# Why Packets Matter

Capturing Packets and Solving WLAN Issues (Why, How, Where, When)

Jay Botelho Director of Product Management, Savvius jbotelho@savvius.com Follow me @jaybotelho

IT Professional Wi-Fi Trek 2015 #wifitrek





# Packet analysis shouldn't be a last resort. It should be an integral part of any WLAN analysis procedure.



Why?

Certified Wireless Network Professional

IT Professional Wi-Fi Trek 2015 #wifitrek

### Why a Packet Analyzer?

802.11 is the language of Wi-Fi

- 802.11 is a complex protocol strong foundation but many, many layers
- Unlike wired networks, an inefficient physical layer (Layer 1) leads to protocol issues that require packet analysis
- Interpreting 802.11 packets captures requires experience and a good understanding of the 802.11 protocol



### But Don't Just Take It From Me ...

#### What's in Your Wi-Fi Tool Box?

- Spectrum Analyzer
- Protocol Analyzer (packet analyzer or sniffer)
- Site Survey



#### George Stefanick

- In Wi-Fi since early 2000s
- Numerous certifications
- Wireless Architect for a large healthcare system managing 25,000+ Wi-Fi Clients
- Consultant
- Cisco VIP 2012, 2013, 2014
- Aruba MVP 2014
- Blog <u>www.my80211.com</u>

http://www.informationweek.com/interop/whats-in-your-wi-fi-tool-box/d/d-id/1113592



### What Can You Address with a Protocol Analyzer?

- Wi-Fi is not authenticating ....
- Wi-Fi is slow ....
- Wi-Fi is dropping connections ....
- Wi-Fi doesn't work
- Wi-Fi is unreliable ....



### Critical Elements of a Protocol Analyzer

- High fidelity, high-speed packet capture
- Multi-channel analysis
- Long-term packet storage
- Visualization
- Analysis modules
- High-quality decodes

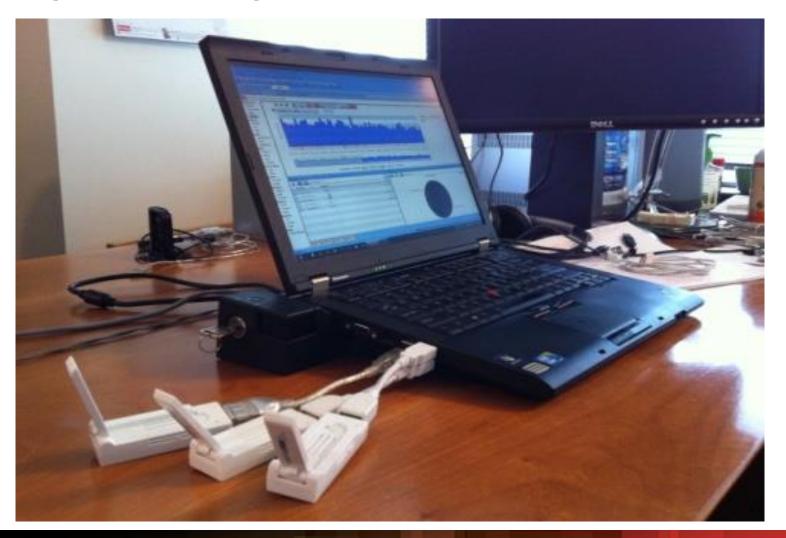


## How? Where?

IT Professional Wi-Fi Trek 2015 #wifitrek



#### Packet Capture Requires a Point-of-Presence

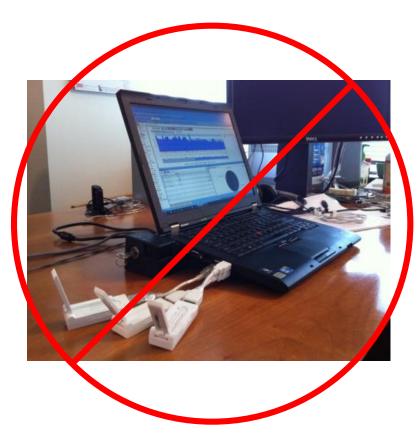




# But Don't Confuse Portable with Point-of-Presence

Portable,

but not the only way, and maybe not the best way, to be "present"

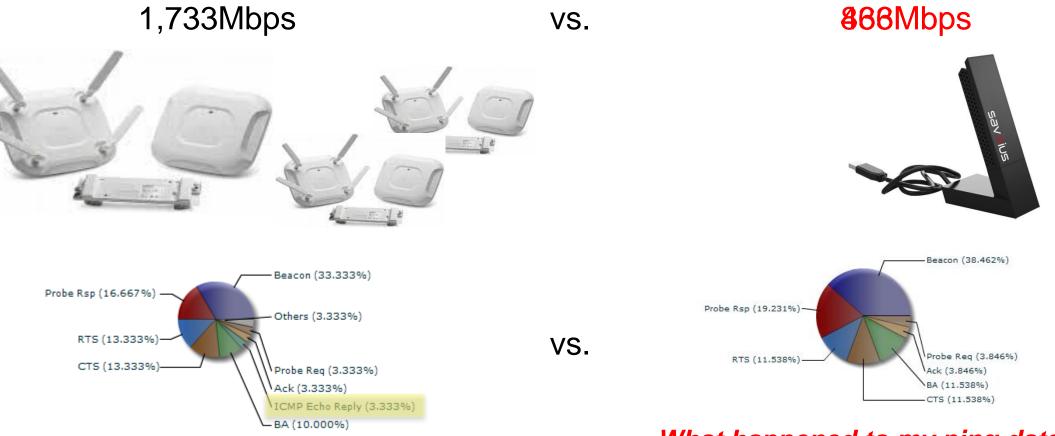






#### 802.11ac vs. Portable Packet Capture

#wifitrek





#### What happened to my ping data?

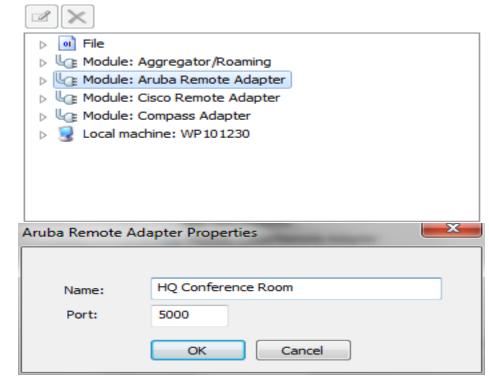
#### Remote Point-of-Presence

- As wireless approaches wired speeds, it's time to start relying on the wire
- Distributed analysis using deployed assets typically APs is the only effective solution as wireless capabilities and speeds grow
- The choices:
  - Custom Remote Adapters
  - Remote PCAP
  - Remote sensors



### **Custom Remote Adapters**

- Specific to Savvius and OmniPeek
- Allow an AP to be put into promiscuous mode and act like a direct-connected sniffing device
- APs are "reconfigured" via the AP controller software
- Depending on the manufacturer and the model, APs may or may not be able to continue sending traffic



