Interpreting Protocol Trace Files

Peter Mackenzie @mackenziewifi

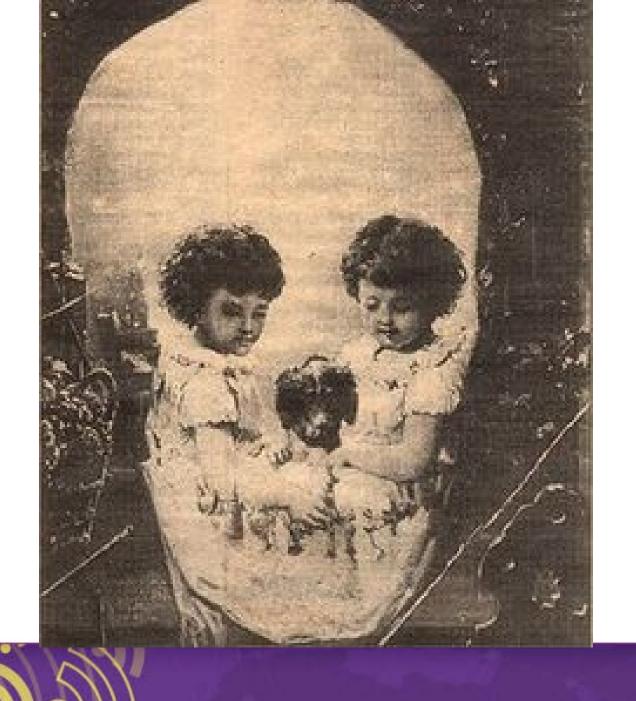






















Source	Destination	BSSID	Flags	Protocol	Signal dBm	Data Rate
Cisco:FC:C7:FF	Mobile Client	Access Point	W	802.11 WEP Data	-64	36.0
Cisco:FC:C7:FF	Mobile Client	<pre>Access Point</pre>	W+	802.11 WEP Data	-65	36.0
Cisco:FC:C7:FF	Mobile Client	<pre> Access Point </pre>	W+	802.11 WEP Data	-65	36.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-65	18.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-64	18.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-65	18.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-64	18.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-65	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-65	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-64	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-65	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-65	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-65	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-65	12.0
Mobile Client	Access Point	Access Point		802.11 Null Data	-41	11.0
Access Point	Mobile Client	(ren)	#	802.11 Ack	-59	2.0
Mobile Client	E Cisco:07:AC:96	Access Point	W	802.11 WEP Data	-43	11.0
Access Point	Mobile Client	(000)	#	802.11 Ack	-59	2.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W	802.11 WEP Data	-63	36.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-64	36.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	36.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-64	36.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	18.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	18.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	18.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	18.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-64	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-64	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	12.0
Mobile Client	Access Point	Access Point	44	802.11 Null Data	-41	11.0
Access Point	Mobile Client	(98) A D - i - +	#	802.11 Ack	-59	2.0
Mobile Client	Cisco:07:AC:96	Access Point	W #	802.11 WEP Data	-47	11.0
Access Point	Mobile Client	(90) Account Design		802.11 Ack	-60	2.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-64	36.0
Cisco:FC:C7:FF Cisco:FC:C7:FF	Mobile Client Mobile Client	Access Point Access Point	W+ W+	802.11 WEP Data 802.11 WEP Data	-63 -63	36.0 18.0
Cisco:FC:C7:FF		Access Point	W+	802.11 WEP Data	-63	18.0
	Mobile Client	Access Point	W+	802.11 WEP Data	-63	18.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+		-63	
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	12.0





Source	Destination	BSSID	Flags	Protocol	Signal dBm	Data Rate
Cisco:FC:C7:FF	Mobile Client	<pre>Access Point</pre>	W	802.11 WEP Data	- 64	36.0
Cisco:FC:C7:FF	Mobile Client	<pre>Access Point</pre>	W+	802.11 WEP Data	-65	36.0
EPCisco:FC:C7:FF	Mobile Client	<pre>Access Point</pre>	W+	802.11 WEP Data	-65	36.0
Cisco:FC:C7:FF	Mobile Client	<pre>Access Point</pre>	W+	802.11 WEP Data	-65	18.0
Cisco:FC:C7:FF	Mobile Client	<pre>Access Point</pre>	W+	802.11 WEP Data	-64	18.0
EDCisco:FC:C7:FF	Mobile Client	<pre>Access Point</pre>	W+	802.11 WEP Data	-65	18.0
Cisco:FC:C7:FF	Mobile Client	<pre>Access Point</pre>	W+	802.11 WEP Data	-64	18.0
Cisco:FC:C7:FF	Mobile Client	<pre>Access Point</pre>	W+	802.11 WEP Data	-65	12.0
Cisco:FC:C7:FF	Mobile Client	<pre>Access Point</pre>	W+	802.11 WEP Data	-65	12.0
Cisco:FC:C7:FF	Mobile Client	<pre>Access Point</pre>	W+	802.11 WEP Data	-64	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-65	12.0
Cisco:FC:C7:FF	Mobile Client	<pre>Access Point</pre>	W+	802.11 WEP Data	-65	12.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-65	12.0
EDCisco:FC:C7:FF	Mobile Client	<pre>Access Point</pre>	W+	802.11 WEP Data	-65	12.0
Mobile Client	Access Point	Access Point		802.11 Null Data	-41	11.0
Access Point	Mobile Client	_	#	802.11 Ack	-59	2.0
Mobile Client	ED Cisco:07:AC:96	Access Point	W	802.11 WEP Data	-43	11.0
Access Point	Mobile Client	_	#	802.11 Ack	-59	2.0
E Cisco:FC:C7:FF	Mobile Client	Access Point	W	802.11 WEP Data	-63	36.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	- 64	36.0
E Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-63	36.0
Cisco:FC:C7:FF	Mobile Client	Access Point	W+	802.11 WEP Data	-64	36.0





