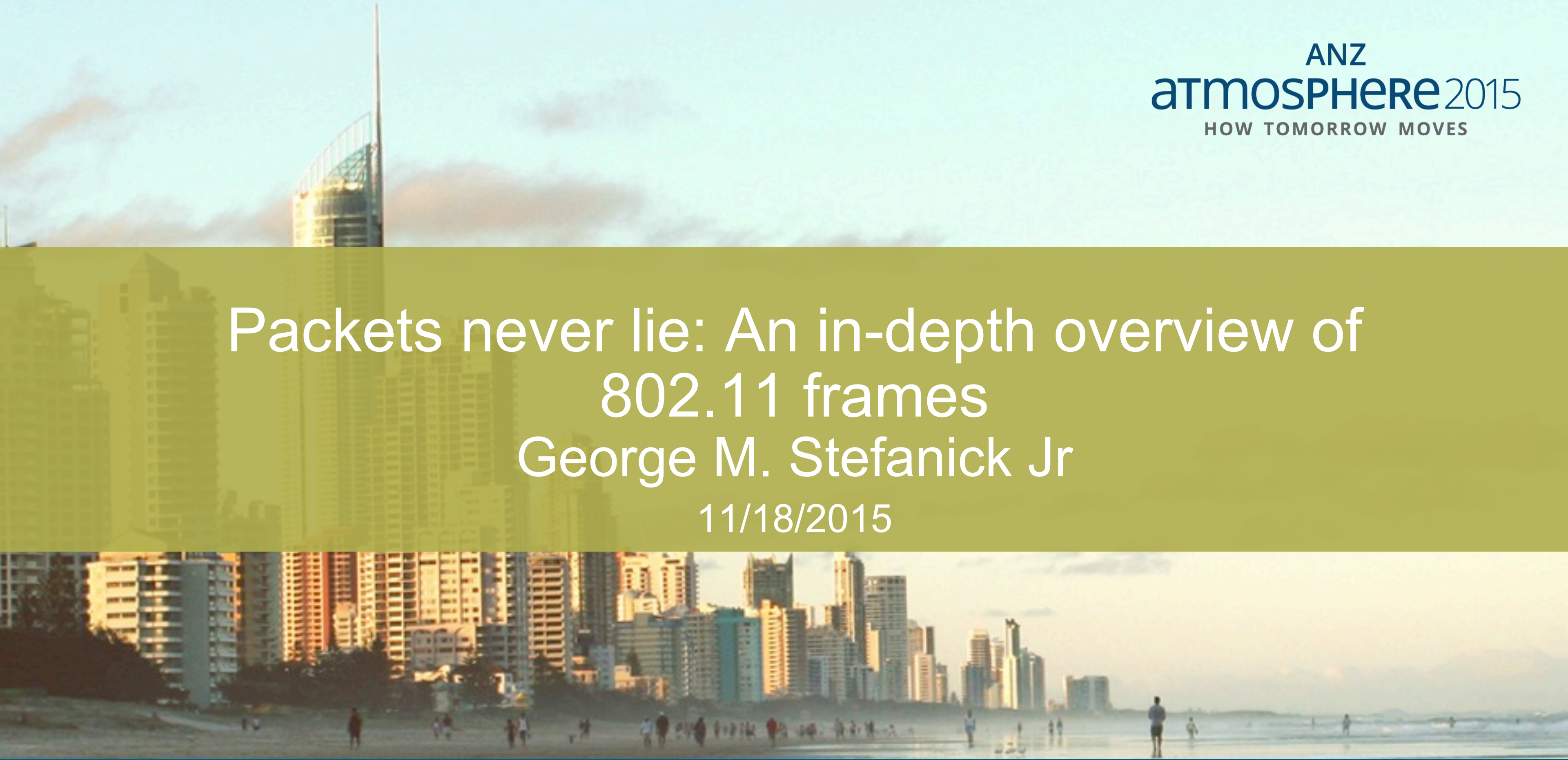


ANZ
atmosphere 2015
HOW TOMORROW MOVES

Packets never lie: An in-depth overview of 802.11 frames

George M. Stefanick Jr

11/18/2015

#ATM15ANZ | @ArubaANZ

aruba
a Hewlett Packard Enterprise company

Agenda

- **This session covers different 802.11 frame types as well as MSDU, MPDU, PSDU, PPDU and other terminology.**
- **We will explain and showcase some of the common problems you can solve with a packet analyzer.**

BIO

George M. Stefanick Jr.

Wireless Architect @ Houston Methodist Hospital – 7 years (9 WiFi Distros, 4,300 aps, 35,000 clients)

Previously worked for a Cisco Partner focused on Mobility for 8 years

Vendor and vendor neutral certifications

www.my80211.com and www.nostringsattachedshow.com

Cisco VIP 2012,2013 and 2014 - Aruba MVP 2014 and 2015

Consulting Free Space WiFi (training, site survey, deployment and troubleshooting)

Tech Editor:

Sybex: CCNA Wireless Study Guide; Todd Lammle

Cisco Press: Designing and Deploying 802.11 Wireless Networks: A Practical Guide to Implementing 802.11n and 802.11ac; Jim Geier

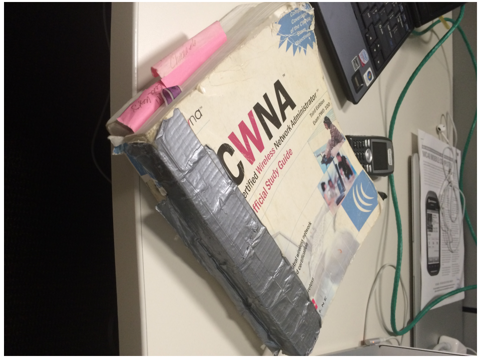
Devices that are in my wheelhouse

ANZ atmosphere 2015 HOW TOMORROW MOVES

- Cardiac Imaging
- Electronic Medical Record (EMR)
- Mobile Ultrasound
- Mobile Picture Archiving and Communications systems (PACS)
- RTLS
- Mobile Robots
- Infusion Pumps
- Cows (Computer on Wheels)
- Cisco 7925 Handsets
- Vocera Badges
- Mobile Cisco TelePresence VX Clinical Assistant
- Roche Diagnostics ACCU-CHECK
- Mobile EKG Carts
- Mobile Med Dispensing Carts
- WorkGroup Bridges (WGB)
- Mobile Deaf Response Devices
- DaVinci Simulators
- Laptops
- Tablets
- Smartphones
- Crestron
- Point to Point Links
- Wireless Door Locks

Quick Poll

1. **Any CWNP Certified folks ?**
2. **Who has a WiFi Analyzer in their tool bag ?**
3. **How confident are you with reading and interpreting your captures ?**
4. **Who has solved a problem with packet analysis ?**



What does a WiFi Engineer look like ?

Management, Control, and Data frames

Management

- Beacon, Association Request, Association Response, Reassociation Request, Reassociation Response, Probe Request, Probe Response, Disassociation, Authentication, Deauthentication, Action and Announcement Traffic Indication Message
- Management frames provide the foundation in how WiFi radios are able to detect, join and operate on a WiFi network.

Control

- Power Save Poll (PS-Poll), Request to Send (RTS), Clear to Send (CTS), Acknowledgement (ACK), CF-End +CF +ACK, Block ACK Request (BlockAckReq), and Block ACK (BlockAck).
- Control frames facilitate Data frame delivery. They are the traffic cops of 802.11 data frames.

Data

- Data, NULL, Data+CF-Ack, Data+CF-Poll, Data +CF-ACK+CF-Poll, CF-ACK, CF-Poll, CF-ACK, Qos Data, QoD Null, QoS Data+CF-ACK, QoS Data+CF-Poll, QoS Data +CF-ACK+CF-Poll and more ..
- Data frames are simple. They carry data payload from and to the upper layers.

802.11 Frame Headers, Information Fields, and Information Elements Are Not Encrypted

Layer 2 is not encrypted

Visible to anyone within range of the transmission, on channel and with a protocol analyzer

With the right tools someone can easily ease drop on your network transmissions

WiFi DOS Attacks are easily achieved on Layer 1 and Layer 2

- Layer 2 MFP (Management Frame Protection)

Encryption secures Layer 3 and up (Data Frames)

- NULL Data frames aren't encrypted because they don't carry a data payload

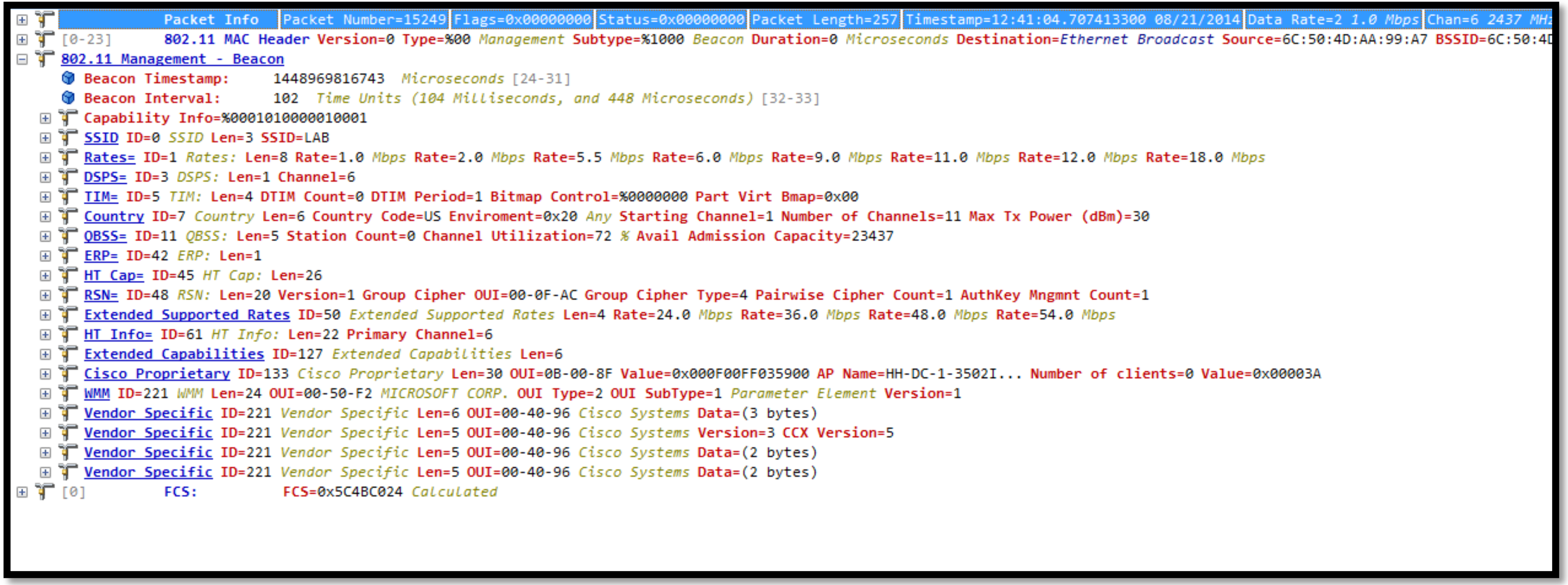
802.11 Management Frames

Management

- Beacon, Association Request, Association Response, Reassociation Request, Reassociation Response, Probe Request, Probe Response, Disassociation, Authentication, Deauthentication, Action and Announcement Traffic Indication Message

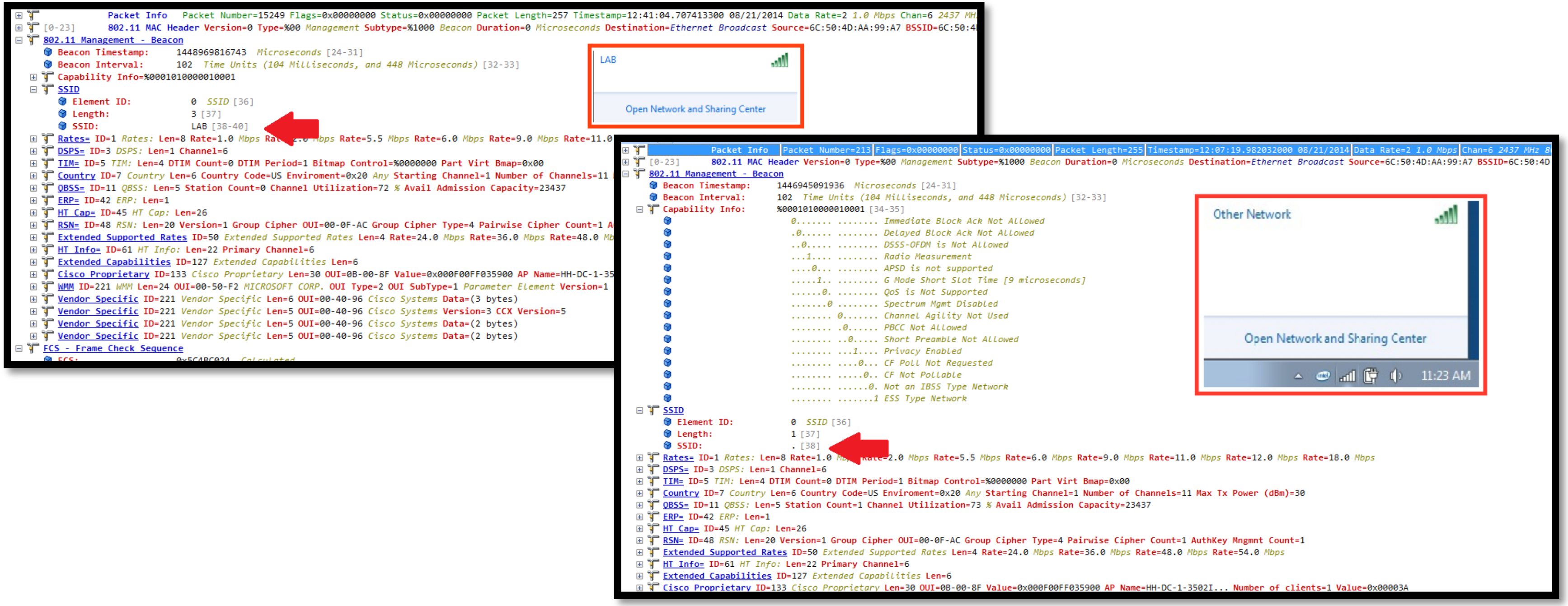
- Management frames provide the foundation in how WiFi radios are able to detect, join and operate on a WiFi network.

802.11 Beacon: What’s inside a Beacon?



```
⊞ Packet Info  Packet Number=15249 Flags=0x00000000 Status=0x00000000 Packet Length=257 Timestamp=12:41:04.707413300 08/21/2014 Data Rate=2 1.0 Mbps Chan=6 2437 MHz
⊞ [0-23]       802.11 MAC Header Version=0 Type=%00 Management Subtype=%1000 Beacon Duration=0 Microseconds Destination=Ethernet Broadcast Source=6C:50:4D:AA:99:A7 BSSID=6C:50:4D
⊟ 802.11 Management - Beacon
     Beacon Timestamp:      1448969816743  Microseconds [24-31]
     Beacon Interval:       102  Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
   ⊞ Capability Info=%0001010000010001
   ⊞ SSID ID=0 SSID Len=3 SSID=LAB
   ⊞ Rates= ID=1 Rates: Len=8 Rate=1.0 Mbps Rate=2.0 Mbps Rate=5.5 Mbps Rate=6.0 Mbps Rate=9.0 Mbps Rate=11.0 Mbps Rate=12.0 Mbps Rate=18.0 Mbps
   ⊞ DSPS= ID=3 DSPS: Len=1 Channel=6
   ⊞ TIM= ID=5 TIM: Len=4 DTIM Count=0 DTIM Period=1 Bitmap Control=%0000000 Part Virt Bmap=0x00
   ⊞ Country ID=7 Country Len=6 Country Code=US Enviroment=0x20 Any Starting Channel=1 Number of Channels=11 Max Tx Power (dBm)=30
   ⊞ QBSS= ID=11 QBSS: Len=5 Station Count=0 Channel Utilization=72 % Avail Admission Capacity=23437
   ⊞ ERP= ID=42 ERP: Len=1
   ⊞ HT Cap= ID=45 HT Cap: Len=26
   ⊞ 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
   ⊞ Extended Supported Rates ID=50 Extended Supported Rates Len=4 Rate=24.0 Mbps Rate=36.0 Mbps Rate=48.0 Mbps Rate=54.0 Mbps
   ⊞ HT Info= ID=61 HT Info: Len=22 Primary Channel=6
   ⊞ Extended Capabilities ID=127 Extended Capabilities Len=6
   ⊞ Cisco Proprietary ID=133 Cisco Proprietary Len=30 OUI=0B-00-8F Value=0x000F00FF035900 AP Name=HH-DC-1-3502I... Number of clients=0 Value=0x00003A
   ⊞ WMM ID=221 WMM Len=24 OUI=00-50-F2 MICROSOFT CORP. OUI Type=2 OUI SubType=1 Parameter Element Version=1
   ⊞ Vendor Specific ID=221 Vendor Specific Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
   ⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Version=3 CCX Version=5
   ⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Data=(2 bytes)
   ⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Data=(2 bytes)
⊞ [0]          FCS:           FCS=0x5C4BC024 Calculated
```

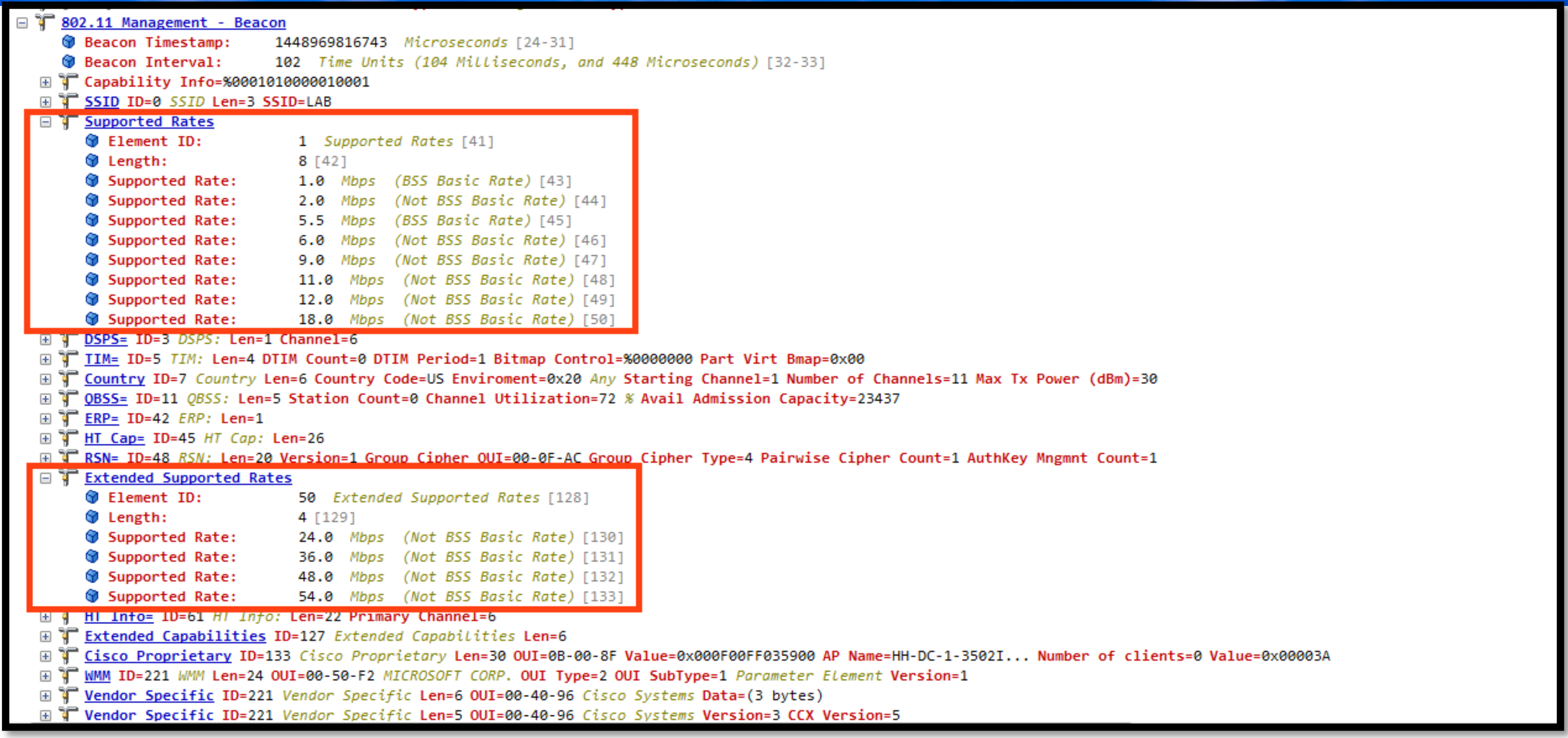
802.11 Beacon: Broadcast vs NonBroadcast



```
⊞ Packet Info   Packet Number=15249 Flags=0x00000000 Status=0x00000000 Packet Length=257 Timestamp=12:41:04.707413300 08/21/2014 Data Rate=2 1.0 Mbps Chan=6 2437 MH
⊞ [0-23]        802.11 MAC Header Version=0 Type=%00 Management Subtype=%1000 Beacon Duration=0 Microseconds Destination=Ethernet Broadcast Source=6C:50:4D:AA:99:A7 BSSID=6C:50:4
⊟ 802.11 Management - Beacon
     Beacon Timestamp:      1448969816743  Microseconds [24-31]
     Beacon Interval:       102  Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
  ⊞ Capability Info=%0001010000010001
  ⊟ SSID
       Element ID:          0  SSID [36]
       Length:              3 [37]
       SSID:                LAB [38-40]
  ⊞ Rates= ID=1 Rates: Len=8 Rate=1.0 Mbps Ra    2.0 Mbps Rate=5.5 Mbps Rate=6.0 Mbps Rate=9.0 Mbps Rate=11.0
  ⊞ DSPS= ID=3 DSPS: Len=1 Channel=6
  ⊞ TIM= ID=5 TIM: Len=4 DTIM Count=0 DTIM Period=1 Bitmap Control=%0000000 Part Virt Bmap=0x00
  ⊞ Country ID=7 Country Len=6 Country Code=US Enviroment=0x20 Any Starting Channel=1 Number of Channels=11
  ⊞ QBSS= ID=11 QBSS: Len=5 Station Count=0 Channel Utilization=72 % Avail Admission Capacity=23437
  ⊞ ERP= ID=42 ERP: Len=1
  ⊞ HT Cap= ID=45 HT Cap: Len=26
  ⊞ RSN= ID=48 RSN: Len=20 Version=1 Group Cipher OUI=00-0F-AC Group Cipher Type=4 Pairwise Cipher Count=1 A
  ⊞ Extended Supported Rates ID=50 Extended Supported Rates Len=4 Rate=24.0 Mbps Rate=36.0 Mbps Rate=48.0 Mb
  ⊞ HT Info= ID=61 HT Info: Len=22 Primary Channel=6
  ⊞ Extended Capabilities ID=127 Extended Capabilities Len=6
  ⊞ Cisco Proprietary ID=133 Cisco Proprietary Len=30 OUI=0B-00-8F Value=0x000F00FF035900 AP Name=HH-DC-1-35
  ⊞ WMM ID=221 WMM Len=24 OUI=00-50-F2 MICROSOFT CORP. OUI Type=2 OUI SubType=1 Parameter Element Version=1
  ⊞ Vendor Specific ID=221 Vendor Specific Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
  ⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Version=3 CCX Version=5
  ⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Data=(2 bytes)
  ⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Data=(2 bytes)
⊟ FCS - Frame Check Sequence
     FCS:                 0x5C4BC024  Calculated
```

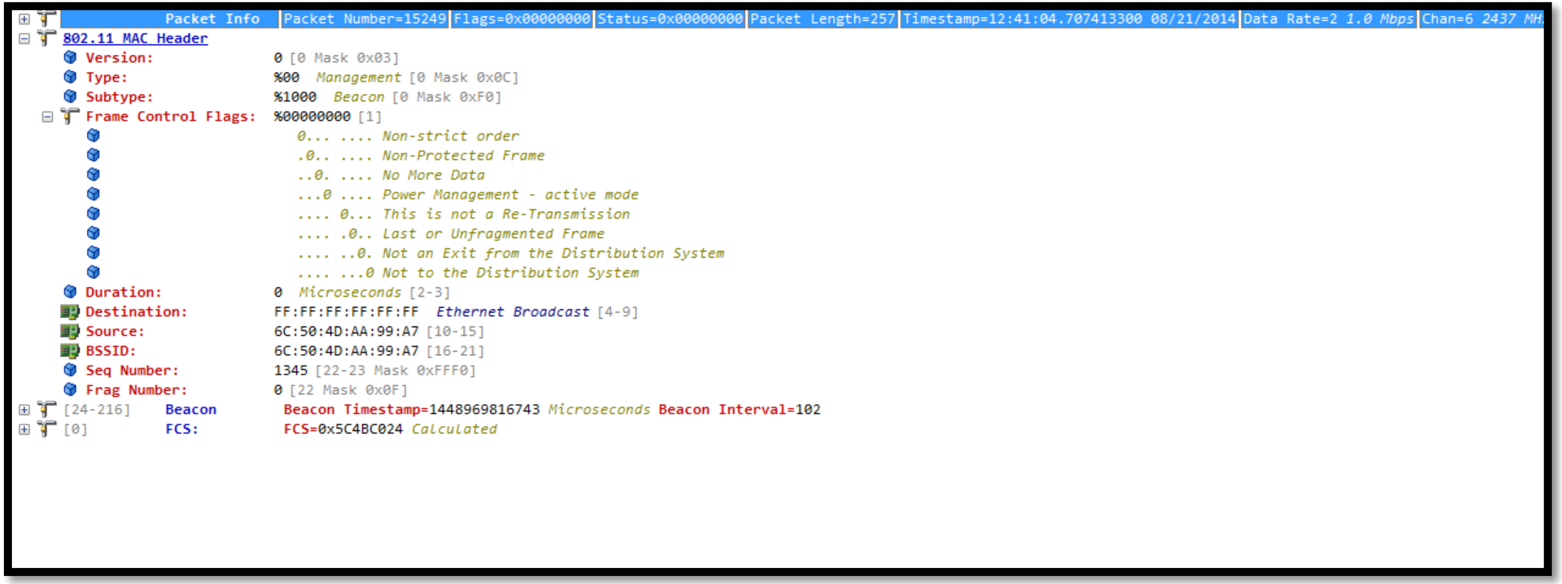
```
⊞ Packet Info | Packet Number=213 | Flags=0x00000000 | Status=0x00000000 | Packet Length=255 | Timestamp=12:07:19.982032000 08/21/2014 | Data Rate=2 1.0 Mbps | Chan=6 2437 MHz 8
⊞ [0-23]        802.11 MAC Header Version=0 Type=%00 Management Subtype=%1000 Beacon Duration=0 Microseconds Destination=Ethernet Broadcast Source=6C:50:4D:AA:99:A7 BSSID=6C:50:4D
⊟ 802.11 Management - Beacon
     Beacon Timestamp:      1446945091936  Microseconds [24-31]
     Beacon Interval:       102  Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
  ⊟ Capability Info:        %0001010000010001 [34-35]
                              0....... ........ Immediate Block Ack Not Allowed
                              .0...... ........ Delayed Block Ack Not Allowed
                              ..0..... ........ DSSS-OFDM is Not Allowed
                              ...1.... ........ Radio Measurement
                              ....0... ........ APSD is not supported
                              .....1.. ........ G Mode Short Slot Time [9 microseconds]
                              ......0. ........ QoS is Not Supported
                              .......0 ........ Spectrum Mgmt Disabled
                              ........ 0....... Channel Agility Not Used
                              ........ .0...... PBCC Not Allowed
                              ........ ..0..... Short Preamble Not Allowed
                              ........ ...1.... Privacy Enabled
                              ........ ....0... CF Poll Not Requested
                              ........ .....0.. CF Not Pollable
                              ........ ......0. Not an IBSS Type Network
                              ........ .......1 ESS Type Network
  ⊟ SSID
       Element ID:          0  SSID [36]
       Length:              1 [37]
       SSID:                . [38]
  ⊞ Rates= ID=1 Rates: Len=8 Rate=1.0 Mb    2.0 Mbps Rate=5.5 Mbps Rate=6.0 Mbps Rate=9.0 Mbps Rate=11.0 Mbps Rate=12.0 Mbps Rate=18.0 Mbps
  ⊞ DSPS= ID=3 DSPS: Len=1 Channel=6
  ⊞ TIM= ID=5 TIM: Len=4 DTIM Count=0 DTIM Period=1 Bitmap Control=%0000000 Part Virt Bmap=0x00
  ⊞ Country ID=7 Country Len=6 Country Code=US Enviroment=0x20 Any Starting Channel=1 Number of Channels=11 Max Tx Power (dBm)=30
  ⊞ QBSS= ID=11 QBSS: Len=5 Station Count=1 Channel Utilization=73 % Avail Admission Capacity=23437
  ⊞ ERP= ID=42 ERP: Len=1
  ⊞ HT Cap= ID=45 HT Cap: Len=26
  ⊞ 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
  ⊞ Extended Supported Rates ID=50 Extended Supported Rates Len=4 Rate=24.0 Mbps Rate=36.0 Mbps Rate=48.0 Mbps Rate=54.0 Mbps
  ⊞ HT Info= ID=61 HT Info: Len=22 Primary Channel=6
  ⊞ Extended Capabilities ID=127 Extended Capabilities Len=6
  ⊞ Cisco Proprietary ID=133 Cisco Proprietary Len=30 OUI=0B-00-8F Value=0x000F00FF035900 AP Name=HH-DC-1-3502I... Number of clients=1 Value=0x00003A
```

802.11 Beacon: Supported Rates



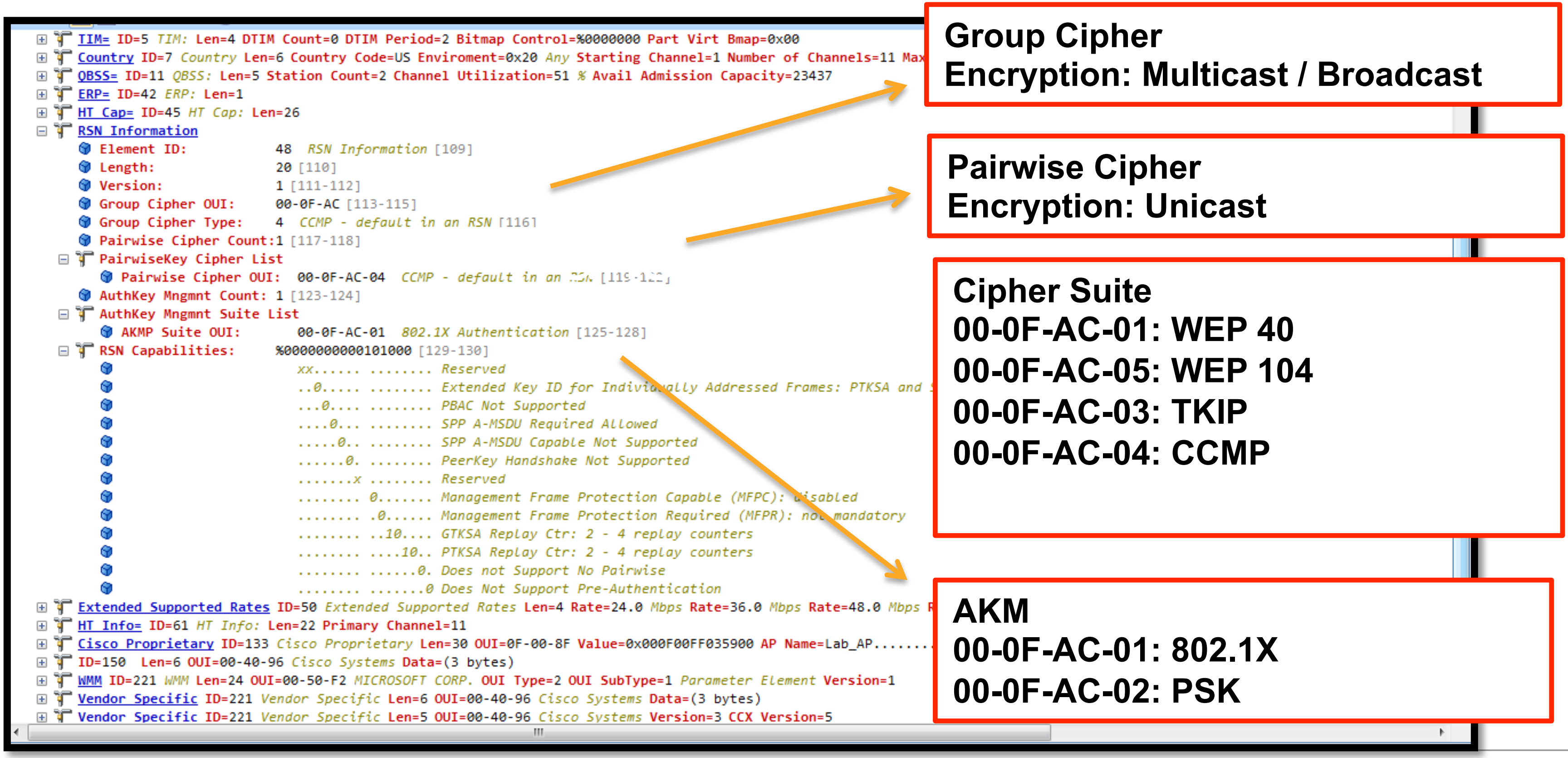
```
⊟ 802.11 Management - Beacon
     Beacon Timestamp:      1448969816743  Microseconds [24-31]
     Beacon Interval:       102  Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
  ⊞ Capability Info=%0001010000010001
  ⊞ SSID ID=0 SSID Len=3 SSID=LAB
  ⊟ Supported Rates
       Element ID:              1  Supported Rates [41]
       Length:                  8 [42]
       Supported Rate:          1.0  Mbps  (BSS Basic Rate) [43]
       Supported Rate:          2.0  Mbps  (Not BSS Basic Rate) [44]
       Supported Rate:          5.5  Mbps  (BSS Basic Rate) [45]
       Supported Rate:          6.0  Mbps  (Not BSS Basic Rate) [46]
       Supported Rate:          9.0  Mbps  (Not BSS Basic Rate) [47]
       Supported Rate:          11.0  Mbps  (Not BSS Basic Rate) [48]
       Supported Rate:          12.0  Mbps  (Not BSS Basic Rate) [49]
       Supported Rate:          18.0  Mbps  (Not BSS Basic Rate) [50]
  ⊞ DSPS= ID=3 DSPS: Len=1 Channel=6
  ⊞ TIM= ID=5 TIM: Len=4 DTIM Count=0 DTIM Period=1 Bitmap Control=%0000000 Part Virt Bmap=0x00
  ⊞ Country ID=7 Country Len=6 Country Code=US Enviroment=0x20 Any Starting Channel=1 Number of Channels=11 Max Tx Power (dBm)=30
  ⊞ QBSS= ID=11 QBSS: Len=5 Station Count=0 Channel Utilization=72 % Avail Admission Capacity=23437
  ⊞ ERP= ID=42 ERP: Len=1
  ⊞ HT Cap= ID=45 HT Cap: Len=26
  ⊞ 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
  ⊟ Extended Supported Rates
       Element ID:              50  Extended Supported Rates [128]
       Length:                  4 [129]
       Supported Rate:          24.0  Mbps  (Not BSS Basic Rate) [130]
       Supported Rate:          36.0  Mbps  (Not BSS Basic Rate) [131]
       Supported Rate:          48.0  Mbps  (Not BSS Basic Rate) [132]
       Supported Rate:          54.0  Mbps  (Not BSS Basic Rate) [133]
  ⊞ HT Info= ID=61 HT Info: Len=22 Primary Channel=6
  ⊞ Extended Capabilities ID=127 Extended Capabilities Len=6
  ⊞ Cisco Proprietary ID=133 Cisco Proprietary Len=30 OUI=0B-00-8F Value=0x000F00FF035900 AP Name=HH-DC-1-3502I... Number of clients=0 Value=0x00003A
  ⊞ WMM ID=221 WMM Len=24 OUI=00-50-F2 MICROSOFT CORP. OUI Type=2 OUI SubType=1 Parameter Element Version=1
  ⊞ Vendor Specific ID=221 Vendor Specific Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
  ⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Version=3 CCX Version=5
```

802.11 Beacon: Interval



```
⊞     Packet Info      Packet Number=15249 Flags=0x00000000 Status=0x00000000 Packet Length=257 Timestamp=12:41:04.707413300 08/21/2014 Data Rate=2 1.0 Mbps Chan=6 2437 MH
⊟ 802.11 MAC Header
     Version:                  0 [0 Mask 0x03]
     Type:                     %00  Management [0 Mask 0x0C]
     Subtype:                  %1000  Beacon [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:                 0  Microseconds [2-3]
     Destination:              FF:FF:FF:FF:FF:FF  Ethernet Broadcast [4-9]
     Source:                   6C:50:4D:AA:99:A7 [10-15]
     BSSID:                    6C:50:4D:AA:99:A7 [16-21]
     Seq Number:               1345 [22-23 Mask 0xFFF0]
     Frag Number:              0 [22 Mask 0x0F]
⊞ [24-216]     Beacon           Beacon Timestamp=1448969816743 Microseconds Beacon Interval=102
⊞ [0]          FCS:             FCS=0x5C4BC024 Calculated
```

802.11 Beacon: Cipher and AKM (CCMP/802.1X)



```
⊞ TIM= ID=5 TIM: Len=4 DTIM Count=0 DTIM Period=2 Bitmap Control=%0000000 Part Virt Bmap=0x00
⊞ Country ID=7 Country Len=6 Country Code=US Enviroment=0x20 Any Starting Channel=1 Number of Channels=11 Max
⊞ QBSS= ID=11 QBSS: Len=5 Station Count=2 Channel Utilization=51 % Avail Admission Capacity=23437
⊞ ERP= ID=42 ERP: Len=1
⊞ HT Cap= ID=45 HT Cap: Len=26
⊟ RSN Information
    Element ID:            48  RSN Information [109]
    Length:                20 [110]
    Version:               1 [111-112]
    Group Cipher OUI:      00-0F-AC [113-115]
    Group Cipher Type:     4  CCMP - default in an RSN [116]
    Pairwise Cipher Count:1 [117-118]
  ⊟ PairwiseKey Cipher List
      Pairwise Cipher OUI:  00-0F-AC-04  CCMP - default in an RSN [119-122]
    AuthKey Mngmnt Count: 1 [123-124]
  ⊟ AuthKey Mngmnt Suite List
      AKMP Suite OUI:       00-0F-AC-01  802.1X Authentication [125-128]
  ⊟ RSN Capabilities:      %0000000000101000 [129-130]
                              xx...... ........ Reserved
                              ..0..... ........ Extended Key ID for Individually Addressed Frames: PTKSA and S
                              ...0.... ........ PBAC Not Supported
                              ....0... ........ SPP A-MSDU Required Allowed
                              .....0.. ........ SPP A-MSDU Capable Not Supported
                              ......0. ........ PeerKey Handshake Not Supported
                              .......x ........ Reserved
                              ........ 0....... Management Frame Protection Capable (MFPC): disabled
                              ........ .0...... Management Frame Protection Required (MFPR): not mandatory
                              ........ ..10.... GTKSA Replay Ctr: 2 - 4 replay counters
                              ........ ....10.. PTKSA Replay Ctr: 2 - 4 replay counters
                              ........ ......0. Does not Support No Pairwise
                              ........ .......0 Does Not Support Pre-Authentication
⊞ Extended Supported Rates ID=50 Extended Supported Rates Len=4 Rate=24.0 Mbps Rate=36.0 Mbps Rate=48.0 Mbps R
⊞ HT Info= ID=61 HT Info: Len=22 Primary Channel=11
⊞ Cisco Proprietary ID=133 Cisco Proprietary Len=30 OUI=0F-00-8F Value=0x000F00FF035900 AP Name=Lab_AP........
⊞ ID=150  Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
⊞ WMM ID=221 WMM Len=24 OUI=00-50-F2 MICROSOFT CORP. OUI Type=2 OUI SubType=1 Parameter Element Version=1
⊞ Vendor Specific ID=221 Vendor Specific Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Version=3 CCX Version=5
```

Group Cipher
Encryption: Multicast / Broadcast

Pairwise Cipher
Encryption: Unicast

Cipher Suite
00-0F-AC-01: WEP 40
00-0F-AC-05: WEP 104
00-0F-AC-03: TKIP
00-0F-AC-04: CCMP

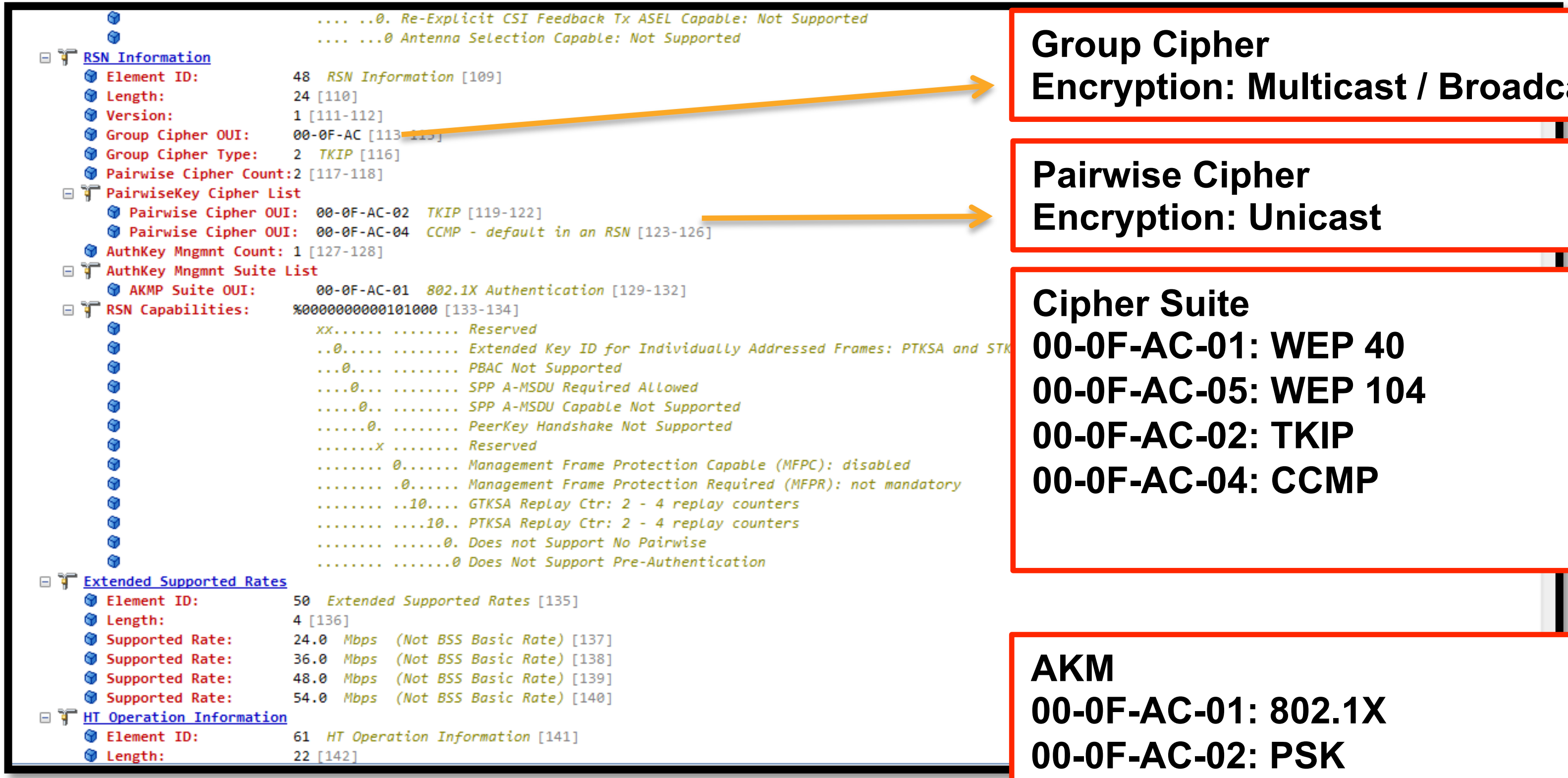
AKM
00-0F-AC-01: 802.1X
00-0F-AC-02: PSK

802.11 Beacon: AirHeads Technology Blog – 30 Random Technical Thoughts by a WiFi Engineer

30) You often see TKIP and AES referenced when securing a WiFi client. Really it should be referenced as TKIP and CCMP, not AES. TKIP and CCMP are encryption protocols. AES and RC4 are ciphers, CCMP/AES and TKIP/RC4. You can see vendors are mixing a cipher with a encryption protocol.

http://community.arubanetworks.com/t5/Technology-Blog/30-Random-Technical-Thoughts-by-a-WiFi-Engineer/ba-p/137033