#### **Remote Pcap**

- A WinPcap feature that allows interaction with a remote machine to capture packets
- Simply start a capture on the analyzer and point it to the available RPCAP interfaces
- Typically not a "marketed feature"
- Devices we have worked with include:
  - Aerohive: Model HiveAP 120
  - Ruckus: ZoneFlex 7363 (requires ZoneDirector Controller)

Adapter	Channel
OmniWiFi	Select
rpcap://[10.4.2.50]:2002/wifi0sniffer	RPCAP_INTF_WIFI
rpcap://[10.4.2.50]:2002/wifi1sniffer	RPCAP_INTF_WIFI



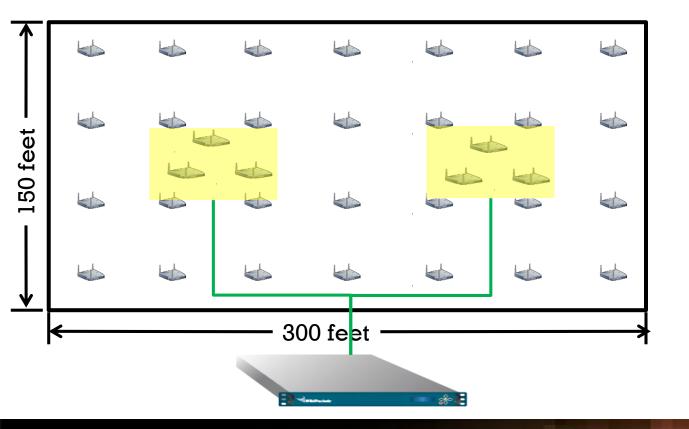
### Example Mission-Critical Financial Trading



- All users on Wi-Fi; BYOD
- 100's of simultaneous users
- 100's of trades per second
- Deliver, verify that each individual gets the same QOS to guarantee fair trading
- Single appliance solution
- 24x7 forensics data capture with additional real-time captures to handle spot problems



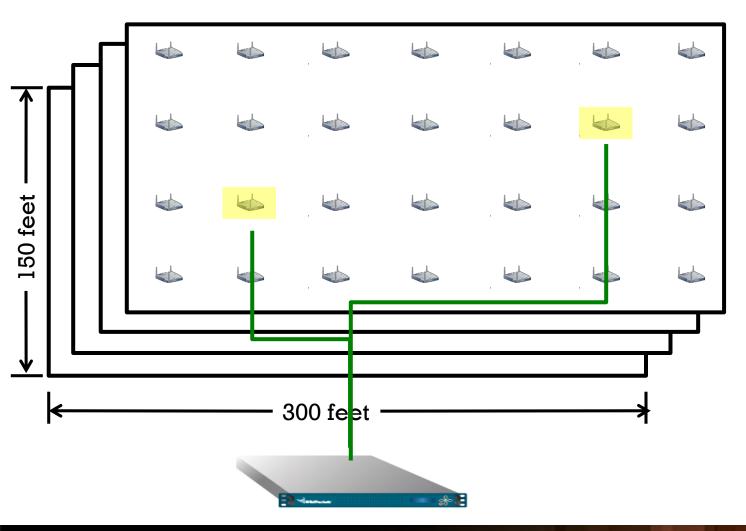
# High Density/Small Physical Footprint Deployment



- Dense deployment 28 APs per trading floor
- Sensor APs 2 groups of 3
- Provides dedicated, 24x7 monitoring



### Highly Distributed, Multi-Campus Deployment



- Dense deployment ~ 28 APs per building floor
- 100's of building floors
- Reactive capture and analysis



# When?

Certified Wireless Network Professional

IT Professional Wi-Fi Trek 2015 #wifitrek

### Solving Problems with Packets

#### Verifying device capabilities

- Network capabilities look at beacons
- Client capabilities look at probe requests

#### Verifying device configuration

QoS enabled/disabled

#wifitrek

- Beacon intervals too long/short
- CTS frames that look like duration attacks (10,000µs duration field)
- Troubleshooting connection/authentication issues

 Identifying sources of poor VoFi quality

#### Identifying network bottlenecks

- Chatty clients
- Probe requests
- Inefficient network utilization
- Wireless is slow
- Analyzing roaming issues
  - Sticky clients
  - Roaming latency



# When? Examples

IT Professional Wi-Fi Trek 2015 #wifitrek



## Verifying Device Capabilities Network Capabilities - Beacons

🖃 🌹 Packet Info		🖃 🍞 HT Capability Info:	%0000100011101111 [77-78]
Packet Number:	7	9	0 L-SIG TXOP Protection Support: Not Supported
<pre>   Flags: </pre>	0x0000000	9	.0 AP does Not allow use of 40MHz Transmissions In Neighboring BSSs
G Status:	0×0000000	9	0 Reserved
Packet Length:	231	9	0 BSS does Not Allow Use of DSSS/CCK Rates @40MHz
<pre>   Timestamp: </pre>	04:08:49.065573700 10/16/2013	9	1 Maximal A-MSDU size: 7935 bytes
Data Rate:	12 6.0 Mbps	9	0 Does Not Support HT-Delayed BlockAck Operation
Channel:	161 5805MHz 802,11a	9	00 No Rx STBC Support
<pre>     Signal Level: </pre>	100%	() ()	1 Transmitter does Support Tx STBC
<pre>Signal dBm:</pre>	-38	() ()	
<pre>     Noise Level: </pre>	0%		1 Short GI for 20 MHz: Supported
Noise dBm:	-5	ø	0 Can Not receive PPDUs with HT-Greenfield format
	eader Version=0 Type=%00 Subtype=%1000 Frame		11 SM Power Save Disabled
■ ■ 802.11 Management - Be			1. Both 20MHz and 40MHz Operation is Supported
Beacon Timestamp:	62290534458 Microseconds [24-31]	A-MPDU Parameters:	1 LDPC coding capability: Supported
Beacon Interval:	100 Time Units (102 Milliseconds, and 400	A-MPDU Parameters:	\$00010111 [79]
Generation Interval: End of the second se	\$0000000000000001 [34-35]	<b>a</b>	101 Minimum MPDU Start Spacing: 4 usec
	14 SSID=Wild Bright AC [36-51]		11 Maximum Rx A-MPDU Size: 65,535 Bytes
	8 Rate=6.0 Rate=9.0 Rate=12.0 Rate=18.0 Rate=	•	II Haxtman KX Arrebo Size. 05,555 Bytes
	4 DTIM Count=0 DTIM Period=1 Bitmap Control=%		
	=5 Station Count=1 Channel Utilization=1 Avai	🖃 🚏 VHT Supported MCS Set	
	=26 HT Capability Info=%0000100011101111 A-MP	🖃 🏹 Rx MCS Map:	<b>%11111111101010</b> [143-144]
		- OP	
	=22 Primary Channel=161 HT Operation Element	9	
	esID=127Len=8 Extended Capabilities=%0000000	<b>(7)</b>	
	ementID=191Len=12 VHT Capabilities Info=%0000	<b>G</b>	11 Supported MCS index for 4 SS: Not provided
	ntID=192Len=5 VHT Operation Information=Chann	9	11 Supported MCS index for 5 SS: Not provided
	EnvelopeID=195Len=4 Transmit Power Informatio	<b>()</b>	11 Supported MCS index for 6 SS: Not provided
	n=24 OUI=00-50-F2 OUI Type=4 Version=0x10 Wi-	() ()	11 Supported MCS index for 7 SS: Not provided
	21Len=9 OUI=00-10-18 Value=(6 bytes) [190-200	Ø	11 Supported MCS index for 8 SS: Not provided
	n=24 OUI=00-50-F2 OUI Type=2 OUI SubType=1 Ve		
FCS - Frame Check Sequ			
<pre> FCS: </pre>	0x469A80BA Calculated		