The Packets Never Lie! But often our interpretation of the packets do





Agenda

- Which channel?
- Which packets should be acknowledged?
- What do corrupted packets mean?
- How important is location?
- Where is my data?
- Getting the complete picture



Which channel?





Where we see channel information?

									vode	Туре	Charinei 🔺 band		Encryption	
Source	Destination	BSSID	Flags	Signal dBm	Data Rate	Delta Time Protocol	Channel	Size [✓ ● Riverwalk NOLA	ESSID	1, 3, 60, 132			Ι
■ Cisco:43:3F:60	Ethernet Broadcast	Cisco:43:3F:60	*	-44	12.0	0.006232 802.11 Beacon	6	246	6C:AA:B3:03:D5:18	AP	1 802.:	11b		ı
_	_	_	#CW+	-84	6.0	0.004749 802.11 Control	6	34 F	6C:AA:B3:05:33:48	AP	3 802,	11h		Ti
Cisco:1A:6F:40	Ethernet Broadcast	Cisco:1A:6F:40	*PC	-84	1.0	0.007421 802.11 Beacon	6	231 F						i.
06:18:0A:79:F0:D6	Ethernet Broadcast	## 06:18:0A:79:F0:D6	*P	-77	1.0	0.002924 802.11 Beacon	6	253 F	6C:AA:B3:05:33:4C	AP	60 <mark>8</mark> 02.	11a		L
84:18:3A:15:5A:38	Ethernet Broadcast	84:18:3A:15:5A:38	*	-69	12.0	0.000159 802.11 Beacon	6	177 F	6C:AA:B3:03:D5:1C	AP	132 802.	11a		l.
84:18:3A:55:5A:38	Ethernet Broadcast	84:18:3A:55:5A:38	*	-69	12.0	0.000156 802.11 Beacon	6	177 F	✓ ● HHCOperations	ESSID	1, 3, 60, 132			
DA:E4:54:9D:07:00	## 84:18:3A:56:06:A8		C+	-83	24.0	0.001331 802.11 QoS CF-Poll	. 6	36 F						
TCisco:1A:6F:44	Ethernet Broadcast		*	-84	1.0	0.007513 802.11 Beacon	6	209 F	6C:AA:B3:43:D5:18	AP	1 802.	11b	CCMP	L
Cisco:1A:6F:42	Ethernet Broadcast	Cisco:1A:6F:42	*P	-89	1.0	0.013074 802.11 Beacon	6	231	6C:AA:B3:45:33:48	AP	3 802,	11b	CCMP	1
■ 0A:18:0A:79:F0:D6	Ethernet Broadcast		*	-79	1.0	0.003006 802.11 Beacon	6	199 F						4.
@0C:27:24:E6:16:01	Ethernet Broadcast	@0C:27:24:E6:16:01	*PC	-80	12.0	0.000254 802.11 Beacon	6	290 F	6C:AA:B3:45:33:4C	AP	60 802.	11a	CCMP	, L
_	6C:8D:C1:55:E3:BD		#	-86	24.0	0.004208 802.11 CTS	6	14	6C:AA:B3:43:D5:1C	AP	132 802.	11a	CCMP	L
84:18:3A:16:06:A8	6C:8D:C1:55:E3:BD		#	-85	24.0	0.000007 802.11 BA	6	32 F	✓ ● Guests	ESSID	1, 149			
	## E8:50:8B:CB:CD:30		#	-86	24.0	0.002492 802.11 Ack	6	14 (_					
## A6:2B:87:FB:98:28		1C:1D:1F:6E:6B:3E		-69	12.0	0.001934 802.11 Data	6	290	CC: 16: 7E: 52: B1: A1	AP	1 8 <mark>02.</mark> :	11b		L
Meraki:79:F0:D6	Ethernet Broadcast	■ Meraki:79:F0:D6	*P	-74	1.0	0.042629 802.11 Beacon	7	253	CC: 16: 7E: 52:B1: AE	AP	149 802.	11a		Ti