802.11 Beacon: Cipher and AKM (CCMP/TKIP/802.1X)



```
                              .... ..0. Re-Explicit CSI Feedback Tx ASEL Capable: Not Supported
                              .... ...0 Antenna Selection Capable: Not Supported
⊟ RSN Information
    Element ID:              48  RSN Information [109]
    Length:                  24 [110]
    Version:                 1 [111-112]
    Group Cipher OUI:        00-0F-AC [113-115]
    Group Cipher Type:       2  TKIP [116]
    Pairwise Cipher Count:2 [117-118]
  ⊟ PairwiseKey Cipher List
      Pairwise Cipher OUI:   00-0F-AC-02  TKIP [119-122]
      Pairwise Cipher OUI:   00-0F-AC-04  CCMP - default in an RSN [123-126]
    AuthKey Mngmnt Count: 1 [127-128]
  ⊟ AuthKey Mngmnt Suite List
      AKMP Suite OUI:        00-0F-AC-01  802.1X Authentication [129-132]
  ⊟ RSN Capabilities:        %0000000000101000 [133-134]
                              xx...... ........ Reserved
                              ..0..... ........ Extended Key ID for Individually Addressed Frames: PTKSA and STK
                              ...0.... ........ PBAC Not Supported
                              ....0... ........ SPP A-MSDU Required Allowed
                              .....0.. ........ SPP A-MSDU Capable Not Supported
                              ......0. ........ PeerKey Handshake Not Supported
                              .......x ........ Reserved
                              ........ 0....... Management Frame Protection Capable (MFPC): disabled
                              ........ .0...... Management Frame Protection Required (MFPR): not mandatory
                              ........ ..10.... GTKSA Replay Ctr: 2 - 4 replay counters
                              ........ ....10.. PTKSA Replay Ctr: 2 - 4 replay counters
                              ........ ......0. Does not Support No Pairwise
                              ........ .......0 Does Not Support Pre-Authentication
⊟ Extended Supported Rates
    Element ID:              50  Extended Supported Rates [135]
    Length:                  4 [136]
    Supported Rate:          24.0  Mbps  (Not BSS Basic Rate) [137]
    Supported Rate:          36.0  Mbps  (Not BSS Basic Rate) [138]
    Supported Rate:          48.0  Mbps  (Not BSS Basic Rate) [139]
    Supported Rate:          54.0  Mbps  (Not BSS Basic Rate) [140]
⊟ HT Operation Information
    Element ID:              61  HT Operation Information [141]
    Length:                  22 [142]
```

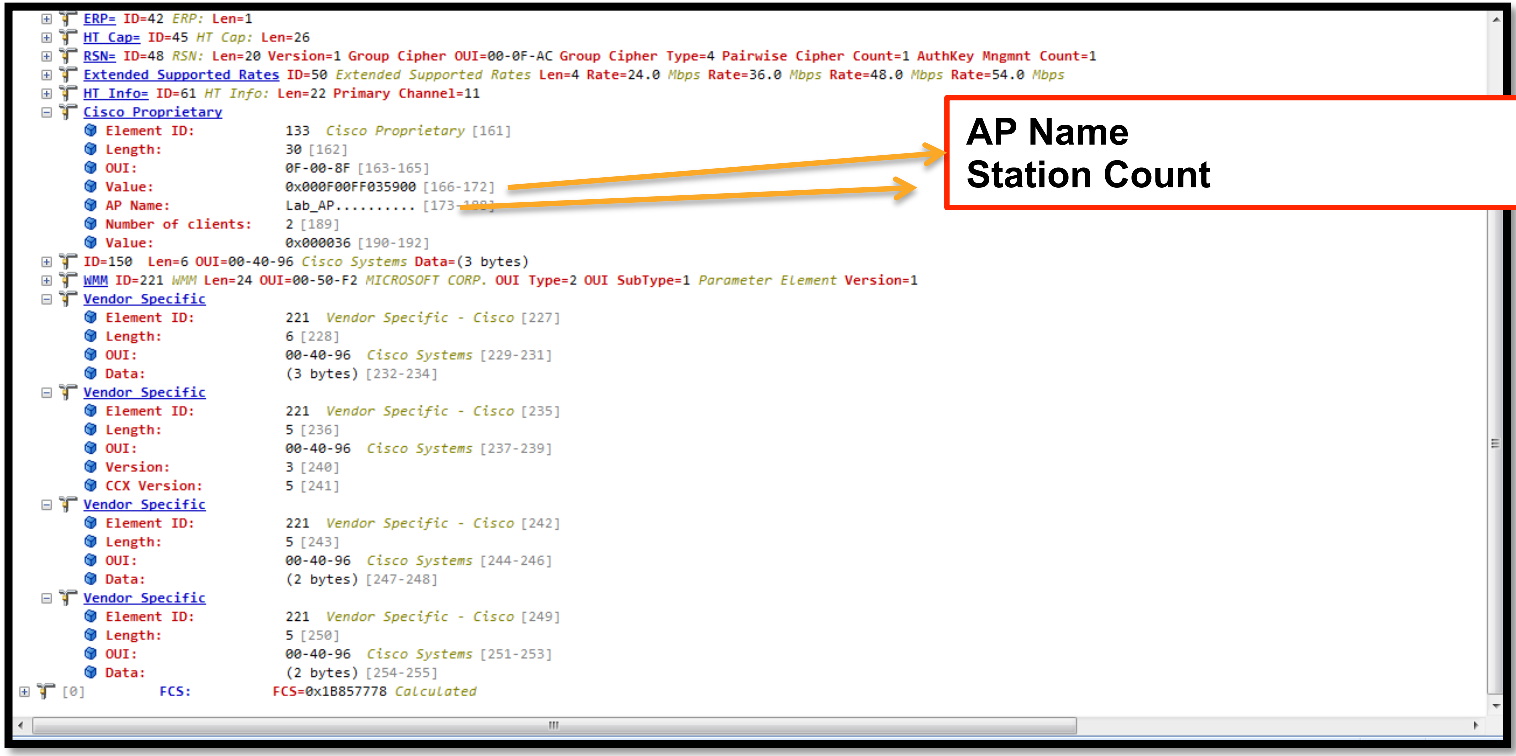
Group Cipher
Encryption: Multicast / Broadcast

Pairwise Cipher
Encryption: Unicast

Cipher Suite
00-0F-AC-01: WEP 40
00-0F-AC-05: WEP 104
00-0F-AC-02: TKIP
00-0F-AC-04: CCMP

AKM
00-0F-AC-01: 802.1X
00-0F-AC-02: PSK

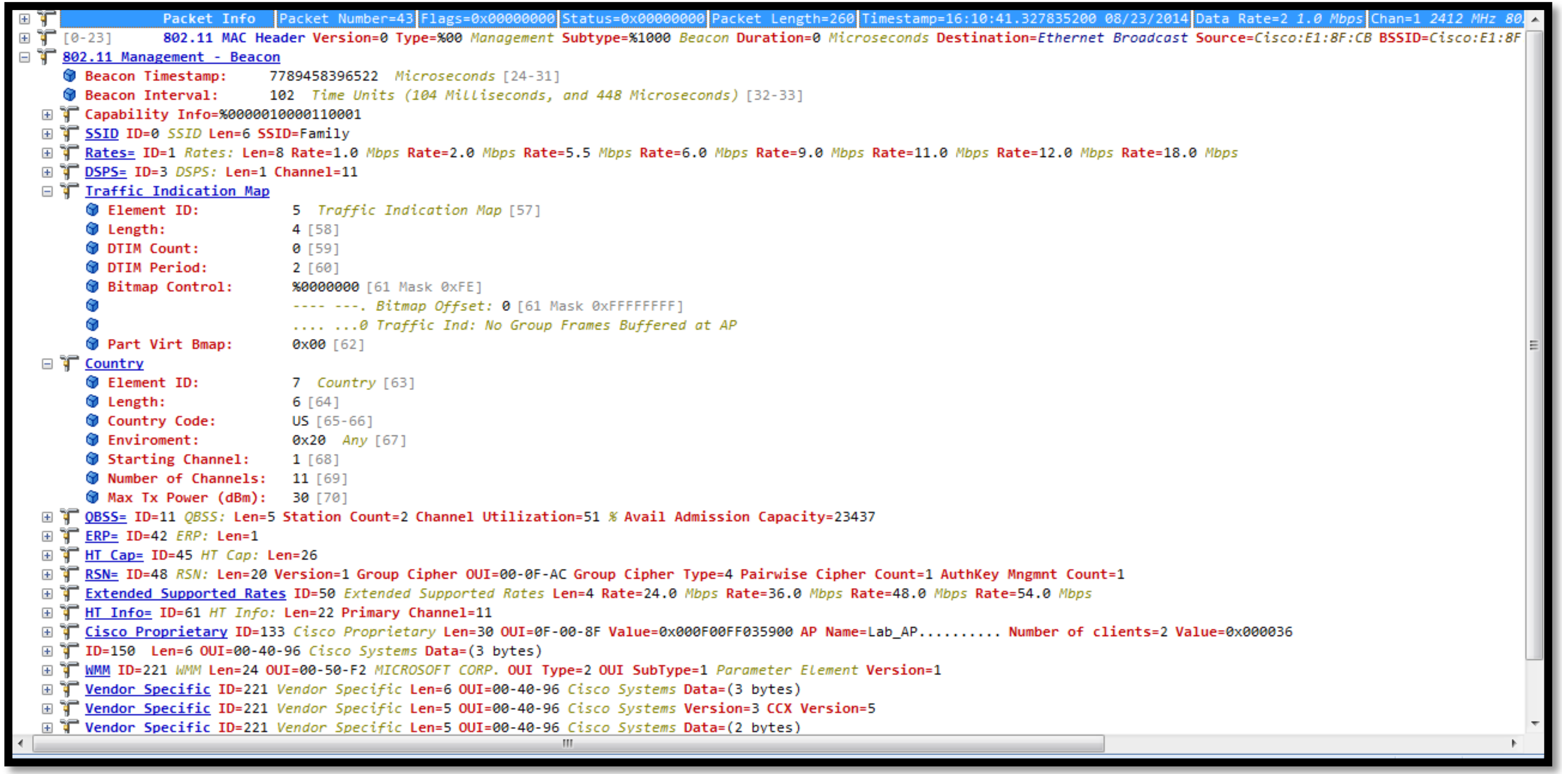
802.11 Beacon: Cisco Proprietary / Vendor Specific



```
⊞ ERP= ID=42 ERP: Len=1
⊞ HT Cap= ID=45 HT Cap: Len=26
⊞ 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
⊞ Extended Supported Rates ID=50 Extended Supported Rates Len=4 Rate=24.0 Mbps Rate=36.0 Mbps Rate=48.0 Mbps Rate=54.0 Mbps
⊞ HT Info= ID=61 HT Info: Len=22 Primary Channel=11
⊟ Cisco Proprietary
      Element ID:            133  Cisco Proprietary [161]
      Length:                30 [162]
      OUI:                   0F-00-8F [163-165]
      Value:                 0x000F00FF035900 [166-172]
      AP Name:               Lab_AP.......... [173-188]
      Number of clients:     2 [189]
      Value:                 0x000036 [190-192]
⊞ ID=150  Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
⊞ WMM ID=221 WMM Len=24 OUI=00-50-F2 MICROSOFT CORP. OUI Type=2 OUI SubType=1 Parameter Element Version=1
⊟ Vendor Specific
      Element ID:            221  Vendor Specific - Cisco [227]
      Length:                6 [228]
      OUI:                   00-40-96  Cisco Systems [229-231]
      Data:                  (3 bytes) [232-234]
⊟ Vendor Specific
      Element ID:            221  Vendor Specific - Cisco [235]
      Length:                5 [236]
      OUI:                   00-40-96  Cisco Systems [237-239]
      Version:               3 [240]
      CCX Version:           5 [241]
⊟ Vendor Specific
      Element ID:            221  Vendor Specific - Cisco [242]
      Length:                5 [243]
      OUI:                   00-40-96  Cisco Systems [244-246]
      Data:                  (2 bytes) [247-248]
⊟ Vendor Specific
      Element ID:            221  Vendor Specific - Cisco [249]
      Length:                5 [250]
      OUI:                   00-40-96  Cisco Systems [251-253]
      Data:                  (2 bytes) [254-255]
⊞ [0]          FCS:           FCS=0x1B857778 Calculated
```

AP Name
Station Count

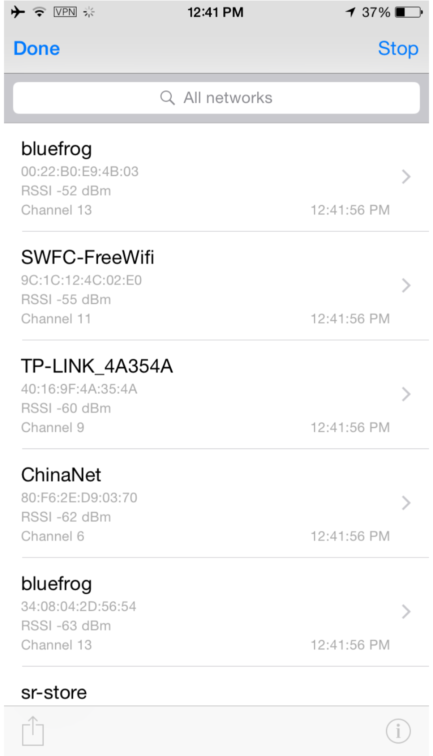
802.11 Beacon: TIM / DTIM / COUNTRY



```
      Packet Info    Packet Number=43 Flags=0x00000000 Status=0x00000000 Packet Length=260 Timestamp=16:10:41.327835200 08/23/2014 Data Rate=2 1.0 Mbps Chan=1 2412 MHz 80
[0-23]      802.11 MAC Header Version=0 Type=%00 Management Subtype=%1000 Beacon Duration=0 Microseconds Destination=Ethernet Broadcast Source=Cisco:E1:8F:CB BSSID=Cisco:E1:8F
802.11 Management - Beacon
    Beacon Timestamp:      7789458396522  Microseconds [24-31]
    Beacon Interval:       102  Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
  Capability Info=%0000010000110001
  SSID ID=0 SSID Len=6 SSID=Family
  Rates= ID=1 Rates: Len=8 Rate=1.0 Mbps Rate=2.0 Mbps Rate=5.5 Mbps Rate=6.0 Mbps Rate=9.0 Mbps Rate=11.0 Mbps Rate=12.0 Mbps Rate=18.0 Mbps
  DSPS= ID=3 DSPS: Len=1 Channel=11
  Traffic Indication Map
      Element ID:            5  Traffic Indication Map [57]
      Length:                4 [58]
      DTIM Count:            0 [59]
      DTIM Period:           2 [60]
      Bitmap Control:        %0000000 [61 Mask 0xFE]
                             ---- ---. Bitmap Offset: 0 [61 Mask 0xFFFFFFFF]
                             .... ...0 Traffic Ind: No Group Frames Buffered at AP
      Part Virt Bmap:        0x00 [62]
  Country
      Element ID:            7  Country [63]
      Length:                6 [64]
      Country Code:          US [65-66]
      Enviroment:            0x20  Any [67]
      Starting Channel:      1 [68]
      Number of Channels:    11 [69]
      Max Tx Power (dBm):    30 [70]
  QBSS= ID=11 QBSS: Len=5 Station Count=2 Channel Utilization=51 % Avail Admission Capacity=23437
  ERP= ID=42 ERP: Len=1
  HT Cap= ID=45 HT Cap: Len=26
  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
  Extended Supported Rates ID=50 Extended Supported Rates Len=4 Rate=24.0 Mbps Rate=36.0 Mbps Rate=48.0 Mbps Rate=54.0 Mbps
  HT Info= ID=61 HT Info: Len=22 Primary Channel=11
  Cisco Proprietary ID=133 Cisco Proprietary Len=30 OUI=0F-00-8F Value=0x000F00FF035900 AP Name=Lab_AP.......... Number of clients=2 Value=0x000036
  ID=150  Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
  WMM ID=221 WMM Len=24 OUI=00-50-F2 MICROSOFT CORP. OUI Type=2 OUI SubType=1 Parameter Element Version=1
  Vendor Specific ID=221 Vendor Specific Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
  Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Version=3 CCX Version=5
  Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Data=(2 bytes)
```

802.11 Beacon: China Atmosphere

ANZ ATMOSPHERE2015 HOW TOMORROW MOVES



bluefrog
00:22:B0:E9:4B:03
RSSI -52 dBm
Channel 13 12:41:56 PM

SWFC-FreeWifi
9C:1C:12:4C:02:E0
RSSI -55 dBm
Channel 11 12:41:56 PM

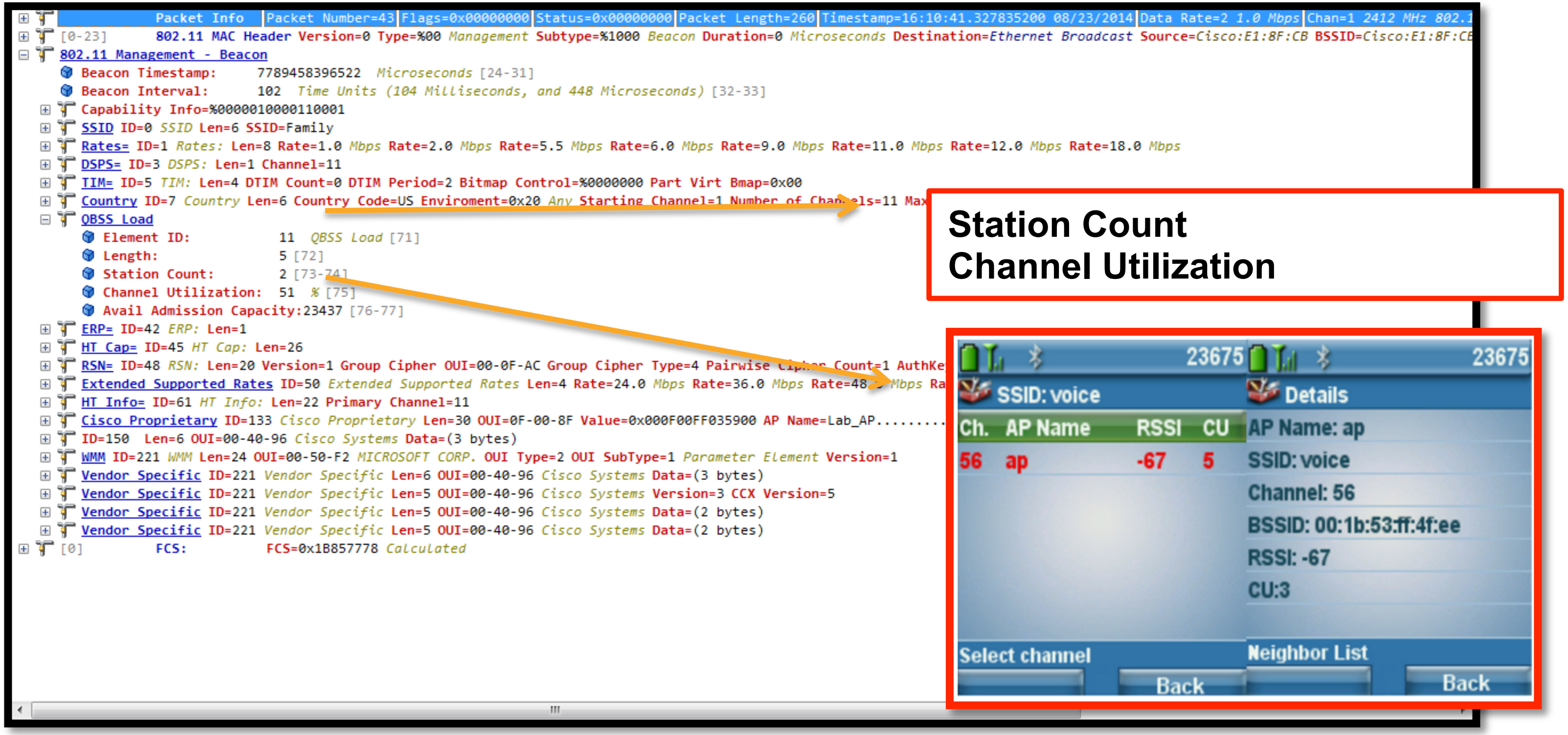
TP-LINK_4A354A
40:16:9F:4A:35:4A
RSSI -60 dBm
Channel 9 12:41:56 PM

ChinaNet
80:F6:2E:D9:03:70
RSSI -62 dBm
Channel 6 12:41:56 PM

bluefrog
34:08:04:2D:56:54
RSSI -63 dBm
Channel 13 12:41:56 PM

sr-store

802.11 Beacon: QBSS Load Station Count / Channel Util.



```
⊞ Packet Info | Packet Number=43 | Flags=0x00000000 | Status=0x00000000 | Packet Length=260 | Timestamp=16:10:41.327835200 08/23/2014 | Data Rate=2 1.0 Mbps | Chan=1 2412 MHz 802.1
⊞ [0-23]     802.11 MAC Header Version=0 Type=%00 Management Subtype=%1000 Beacon Duration=0 Microseconds Destination=Ethernet Broadcast Source=Cisco:E1:8F:CB BSSID=Cisco:E1:8F:CB
⊟ 802.11 Management - Beacon
    Beacon Timestamp:     7789458396522  Microseconds [24-31]
    Beacon Interval:      102  Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
  ⊞ Capability Info=%0000010000110001
  ⊞ SSID ID=0 SSID Len=6 SSID=Family
  ⊞ Rates= ID=1 Rates: Len=8 Rate=1.0 Mbps Rate=2.0 Mbps Rate=5.5 Mbps Rate=6.0 Mbps Rate=9.0 Mbps Rate=11.0 Mbps Rate=12.0 Mbps Rate=18.0 Mbps
  ⊞ DSPS= ID=3 DSPS: Len=1 Channel=11
  ⊞ TIM= ID=5 TIM: Len=4 DTIM Count=0 DTIM Period=2 Bitmap Control=%0000000 Part Virt Bmap=0x00
  ⊞ Country ID=7 Country Len=6 Country Code=US Enviroment=0x20 Any Starting Channel=1 Number of Channels=11 Max
  ⊟ QBSS Load
      Element ID:           11  QBSS Load [71]
      Length:               5 [72]
      Station Count:        2 [73-74]
      Channel Utilization:  51  % [75]
      Avail Admission Capacity:23437 [76-77]
  ⊞ ERP= ID=42 ERP: Len=1
  ⊞ HT Cap= ID=45 HT Cap: Len=26
  ⊞ RSN= ID=48 RSN: Len=20 Version=1 Group Cipher OUI=00-0F-AC Group Cipher Type=4 Pairwise Cipher Count=1 AuthKe
  ⊞ Extended Supported Rates ID=50 Extended Supported Rates Len=4 Rate=24.0 Mbps Rate=36.0 Mbps Rate=48.0 Mbps Ra
  ⊞ HT Info= ID=61 HT Info: Len=22 Primary Channel=11
  ⊞ Cisco Proprietary ID=133 Cisco Proprietary Len=30 OUI=0F-00-8F Value=0x000F00FF035900 AP Name=Lab_AP........
  ⊞ ID=150  Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
  ⊞ WMM ID=221 WMM Len=24 OUI=00-50-F2 MICROSOFT CORP. OUI Type=2 OUI SubType=1 Parameter Element Version=1
  ⊞ Vendor Specific ID=221 Vendor Specific Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
  ⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Version=3 CCX Version=5
  ⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Data=(2 bytes)
  ⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Data=(2 bytes)
⊞ [0]        FCS:         FCS=0x1B857778 Calculated
```

Station Count
Channel Utilization

23675

SSID: voice

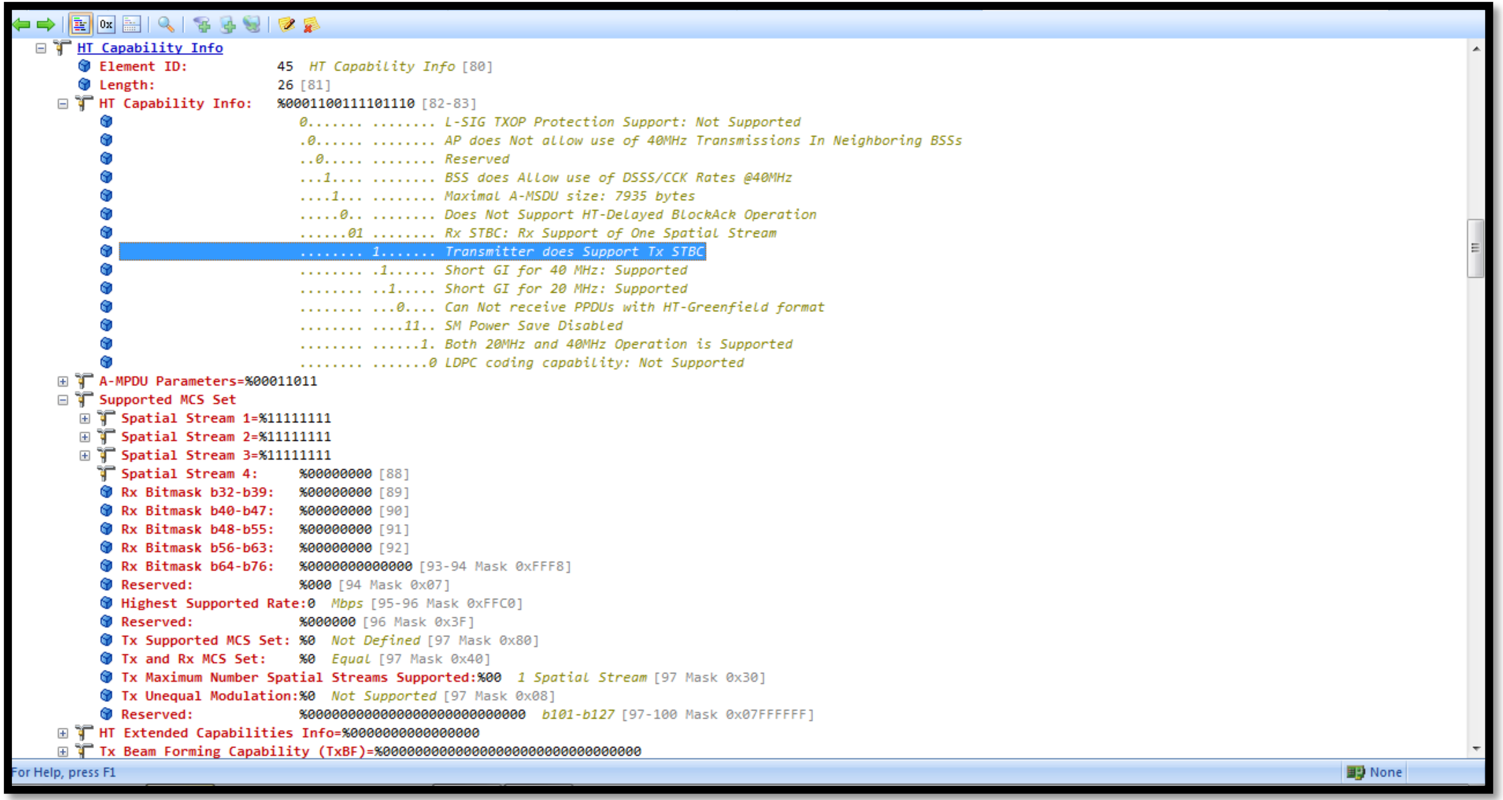
Ch.	AP Name	RSSI	CU
56	ap	-67	5

23675

Details

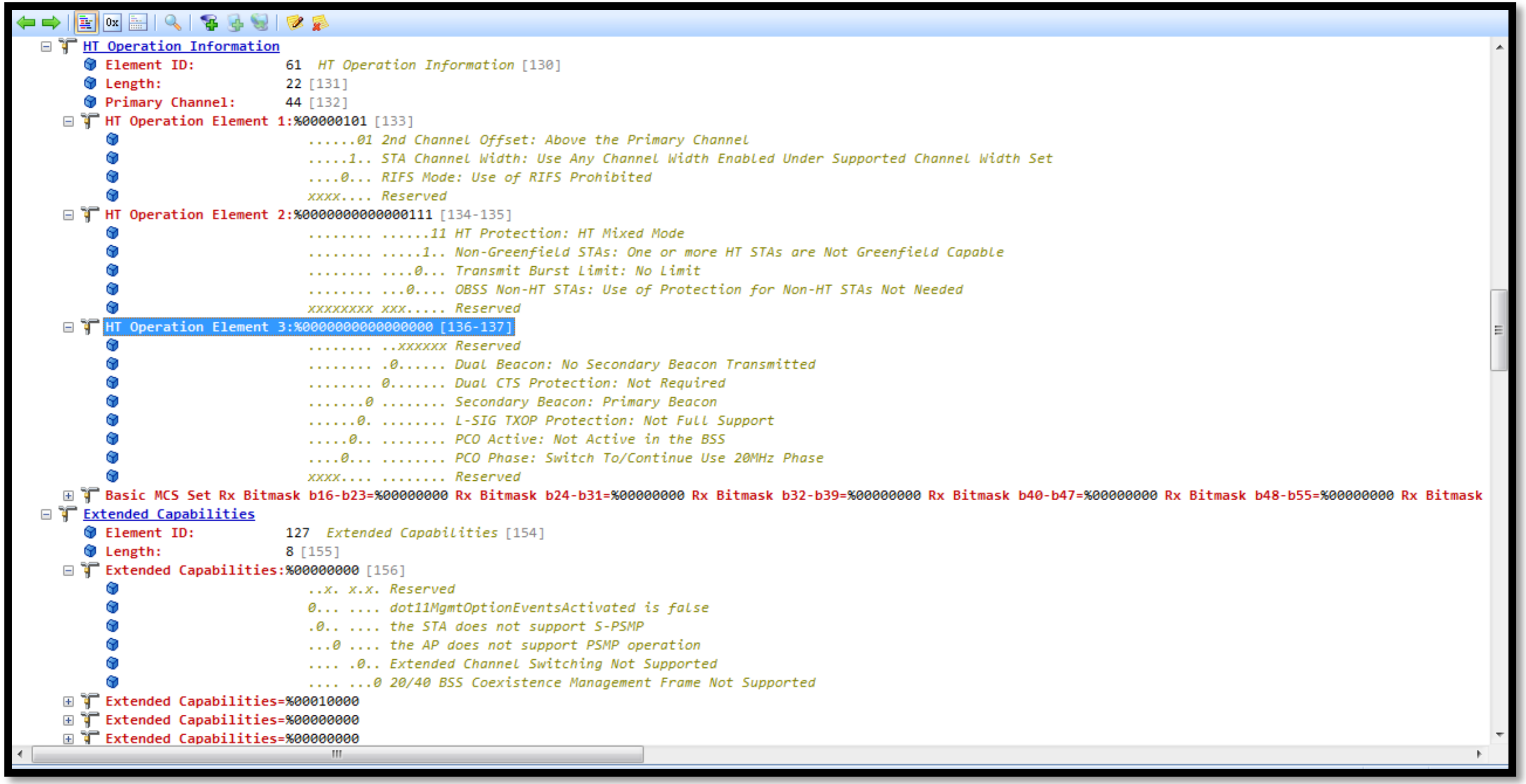
AP Name: ap
SSID: voice
Channel: 56
BSSID: 00:1b:53:ff:4f:ee
RSSI: -67
CU:3

802.11 Beacon: 802.11n (HT) High Throughput



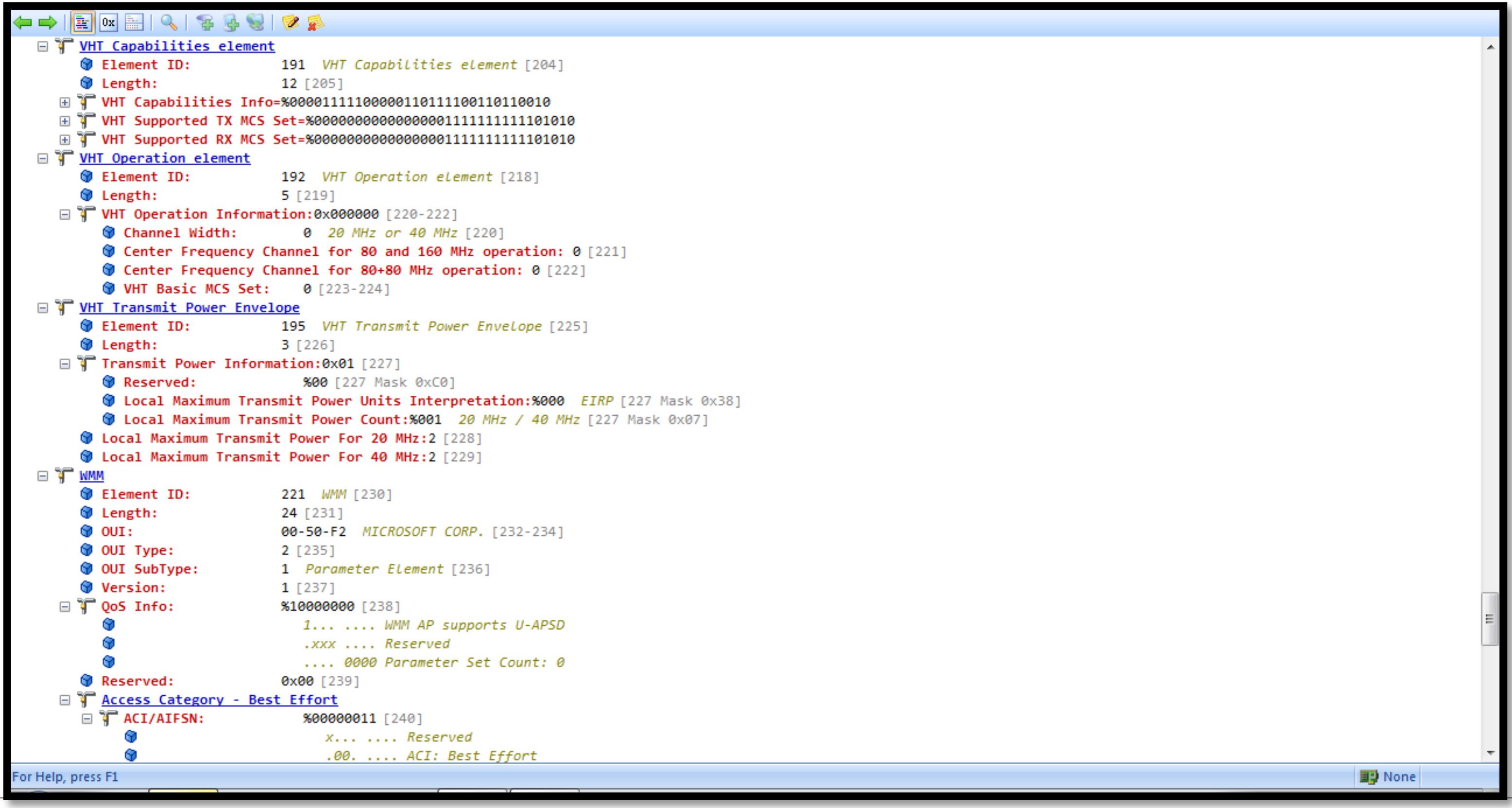
```
HT Capability Info
  Element ID:            45  HT Capability Info [80]
  Length:                26 [81]
  HT Capability Info:    %0001100111101110 [82-83]
                              0....... ........ L-SIG TXOP Protection Support: Not Supported
                              .0...... ........ AP does Not allow use of 40MHz Transmissions In Neighboring BSSs
                              ..0..... ........ Reserved
                              ...1.... ........ BSS does Allow use of DSSS/CCK Rates @40MHz
                              ....1... ........ Maximal A-MSDU size: 7935 bytes
                              .....0.. ........ Does Not Support HT-Delayed BlockAck Operation
                              ......01 ........ Rx STBC: Rx Support of One Spatial Stream
                              ........ 1....... Transmitter does Support Tx STBC
                              ........ .1...... Short GI for 40 MHz: Supported
                              ........ ..1..... Short GI for 20 MHz: Supported
                              ........ ...0.... Can Not receive PPDUs with HT-Greenfield format
                              ........ ....11.. SM Power Save Disabled
                              ........ ......1. Both 20MHz and 40MHz Operation is Supported
                              ........ .......0 LDPC coding capability: Not Supported
  A-MPDU Parameters=%00011011
  Supported MCS Set
    Spatial Stream 1=%11111111
    Spatial Stream 2=%11111111
    Spatial Stream 3=%11111111
    Spatial Stream 4:     %00000000 [88]
    Rx Bitmask b32-b39:   %00000000 [89]
    Rx Bitmask b40-b47:   %00000000 [90]
    Rx Bitmask b48-b55:   %00000000 [91]
    Rx Bitmask b56-b63:   %00000000 [92]
    Rx Bitmask b64-b76:   %0000000000000 [93-94 Mask 0xFFF8]
    Reserved:             %000 [94 Mask 0x07]
    Highest Supported Rate:0  Mbps [95-96 Mask 0xFFC0]
    Reserved:             %000000 [96 Mask 0x3F]
    Tx Supported MCS Set: %0  Not Defined [97 Mask 0x80]
    Tx and Rx MCS Set:    %0  Equal [97 Mask 0x40]
    Tx Maximum Number Spatial Streams Supported:%00  1 Spatial Stream [97 Mask 0x30]
    Tx Unequal Modulation:%0  Not Supported [97 Mask 0x08]
    Reserved:             %000000000000000000000000000  b101-b127 [97-100 Mask 0x07FFFFFF]
  HT Extended Capabilities Info=%0000000000000000
  Tx Beam Forming Capability (TxBF)=%00000000000000000000000000000000
```

802.11 Beacon: 802.11n (HT) High Throughput



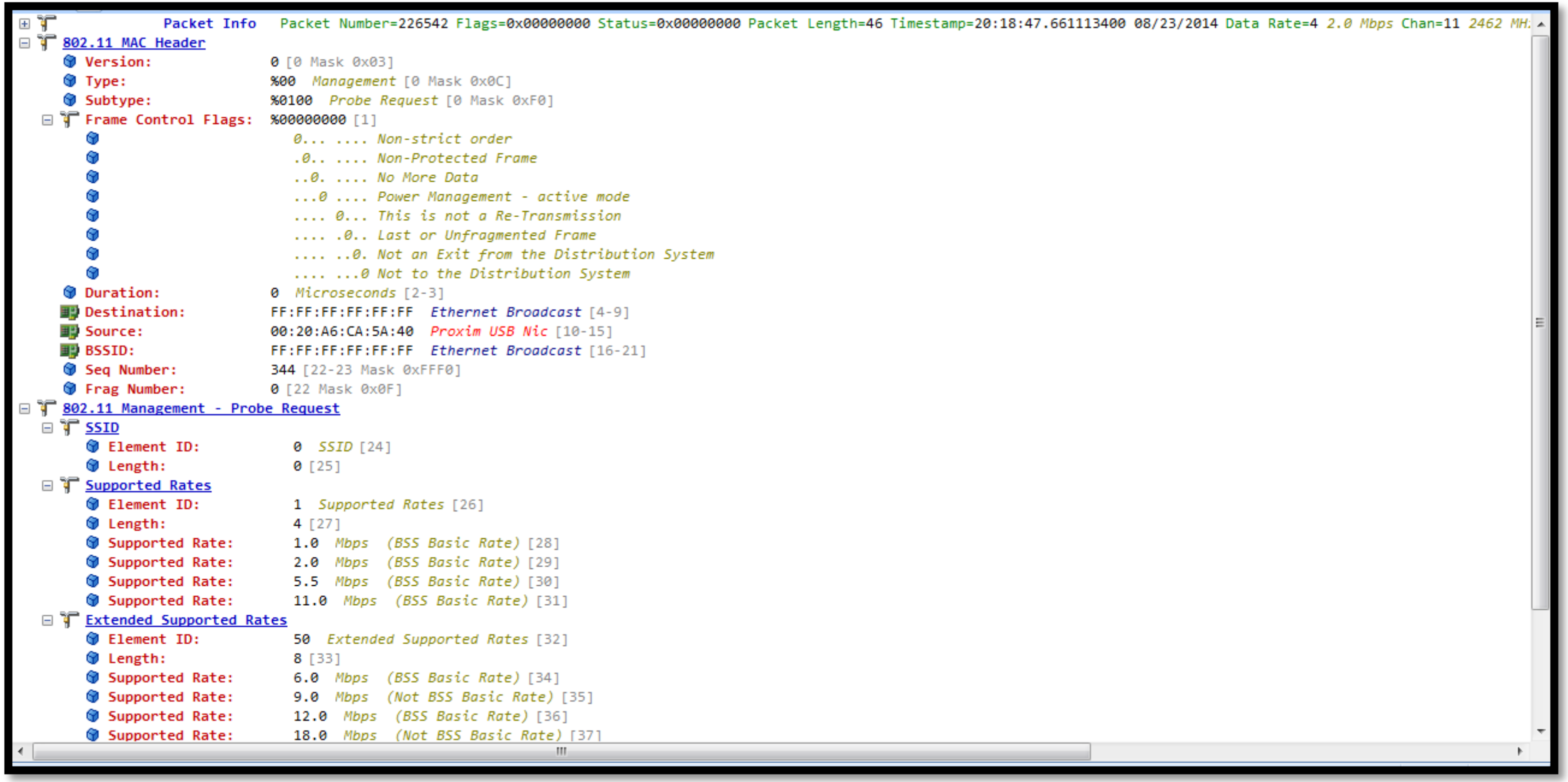
```
⊟ HT Operation Information
      Element ID:                61  HT Operation Information [130]
      Length:                    22 [131]
      Primary Channel:           44 [132]
   ⊟ HT Operation Element 1:%00000101 [133]
                                      ......01 2nd Channel Offset: Above the Primary Channel
                                      .....1.. STA Channel Width: Use Any Channel Width Enabled Under Supported Channel Width Set
                                      ....0... RIFS Mode: Use of RIFS Prohibited
                                      xxxx.... Reserved
   ⊟ HT Operation Element 2:%0000000000000111 [134-135]
                                      ........ ......11 HT Protection: HT Mixed Mode
                                      ........ .....1.. Non-Greenfield STAs: One or more HT STAs are Not Greenfield Capable
                                      ........ ....0... Transmit Burst Limit: No Limit
                                      ........ ...0.... OBSS Non-HT STAs: Use of Protection for Non-HT STAs Not Needed
                                      xxxxxxxx xxx..... Reserved
   ⊟ HT Operation Element 3:%0000000000000000 [136-137]
                                      ........ ..xxxxxx Reserved
                                      ........ .0...... Dual Beacon: No Secondary Beacon Transmitted
                                      ........ 0....... Dual CTS Protection: Not Required
                                      .......0 ........ Secondary Beacon: Primary Beacon
                                      ......0. ........ L-SIG TXOP Protection: Not Full Support
                                      .....0.. ........ PCO Active: Not Active in the BSS
                                      ....0... ........ PCO Phase: Switch To/Continue Use 20MHz Phase
                                      xxxx.... ........ Reserved
   ⊞ Basic MCS Set Rx Bitmask b16-b23=%00000000 Rx Bitmask b24-b31=%00000000 Rx Bitmask b32-b39=%00000000 Rx Bitmask b40-b47=%00000000 Rx Bitmask b48-b55=%00000000 Rx Bitmask
⊟ Extended Capabilities
      Element ID:                127  Extended Capabilities [154]
      Length:                    8 [155]
   ⊟ Extended Capabilities:%00000000 [156]
                                      ..x. x.x. Reserved
                                      0... .... dot11MgmtOptionEventsActivated is false
                                      .0.. .... the STA does not support S-PSMP
                                      ...0 .... the AP does not support PSMP operation
                                      .... .0.. Extended Channel Switching Not Supported
                                      .... ...0 20/40 BSS Coexistence Management Frame Not Supported
   ⊞ Extended Capabilities=%00010000
   ⊞ Extended Capabilities=%00000000
   ⊞ Extended Capabilities=%00000000
```