### Verifying Device Capabilities Client Capabilities – Probe Requests

🖃 🌹 <u>802.11 Management - P</u> r	robe Response	□ 🚏 <u>SSID</u>	
Probe Timestamp:	62294733406 Microseconds [24-31]	🎯 Element ID:	0 SSID [36]
🎯 Beacon Interval:	100 Time Units (102 Milliseconds, and 400 Microseconds) [32-33]	🐨 Length:	14 [37]
🖃 🚏 Capabilit 🔶 Info:	<b>%0000000000001</b> [34-35]	SSID:	Wild Bright AC [38-51]
<b>(</b> )	Ø Immediate Block Ack Not Allowed	🗆 🌹 <u>Supported Rates</u>	
9	.0 Delayed Block Ack Not Allowed	🜍 Element ID:	1 Supported Rates [52]
9	0 DSSS-OFDM is Not Allowed	G Length:	8 [53]
9	0 No Radio Measurement	🜍 Supported Rate:	6.0 Mbps (BSS Basic Rate) [54]
9	0 APSD is not supported	🜍 Supported Rate:	9.0 Mbps (Not BSS Basic Rate) [55]
9	0 G Mode Short Slot Time [20 microseconds]	🜍 Supported Rate:	2.0 Mbps (BSS Basic Rate) [56]
9	0 QoS is Not Supported	🜍 Supported Rate:	18.0 Mbps (Not BSS Basic Rate) [57]
9	0 Spectrum Mgmt Disabled	🜍 Supported Rate:	24.0 Mbps (BSS Basic Rate) [58]
9	Ø Channel Agility Not Used	🜍 Supported Rate:	36.0 Mbps (Not BSS Basic Rate) [59]
9		🜍 Supported Rate:	48.0 Mbps (Not BSS Basic Rate) [60]
9		🜍 Supported Rate:	54.0 Mbps (Not BSS Basic Rate) [61]
9			
9	0 CF Poll Not Requested		
9	0 CF Not Pollable		
9	0. Not an IBSS Type Network		
<b>G</b>	1 ESS Type Network		

Certified Wireless Network Professional

## Verifying Device Configuration QoS

Subtype:
 Subtype:

0 [0 Mask 0x03] %10 Data [0 Mask 0x0C] %1000 QoS Data [0 Mask 0xF0]



### Verifying Device Configuration Beacon Intervals

🗆 🖃 🌹 <u>802.11 Management - Bea</u>	acon
🎯 Beacon Timestamp:	62295040058 Microseconds [24-31]
🎯 Beacon Interval:	100 Time Units (102 Milliseconds, and 400 Microseconds) [32-33]
🖃 🚏 Capability Info:	%00000000000001 [34-35]
9	Ø Immediate Block Ack Not Allowed
9	.0 Delayed Block Ack Not Allowed
9	0 DSSS-OFDM is Not Allowed
9	0 No Radio Measurement
9	0 APSD is not supported
9	0 G Mode Short Slot Time [20 microseconds]
9	0 QoS is Not Supported
~	

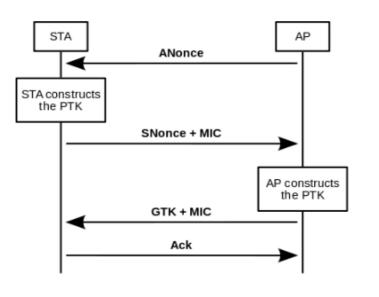


### Verifying Device Configuration CTS Excessive Duration

🖃 🎙 Packet Info	
Packet Number:	10
G Flags:	0×00000001
G Status:	0×00000000
Packet Length:	14
Timestamp:	23:07:55.313722100 11/19/2012
🕥 Data Rate:	12 6.0 Mbps
G Channel:	149 5745MHz 802.11a
🕥 Signal Level:	36%
🜍 Signal dBm:	-59
🕥 Noise Level:	60%
🕥 Noise dBm:	-68
<pre>G Expert:</pre>	
🗆 🌹 <u>802.11 MAC Header</u>	
🕥 Version:	0 [0 Mask 0x03]
🜍 Type:	%01 Control [0 Mask 0x0C]
🕥 Subtype:	%1100 Clear To Send (CTS) [0 Mask 0xF0]
🖃 🍟 Frame Control Flags:	
9	0 Non-strict order
9	.0 Non-Protected Frame
9	0 No More Data
9	1 Power Management - power save mode
() ()	0 This is not a Re-Transmission
<b>()</b>	0 Last or Unfragmented Frame
<b>()</b>	0. Not an Exit from the Distribution System
<b>()</b>	0 Not to the Distribution System
<pre>     Duration:     </pre>	18800 Microseconds [2-3]
Receiver:	68:EF:BD:B3:8C:49 Geo Cisco Phone [4-9]
FCS - Frame Check Sequer	
G FCS:	0xA200C8BD Calculated



#### Troubleshooting Connection/Authentication Issues Authentication – EAPOL Key Exchange



- The AP sends a nOnce key to the STA
- The STA sends its own nOnce key to the AP with a Key MIC
- The AP sends the key data with another MIC
- The STA sends a confirmation to the AP

3 🖏 Symbol	AP	🗐 Client	Computer	Symbol 🕲	AP	EAPOL-Key
4 🌒 Client		🖑 Symbol	AP	🕲 Symbol	AP	EAPOL-Key
5 🖑 Symbol	AP	🌒 Client	Computer	🕮 Symbol	AP	EAPOL-Key
6 🞲 Client	Computer	💩 Symbol	AP	👛 Symbol	AP	EAPOL-Key

