802.11 Complexity

An introduction to 802.11 protocol chaos

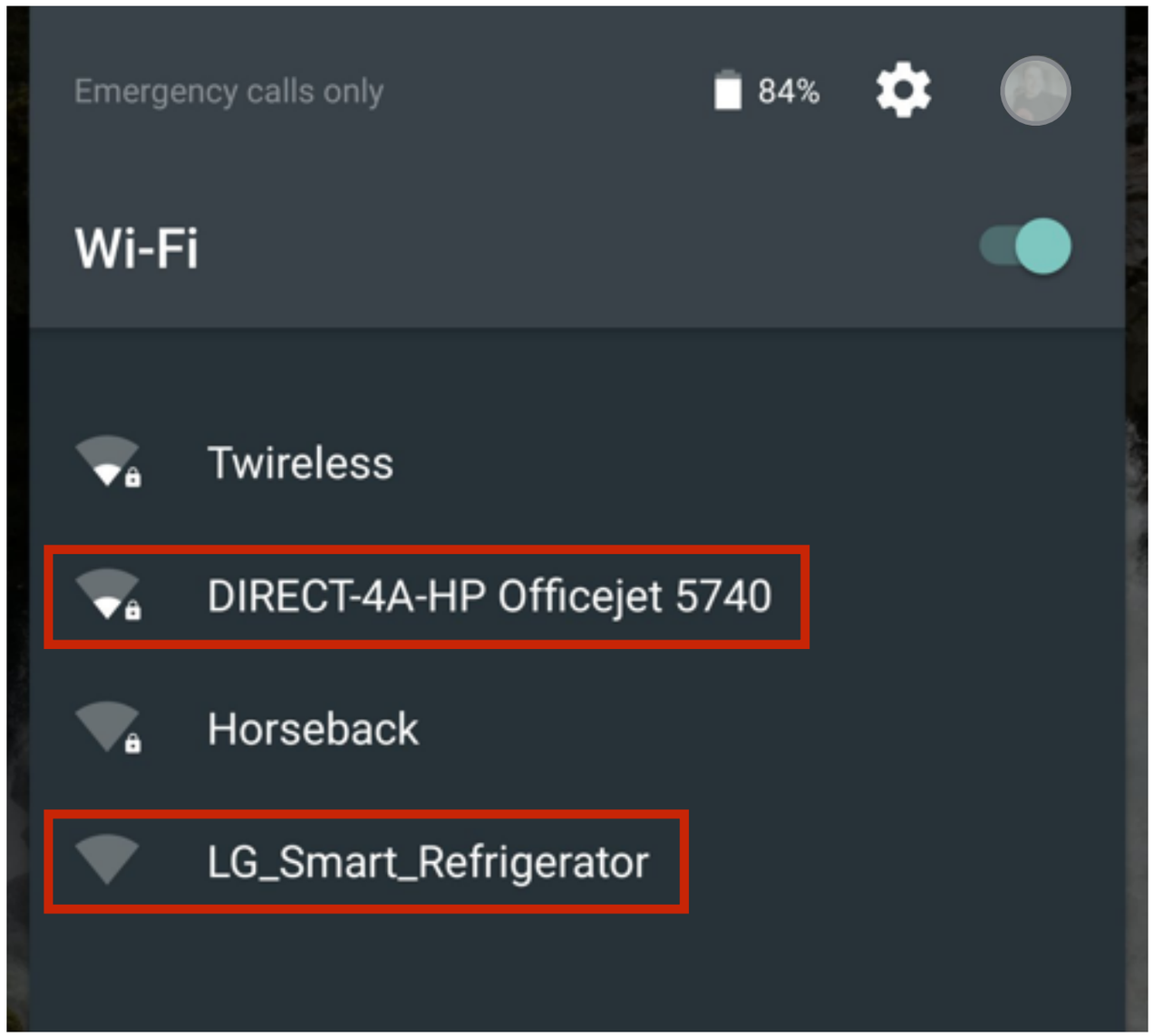
Andrés Blanco

Email: 6e726d@gmail.com

Twitter: @6e726d

DEEPSEC

Motivation



802.11 it’s everywhere

https://twitter.com/skrud/status/767243097331736578

Motivation

Radio frequency has no defined boundaries

Motivation

Modern devices move between networks all the time

Motivation

- IEEE 802.11-1997
- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11c
- IEEE 802.11d
- IEEE 802.11e
- IEEE 802.11F
- IEEE 802.11g
- IEEE 802.11h
- IEEE 802.11i
- IEEE 802.11j
- IEEE 802.11k
- IEEE 802.11n
- IEEE 802.11p
- IEEE 802.11r
- IEEE 802.11s
- IEEE 802.11T
- IEEE 802.11u
- IEEE 802.11v
- IEEE 802.11w
- IEEE 802.11y
- IEEE 802.11z
- IEEE 802.11-2012
- IEEE 802.11aa
- IEEE 802.11ac
- IEEE 802.11ad
- IEEE 802.11ae
- IEEE 802.11af
- IEEE 802.11mc
- IEEE 802.11ah
- IEEE 802.11ai
- IEEE 802.11aj
- …