802.11 Beacon: 802.11ac (VHT) Very High Throughput



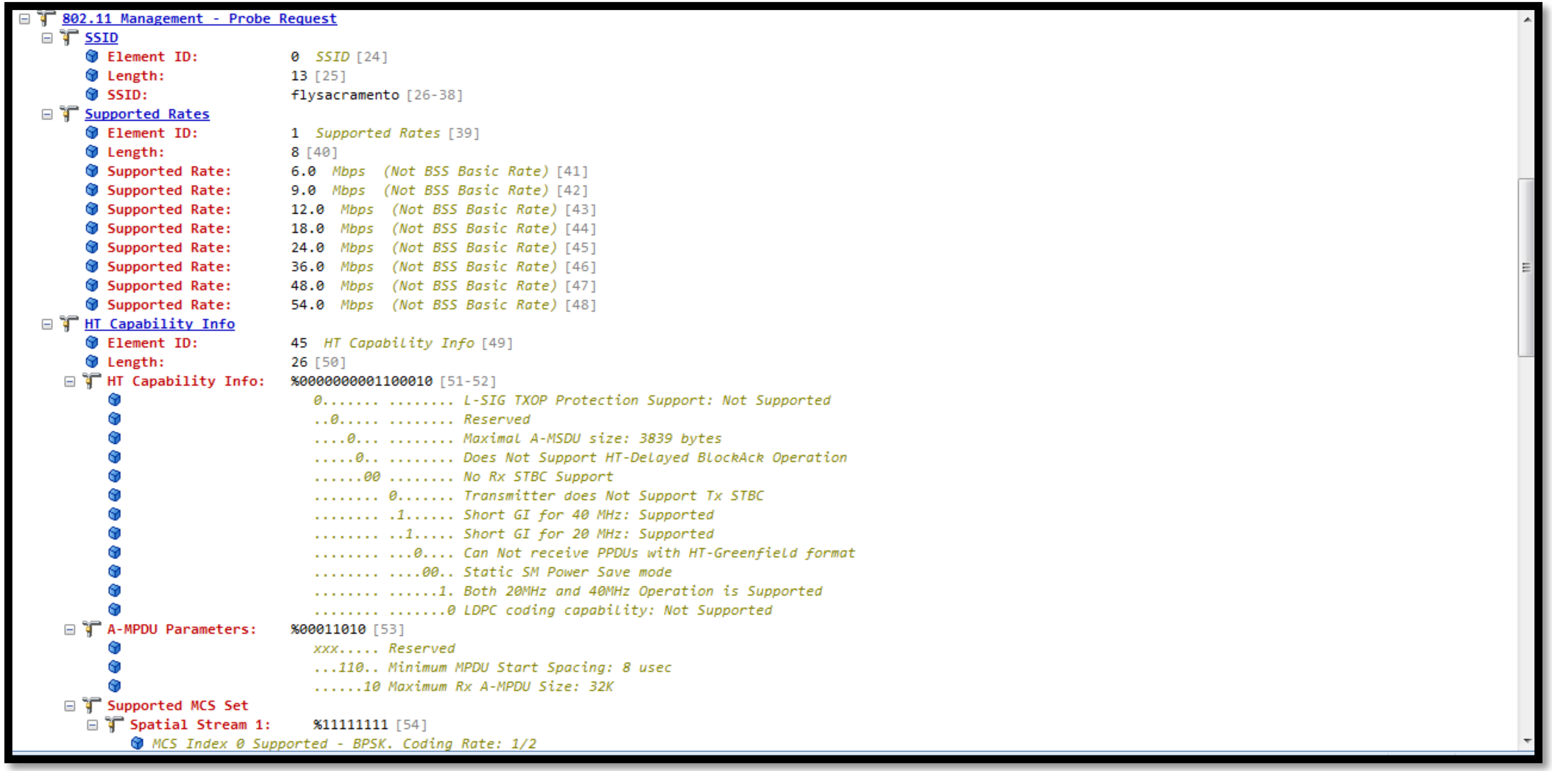
```
⊟ VHT Capabilities element
     Element ID:             191  VHT Capabilities element [204]
     Length:                 12 [205]
  ⊞ VHT Capabilities Info=%00001111100000110111100110110010
  ⊞ VHT Supported TX MCS Set=%00000000000000001111111111101010
  ⊞ VHT Supported RX MCS Set=%00000000000000001111111111101010
⊟ VHT Operation element
     Element ID:             192  VHT Operation element [218]
     Length:                 5 [219]
  ⊟ VHT Operation Information:0x000000 [220-222]
        Channel Width:           0  20 MHz or 40 MHz [220]
        Center Frequency Channel for 80 and 160 MHz operation: 0 [221]
        Center Frequency Channel for 80+80 MHz operation: 0 [222]
        VHT Basic MCS Set:       0 [223-224]
⊟ VHT Transmit Power Envelope
     Element ID:             195  VHT Transmit Power Envelope [225]
     Length:                 3 [226]
  ⊟ Transmit Power Information:0x01 [227]
        Reserved:                %00 [227 Mask 0xC0]
        Local Maximum Transmit Power Units Interpretation:%000  EIRP [227 Mask 0x38]
        Local Maximum Transmit Power Count:%001  20 MHz / 40 MHz [227 Mask 0x07]
     Local Maximum Transmit Power For 20 MHz:2 [228]
     Local Maximum Transmit Power For 40 MHz:2 [229]
⊟ WMM
     Element ID:             221  WMM [230]
     Length:                 24 [231]
     OUI:                    00-50-F2  MICROSOFT CORP. [232-234]
     OUI Type:               2 [235]
     OUI SubType:            1  Parameter Element [236]
     Version:                1 [237]
  ⊟ QoS Info:                %10000000 [238]
                                 1... .... WMM AP supports U-APSD
                                 .xxx .... Reserved
                                 .... 0000 Parameter Set Count: 0
     Reserved:               0x00 [239]
  ⊟ Access Category - Best Effort
     ⊟ ACI/AIFSN:                %00000011 [240]
                                     x... .... Reserved
                                     .00. .... ACI: Best Effort
For Help, press F1                                                                None
```

802.11 Probe: NULL Request



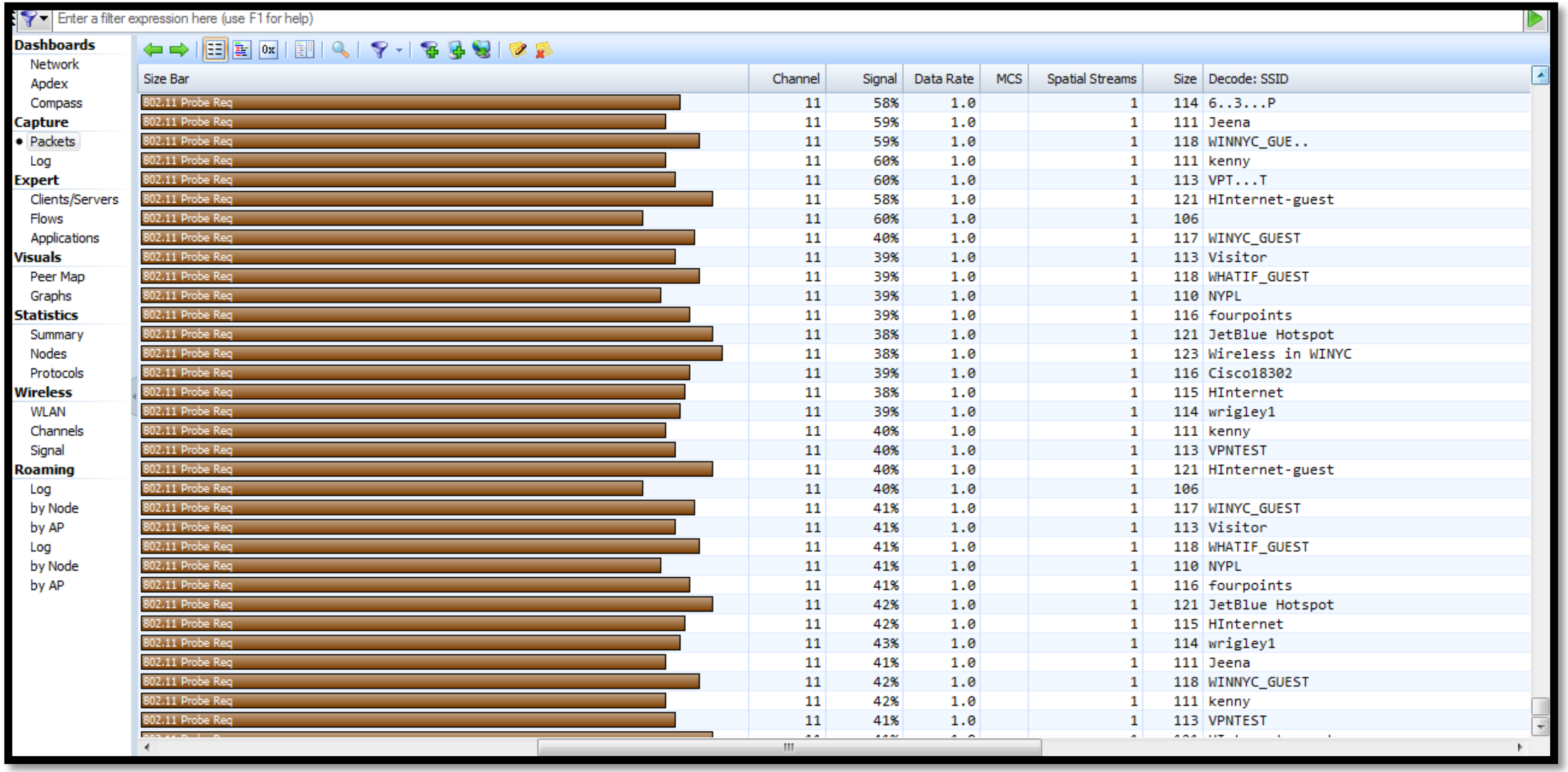
```
⊞          Packet Info   Packet Number=226542 Flags=0x00000000 Status=0x00000000 Packet Length=46 Timestamp=20:18:47.661113400 08/23/2014 Data Rate=4 2.0 Mbps Chan=11 2462 MH:
⊟ 802.11 MAC Header
     Version:                 0 [0 Mask 0x03]
     Type:                    %00  Management [0 Mask 0x0C]
     Subtype:                 %0100  Probe Request [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:                0  Microseconds [2-3]
     Destination:             FF:FF:FF:FF:FF:FF  Ethernet Broadcast [4-9]
     Source:                  00:20:A6:CA:5A:40  Proxim USB Nic [10-15]
     BSSID:                   FF:FF:FF:FF:FF:FF  Ethernet Broadcast [16-21]
     Seq Number:              344 [22-23 Mask 0xFFF0]
     Frag Number:             0 [22 Mask 0x0F]
⊟ 802.11 Management - Probe Request
  ⊟  SSID
        Element ID:              0  SSID [24]
        Length:                  0 [25]
  ⊟  Supported Rates
        Element ID:              1  Supported Rates [26]
        Length:                  4 [27]
        Supported Rate:          1.0  Mbps  (BSS Basic Rate) [28]
        Supported Rate:          2.0  Mbps  (BSS Basic Rate) [29]
        Supported Rate:          5.5  Mbps  (BSS Basic Rate) [30]
        Supported Rate:          11.0  Mbps  (BSS Basic Rate) [31]
  ⊟  Extended Supported Rates
        Element ID:              50  Extended Supported Rates [32]
        Length:                  8 [33]
        Supported Rate:          6.0  Mbps  (BSS Basic Rate) [34]
        Supported Rate:          9.0  Mbps  (Not BSS Basic Rate) [35]
        Supported Rate:          12.0  Mbps  (BSS Basic Rate) [36]
        Supported Rate:          18.0  Mbps  (Not BSS Basic Rate) [37]
```

802.11 Probe: Direct Request



```
802.11 Management - Probe Request
  SSID
      Element ID:           0  SSID [24]
      Length:               13 [25]
      SSID:                 flysacramento [26-38]
  Supported Rates
      Element ID:           1  Supported Rates [39]
      Length:               8 [40]
      Supported Rate:       6.0  Mbps  (Not BSS Basic Rate) [41]
      Supported Rate:       9.0  Mbps  (Not BSS Basic Rate) [42]
      Supported Rate:       12.0  Mbps  (Not BSS Basic Rate) [43]
      Supported Rate:       18.0  Mbps  (Not BSS Basic Rate) [44]
      Supported Rate:       24.0  Mbps  (Not BSS Basic Rate) [45]
      Supported Rate:       36.0  Mbps  (Not BSS Basic Rate) [46]
      Supported Rate:       48.0  Mbps  (Not BSS Basic Rate) [47]
      Supported Rate:       54.0  Mbps  (Not BSS Basic Rate) [48]
  HT Capability Info
      Element ID:           45  HT Capability Info [49]
      Length:               26 [50]
    HT Capability Info:     %0000000001100010 [51-52]
                              0....... ........ L-SIG TXOP Protection Support: Not Supported
                              ..0..... ........ Reserved
                              ....0... ........ Maximal A-MSDU size: 3839 bytes
                              .....0.. ........ Does Not Support HT-Delayed BlockAck Operation
                              ......00 ........ No Rx STBC Support
                              ........ 0....... Transmitter does Not Support Tx STBC
                              ........ .1...... Short GI for 40 MHz: Supported
                              ........ ..1..... Short GI for 20 MHz: Supported
                              ........ ...0.... Can Not receive PPDUs with HT-Greenfield format
                              ........ ....00.. Static SM Power Save mode
                              ........ ......1. Both 20MHz and 40MHz Operation is Supported
                              ........ .......0 LDPC coding capability: Not Supported
    A-MPDU Parameters:      %00011010 [53]
                              xxx..... Reserved
                              ...110.. Minimum MPDU Start Spacing: 8 usec
                              ......10 Maximum Rx A-MPDU Size: 32K
    Supported MCS Set
      Spatial Stream 1:       %11111111 [54]
          MCS Index 0 Supported - BPSK. Coding Rate: 1/2
```

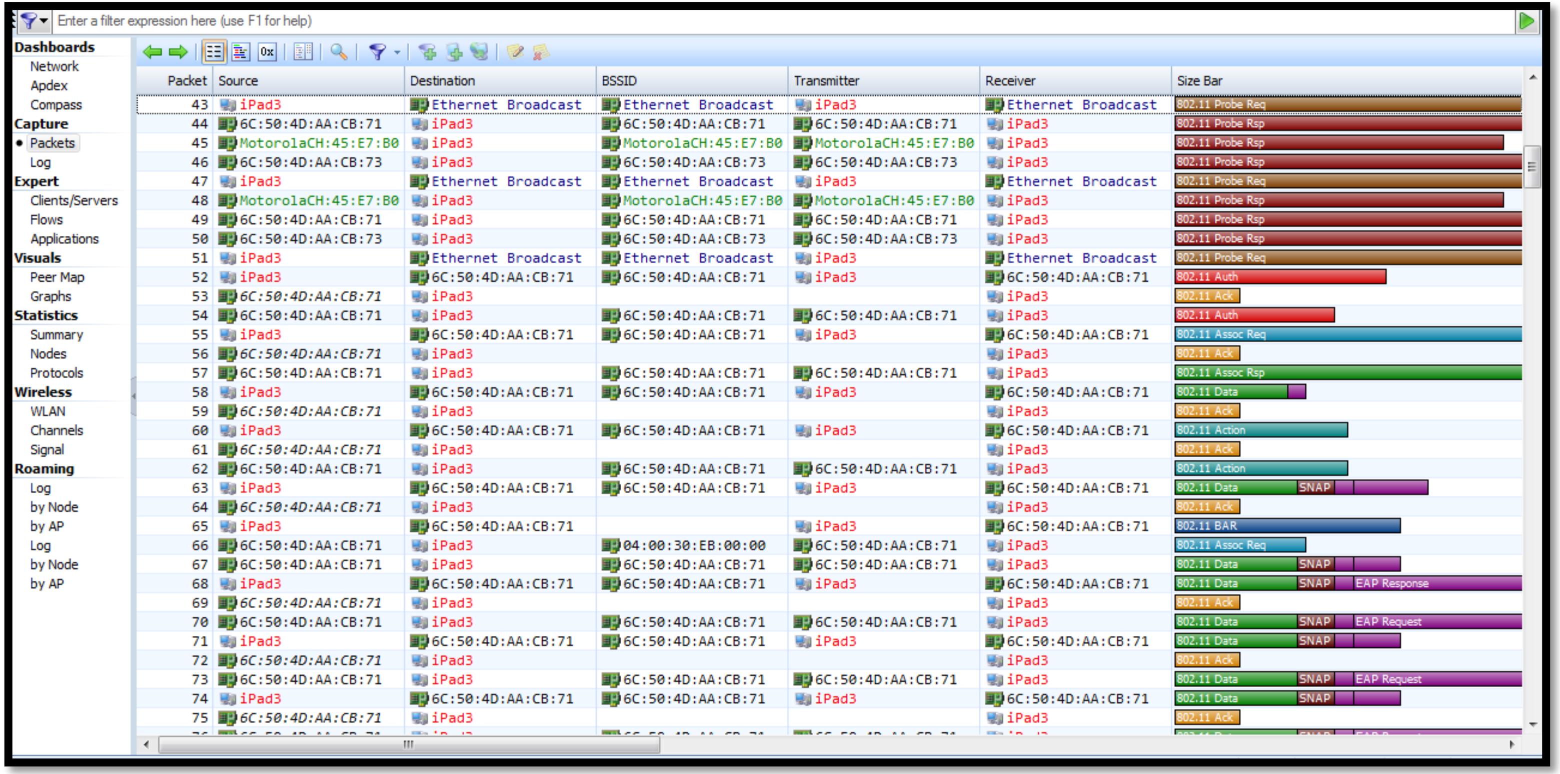
802.11 Probe: Request – Remembered Networks



Size Bar	Channel	Signal	Data Rate	MCS	Spatial Streams	Size	Decode: SSID
802.11 Probe Req	11	58%	1.0		1	114	6..3...P
802.11 Probe Req	11	59%	1.0		1	111	Jeena
802.11 Probe Req	11	59%	1.0		1	118	WINNYC_GUE..
802.11 Probe Req	11	60%	1.0		1	111	kenny
802.11 Probe Req	11	60%	1.0		1	113	VPT...T
802.11 Probe Req	11	58%	1.0		1	121	HInternet-guest
802.11 Probe Req	11	60%	1.0		1	106	
802.11 Probe Req	11	40%	1.0		1	117	WINYC_GUEST
802.11 Probe Req	11	39%	1.0		1	113	Visitor
802.11 Probe Req	11	39%	1.0		1	118	WHATIF_GUEST
802.11 Probe Req	11	39%	1.0		1	110	NYPL
802.11 Probe Req	11	39%	1.0		1	116	fourpoints
802.11 Probe Req	11	38%	1.0		1	121	JetBlue Hotspot
802.11 Probe Req	11	38%	1.0		1	123	Wireless in WINYC
802.11 Probe Req	11	39%	1.0		1	116	Cisco18302
802.11 Probe Req	11	38%	1.0		1	115	HInternet
802.11 Probe Req	11	39%	1.0		1	114	wrigley1
802.11 Probe Req	11	40%	1.0		1	111	kenny
802.11 Probe Req	11	40%	1.0		1	113	VPNTEST
802.11 Probe Req	11	40%	1.0		1	121	HInternet-guest
802.11 Probe Req	11	40%	1.0		1	106	
802.11 Probe Req	11	41%	1.0		1	117	WINYC_GUEST
802.11 Probe Req	11	41%	1.0		1	113	Visitor
802.11 Probe Req	11	41%	1.0		1	118	WHATIF_GUEST
802.11 Probe Req	11	41%	1.0		1	110	NYPL
802.11 Probe Req	11	41%	1.0		1	116	fourpoints
802.11 Probe Req	11	42%	1.0		1	121	JetBlue Hotspot
802.11 Probe Req	11	42%	1.0		1	115	HInternet
802.11 Probe Req	11	43%	1.0		1	114	wrigley1
802.11 Probe Req	11	41%	1.0		1	111	Jeena
802.11 Probe Req	11	42%	1.0		1	118	WINNYC_GUEST
802.11 Probe Req	11	42%	1.0		1	111	kenny
802.11 Probe Req	11	41%	1.0		1	113	VPNTEST

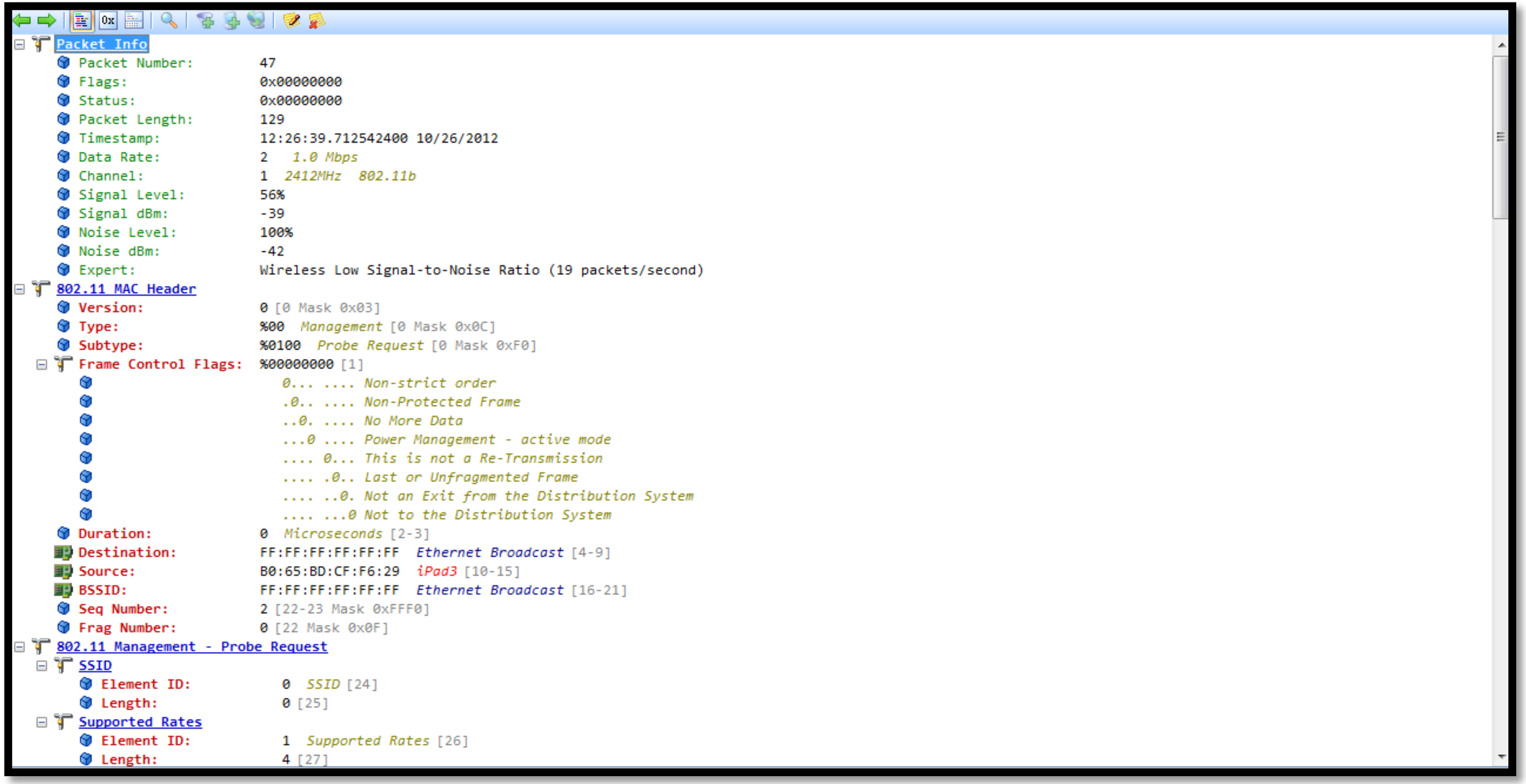
802.11 Probe / Auth / Assoc Flow

ANZ atmosphere2015 HOW TOMORROW MOVES



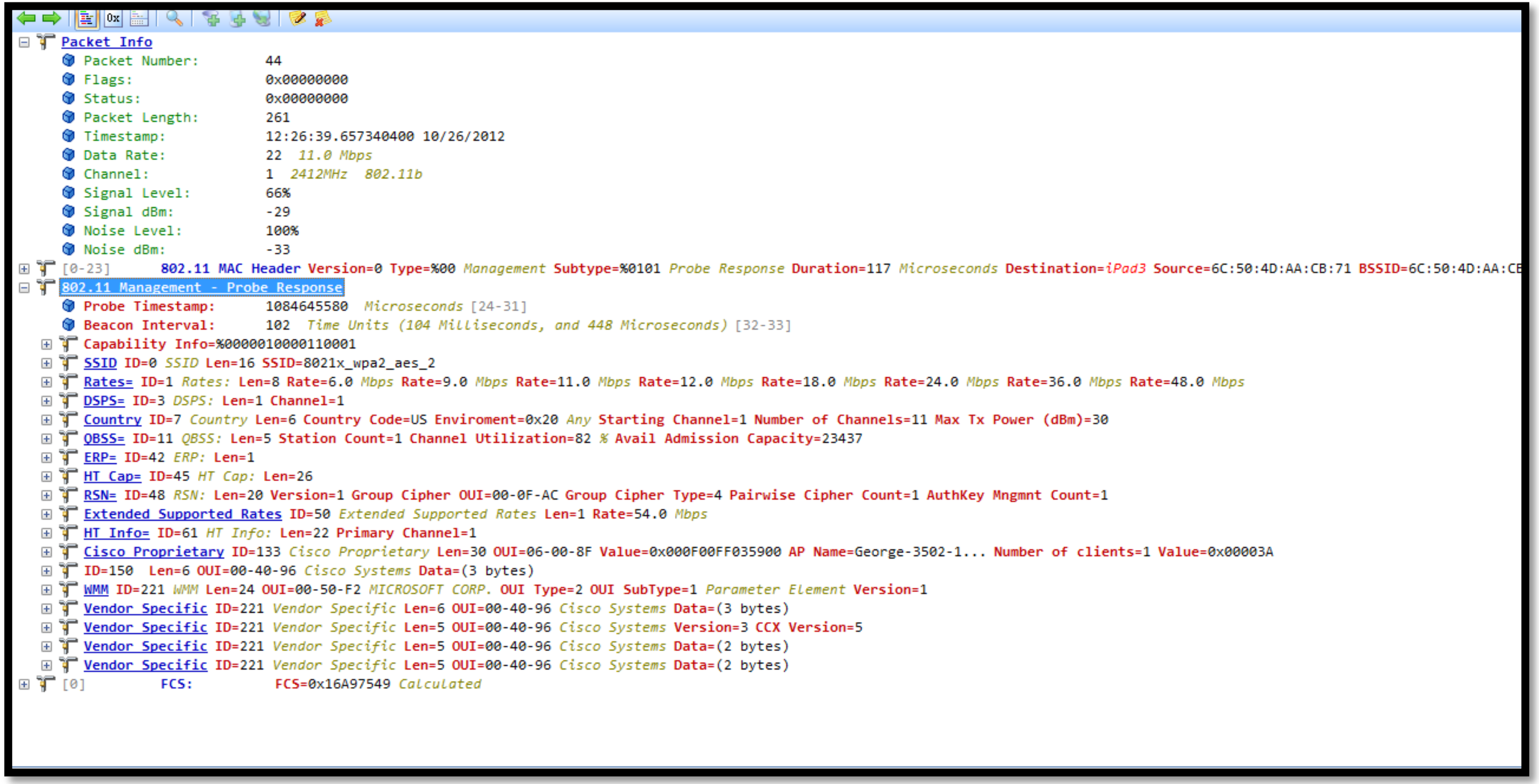
Packet	Source	Destination	BSSID	Transmitter	Receiver	Size Bar
43	iPad3	Ethernet Broadcast	Ethernet Broadcast	iPad3	Ethernet Broadcast	802.11 Probe Req
44	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Probe Rsp
45	MotorolaCH:45:E7:B0	iPad3	MotorolaCH:45:E7:B0	MotorolaCH:45:E7:B0	iPad3	802.11 Probe Rsp
46	6C:50:4D:AA:CB:73	iPad3	6C:50:4D:AA:CB:73	6C:50:4D:AA:CB:73	iPad3	802.11 Probe Rsp
47	iPad3	Ethernet Broadcast	Ethernet Broadcast	iPad3	Ethernet Broadcast	802.11 Probe Req
48	MotorolaCH:45:E7:B0	iPad3	MotorolaCH:45:E7:B0	MotorolaCH:45:E7:B0	iPad3	802.11 Probe Rsp
49	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Probe Rsp
50	6C:50:4D:AA:CB:73	iPad3	6C:50:4D:AA:CB:73	6C:50:4D:AA:CB:73	iPad3	802.11 Probe Rsp
51	iPad3	Ethernet Broadcast	Ethernet Broadcast	iPad3	Ethernet Broadcast	802.11 Probe Req
52	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Auth
53	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
54	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Auth
55	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Assoc Req
56	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
57	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Assoc Rsp
58	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data
59	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
60	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Action
61	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
62	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Action
63	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP
64	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
65	iPad3	6C:50:4D:AA:CB:71		iPad3	6C:50:4D:AA:CB:71	802.11 BAR
66	6C:50:4D:AA:CB:71	iPad3	04:00:30:EB:00:00	6C:50:4D:AA:CB:71	iPad3	802.11 Assoc Req
67	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP
68	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP EAP Response
69	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
70	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP
72	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
73	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
74	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP
75	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack

802.11 Probe: Request



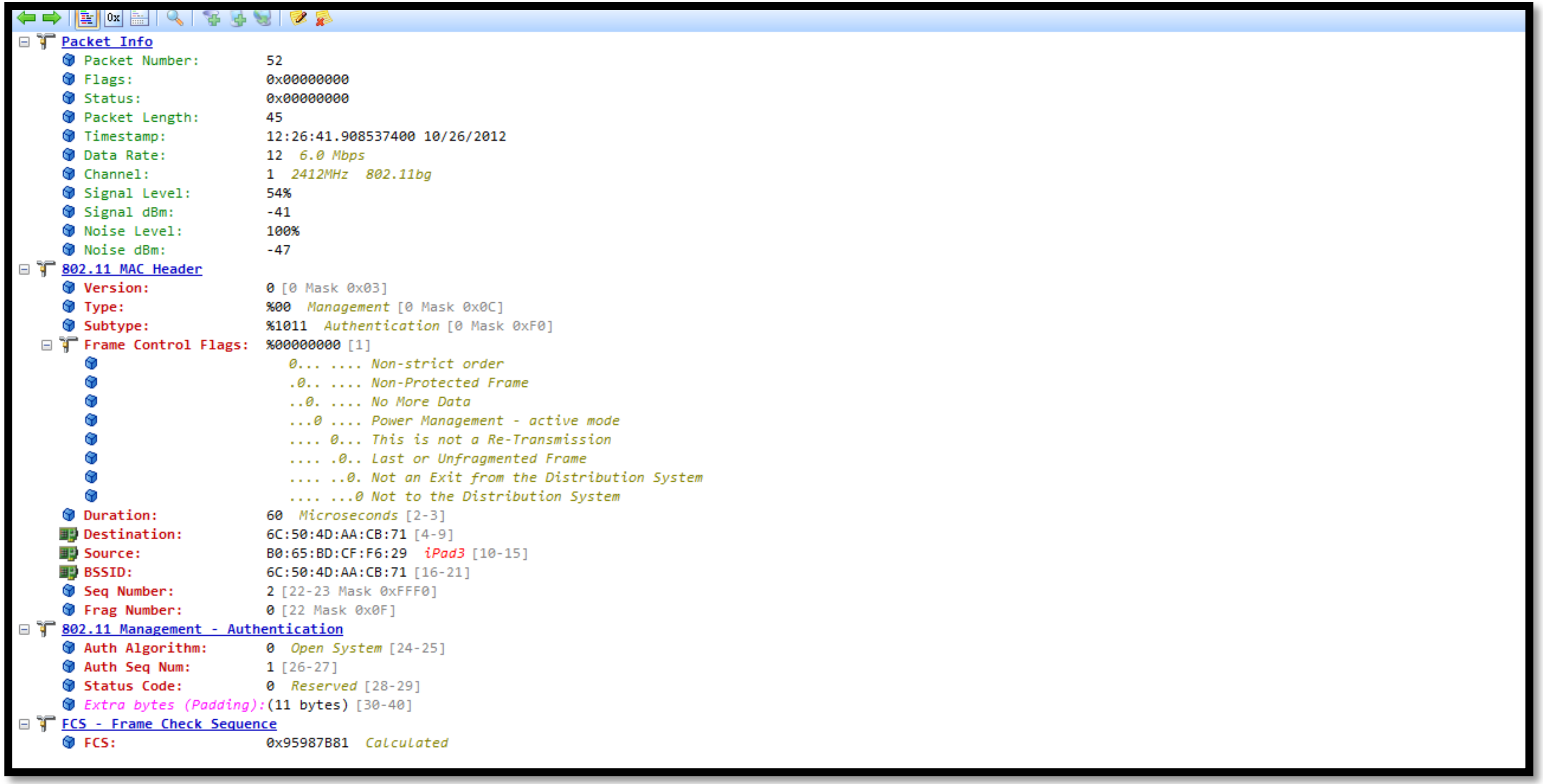
```
⊟ Packet Info
      Packet Number:          47
      Flags:                  0x00000000
      Status:                 0x00000000
      Packet Length:          129
      Timestamp:              12:26:39.712542400 10/26/2012
      Data Rate:              2   1.0 Mbps
      Channel:                1  2412MHz  802.11b
      Signal Level:           56%
      Signal dBm:             -39
      Noise Level:            100%
      Noise dBm:              -42
      Expert:                 Wireless Low Signal-to-Noise Ratio (19 packets/second)
⊟ 802.11 MAC Header
      Version:                0 [0 Mask 0x03]
      Type:                   %00  Management [0 Mask 0x0C]
      Subtype:                %0100  Probe Request [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:               0  Microseconds [2-3]
      Destination:            FF:FF:FF:FF:FF:FF  Ethernet Broadcast [4-9]
      Source:                 B0:65:BD:CF:F6:29  iPad3 [10-15]
      BSSID:                  FF:FF:FF:FF:FF:FF  Ethernet Broadcast [16-21]
      Seq Number:             2 [22-23 Mask 0xFFF0]
      Frag Number:            0 [22 Mask 0x0F]
⊟ 802.11 Management - Probe Request
   ⊟ SSID
         Element ID:             0  SSID [24]
         Length:                 0 [25]
   ⊟ Supported Rates
         Element ID:             1  Supported Rates [26]
         Length:                 4 [27]
```

802.11 Probe: Response



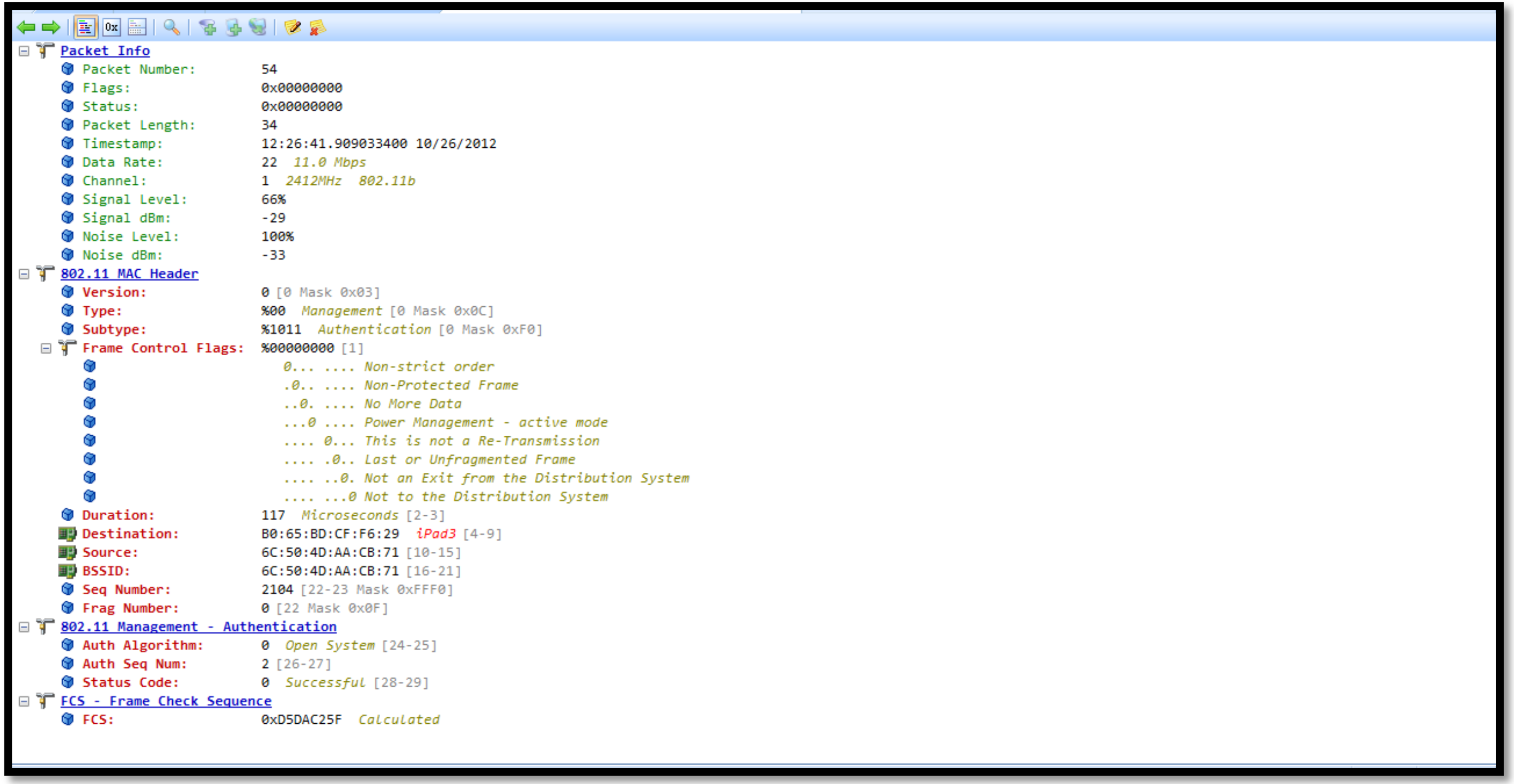
```
⊟ Packet Info
     Packet Number:         44
     Flags:                 0x00000000
     Status:                0x00000000
     Packet Length:         261
     Timestamp:             12:26:39.657340400 10/26/2012
     Data Rate:             22  11.0 Mbps
     Channel:               1  2412MHz  802.11b
     Signal Level:          66%
     Signal dBm:            -29
     Noise Level:           100%
     Noise dBm:             -33
⊞ [0-23]      802.11 MAC Header Version=0 Type=%00 Management Subtype=%0101 Probe Response Duration=117 Microseconds Destination=iPad3 Source=6C:50:4D:AA:CB:71 BSSID=6C:50:4D:AA:CB
⊟ 802.11 Management - Probe Response
     Probe Timestamp:       1084645580  Microseconds [24-31]
     Beacon Interval:       102  Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
  ⊞ Capability Info=%0000010000110001
  ⊞ SSID ID=0 SSID Len=16 SSID=8021x_wpa2_aes_2
  ⊞ Rates= ID=1 Rates: Len=8 Rate=6.0 Mbps Rate=9.0 Mbps Rate=11.0 Mbps Rate=12.0 Mbps Rate=18.0 Mbps Rate=24.0 Mbps Rate=36.0 Mbps Rate=48.0 Mbps
  ⊞ DSPS= ID=3 DSPS: Len=1 Channel=1
  ⊞ Country ID=7 Country Len=6 Country Code=US Enviroment=0x20 Any Starting Channel=1 Number of Channels=11 Max Tx Power (dBm)=30
  ⊞ QBSS= ID=11 QBSS: Len=5 Station Count=1 Channel Utilization=82 % Avail Admission Capacity=23437
  ⊞ ERP= ID=42 ERP: Len=1
  ⊞ HT Cap= ID=45 HT Cap: Len=26
  ⊞ 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
  ⊞ Extended Supported Rates ID=50 Extended Supported Rates Len=1 Rate=54.0 Mbps
  ⊞ HT Info= ID=61 HT Info: Len=22 Primary Channel=1
  ⊞ Cisco Proprietary ID=133 Cisco Proprietary Len=30 OUI=06-00-8F Value=0x000F00FF035900 AP Name=George-3502-1... Number of clients=1 Value=0x00003A
  ⊞ ID=150  Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
  ⊞ WMM ID=221 WMM Len=24 OUI=00-50-F2 MICROSOFT CORP. OUI Type=2 OUI SubType=1 Parameter Element Version=1
  ⊞ Vendor Specific ID=221 Vendor Specific Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
  ⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Version=3 CCX Version=5
  ⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Data=(2 bytes)
  ⊞ Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Data=(2 bytes)
⊞ [0]         FCS:            FCS=0x16A97549 Calculated
```

802.11: Authentication



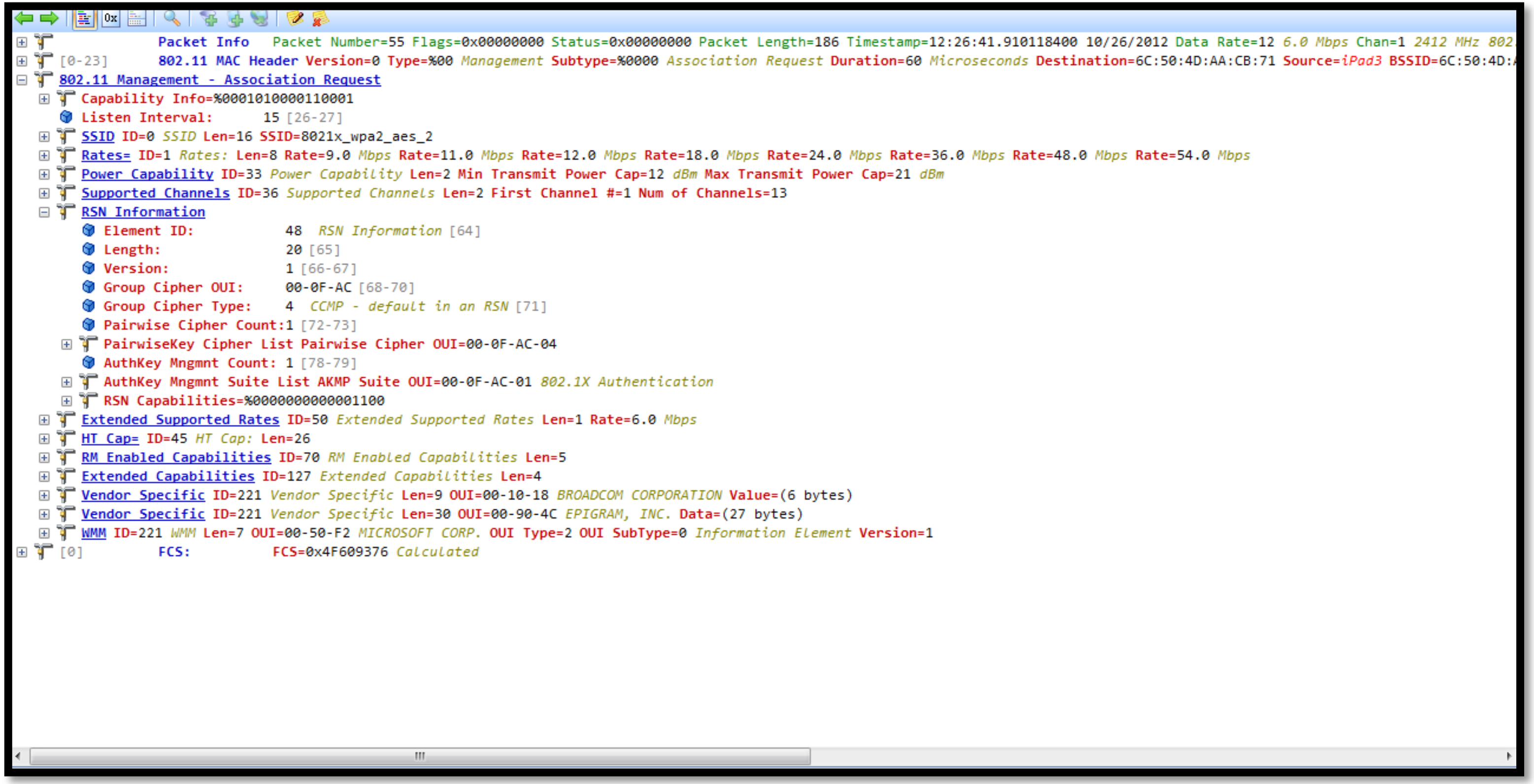
```
⊟ Packet Info
     Packet Number:          52
     Flags:                  0x00000000
     Status:                 0x00000000
     Packet Length:          45
     Timestamp:              12:26:41.908537400 10/26/2012
     Data Rate:              12  6.0 Mbps
     Channel:                1  2412MHz  802.11bg
     Signal Level:           54%
     Signal dBm:             -41
     Noise Level:            100%
     Noise dBm:              -47
⊟ 802.11 MAC Header
     Version:                0 [0 Mask 0x03]
     Type:                   %00  Management [0 Mask 0x0C]
     Subtype:                %1011  Authentication [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:               60  Microseconds [2-3]
     Destination:            6C:50:4D:AA:CB:71 [4-9]
     Source:                 B0:65:BD:CF:F6:29  iPad3 [10-15]
     BSSID:                  6C:50:4D:AA:CB:71 [16-21]
     Seq Number:             2 [22-23 Mask 0xFFF0]
     Frag Number:            0 [22 Mask 0x0F]
⊟ 802.11 Management - Authentication
     Auth Algorithm:         0  Open System [24-25]
     Auth Seq Num:           1 [26-27]
     Status Code:            0  Reserved [28-29]
     Extra bytes (Padding):(11 bytes) [30-40]
⊟ FCS - Frame Check Sequence
     FCS:                    0x95987B81  Calculated
```