🕥 Туре:	254 WPA key descriptor [36]
🗄 🚏 Key Information:	%000000010001001 [37-38]
Key Length:	32 TKIP [39-40]
Replay Counter:	8027 [41-48]
🞯 Key nOnce:	0x18E53C7DC10DFE66E444D27212FDB8827845340A1E3FF101A6D8DE6E391(
<pre>G EAPOL-Key IV:</pre>	0x000000000000000000000000000000000000
Wey RSC:	0x000000000000000 [97-104]
🕥 Key ID:	0x000000000000000 [105-112]
Key MIC:	0x000000000000000000000000000000000000
🜍 Key Data Length:	0 [129-130]
EAPOL - Key	
Type:	254 WPA key descriptor [36]
🗄 🚏 Key Information:	%00000010001001 [37-38]
G Key Length:	32 TKIP [39-40]
Replay Counter:	8027 [41-48]
🕲 Key nOnce:	0x5FCFCF061936365CB8F2E4DFBE30CFEC13FAFA17E8D52A2DD2F7086464D
<pre>G EAPOL-Key IV:</pre>	0x000000000000000000000000000000000000
Wey RSC:	0x000000000000000 [97-104]
🗑 Key ID:	0x00000000000000 [105-112]
W Key MIC:	0x9026181E57DF809B9BFD11B6B013718C [113-128]
EAPOL - Key	
Type:	254 WPA key descriptor [36]
Type: Key Information:	254 WPA Rey descriptor [36] %0000001110100001 [37-38]
Key Length:	32 TKIP [39-40]
Replay Counter:	8029 [41-48]
Wey nOnce:	0x18E53C7DC10DFE66E444D27212FDB8827845340A1E3FF101A6D8DE6E391
BAPOL-Key IV:	0x18E53C7DC10DFE66E444D27212FDB882 [81-96] 0x18E53C7DC10DFE66E444D27212FDB882 [81-96]
WEAPOL-KEY IV:	0x18655C7DC10DF6066444027212FD6882 [81-98] 0x1A00000000000000 [97-104]
Wey ID:	0x00000000000000 [105-112]
Wey MIC:	0xEC203AB8313F8E10C0424C4CBF20F98C [113-128]
Key Data Length:	32 [129-130] 0-0785405205550556472448588141887777895558472441648914555564857248
🗑 Key Data:	0x278EA9526DFCA2A4BEBB141BB737D0D6EB472416410AD1AEF59CAB5724B
EAPOL - Key	
🕥 Type:	254 WPA key descriptor [36]
🗉 🚏 Key Information:	%0000001100000001 [37-38]
9	000 Reserved
9	0 Key Data is Not Encrypted
9	Ø Handshake Not Requested
G	1 Initial Kev Exchange Complete
	1 Initial Key Exchange Complete
9 4	1 MIC Included in Frame
9 - 4 9	1 MIC Included in Frame 0ACK Not Set
0 4 6 7 8	1 MIC Included in Frame 0 ACK Not Set 0Install Flag: Ignored
() () () () () () () () ()	MIC Included in Frame 
0 4 6 7 8	1 MIC Included in Frame 0 ACK Not Set 0Install Flag: Ignored



### Identifying Sources of Poor VoFi Quality

- RTP packets (G.711)
- Overall VoIP analysis
- Jitter, packet loss, latency

Protocol 🔺	Percentage	Bytes	Packets
루 G.711	95.544%	1,386,826	5,827
TRTCP	0.107%	1,560	12
🗍 SIP	0.437%	6,341	9

Call Number 🔺	SSRC	Name	End Cause	Codec	Media Type
	3942986A	G.711 10.10.1.232:safetynetp<10	BYE	G.711µ-law	Voice
0 1	000018BE	G.711 10.10.1.232:safetynetp>10	BYE	G.711 µ-law	Voice

A Datalla Durat C	Event Les			V 💌 /
	ummary Event Log			1
Name	Value	Name	Value	
Call Number	1	Name	G.711 10.10.1.232:safetynet	o<10.10.1.200:12242
Flow Index	2	From	"3CXPhone" <sip:200@10.10.1< td=""><td>1.200:5060&gt;;tag=f34f1106</td></sip:200@10.10.1<>	1.200:5060>;tag=f34f1106
SSRC	3942986A	То	<sip:2745495@10.10.1.200:5< td=""><td>5060&gt;</td></sip:2745495@10.10.1.200:5<>	5060>
Flow ID	-		OGZIZDk5MTAzNjg4MzdjYzhhZ	GFmZjA3NTY0Y2UwMmE.
Caller Address		End Cause	BYE	
	40000 safetynetp	Signaling		
Callee Address		Protocol		
Callee Port			G.711 µ-law	
Gatekeeper Address		Bit Rate		
Gatekeeper Port		Media Type		
	10.10.1.200	Setup Time		
Source Port			3.185682	
	10.10.1.232		10/13/2009 12:42:56	
	40000 safetynetp		10/13/2009 12:43:52	
Media Packets			55.496566	
Media Frames	122160	One-Way Delay		
		Packet Loss %		
R Factor Listening			0.000553	
R Factor Conversational		MOS-LQ		
R Factor G. 107		MOS-CQ		
R Factor Nominal	93	MOS-PQ		
VS-AQ		MOS-Nom	4.19	
VS-MQ		MOS-A		
VS-PQ		MOS-AV		
VS-TQ		MOS-V		



### Identifying Network Bottlenecks

- Chatty/probing clients, i.e. phones
- Inefficient network utilization
- Wireless is slow



## **Chatty Clients**

File Edit Vie	IN CAR	ture Send	A CONTRACT OF THE OWNER OWNER OF THE OWNER	and the second second						WildPa	ckets Omin	Peek
2 - 12 - H	6	C 3 6	0.00.00	**	計測工		8.9					
Start Page	- Ca	phare 1 🖂	Name Tabl	e								E.
Packets received:			Euffer usage: filler state:			kets matching one	all the second s				Start Cast	re
Y-	1.00		THE MAR	-	cebe pash bac	sets matching dis	1998					
Dashboards	1.000	LOW NO.	ALE	× #11	0.10	10.000						1970
Network	1000	ALC: NO.	and the second se			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-			monort		14
Voice & lideo		Flags	Channel	Signal		802.11 Plags	Sae	Delta Time	Relative Time			1
Apdex	loas's	1.00	3	1004			117	0.053159000	84.461738000			
Compete	losat	10	3	1004		**** ****	117	2.518586000	58.980324000			
Packets	1114	+2+	2	104		**** ****	349	0.003186000	58.983510000			
			1	158			369	0.003470000	58.986960000			
Log		*2+	1			····R ····	269	0.003483030	58.990463000			
Piters		1.124	1	154		***R ****	269	0.004115000	58.994576000			
spert		424	*	154		····R ····	369	0.003469000	58.995047000			
Herarchy		124	1	104			269	0,003495000	59.001542000			
Flat		*2+	-	204		····R ·····	369	0.004577000	59.006119000			
Application	loast.		2	1004		**** ****	217	0.032373000	59.038492000			
Feb	loast		1	1004			117	0.055591000	59.094063000			
Servers	11116	1 mg	1	104	1.0		249	0.003188000	\$9.097271000	802-31	shope wab	1000
Clients Pages					ALC: NO.							
Reguesta Vicice & Video Calls Media Visualis Peer Map Graphs Statistics Nooles Protocols Summery	- Y	[0-23] [24-200 [0]	002.11		Timestan	Lon-d Type-4	00 Hanap	occoc Status-Co anat Subtype-W nerconts Seacon	101 Friche Reap			
the second second					100 10	Gross Patternal Vill	ration One	Innet T - 2412 MHz B	Dector 1938	0	aution: 0.011	
						arthi continua in	reative cons	HANKE & FRAME MARKED	of second and		man and property in the	-
or Held, great F1											None	

