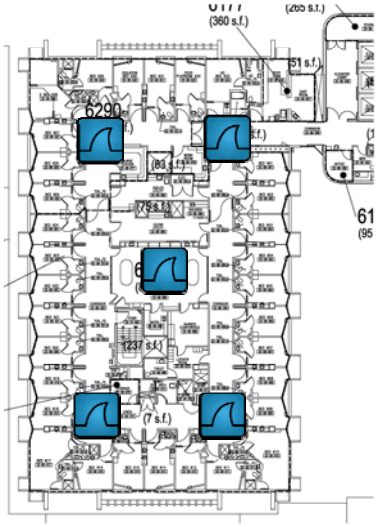
SHARKFEST '11 | Stanford University | June 13–16, 2011

"Dirty" Spectrum (Microwave)



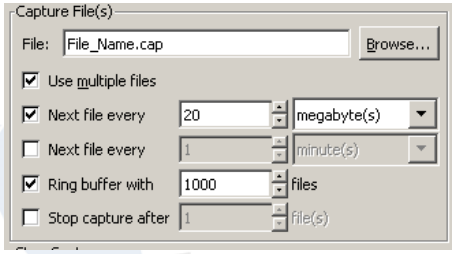
A Distributed Problem

- 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



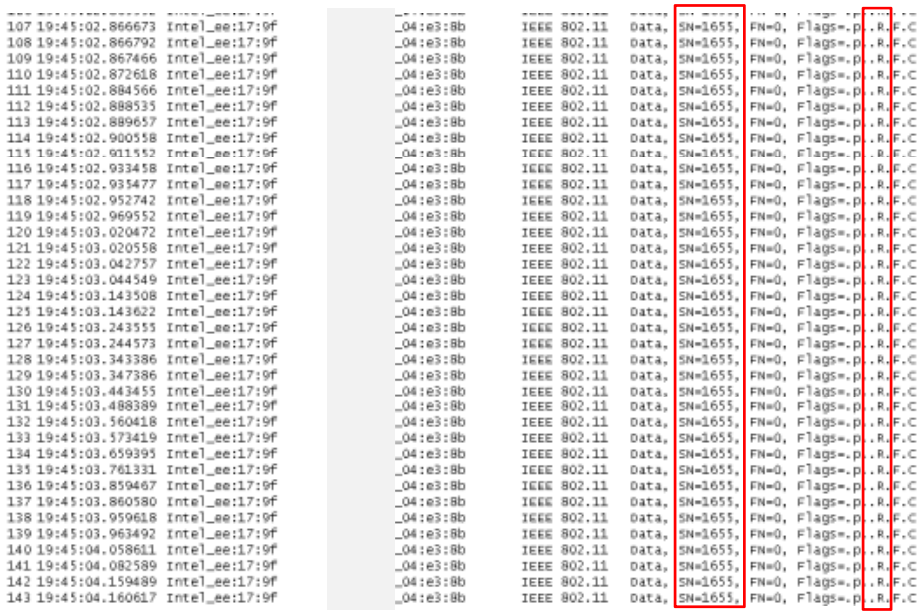
Long-Term Capturing

- 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



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

What We Found: Retries



107	19:45:02.866673	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
108	19:45:02.866792	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
109	19:45:02.867466	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
110	19:45:02.872618	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
111	19:45:02.884566	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
112	19:45:02.888535	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
113	19:45:02.889657	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
114	19:45:02.900558	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
115	19:45:02.911552	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
116	19:45:02.933458	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
117	19:45:02.935477	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
118	19:45:02.952742	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
119	19:45:02.969552	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
120	19:45:03.020472	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
121	19:45:03.020558	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
122	19:45:03.042757	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
123	19:45:03.044549	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
124	19:45:03.143508	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
125	19:45:03.143622	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
126	19:45:03.243555	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
127	19:45:03.244573	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
128	19:45:03.343386	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
129	19:45:03.347386	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
130	19:45:03.443455	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
131	19:45:03.488389	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
132	19:45:03.560418	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
133	19:45:03.573419	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
134	19:45:03.659395	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
135	19:45:03.761331	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
136	19:45:03.859467	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
137	19:45:03.860580	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
138	19:45:03.959618	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
139	19:45:03.963492	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
140	19:45:04.058611	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
141	19:45:04.082589	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
142	19:45:04.159489	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C
143	19:45:04.160617	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data,	SN=1655,	FN=0,	Flags=.p	.R.	F.C

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

```
135 19:45:03.761331 Intel_ee:17:9f   _04:e3:8b   IEEE 802.11  Data, SN=1655, FN=0, Flags=.p..R.F.C
136 19:45:03.859467 Intel_ee:17:9f   _04:e3:8b   IEEE 802.11  Data, SN=1655, FN=0, Flags=.p..R.F.C
137 19:45:03.860580 Intel_ee:17:9f   _04:e3:8b   IEEE 802.11  Data, SN=1655, FN=0, Flags=.p..R.F.C
138 19:45:03.959618 Intel_ee:17:9f   _04:e3:8b   IEEE 802.11  Data, SN=1655, FN=0, Flags=.p..R.F.C
139 19:45:03.963492 Intel_ee:17:9f   _04:e3:8b   IEEE 802.11  Data, SN=1655, FN=0, Flags=.p..R.F.C
140 19:45:04.058611 Intel_ee:17:9f   _04:e3:8b   IEEE 802.11  Data, SN=1655, FN=0, Flags=.p..R.F.C
141 19:45:04.082589 Intel_ee:17:9f   _04:e3:8b   IEEE 802.11  Data, SN=1655, FN=0, Flags=.p..R.F.C
142 19:45:04.159489 Intel_ee:17:9f   _04:e3:8b   IEEE 802.11  Data, SN=1655, FN=0, Flags=.p..R.F.C
143 19:45:04.160617 Intel_ee:17:9f   _04:e3:8b   IEEE 802.11  Data, SN=1655, FN=0, Flags=.p..R.F.C
```