802.11: Authentication



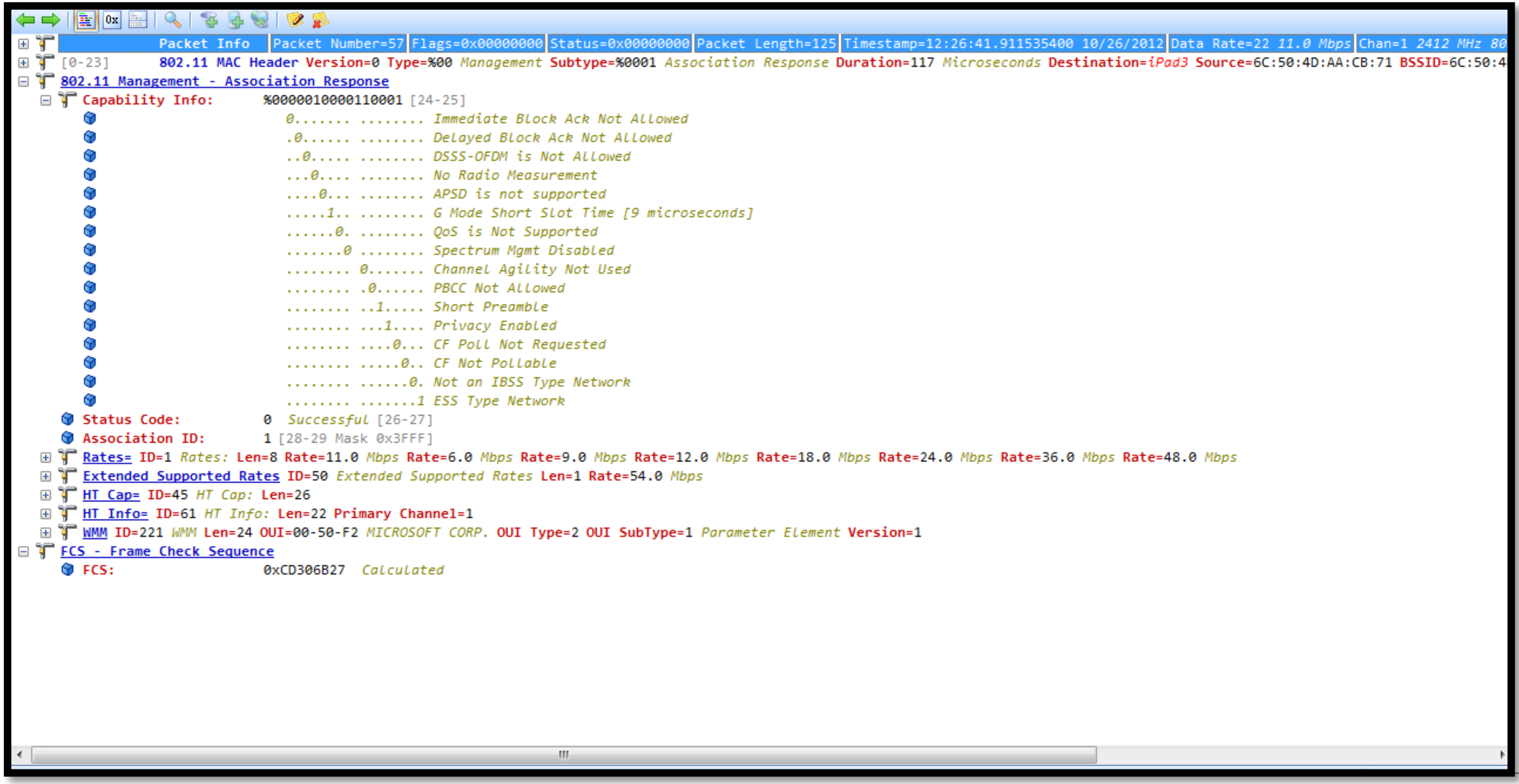
```
⊟ Packet Info
     Packet Number:          54
     Flags:                  0x00000000
     Status:                 0x00000000
     Packet Length:          34
     Timestamp:              12:26:41.909033400 10/26/2012
     Data Rate:              22  11.0 Mbps
     Channel:                1  2412MHz  802.11b
     Signal Level:           66%
     Signal dBm:             -29
     Noise Level:            100%
     Noise dBm:              -33
⊟ 802.11 MAC Header
     Version:                0 [0 Mask 0x03]
     Type:                   %00  Management [0 Mask 0x0C]
     Subtype:                %1011  Authentication [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:               117  Microseconds [2-3]
     Destination:            B0:65:BD:CF:F6:29  iPad3 [4-9]
     Source:                 6C:50:4D:AA:CB:71 [10-15]
     BSSID:                  6C:50:4D:AA:CB:71 [16-21]
     Seq Number:             2104 [22-23 Mask 0xFFF0]
     Frag Number:            0 [22 Mask 0x0F]
⊟ 802.11 Management - Authentication
     Auth Algorithm:         0  Open System [24-25]
     Auth Seq Num:           2 [26-27]
     Status Code:            0  Successful [28-29]
⊟ FCS - Frame Check Sequence
     FCS:                    0xD5DAC25F  Calculated
```

802.11: Association Request



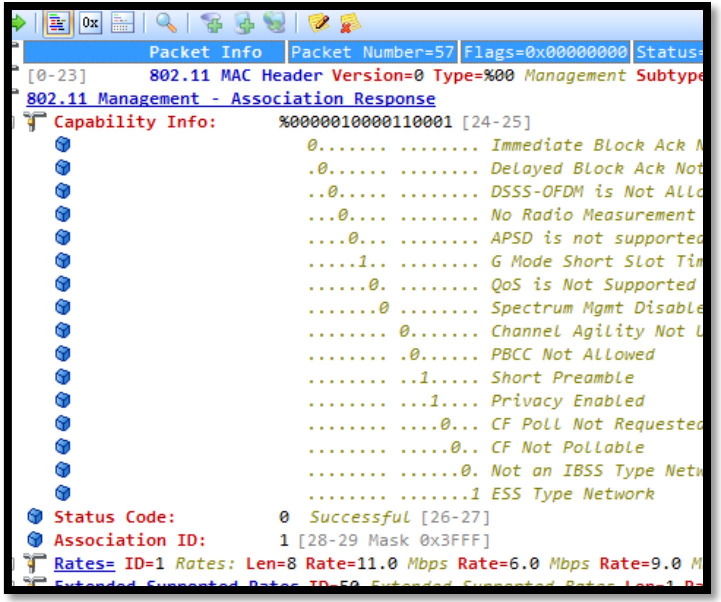
```
⊞          Packet Info   Packet Number=55 Flags=0x00000000 Status=0x00000000 Packet Length=186 Timestamp=12:26:41.910118400 10/26/2012 Data Rate=12 6.0 Mbps Chan=1 2412 MHz 802
⊞ [0-23]   802.11 MAC Header Version=0 Type=%00 Management Subtype=%0000 Association Request Duration=60 Microseconds Destination=6C:50:4D:AA:CB:71 Source=iPad3 BSSID=6C:50:4D:
⊟ 802.11 Management - Association Request
   ⊞ Capability Info=%0001010000110001
     Listen Interval:       15 [26-27]
   ⊞ SSID ID=0 SSID Len=16 SSID=8021x_wpa2_aes_2
   ⊞ Rates= ID=1 Rates: Len=8 Rate=9.0 Mbps Rate=11.0 Mbps Rate=12.0 Mbps Rate=18.0 Mbps Rate=24.0 Mbps Rate=36.0 Mbps Rate=48.0 Mbps Rate=54.0 Mbps
   ⊞ Power Capability ID=33 Power Capability Len=2 Min Transmit Power Cap=12 dBm Max Transmit Power Cap=21 dBm
   ⊞ Supported Channels ID=36 Supported Channels Len=2 First Channel #=1 Num of Channels=13
   ⊟ RSN Information
        Element ID:           48  RSN Information [64]
        Length:               20 [65]
        Version:              1 [66-67]
        Group Cipher OUI:     00-0F-AC [68-70]
        Group Cipher Type:    4  CCMP - default in an RSN [71]
        Pairwise Cipher Count:1 [72-73]
      ⊞ PairwiseKey Cipher List Pairwise Cipher OUI=00-0F-AC-04
        AuthKey Mngmnt Count: 1 [78-79]
      ⊞ AuthKey Mngmnt Suite List AKMP Suite OUI=00-0F-AC-01 802.1X Authentication
      ⊞ RSN Capabilities=%0000000000001100
   ⊞ Extended Supported Rates ID=50 Extended Supported Rates Len=1 Rate=6.0 Mbps
   ⊞ HT Cap= ID=45 HT Cap: Len=26
   ⊞ RM Enabled Capabilities ID=70 RM Enabled Capabilities Len=5
   ⊞ Extended Capabilities ID=127 Extended Capabilities Len=4
   ⊞ Vendor Specific ID=221 Vendor Specific Len=9 OUI=00-10-18 BROADCOM CORPORATION Value=(6 bytes)
   ⊞ Vendor Specific ID=221 Vendor Specific Len=30 OUI=00-90-4C EPIGRAM, INC. Data=(27 bytes)
   ⊞ WMM ID=221 WMM Len=7 OUI=00-50-F2 MICROSOFT CORP. OUI Type=2 OUI SubType=0 Information Element Version=1
⊞ [0]      FCS:          FCS=0x4F609376 Calculated
```

802.11: Association Response

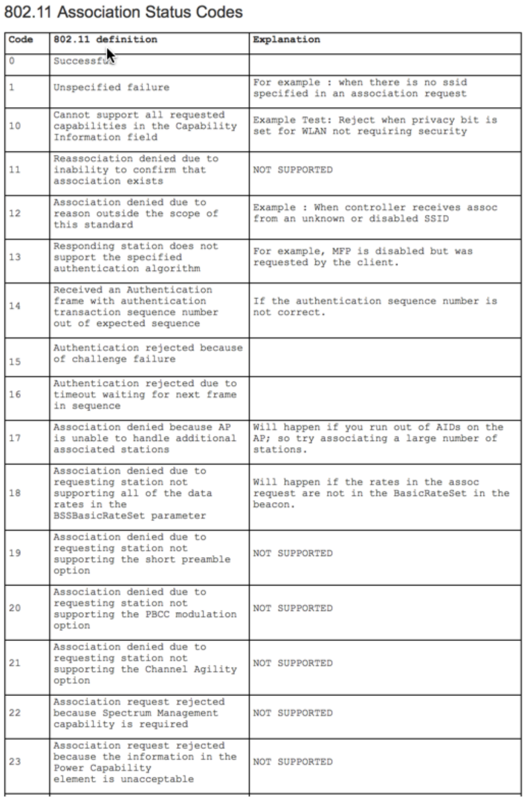


```
⊞           Packet Info   Packet Number=57 Flags=0x00000000 Status=0x00000000 Packet Length=125 Timestamp=12:26:41.911535400 10/26/2012 Data Rate=22 11.0 Mbps Chan=1 2412 MHz 80
⊞ [0-23]       802.11 MAC Header Version=0 Type=%00 Management Subtype=%0001 Association Response Duration=117 Microseconds Destination=iPad3 Source=6C:50:4D:AA:CB:71 BSSID=6C:50:4
⊟ 802.11 Management - Association Response
  ⊟ Capability Info:        %0000010000110001 [24-25]
                              0....... ........ Immediate Block Ack Not Allowed
                              .0...... ........ Delayed Block Ack Not Allowed
                              ..0..... ........ DSSS-OFDM is Not Allowed
                              ...0.... ........ No Radio Measurement
                              ....0... ........ APSD is not supported
                              .....1.. ........ G Mode Short Slot Time [9 microseconds]
                              ......0. ........ QoS is Not Supported
                              .......0 ........ Spectrum Mgmt Disabled
                              ........ 0....... Channel Agility Not Used
                              ........ .0...... PBCC Not Allowed
                              ........ ..1..... Short Preamble
                              ........ ...1.... Privacy Enabled
                              ........ ....0... CF Poll Not Requested
                              ........ .....0.. CF Not Pollable
                              ........ ......0. Not an IBSS Type Network
                              ........ .......1 ESS Type Network
    Status Code:            0  Successful [26-27]
    Association ID:         1 [28-29 Mask 0x3FFF]
  ⊞ Rates= ID=1 Rates: Len=8 Rate=11.0 Mbps 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
  ⊞ Extended Supported Rates ID=50 Extended Supported Rates Len=1 Rate=54.0 Mbps
  ⊞ HT Cap= ID=45 HT Cap: Len=26
  ⊞ HT Info= ID=61 HT Info: Len=22 Primary Channel=1
  ⊞ WMM ID=221 WMM Len=24 OUI=00-50-F2 MICROSOFT CORP. OUI Type=2 OUI SubType=1 Parameter Element Version=1
⊟ FCS - Frame Check Sequence
    FCS:                    0xCD306B27   Calculated
```

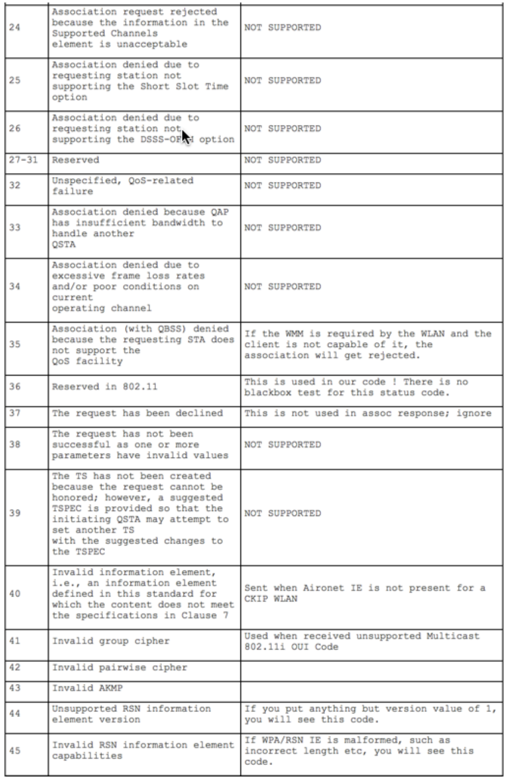
802.11: Status Codes



```
Packet Info    Packet Number=57 Flags=0x00000000 Status=
[0-23]      802.11 MAC Header Version=0 Type=%00 Management Subtype
802.11 Management - Association Response
Capability Info:       %0000010000110001 [24-25]
                          0....... ........ Immediate Block Ack N
                          .0...... ........ Delayed Block Ack Not
                          ..0..... ........ DSSS-OFDM is Not Allo
                          ...0.... ........ No Radio Measurement
                          ....0... ........ APSD is not supported
                          .....1.. ........ G Mode Short Slot Tim
                          ......0. ........ QoS is Not Supported
                          .......0 ........ Spectrum Mgmt Disable
                          ........ 0....... Channel Agility Not U
                          ........ .0...... PBCC Not Allowed
                          ........ ..1..... Short Preamble
                          ........ ...1.... Privacy Enabled
                          ........ ....0... CF Poll Not Requested
                          ........ .....0.. CF Not Pollable
                          ........ ......0. Not an IBSS Type Netw
                          ........ .......1 ESS Type Network
Status Code:           0  Successful [26-27]
Association ID:        1 [28-29 Mask 0x3FFF]
Rates= ID=1 Rates: Len=8 Rate=11.0 Mbps Rate=6.0 Mbps Rate=9.0 M
```



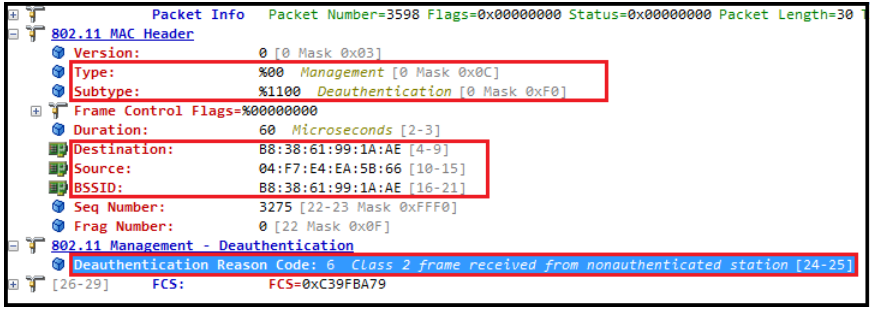
802.11 Association Status Codes



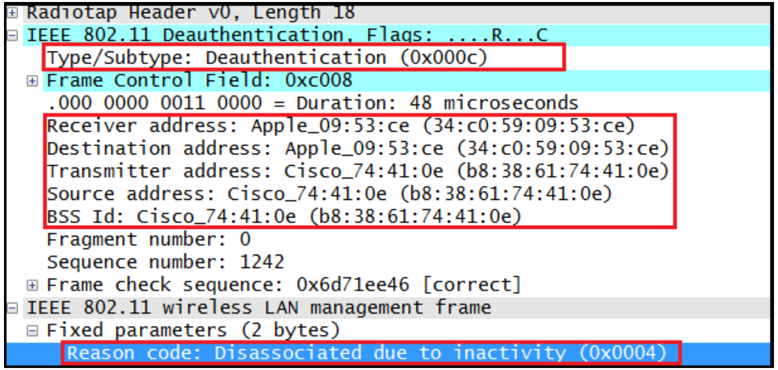
Code	802.11 definition	Explanation
0	Successful	
1	Unspecified failure	For example : when there is no ssid specified in an association request
10	Cannot support all requested capabilities in the Capability Information field	Example Test: Reject when privacy bit is set for WLAN not requiring security
11	Reassociation denied due to inability to confirm that association exists	NOT SUPPORTED
12	Association denied due to reason outside the scope of this standard	Example : When controller receives assoc from an unknown or disabled SSID
13	Responding station does not support the specified authentication algorithm	For example, MFP is disabled but was requested by the client.
14	Received an Authentication frame with authentication transaction sequence number out of expected sequence	If the authentication sequence number is not correct.
15	Authentication rejected because of challenge failure	
16	Authentication rejected due to timeout waiting for next frame in sequence	
17	Association denied because AP is unable to handle additional associated stations	Will happen if you run out of AIDs on the AP; so try associating a large number of stations.
18	Association denied due to requesting station not supporting all of the data rates in the BSSBasicRateSet parameter	Will happen if the rates in the assoc request are not in the BasicRateSet in the beacon.
19	Association denied due to requesting station not supporting the short preamble option	NOT SUPPORTED
20	Association denied due to requesting station not supporting the PBCC modulation option	NOT SUPPORTED
21	Association denied due to requesting station not supporting the Channel Agility option	NOT SUPPORTED
22	Association request rejected because Spectrum Management capability is required	NOT SUPPORTED
23	Association request rejected because the information in the Power Capability element is unacceptable	NOT SUPPORTED
24	Association request rejected because the information in the Supported Channels element is unacceptable	NOT SUPPORTED
25	Association denied due to requesting station not supporting the Short Slot Time option	NOT SUPPORTED
26	Association denied due to requesting station not supporting the DSSS-OFDM option	NOT SUPPORTED
27-31	Reserved	NOT SUPPORTED
32	Unspecified, QoS-related failure	NOT SUPPORTED
33	Association denied because QAP has insufficient bandwidth to handle another QSTA	NOT SUPPORTED
34	Association denied due to excessive frame loss rates and/or poor conditions on current operating channel	NOT SUPPORTED
35	Association (with QBSS) denied because the requesting STA does not support the QoS facility	If the WMM is required by the WLAN and the client is not capable of it, the association will get rejected.
36	Reserved in 802.11	This is used in our code ! There is no blackbox test for this status code.
37	The request has been declined	This is not used in assoc response; ignore
38	The request has not been successful as one or more parameters have invalid values	NOT SUPPORTED
39	The TS has not been created because the request cannot be honored; however, a suggested TSPEC is provided so that the initiating QSTA may attempt to set another TS with the suggested changes to the TSPEC	NOT SUPPORTED
40	Invalid information element, i.e., an information element defined in this standard for which the content does not meet the specifications in Clause 7	Sent when Aironet IE is not present for a CKIP WLAN
41	Invalid group cipher	Used when received unsupported Multicast 802.11i OUI Code
42	Invalid pairwise cipher	
43	Invalid AKMP	
44	Unsupported RSN information element version	If you put anything but version value of 1, you will see this code.
45	Invalid RSN information element capabilities	If WPA/RSN IE is malformed, such as incorrect length etc, you will see this code.

802.11: Reason Codes

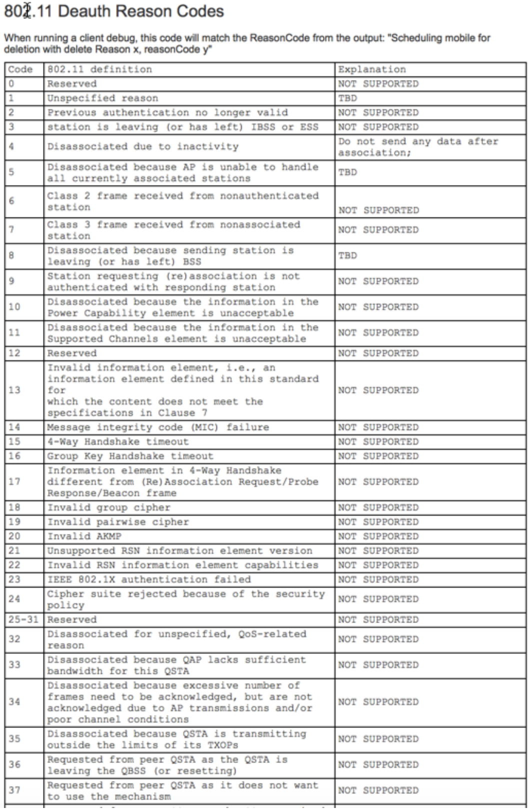
ANZ atmosphere 2015 HOW TOMORROW MOVES



```
⊞ Packet Info   Packet Number=3598 Flags=0x00000000 Status=0x00000000 Packet Length=30
⊟ 802.11 MAC Header
    Version:              0 [0 Mask 0x03]
    Type:                 %00  Management [0 Mask 0x0C]
    Subtype:              %1100  Deauthentication [0 Mask 0xF0]
  ⊞ Frame Control Flags=%00000000
    Duration:             60  Microseconds [2-3]
    Destination:          B8:38:61:99:1A:AE [4-9]
    Source:               04:F7:E4:EA:5B:66 [10-15]
    BSSID:                B8:38:61:99:1A:AE [16-21]
    Seq Number:           3275 [22-23 Mask 0xFFF0]
    Frag Number:          0 [22 Mask 0x0F]
⊟ 802.11 Management - Deauthentication
    Deauthentication Reason Code: 6  Class 2 frame received from nonauthenticated station [24-25]
⊞ [26-29]      FCS:        FCS=0xC39FBA79
```



```
⊞ Radiotap Header v0, Length 18
⊟ IEEE 802.11 Deauthentication, Flags: ....R...C
    Type/Subtype: Deauthentication (0x000c)
  ⊞ Frame Control Field: 0xc008
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: Apple_09:53:ce (34:c0:59:09:53:ce)
    Destination address: Apple_09:53:ce (34:c0:59:09:53:ce)
    Transmitter address: Cisco_74:41:0e (b8:38:61:74:41:0e)
    Source address: Cisco_74:41:0e (b8:38:61:74:41:0e)
    BSS Id: Cisco_74:41:0e (b8:38:61:74:41:0e)
    Fragment number: 0
    Sequence number: 1242
  ⊞ Frame check sequence: 0x6d71ee46 [correct]
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters (2 bytes)
      Reason code: Disassociated due to inactivity (0x0004)
```

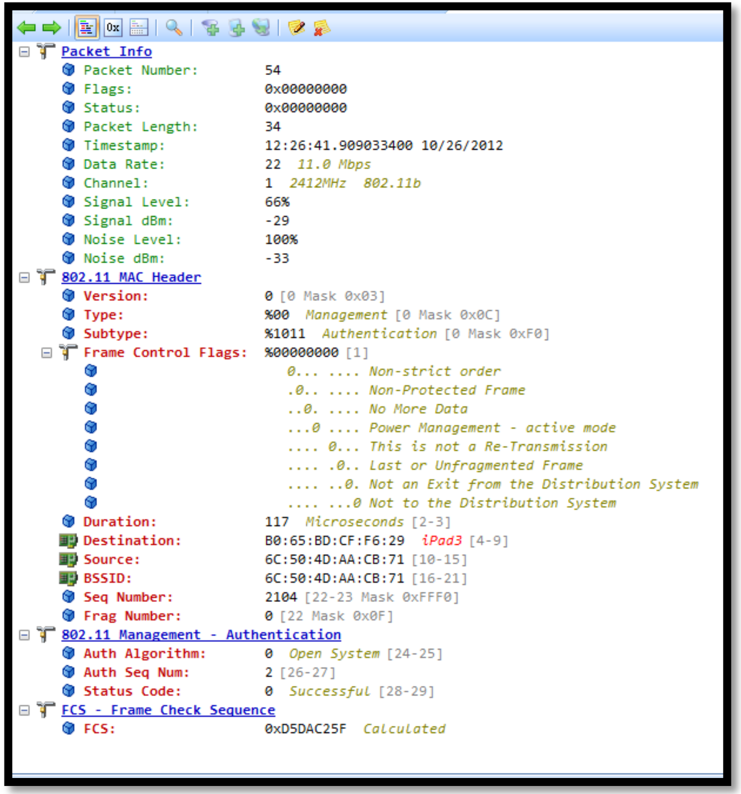


802.11 Deauth Reason Codes

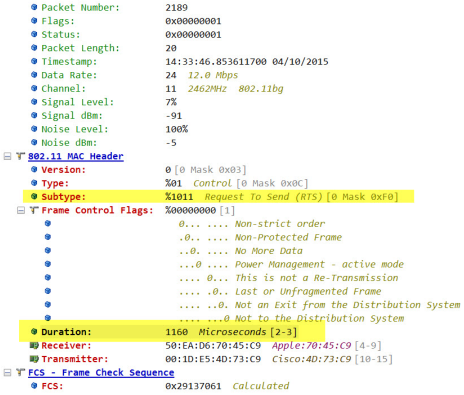
When running a client debug, this code will match the ReasonCode from the output: "Scheduling mobile for deletion with delete Reason x, reasonCode y"

Code	802.11 definition	Explanation
0	Reserved	NOT SUPPORTED
1	Unspecified reason	TBD
2	Previous authentication no longer valid	NOT SUPPORTED
3	station is leaving (or has left) IBSS or ESS	NOT SUPPORTED
4	Disassociated due to inactivity	Do not send any data after association;
5	Disassociated because AP is unable to handle all currently associated stations	TBD
6	Class 2 frame received from nonauthenticated station	NOT SUPPORTED
7	Class 3 frame received from nonassociated station	NOT SUPPORTED
8	Disassociated because sending station is leaving (or has left) BSS	TBD
9	Station requesting (re)association is not authenticated with responding station	NOT SUPPORTED
10	Disassociated because the information in the Power Capability element is unacceptable	NOT SUPPORTED
11	Disassociated because the information in the Supported Channels element is unacceptable	NOT SUPPORTED
12	Reserved	NOT SUPPORTED
13	Invalid information element, i.e., an information element defined in this standard for which the content does not meet the specifications in Clause 7	NOT SUPPORTED
14	Message integrity code (MIC) failure	NOT SUPPORTED
15	4-Way Handshake timeout	NOT SUPPORTED
16	Group Key Handshake timeout	NOT SUPPORTED
17	Information element in 4-Way Handshake different from (Re)Association Request/Probe Response/Beacon frame	NOT SUPPORTED
18	Invalid group cipher	NOT SUPPORTED
19	Invalid pairwise cipher	NOT SUPPORTED
20	Invalid AKMP	NOT SUPPORTED
21	Unsupported RSN information element version	NOT SUPPORTED
22	Invalid RSN information element capabilities	NOT SUPPORTED
23	IEEE 802.1X authentication failed	NOT SUPPORTED
24	Cipher suite rejected because of the security policy	NOT SUPPORTED
25-31	Reserved	NOT SUPPORTED
32	Disassociated for unspecified, QoS-related reason	NOT SUPPORTED
33	Disassociated because QAP lacks sufficient bandwidth for this QSTA	NOT SUPPORTED
34	Disassociated because excessive number of frames need to be acknowledged, but are not acknowledged due to AP transmissions and/or poor channel conditions	NOT SUPPORTED
35	Disassociated because QSTA is transmitting outside the limits of its TXOPs	NOT SUPPORTED
36	Requested from peer QSTA as the QSTA is leaving the QBSS (or resetting)	NOT SUPPORTED
37	Requested from peer QSTA as it does not want to use the mechanism	NOT SUPPORTED

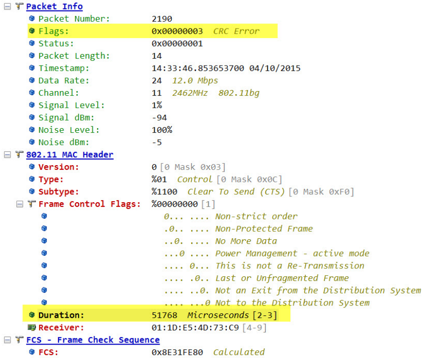
802.11: Frame Control Field



```
Packet Info
    Packet Number:         54
    Flags:                 0x00000000
    Status:                0x00000000
    Packet Length:         34
    Timestamp:             12:26:41.909033400 10/26/2012
    Data Rate:             22  11.0 Mbps
    Channel:               1  2412MHz  802.11b
    Signal Level:          66%
    Signal dBm:            -29
    Noise Level:           100%
    Noise dBm:             -33
802.11 MAC Header
    Version:               0 [0 Mask 0x03]
    Type:                  %00  Management [0 Mask 0x0C]
    Subtype:               %1011  Authentication [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:              117  Microseconds [2-3]
    Destination:           B0:65:BD:CF:F6:29  iPad3 [4-9]
    Source:                6C:50:4D:AA:CB:71 [10-15]
    BSSID:                 6C:50:4D:AA:CB:71 [16-21]
    Seq Number:            2104 [22-23 Mask 0xFFF0]
    Frag Number:           0 [22 Mask 0x0F]
802.11 Management - Authentication
    Auth Algorithm:        0  Open System [24-25]
    Auth Seq Num:          2 [26-27]
    Status Code:           0  Successful [28-29]
FCS - Frame Check Sequence
    FCS:                   0xD5DAC25F  Calculated
```



```
    Packet Number:         2189
    Flags:                 0x00000001
    Status:                0x00000001
    Packet Length:         20
    Timestamp:             14:33:46.853611700 04/10/2015
    Data Rate:             24  12.0 Mbps
    Channel:               11  2462MHz  802.11bg
    Signal Level:          7%
    Signal dBm:            -91
    Noise Level:           100%
    Noise dBm:             -5
802.11 MAC Header
    Version:               0 [0 Mask 0x03]
    Type:                  %01  Control [0 Mask 0x0C]
    Subtype:               %1011  Request To Send (RTS) [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:              1160  Microseconds [2-3]
    Receiver:              50:EA:D6:70:45:C9  Apple:70:45:C9 [4-9]
    Transmitter:           00:1D:E5:4D:73:C9  Cisco:4D:73:C9 [10-15]
FCS - Frame Check Sequence
    FCS:                   0x29137061  Calculated
```

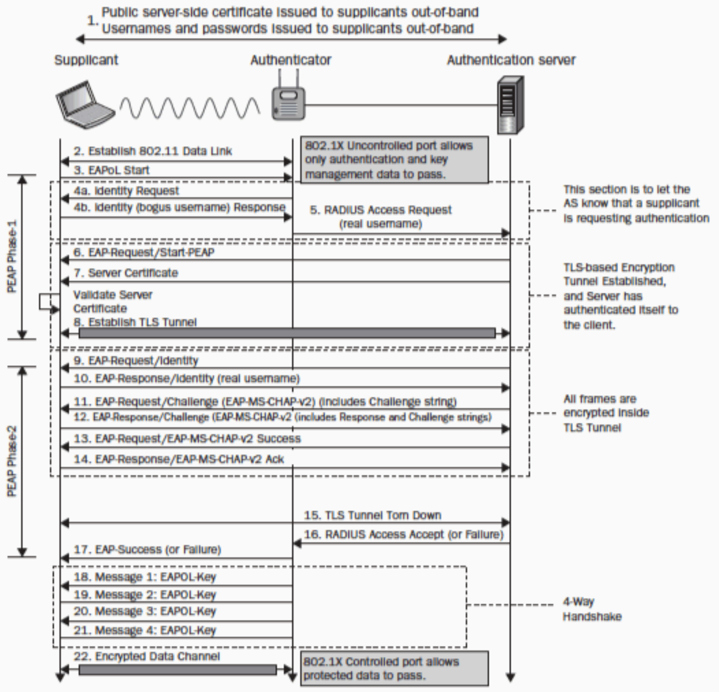


```
Packet Info
    Packet Number:         2190
    Flags:                 0x00000003  CRC Error
    Status:                0x00000001
    Packet Length:         14
    Timestamp:             14:33:46.853653700 04/10/2015
    Data Rate:             24  12.0 Mbps
    Channel:               11  2462MHz  802.11bg
    Signal Level:          1%
    Signal dBm:            -94
    Noise Level:           100%
    Noise dBm:             -5
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:              51768  Microseconds [2-3]
    Receiver:              01:1D:E5:4D:73:C9 [4-9]
FCS - Frame Check Sequence
    FCS:                   0x8E31FE80  Calculated
```

802.11 EAP Flow

ANZ atmosphere2015 HOW TOMORROW MOVES

FIGURE 4.27 EAP-PEAP process



1. Public server-side certificate issued to supplicants out-of-band
Usernames and passwords issued to supplicants out-of-band

Supplicant

Authenticator

Authentication server

2. Establish 802.11 Data Link

3. EAPoL Start

802.1X Uncontrolled port allows only authentication and key management data to pass.

4a. Identity Request

4b. Identity (bogus username) Response

5. RADIUS Access Request (real username)

This section is to let the AS know that a supplicant is requesting authentication

PEAP Phase-1

6. EAP-Request/Start-PEAP

7. Server Certificate

Validate Server Certificate

8. Establish TLS Tunnel

TLS-based Encryption Tunnel Established, and Server has authenticated itself to the client.

PEAP Phase-2

9. EAP-Request/Identity

10. EAP-Response/Identity (real username)

11. EAP-Request/Challenge (EAP-MS-CHAP-v2) (includes Challenge string)

12. EAP-Response/Challenge (EAP-MS-CHAP-v2 (includes Response and Challenge strings)

13. EAP-Request/EAP-MS-CHAP-v2 Success

14. EAP-Response/EAP-MS-CHAP-v2 Ack

All frames are encrypted inside TLS Tunnel

15. TLS Tunnel Torn Down

16. RADIUS Access Accept (or Failure)

17. EAP-Success (or Failure)

18. Message 1: EAPOL-Key

19. Message 2: EAPOL-Key

20. Message 3: EAPOL-Key

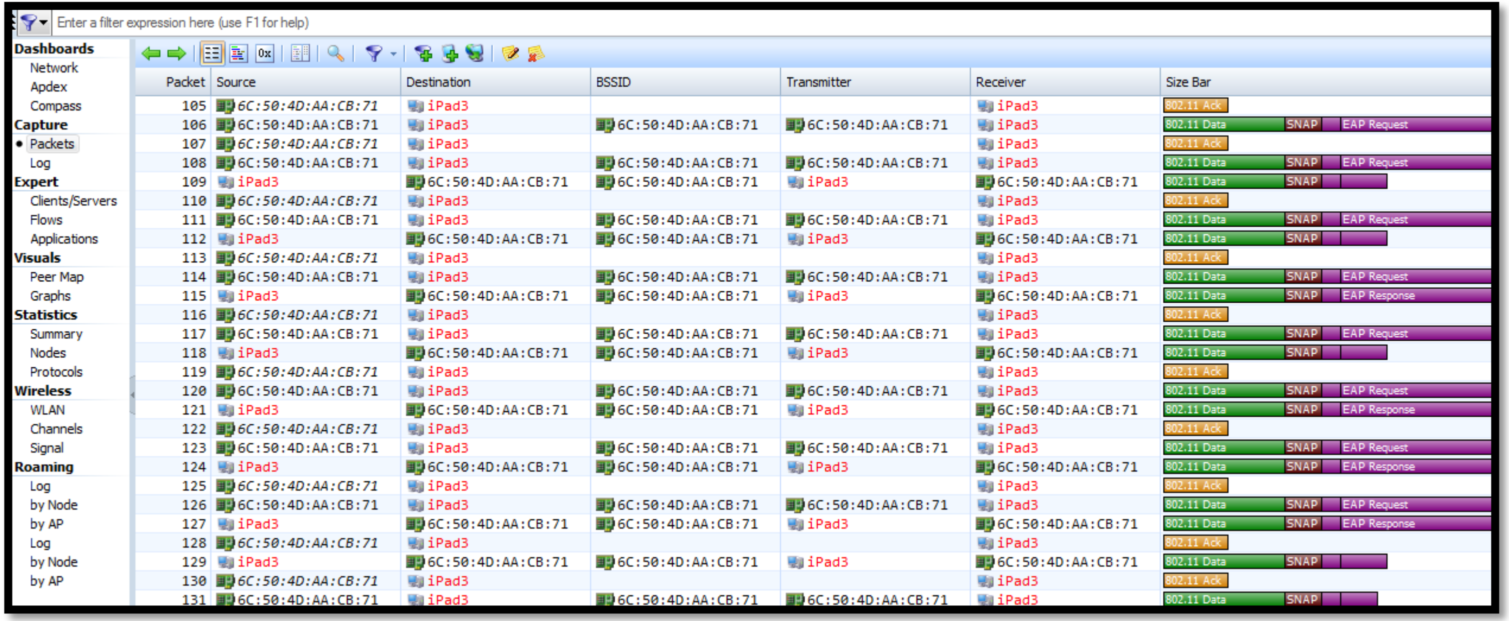
21. Message 4: EAPOL-Key

4-Way Handshake

22. Encrypted Data Channel

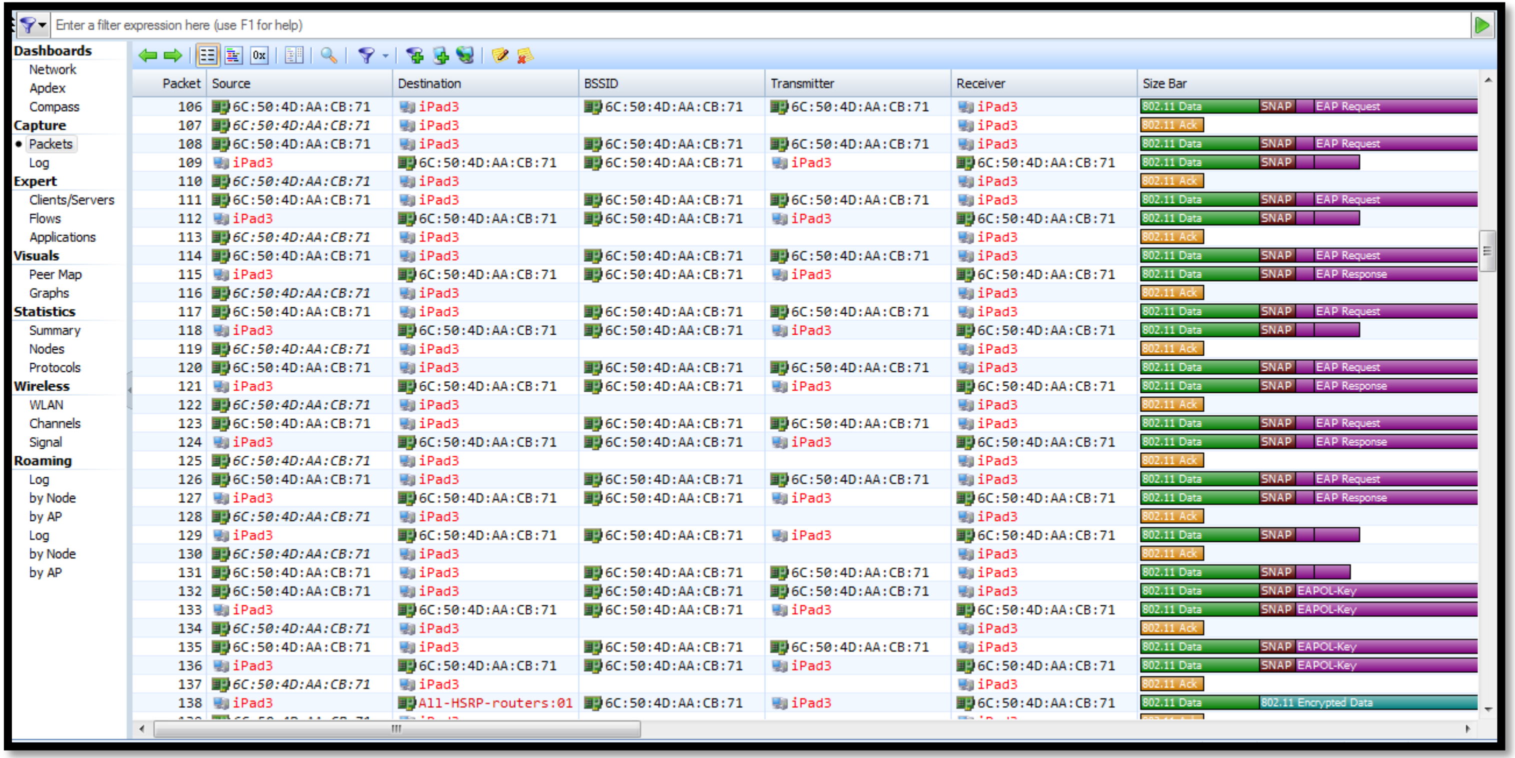
802.1X Controlled port allows protected data to pass.

802.11 EAP Flow



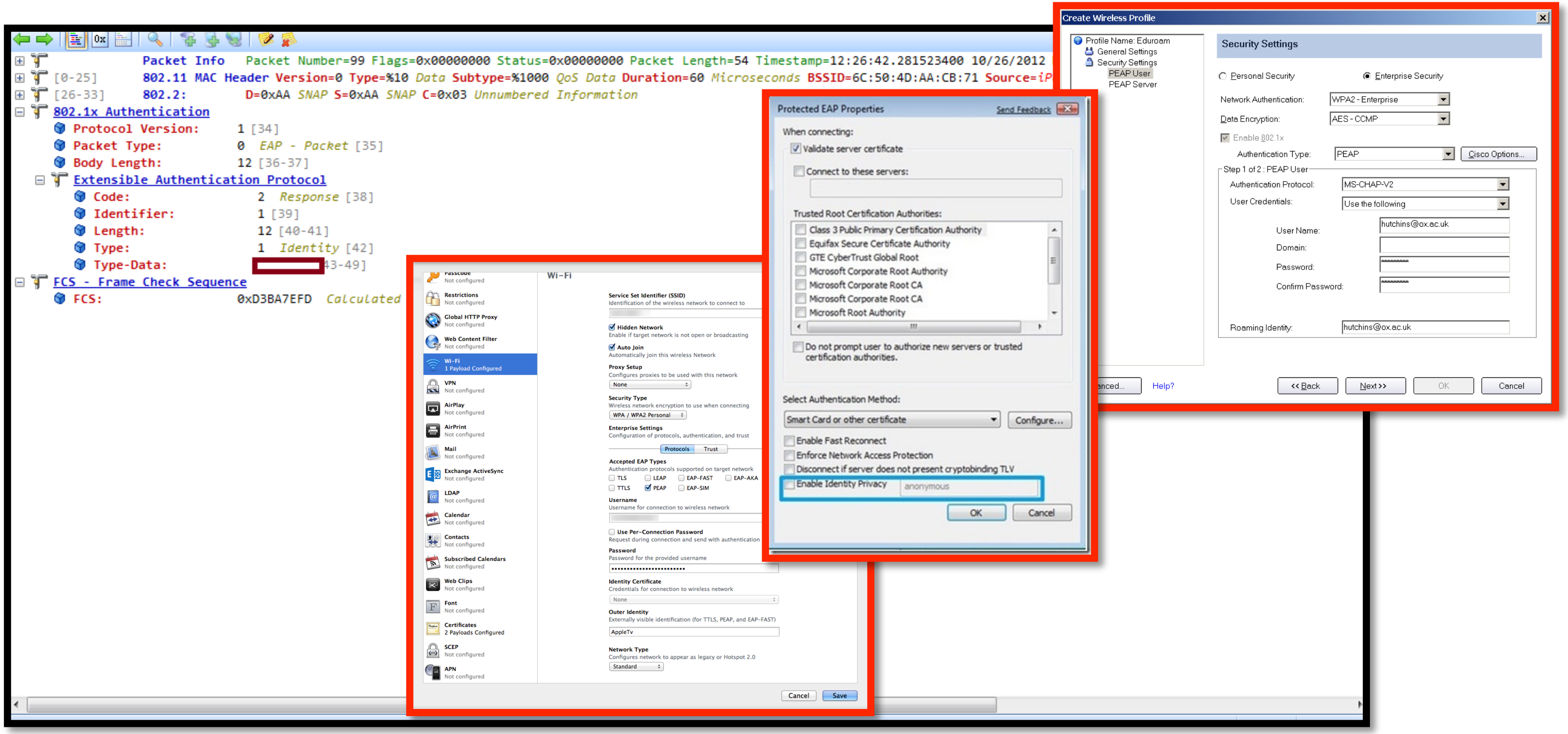
Packet	Source	Destination	BSSID	Transmitter	Receiver	Size Bar
105	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
106	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
107	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
108	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
109	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP
110	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
111	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
112	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP
113	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
114	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
115	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP EAP Response
116	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
117	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
118	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP
119	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
120	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
121	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP EAP Response
122	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
123	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
124	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP EAP Response
125	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
126	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
127	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP EAP Response
128	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
129	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP
130	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
131	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP

802.11 EAP 4 Way Hand Shake



Packet	Source	Destination	BSSID	Transmitter	Receiver	Size Bar
106	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
107	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
108	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
109	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP
110	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
111	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
112	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP
113	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
114	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
115	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP EAP Response
116	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
117	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
118	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP
119	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
120	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
121	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP EAP Response
122	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
123	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
124	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP EAP Response
125	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
126	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAP Request
127	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP EAP Response
128	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
129	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP
130	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
131	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP
132	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAPOL-Key
133	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP EAPOL-Key
134	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
135	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	802.11 Data SNAP EAPOL-Key
136	iPad3	6C:50:4D:AA:CB:71	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data SNAP EAPOL-Key
137	6C:50:4D:AA:CB:71	iPad3			iPad3	802.11 Ack
138	iPad3	All-HSRP-routers:01	6C:50:4D:AA:CB:71	iPad3	6C:50:4D:AA:CB:71	802.11 Data 802.11 Encrypted Data

802.11 EAP: ID



```
Packet Info         Packet Number=99 Flags=0x00000000 Status=0x00000000 Packet Length=54 Timestamp=12:26:42.281523400 10/26/2012
[0-25]  802.11 MAC Header Version=0 Type=%10 Data Subtype=%1000 QoS Data Duration=60 Microseconds BSSID=6C:50:4D:AA:CB:71 Source=iP
[26-33] 802.2:      D=0xAA SNAP S=0xAA SNAP C=0x03 Unnumbered Information
802.1x Authentication
    Protocol Version:      1 [34]
    Packet Type:           0  EAP - Packet [35]
    Body Length:           12 [36-37]
    Extensible Authentication Protocol
        Code:              2  Response [38]
        Identifier:        1 [39]
        Length:            12 [40-41]
        Type:              1  Identity [42]
        Type-Data:         [redacted] 43-49]
FCS - Frame Check Sequence
    FCS:                   0xD3BA7EFD   Calculated
```

Wi-Fi

Passcode – Not configured
Restrictions – Not configured
Global HTTP Proxy – Not configured
Web Content Filter – Not configured
Wi-Fi – 1 Payload Configured
VPN – Not configured
AirPlay – Not configured
AirPrint – Not configured
Mail – Not configured
Exchange ActiveSync – Not configured
LDAP – Not configured
Calendar – Not configured
Contacts – Not configured
Subscribed Calendars – Not configured
Web Clips – Not configured
Font – Not configured
Certificates – 2 Payloads Configured
SCEP – Not configured
APN – Not configured

Service Set Identifier (SSID): Identification of the wireless network to connect to — [redacted]
☑ Hidden Network: Enable if target network is not open or broadcasting
☑ Auto Join: Automatically join this wireless Network
Proxy Setup: Configures proxies to be used with this network — None
Security Type: Wireless network encryption to use when connecting — WPA / WPA2 Personal
Enterprise Settings: Configuration of protocols, authentication, and trust — Protocols | Trust
Accepted EAP Types: Authentication protocols supported on target network — □ TLS □ LEAP □ EAP-FAST □ EAP-AKA □ TTLS ☑ PEAP □ EAP-SIM
Username: Username for connection to wireless network — [redacted]
□ Use Per-Connection Password: Request during connection and send with authentication
Password: Password for the provided username — ••••••••••••••••••••••
Identity Certificate: Credentials for connection to wireless network — None
Outer Identity: Externally visible identification (for TTLS, PEAP, and EAP-FAST) — AppleTv
Network Type: Configures network to appear as legacy or Hotspot 2.0 — Standard

Cancel | Save

Protected EAP Properties — Send Feedback

When connecting:
☑ Validate server certificate
□ Connect to these servers:

Trusted Root Certification Authorities:
□ Class 3 Public Primary Certification Authority
□ Equifax Secure Certificate Authority
□ GTE CyberTrust Global Root
□ Microsoft Corporate Root Authority
□ Microsoft Corporate Root CA
□ Microsoft Corporate Root CA
□ Microsoft Root Authority

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method: Smart Card or other certificate — Configure...
□ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy — anonymous

OK | Cancel

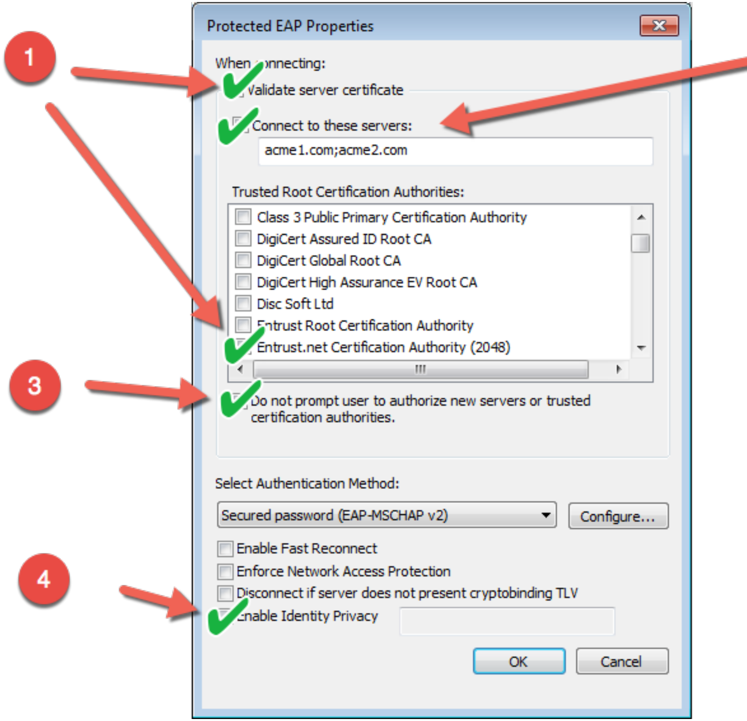
Create Wireless Profile

Profile Name: Eduroam
General Settings
Security Settings
PEAP User
PEAP Server

Security Settings
○ Personal Security ● Enterprise Security
Network Authentication: WPA2 - Enterprise
Data Encryption: AES - CCMP
☑ Enable 802.1x
Authentication Type: PEAP — Cisco Options...
Step 1 of 2 : PEAP User
Authentication Protocol: MS-CHAP-V2
User Credentials: Use the following
User Name: hutchins@ox.ac.uk
Domain:
Password: ********
Confirm Password: ********
Roaming Identity: hutchins@ox.ac.uk

anced... | Help? | << Back | Next >> | OK | Cancel

How secure is your EAP-PEAPv0 deployment ?



