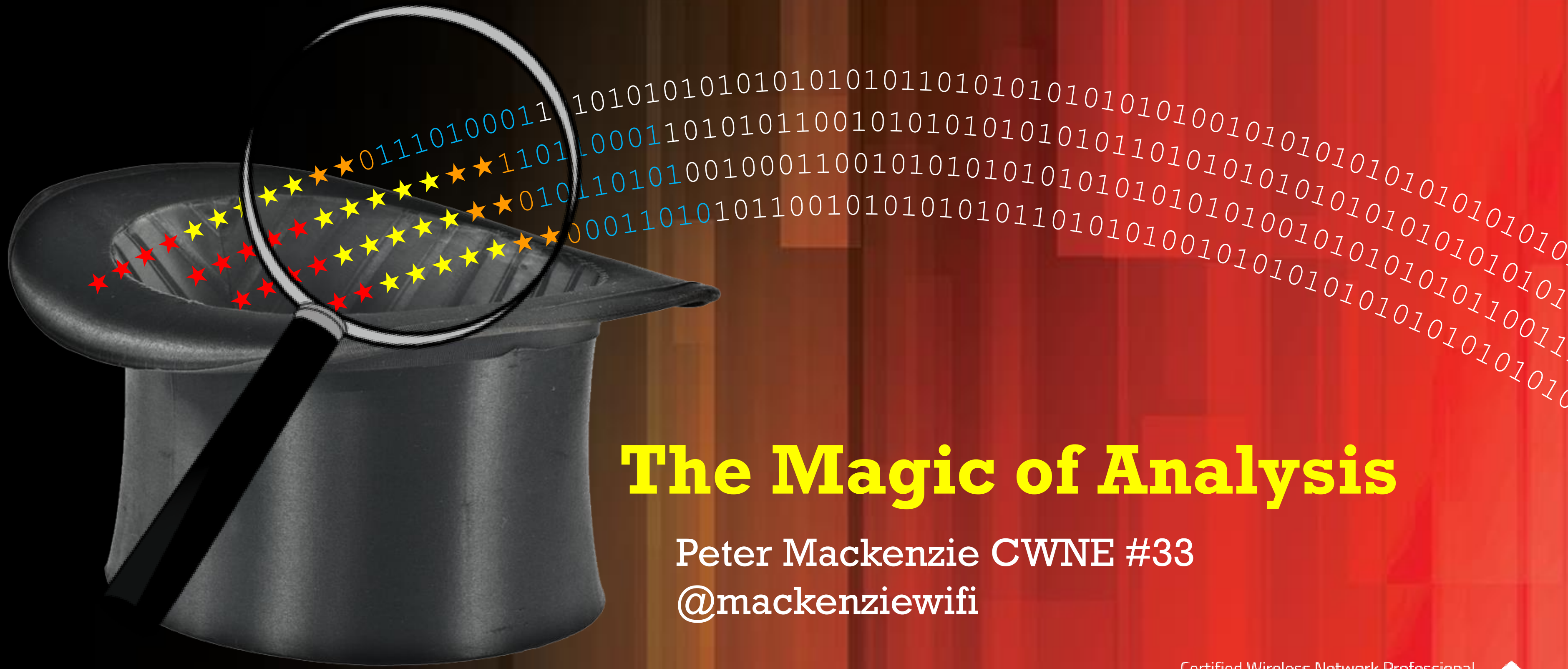


The Magic of Analysis

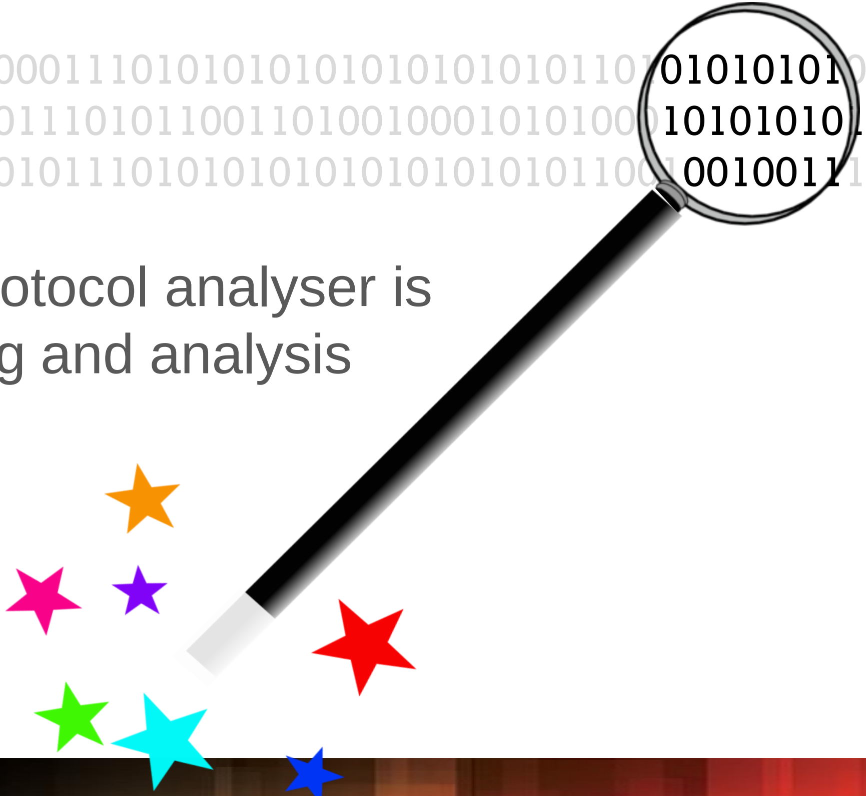
Peter Mackenzie CWNE #33
@mackenziewifi

IT Professional Wi-Fi Trek 2015
#wifitrek