SHARKFEST '11 | Stanford University | June 13–16, 2011

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!

```
/* Declarations of MIB attributes exported from
   this process */

      /* Read-Write attributes */
dcl exported
  dot11AuthenticationAlgorithms  AuthTypeSet:=
    incl(open_system, shared_key),
  dot11ExcludeUnencrypted  Boolean:= false,
  dot11FragmentationThreshold  Integer:= 2346,
  dot11GroupAddresses  MacAddrSet:= empty,
  dot11LongRetryLimit  Integer:= 4,
  dot11MaxReceiveLifetime  Kusec:= 512,
  dot11MaxTransmitMsduLifetime  Kusec:= 512,
  dot11MediumOccupancyLimit  Kusec:= 100,
  dot11PrivacyInvoked  Boolean:= false,
  mReceiveDTIMs  Boolean:= true,
  dot11CfpPeriod  Integer:= 1,
  dot11CfpMaxDuration  Kusec:= 200,
  dot11AuthenticationResponseTimeout  Kusec:= 512,
  dot11RtsThreshold  Integer:= 3000,
  dot11ShortRetryLimit  Integer:= 7,
  dot11WepDefaultKeyId  KeyIndex:= 0,
  dot11CurrentChannelNumber  Integer:= 0,
  dot11CurrentSet  Integer:= 0,
  dot11CurrentPattern  Integer:= 0,
  dot11CurrentIndex  Integer:= 0 ;

      /* Write-Only attributes */
dcl exported
  dot11WepDefaultKeys  KeyVector:= nullKey,
  dot11WepKeyMappings
    KeyMapArray:= (. nullAddr, false, nullKey .) ;
```

SHARKFEST '11 | Stanford University | June 13–16, 2011

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)

```
Data rate (Mb/s)  Info
36.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
36.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
36.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
12.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
12.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
11.000000   Data, SN=1655, FN=0, Flags=.p..R.F.C
```

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 <u>not</u> the STA in question
- Orange line indicates the anomalous event
- Does anything seem to change before/after?

SHARKFEST '11 | Stanford University | June 13–16, 2011

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)

SHARKFEST '11 | Stanford University | June 13–16, 2011

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

255	19:45:08.426549	Intel_ee:17:9f	[illegible]	IEEE 802.11	Data, SN=1966, FN=0, Flags=.p..R.F.C
256	19:45:08.427549	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data, SN=1966, FN=0, Flags=.p..R.F.C
257	19:45:08.444631	_04:e3:8b	Broadcast	IEEE 802.11	Probe Request, SN=1, FN=0, Flags=....
258	19:45:08.445561	Cisco_36:35:d4	_04:e3:8b	IEEE 802.11	Probe Response, SN=1119, FN=0, Flags=
259	19:45:08.509492	_04:e3:8b	Broadcast	IEEE 802.11	Probe Request, SN=2, FN=0, Flags=....
260	19:45:08.509497	Cisco_36:26:24	_04:e3:8b	IEEE 802.11	Probe Response, SN=3972, FN=0, Flags=
261	19:45:08.510521	Cisco_36:37:04	_04:e3:8b	IEEE 802.11	Probe Response, SN=3037, FN=0, Flags=
262	19:45:08.530478	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data, SN=1966, FN=0, Flags=.p..R.F.C
263	19:45:08.530483	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data, SN=1966, FN=0, Flags=.p..R.F.C
264	19:45:08.573555	_04:e3:8b	Broadcast	IEEE 802.11	Probe Request, SN=3, FN=0, Flags=....
265	19:45:08.644854	_04:e3:8b	Cisco_36:28:84	IEEE 802.11	Authentication, SN=4, FN=0, Flags=...
266	19:45:08.644965		_04:e3:8b (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
267	19:45:08.644992	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data, SN=1966, FN=0, Flags=.p..R.F.C
268	19:45:08.645034	Cisco_36:28:84	_04:e3:8b	IEEE 802.11	Authentication, SN=165, FN=0, Flags=.
269	19:45:08.646804	_04:e3:8b	Cisco_36:28:84	IEEE 802.11	Association Request, SN=5, FN=0, Flag
270	19:45:08.646831		DraegerM_04:e3:8b (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
271	19:45:08.647675	Intel_ee:17:9f	DraegerM_04:e3:8b	IEEE 802.11	Data, SN=1966, FN=0, Flags=.p..R.F.C
272	19:45:08.654730	Cisco_36:28:84	DraegerM_04:e3:8b	EAPOL	Key (msg 1/4)

"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!

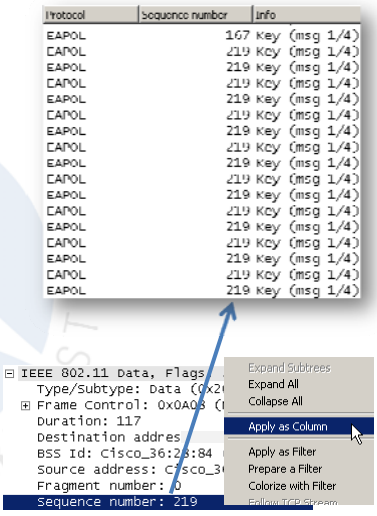
What We Found: More Retries!