#### **Device On – Unassociated**

- Larger frames, low data rate, fewer packets
- ~250µsec/frame

#### http://www.sniffwifi.com/2012/04/phones-on-wlan.html

Packets sective:         43,870 Filter state:         Define sugge ON Filter state:         Sector of packets matching one filter           Packets State         Packets State         Packets State         Packets State         Packets State           Daskbaande Vector         Packets	4 Start Page	Cap	ture 1 ×	Name Tab	le l			-					
Deskloards Nethork Vace & Ndeo Acdex         Comment         Signet         Deta Rate         402.11 Flags         Size         Deta Time         Relative Time         Practed           Acdex Company Company         1         1.55         2.0         1.1         0.000124000         S5.343365000         002.11         Acid           Company Company         1         1.55         2.0         1.1         0.0000124000         S5.343365000         002.11         Built						ept only pac	Sets matching one	Bur .				Start Castur	
Network Vace & Noted Apdex         Page         Obsine Rate         Some         Deta Rate         Some         Deta Rate         Reletive Time         Reletit Time         Reletive Time         Re	8-						and the second second second						
Vace & Make Appler         Page         Charmel         Sign         Data Rale         802:11 Flags         Sign         Defa Time         Relative Time         Relatit Time         Relative Time </th <th></th> <th>-04.10</th> <th>- Inthate</th> <th>1.61</th> <th>9. 3.1</th> <th>8-18</th> <th>38122</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>		-04.10	- Inthate	1.61	9. 3.1	8-18	38122						
Appler Compass Compass Capture Prest B         *         1         154 1         2.0          14         0.000124000 55.00202000         55.34336900 55.00220000         002.11 Mult Data           Capture Prior Englet Log         11:45 1         1         1004 24.0         24.0         T         28         0.000019000 55.00200000         55.403220000         002.11 Mult Data           Prior Englet         11:45 1         1         1004 24.0         24.0          14         0.00000000 55.55924000         55.35321000         002.11 Mult Data           Prior Englet         11:45 1         1         1004 24.0         24.0          14         0.00000000 55.559240000         55.553251000         002.11 Mult Data           Prior Englet         11:45 1         1         1024 24.0         24.0          14         0.00000000 55.559240000         55.559240000         002.11 Mult Data           Mathematics         1         154 24.0         24.0          14         0.000000000         55.559240000         002.11 Mult Data           Berners         1         154 24.0         24.0          14         0.0000125040000         56.457357000         002.11 Mult Data           Pages         1         158 24			Flags (	Channel	Signal	Data Rate	802.11 Flags	See	Delta Time	Relative Time	Protocol		
Company approve > Packets ing When > Packets ing When > Packets ing When > Packets ing When > Packets ing When > Packets > 1:1:65 1:1:05 1:1				1	154	2.0		14	0.000124000	55,363365000	002.11	Ack	-
P Packers         1         104         24.0         1.000         55.402371000         002111 Ank           ing         PHars         1         104         24.0         24.0         23715000         55.55224000         002.111 Bulk           xgert         1         104         24.0         1         14         0.00000000         55.55224000         002.111 Bulk         Bulk           Hermothy         1         104         24.0         1         14         0.00000000         55.552251000         002.111 Bulk         Bulk           Hermothy         1         104         24.0         1         14         0.00000000         55.552251000         002.111 Bulk         Bulk           Metmothy         11:05         1         104         24.0         1         14         0.00000000         55.55251000         002.111 Bulk         Bulk           Metmothy         11:05         1         154         24.0         1         14         0.00000000         56.553251000         002.11 Bulk         Bulk           Bernets         1         154         24.0         T         12         0.001350000         56.547357000         002.11 Bulk         Bulk           Bages <td></td> <td>11:63</td> <td></td> <td>1</td> <td>1009</td> <td></td> <td></td> <td>28</td> <td>0.035537000</td> <td>55,402202000</td> <td>802.21</td> <td>Sull Date</td> <td></td>		11:63		1	1009			28	0.035537000	55,402202000	802.21	Sull Date	
Packers         1         104         24.0         1.000         55.402370500         002111 Refe           ing         Phars         1         104         24.0         24.0         23.2715000         55.55224000         002.11 Rufe           spect         1         104         24.0         1         14         0.00000000         55.55224000         002.11 Rufe           Hermotive         1         104         24.0         1         14         0.00000000         55.55224000         002.11 Rufe           Hermotive         1         104         24.0         1         14         0.00000000         55.55224000         002.11 Rufe           Hermotive         1         104         24.0         1         14         0.00000000         55.55224000         002.11 Rufe           Hermotive         1         104         24.0         1         14         0.00000000         55.55254000         002.11 Rufe           Hermotive         1         104         24.0         T         14         0.000000000         56.547357000         002.11 Rufe           Hermotive         1         154         1.0         Tr         14         0.000000000         56.5473450000         <	anture	11165		1	1004	24.0	T R. P	2.8	0.000319000	55.402521000	802.11	Mull Dets	
ing PHers Sevent         11:45         1         1004         24.0         7         28         0.532715000         55.553242000         102.11         Bull Date           Hersdry Hersdry Hersdry Hersdry Hersdry Reb Sevents         1         1004         24.0         1         14         0.00000000         55.55324000         102.11         Bull Date           Hersdry Hersdry Hersdry Reb Sevents         1         1054         24.0         1         14         0.00000000         55.558240000         602.11         Bull Date           Application Feb         1         154         24.0         1         14         0.00000000         55.55826000         602.11         Bull Date           Sevents         1         154         24.0         1         14         0.00000000         56.475857000         602.11         Bull Date           Sevents         1         154         24.0         1         14         0.00000000         56.475857000         602.11         Bull Date           Sevents         1         154         24.0         1         14         0.100000000         56.47585000         602.11         Bull Date           Sevents         1         154         24.0         1         1				1									
Piters         1         104         24.0         1.1         14         0.00000000         55.553251000         002.11         Ank           Meratchy         1         1064         24.0          24         0.00000000         55.553251000         002.11         Built         Dates           Meratchy         1         154         24.0          14         0.0000000         55.554260000         002.11         Built         Dates           Application         1         154         24.0          14         0.00000000         55.594260000         002.11         Built         Dates           Application         1         154         24.0          14         0.00000000         55.594260000         002.11         Built         Dates           Servers         1         154         24.0          14         0.000040000         56.475350000         002.11         Built         Dates           Berders         1         154         24.0          14         0.000040000         56.475350000         002.11         Built         Dates           Berders         1         154         24.0          10 </td <td>Log</td> <td>11145</td> <td></td> <td>1</td> <td>1004</td> <td>24.0</td> <td>T</td> <td>28</td> <td>0.132715000</td> <td>\$5.535242000</td> <td>802.11</td> <td>Bull Deta</td> <td></td>	Log	11145		1	1004	24.0	T	28	0.132715000	\$5.535242000	802.11	Bull Deta	
Here depkasion         I         1         154         24.0         1.4         0.00000000         55.554840000         500.11         Aces           Applexation         I         154         24.0         I.2         2.75481000         56.47535000         500.11         Back           Applexation         I         154         24.0         I.2         2.75481000         56.47535000         500.11         Back           Servers         1         154         24.0         I.2         2.75481000         56.47435000         600.11         Back           Servers         1         154         24.0         I.2         16         0.0001385000         56.474345000         600.11         Back           Clents         1         154         24.0         I.2	Files		1.8	1	204			14	0.000009000	55,535251000	502.31	Ack	
Here are the first set of the se	speet	11:45		1	1004	24.0	T P	28	0.061609000	55.596260000	802.11	Sull Date	
Application         1         154         24.0         1         16         0.000010000         54.475357000         F02-11 ApX           Servers         1         154         1.0         F.         20         0.0001385000         54.475357000         F02-11 ApX           Servers         1         154         1.0         F.         20         0.0001385000         54.4754500         50.11 ApX           Cleris         1         154         24.0          14         0.10565500         54.54543000         F02-11 ApX           Pages         Requests         * <t< td=""><td>Herarchy</td><td></td><td></td><td>1</td><td>154</td><td></td><td></td><td>14</td><td>0.0000080000</td><td>55.596868000</td><td>802.11</td><td>Acc</td><td></td></t<>	Herarchy			1	154			14	0.0000080000	55.596868000	802.11	Acc	
Web         1         154         1.0.F         30         0.001388000         55.478745080         60.2111         205         Multi Data           Clents         1         154         24.0          14         0.105485000         55.4787450800         602.112         26.5         Multi Data           Pages         1         154         24.0          14         0.105485000         55.4787450800         602.112         26.5           Pages         Reservers          14         0.105485000         55.4787450800         602.112         26.5           Reservers         Reservers          14         0.105485000         55.4787450800         602.112         26.5           Reservers         Reservers	Plat	11:65	*	1	1004	24.0	T R	28	2.076405000	58.475353000	802.11	Sull Date	
Reb Servers         11:65         1         154         1.0          30         0.001380000         56.4149445000         602.11 QoS Thuil Data           Clents         *         1         154         24.0          14         0.105485000         56.4149445000         602.11 QoS Thuil Data           Pages         *         1         154         24.0          14         0.105485000         56.4149445000         602.11 Loss           Pages         Repuests         *         1         154         24.0          14         0.105485000         56.419445000         602.11 Loss         16.00 <td>Application</td> <td></td> <td>*</td> <td>1</td> <td>154</td> <td>24.0</td> <td></td> <td>1.4</td> <td>0.000004000</td> <td>58.475357000</td> <td>802-11</td> <td>Ack .</td> <td></td>	Application		*	1	154	24.0		1.4	0.000004000	58.475357000	802-11	Ack .	
Clerts Pages Requests Requests Refer to the sector that the se	Web #	11:45		1	154			30	0.0013880000	55.476745000	802.11	QoS Bull Det	
Pages     Packet Info     Packet Info       Requests     Soft     10-91     922.11 MAC Header Version-0 Type=401 Control Subtype=41101 Duration=0 Microseccode Receiver=D       Meda     Meda     PCS=0xF6410563 Calculated       Meda     Poer Map Graphs     PCS=0xF6410563 Calculated       Nodes     Poet Map Summary     PCS=0xF6410563 Calculated	Servers			1	154	24.0		2.4	0.108685000	58.585430000	802-21	Act	
Pages Requests Recent Market Info Factort Humber-229 Flags-Ox00000001 Status-Ox00000000 Tecket Length-14 Timestamp Safe & Video Cols Meda Nucles Peer Map Graphs Retables Nodes Nodes Per Map Graphs Summary	Clients					-		-					
Police & Welso Cole Meda Meda Per Nop Graphs Nodes Police Summary	Pages					had in the second							1
Calls B: Y (0) PCS: PCS=0xP6410563 Caloulated Peer Map Graphs Retristics Protocols Summary													
Media Pissable Deer Map Graphs Skatistics Nodes Pretoole Summary	foice & Video			022.1	1 MAC Be	ader Vers	sion-d Type-40	Contro	ol Subtype=\$1101	Durstins-0 Mi	centercol	ods Receiver-	Car
Peer Map Graphs RatinStors Nodes Pretools Summary		- T	103	PCS /		PCS-ORF6	410563 Caloud	47-04					
Peer Map Graphs Skatistics Nodes Pretocals Summary													
Graphis Startistics Nodes Protocilis Summary	risuals												
Ratistics Nodes Protocols Summary													
Nodes Pretocols Summary	Graphs												
Protocols Summary	tatistics												
Sumary													
	Protocors												
	Summary Fireless	1					stress Paternal Vila	dans Dea	and To 2412 Eller D	Partners 100	0	mation: 0.0140	
Idle By Linksys External Winnless Channet I - 2412 MHz (bg) Packets: 229 Durations: 0:02:00	Summary	1		_	- 200	190	nktys External Vile	eless Cha	mmett II - 2402 MMz (B	gi Packets: 229	D	unation: 0:01:00	