Certified Wireless Network Professional
cwnp

Your Magic Wand

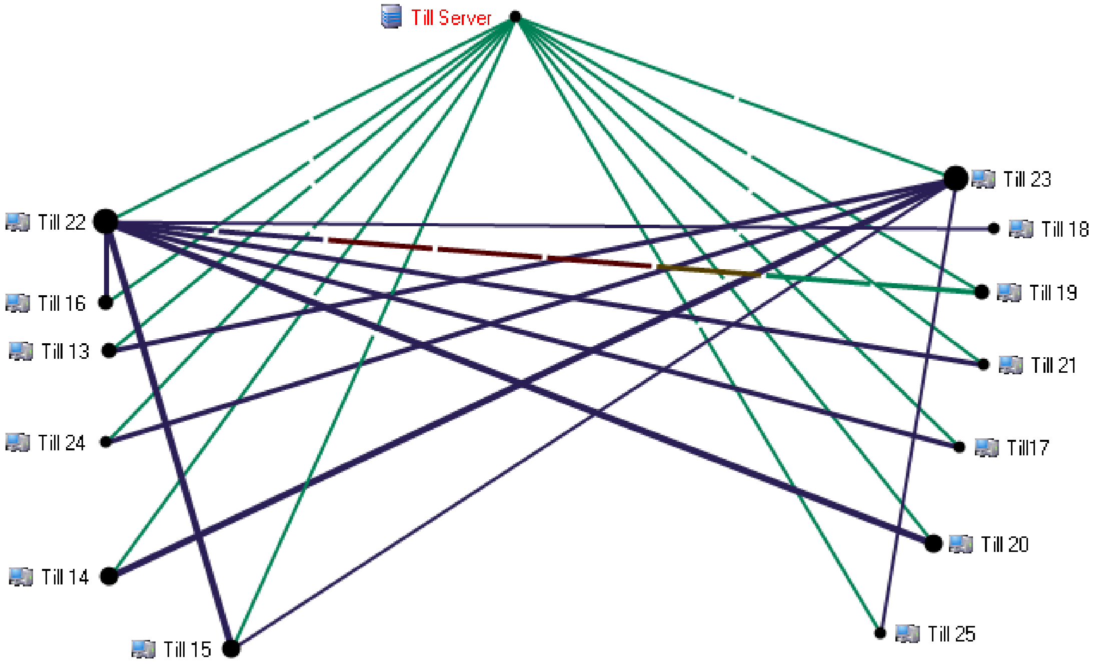
Used correctly, a protocol analyser is your troubleshooting and analysis magic wand