- The Association is interrupted during WPA authentication

256	19:45:08.427549	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data, SN=1966, FN=0, Flags=.p..R.F.C
257	19:45:08.444631	_ _04:e3:8b	Broadcast	IEEE 802.11	Probe Request, SN=1, FN=0, Flags=....
258	19:45:08.445561	Cisco_36:35:d4	_ _04:e3:8b	IEEE 802.11	Probe Response, SN=1159, FN=0, Flags=
259	19:45:08.509492	_ _04:e3:8b	Broadcast	IEEE 802.11	Probe Request, SN=2, FN=0, Flags=....
260	19:45:08.509497	Cisco_36:26:24	_04:e3:8b	IEEE 802.11	Probe Response, SN=3972, FN=0, Flags=
261	19:45:08.510521	Cisco_36:37:04	_04:e3:8b	IEEE 802.11	Probe Response, SN=3037, FN=0, Flags=
262	19:45:08.530478	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data, SN=1966, FN=0, Flags=.p..R.F.C
263	19:45:08.530483	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data, SN=1966, FN=0, Flags=.p..R.F.C
264	19:45:08.573555	_04:e3:8b	Broadcast	IEEE 802.11	Probe Request, SN=3, FN=0, Flags=....
265	19:45:08.644854	_04:e3:8b	Cisco_36:28:84	IEEE 802.11	Authentication, SN=4, FN=0, Flags=...
266	19:45:08.644965		_04:e3:8b (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
267	19:45:08.644992	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data, SN=1966, FN=0, Flags=.p..R.F.C
268	19:45:08.645034	Cisco_36:28:84	_04:e3:8b	IEEE 802.11	Authentication, SN=165, FN=0, Flags=.
269	19:45:08.646804	_04:e3:8b	Cisco_36:28:84	IEEE 802.11	Association Request, SN=5, FN=0, Flag
270	19:45:08.646831		_04:e3:8b (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
271	19:45:08.647675	Intel_ee:17:9f	_04:e3:8b	IEEE 802.11	Data, SN=1966, FN=0, Flags=.p..R.F.C
272	19:45:08.654730	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)
272	19:45:08.654730	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)
273	19:45:09.521585	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)
274	19:45:09.522627	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)
275	19:45:09.523626	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)
276	19:45:09.524625	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)
277	19:45:09.526625	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)
278	19:45:09.528625	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)

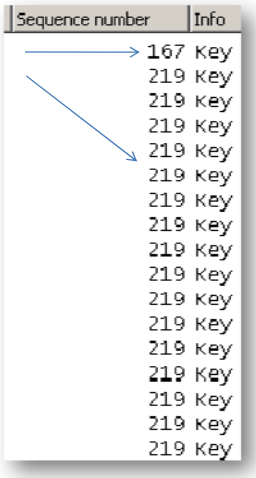
Retry Analysis

- 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

- 1st Packet has SEQ 167
- 2nd and subsequent packets have SEQ 219
- 1st 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 <u>with</u> 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

```
[TCP Retransmission] ismaeasdaqtest > 43120 [PSH, ACK] Seq=1 Ack
[TCP Dup ACK 182#1] 43120 > ismaeasdaqtest [ACK] Seq=5 Ack=5921
biimenu > 30019 [ACK] Seq=1 Ack=2481 Win=65535 Len=0
[TCP Retransmission] ismaeasdaqtest > 43120 [PSH, ACK] Seq=1461
[TCP Dup ACK 182#2] 43120 > ismaeasdaqtest [ACK] Seq=5 Ack=5921
Who is 00:30:e6:04:28:ad?  Tell 00:30:e6:04:28:ad
```

SHARKFEST '11 | Stanford University | June 13–16, 2011

Retry Analysis

- This same process can be applied going up the layers of the OSI model
  - TCP retransmissions <u>without</u> 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