WILLS 40 04 70 70 70	Xerox:00:00:00	WILLS 40 04 70 50 DC	#	-42	1.0	0.012262 802.11 Ack		14 1						-
0A:18:0A:79:F0:D6	Ethernet Broadcast			-75	1.0	0.040196 802.11 Beacon		199 1	✓ ● W2L3	ESSID	1, 149			
Meraki:79:F0:D6	Ethernet Broadcast	Meraki:79:F0:D6	*P	-75	1.0	0.049946 802.11 Beacon	/	253 F	CC: 16: 7E: 52:B1:A0	AP	1 802,	11b	CCMP	l.
Cisco:1A:6F:45	FF:FF:FF:FF:3F:93 Xerox:00:00:00	EP C8:F9:39:76:6F:45	*PC	-83 -83	1.0	0.008336 802.11 Beacon 0.003875 802.11 Ack	/	231 F	CC:16:7E:52:B1:AF	AP	149 802.		CCMP	
■ 06:18:0A:79:F0:D6	Ethernet Broadcast	WINGS, 18, 04, 70, 50, DC	# *p	-83	1.0	0.003875 802.11 ACK 0.013386 802.11 Beacon	/	253 F				11a	CCMP	- 1
## 0A:18:0A:79:F0:D6	Ethernet Broadcast	06:18:0A:79:F0:D6	*P	-74	1.0	0.025206 802.11 Beacon		199	✓ ☐ IT Admin	ESSID	1, 6, 11			
Cisco:1A:6F:42	FF:FF:33:61:F2:FF	E C8:61:F4:1A:6F:42	*PC	-73	1.0	0.002059 802.11 Beacon	7	231	√	AP	1 802,	11ba	TKIP	
CISCO.IA.OI.42	Xerox:00:00:00	mg*C8.01.14.1A.01.42	# .	-//	1.0	0.002033 802.11 Beacon	,	231 7	00.27.2 1.20.30.21			-	TICLE	-
Meraki:79:F0:D6	Ethernet Broadcast	Meraki:79:F0:D6	*P	Pac	ket Ir	nfo.				STA	1 802.	11bg		L
Cisco:1A:6F:45	Ethernet Broadcast	Cisco:1A:6F:45	*C	iar .						STA	1 802.	11ba		L
	Xerox:00:00:00	25 61360121101113	#		Packet	: Number:	288			AP		-		т.
■ 5C:E0:C5:EF:50:A1	Ethernet Broadcast	Ethernet Broadcast	*								1 802.	1100		
06:18:0A:79:F0:D6	Ethernet Broadcast	## 06:18:0A:79:F0:D6	*PC	(P)	Flags:		0x00	000000		AP	1 802.:	11bg	TKIP	- L
0A:18:0A:79:F0:D6	Ethernet Broadcast		*							AP	6 802.	11ba	TKIP	Ti-
Meraki:79:F0:D6	Ethernet Broadcast		*P	9 9	Status	:	0x00	000000					TIXE	-
_	EXerox:00:00:00	_	#	_						STA	6 8 <mark>02.</mark> :	11bg		L
■ 06:18:0A:79:F0:D6	Ethernet Broadcast	## 06:18:0A:79:F0:D6	*P	⊘	Packet	: Length:	113			AP	6 802.	11ba	TKIP	ı
■ 0A:18:0A:79:F0:D6	Fthernet Broadcast	■ 0A:18:0A:79:F0:D6					14.4	2.31 010036500 0	0/10/2016	AP	11 802.			
				90	Timest	amp:	14:4	2:31.019826500 0	0/12/2010					4
				(A) 1	Data R	ate:	2	1.0 Mbps		AP	11 802.	11bg		U
			Г						1					
				9 (Channe	:1:	2 2	417MHz 802.11b		_				
				9 9	Signal	Level:	100%	5						
				_	Signal		-47							
					_	Level:	10%							
The same of the sa														
				(A)	Noise	dBm:	-86							