Power and Limitation of a Protocol Analyser

- The packets never lie!
  - Lets you see exactly what is happening on your network
- You can only see the packets
  - If your problem is not manifested in the packets, you will not see it.
    - For Wi-Fi, a Spectrum Analyser is also a key troubleshooting tool
  - Sometimes the lack of packets can point you in the right direction

POS Cross-Chatter – Who’s Talking To Who?



When to Capture?

- Troubleshooting
  - Protocol analysers shouldn’t only be used as a last resort
- Performance Analysis
- Baselining
  - What is normal
  - Understanding the 802.11 environment
- Education
  - Finding out how things work

Troubleshooting Methodology

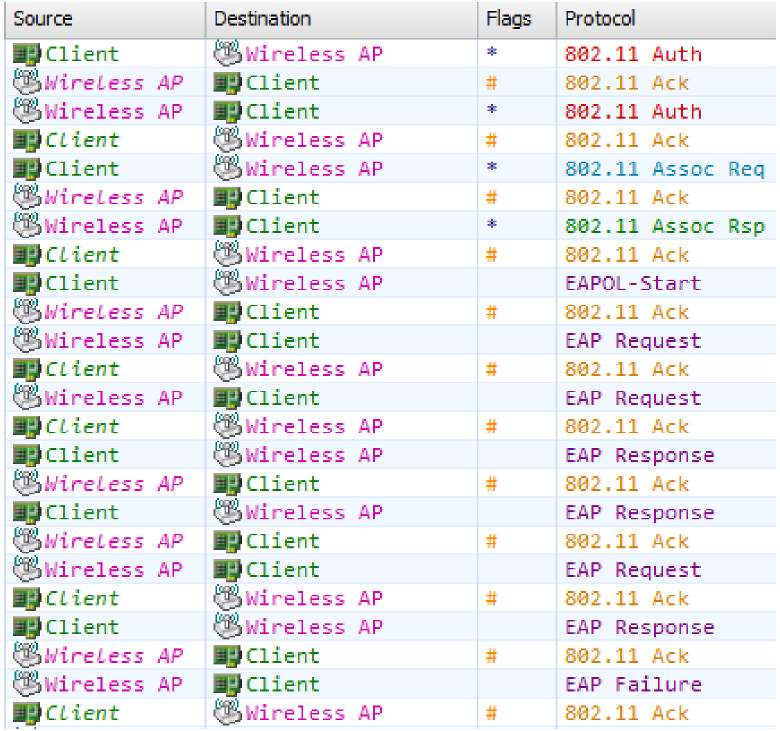
- Assume nothing
  - Talk to the end users experiencing the problem
  - Observe the problem
- A bit like real detective work
  - Look for leads and then follow them

Troubleshooting Methodology

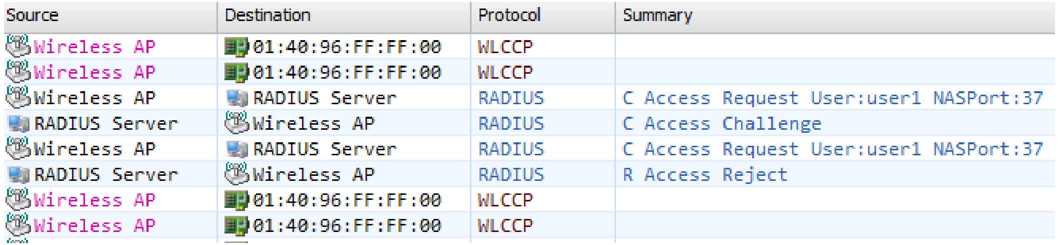
- Looking for leads
  - Suspicious protocols, nodes & conversations
  - Anything abnormal (Know what is normal)
    - Know your protocol
    - Baseline
- Following leads
  - Filtering
  - Select-related
  - More captures