SHARKFEST '11 | Stanford University | June 13–16, 2011

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

320	19:45:11.168640	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)
321	19:45:11.269643	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)
322	19:45:11.270642	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)
323	19:45:11.368691	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)
324	19:45:11.373646	Cisco_36:28:84	_04:e3:8b	LLC	U, func=UI; DSAP 0xd0 Individual, SSAP 0x5a Res
325	19:45:11.450735	Cisco_36:28:84	_04:e3:8b	IEEE 802.11	Deauthentication, SN=335, FN=0, Flags=....R...C
326	19:45:11.450742	Cisco_36:28:84	_04:e3:8b	IEEE 802.11	Deauthentication, SN=335, FN=0, Flags=....R...C
327	19:45:11.451931	Cisco_36:28:84	_04:e3:8b	IEEE 802.11	Deauthentication, SN=335, FN=0, Flags=....R...C
328	19:45:12.603874	_04:e3:8b	Broadcast	IEEE 802.11	Probe Request, SN=1, FN=0, Flags=.....C, SSI
329	19:45:12.604868	Cisco_36:28:84	_04:e3:8b	IEEE 802.11	Probe Response, SN=3072, FN=0, Flags=....R...C,
330	19:45:12.606893	Cisco_36:28:84	_04:e3:8b	IEEE 802.11	Probe Response, SN=3072, FN=0, Flags=....R...C,
331	19:45:12.667964	_04:e3:8b	Broadcast	IEEE 802.11	Probe Request, SN=2, FN=0, Flags=.....C, SSI
332	19:45:12.668792	Cisco_36:26:24	_04:e3:8b	IEEE 802.11	Probe Response, SN=3980, FN=0, Flags=....R...C,
333	19:45:12.670787	Cisco_36:33:b4	_04:e3:8b	IEEE 802.11	Probe Response, SN=897, FN=10, Flags=....R.....,
334	19:45:12.671945	Cisco_89:98:d4	_04:e3:8b	IEEE 802.11	Probe Response, SN=1087, FN=0, Flags=....R...C,
335	19:45:12.672855	Cisco_36:26:24	_04:e3:8b	IEEE 802.11	Probe Response, SN=3980, FN=0, Flags=....R...C,
336	19:45:12.677798	Cisco_36:37:04	_04:e3:8b	IEEE 802.11	Probe Response, SN=3047, FN=0, Flags=....R...C,
337	19:45:12.733010	_04:e3:8b	Broadcast	IEEE 802.11	Probe Request, SN=3, FN=0, Flags=.....C, SSI
338	19:45:12.733843	Cisco_36:36:64	_04:e3:8b	IEEE 802.11	Probe Response, SN=800, FN=9, Flags=....R.....,
339	19:45:12.735870	C0:eb:2e:d9:17:f5	_04:e3:8b	IEEE 802.11	Probe Response, SN=2386, FN=1, Flags=....R.....,
340	19:45:12.803868	_04:e3:8b	Cisco_36:28:84	IEEE 802.11	Authentication, SN=4, FN=0, Flags=.....C
341	19:45:12.803904		_04:e3:8b (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
342	19:45:12.804880	Cisco_36:28:84	_04:e3:8b	IEEE 802.11	Authentication, SN=422, FN=0, Flags=.....C
343	19:45:12.806041	_04:e3:8b	Cisco_36:28:84	IEEE 802.11	Association Request, SN=5, FN=0, Flags=.....
344	19:45:12.806067		_04:e3:8b (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
345	19:45:12.807846	Cisco_36:28:84	_04:e3:8b	IEEE 802.11	Association Response, SN=423, FN=0, Flags=.....
346	19:45:12.812988	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)
347	19:45:13.351778	_04:e3:8b	Cisco_36:28:84	EAPOL	Start
348	19:45:13.723853	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 1/4)
349	19:45:13.729909	Cisco_36:28:84	_04:e3:8b	EAPOL	Key (msg 3/4)
350	19:45:13.733924	_04:e3:8b	Cisco_36:28:84	EAPOL	Key (msg 4/4)
351	19:45:13.744936	_04:e3:8b	Intel_ee:17:9f	IEEE 802.11	Data, SN=9, FN=0, Flags=.p.....TC
352	19:45:13.746094	_04:e3:8b	Broadcast	IEEE 802.11	Data, SN=10, FN=0, Flags=.p.....TC
353	19:45:13.817945	_04:e3:8b	Cisco_36:28:84	IEEE 802.11	Null function (No data), SN=11, FN=0, Flags=...
354	19:45:14.036007	_04:e3:8b	Broadcast	IEEE 802.11	Data, SN=12, FN=0, Flags=.p.P...TC

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.

```
EAPOL        Key (msg 1/4)
EAPOL        Key (msg 1/4)
EAPOL        Key (msg 1/4)
EAPOL        Key (msg 1/4)
LLC          U, func=UI; DSAP 0xd0 Individual, SSAP 0x5a Res
IEEE 802.11  Deauthentication, SN=335, FN=0, Flags=....R...C
IEEE 802.11  Deauthentication, SN=335, FN=0, Flags=....R...C
IEEE 802.11  Deauthentication, SN=335, FN=0, Flags=....R...C
IEEE 802.11  Probe Request, SN=1, FN=0, Flags=........C, SSI
IEEE 802.11  Probe Response, SN=3072, FN=0, Flags=....R...C,
IEEE 802.11  Probe Response, SN=3072, FN=0, Flags=....R...C,
IEEE 802.11  Probe Request, SN=2, FN=0, Flags=........C, SSI
IEEE 802.11  Probe Response, SN=3980, FN=0, Flags=....R...C,
IEEE 802.11  Probe Response, SN=897, FN=10, Flags=....R....,
IEEE 802.11  Probe Response, SN=1087, FN=0, Flags=....R...C,
IEEE 802.11  Probe Response, SN=3980, FN=0, Flags=....R...C,
IEEE 802.11  Probe Response, SN=3047, FN=0, Flags=....R...C,
IEEE 802.11  Probe Request, SN=3, FN=0, Flags=........C, SSI
IEEE 802.11  Probe Response, SN=800, FN=9, Flags=....R....,
IEEE 802.11  Probe Response, SN=2386, FN=1, Flags=....R....,
IEEE 802.11  Authentication, SN=4, FN=0, Flags=........C
IEEE 802.11  Acknowledgement, Flags=........C
IEEE 802.11  Authentication, SN=422, FN=0, Flags=........C
IEEE 802.11  Association Request, SN=5, FN=0, Flags=........
IEEE 802.11  Acknowledgement, Flags=........C
IEEE 802.11  Association Response, SN=423, FN=0, Flags=.....
EAPOL        Key (msg 1/4)
EAPOL        Start
EAPOL        Key (msg 1/4)
EAPOL        Key (msg 3/4)
EAPOL        Key (msg 4/4)
IEEE 802.11  Data, SN=9, FN=0, Flags=.p.....TC
IEEE 802.11  Data, SN=10, FN=0, Flags=.p.....TC
IEEE 802.11  Null function (No data), SN=11, FN=0, Flags=...
IEEE 802.11  Data, SN=12, FN=0, Flags=.p.P...TC
```


… 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?