Channel Information – Beacon

```
Packet Info
  Packet Number:
                       288
  Flags:
                       0x000000000
  0x00000000
  Packet Length:
                    113
                                                          Channel the packet was capture on
  Timestamp:
                  14:42:31.019826500 08/12/2016
  Data Rate:
                          1.0 Mbps
                      2 42417MHz 802.11b
  Signal Level:
                      100%
  Signal dBm:
                       -47
  Noise Level:
                       10%
                                                     Channel the packet was transmitted on
  Noise dBm:
                       -86
                        □ Interpret Sequence Parameter Set
                               Element ID:
                                                      3 Direct Sequence Parameter Set [60]
                               Length:
```

1 [62]

Channel:



Which packets should be acknowledged?





CTS / ACK

```
□ 📅 802.11 MAC Header
     Version:
                            0 [0 Mask 0x03]
     Type:
                            %01 Control [0 Mask 0x0C]
     Subtype:
                            %1100 Clear To Send (CTS) [0 Mask 0xF0]
  ☐ Frame Control Flags: %00000000 [1]
                               0... Non-strict order
                               .0.. .... Non-Protected Frame
                               ..0. .... No More Data
                               ...0 .... Power Management - active mode
                               .... 0... This is not a Re-Transmission
                               .... .0.. Last or Unfragmented Frame
                               .... .. 0. Not an Exit from the Distribution System
                               .... ... 0 Not to the Distribution System
     Duration:
                            118 Microseconds [2-3]
     Receiver:
                            A8:5B:78:3B:6A:16 [4-9]
□ FCS - Frame Check Sequence
     FCS:
                            0x9D871EAF [10-13]
```

```
□ 🕯 802.11 MAC Header
     Version:
                            0 [0 Mask 0x03]
     Tvpe:
                            %01 Control [0 Mask 0x0C]
     Subtype:
                            %1101 Acknowledgment (ACK) [0 Mask 0xF0]
  ☐ Frame Control Flags: %00000000 [1]
                               0... Non-strict order
                               .0.. .... Non-Protected Frame
                               ..0. .... No More Data
                               ...0 .... Power Management - active mode
                               .... 0... This is not a Re-Transmission
                               .... .0.. Last or Unfraamented Frame
                               .... .. 0. Not an Exit from the Distribution System
                               .... ... 0 Not to the Distribution System
     Duration:
                            0 Microseconds [2-3]
    Receiver:
                            A8:5B:78:3B:6A:16 [4-9]
☐ 🏋 FCS - Frame Check Sequence
     FCS:
                            0x629E8FE2 [10-13]
```





Client Troubleshooting

Packet	Source	Destination		Flags	Channel	Signal dBm	Data Rate	Protocol
1268	∰ Wireless Cl	ient 🔛 Wirele	ss AP	*	112	-57	6.0	802.11 Auth
1269	■₩Wireless AP	Wirele	ss Client	#	112	-61	6.0	802.11 Ack
1270	■ Wireless AP	Wirele	ss Client	*	112	-61	6.0	802.11 Auth
1271	💹 Wireless Cl	lient Wirele	ss AP	*	112	-55	6.0	802.11 Assoc Req
1272	■₩ Wireless AP	Wirele	ss Client	#	112	-62	6.0	802.11 Ack
1273	■ Wireless AP	Wirele	ss Client	*	112	-61	6.0	802.11 Assoc Rsp
1274	■ Wireless AP	Wirele	ss Client	*	112	-62	6.0	802.11 Action
1275	■ Wireless AP	Wirele	ss Client		112	-64	6.0	EAP Request





Acknowledgment

```
Packet Info
  Packet Number:
                          1300
   Flags:
                           0x00000001
  Status:
                          0x00000000
  Packet Length:
  Timestamp:
                          13:23:39.594567900 01/22/2015
   Data Rate:
                          12 6.0 Mbps
   Channel:
                          112 5560MHz 802.11a

    Signal Level:

  Signal dBm:
                          -63
   Noise Level:

    Noise dBm:

                           -5
📅 802.11 MAC Header
  Version:
                          0 [0 Mask 0x03]
  Type:
                          %01 Control [0 Mask 0x0C]
  Subtype:
                          %1101 Acknowledgment (ACK) [0 Mask 0xF0]
☐ $\frac{1}{3}$ Frame Control Flags: %00000000 [1]
                             0... Non-strict order
                             .0.. .... Non-Protected Frame
                             ..0. .... No More Data
                             ...0 .... Power Management - active mode
                             .... 0... This is not a Re-Transmission
                             .... .O.. Last or Unfragmented Frame
                             .... .. 0. Not an Exit from the Distribution System
                             .... ... 0 Not to the Distribution System
  Duration:
                          14 Microseconds [2-3]
  Receiver:
                          2C:F0:EE:DC:07:01 Wireless Client [4-9]
🚏 FCS - Frame Check Sequence
  FCS:
                           0x699CD512 Calculated
```





What do corrupted packets mean?