Know Your Protocol

- Wireless and Wired



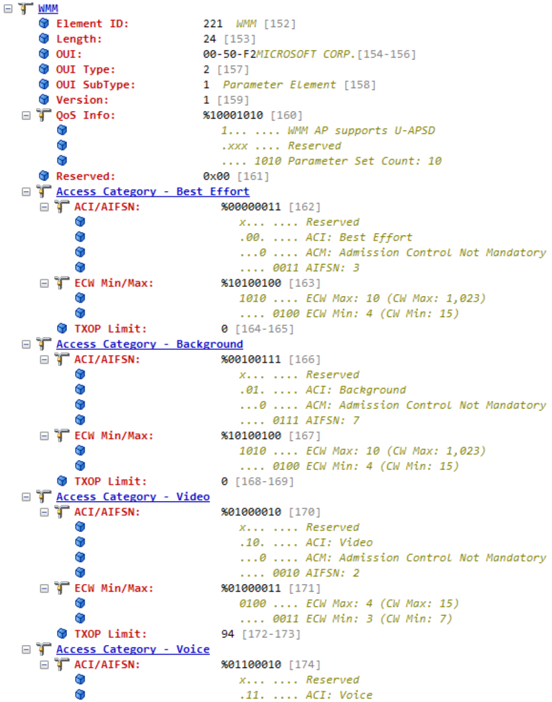
Source	Destination	Flags	Protocol
Client	Wireless AP	*	802.11 Auth
Wireless AP	Client	#	802.11 Ack
Wireless AP	Client	*	802.11 Auth
Client	Wireless AP	#	802.11 Ack
Client	Wireless AP	*	802.11 Assoc Req
Wireless AP	Client	#	802.11 Ack
Wireless AP	Client	*	802.11 Assoc Rsp
Client	Wireless AP	#	802.11 Ack
Client	Wireless AP		EAPOL-Start
Wireless AP	Client	#	802.11 Ack
Wireless AP	Client		EAP Request
Client	Wireless AP	#	802.11 Ack
Wireless AP	Client		EAP Request
Client	Wireless AP	#	802.11 Ack
Client	Wireless AP		EAP Response
Wireless AP	Client	#	802.11 Ack
Client	Wireless AP		EAP Response
Wireless AP	Client	#	802.11 Ack
Wireless AP	Client		EAP Request
Client	Wireless AP	#	802.11 Ack
Client	Wireless AP		EAP Response
Wireless AP	Client	#	802.11 Ack
Wireless AP	Client		EAP Failure
Client	Wireless AP	#	802.11 Ack



Source	Destination	Protocol	Summary
Wireless AP	01:40:96:FF:FF:00	WLCCP	
Wireless AP	01:40:96:FF:FF:00	WLCCP	
Wireless AP	RADIUS Server	RADIUS	C Access Request User:user1 NASPort:37
RADIUS Server	Wireless AP	RADIUS	C Access Challenge
Wireless AP	RADIUS Server	RADIUS	C Access Request User:user1 NASPort:37
RADIUS Server	Wireless AP	RADIUS	R Access Reject
Wireless AP	01:40:96:FF:FF:00	WLCCP	
Wireless AP	01:40:96:FF:FF:00	WLCCP	