Protected EAP Properties

When connecting:

☑ Validate server certificate

☑ Connect to these servers:

acme1.com;acme2.com

Trusted Root Certification Authorities:

- □ Class 3 Public Primary Certification Authority
- □ DigiCert Assured ID Root CA
- □ DigiCert Global Root CA
- □ DigiCert High Assurance EV Root CA
- □ Disc Soft Ltd
- □ Entrust Root Certification Authority
- ☑ Entrust.net Certification Authority (2048)

☑ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2) Configure...

□ Enable Fast Reconnect

□ Enforce Network Access Protection

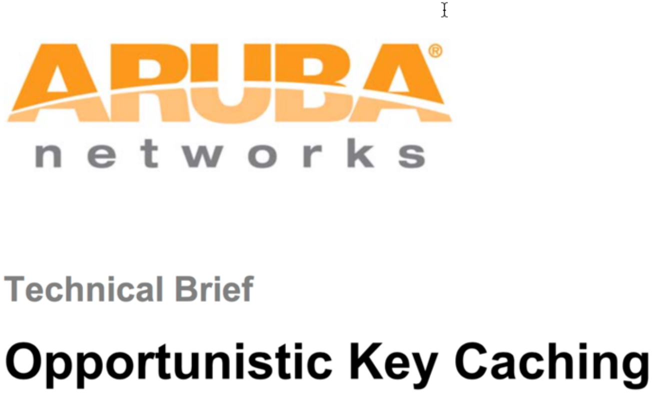
□ Disconnect if server does not present cryptobinding TLV

☑ Enable Identity Privacy

OK Cancel

http://community.arubanetworks.com/t5/Technology-Blog/How-secure-is-your-EAP-PEAPv0-deployment/ba-p/216683

Aruba Technical Brief



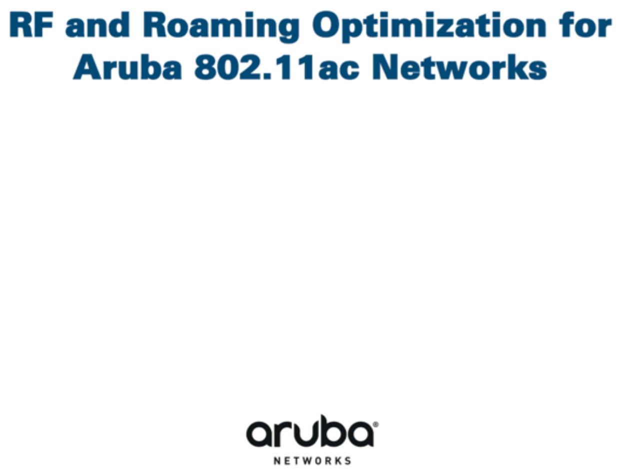
ARUBA networks

Technical Brief

Opportunistic Key Caching

https://community.arubanetworks.com/aruba/attachments/aruba/115/1097/1/Aruba+OKC+Implementation.pdf

Aruba Technical Brief



RF and Roaming Optimization for
Aruba 802.11ac Networks

aruba
NETWORKS

http://community.arubanetworks.com/t5/Validated-Reference-Design/RF-and-Roaming-Optimization-for-Aruba-802-11ac-Networks/ta-p/227716

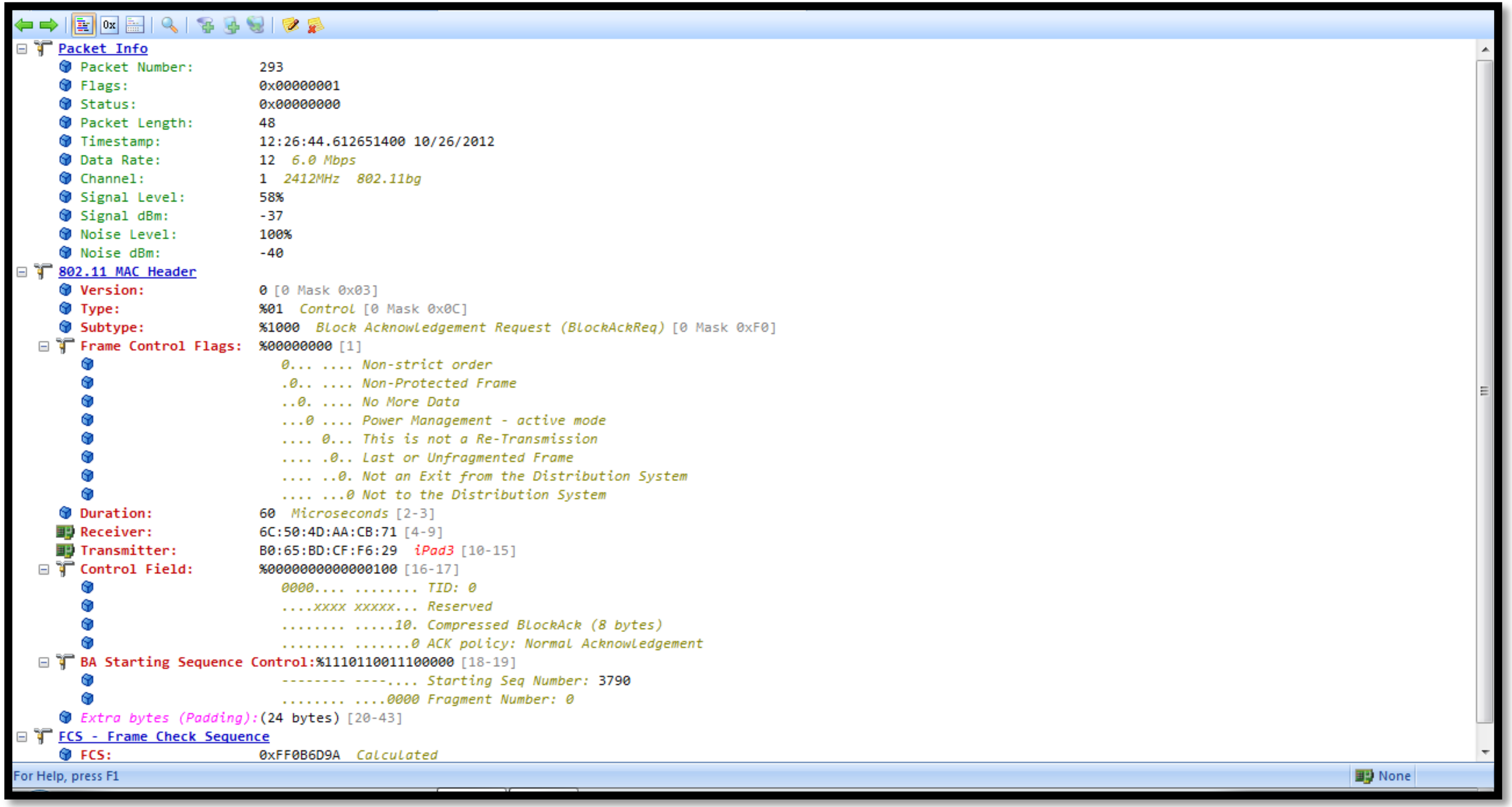
802.11 Control Frames

Control

Power Save Poll (PS-Poll), Request to Send (RTS), Clear to Send (CTS), Acknowledgement (ACK), CF-End +CF +ACK, Block ACK Request (BlockAckReq), and Block ACK (BlockAck).

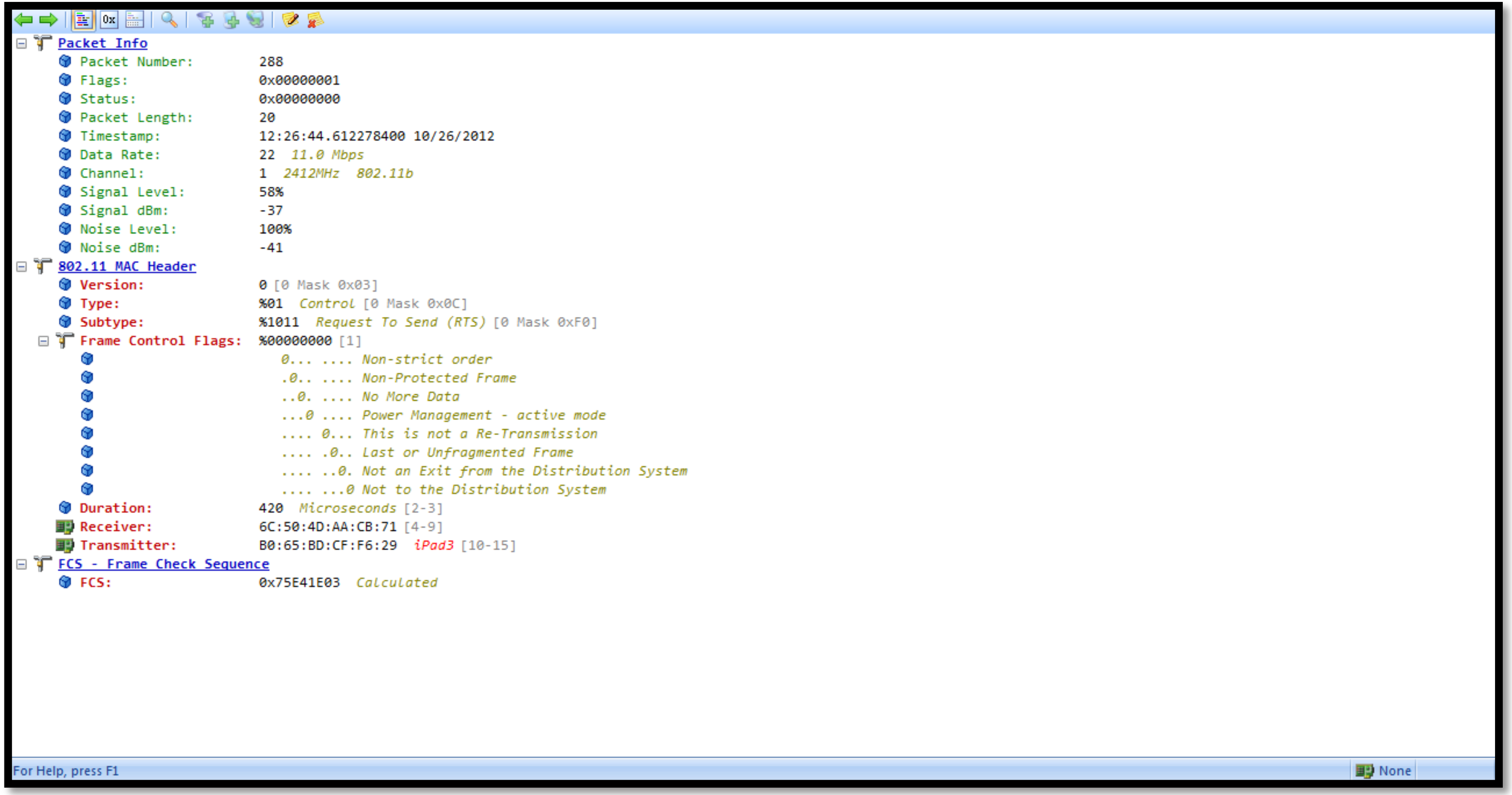
Control frames facilitate Data frame delivery. Control frames are the traffic cops of 802.11 data frames.

802.11 Frame Control Header Retry/To/From/NAV



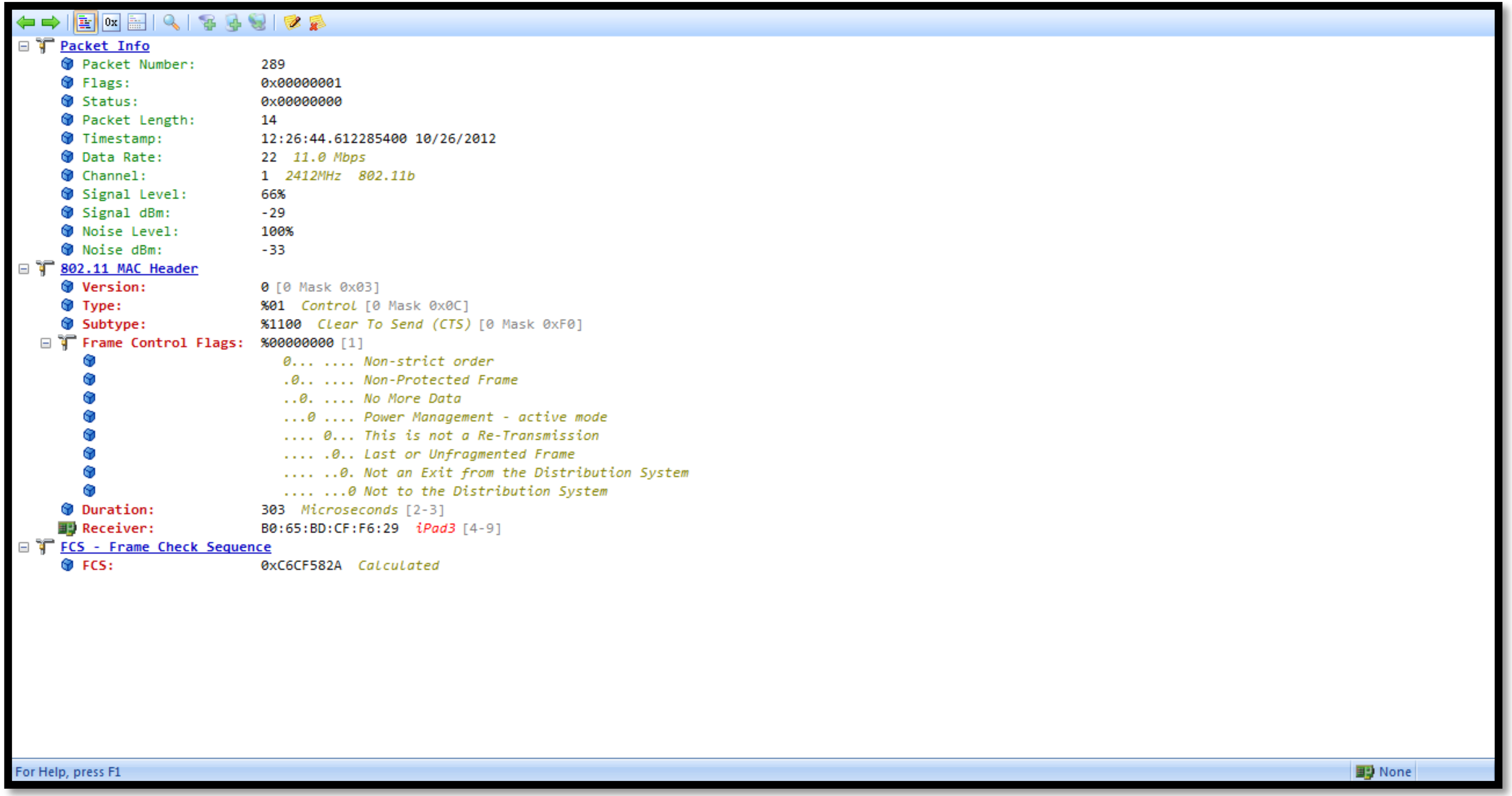
```
⊟ Packet Info
     Packet Number:           293
     Flags:                   0x00000001
     Status:                  0x00000000
     Packet Length:           48
     Timestamp:               12:26:44.612651400 10/26/2012
     Data Rate:               12  6.0 Mbps
     Channel:                 1  2412MHz  802.11bg
     Signal Level:            58%
     Signal dBm:              -37
     Noise Level:             100%
     Noise dBm:               -40
⊟ 802.11 MAC Header
     Version:                 0 [0 Mask 0x03]
     Type:                    %01  Control [0 Mask 0x0C]
     Subtype:                 %1000  Block Acknowledgement Request (BlockAckReq) [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:                60  Microseconds [2-3]
     Receiver:                6C:50:4D:AA:CB:71 [4-9]
     Transmitter:             B0:65:BD:CF:F6:29  iPad3 [10-15]
  ⊟  Control Field:           %0000000000000100 [16-17]
                                 0000.... ........ TID: 0
                                 ....xxxx xxxxx... Reserved
                                 ........ .....10. Compressed BlockAck (8 bytes)
                                 ........ .......0 ACK policy: Normal Acknowledgement
  ⊟  BA Starting Sequence Control:%1110110011100000 [18-19]
                                 -------- ----.... Starting Seq Number: 3790
                                 ........ ....0000 Fragment Number: 0
     Extra bytes (Padding):(24 bytes) [20-43]
⊟ FCS - Frame Check Sequence
     FCS:                     0xFF0B6D9A  Calculated
For Help, press F1                                                            None
```

802.11 RTS



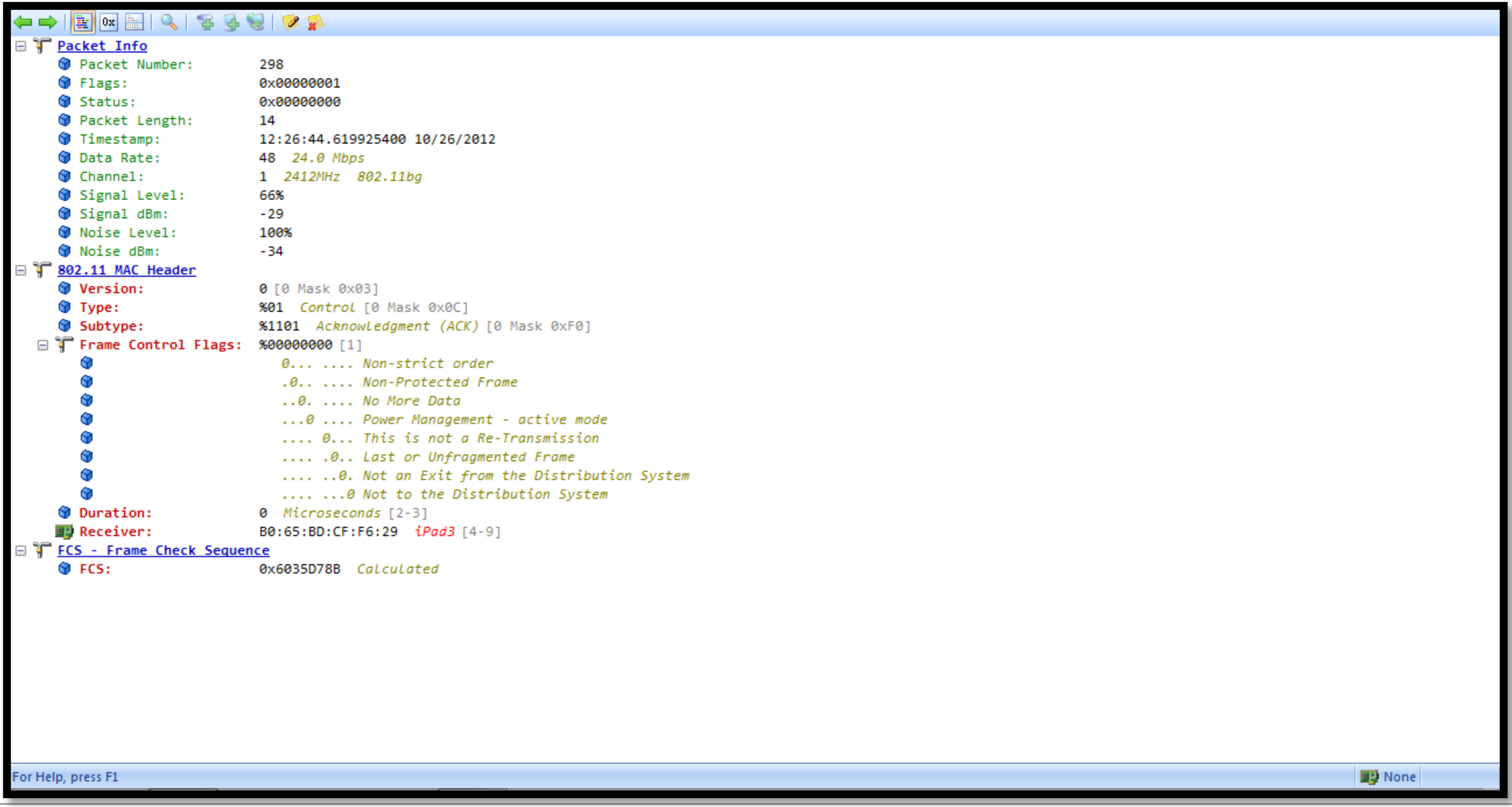
```
⊟ Packet Info
     Packet Number:          288
     Flags:                  0x00000001
     Status:                 0x00000000
     Packet Length:          20
     Timestamp:              12:26:44.612278400 10/26/2012
     Data Rate:              22  11.0 Mbps
     Channel:                1  2412MHz  802.11b
     Signal Level:           58%
     Signal dBm:             -37
     Noise Level:            100%
     Noise dBm:              -41
⊟ 802.11 MAC Header
     Version:                0 [0 Mask 0x03]
     Type:                   %01  Control [0 Mask 0x0C]
     Subtype:                %1011  Request To Send (RTS) [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:               420  Microseconds [2-3]
     Receiver:               6C:50:4D:AA:CB:71 [4-9]
     Transmitter:            B0:65:BD:CF:F6:29  iPad3 [10-15]
⊟ FCS - Frame Check Sequence
     FCS:                    0x75E41E03  Calculated

For Help, press F1                                                    None
```

802.11 CTS



```
⊟ Packet Info
    Packet Number:          289
    Flags:                  0x00000001
    Status:                 0x00000000
    Packet Length:          14
    Timestamp:              12:26:44.612285400 10/26/2012
    Data Rate:              22  11.0 Mbps
    Channel:                1  2412MHz  802.11b
    Signal Level:           66%
    Signal dBm:             -29
    Noise Level:            100%
    Noise dBm:              -33
⊟ 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:               303  Microseconds [2-3]
    Receiver:               B0:65:BD:CF:F6:29  iPad3 [4-9]
⊟ FCS - Frame Check Sequence
    FCS:                    0xC6CF582A  Calculated
```

802.11 ACK

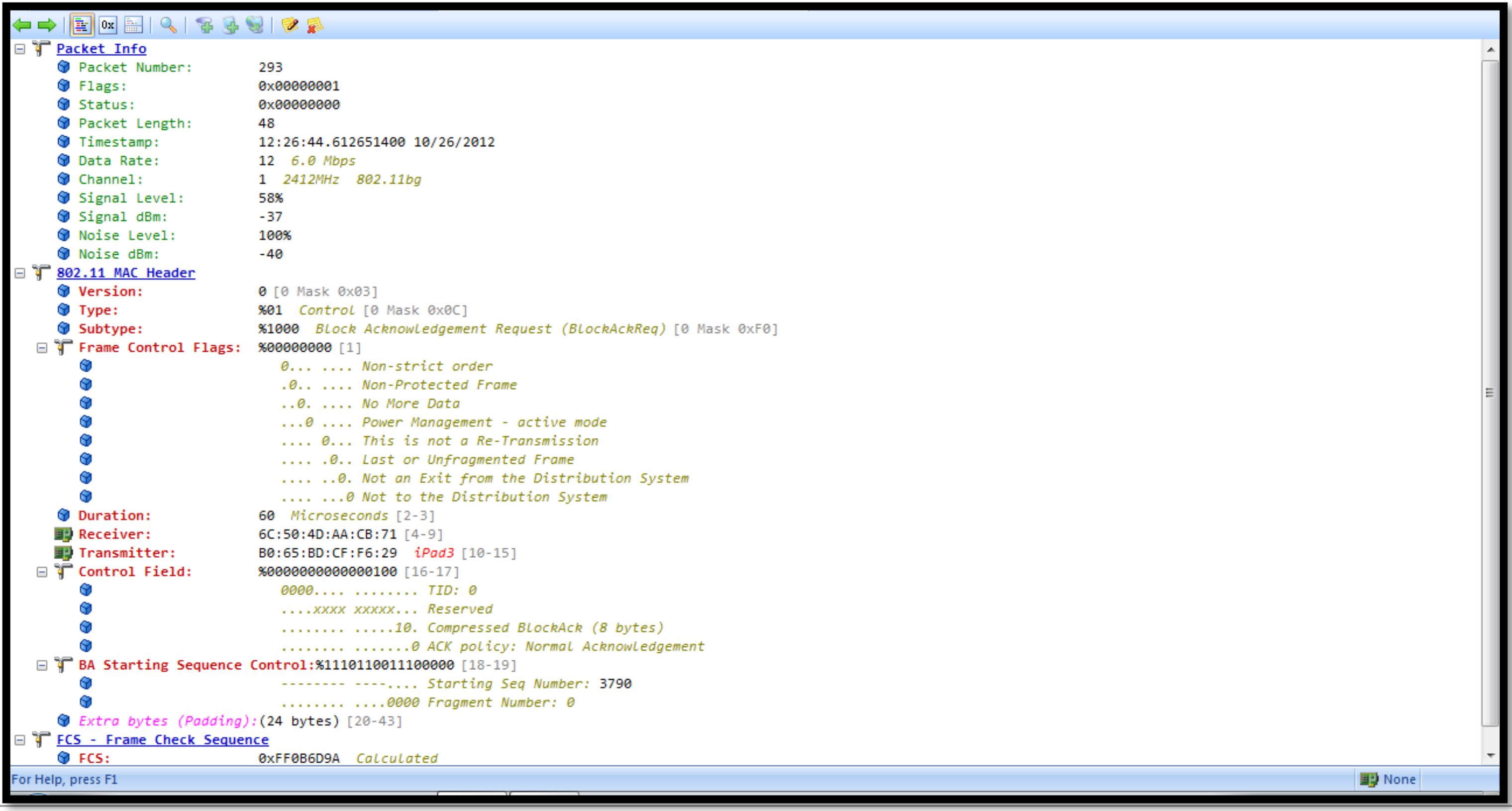


```
⊟ Packet Info
    Packet Number:          298
    Flags:                  0x00000001
    Status:                 0x00000000
    Packet Length:          14
    Timestamp:              12:26:44.619925400 10/26/2012
    Data Rate:              48  24.0 Mbps
    Channel:                1  2412MHz  802.11bg
    Signal Level:           66%
    Signal dBm:             -29
    Noise Level:            100%
    Noise dBm:              -34
⊟ 802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %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 Unfragmented Frame
                              .... ..0. Not an Exit from the Distribution System
                              .... ...0 Not to the Distribution System
    Duration:               0  Microseconds [2-3]
    Receiver:               B0:65:BD:CF:F6:29  iPad3 [4-9]
⊟ FCS - Frame Check Sequence
    FCS:                    0x6035D78B  Calculated
```

For Help, press F1 | None

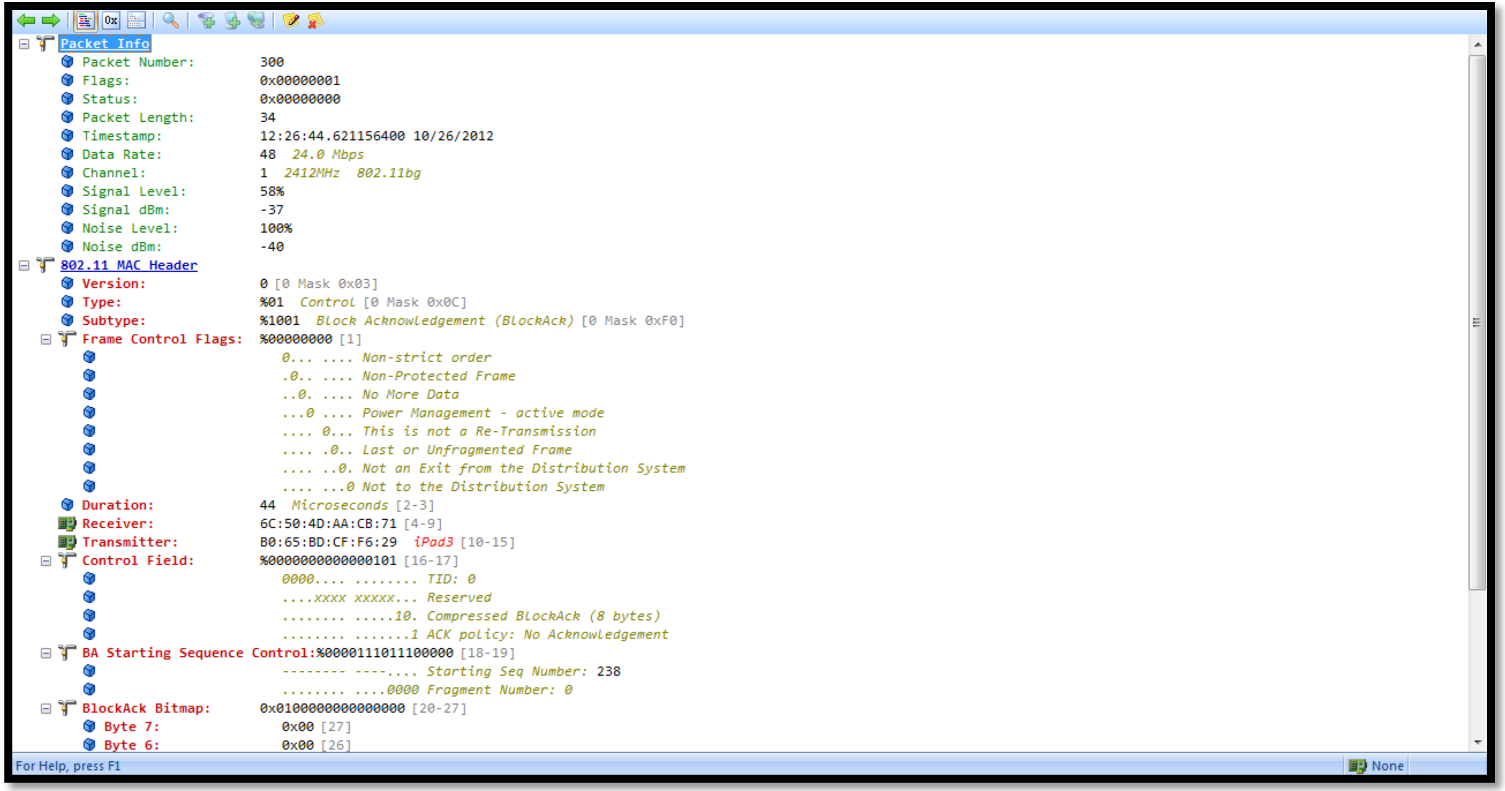
802.11 Block Acknowledgement Request

ANZ atmosphere2015 HOW TOMORROW MOVES



```
⊟ Packet Info
     Packet Number:          293
     Flags:                  0x00000001
     Status:                 0x00000000
     Packet Length:          48
     Timestamp:              12:26:44.612651400 10/26/2012
     Data Rate:              12  6.0 Mbps
     Channel:                1  2412MHz  802.11bg
     Signal Level:           58%
     Signal dBm:             -37
     Noise Level:            100%
     Noise dBm:              -40
⊟ 802.11 MAC Header
     Version:                0 [0 Mask 0x03]
     Type:                   %01  Control [0 Mask 0x0C]
     Subtype:                %1000  Block Acknowledgement Request (BlockAckReq) [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:               60  Microseconds [2-3]
     Receiver:               6C:50:4D:AA:CB:71 [4-9]
     Transmitter:            B0:65:BD:CF:F6:29  iPad3 [10-15]
  ⊟  Control Field:          %0000000000000100 [16-17]
                               0000.... ........ TID: 0
                               ....xxxx xxxxx... Reserved
                               ........ .....10. Compressed BlockAck (8 bytes)
                               ........ .......0 ACK policy: Normal Acknowledgement
  ⊟  BA Starting Sequence Control:%1110110011100000 [18-19]
                               -------- ----.... Starting Seq Number: 3790
                               ........ ....0000 Fragment Number: 0
     Extra bytes (Padding):(24 bytes) [20-43]
⊟ FCS - Frame Check Sequence
     FCS:                    0xFF0B6D9A  Calculated
For Help, press F1                                                         None
```

802.11 Block Acknowledgement



```
⊟ Packet Info
    Packet Number:          300
    Flags:                  0x00000001
    Status:                 0x00000000
    Packet Length:          34
    Timestamp:              12:26:44.621156400 10/26/2012
    Data Rate:              48  24.0 Mbps
    Channel:                1  2412MHz  802.11bg
    Signal Level:           58%
    Signal dBm:             -37
    Noise Level:            100%
    Noise dBm:              -40
⊟ 802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %01  Control [0 Mask 0x0C]
    Subtype:                %1001  Block Acknowledgement (BlockAck) [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:               44  Microseconds [2-3]
    Receiver:               6C:50:4D:AA:CB:71 [4-9]
    Transmitter:            B0:65:BD:CF:F6:29  iPad3 [10-15]
  ⊟ Control Field:          %0000000000000101 [16-17]
                              0000.... ........ TID: 0
                              ....xxxx xxxxx... Reserved
                              ........ .....10. Compressed BlockAck (8 bytes)
                              ........ .......1 ACK policy: No Acknowledgement
  ⊟ BA Starting Sequence Control:%0000111011100000 [18-19]
                              -------- ----.... Starting Seq Number: 238
                              ........ ....0000 Fragment Number: 0
  ⊟ BlockAck Bitmap:        0x0100000000000000 [20-27]
      Byte 7:                 0x00 [27]
      Byte 6:                 0x00 [26]
```

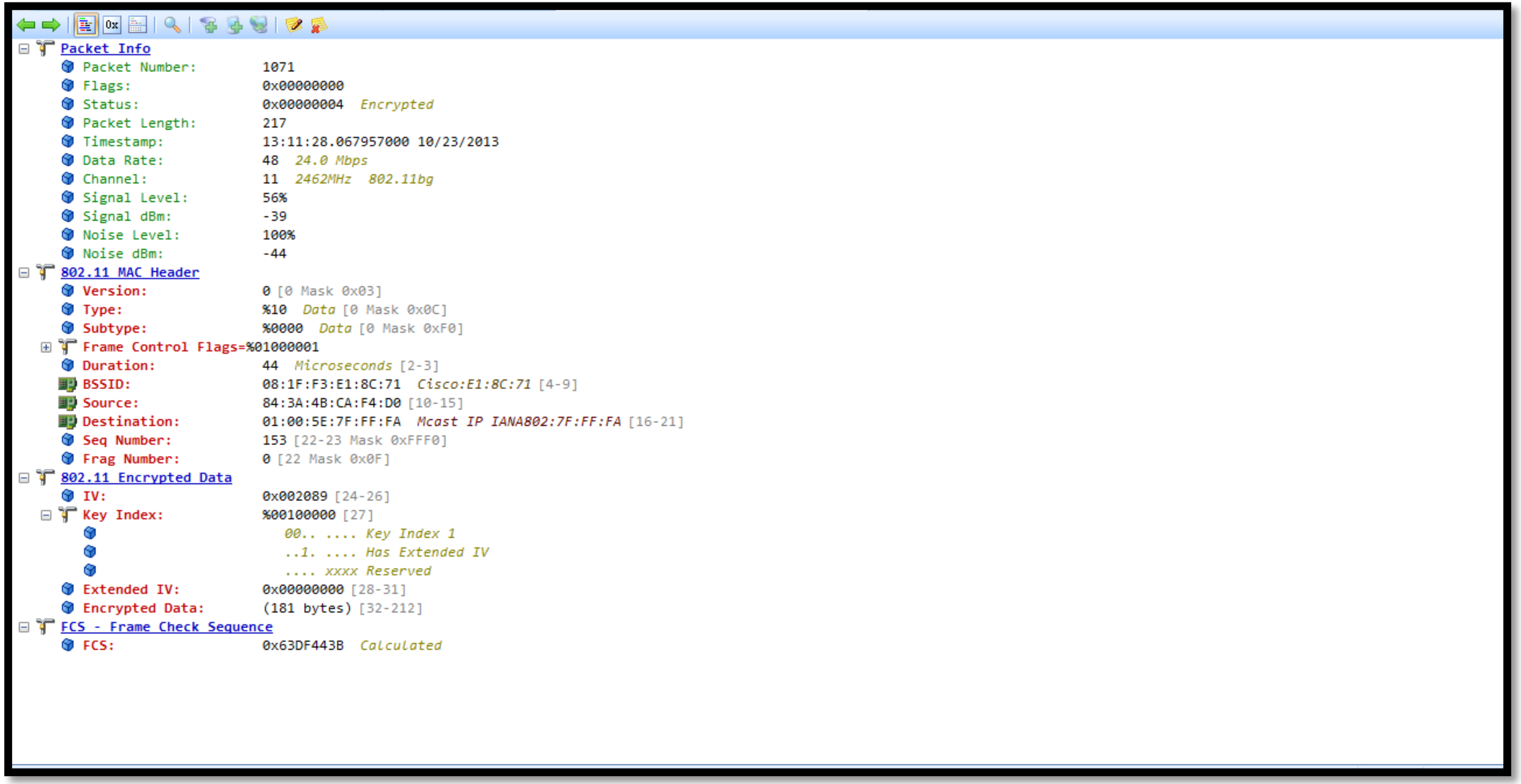
802.11 Data Frames

Data

Data, NULL, Data+CF-Ack, Data+CF-Poll, Data+CF-ACK+CF-Poll, CF-ACK, CF-Poll, CF-ACK, Qos Data, QoD Null, QoS Data+CF-ACK, QoS Data+CF-Poll, QoS Data +CF-ACK+CF-Poll and more ..

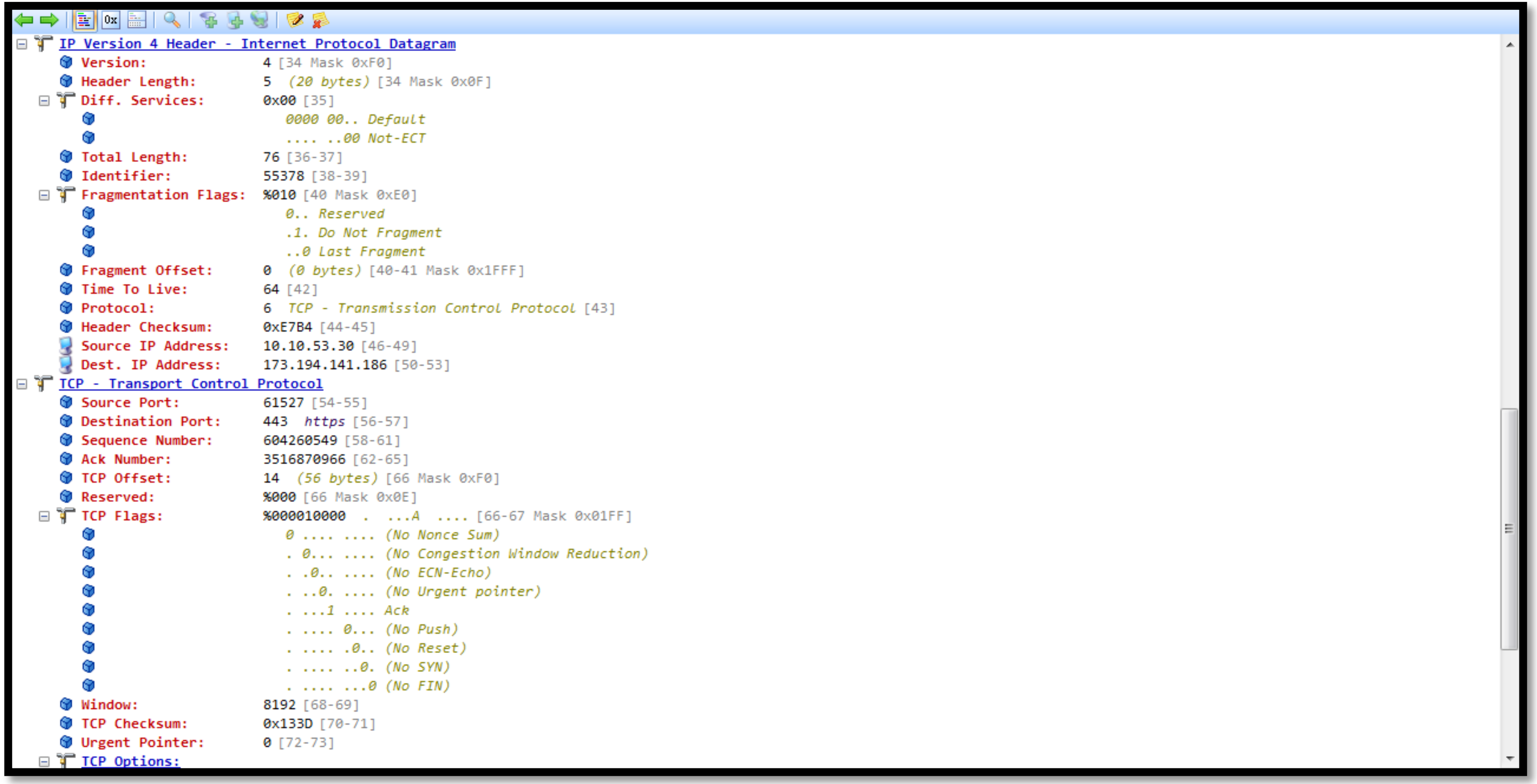
Data frames are simple. They carry data payload from and to the upper layers.