#### Associated

- Smaller frames, higher data rate, more packets
- ~1µsec/frame



### Inefficient Network Utilization

#### OmniPeek

File Edit View Capture Send Monitor Tools Window Help

#### 🔊 - ઇ - 🖟 🗞 " i 🖬 Y 🗉 🛦 🖄 " i 🧄 🎄 " i 🕑 T 🤶 🥙 🗉 🖬 Y 🗢 " i 🗈 i 🚱 🐧 "

4	Alarms	Start Page	Capture 1	Capture 1 - Packet #65	х

#### 🗢 🔿 📳 📖 🔠 🔍 🗣 🚱 🥩 🦻

- ± 🍸 Packet Info Packet Number=65 Flags=0x00000000 Status=0x00000000 Packet Length=358 Timestamp=15:50:05.672259000 05/29/2014 Dat Image: Text and te 802.11 MAC Header Version=0 Type=%00 Management Subtype=%0101 Probe Response Duration=60 Microseconds Destination=Bens Laptop S 🖃 🏋 802.11 Management - Probe Response
- 🎯 Probe Timestamp: 11761949141501 Microseconds [24-31]
- 100 Time Units (102 Milliseconds, and 400 Microseconds) [32-33] Beacon Interval:
- H Capability Info=%0000010000110001
- ∃ SSID ID=0 SSID Len=3 SSID=R&T
- 🗄 🗍 Rates= ID=1 Rotes: Len=8 Rate=6.0 Mbps Rate=9.0 Mbps Rate=12.0 Mbps Rate=18.0 Mbps Rate=24.0 Mbps Rate=36.0 Mbps Rate=48.0 Mbps Rate=54.0
- DSPS= ID=3 DSPS: Len=1 Channel=40
- ⊞ 🐨 CFPS= ID=4 CFPS: Len=6 CFP Count=0 CFP Period=2 CFP Max Dur=0 CFP Dur Remaining=0
- 🗄 🚏 RSN= ID=48 RSN: Len=20 Version=1 Group Cipher OUI=00-0F-AC Group Cipher Type=4 Pairwise Cipher Count=1 AuthKey Mngmnt Count=1 TO THE AT Case TD=45 HT Case Lone 26