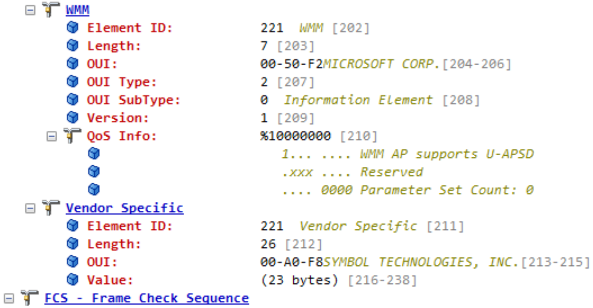
Vendor Differences - Example

- Cisco – Beacon
  - WMM Parameter Element

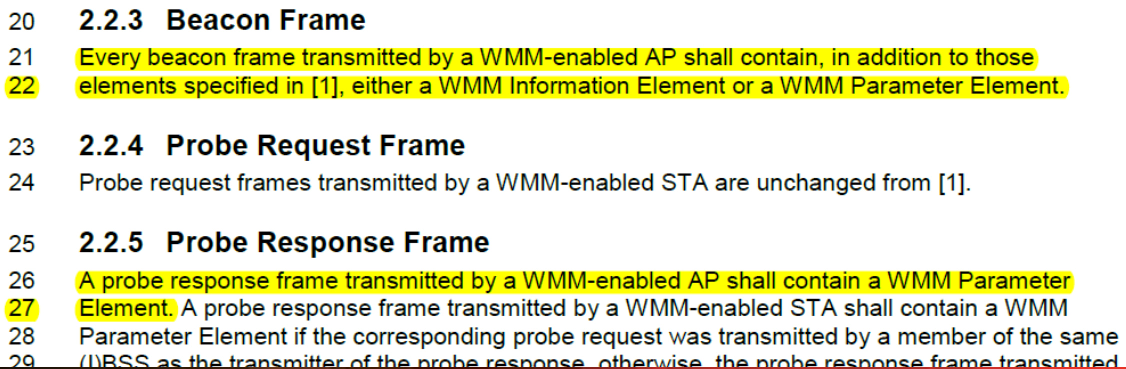


```
⊟ WMM
    Element ID:            221  WMM [152]
    Length:                24 [153]
    OUI:                   00-50-F2MICROSOFT CORP.[154-156]
    OUI Type:              2 [157]
    OUI SubType:           1  Parameter Element [158]
    Version:               1 [159]
  ⊟ QoS Info:              %10001010 [160]
                             1... .... WMM AP supports U-APSD
                             .xxx .... Reserved
                             .... 1010 Parameter Set Count: 10
    Reserved:              0x00 [161]
  ⊟ Access Category - Best Effort
    ⊟ ACI/AIFSN:             %00000011 [162]
                               x... .... Reserved
                               .00. .... ACI: Best Effort
                               ...0 .... ACM: Admission Control Not Mandatory
                               .... 0011 AIFSN: 3
    ⊟ ECW Min/Max:           %10100100 [163]
                               1010 .... ECW Max: 10 (CW Max: 1,023)
                               .... 0100 ECW Min: 4 (CW Min: 15)
      TXOP Limit:            0 [164-165]
  ⊟ Access Category - Background
    ⊟ ACI/AIFSN:             %00100111 [166]
                               x... .... Reserved
                               .01. .... ACI: Background
                               ...0 .... ACM: Admission Control Not Mandatory
                               .... 0111 AIFSN: 7
    ⊟ ECW Min/Max:           %10100100 [167]
                               1010 .... ECW Max: 10 (CW Max: 1,023)
                               .... 0100 ECW Min: 4 (CW Min: 15)
      TXOP Limit:            0 [168-169]
  ⊟ Access Category - Video
    ⊟ ACI/AIFSN:             %01000010 [170]
                               x... .... Reserved
                               .10. .... ACI: Video
                               ...0 .... ACM: Admission Control Not Mandatory
                               .... 0010 AIFSN: 2
    ⊟ ECW Min/Max:           %01000011 [171]
                               0100 .... ECW Max: 4 (CW Max: 15)
                               .... 0011 ECW Min: 3 (CW Min: 7)
      TXOP Limit:            94 [172-173]
  ⊟ Access Category - Voice
    ⊟ ACI/AIFSN:             %01100010 [174]
                               x... .... Reserved
                               .11. .... ACI: Voice
```