802.11 Data Encrypted



```
⊟ Packet Info
      Packet Number:          1071
      Flags:                  0x00000000
      Status:                 0x00000004  Encrypted
      Packet Length:          217
      Timestamp:              13:11:28.067957000 10/23/2013
      Data Rate:              48  24.0 Mbps
      Channel:                11  2462MHz  802.11bg
      Signal Level:           56%
      Signal dBm:             -39
      Noise Level:            100%
      Noise dBm:              -44
⊟ 802.11 MAC Header
      Version:                0 [0 Mask 0x03]
      Type:                   %10  Data [0 Mask 0x0C]
      Subtype:                %0000  Data [0 Mask 0xF0]
   ⊞ Frame Control Flags=%01000001
      Duration:               44  Microseconds [2-3]
      BSSID:                  08:1F:F3:E1:8C:71  Cisco:E1:8C:71 [4-9]
      Source:                 84:3A:4B:CA:F4:D0 [10-15]
      Destination:            01:00:5E:7F:FF:FA  Mcast IP IANA802:7F:FF:FA [16-21]
      Seq Number:             153 [22-23 Mask 0xFFF0]
      Frag Number:            0 [22 Mask 0x0F]
⊟ 802.11 Encrypted Data
      IV:                     0x002089 [24-26]
   ⊟ Key Index:               %00100000 [27]
                                 00.. .... Key Index 1
                                 ..1. .... Has Extended IV
                                 .... xxxx Reserved
      Extended IV:            0x00000000 [28-31]
      Encrypted Data:         (181 bytes) [32-212]
⊟ FCS - Frame Check Sequence
      FCS:                    0x63DF443B  Calculated
```

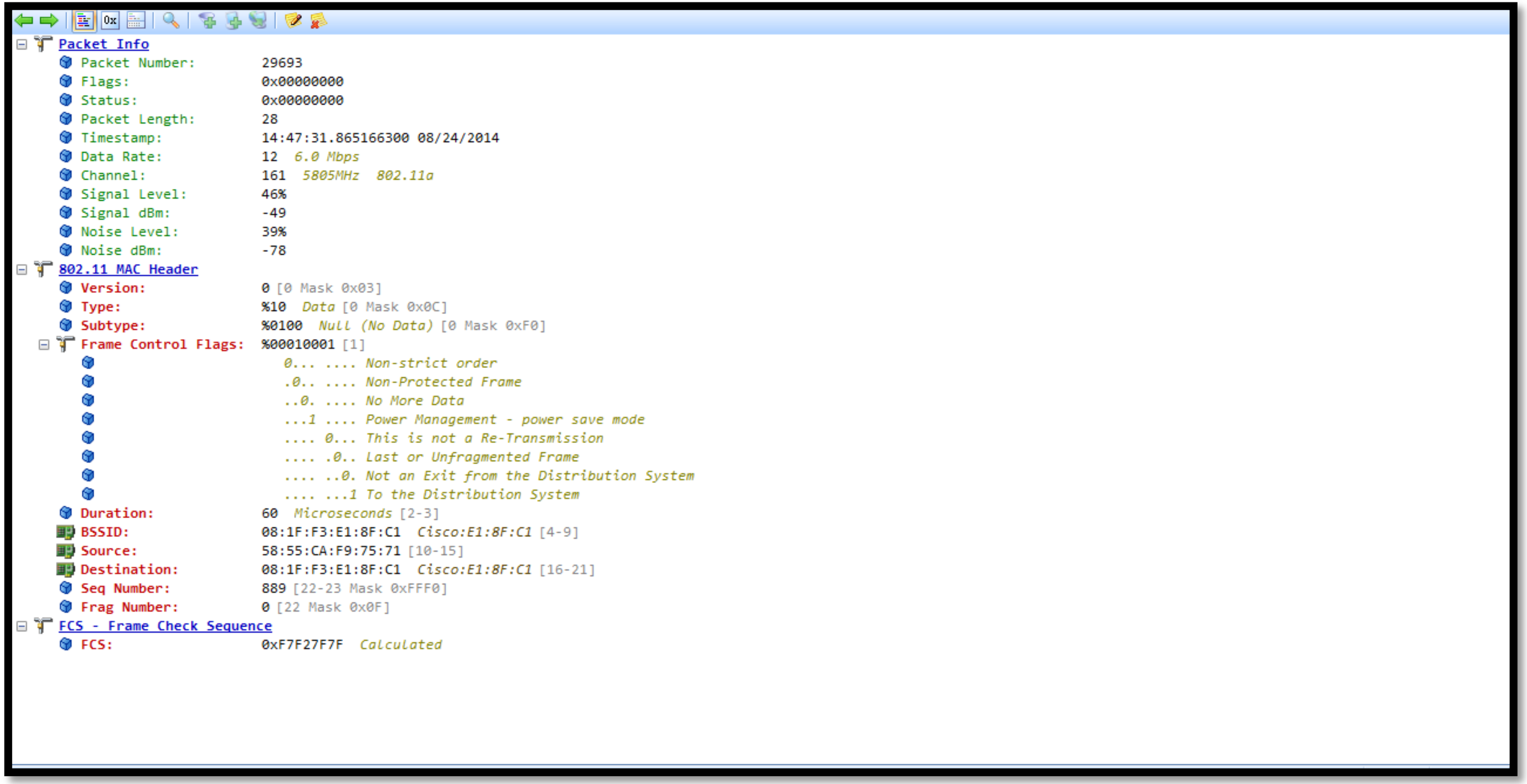
802.11 Data Not Encrypted



```
⊟ IP Version 4 Header - Internet Protocol Datagram
     Version:                  4 [34 Mask 0xF0]
     Header Length:            5  (20 bytes) [34 Mask 0x0F]
   ⊟ Diff. Services:           0x00 [35]
                                 0000 00.. Default
                                 .... ..00 Not-ECT
     Total Length:             76 [36-37]
     Identifier:               55378 [38-39]
   ⊟ Fragmentation Flags:      %010 [40 Mask 0xE0]
                                 0.. Reserved
                                 .1. Do Not Fragment
                                 ..0 Last Fragment
     Fragment Offset:          0  (0 bytes) [40-41 Mask 0x1FFF]
     Time To Live:             64 [42]
     Protocol:                 6  TCP - Transmission Control Protocol [43]
     Header Checksum:          0xE7B4 [44-45]
     Source IP Address:        10.10.53.30 [46-49]
     Dest. IP Address:         173.194.141.186 [50-53]
⊟ TCP - Transport Control Protocol
     Source Port:              61527 [54-55]
     Destination Port:         443  https [56-57]
     Sequence Number:          604260549 [58-61]
     Ack Number:               3516870966 [62-65]
     TCP Offset:               14  (56 bytes) [66 Mask 0xF0]
     Reserved:                 %000 [66 Mask 0x0E]
   ⊟ TCP Flags:                %000010000  .  ...A  .... [66-67 Mask 0x01FF]
                                 0 .... .... (No Nonce Sum)
                                 . 0... .... (No Congestion Window Reduction)
                                 . .0.. .... (No ECN-Echo)
                                 . ..0. .... (No Urgent pointer)
                                 . ...1 .... Ack
                                 . .... 0... (No Push)
                                 . .... .0.. (No Reset)
                                 . .... ..0. (No SYN)
                                 . .... ...0 (No FIN)
     Window:                   8192 [68-69]
     TCP Checksum:             0x133D [70-71]
     Urgent Pointer:           0 [72-73]
   ⊟ TCP Options:
```

802.11 Data NULL Frame

ANZ atmosphere 2015
HOW TOMORROW MOVES



```
⊟ Packet Info
    Packet Number:          29693
    Flags:                  0x00000000
    Status:                 0x00000000
    Packet Length:          28
    Timestamp:              14:47:31.865166300 08/24/2014
    Data Rate:              12  6.0 Mbps
    Channel:                161  5805MHz  802.11a
    Signal Level:           46%
    Signal dBm:             -49
    Noise Level:            39%
    Noise dBm:              -78
⊟ 802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %10  Data [0 Mask 0x0C]
    Subtype:                %0100  Null (No Data) [0 Mask 0xF0]
  ⊟ Frame Control Flags:    %00010001 [1]
                               0... .... Non-strict order
                               .0.. .... Non-Protected Frame
                               ..0. .... No More Data
                               ...1 .... Power Management - power save mode
                               .... 0... This is not a Re-Transmission
                               .... .0.. Last or Unfragmented Frame
                               .... ..0. Not an Exit from the Distribution System
                               .... ...1 To the Distribution System
    Duration:               60  Microseconds [2-3]
    BSSID:                  08:1F:F3:E1:8F:C1  Cisco:E1:8F:C1 [4-9]
    Source:                 58:55:CA:F9:75:71 [10-15]
    Destination:            08:1F:F3:E1:8F:C1  Cisco:E1:8F:C1 [16-21]
    Seq Number:             889 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
⊟ FCS - Frame Check Sequence
    FCS:                    0xF7F27F7F  Calculated
```

WMM QoS

Differentiate sensitive application traffic

- Contention Windows cW

Wireless QoS Myths

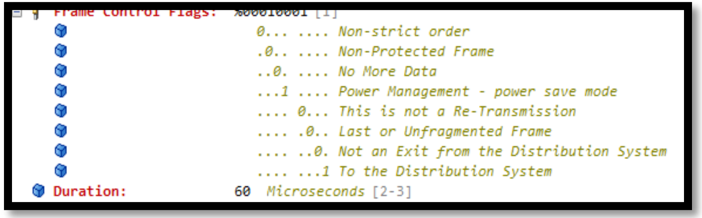
- I have big pipes I don’t need QoS
- Voice and video are fine on the wired; Don’t need wireless QoS

WMM QoS

CSMA-CA

- Layer 1
  - CCA
  - ED Energy Detect

- Layer 2
  - Duration Timer (NAV)

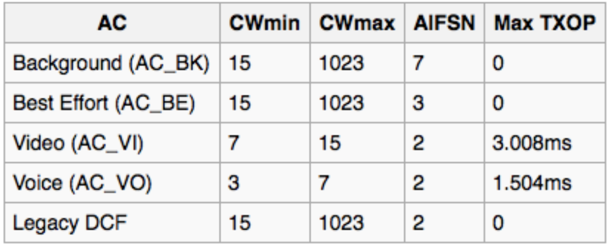


```
Frame Control Flags:   %00010001 [1]
                          0... .... Non-strict order
                          .0.. .... Non-Protected Frame
                          ..0. .... No More Data
                          ...1 .... Power Management - power save mode
                          .... 0... This is not a Re-Transmission
                          .... .0.. Last or Unfragmented Frame
                          .... ..0. Not an Exit from the Distribution System
                          .... ...1 To the Distribution System
Duration:              60  Microseconds [2-3]
```

NO Differentiation of Services (Applications)

WMM QoS

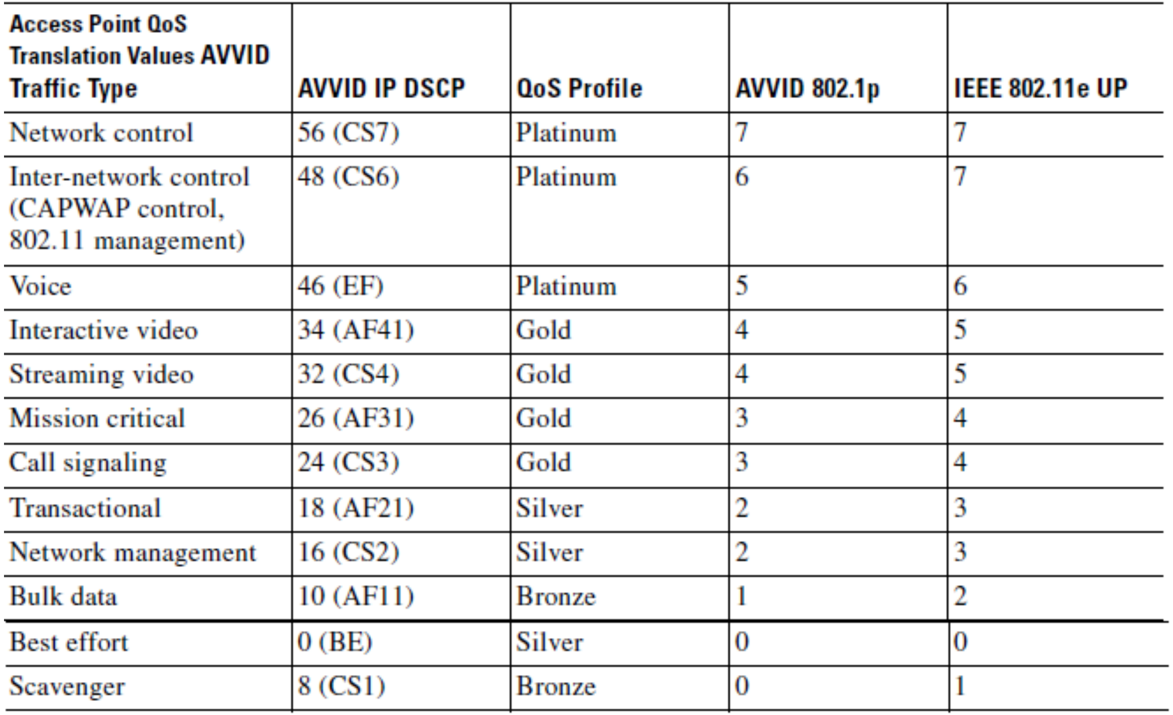
Default EDCA Parameters for each AC



AC	CWmin	CWmax	AIFSN	Max TXOP
Background (AC_BK)	15	1023	7	0
Best Effort (AC_BE)	15	1023	3	0
Video (AC_VI)	7	15	2	3.008ms
Voice (AC_VO)	3	7	2	1.504ms
Legacy DCF	15	1023	2	0

WMM QoS

- WiFi QoS Queues
- (1,2)(,0,3)(,4,5)(,6)

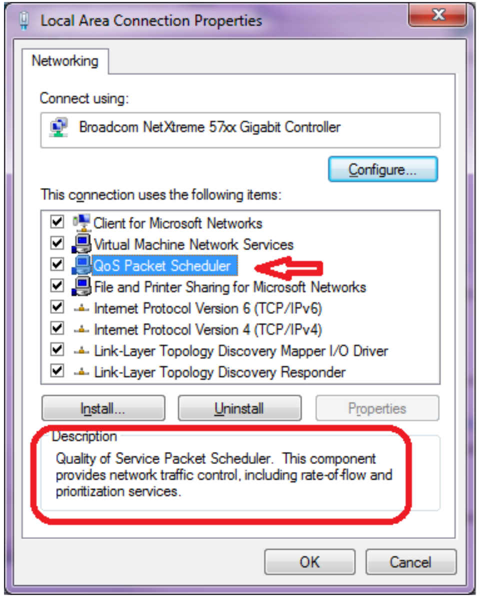


Access Point QoS Translation Values AVVID Traffic Type	AVVID IP DSCP	QoS Profile	AVVID 802.1p	IEEE 802.11e UP
Network control	56 (CS7)	Platinum	7	7
Inter-network control (CAPWAP control, 802.11 management)	48 (CS6)	Platinum	6	7
Voice	46 (EF)	Platinum	5	6
Interactive video	34 (AF41)	Gold	4	5
Streaming video	32 (CS4)	Gold	4	5
Mission critical	26 (AF31)	Gold	3	4
Call signaling	24 (CS3)	Gold	3	4
Transactional	18 (AF21)	Silver	2	3
Network management	16 (CS2)	Silver	2	3
Bulk data	10 (AF11)	Bronze	1	2
Best effort	0 (BE)	Silver	0	0
Scavenger	8 (CS1)	Bronze	0	1

WMM QoS

QOS

- Applications must mark
- NIC honors markings



Local Area Connection Properties

Networking

Connect using:

Broadcom NetXtreme 57xx Gigabit Controller

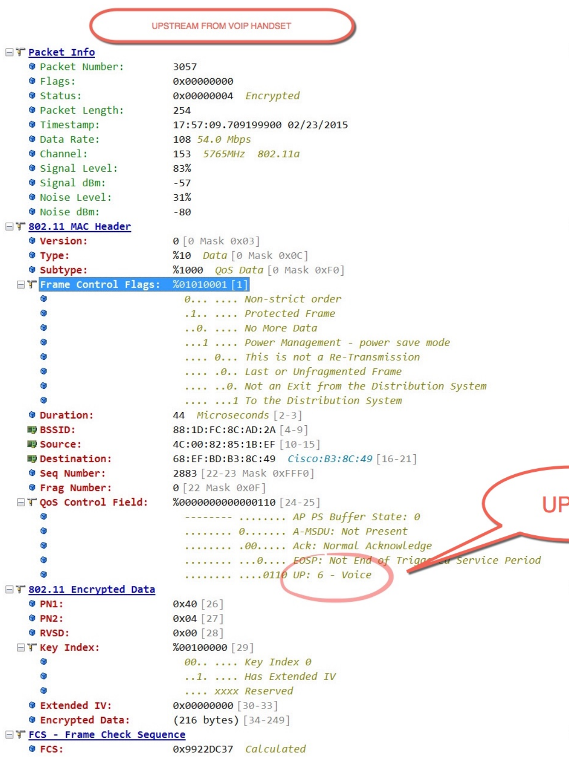
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Virtual Machine Network Services
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

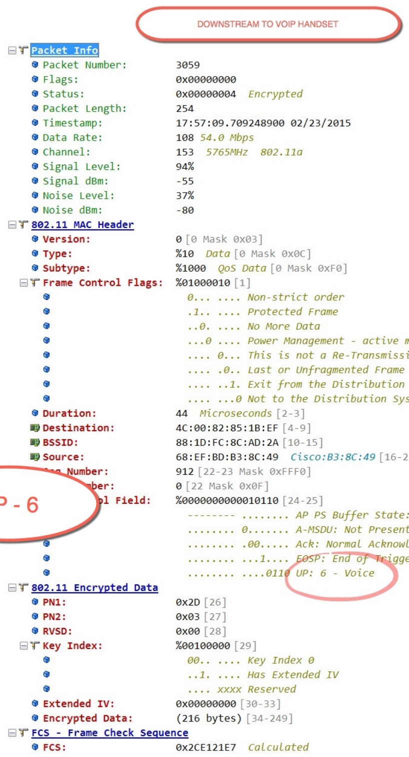
Quality of Service Packet Scheduler. This component provides network traffic control, including rate-of-flow and prioritization services.

WMM QoS



UPSTREAM FROM VOIP HANDSET

```
⊟ Packet Info
    Packet Number:          3057
    Flags:                  0x00000000
    Status:                 0x00000004  Encrypted
    Packet Length:          254
    Timestamp:              17:57:09.709199900 02/23/2015
    Data Rate:              108 54.0 Mbps
    Channel:                153  5765MHz  802.11a
    Signal Level:           83%
    Signal dBm:             -57
    Noise Level:            31%
    Noise dBm:              -80
⊟ 802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %10  Data [0 Mask 0x0C]
    Subtype:                %1000  QoS Data [0 Mask 0xF0]
  ⊟ Frame Control Flags:    %01010001 [1]
                              0... .... Non-strict order
                              .1.. .... Protected Frame
                              ..0. .... No More Data
                              ...1 .... Power Management - power save mode
                              .... 0... This is not a Re-Transmission
                              .... .0.. Last or Unfragmented Frame
                              .... ..0. Not an Exit from the Distribution System
                              .... ...1 To the Distribution System
    Duration:               44  Microseconds [2-3]
    BSSID:                  88:1D:FC:8C:AD:2A [4-9]
    Source:                 4C:00:82:85:1B:EF [10-15]
    Destination:            68:EF:BD:B3:8C:49  Cisco:B3:8C:49 [16-21]
    Seq Number:             2883 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
  ⊟ QoS Control Field:      %0000000000000110 [24-25]
                              -------- ........ AP PS Buffer State: 0
                              ........ 0....... A-MSDU: Not Present
                              ........ .00..... Ack: Normal Acknowledge
                              ........ ...0.... EOSP: Not End of Triggered Service Period
                              ........ ....0110 UP: 6 - Voice
⊟ 802.11 Encrypted Data
    PN1:                    0x40 [26]
    PN2:                    0x04 [27]
    RVSD:                   0x00 [28]
  ⊟ Key Index:              %00100000 [29]
                              00.. .... Key Index 0
                              ..1. .... Has Extended IV
                              .... xxxx Reserved
    Extended IV:            0x00000000 [30-33]
    Encrypted Data:         (216 bytes) [34-249]
⊟ FCS - Frame Check Sequence
    FCS:                    0x9922DC37  Calculated
```



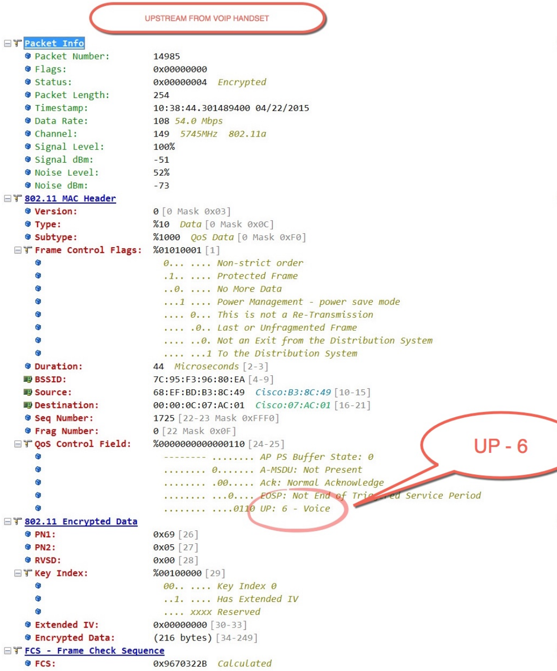
DOWNSTREAM TO VOIP HANDSET

```
⊟ Packet Info
    Packet Number:          3059
    Flags:                  0x00000000
    Status:                 0x00000004  Encrypted
    Packet Length:          254
    Timestamp:              17:57:09.709248900 02/23/2015
    Data Rate:              108 54.0 Mbps
    Channel:                153  5765MHz  802.11a
    Signal Level:           94%
    Signal dBm:             -55
    Noise Level:            37%
    Noise dBm:              -80
⊟ 802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %10  Data [0 Mask 0x0C]
    Subtype:                %1000  QoS Data [0 Mask 0xF0]
  ⊟ Frame Control Flags:    %01000010 [1]
                              0... .... Non-strict order
                              .1.. .... Protected Frame
                              ..0. .... No More Data
                              ...0 .... Power Management - active mode
                              .... 0... This is not a Re-Transmission
                              .... .0.. Last or Unfragmented Frame
                              .... ..1. Exit from the Distribution System
                              .... ...0 Not to the Distribution System
    Duration:               44  Microseconds [2-3]
    Destination:            4C:00:82:85:1B:EF [4-9]
    BSSID:                  88:1D:FC:8C:AD:2A [10-15]
    Source:                 68:EF:BD:B3:8C:49  Cisco:B3:8C:49 [16-21]
      q Number:             912 [22-23 Mask 0xFFF0]
         ber:               0 [22 Mask 0x0F]
         l Field:           %0000000000010110 [24-25]
                              -------- ........ AP PS Buffer State: 0
                              ........ 0....... A-MSDU: Not Present
                              ........ .00..... Ack: Normal Acknowledge
                              ........ ...1.... EOSP: End of Triggered Service Period
                              ........ ....0110 UP: 6 - Voice
⊟ 802.11 Encrypted Data
    PN1:                    0x2D [26]
    PN2:                    0x03 [27]
    RVSD:                   0x00 [28]
  ⊟ Key Index:              %00100000 [29]
                              00.. .... Key Index 0
                              ..1. .... Has Extended IV
                              .... xxxx Reserved
    Extended IV:            0x00000000 [30-33]
    Encrypted Data:         (216 bytes) [34-249]
⊟ FCS - Frame Check Sequence
    FCS:                    0x2CE121E7  Calculated
```

Default EDCA Parameters for each AC

AC	CWmin	CWmax	AIFSN	Max TXOP
Background (AC_BK)	15	1023	7	0
Best Effort (AC_BE)	15	1023	3	0
Video (AC_VI)	7	15	2	3.008ms
Voice (AC_VO)	3	7	2	1.504ms
Legacy DCF	15	1023	2	0

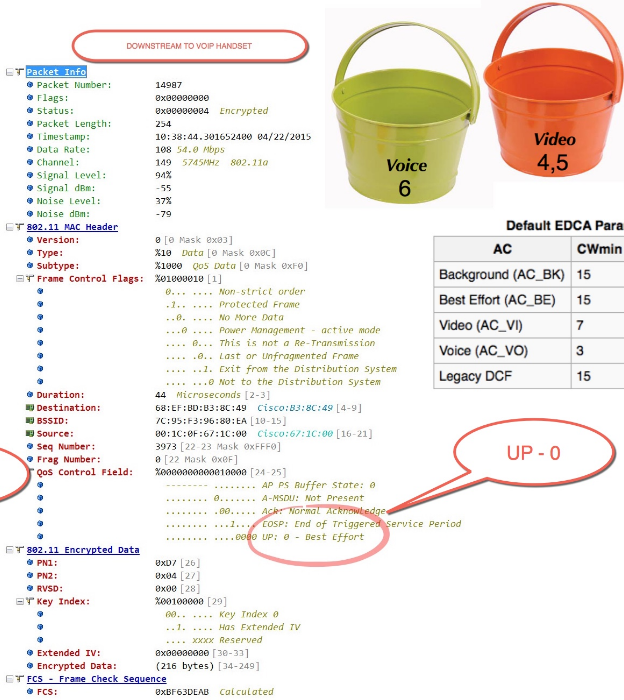
WMM QoS



UPSTREAM FROM VOIP HANDSET

```
⊟ Packet Info
    Packet Number:          14985
    Flags:                  0x00000000
    Status:                 0x00000004  Encrypted
    Packet Length:          254
    Timestamp:              10:38:44.301489400 04/22/2015
    Data Rate:              108 54.0 Mbps
    Channel:                149  5745MHz  802.11a
    Signal Level:           100%
    Signal dBm:             -51
    Noise Level:            52%
    Noise dBm:              -73
⊟ 802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %10  Data [0 Mask 0x0C]
    Subtype:                %1000  QoS Data [0 Mask 0xF0]
  ⊟ Frame Control Flags:    %01010001 [1]
                              0... .... Non-strict order
                              .1.. .... Protected Frame
                              ..0. .... No More Data
                              ...1 .... Power Management - power save mode
                              .... 0... This is not a Re-Transmission
                              .... .0.. Last or Unfragmented Frame
                              .... ..0. Not an Exit from the Distribution System
                              .... ...1 To the Distribution System
    Duration:               44  Microseconds [2-3]
    BSSID:                  7C:95:F3:96:80:EA [4-9]
    Source:                 68:EF:BD:B3:8C:49  Cisco:B3:8C:49 [10-15]
    Destination:            00:00:0C:07:AC:01  Cisco:07:AC:01 [16-21]
    Seq Number:             1725 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
  ⊟ QoS Control Field:      %0000000000000110 [24-25]
                              -------- ........ AP PS Buffer State: 0
                              ........ 0....... A-MSDU: Not Present
                              ........ .00..... Ack: Normal Acknowledge
                              ........ ...0.... EOSP: Not End of Triggered Service Period
                              ........ ....0110 UP: 6 - Voice
⊟ 802.11 Encrypted Data
    PN1:                    0x69 [26]
    PN2:                    0x05 [27]
    RVSD:                   0x00 [28]
  ⊟ Key Index:              %00100000 [29]
                              00.. .... Key Index 0
                              ..1. .... Has Extended IV
                              .... xxxx Reserved
    Extended IV:            0x00000000 [30-33]
    Encrypted Data:         (216 bytes) [34-249]
⊟ FCS - Frame Check Sequence
    FCS:                    0x9670322B  Calculated
```

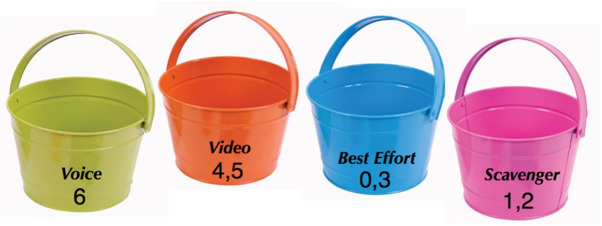
UP - 6



DOWNSTREAM TO VOIP HANDSET

```
⊟ Packet Info
    Packet Number:          14987
    Flags:                  0x00000000
    Status:                 0x00000004  Encrypted
    Packet Length:          254
    Timestamp:              10:38:44.301652400 04/22/2015
    Data Rate:              108 54.0 Mbps
    Channel:                149  5745MHz  802.11a
    Signal Level:           94%
    Signal dBm:             -55
    Noise Level:            37%
    Noise dBm:              -79
⊟ 802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %10  Data [0 Mask 0x0C]
    Subtype:                %1000  QoS Data [0 Mask 0xF0]
  ⊟ Frame Control Flags:    %01000010 [1]
                              0... .... Non-strict order
                              .1.. .... Protected Frame
                              ..0. .... No More Data
                              ...0 .... Power Management - active mode
                              .... 0... This is not a Re-Transmission
                              .... .0.. Last or Unfragmented Frame
                              .... ..1. Exit from the Distribution System
                              .... ...0 Not to the Distribution System
    Duration:               44  Microseconds [2-3]
    Destination:            68:EF:BD:B3:8C:49  Cisco:B3:8C:49 [4-9]
    BSSID:                  7C:95:F3:96:80:EA [10-15]
    Source:                 00:1C:0F:67:1C:00  Cisco:67:1C:00 [16-21]
    Seq Number:             3973 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
  ⊟ QoS Control Field:      %0000000000010000 [24-25]
                              -------- ........ AP PS Buffer State: 0
                              ........ 0....... A-MSDU: Not Present
                              ........ .00..... Ack: Normal Acknowledge
                              ........ ...1.... EOSP: End of Triggered Service Period
                              ........ ....0000 UP: 0 - Best Effort
⊟ 802.11 Encrypted Data
    PN1:                    0xD7 [26]
    PN2:                    0x04 [27]
    RVSD:                   0x00 [28]
  ⊟ Key Index:              %00100000 [29]
                              00.. .... Key Index 0
                              ..1. .... Has Extended IV
                              .... xxxx Reserved
    Extended IV:            0x00000000 [30-33]
    Encrypted Data:         (216 bytes) [34-249]
⊟ FCS - Frame Check Sequence
    FCS:                    0xBF63DEAB  Calculated
```

UP - 0



Default EDCA Parameters for each AC

AC	CWmin	CWmax	AIFSN	Max TXOP
Background (AC_BK)	15	1023	7	0
Best Effort (AC_BE)	15	1023	3	0
Video (AC_VI)	7	15	2	3.008ms
Voice (AC_VO)	3	7	2	1.504ms
Legacy DCF	15	1023	2	0

WMM QoS

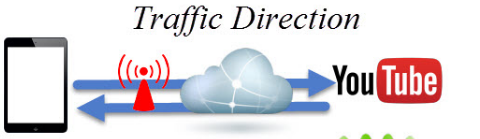
QoS marking is critical to getting frames in the right bucket for over the air priority!

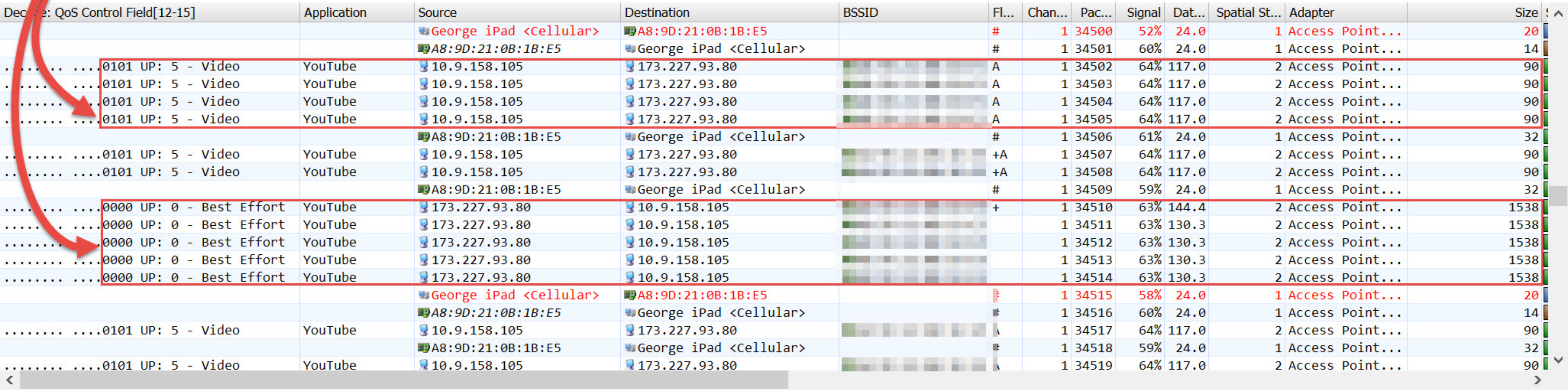
WMM QoS

Device: Apple iPad Air 2	
iOS 9.1	YOUTUBE APP

Frames arriving at the iPad marked with a UP <0>

Frames leaving the iPad marked with a UP <5>





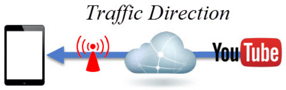
Decode: QoS Control Field[12-15]	Application	Source	Destination	BSSID	Fl...	Chan...	Pac...	Signal	Dat...	Spatial St...	Adapter	Size
		George iPad <Cellular>	A8:9D:21:0B:1B:E5		#	1	34500	52%	24.0	1	Access Point...	20
		A8:9D:21:0B:1B:E5	George iPad <Cellular>		#	1	34501	60%	24.0	1	Access Point...	14
....0101 UP: 5 - Video	YouTube	10.9.158.105	173.227.93.80	[redacted]	A	1	34502	64%	117.0	2	Access Point...	90
....0101 UP: 5 - Video	YouTube	10.9.158.105	173.227.93.80	[redacted]	A	1	34503	64%	117.0	2	Access Point...	90
....0101 UP: 5 - Video	YouTube	10.9.158.105	173.227.93.80	[redacted]	A	1	34504	64%	117.0	2	Access Point...	90
....0101 UP: 5 - Video	YouTube	10.9.158.105	173.227.93.80	[redacted]	A	1	34505	64%	117.0	2	Access Point...	90
		A8:9D:21:0B:1B:E5	George iPad <Cellular>		#	1	34506	61%	24.0	1	Access Point...	32
....0101 UP: 5 - Video	YouTube	10.9.158.105	173.227.93.80	[redacted]	+A	1	34507	64%	117.0	2	Access Point...	90
....0101 UP: 5 - Video	YouTube	10.9.158.105	173.227.93.80	[redacted]	+A	1	34508	64%	117.0	2	Access Point...	90
		A8:9D:21:0B:1B:E5	George iPad <Cellular>		#	1	34509	59%	24.0	1	Access Point...	32
....0000 UP: 0 - Best Effort	YouTube	173.227.93.80	10.9.158.105	[redacted]	+	1	34510	63%	144.4	2	Access Point...	1538
....0000 UP: 0 - Best Effort	YouTube	173.227.93.80	10.9.158.105	[redacted]		1	34511	63%	130.3	2	Access Point...	1538
....0000 UP: 0 - Best Effort	YouTube	173.227.93.80	10.9.158.105	[redacted]		1	34512	63%	130.3	2	Access Point...	1538
....0000 UP: 0 - Best Effort	YouTube	173.227.93.80	10.9.158.105	[redacted]		1	34513	63%	130.3	2	Access Point...	1538
....0000 UP: 0 - Best Effort	YouTube	173.227.93.80	10.9.158.105	[redacted]		1	34514	63%	130.3	2	Access Point...	1538
		George iPad <Cellular>	A8:9D:21:0B:1B:E5		[redacted]	1	34515	58%	24.0	1	Access Point...	20
		A8:9D:21:0B:1B:E5	George iPad <Cellular>		[redacted]	1	34516	60%	24.0	1	Access Point...	14
....0101 UP: 5 - Video	YouTube	10.9.158.105	173.227.93.80	[redacted]	[redacted]	1	34517	64%	117.0	2	Access Point...	90
		A8:9D:21:0B:1B:E5	George iPad <Cellular>		[redacted]	1	34518	59%	24.0	1	Access Point...	32
....0101 UP: 5 - Video	YouTube	10.9.158.105	173.227.93.80	[redacted]	[redacted]	1	34519	64%	117.0	2	Access Point...	90

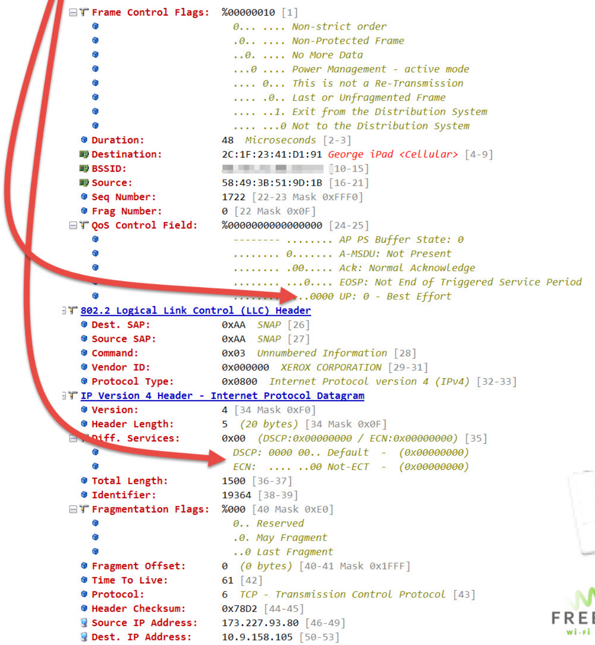
WMM QoS

Device: Apple iPad Air 2	
iOS 9.1	YOUTUBE APP

Frames arriving at the iPad marked with UP <0>

Layer 3 DSCP <0>





```
⊟ Frame Control Flags:    %00000010 [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
                            .... ..1. Exit from the Distribution System
                            .... ...0 Not to the Distribution System
  Duration:               48  Microseconds [2-3]
  Destination:            2C:1F:23:41:D1:91 George iPad <Cellular> [4-9]
  BSSID:                  [redacted] [10-15]
  Source:                 58:49:3B:51:9D:1B [16-21]
  Seq Number:             1722 [22-23 Mask 0xFFF0]
  Frag Number:            0 [22 Mask 0x0F]
⊟ QoS Control Field:      %0000000000000000 [24-25]
                            -------- ........ AP PS Buffer State: 0
                            ........ 0....... A-MSDU: Not Present
                            ........ .00..... Ack: Normal Acknowledge
                            ........ ...0.... EOSP: Not End of Triggered Service Period
                            ........ ....0000 UP: 0 - Best Effort
802.2 Logical Link Control (LLC) Header
  Dest. SAP:              0xAA  SNAP [26]
  Source SAP:             0xAA  SNAP [27]
  Command:                0x03  Unnumbered Information [28]
  Vendor ID:              0x000000  XEROX CORPORATION [29-31]
  Protocol Type:          0x0800  Internet Protocol version 4 (IPv4) [32-33]
IP Version 4 Header - Internet Protocol Datagram
  Version:                4 [34 Mask 0xF0]
  Header Length:          5  (20 bytes) [34 Mask 0x0F]
⊟ Diff. Services:         0x00  (DSCP:0x00000000 / ECN:0x00000000) [35]
                            DSCP: 0000 00.. Default  -  (0x00000000)
                            ECN:  .... ..00 Not-ECT  -  (0x00000000)
  Total Length:           1500 [36-37]
  Identifier:             19364 [38-39]
⊟ Fragmentation Flags:    %000 [40 Mask 0xE0]
                            0.. Reserved
                            .0. May Fragment
                            ..0 Last Fragment
  Fragment Offset:        0  (0 bytes) [40-41 Mask 0x1FFF]
  Time To Live:           61 [42]
  Protocol:               6  TCP - Transmission Control Protocol [43]
  Header Checksum:        0x78D2 [44-45]
  Source IP Address:      173.227.93.80 [46-49]
  Dest. IP Address:       10.9.158.105 [50-53]
```

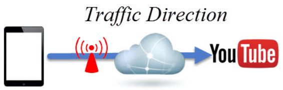
FREE SPACE wi-fi networking

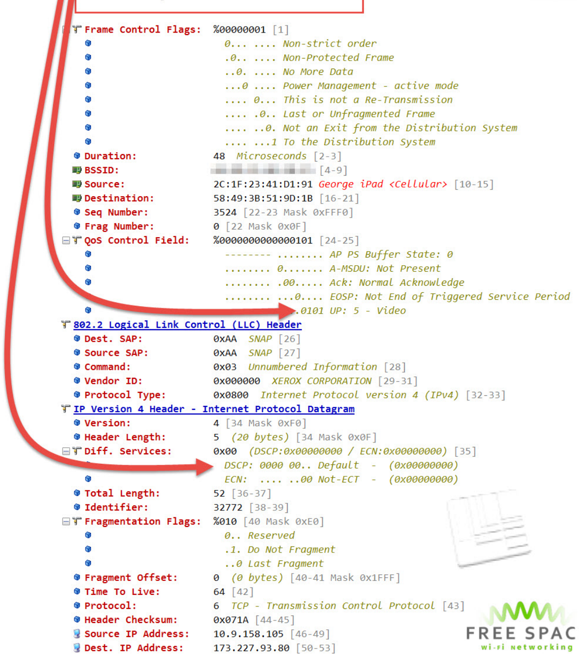
WMM QoS

Device: Apple iPad Air 2	
iOS 9.1	YOUTUBE APP

Layer 3 DSCP <0>

Frames leaving the iPad marked with a UP <5>


Traffic Direction


```
Frame Control Flags:   %00000001 [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
                         .... ...1 To the Distribution System
Duration:              48  Microseconds [2-3]
BSSID:                 [redacted] [4-9]
Source:                2C:1F:23:41:D1:91 George iPad <Cellular> [10-15]
Destination:           58:49:3B:51:9D:1B [16-21]
Seq Number:            3524 [22-23 Mask 0xFFF0]
Frag Number:           0 [22 Mask 0x0F]
QoS Control Field:     %0000000000000101 [24-25]
                         -------- ........ AP PS Buffer State: 0
                         ........ 0....... A-MSDU: Not Present
                         ........ .00..... Ack: Normal Acknowledge
                         ........ ...0.... EOSP: Not End of Triggered Service Period
                                    .0101 UP: 5 - Video
802.2 Logical Link Control (LLC) Header
Dest. SAP:             0xAA  SNAP [26]
Source SAP:            0xAA  SNAP [27]
Command:               0x03  Unnumbered Information [28]
Vendor ID:             0x000000  XEROX CORPORATION [29-31]
Protocol Type:         0x0800  Internet Protocol version 4 (IPv4) [32-33]
IP Version 4 Header - Internet Protocol Datagram
Version:               4 [34 Mask 0xF0]
Header Length:         5  (20 bytes) [34 Mask 0x0F]
Diff. Services:        0x00  (DSCP:0x00000000 / ECN:0x00000000) [35]
                         DSCP: 0000 00.. Default  -  (0x00000000)
                         ECN:  .... ..00 Not-ECT  -  (0x00000000)
Total Length:          52 [36-37]
Identifier:            32772 [38-39]
Fragmentation Flags:   %010 [40 Mask 0xE0]
                         0.. Reserved
                         .1. Do Not Fragment
                         ..0 Last Fragment
Fragment Offset:       0  (0 bytes) [40-41 Mask 0x1FFF]
Time To Live:          64 [42]
Protocol:              6  TCP - Transmission Control Protocol [43]
Header Checksum:       0x071A [44-45]
Source IP Address:     10.9.158.105 [46-49]
Dest. IP Address:      173.227.93.80 [50-53]
```

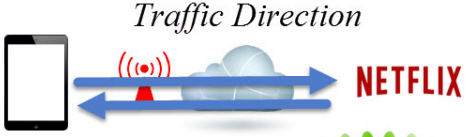
WMM QoS

Device: Apple iPad Air 2	
iOS 9.1	NETFLIX APP

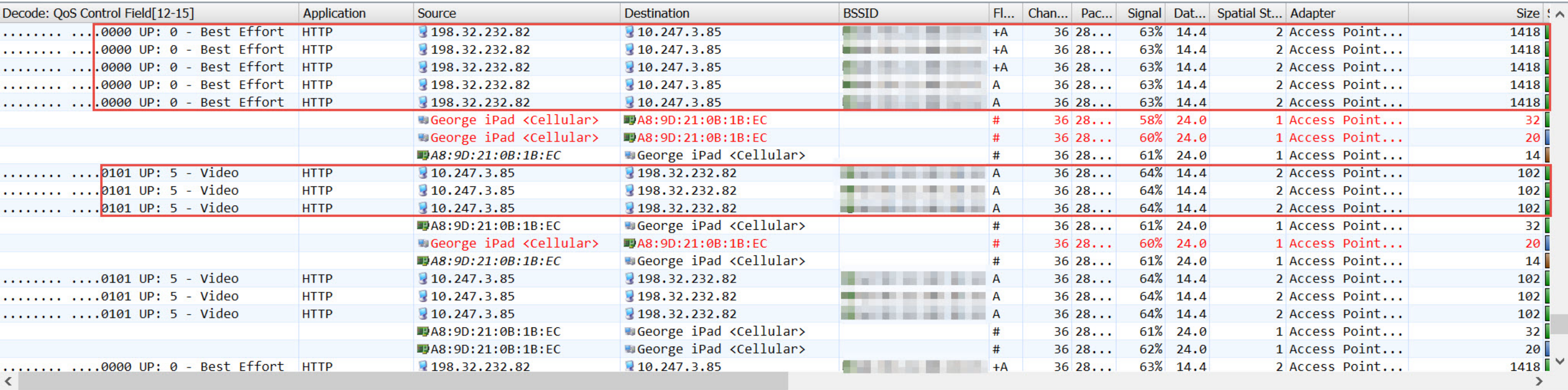
Frames arriving at the iPad marked with a UP <0>