370	19:45:14.829101		_04:e3:8b	Cisco_36:28:84	IEEE 802.11	Disassociate, SN=16, FN=0, Flags=...P....C
371	19:45:14.829127			_04:e3:8b (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
372	19:45:14.916860		_04:e3:8b	Broadcast	IEEE 802.11	Probe Request, SN=17, FN=0, Flags=.....C, SS
373	19:45:14.917828	Cisco_36:35:14		_04:e3:8b	IEEE 802.11	Probe Response, SN=1169, FN=0, Flags=o.m...F..,
374	19:45:14.918833	Cisco_36:35:d4		_04:e3:8b	IEEE 802.11	Probe Response, SN=1169, FN=0, Flags=....R....
375	19:45:14.974843		_04:e3:8b	Broadcast	IEEE 802.11	Probe Request, SN=18, FN=0, Flags=.....C, SS
376	19:45:14.974851	Cisco_36:26:24		_04:e3:8b	IEEE 802.11	Probe Response, SN=3983, FN=0, Flags=....R...C,
377	19:45:14.975915	Cisco_2f:15:b5		_04:e3:8b	IEEE 802.11	Probe Response, SN=919, FN=0, Flags=....R....
378	19:45:14.975924	Cisco_89:98:d4		_04:e3:8b	IEEE 802.11	Probe Response, SN=1090, FN=0, Flags=....R...C,
379	19:45:14.977850	Cisco_36:37:04		_04:e3:8b	IEEE 802.11	Probe Response, SN=3048, FN=0, Flags=....R...C,
380	19:45:15.030850		_04:e3:8b	Broadcast	IEEE 802.11	Probe Request, SN=19, FN=0, Flags=.....C, SS
381	19:45:15.032846	Cisco_36:36:64		_04:e3:8b	IEEE 802.11	Probe Response, SN=1599, FN=0, Flags=....R...C,
382	19:45:15.101999		_04:e3:8b	Cisco_36:26:24	IEEE 802.11	Authentication, SN=20, FN=0, Flags=.....C
383	19:45:15.102078			_04:e3:8b (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
384	19:45:15.102120	Cisco_36:26:24		_04:e3:8b	IEEE 802.11	Authentication, SN=2404, FN=0, Flags=.....C
385	19:45:15.104003		_04:e3:8b	Cisco_36:26:24	IEEE 802.11	Association Request, SN=21, FN=0, Flags=.....
386	19:45:15.104030			_04:e3:8b (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
387	19:45:15.105895	Cisco_36:26:24		_04:e3:8b	IEEE 802.11	Association Response, SN=2405, FN=0, Flags=....
388	19:45:15.111900	Cisco_36:26:24		_04:e3:8b	EAPOL	Key (msg 1/4)
389	19:45:15.651780		_04:e3:8b	Cisco_36:26:24	EAPOL	Start
390	19:45:15.652759			_04:e3:8b (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
391	19:45:16.015966	Cisco_36:26:24		_04:e3:8b	EAPOL	Key (msg 1/4)
392	19:45:16.021046		_04:e3:8b	Cisco_36:26:24	EAPOL	Key (msg 2/4)
393	19:45:16.021900	Cisco_36:26:24		_04:e3:8b	EAPOL	Key (msg 3/4)
394	19:45:16.024888		_04:e3:8b	Cisco_36:26:24	EAPOL	Key (msg 4/4)
395	19:45:16.024896			_04:e3:8b (RA)	IEEE 802.11	Acknowledgement, Flags=.....C

What We Found: Disassociate

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.

```
Disassociate, SN=16, FN=0, Flags=...P....C
Acknowledgement, Flags=.....C
Probe Request, SN=17, FN=0, Flags=.....C, SS
Probe Response, SN=1169, FN=0, Flags=o.m...F..,
Probe Response, SN=1169, FN=0, Flags=....R....,
Probe Request, SN=18, FN=0, Flags=.....C, SS
Probe Response, SN=3983, FN=0, Flags=....R...C,
Probe Response, SN=919, FN=0, Flags=....R....,
Probe Response, SN=1090, FN=0, Flags=....R...C,
Probe Response, SN=3048, FN=0, Flags=....R...C,
Probe Request, SN=19, FN=0, Flags=.....C, SS
Probe Response, SN=1599, FN=0, Flags=....R...C,
Authentication, SN=20, FN=0, Flags=.....C
Acknowledgement, Flags=.....C
Authentication, SN=2404, FN=0, Flags=.....C
Association Request, SN=21, FN=0, Flags=.....
Acknowledgement, Flags=.....C
Association Response, SN=2405, FN=0, Flags=....
Key (msg 1/4)
Start
Acknowledgement, Flags=.....C
Key (msg 1/4)
Key (msg 2/4)
Key (msg 3/4)
Key (msg 4/4)
Acknowledgement, Flags=.....C
```

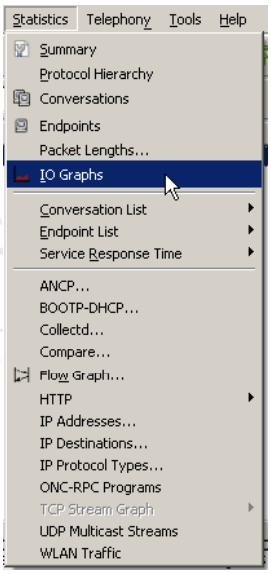
What Do We Know?

- 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?