- Motorola/Zebra– Beacon
  - WMM Information Element



```
⊟ WMM
    Element ID:            221  WMM [202]
    Length:                7 [203]
    OUI:                   00-50-F2MICROSOFT CORP.[204-206]
    OUI Type:              2 [207]
    OUI SubType:           0  Information Element [208]
    Version:               1 [209]
  ⊟ QoS Info:              %10000000 [210]
                             1... .... WMM AP supports U-APSD
                             .xxx .... Reserved
                             .... 0000 Parameter Set Count: 0
⊟ Vendor Specific
    Element ID:            221  Vendor Specific [211]
    Length:                26 [212]
    OUI:                   00-A0-F8SYMBOL TECHNOLOGIES, INC.[213-215]
    Value:                 (23 bytes) [216-238]
⊟ FCS - Frame Check Sequence
```



2.2.3 Beacon Frame

Every beacon frame transmitted by a WMM-enabled AP shall contain, in addition to those elements specified in [1], either a WMM Information Element or a WMM Parameter Element.

2.2.4 Probe Request Frame

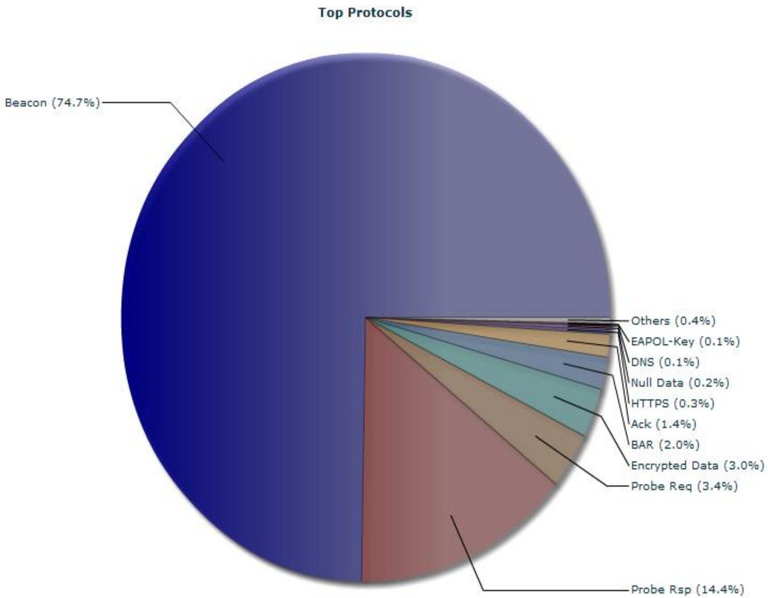
Probe request frames transmitted by a WMM-enabled STA are unchanged from [1].

2.2.5 Probe Response Frame

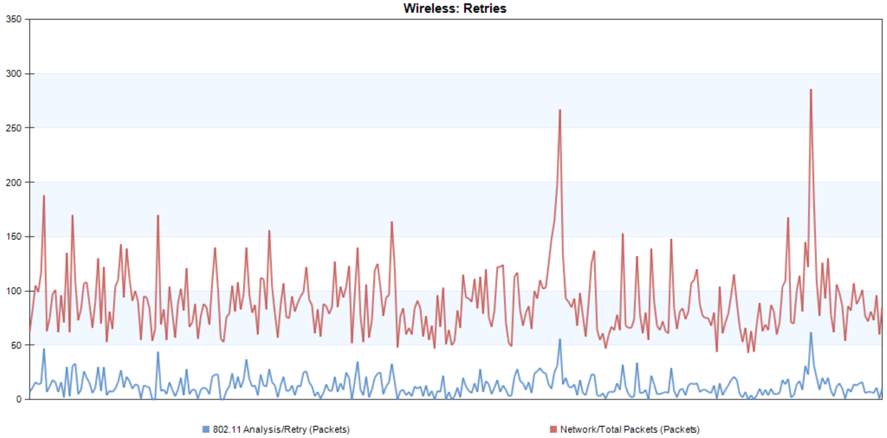
A probe response frame transmitted by a WMM-enabled AP shall contain a WMM Parameter Element. A probe response frame transmitted by a WMM-enabled STA shall contain a WMM Parameter Element if the corresponding probe request was transmitted by a member of the same (I)BSS as the transmitter of the probe response, otherwise, the probe response frame transmitted