Frames leaving the iPad marked with a UP <5>

NETFLIX traffic sourced from Rice University GigPop



FREE SPACE wi-fi networking



Decode: QoS Control Field[12-15]	Application	Source	Destination	BSSID	Fl...	Chan...	Pac...	Signal	Dat...	Spatial St...	Adapter	Size
....0000 UP: 0 - Best Effort	HTTP	198.32.232.82	10.247.3.85	[redacted]	+A	36	28...	63%	14.4	2	Access Point...	1418
....0000 UP: 0 - Best Effort	HTTP	198.32.232.82	10.247.3.85	[redacted]	+A	36	28...	63%	14.4	2	Access Point...	1418
....0000 UP: 0 - Best Effort	HTTP	198.32.232.82	10.247.3.85	[redacted]	+A	36	28...	63%	14.4	2	Access Point...	1418
....0000 UP: 0 - Best Effort	HTTP	198.32.232.82	10.247.3.85	[redacted]	A	36	28...	63%	14.4	2	Access Point...	1418
....0000 UP: 0 - Best Effort	HTTP	198.32.232.82	10.247.3.85	[redacted]	A	36	28...	63%	14.4	2	Access Point...	1418
		George iPad <Cellular>	A8:9D:21:0B:1B:EC		#	36	28...	58%	24.0	1	Access Point...	32
		George iPad <Cellular>	A8:9D:21:0B:1B:EC		#	36	28...	60%	24.0	1	Access Point...	20
		A8:9D:21:0B:1B:EC	George iPad <Cellular>		#	36	28...	61%	24.0	1	Access Point...	14
....0101 UP: 5 - Video	HTTP	10.247.3.85	198.32.232.82	[redacted]	A	36	28...	64%	14.4	2	Access Point...	102
....0101 UP: 5 - Video	HTTP	10.247.3.85	198.32.232.82	[redacted]	A	36	28...	64%	14.4	2	Access Point...	102
....0101 UP: 5 - Video	HTTP	10.247.3.85	198.32.232.82	[redacted]	A	36	28...	64%	14.4	2	Access Point...	102
		A8:9D:21:0B:1B:EC	George iPad <Cellular>		#	36	28...	61%	24.0	1	Access Point...	32
		George iPad <Cellular>	A8:9D:21:0B:1B:EC		#	36	28...	60%	24.0	1	Access Point...	20
		A8:9D:21:0B:1B:EC	George iPad <Cellular>		#	36	28...	61%	24.0	1	Access Point...	14
....0101 UP: 5 - Video	HTTP	10.247.3.85	198.32.232.82	[redacted]	A	36	28...	64%	14.4	2	Access Point...	102
....0101 UP: 5 - Video	HTTP	10.247.3.85	198.32.232.82	[redacted]	A	36	28...	64%	14.4	2	Access Point...	102
....0101 UP: 5 - Video	HTTP	10.247.3.85	198.32.232.82	[redacted]	A	36	28...	64%	14.4	2	Access Point...	102
		A8:9D:21:0B:1B:EC	George iPad <Cellular>		#	36	28...	61%	24.0	1	Access Point...	32
		A8:9D:21:0B:1B:EC	George iPad <Cellular>		#	36	28...	62%	24.0	1	Access Point...	20
....0000 UP: 0 - Best Effort	HTTP	198.32.232.82	10.247.3.85	[redacted]	+A	36	28...	63%	14.4	2	Access Point...	1418

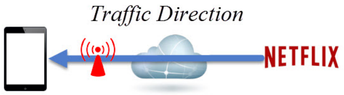
WMM QoS

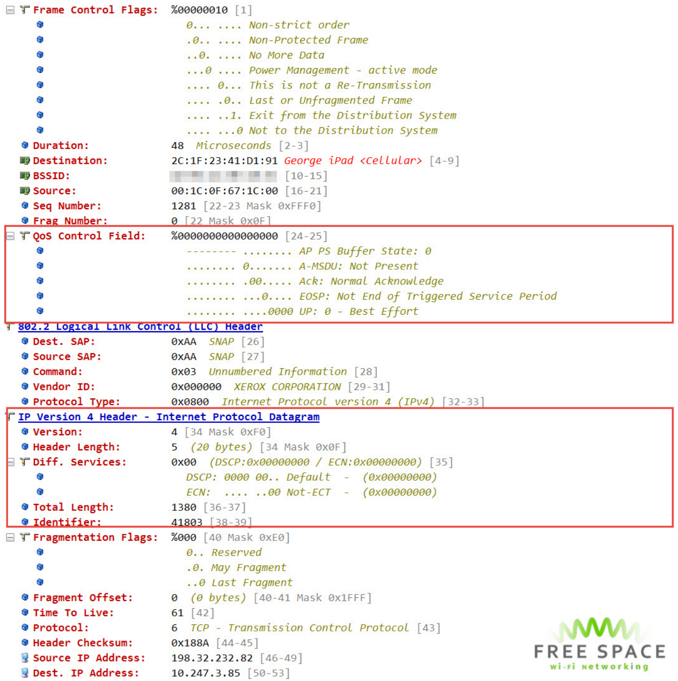
Device: Apple iPad Air 2

iOS 9.1 | NETFLIX APP

Frames arriving at the iPad marked with UP <0>
Layer 3 DSCP <0>

NETFLIX traffic sourced from Rice University GigPop





```
⊟ Frame Control Flags:   %00000010 [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
                          .... ..1. Exit from the Distribution System
                          .... ...0 Not to the Distribution System
  Duration:              48  Microseconds [2-3]
  Destination:           2C:1F:23:41:D1:91 George iPad <Cellular> [4-9]
  BSSID:                 [redacted] [10-15]
  Source:                00:1C:0F:67:1C:00 [16-21]
  Seq Number:            1281 [22-23 Mask 0xFFF0]
  Frag Number:           0 [22 Mask 0x0F]
⊟ QoS Control Field:     %0000000000000000 [24-25]
                          -------- ........ AP PS Buffer State: 0
                          ........ 0....... A-MSDU: Not Present
                          ........ .00..... Ack: Normal Acknowledge
                          ........ ...0.... EOSP: Not End of Triggered Service Period
                          ........ ....0000 UP: 0 - Best Effort
802.2 Logical Link Control (LLC) Header
  Dest. SAP:             0xAA  SNAP [26]
  Source SAP:            0xAA  SNAP [27]
  Command:               0x03  Unnumbered Information [28]
  Vendor ID:             0x000000  XEROX CORPORATION [29-31]
  Protocol Type:         0x0800  Internet Protocol version 4 (IPv4) [32-33]
IP Version 4 Header - Internet Protocol Datagram
  Version:               4 [34 Mask 0xF0]
  Header Length:         5  (20 bytes) [34 Mask 0x0F]
⊟ Diff. Services:        0x00  (DSCP:0x00000000 / ECN:0x00000000) [35]
                          DSCP: 0000 00.. Default  -  (0x00000000)
                          ECN:  .... ..00 Not-ECT  -  (0x00000000)
  Total Length:          1380 [36-37]
  Identifier:            41803 [38-39]
⊟ Fragmentation Flags:   %000 [40 Mask 0xE0]
                          0.. Reserved
                          .0. May Fragment
                          ..0 Last Fragment
  Fragment Offset:       0  (0 bytes) [40-41 Mask 0x1FFF]
  Time To Live:          61 [42]
  Protocol:              6  TCP - Transmission Control Protocol [43]
  Header Checksum:       0x188A [44-45]
  Source IP Address:     198.32.232.82 [46-49]
  Dest. IP Address:      10.247.3.85 [50-53]
```

FREE SPACE wi-fi networking

WMM QoS

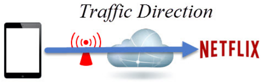
Device: Apple iPad Air 2

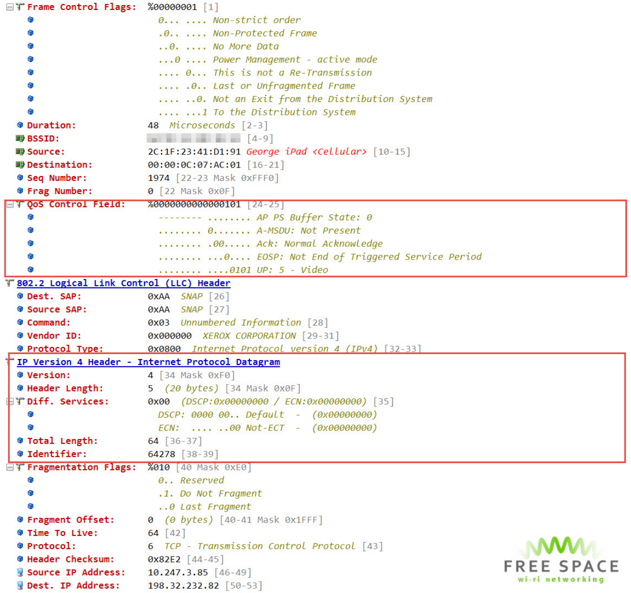
iOS 9.1	NETFLIX APP

Layer 3 DSCP <0>

Frames leaving the iPad marked with UP <5>

NETFLIX traffic sourced from Rice University GigPop





```
Frame Control Flags:   %00000001 [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
                         .... ...1 To the Distribution System
Duration:              48  Microseconds [2-3]
BSSID:                 [redacted] [4-9]
Source:                2C:1F:23:41:D1:91 George iPad <Cellular> [10-15]
Destination:           00:00:0C:07:AC:01 [16-21]
Seq Number:            1974 [22-23 Mask 0xFFF0]
Frag Number:           0 [22 Mask 0x0F]
QoS Control Field:     %0000000000000101 [24-25]
                         -------- ........ AP PS Buffer State: 0
                         ........ 0....... A-MSDU: Not Present
                         ........ .00..... Ack: Normal Acknowledge
                         ........ ...0.... EOSP: Not End of Triggered Service Period
                         ........ ....0101 UP: 5 - Video
802.2 Logical Link Control (LLC) Header
Dest. SAP:             0xAA  SNAP [26]
Source SAP:            0xAA  SNAP [27]
Command:               0x03  Unnumbered Information [28]
Vendor ID:             0x000000  XEROX CORPORATION [29-31]
Protocol Type:         0x0800  Internet Protocol version 4 (IPv4) [32-33]
IP Version 4 Header - Internet Protocol Datagram
Version:               4 [34 Mask 0xF0]
Header Length:         5  (20 bytes) [34 Mask 0x0F]
Diff. Services:        0x00  (DSCP:0x00000000 / ECN:0x00000000) [35]
                         DSCP: 0000 00.. Default  -  (0x00000000)
                         ECN:  .... ..00 Not-ECT  -  (0x00000000)
Total Length:          64 [36-37]
Identifier:            64278 [38-39]
Fragmentation Flags:   %010 [40 Mask 0xE0]
                         0.. Reserved
                         .1. Do Not Fragment
                         ..0 Last Fragment
Fragment Offset:       0  (0 bytes) [40-41 Mask 0x1FFF]
Time To Live:          64 [42]
Protocol:              6  TCP - Transmission Control Protocol [43]
Header Checksum:       0x82E2 [44-45]
Source IP Address:     10.247.3.85 [46-49]
Dest. IP Address:      198.32.232.82 [50-53]
```

FREE SPACE wi-fi networking

WMM QoS

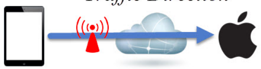
Device: Apple iPad Air 2

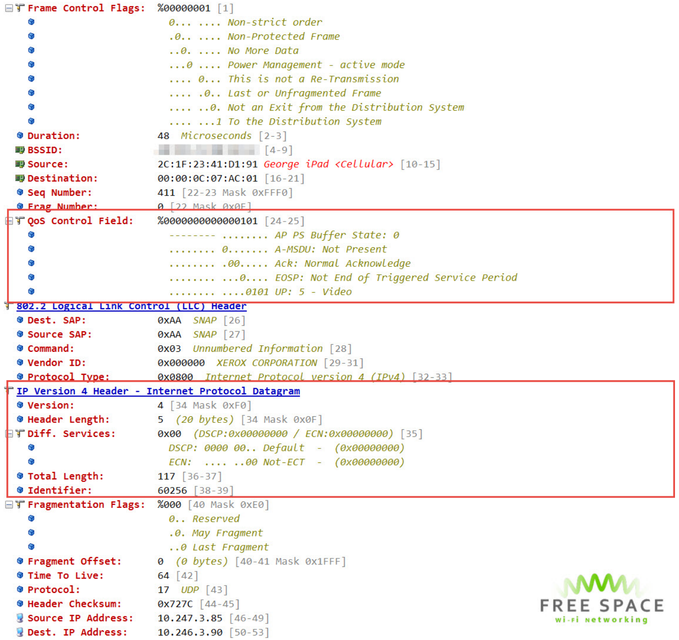
iOS 9.1	FACETIME

Layer 3 DSCP <0>

Frames leaving the iPad marked with UP <5>

Traffic Direction





```
⊟ Frame Control Flags:   %00000001 [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
                           .... ...1 To the Distribution System
   Duration:             48  Microseconds [2-3]
   BSSID:                [redacted] [4-9]
   Source:               2C:1F:23:41:D1:91 George iPad <Cellular> [10-15]
   Destination:          00:00:0C:07:AC:01 [16-21]
   Seq Number:           411 [22-23 Mask 0xFFF0]
   Frag Number:          0 [22 Mask 0x0F]
⊟ QoS Control Field:     %0000000000000101 [24-25]
                           -------- ........ AP PS Buffer State: 0
                           ........ 0....... A-MSDU: Not Present
                           ........ .00..... Ack: Normal Acknowledge
                           ........ ...0.... EOSP: Not End of Triggered Service Period
                           ........ ....0101 UP: 5 - Video
 802.2 Logical Link Control (LLC) Header
   Dest. SAP:            0xAA  SNAP [26]
   Source SAP:           0xAA  SNAP [27]
   Command:              0x03  Unnumbered Information [28]
   Vendor ID:            0x000000  XEROX CORPORATION [29-31]
   Protocol Type:        0x0800  Internet Protocol version 4 (IPv4) [32-33]
 IP Version 4 Header - Internet Protocol Datagram
   Version:              4 [34 Mask 0xF0]
   Header Length:        5  (20 bytes) [34 Mask 0x0F]
⊟ Diff. Services:        0x00  (DSCP:0x00000000 / ECN:0x00000000) [35]
                           DSCP: 0000 00.. Default  -  (0x00000000)
                           ECN:  .... ..00 Not-ECT  -  (0x00000000)
   Total Length:         117 [36-37]
   Identifier:           60256 [38-39]
⊟ Fragmentation Flags:   %000 [40 Mask 0xE0]
                           0.. Reserved
                           .0. May Fragment
                           ..0 Last Fragment
   Fragment Offset:      0  (0 bytes) [40-41 Mask 0x1FFF]
   Time To Live:         64 [42]
   Protocol:             17  UDP [43]
   Header Checksum:      0x727C [44-45]
   Source IP Address:    10.247.3.85 [46-49]
   Dest. IP Address:     10.246.3.90 [50-53]
```

FREE SPACE wi-fi networking

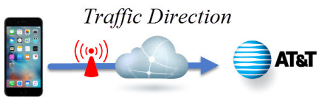
WMM QoS

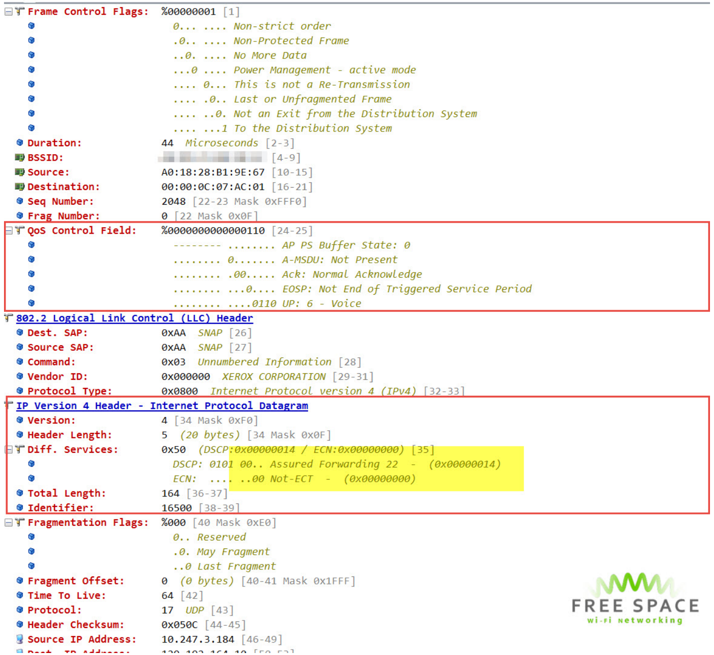
Device: Apple iPad Air 2

iOS 9.1	ATT WiFi Calling

Layer 3 DSCP <AF22>

Frames leaving the iPhone marked with UP <6>



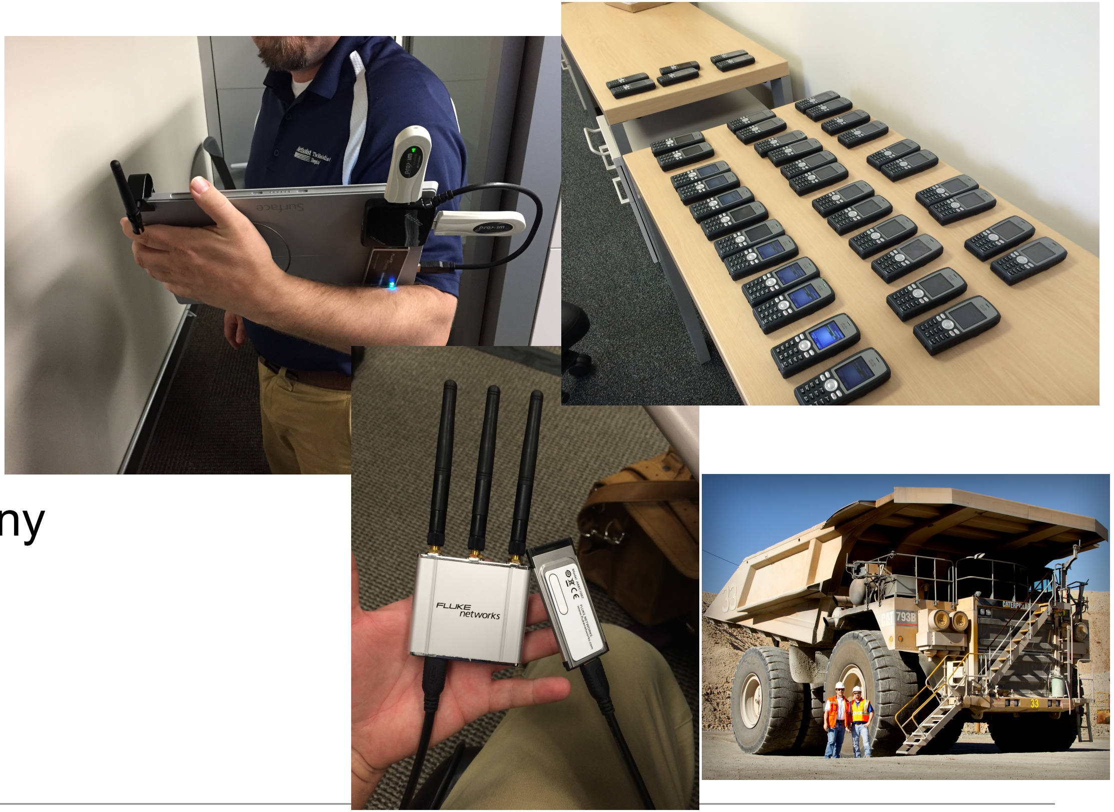


```
⊟ Frame Control Flags:   %00000001 [1]
                           0... .... Non-strict order
                           .0.. .... Non-Protected Frame
                           ..0. .... No More Data
                           ...0 .... Power Management - active mode
                           .... 0... This is not a Re-Transmission
                           .... .0.. Last or Unfragmented Frame
                           .... ..0. Not an Exit from the Distribution System
                           .... ...1 To the Distribution System
  Duration:              44  Microseconds [2-3]
  BSSID:                 [redacted] [4-9]
  Source:                A0:18:28:B1:9E:67 [10-15]
  Destination:           00:00:0C:07:AC:01 [16-21]
  Seq Number:            2048 [22-23 Mask 0xFFF0]
  Frag Number:           0 [22 Mask 0x0F]
⊟ QoS Control Field:     %0000000000000110 [24-25]
                           -------- ........ AP PS Buffer State: 0
                           ........ 0....... A-MSDU: Not Present
                           ........ .00..... Ack: Normal Acknowledge
                           ........ ...0.... EOSP: Not End of Triggered Service Period
                           ........ ....0110 UP: 6 - Voice
802.2 Logical Link Control (LLC) Header
  Dest. SAP:             0xAA  SNAP [26]
  Source SAP:            0xAA  SNAP [27]
  Command:               0x03  Unnumbered Information [28]
  Vendor ID:             0x000000  XEROX CORPORATION [29-31]
  Protocol Type:         0x0800  Internet Protocol version 4 (IPv4) [32-33]
IP Version 4 Header - Internet Protocol Datagram
  Version:               4 [34 Mask 0xF0]
  Header Length:         5  (20 bytes) [34 Mask 0x0F]
⊟ Diff. Services:        0x50  (DSCP:0x00000014 / ECN:0x00000000) [35]
                           DSCP: 0101 00.. Assured Forwarding 22  -  (0x00000014)
                           ECN:  .... ..00 Not-ECT  -  (0x00000000)
  Total Length:          164 [36-37]
  Identifier:            16500 [38-39]
⊟ Fragmentation Flags:   %000 [40 Mask 0xE0]
                           0.. Reserved
                           .0. May Fragment
                           ..0 Last Fragment
  Fragment Offset:       0  (0 bytes) [40-41 Mask 0x1FFF]
  Time To Live:          64 [42]
  Protocol:              17  UDP [43]
  Header Checksum:       0x050C [44-45]
  Source IP Address:     10.247.3.184 [46-49]
  Dest. IP Address:      130.102.164.10 [50-53]
```

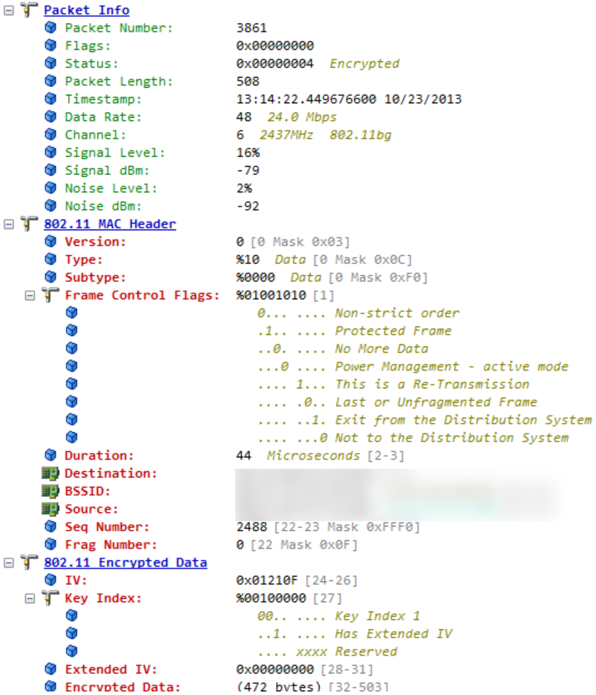
FREE SPACE
wi-fi networking

Sniffing Challenges

802.11ac
Get close to the radio
Use Aps as sniffers
Build filters and use triggers
Know that you may miss frames
Wildpackets WiFi Appliance
Fluke AirMagnet a Netscout Company

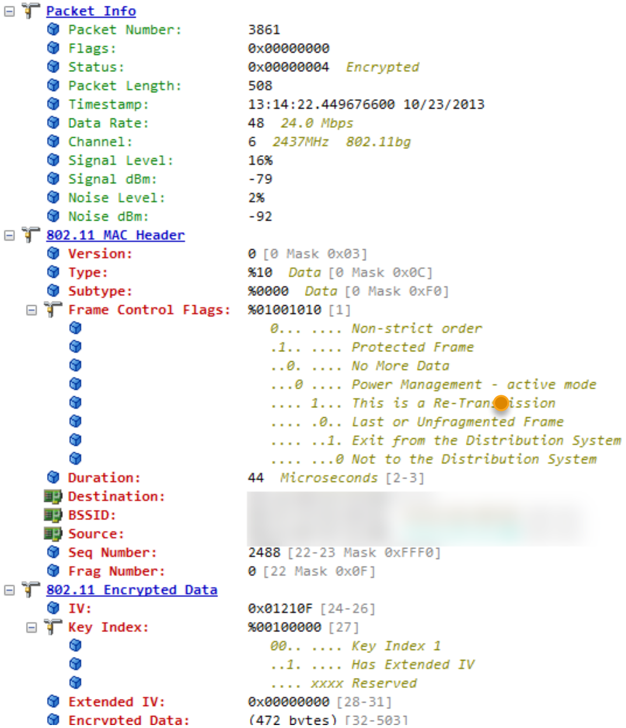


Real World Example – Wireless is slow



```
⊟ Packet Info
    Packet Number:          3861
    Flags:                  0x00000000
    Status:                 0x00000004  Encrypted
    Packet Length:          508
    Timestamp:              13:14:22.449676600 10/23/2013
    Data Rate:              48  24.0 Mbps
    Channel:                6  2437MHz  802.11bg
    Signal Level:           16%
    Signal dBm:             -79
    Noise Level:            2%
    Noise dBm:              -92
⊟ 802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %10  Data [0 Mask 0x0C]
    Subtype:                %0000  Data [0 Mask 0xF0]
  ⊟ Frame Control Flags:    %01001010 [1]
                              0... .... Non-strict order
                              .1.. .... Protected Frame
                              ..0. .... No More Data
                              ...0 .... Power Management - active mode
                              .... 1... This is a Re-Transmission
                              .... .0.. Last or Unfragmented Frame
                              .... ..1. Exit from the Distribution System
                              .... ...0 Not to the Distribution System
    Duration:               44  Microseconds [2-3]
    Destination:            [redacted]
    BSSID:
    Source:
    Seq Number:             2488 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
⊟ 802.11 Encrypted Data
    IV:                     0x01210F [24-26]
  ⊟ Key Index:              %00100000 [27]
                              00.. .... Key Index 1
                              ..1. .... Has Extended IV
                              .... xxxx Reserved
    Extended IV:            0x00000000 [28-31]
    Encrypted Data:         (472 bytes) [32-503]
```

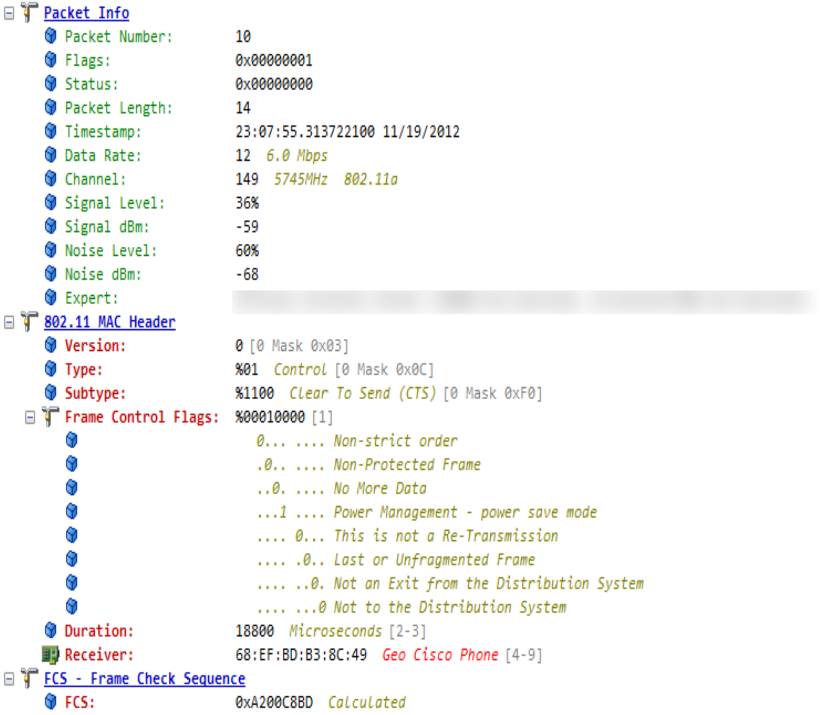
Real World Example – Wireless is slow



```
⊟ Packet Info
    Packet Number:          3861
    Flags:                  0x00000000
    Status:                 0x00000004  Encrypted
    Packet Length:          508
    Timestamp:              13:14:22.449676600 10/23/2013
    Data Rate:              48  24.0 Mbps
    Channel:                6  2437MHz  802.11bg
    Signal Level:           16%
    Signal dBm:             -79
    Noise Level:            2%
    Noise dBm:              -92
⊟ 802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %10  Data [0 Mask 0x0C]
    Subtype:                %0000  Data [0 Mask 0xF0]
  ⊟ Frame Control Flags:    %01001010 [1]
                              0... ....  Non-strict order
                              .1.. ....  Protected Frame
                              ..0. ....  No More Data
                              ...0 ....  Power Management - active mode
                              .... 1...  This is a Re-Transmission
                              .... .0..  Last or Unfragmented Frame
                              .... ..1.  Exit from the Distribution System
                              .... ...0  Not to the Distribution System
    Duration:               44  Microseconds [2-3]
    Destination:            [redacted]
    BSSID:
    Source:
    Seq Number:             2488 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
⊟ 802.11 Encrypted Data
    IV:                     0x01210F [24-26]
  ⊟ Key Index:              %00100000 [27]
                              00.. ....  Key Index 1
                              ..1. ....  Has Extended IV
                              .... xxxx  Reserved
    Extended IV:            0x00000000 [28-31]
    Encrypted Data:         (472 bytes) [32-503]
```

Retry (Frame Retransmission)

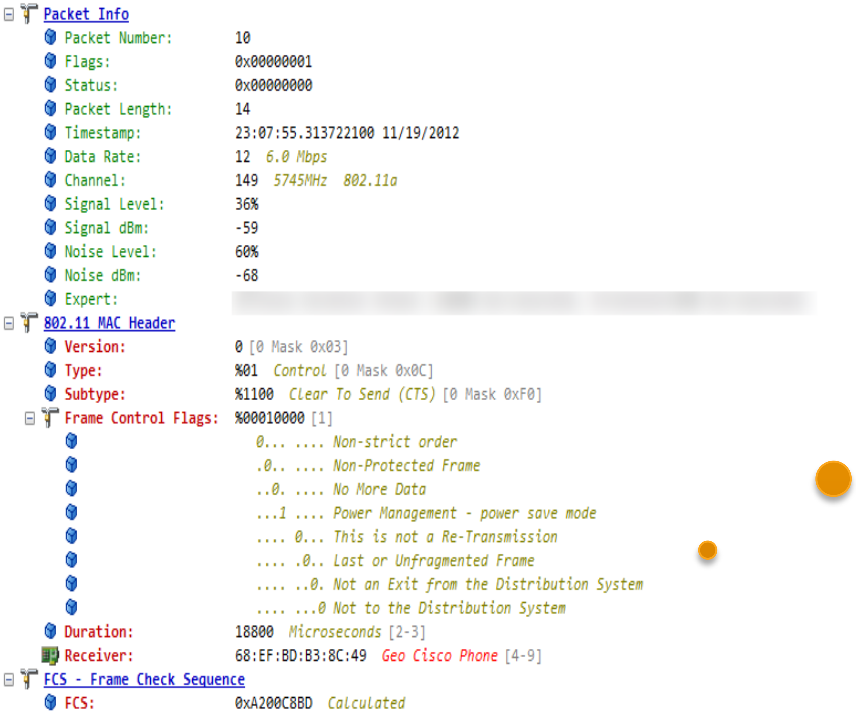
Real World Example – Clients dropping connection



```
⊟ Packet Info
     Packet Number:        10
     Flags:                0x00000001
     Status:               0x00000000
     Packet Length:        14
     Timestamp:            23:07:55.313722100 11/19/2012
     Data Rate:            12  6.0 Mbps
     Channel:              149  5745MHz  802.11a
     Signal Level:         36%
     Signal dBm:           -59
     Noise Level:          60%
     Noise dBm:            -68
     Expert:               [redacted]
⊟ 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:  %00010000 [1]
                             0... .... Non-strict order
                             .0.. .... Non-Protected Frame
                             ..0. .... No More Data
                             ...1 .... Power Management - power save 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:             18800  Microseconds [2-3]
     Receiver:             68:EF:BD:B3:8C:49  Geo Cisco Phone [4-9]
⊟ FCS - Frame Check Sequence
     FCS:                  0xA200C8BD  Calculated
```

Real World Example – Clients dropping connection

ANZ ATMOSPHERE 2015 HOW TOMORROW MOVES

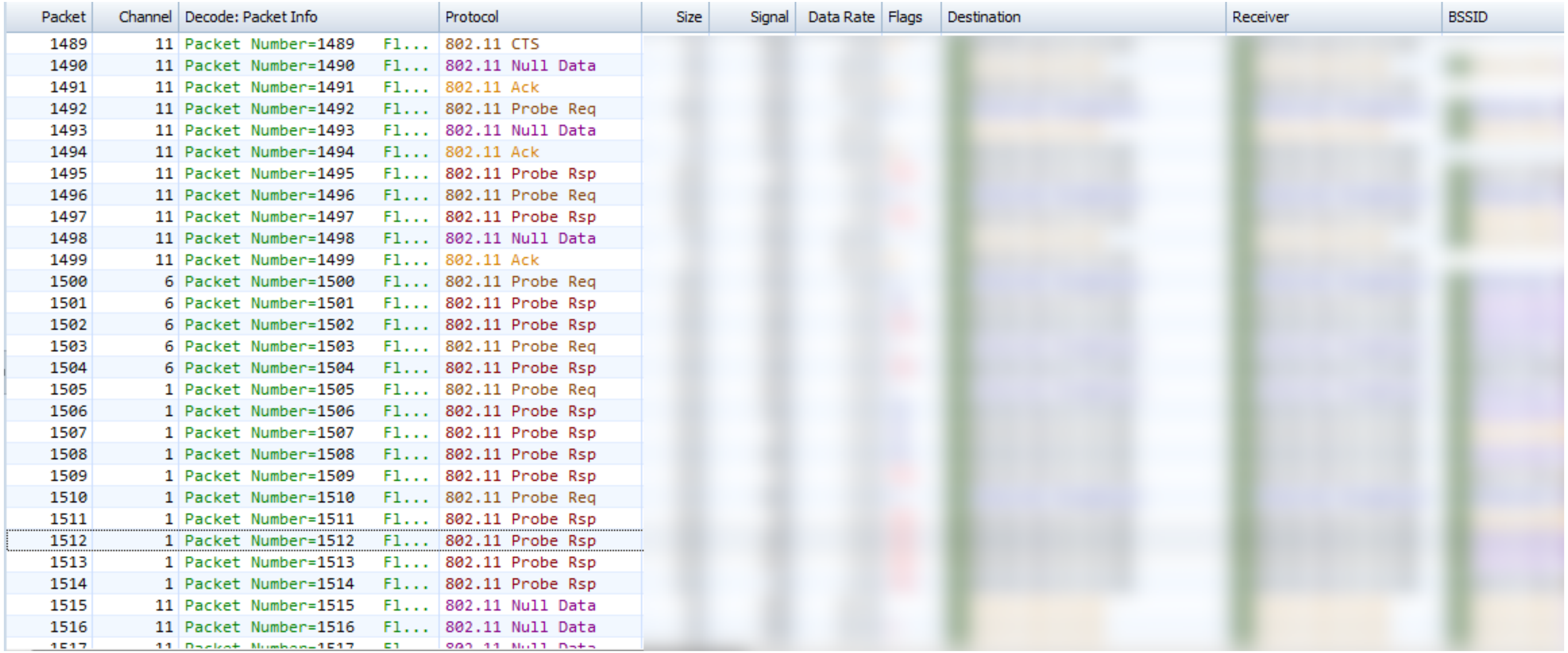


```
⊟ Packet Info
    Packet Number:          10
    Flags:                  0x00000001
    Status:                 0x00000000
    Packet Length:          14
    Timestamp:              23:07:55.313722100 11/19/2012
    Data Rate:              12  6.0 Mbps
    Channel:                149  5745MHz  802.11a
    Signal Level:           36%
    Signal dBm:             -59
    Noise Level:            60%
    Noise dBm:              -68
    Expert:                 [redacted]
⊟ 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:    %00010000 [1]
                              0... .... Non-strict order
                              .0.. .... Non-Protected Frame
                              ..0. .... No More Data
                              ...1 .... Power Management - power save 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:               18800  Microseconds [2-3]
    Receiver:               68:EF:BD:B3:8C:49  Geo Cisco Phone [4-9]
⊟ FCS - Frame Check Sequence
    FCS:                    0xA200C8BD  Calculated
```

NAV 18,800 us

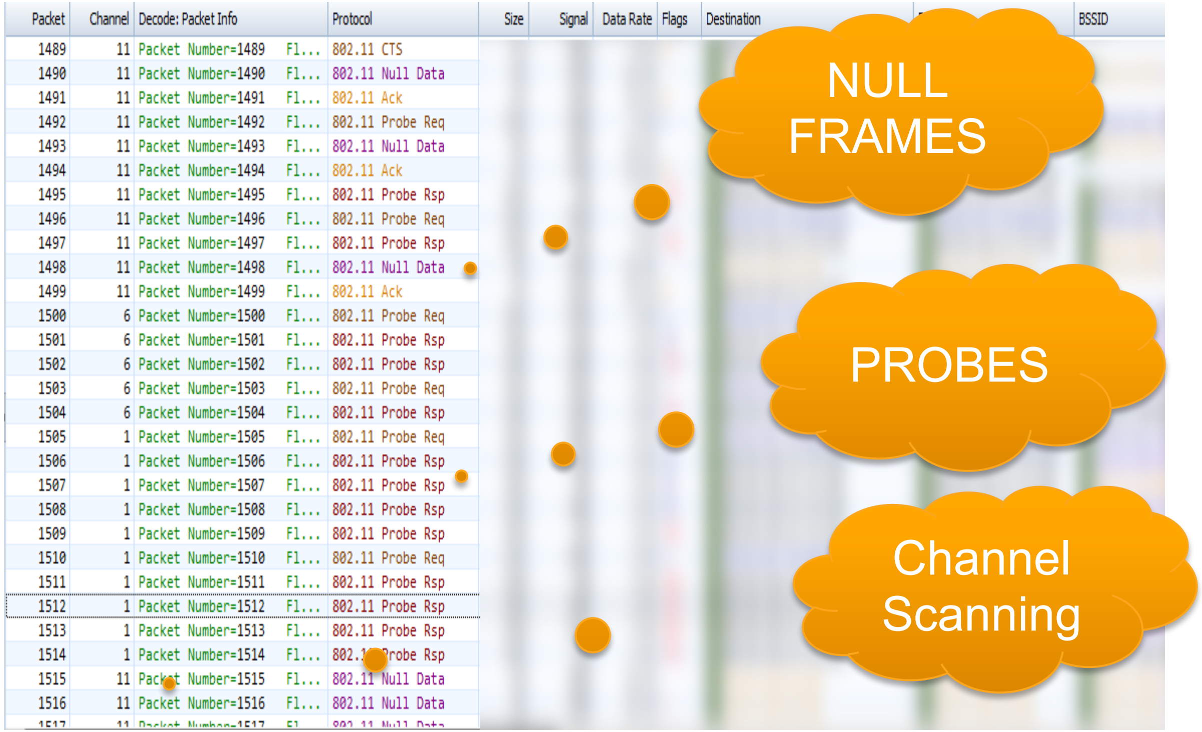
Real World Example – Slow connection lots of application drops

ANZ ATMOSPHERE 2015
HOW TOMORROW MOVES



Packet	Channel	Decode: Packet Info	Protocol	Size	Signal	Data Rate	Flags	Destination	Receiver	BSSID
1489	11	Packet Number=1489 Fl...	802.11 CTS	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1490	11	Packet Number=1490 Fl...	802.11 Null Data	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1491	11	Packet Number=1491 Fl...	802.11 Ack	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1492	11	Packet Number=1492 Fl...	802.11 Probe Req	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1493	11	Packet Number=1493 Fl...	802.11 Null Data	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1494	11	Packet Number=1494 Fl...	802.11 Ack	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1495	11	Packet Number=1495 Fl...	802.11 Probe Rsp	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1496	11	Packet Number=1496 Fl...	802.11 Probe Req	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1497	11	Packet Number=1497 Fl...	802.11 Probe Rsp	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1498	11	Packet Number=1498 Fl...	802.11 Null Data	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1499	11	Packet Number=1499 Fl...	802.11 Ack	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1500	6	Packet Number=1500 Fl...	802.11 Probe Req	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1501	6	Packet Number=1501 Fl...	802.11 Probe Rsp	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1502	6	Packet Number=1502 Fl...	802.11 Probe Rsp	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1503	6	Packet Number=1503 Fl...	802.11 Probe Req	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1504	6	Packet Number=1504 Fl...	802.11 Probe Rsp	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1505	1	Packet Number=1505 Fl...	802.11 Probe Req	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1506	1	Packet Number=1506 Fl...	802.11 Probe Rsp	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1507	1	Packet Number=1507 Fl...	802.11 Probe Rsp	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1508	1	Packet Number=1508 Fl...	802.11 Probe Rsp	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1509	1	Packet Number=1509 Fl...	802.11 Probe Rsp	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1510	1	Packet Number=1510 Fl...	802.11 Probe Req	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1511	1	Packet Number=1511 Fl...	802.11 Probe Rsp	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1512	1	Packet Number=1512 Fl...	802.11 Probe Rsp	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1513	1	Packet Number=1513 Fl...	802.11 Probe Rsp	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1514	1	Packet Number=1514 Fl...	802.11 Probe Rsp	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1515	11	Packet Number=1515 Fl...	802.11 Null Data	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1516	11	Packet Number=1516 Fl...	802.11 Null Data	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1517	11	Packet Number=1517 Fl...	802.11 Null Data	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Real World Example – Slow connection lots of application drops



Packet	Channel	Decode: Packet Info	Protocol
1489	11	Packet Number=1489 Fl...	802.11 CTS
1490	11	Packet Number=1490 Fl...	802.11 Null Data
1491	11	Packet Number=1491 Fl...	802.11 Ack
1492	11	Packet Number=1492 Fl...	802.11 Probe Req
1493	11	Packet Number=1493 Fl...	802.11 Null Data
1494	11	Packet Number=1494 Fl...	802.11 Ack
1495	11	Packet Number=1495 Fl...	802.11 Probe Rsp
1496	11	Packet Number=1496 Fl...	802.11 Probe Req
1497	11	Packet Number=1497 Fl...	802.11 Probe Rsp
1498	11	Packet Number=1498 Fl...	802.11 Null Data
1499	11	Packet Number=1499 Fl...	802.11 Ack
1500	6	Packet Number=1500 Fl...	802.11 Probe Req
1501	6	Packet Number=1501 Fl...	802.11 Probe Rsp
1502	6	Packet Number=1502 Fl...	802.11 Probe Rsp
1503	6	Packet Number=1503 Fl...	802.11 Probe Req
1504	6	Packet Number=1504 Fl...	802.11 Probe Rsp
1505	1	Packet Number=1505 Fl...	802.11 Probe Req
1506	1	Packet Number=1506 Fl...	802.11 Probe Rsp
1507	1	Packet Number=1507 Fl...	802.11 Probe Rsp
1508	1	Packet Number=1508 Fl...	802.11 Probe Rsp
1509	1	Packet Number=1509 Fl...	802.11 Probe Rsp
1510	1	Packet Number=1510 Fl...	802.11 Probe Req
1511	1	Packet Number=1511 Fl...	802.11 Probe Rsp
1512	1	Packet Number=1512 Fl...	802.11 Probe Rsp
1513	1	Packet Number=1513 Fl...	802.11 Probe Rsp
1514	1	Packet Number=1514 Fl...	802.11 Probe Rsp
1515	11	Packet Number=1515 Fl...	802.11 Null Data
1516	11	Packet Number=1516 Fl...	802.11 Null Data
1517	11	Packet Number=1517 Fl...	802.11 Null Data

NULL FRAMES

PROBES

Channel Scanning

LLC, MAC, PLCP, PMD

ANZ atmosphere2015 HOW TOMORROW MOVES

LLC, MAC, PLCP, PMD: Know the layers and what each layer does

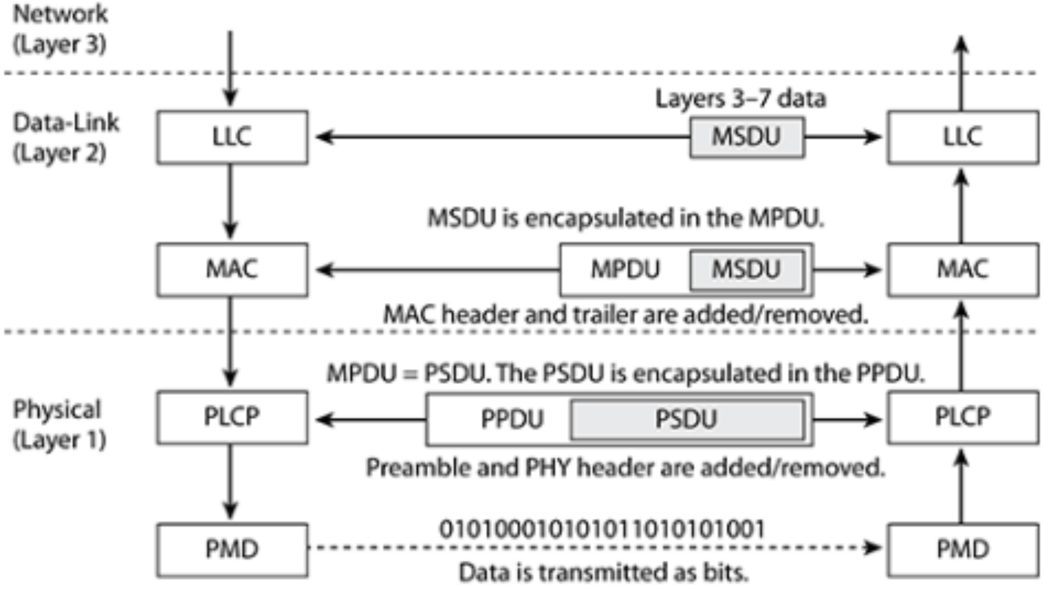
LLC, MAC, PLCP, PMD

LAYER 2	LLC – Logical Link Control
LAYER 2	MAC – Media Access Control
LAYER 1	PLCP – Physical Layer Convergence Procedure
LAYER 1	PMD – Physical Medium Dependent

LLC, MAC, PLCP, PMD

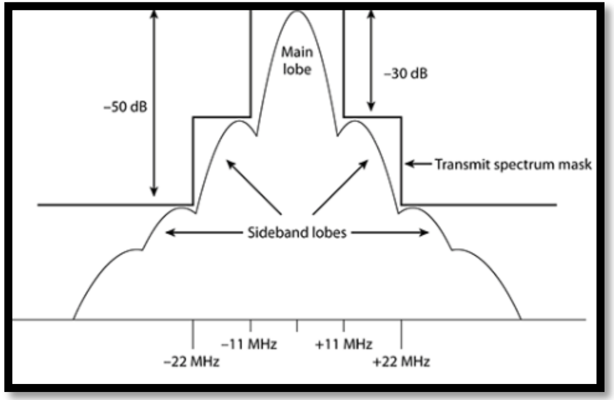
LAYER 2	LLC – Logical Link Control (MSDU) *Packet
LAYER 2	MAC – Media Access Control (MPDU) * Frame
LAYER 1	PLCP – Physical Layer Convergence Procedure(PSDU/PPDU)
LAYER 1	PMD – Physical Medium Dependent (Bits)

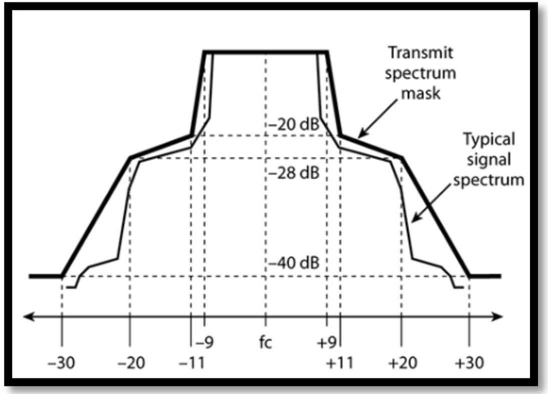
LLC, MAC, PLCP, PMD – Encapsulated Headers


Network
(Layer 3)
Data-Link
(Layer 2)
Physical
(Layer 1)
LLC
Layers 3–7 data
MSDU
LLC
MSDU is encapsulated in the MPDU.
MAC
MPDU
MSDU
MAC
MAC header and trailer are added/removed.
MPDU = PSDU. The PSDU is encapsulated in the PPDU.
PLCP
PPDU
PSDU
PLCP
Preamble and PHY header are added/removed.
PMD
010100010101011010101001
PMD
Data is transmitted as bits.