SHARKFEST '11 | Stanford University | June 13–16, 2011

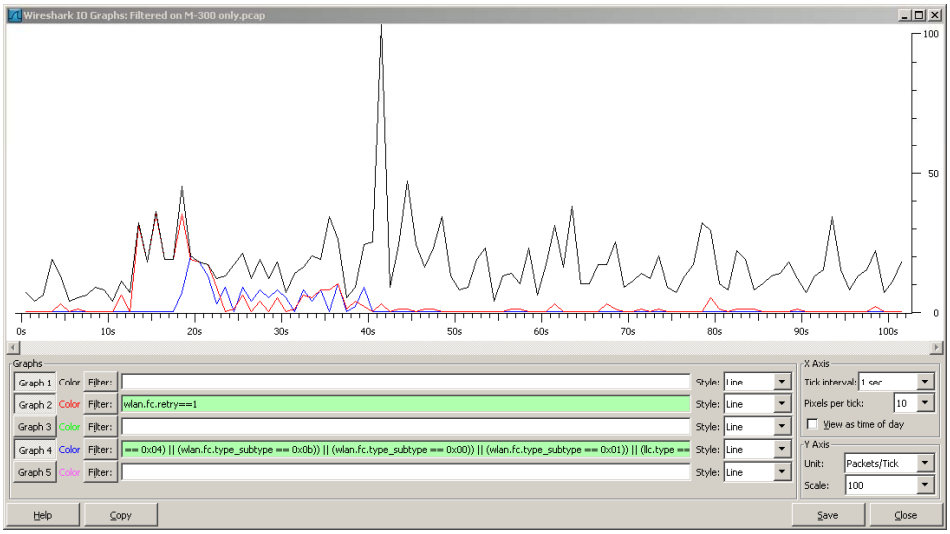
Analysis With I/O Graphs

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

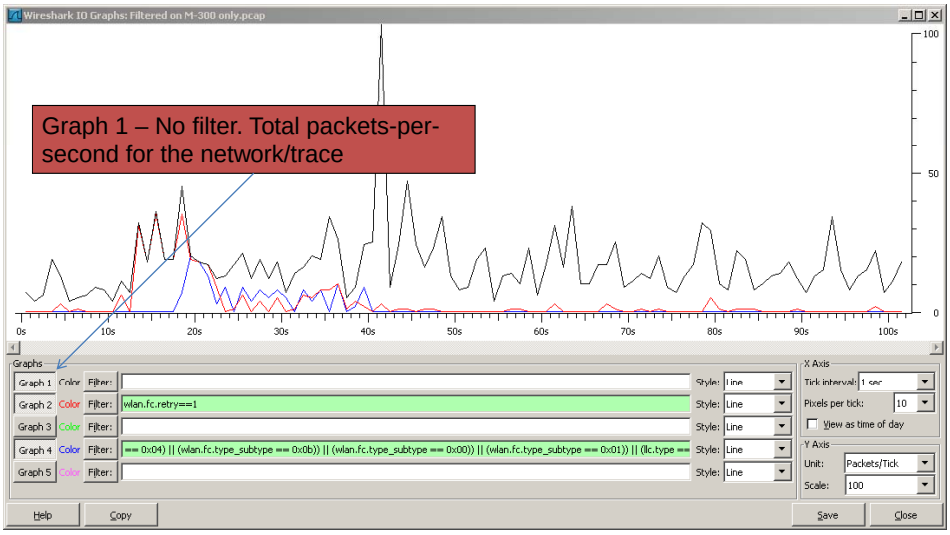


SHARKFEST '11 | Stanford University | June 13–16, 2011

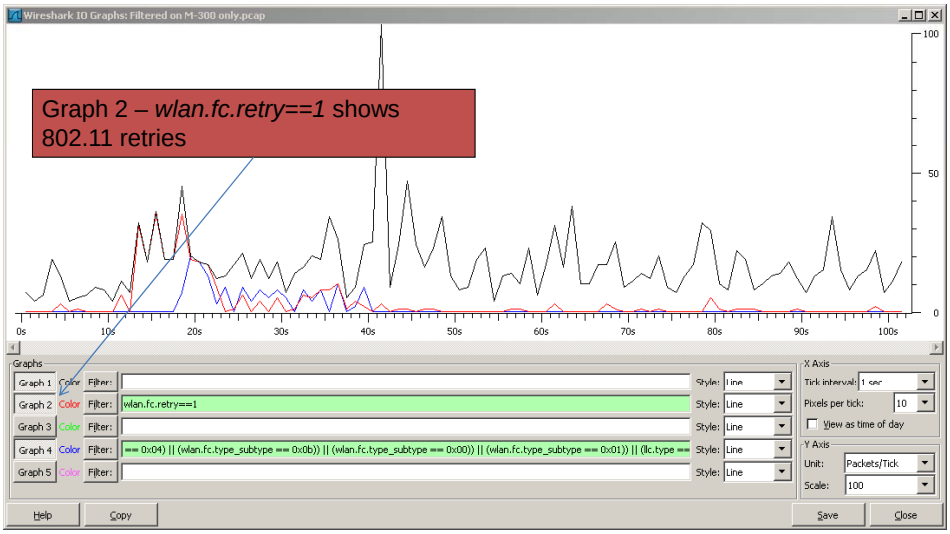
Analysis With I/O Graphs



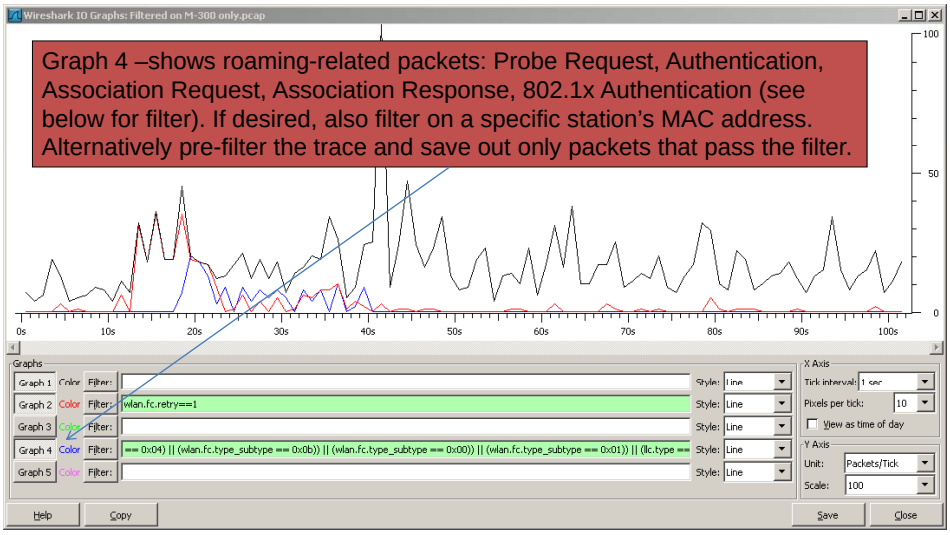
Analysis With I/O Graphs



Analysis With I/O Graphs

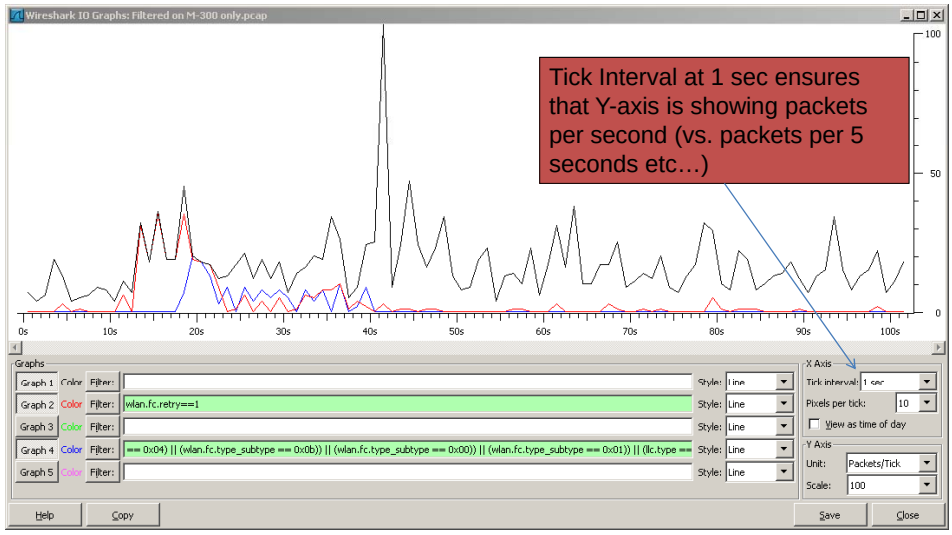


Analysis With I/O Graphs

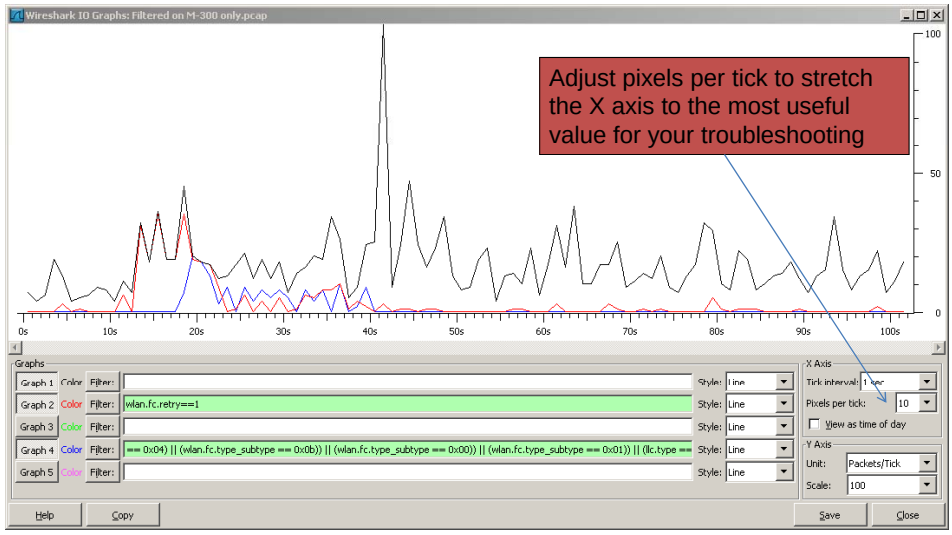