Performance Analysis

- Beacons, Probe Request & Probe Responses = 92.5% of Total



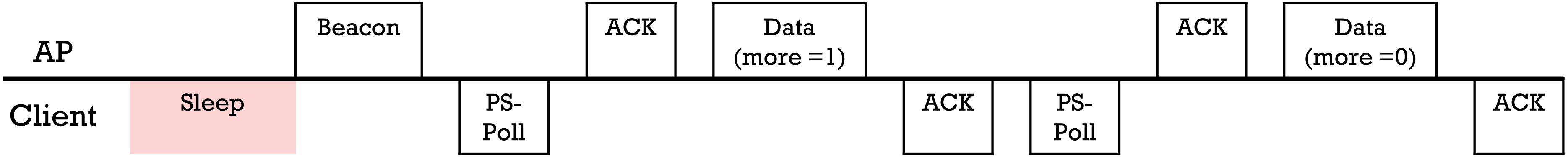
- Retries
  - Per Channel
  - Per AP
  - Per Client



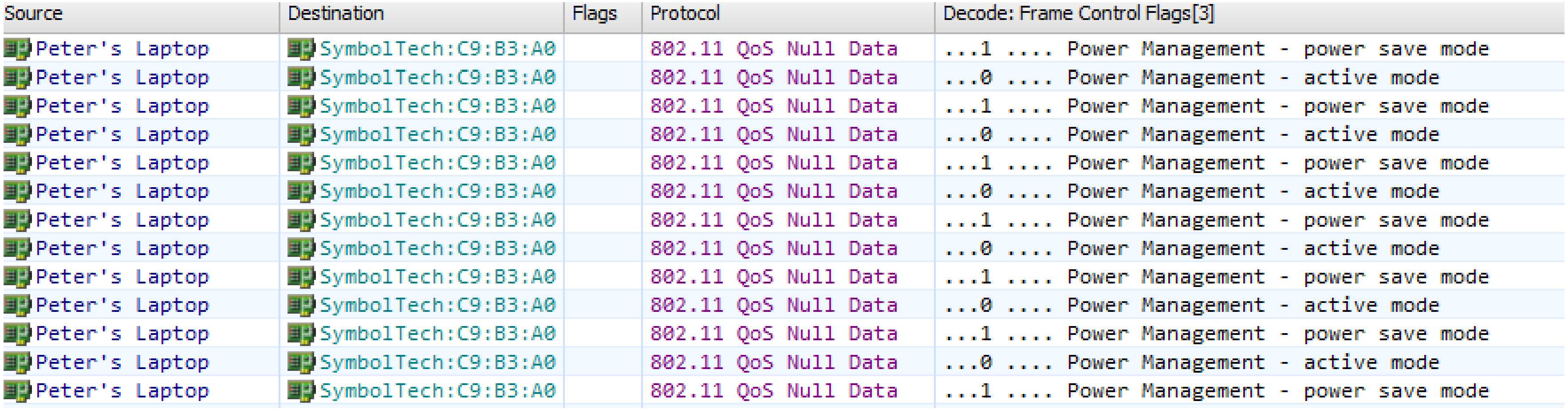
Capture Before you Write

- Can’t I just read the Standard?
  - Standard vs proprietary
  - Standard interpretation