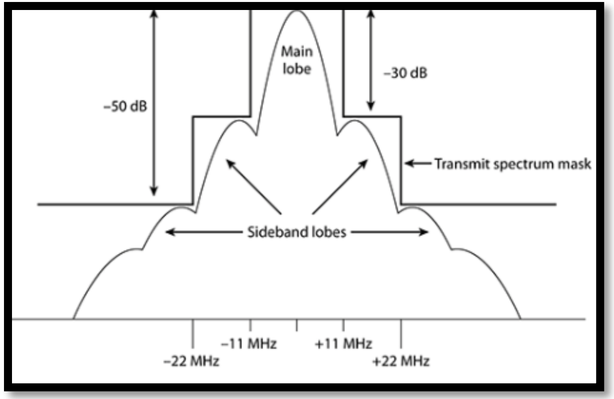
Spectrum Masks – DSSS / OFDM

ANZ atmosphere2015 HOW TOMORROW MOVES



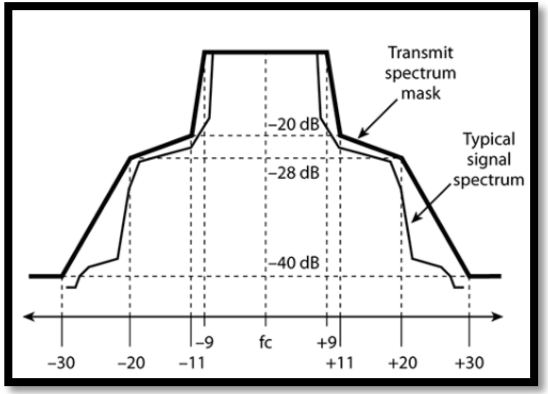


Modulation – 802.11 PRIME and 802.11b



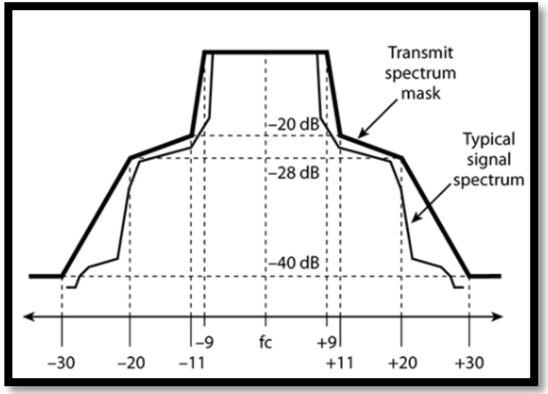
1	PHY	DBPSK
2	PHY	DQPSK
5.5	PHY	CCK
11	PHY	CCK

Modulation – ERP-OFDM 802.11g



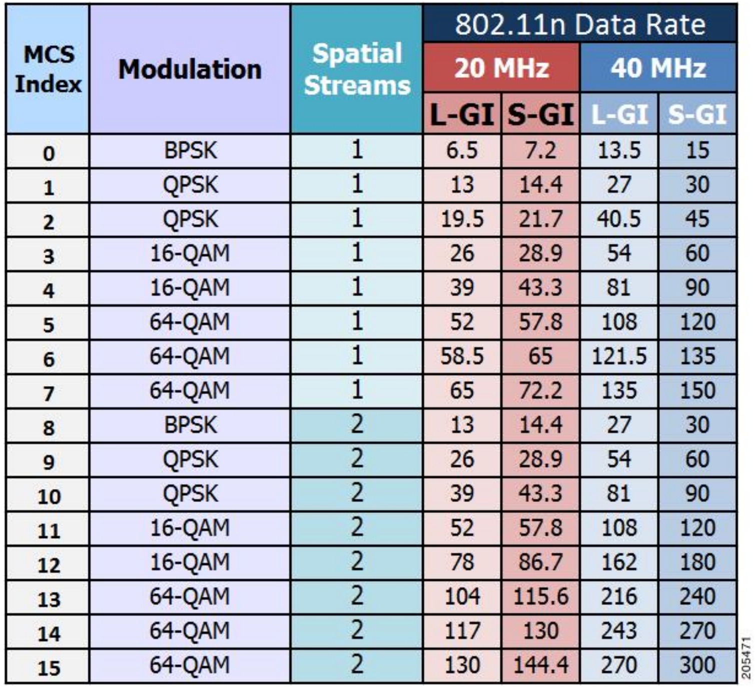
6	PHY	BPSK
9	PHY	BPSK
12	PHY	QPSK
18	PHY	QPSK
24	PHY	QAM16
36	PHY	QAM16
48	PHY	QAM64
54	PHY	QAM64

Modulation – OFDM 802.11a



6	PHY	BPSK
9	PHY	BPSK
12	PHY	QPSK
18	PHY	QPSK
24	PHY	QAM16
36	PHY	QAM16
48	PHY	QAM64
54	PHY	QAM64

Modulation MIMO-OFDM 802.11n/ac



MCS Index	Modulation	Spatial Streams	802.11n Data Rate			
			20 MHz		40 MHz	
			L-GI	S-GI	L-GI	S-GI
0	BPSK	1	6.5	7.2	13.5	15
1	QPSK	1	13	14.4	27	30
2	QPSK	1	19.5	21.7	40.5	45
3	16-QAM	1	26	28.9	54	60
4	16-QAM	1	39	43.3	81	90
5	64-QAM	1	52	57.8	108	120
6	64-QAM	1	58.5	65	121.5	135
7	64-QAM	1	65	72.2	135	150
8	BPSK	2	13	14.4	27	30
9	QPSK	2	26	28.9	54	60
10	QPSK	2	39	43.3	81	90
11	16-QAM	2	52	57.8	108	120
12	16-QAM	2	78	86.7	162	180
13	64-QAM	2	104	115.6	216	240
14	64-QAM	2	117	130	243	270
15	64-QAM	2	130	144.4	270	300

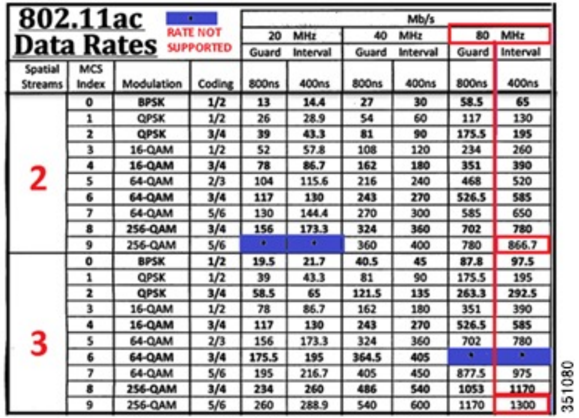
205471

802.11ac (Wave-1)

.11ac MCS rates (unlike 802.11n) don't exceed 0-9 -- but rather **it is 0-9** and then you **call out how many Spatial Streams** are being used so a chart like this is quite extensive.

Depicted to the right are 2 & 3 SS Supported in Wave-1 of the 8 possible spatial streams supported in Wave-2

1 stream (80MHz) is 433 Mbps
2 stream (80MHz) is 866 Mbps
3 stream (80MHz) is 1300 Mbps

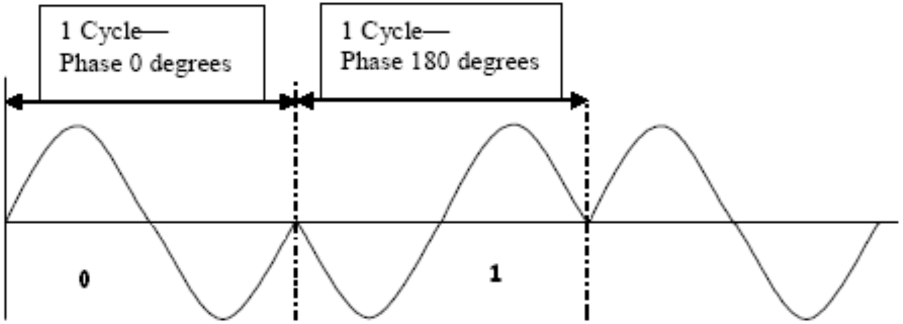


802.11ac Data Rates		• RATE NOT SUPPORTED		Mb/s					
				20 MHz		40 MHz		80 MHz	
				Guard	Interval	Guard	Interval	Guard	Interval
Spatial Streams	MCS Index	Modulation	Coding	800ns	400ns	800ns	400ns	800ns	400ns
2	0	BPSK	1/2	13	14.4	27	30	58.5	65
	1	QPSK	1/2	26	28.9	54	60	117	130
	2	QPSK	3/4	39	43.3	81	90	175.5	195
	3	16-QAM	1/2	52	57.8	108	120	234	260
	4	16-QAM	3/4	78	86.7	162	180	351	390
	5	64-QAM	2/3	104	115.6	216	240	468	520
	6	64-QAM	3/4	117	130	243	270	526.5	585
	7	64-QAM	5/6	130	144.4	270	300	585	650
	8	256-QAM	3/4	156	173.3	324	360	702	780
	9	256-QAM	5/6	•	•	360	400	780	866.7
3	0	BPSK	1/2	19.5	21.7	40.5	45	87.8	97.5
	1	QPSK	1/2	39	43.3	81	90	175.5	195
	2	QPSK	3/4	58.5	65	121.5	135	263.3	292.5
	3	16-QAM	1/2	78	86.7	162	180	351	390
	4	16-QAM	3/4	117	130	243	270	526.5	585
	5	64-QAM	2/3	156	173.3	324	360	702	780
	6	64-QAM	3/4	175.5	195	364.5	405	•	•
	7	64-QAM	5/6	195	216.7	405	450	877.5	975
	8	256-QAM	3/4	234	260	486	540	1053	1170
	9	256-QAM	5/6	260	288.9	540	600	1170	1300

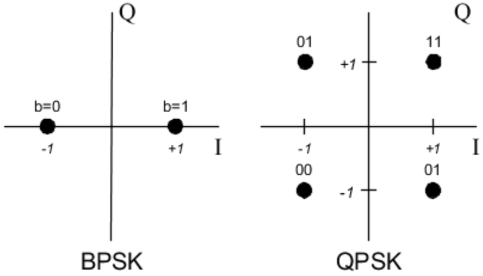
351080

How Bits Get Modulated

BPSK – 1 bit per modulation symbol at 180 degrees phase
2 wave forms (phases)

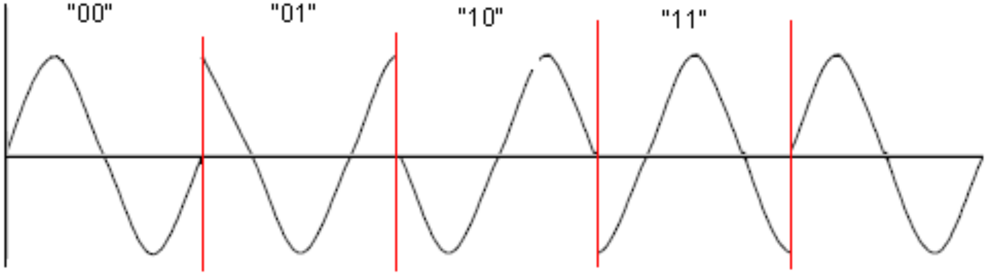


Binary Phase Shift keying

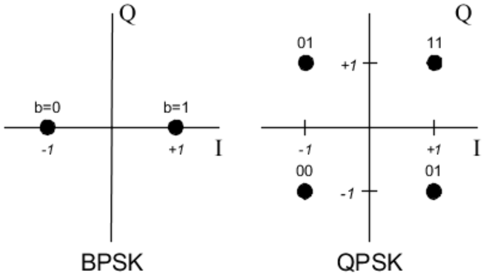


How Bits Get Modulated

QPSK – 2 bits per modulation symbol at 90 degrees phase
4 wave forms (phases)

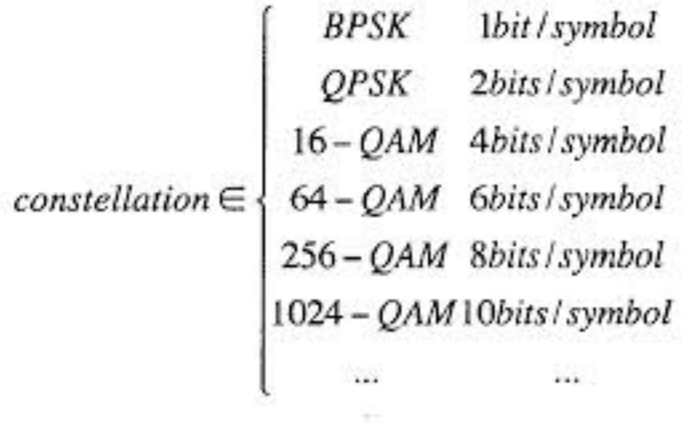


Quadrature Phase Shift keying

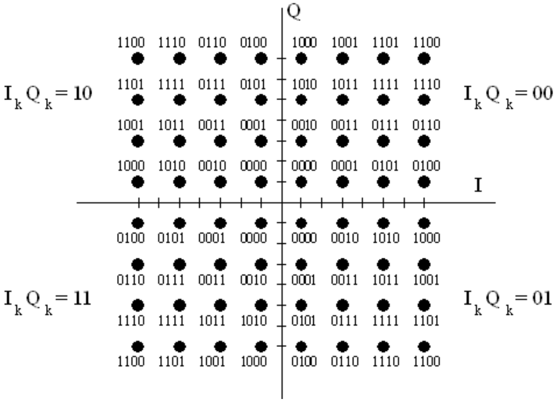


How Bits Get Modulated

QAM64 – 6 bits per symbol / amplitude modulation

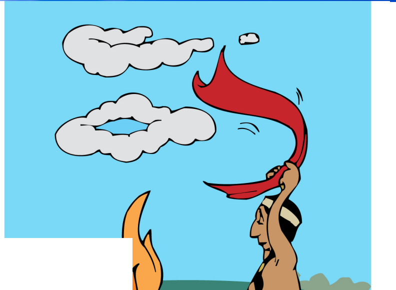


$$constellation \in \begin{cases} BPSK & 1bit/symbol \\ QPSK & 2bits/symbol \\ 16-QAM & 4bits/symbol \\ 64-QAM & 6bits/symbol \\ 256-QAM & 8bits/symbol \\ 1024-QAM & 10bits/symbol \\ \ldots & \ldots \end{cases}$$



1100	1110	0110	0100	1000	1001	1101	1100
1101	1111	0111	0101	1010	1011	1111	1110
1001	1011	0011	0001	0010	0011	0111	0110
1000	1010	0010	0000	0000	0001	0101	0100
0100	0101	0001	0000	0000	0010	1010	1000
0110	0111	0011	0010	0001	0011	1011	1001
1110	1111	1011	1010	0101	0111	1111	1101
1100	1101	1001	1000	0100	0110	1110	1100

How Bits Get Modulated



QAM256 – 8 bits per symbol / amplitude modulation

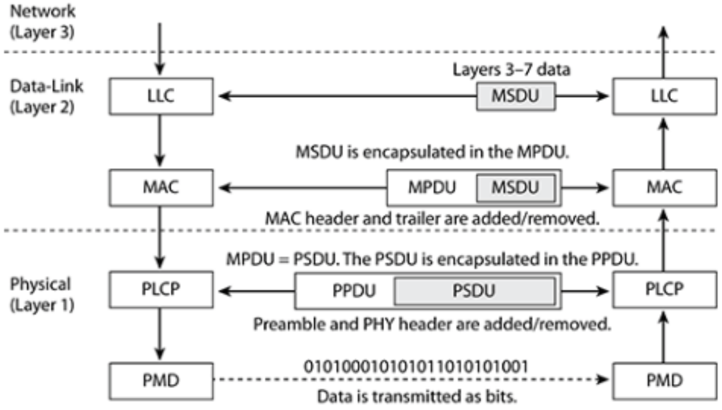
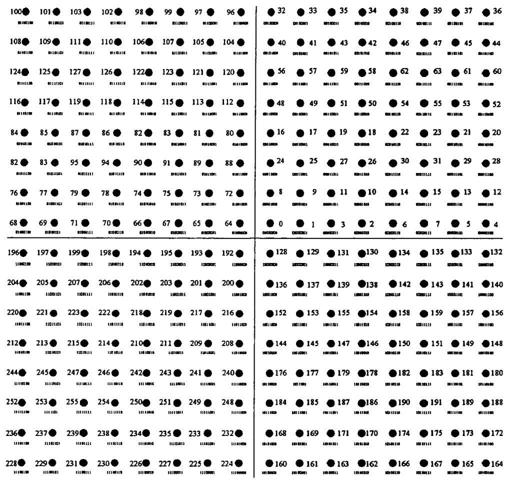
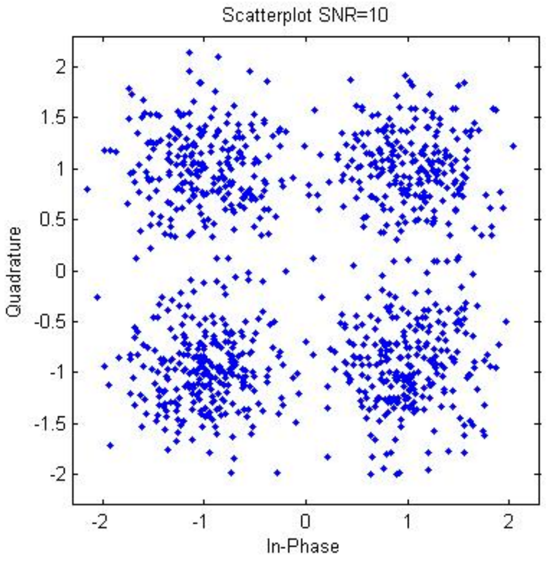
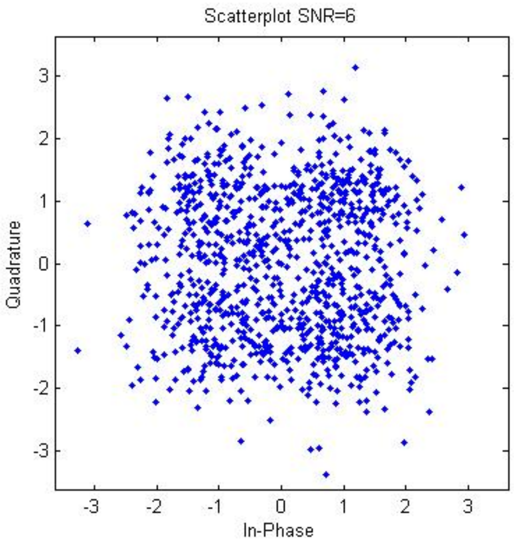

Network
(Layer 3)
Data-Link
(Layer 2)
Physical
(Layer 1)
LLC
LLC
Layers 3–7 data
MSDU
MSDU is encapsulated in the MPDU.
MAC
MAC
MPDU
MSDU
MAC header and trailer are added/removed.
MPDU = PSDU. The PSDU is encapsulated in the PPDU.
PLCP
PLCP
PPDU
PSDU
Preamble and PHY header are added/removed.
PMD
PMD
0101000101010110101010001
Data is transmitted as bits.

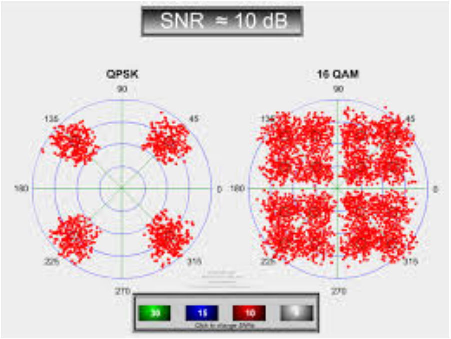
FIG. 4G

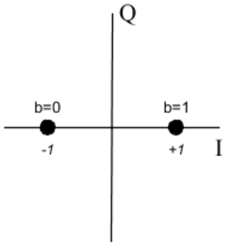


How Bits Get Modulated

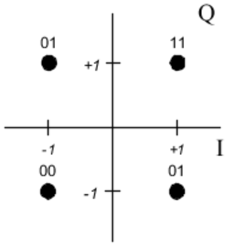






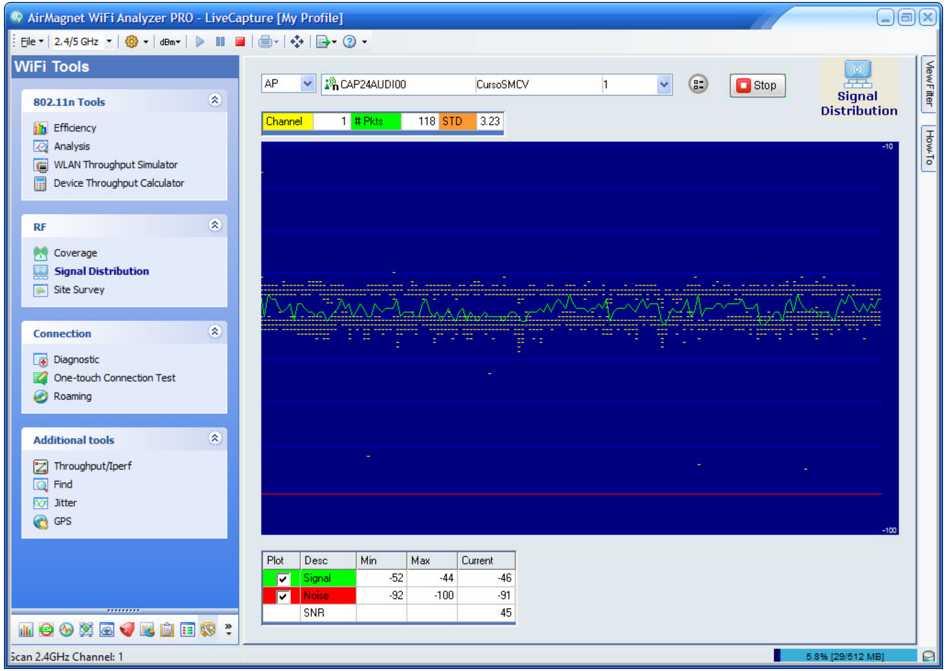


BPSK



QPSK

Have you seen Multipath ?



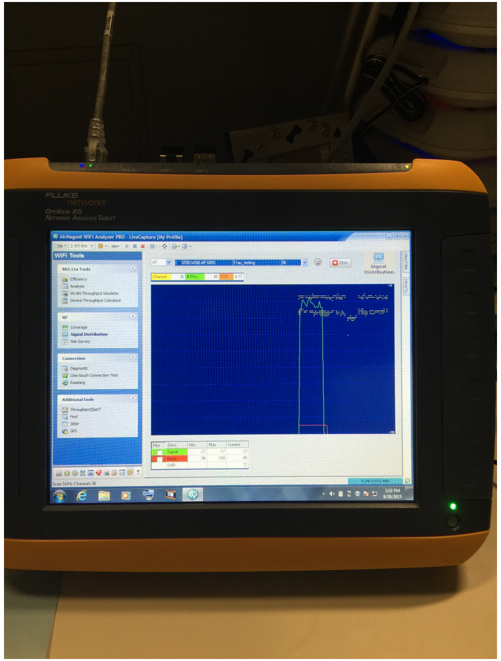
AP | CAP24AUDI00 | CursoSMCV | 1

Channel 1 | # Pkts 118 | STD 3.23

Plot	Desc	Min	Max	Current
☑	Signal	-52	-44	-46
☑	Noise	-92	-100	-91
	SNR			45

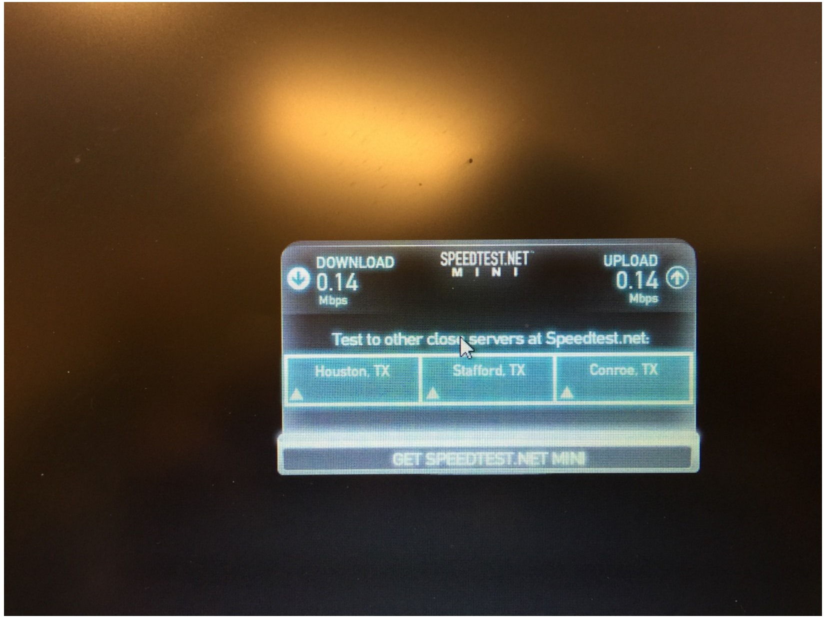
Scan 2.4GHz Channel: 1

5.8% [29/512 MB]



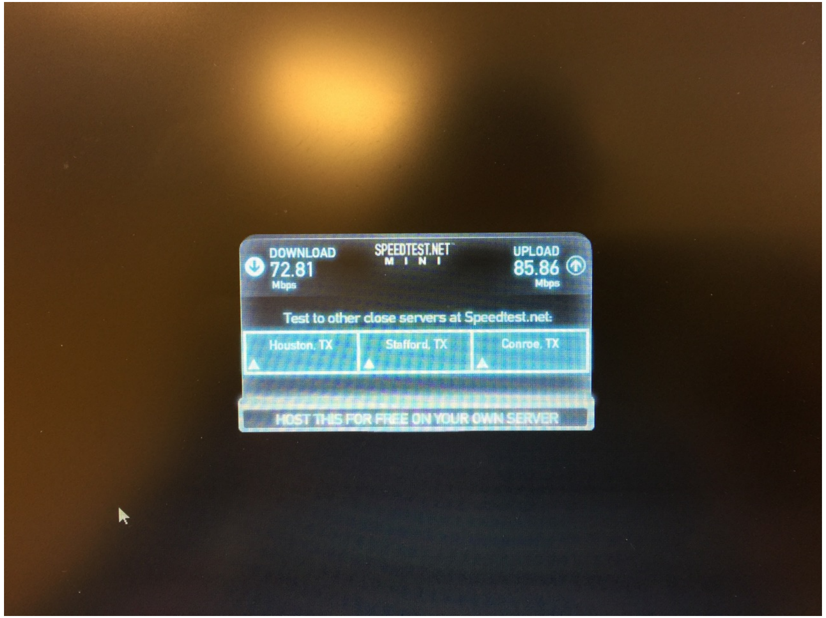
WiFi Clients are 80% of my issues!

Intel U-APSD Issue



DOWNLOAD 0.14 Mbps

UPLOAD 0.14 Mbps

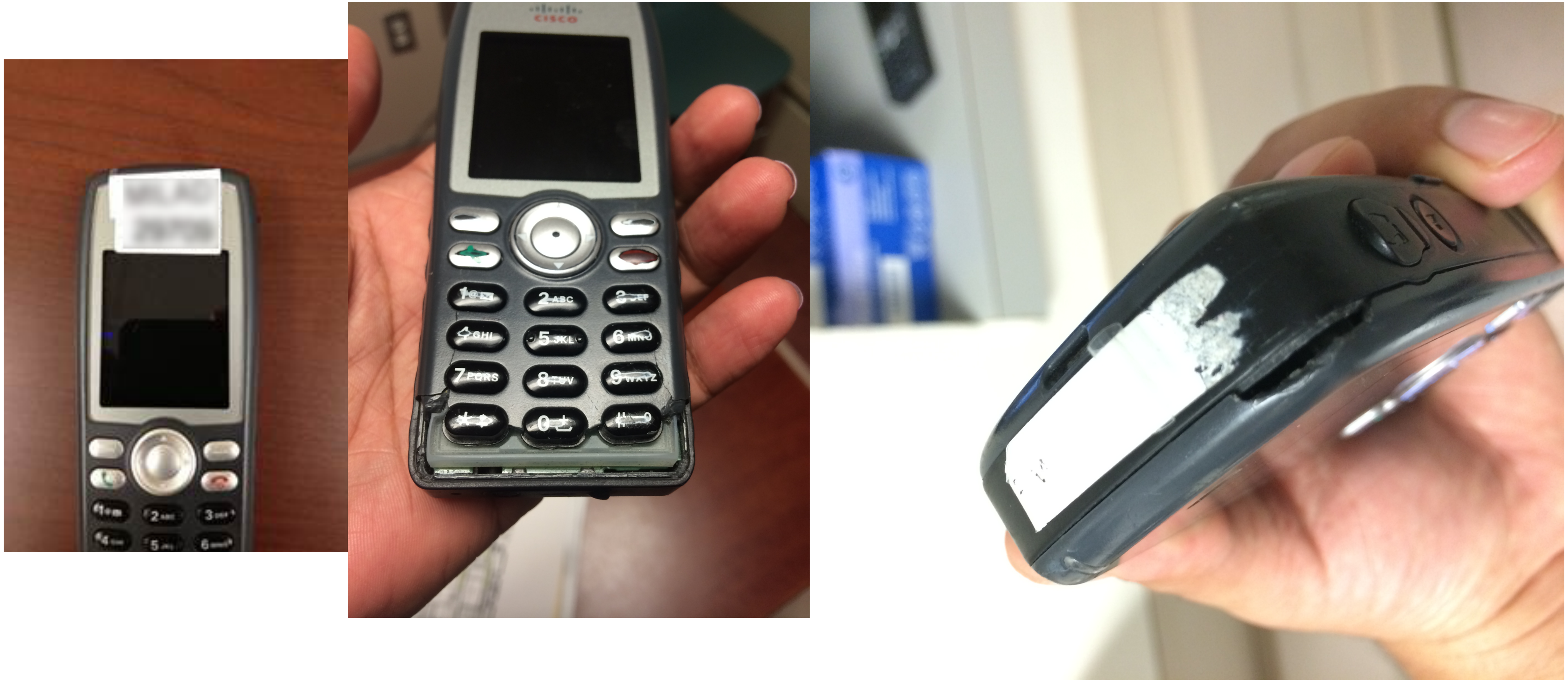


DOWNLOAD 72.81 Mbps

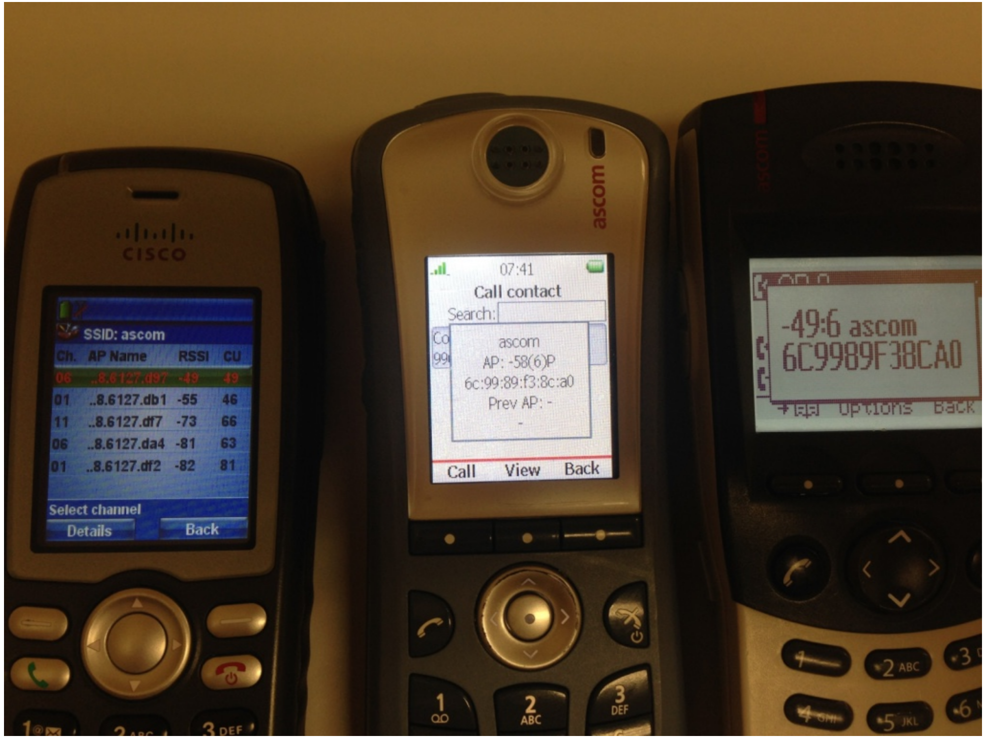
UPLOAD 85.86 Mbps

SPEEDTEST.NET MINI
Test to other close servers at Speedtest.net:
Houston, TX
Stafford, TX
Conroe, TX
HOST THIS FOR FREE ON YOUR OWN SERVER

WiFi Clients are 80% of my issues!



WiFi Clients are 80% of my issues!



SSID: ascom

Ch.	AP Name	RSSI	CU
06	..8.6127.d97	-49	49
01	..8.6127.db1	-55	46
11	..8.6127.df7	-73	66
06	..8.6127.da4	-81	63
01	..8.6127.df2	-82	81

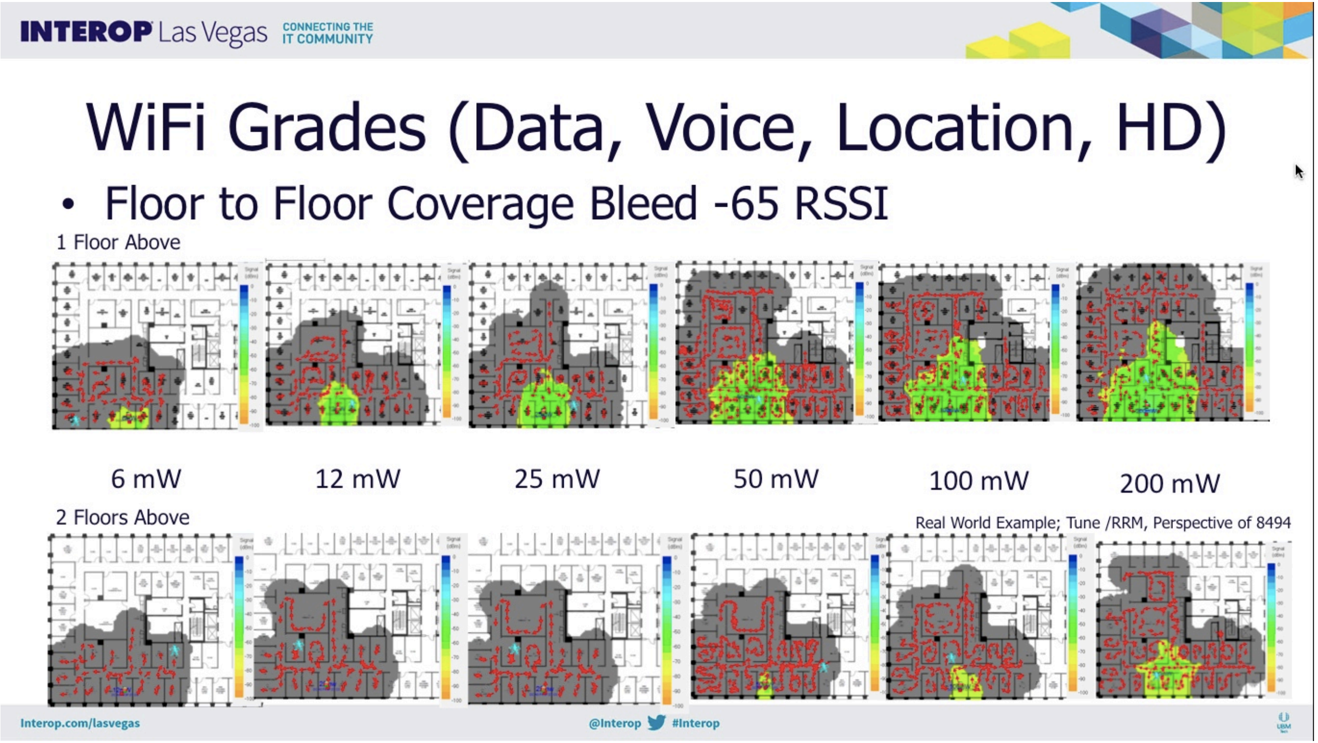
Select channel

07:41
Call contact
Search:

ascom
AP: -58(6)P
6c:99:89:f3:8c:a0
Prev AP: -

-49:6 ascom
6C9989F38CA0

Avoid Excessive TX Power



INTEROP Las Vegas CONNECTING THE IT COMMUNITY

WiFi Grades (Data, Voice, Location, HD)

- Floor to Floor Coverage Bleed -65 RSSI

1 Floor Above

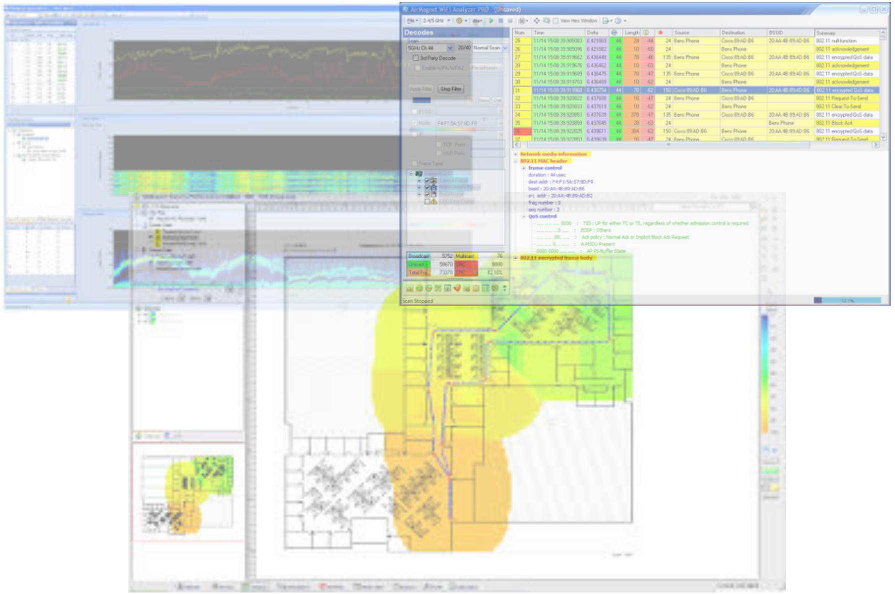
6 mW 12 mW 25 mW 50 mW 100 mW 200 mW

2 Floors Above

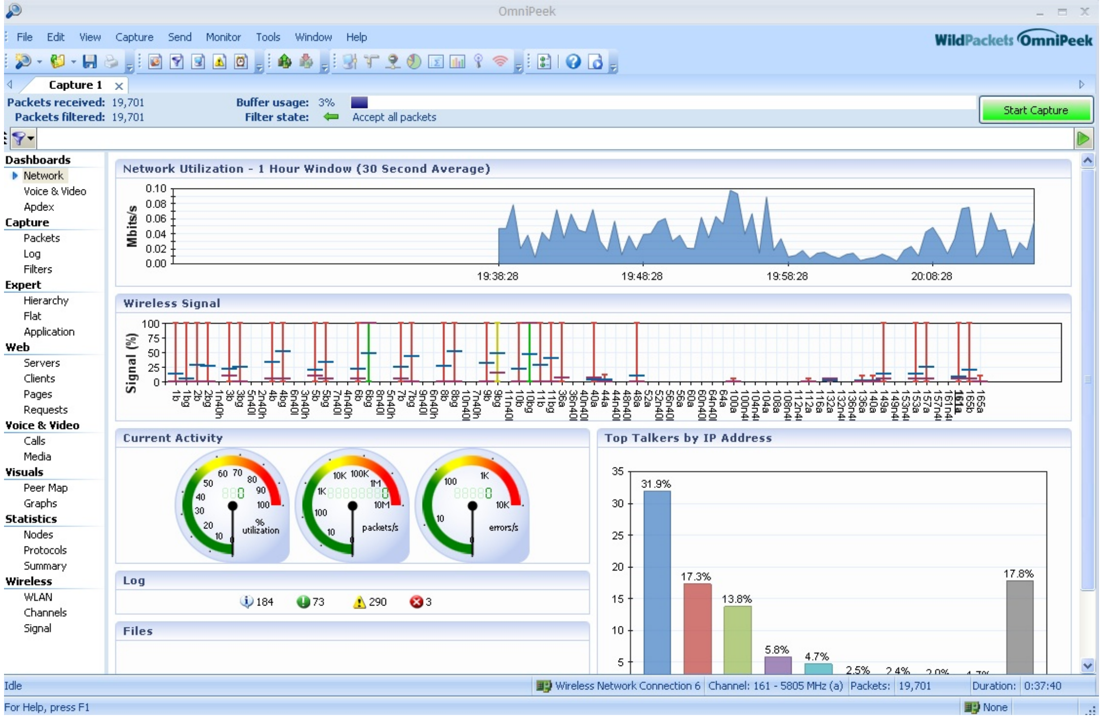
Real World Example; Tune /RRM, Perspective of 8494

Interop.com/lasvegas @Interop #Interop

Tools – Fluke AirMagnet a NetScout Company



Savvius - OmniPeek



Packets received: 19,701

Packets filtered: 19,701

Buffer usage: 3%

Filter state: Accept all packets

Log: 184 73 290 3

Idle

Wireless Network Connection 6 | Channel: 161 - 5805 MHz (a) | Packets: 19,701 | Duration: 0:37:40

For Help, press F1

None

ANZ atmosphere 2015

HOW TOMORROW MOVES

ANZ
atmosphere 2015
HOW TOMORROW MOVES

THANK YOU