± 9 <u>n </u>	<u>Cap=</u> 10=45 HI Cap: Le	1=20
🗆 🍞 <u>ht i</u>	<u>Information</u>	
) 🕤 🕄	Element ID:	61 HT Information [112]
I 🕲	Length:	22 [113]
🐨 F	Primary Channel:	40 [114]
🕀 🏋 🗄	HT Info Element 1=%00	300111
- T	HT Info Element 2:	%0000000000100 [116-117]
	9	
	3	1. Non-Greenfield STAs: One or more HT STAs are Not Greenfield Capable
	3	0 Transmit Burst Limit: No Limit
	3	
	3	xxxxxxx xxx Reserved
🗉 🏋 H	HT Info Element 3=%00	300000000000
🗉 🏋 🛙	Basic MCS Set Rx Bitma	ask b16-b23=%00000000 Rx Bitmask b24-b31=%00000000 Rx Bitmask b32-b39=%00000000 Rx Bitmask b40-b47=%00000000 Rx
🗄 🏋 Ven	dor Specific ID=221 V	endor Specific Len=30 OUI=00-90-4C Epigram Data=(27 bytes)
🗄 🏋 <u>Ven</u>	dor Specific ID=221 V	endor Specific Len=26 OUI=00-90-4C Epigram Data=(23 bytes)
🗄 🏋 <u>Ven</u>	dor Specific ID=221 V	endor Specific Len=6 OUI=00-50-43 Marvell Data=(3 bytes)
🕀 🏋 WMM	TD=221 WMM Len=24 OU	[=90-50-F2 Microsoft OUI Type=2 OUI SubType=1 Parameter Element Version=1

- Microsoft OUI Type=2 OUI SubType=1 Par 🗄 🐨 WP5 ID=221 WP5 Len=122 OUI=00-50-F2 Microsoft OUI Type=4 Version=0x10 1.0 Wi-Fi Protected Setup=2 Configured Response Type=0x03 AP UUID-
- 🕀 🏋 [0] FCS: FCS=0x4760A21A Calculated

#### **Probe response**

- Pure HT mode
- No protection should be used (no RTS/CTS)

http://www.sniffwifi.com/2014/05/why-are-you-slowing-down-my-wifi-apple.html

#### OmniPeek

Visuals

Peer Map Graphs Statistics

Summary

Protocols w......

Nodes

File Edit View Capture Send Monitor Tools Window Help

#### 🔊 - 📁 - 🔲 😂 , i 🖬 🖓 🖳 🙆 , i 🏘 🦓 , i 🕃 T 🌻 🥙 🗊 🖬 🤋 , i 😫 🖓 🖉

Alarms Start Page Capture 1 × Capture 1 - Packet #65

Packets received:	47,857	Buffer usage:	4%	
Packets filtered:	17,314	Filter state:		Accept only packets matching one filter

Enter a filter expression here (use F1 for help)

🕀 🏹 [0]

Dusingentus	<b>^</b>	♦ ♦	E E Ox	🔠   🔍 🧞   🤊	🖓 •   🗣 😼 🥵 📝 🖗										
Network	10	Dackat	Transmitter		Receiver	BSSID		Flags	Signal	Data	MCS	Spatial St	Size	Protocol	
Voice & Video					1.3			nays	-		MCS	Spauai St			
Apdex		15777	関 Bens	Laptop	Rough & Tumble AP	Rough &	Tumble AP		-49	6.0		1	28	802.11	Null Data
Compass		15778			🖏 Bens Laptop			#	- 57	6.0		1	14	802.11	Ack
Capture			👛 Rough	& Tumble AP	🕼 Bens Laptop	📥 Rough &	Tumble AP		- 61	243.0	14	2	136	802.11	Encrypted
<ul> <li>Packets</li> </ul>		15780	関 Bens	Laptop	🕲 Rough & Tumble AP			#	-51	24.0		1	34	802.11	BA
Log		15781	🌒 Bens	Laptop	🕮 Rough & Tumble AP			#	- 50	24.0		1	20	802.11	RTS
Filters		15782			🌒 Bens Laptop			#	- 59	24.0		1	14	802.11	CTS
Expert		15783	関 Bens	Laptop	🕲 Rough & Tumble AP	Rough &	Tumble AP	WA	-42	300.0	15	2	106	802.11	Encrypted
Clients/Server		15784	Rough	& Tumble AP	Bens Laptop	Rough &	Tumble AP	WA	-61	243.0	14	2	1204	802.11	Encrypted
Flows		15785	🌒 Bens	Laptop	🕲 Rough & Tumble AP			#	-49	24.0		1	34	802.11	BA
Applications		15786	🌒 Bens	Laptop	🕲 Rough & Tumble AP			#	-49	24.0		1	20	802.11	RTS
Web		15787			Bens Laptop			#	- 59	24.0		1	14	802.11	CTS
Servers		15788	🕼 Bens	Laptop	🐻 Rough & Tumble AP	🚳 Rough &	Tumble AP	WA	-41	300.0	15	2	106	802.11	Encrypted
Clients		15789	Rough	& Tumble AP	🗐 Bens Laptop			#	- 59	24.0		1	34	802.11	BA
Pages	Ξ /	15790	💷 Bens	Laptop	Rough & Tumble AP	CROUGH &	Tumble AP		-49	6.0		1	28	802.11	Null Data
Requests	4	•						111							
Voice & Video	4	🕀 🏋		Packet Info	Packet Number=15779 F	Flags=0x00000	000 Status=0	×000000	04 Encry	pted Pa	acket	Length=136	Times	tamp=15	:54:04.274332
Calls			25]	802.11 MAC Hea	ader Version=0 Type=%	10 Data Subty	e=%1000 QoS	Data D	uration=	48 Micro	osecon	ds Destinat	tion=B	ens Lap	top BSSID=Rou
Media		E T [26	5-127]	802.11 Encrypt	ted Data IV=0x1F0800 H	Extended IV=0		crypted	Data=(9	8 bytes	)				
			-												

ECS: FCS=0x02B8476E Calculated

#### Data transmission

- Some HT clients still using protection
- Unnecessary mgmt packets @ 24Mbps diminish WLAN efficiency