802.11 Power Save



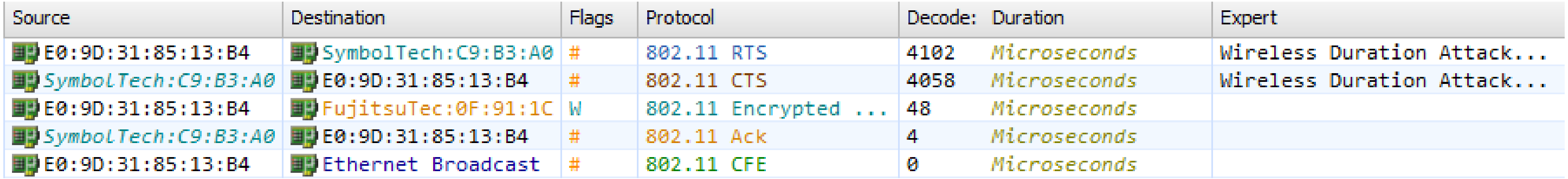
Power Save – As Implemented



Source	Destination	Flags	Protocol	Decode: Frame Control Flags[3]
Peter's Laptop	SymbolTech:C9:B3:A0		802.11 QoS Null Data	...1 .... Power Management - power save mode
Peter's Laptop	SymbolTech:C9:B3:A0		802.11 QoS Null Data	...0 .... Power Management - active mode
Peter's Laptop	SymbolTech:C9:B3:A0		802.11 QoS Null Data	...1 .... Power Management - power save mode
Peter's Laptop	SymbolTech:C9:B3:A0		802.11 QoS Null Data	...0 .... Power Management - active mode
Peter's Laptop	SymbolTech:C9:B3:A0		802.11 QoS Null Data	...1 .... Power Management - power save mode
Peter's Laptop	SymbolTech:C9:B3:A0		802.11 QoS Null Data	...0 .... Power Management - active mode
Peter's Laptop	SymbolTech:C9:B3:A0		802.11 QoS Null Data	...1 .... Power Management - power save mode
Peter's Laptop	SymbolTech:C9:B3:A0		802.11 QoS Null Data	...0 .... Power Management - active mode
Peter's Laptop	SymbolTech:C9:B3:A0		802.11 QoS Null Data	...1 .... Power Management - power save mode
Peter's Laptop	SymbolTech:C9:B3:A0		802.11 QoS Null Data	...0 .... Power Management - active mode
Peter's Laptop	SymbolTech:C9:B3:A0		802.11 QoS Null Data	...1 .... Power Management - power save mode
Peter's Laptop	SymbolTech:C9:B3:A0		802.11 QoS Null Data	...0 .... Power Management - active mode
Peter's Laptop	SymbolTech:C9:B3:A0		802.11 QoS Null Data	...1 .... Power Management - power save mode

Proprietary 802.11n Protection Mechanism

- Intel(R) Centrino(R) Ultimate-N 6300 AGN – Power Save



Source	Destination	Flags	Protocol	Decode: Duration	Expert
E0:9D:31:85:13:B4	SymbolTech:C9:B3:A0	#	802.11 RTS	4102 Microseconds	Wireless Duration Attack...
SymbolTech:C9:B3:A0	E0:9D:31:85:13:B4	#	802.11 CTS	4058 Microseconds	Wireless Duration Attack...
E0:9D:31:85:13:B4	FujitsuTec:0F:91:1C	W	802.11 Encrypted ...	48 Microseconds	
SymbolTech:C9:B3:A0	E0:9D:31:85:13:B4	#	802.11 Ack	4 Microseconds	
E0:9D:31:85:13:B4	Ethernet Broadcast	#	802.11 CFE	0 Microseconds	

Win Arguments with Packets

- Prove it with a capture
- The packets never lie!

Questions