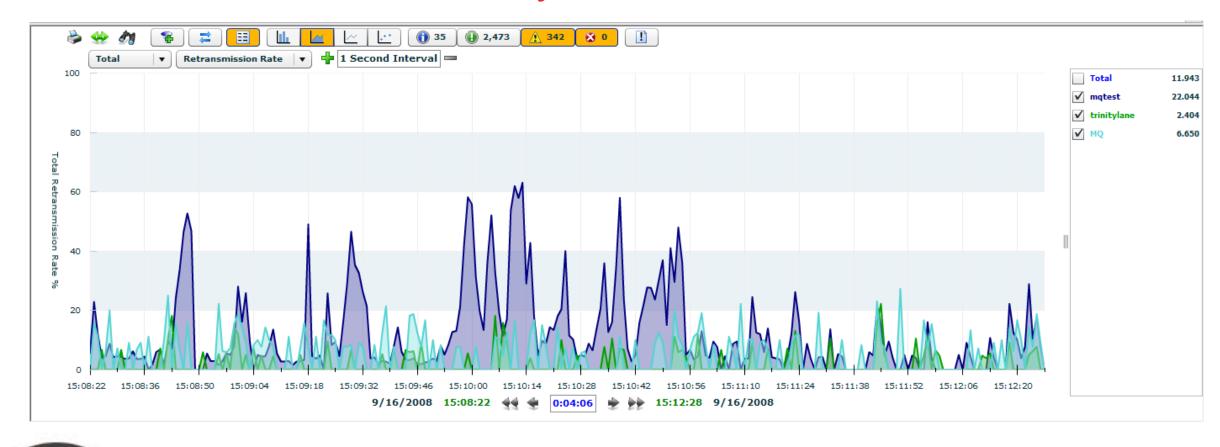
CRC Errors

acket	Source	Destination	Flags	Channel	Signal dBm	Data Rate	Protocol
1200		B0:16:80:26:F6:63	#C	8	-65	36.0	802.11 Ack
1201	33:05:7D:BC:67:4B	2D:2E:B9:56:F6:DC	*CW	8	-63	18.0	802.11 Deauth
1202	2F:DD:AD:8A:7B:91	■ A3:96:3C:C6:09:A0	CW+	8	-65	18.0	802.11 Frag
1203	■ D9:17:F2:14:31:6B	ME:58:A7:7F:49:41	CW+	8	-63	12.0	802.11 Frag
1204			C+	8	-65	48.0	802.11
1205	34:E3:9A:EC:83:A2	56:DD:67:31:75:58	CW	8	-63	48.0	802.11 Frag
1206	<pre>## 0F:00:8B:85:81:DB</pre>	<pre>6D:B7:38:3F:5E:42</pre>	CW+	8	-64	18.0	802.11 Frag
1207	CC:EC:4C:84:E9:40	38:C5:08:B7:98:09	*CW+	8	-65	12.0	802.11 Management
1208	AB:A5:0B:57:33:EA	80:94:F0:B2:AA:75	*C+	8	-65	36.0	802.11 Probe Req
1209	B1:A0:7F:2A:1D:AC	<pre>## 6D:E6:89:45:C1:C1</pre>	*C+	8	-64	54.0	802.11 Management
1210			CW+	8	-64	48.0	802.11
1211	85:73:62:44:CA:AB	■ 0B:C0:29:0B:0F:9F	CW+	8	-65	54.0	802.11 Frag
1212	## 46:19:DD:47:37:22	2D:4F:AD:D5:C4:59	C+	8	-67	18.0	802.11 Null Data
1213		## 42:8D:30:22:51:F8	#C	8	-64	18.0	802.11 CTS
1214			#C+	8	-66	48.0	802.11 Control
1215	CD:94:4F:90:E2:E4	1C:A4:40:10:AE:B3	C+	8	-66	48.0	802.11 Frag
1216	379:95:85:A5:D3:21	E9:59:11:08:B0:11	#CW+	8	-64	48.0	802.11 BAR
1217	37B:8E:8F:32:04:87	## 4F:3E:65:5F:59:03	*C+	8	-65	48.0	802.11 Management
1218	D1:91:6C:F0:7F:1B	2D:05:78:2F:13:BB	*C	8	-64	18.0	802.11 Assoc Rsp
1219	E6:CE:89:21:2D:98	11:13:E8:E4:02:29	*CW	8	-64	18.0	802.11 Reassoc Req
1220	CD:EE:89:AC:48:BF	■ D6:C7:71:3D:37:ED	CW	8	-64	48.0	802.11 Frag
1221	■ A8:7B:AC:C2:F9:07	BD:CB:40:7E:F8:56	*CW	8	-64	12.0	802.11 Disassoc
1222	<pre>62:99:10:84:B5:72</pre>	24:ED:C8:33:1A:3B	#C	8	-65	18.0	802.11 Control





Retries tell a better story







How important is location?

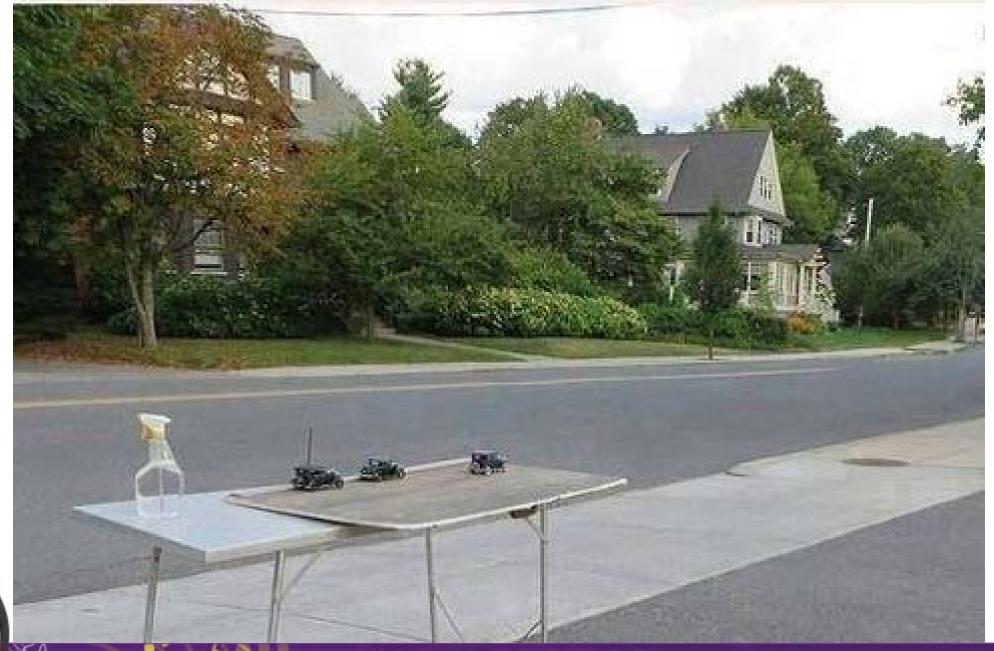
















Capture location







Capture location



Is there a problem?