wlan.fc.type_subtype == 0x04 || wlan.fc.type_subtype == 0x0b || wlan.fc.type_subtype == 0x00 || wlan.fc.type_subtype == 0x01 || llc.type == 0x888e

Analysis With I/O Graphs



Analysis With I/O Graphs

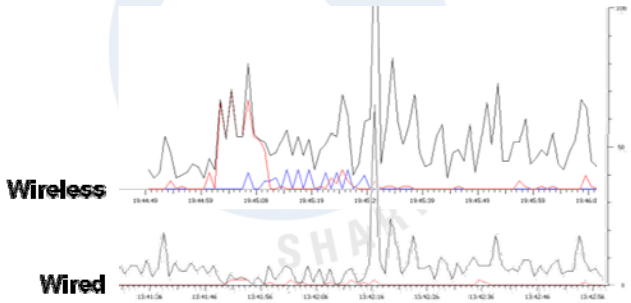


A Visual Guide

SHARKFEST '11 | Stanford University | June 13–16, 2011

Using I/O Graphs To Compare

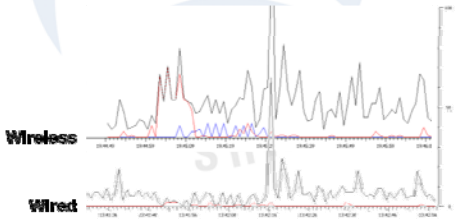
- These two graphs compare the wireless and the wired side of the same conversation
- Red lines indicate retries (wireless) or TCP retransmissions (wired)