#### Wireless Is Slow - Retransmissions

Pa	Source	Destination	BSSID	Flags	Size Bar					
1949	2 10.8.0.175	2 10.4.58.73	ProximWire:4F:1B:06	5 +	802.11 Data IP	TCP				
1950	3 10.8.0.175	3 10.4.58.73	ProximWire:4F:1B:06	5 +	802.11 Data IP	TCP				
1951	3 10.4.58.73	3 10.8.0.175	ProximWire:4F:1B:06	5	802.11 Data IP	TCP	HTTP	. 🖃 🅴 Frame	Control Flags:	%00001010 [1]
1952	🧕 10.4.58.73	3 10.8.0.175	ProximWire:4F:1B:06	5 +	802.11 Data IP	TCP	HTTP	· 😙		0 Non-strict order
1953	3 10.4.58.73		ProximWire:4F:1B:06		802.11 Data IP	TCP	HTTP	· 🔗		.0 Non-Protected Frame
1954	3 10.4.58.73	3 10.8.0.175	ProximWire:4F:1B:06	5	802.11 Data IP	TCP	HTTP			
1955	😼 10.4.58.73	3 10.8.0.175	ProximWire:4F:1B:06	5	802.11 Data IP	TCP	HTTP	. 🐨		0 No More Data
1956	🧕 10.4.58.73	3 10.8.0.175	ProximWire:4F:1B:06	5 +	802.11 Data IP	TCP	HTTP	· 😙		0 Power Management - active mode
1957	😼 10.4.58.73	3 10.8.0.175	ProximWire:4F:1B:06	5	802.11 Data IP	TCP	HTTP	6		1 This is a Re-Transmission
1958	🧕 10.8.0.175	3 10.4.58.73	ProximWire:4F:1B:06	5	802.11 Data IP	TCP				
1959	🧕 10.8.0.175	3 10.4.58.73	ProximWire:4F:1B:06	5 C+	802.11 Data IP	TCP		9		
1960	🧕 10.8.0.175	3 10.4.58.73	ProximWire:4F:1B:06	5 +	802.11 Data IP	TCP		67		1. Exit from the Distribution System
1961	😼 10.4.58.73	3 10.8.0.175	ProximWire:4F:1B:06	5	802.11 Data IP	TCP	HTTP			0 Not to the Distribution System
1962	🧕 10.4.58.73	3 10.8.0.175	ProximWire:4F:1B:06	5 +	802.11 Data IP	TCP	HTTP	. 🖤		NOL LO LNE DISTRIBUTION System
1963	😼 10.4.58.73	3 10.8.0.175	ProximWire:4F:1B:06	5 +	802.11 Data IP	TCP	HTTP			
1964	😼 10.4.58.73	3 10.8.0.175	ProximWire:4F:1B:06	5	802.11 Data IP	TCP	HTTP			
1965	🧕 10.8.0.175	3 10.4.58.73	ProximWire:4F:1B:06	5 +	802.11 Data IP	TCP				
1966	3 10.4.58.73	3 10.8.0.175	ProximWire:4F:1B:06	5	802.11 Data IP	TCP	нттр			
1967	9 10.4.58.73	10.8.0.175	ProximWire:4F:1B:06	5	802.11 Data IP	TCP	HTTP			

Packe	Relative Time	IP ID	Expert	*		Packet	Relative Time	IP ID	Expert
	0.000000	3295				11	0.408702	3306	
	0.091011	18563			Γ	12	5.419631	3314	
	0.091014	3300			$ \Lambda$	13	5.420315	3314	
-	4 0.091017	3301			/ -	14	5.421547	3314	
	0.185298	18571		,	/ [	16	7.830755	3316	TCP Retransmission (2.409208 seconds from pack
	0.188321	18572		/		17	7.831347	3316	
	0.189393	3305			/ -	18	7.832359	3316	
	0.274432	18573				19	8.094958	19690	
	0.408863	3306				20	8.095627	3317	TCP Retransmission (2.674080 seconds from pack
1	5.421561	3314				21	8.201915	19696	
1	2 7.832377	3316	TCP Slow First Retransmission (2.410816 seconds		Γ	22	8.207849	19697	
- 1	8.094537	19690				23	8.208364	19697	
= 1	8.095559	3317	TCP Retransmission (2.673998 seconds from pack			24	8.209149	19697	
1	8.201252	19696				25	8.210565	19697	
1	8.207219	19697			_	26	8.213458	19697	
	0.040005	10000					0.040004	10000	

## **Analyzing Roaming Issues**

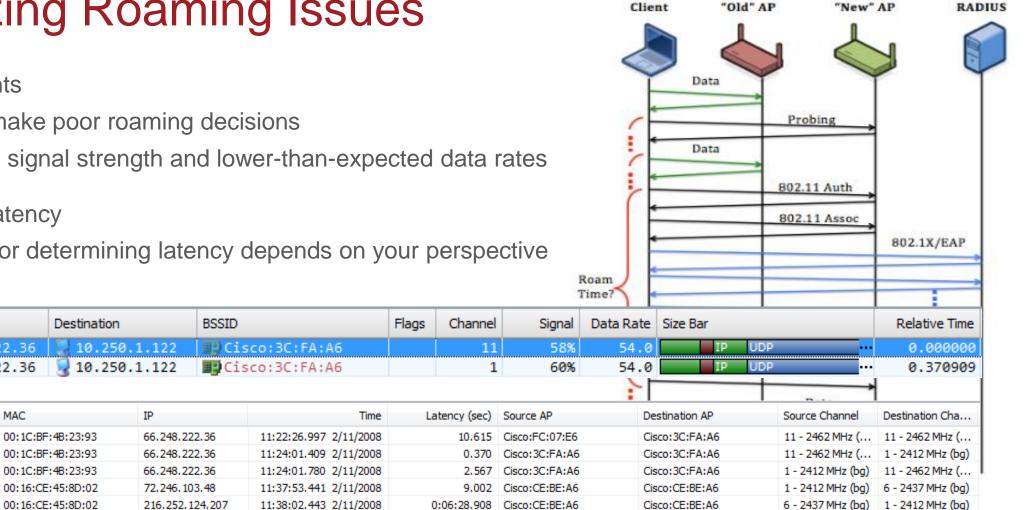
- Sticky clients
  - Clients make poor roaming decisions
  - Look for: signal strength and lower-than-expected data rates
- Roaming latency

66.248.222.36

66.248.222.36

MAC

Criteria for determining latency depends on your perspective



Certified Wireless Network Profes



Pa...

Name

2

Intel:48:23:93

Intel:48:23:93

Intel:48:23:93

HonHaiPrec:45:8D:02

HonHaiPrec:45:8D:02

Source



- Packet analysis is an essential part of any wireless engineer's toolkit
- In many cases packets are the ONLY way to determine the root cause of an issue
- Packet analysis doesn't always involve just looking at the packets themselves
- Don't assume portable, in-person analysis is your only choice



## **Thank You!**

Savvius, Inc. 1340 Treat Boulevard, Suite 500 Walnut Creek, CA 94597 (925) 937-3200

IT Professional Wi-Fi Trek 2015 #wifitrek Certified Wireless Network Professional