Where is my data?





No data

	Source	Destination	Protocol	Delta Time	
	Meru:02:5B:A2	■D4:F4:6F:05:E6:74	802.11 RTS	0.000491	
Missing Data ——	■ D4:F4:6F:05:E6:74	■■ Meru:02:5B:A2	802.11 CTS	0.000000	
Missing Data ——	mp D4:F4:6F:05:E6:74	Meru:02:5B:A2	802.11 BA	0.001636	
	D4:F4:6F:05:E6:74	Meru:02:5B:A2	802.11 RTS	0.000000	
	Meru:02:5B:A2	D4:F4:6F:05:E6:74	802.11 CTS	0.000002	
	Meru:02:5B:A2	■ D4:F4:6F:05:E6:74	802.11 BA	0.000245	
	Meru:02:5B:A2	D4:F4:6F:05:E6:74	802.11 RTS	0.000120	
	D4:F4:6F:05:E6:74	Meru:02:5B:A2	802.11 CTS	0.000001	Duration time
	D4:F4:6F:05:E6:74	Meru:02:5B:A2	802.11 BA	0.001506	between CTS and
	D4:F4:6F:05:E6:74	Meru:02:5B:A2	802.11 RTS	0.000001	
	■■ Meru:02:5B:A2	■D4:F4:6F:05:E6:74	802.11 CTS	0.000000	Block Ack is an
	■■ Meru:02:5B:A2	■D4:F4:6F:05:E6:74	802.11 BA	0.000117	indication of the
	Meru:02:5B:A2	■ D4:F4:6F:05:E6:74	802.11 RTS	0.000250	data transmission
	■ D4:F4:6F:05:E6:74	Meru:02:5B:A2	802.11 CTS	0.000001	
	■ D4:F4:6F:05:E6:74	Meru:02:5B:A2	802.11 BA	0.001504	
	D4:F4:6F:05:E6:74	Meru:02:5B:A2	802.11 RTS	0.000001	
	■■ Meru:02:5B:A2	■D4:F4:6F:05:E6:74	802.11 CTS	0.000001	
	■■ Meru:02:5B:A2	■D4:F4:6F:05:E6:74	802.11 BA	0.000241	
	Meru:02:5B:A2	■D4:F4:6F:05:E6:74	802.11 RTS	0.000001	
	III D4:F4:6F:05:E6:74	Meru:02:5B:A2	802.11 CTS	0.000001	
	■ D4:F4:6F:05:E6:74	Meru:02:5B:A2	802.11 BA	0.001380	
	D4:F4:6F:05:E6:74	Meru:02:5B:A2	802.11 RTS	0.000001	
	■■Meru:02:5B:A2	■D4:F4:6F:05:E6:74	802.11 CTS	0.000001	
Total Control	Meru:02:5B:A2	■D4:F4:6F:05:E6:74	802.11 BA	0.000243	



MU-MIMO Data Exchange

	Source	Destination	Protocol	Decode: Subtype	Delta Time
	Access Point MU	Ethernet Broadcast	802.11 Control	%0101 VHT NDP Announcement	0.000558
N. 611 C 11	Client #3	<pre>Access Point</pre>	802.11 Management	%1110 Action No Ack	0.000542
MU Sounding	Access Point MU	<pre>Selient #1</pre>	802.11 Control	%0100 Beamforming Report Poll	0.000009
Exchange	<pre>Client #1</pre>	<pre>Access Point</pre>	802.11 Management	%1110 Action No Ack	0.000512
	Access Point MU	<pre>Sillient #2</pre>	802.11 Control	%0100 Beamforming Report Poll	0.000009
MU Data —	Client #2	<pre>Access Point</pre>	802.11 Management	%1110 Action No Ack	0.001988
MO Data —	Client #3	<pre>Access Point</pre>	802.11 BA	%1001 Block Acknowledgement (BlockAck)	0.001901
	Access Point	<pre>Silent #1</pre>	802.11 BAR	%1000 Block Acknowledgement Request (BlockAckReq)	0.000008
Data Ack —	Client #1	<pre>Access Point</pre>	802.11 BA	%1001 Block Acknowledgement (BlockAck)	0.000004
	Access Point	<pre>Sillient #2</pre>	802.11 BAR	%1000 Block Acknowledgement Request (BlockAckReq)	0.000005
	Client #2	<pre>Access Point</pre>	802.11 BA	%1001 Block Acknowledgement (BlockAck)	0.000026
	Client #2	Access Point	802.11 CTS	%1100 Clear To Send (CTS)	0.000187
	Client #3	<pre>Access Point</pre>	802.11 BA	%1001 Block Acknowledgement (BlockAck)	0.001934
	Access Point	Client #1	802.11 BAR	%1000 Block Acknowledgement Request (BlockAckReq)	0.000009
	Client #1	<pre>Access Point</pre>	802.11 BA	%1001 Block Acknowledgement (BlockAck)	0.000004
	<pre>Access Point</pre>	Client #2	802.11 BAR	%1000 Block Acknowledgement Request (BlockAckReq)	0.000028
	Client #2	<pre>Access Point</pre>	802.11 BA	%1001 Block Acknowledgement (BlockAck)	0.000004
	<pre>Selient #2</pre>	<pre>Access Point</pre>	802.11 CTS	%1100 Clear To Send (CTS)	0.000207