SHARKFEST '11 | Stanford University | June 13–16, 2011

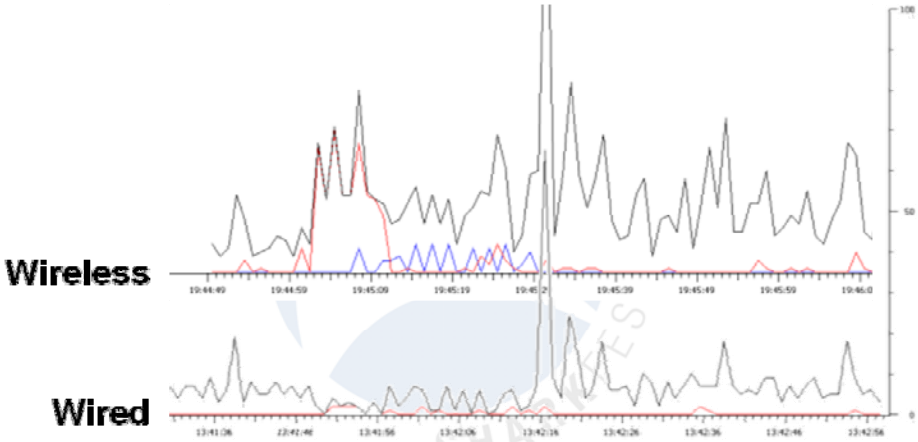
Using I/O Graphs To Compare

- 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)



SHARKFEST '11 | Stanford University | June 13–16, 2011

Using I/O Graphs To Compare



SHARKFEST '11 | Stanford University | June 13–16, 2011

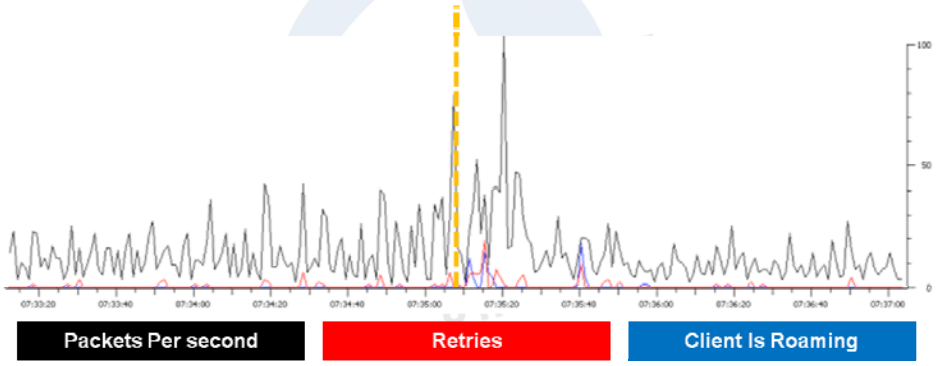
Clock Synchronization

- 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

SHARKFEST '11 | Stanford University | June 13–16, 2011

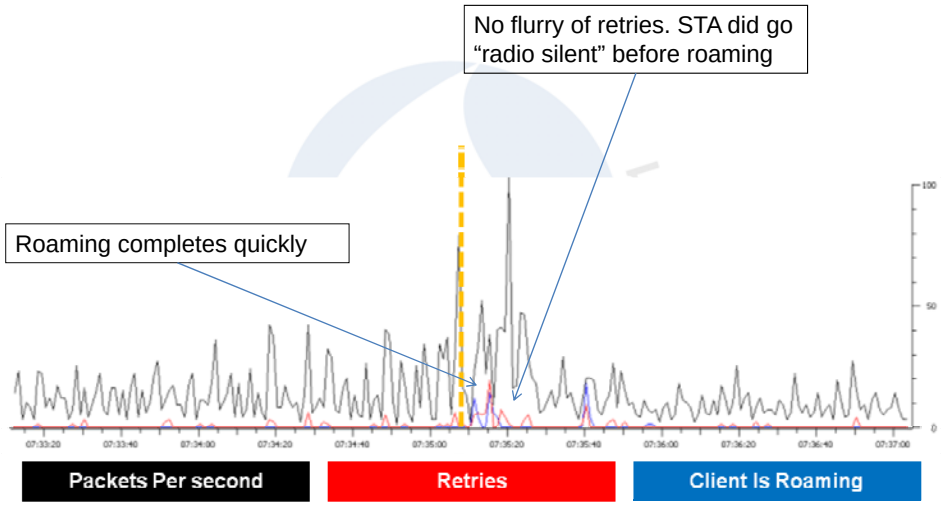
"Normal" Roaming

- Same device, slightly different behavior
- Just based on the graph, how does this compare?



SHARKFEST '11 | Stanford University | June 13–16, 2011

"Normal" Roaming



SHARKFEST '11 | Stanford University | June 13–16, 2011

Conclusion

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

SHARKFEST '11 | Stanford University | June 13–16, 2011

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/
  - TCP/IP Protocols: http://www.ietf.org/rfc.html
  - 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

SHARKFEST '11 | Stanford University | June 13–16, 2011

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!

SHARKFEST '11 | Stanford University | June 13–16, 2011

Thank You!

Joe Bardwell
Connect802 Corporation
San Ramon, CA
(925) 552-0802
joe@Connect802.com

Connect802
Wireless Data Solutions

Connect802
follow us on
twitter

SHARKFEST '11 | Stanford University | June 13–16, 2011