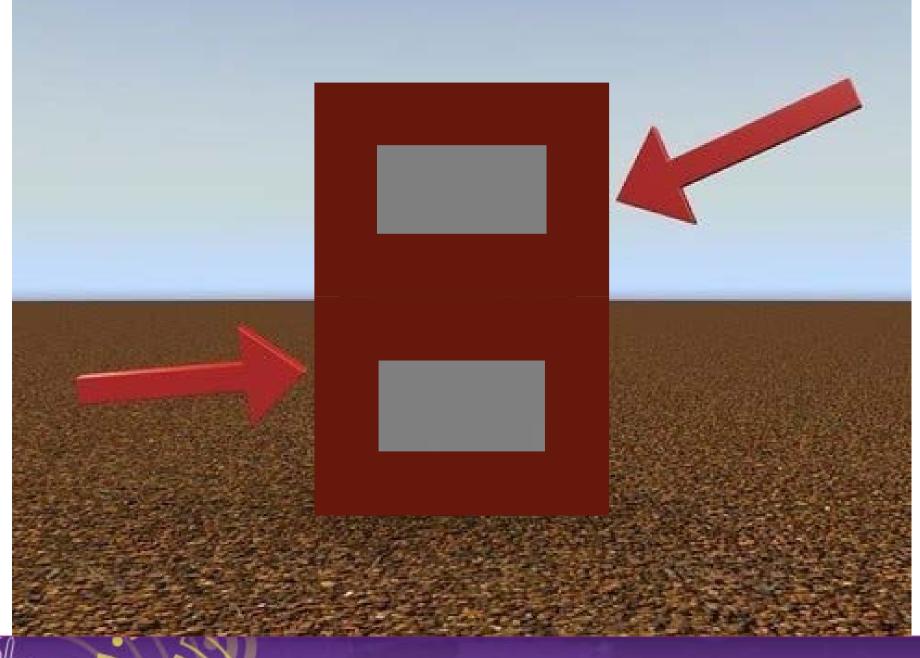




Getting the complete picture



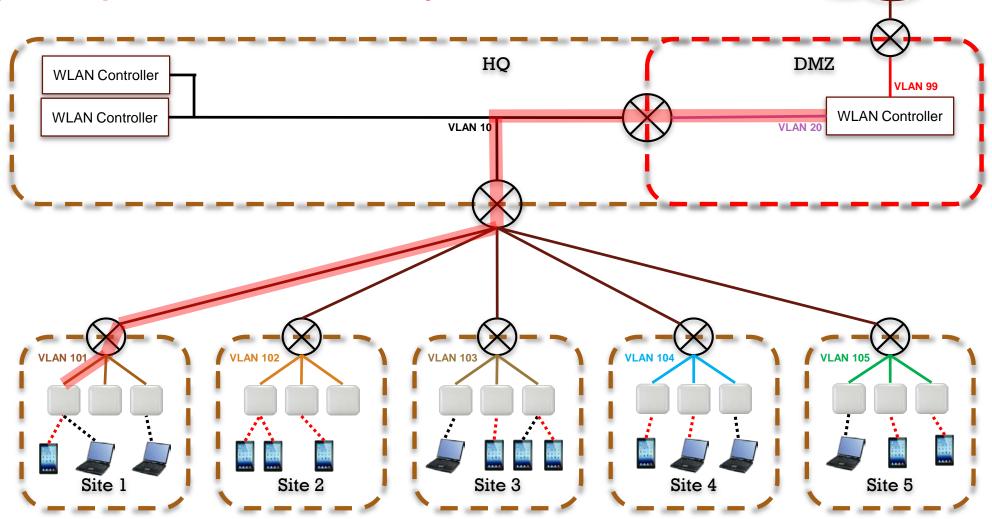


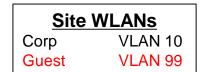






Know your protocol, know your network

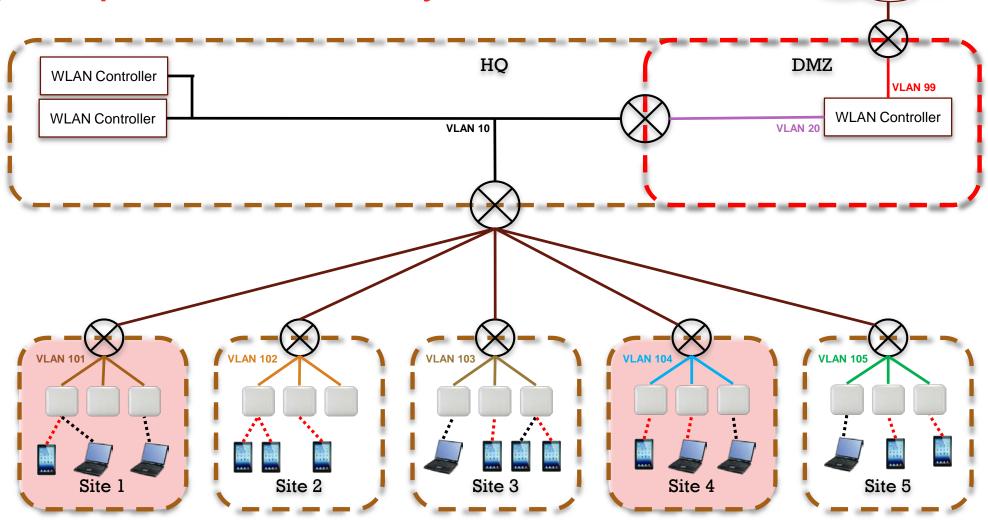


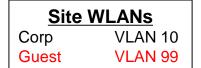






Know your protocol, know your network









Each location provides a different view HQ DMZWLAN Controller **VLAN 99** WLAN Controller WLAN Controller **VLAN 10 VLAN 20** AP Capture - VAN 99 **Controller Capture VLAN 99** DHCP Discover DHCP Discover DHCP Offer DHCP Discover **VLAN 103 VLAN 104 VLAN 105 Wireless Capture** DHCP Discover DHCP Discover Site 1 Site 2 Site 3 Site 4 Site 5



Each location provides a different view



VLAN 99

WLAN Controller

DMZ

VLAN 20

AP Capture – Filter: Dropped Packets

Packet 1:

Time: 14:12:18.565600, Len: 324, 802.3, Proto: 0x0800, Vlan: 343, Priority: 0, Ingress: extvlan,

vlan343, 13_off: 18, 14_off: 38

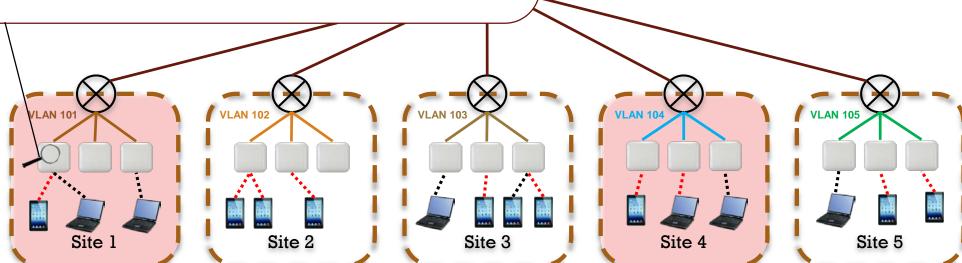
DropReason: wireless client-to-client disallow(228)

802.3:00-04-96-35-01-87 > D8-BB-2C-30-09-68, 802.11p pri 0, 802.11q vlan 343, protocol 0x0800

IPv4: 10.187.36.2 > 10.187.37.92, proto UDP, IPv4 length 306, DSCP 0, Id 0, DF

UDP: ports 67 > 68, data length 286

DHCP: Offer from 0.0.0.0 to D8-BB-2C-30-09-68 of 10.187.37.92/255.255.254.0



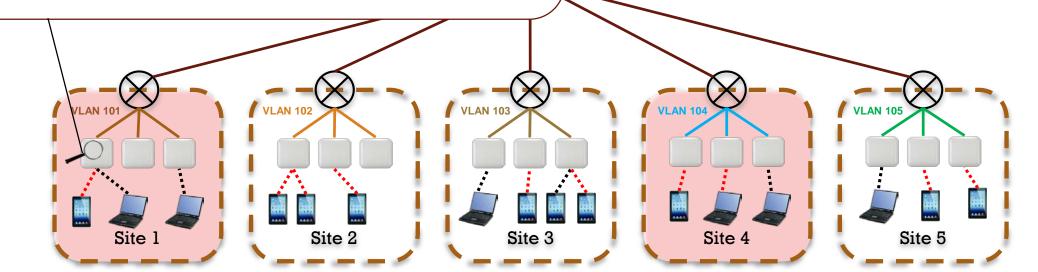




Each location provides a different view

Forwarding Database - Analsyis

#more system:/proc/dataplane/bridge/fdb | grep 00-04-96-35-01-87 [1259.0 key 3fe5] 00-04-96-35-01-87 vlan 343 -> Tunnel to 46.4A.B5.8C, 296 sec to live, wireless-client





DMZ

VLAN 20

VLAN 99

WLAN Controller

Thank you!