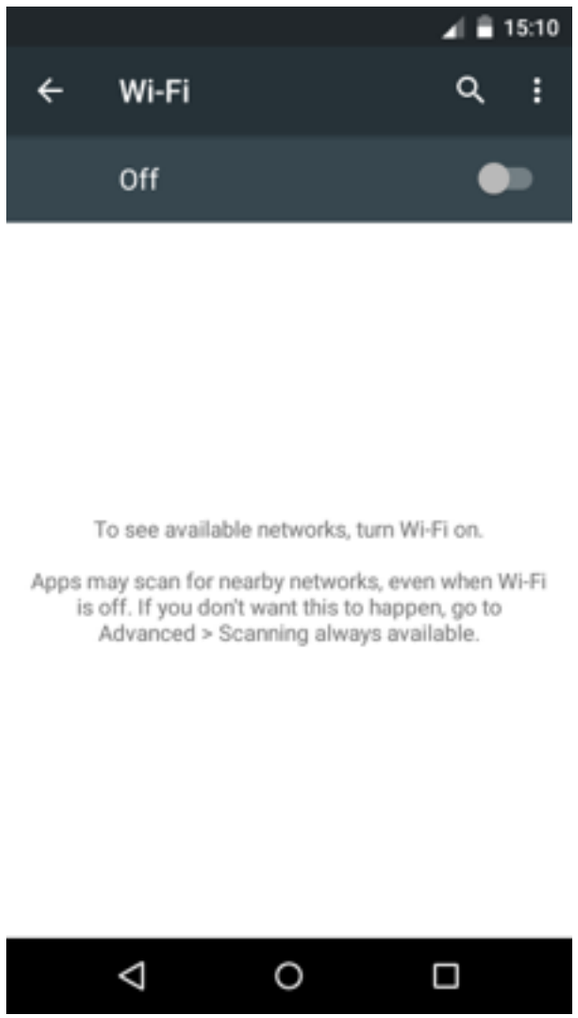
802.11 protocol is growing and constantly changing

Motivation

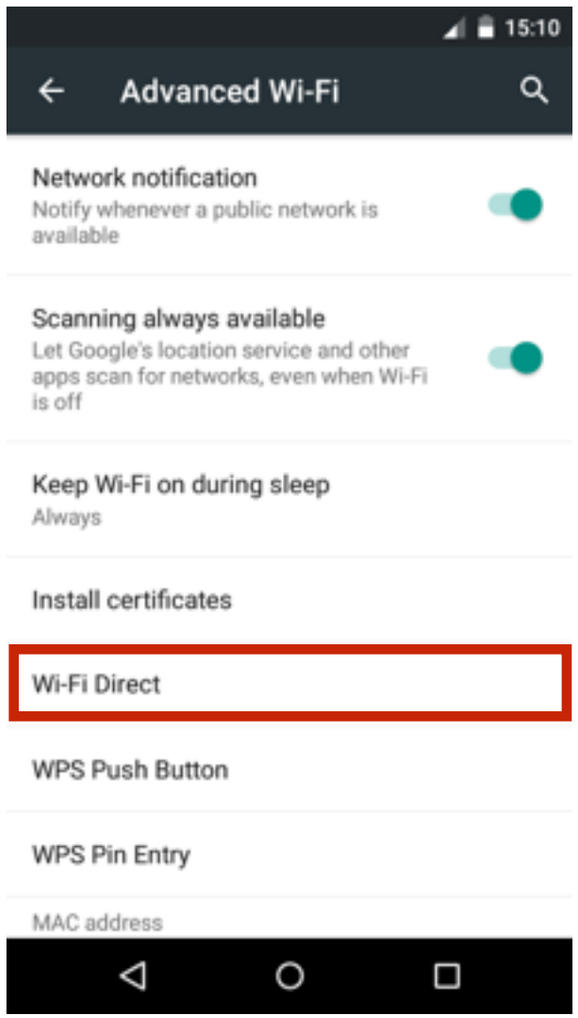
802.11 is growing and constantly changing

Motivation

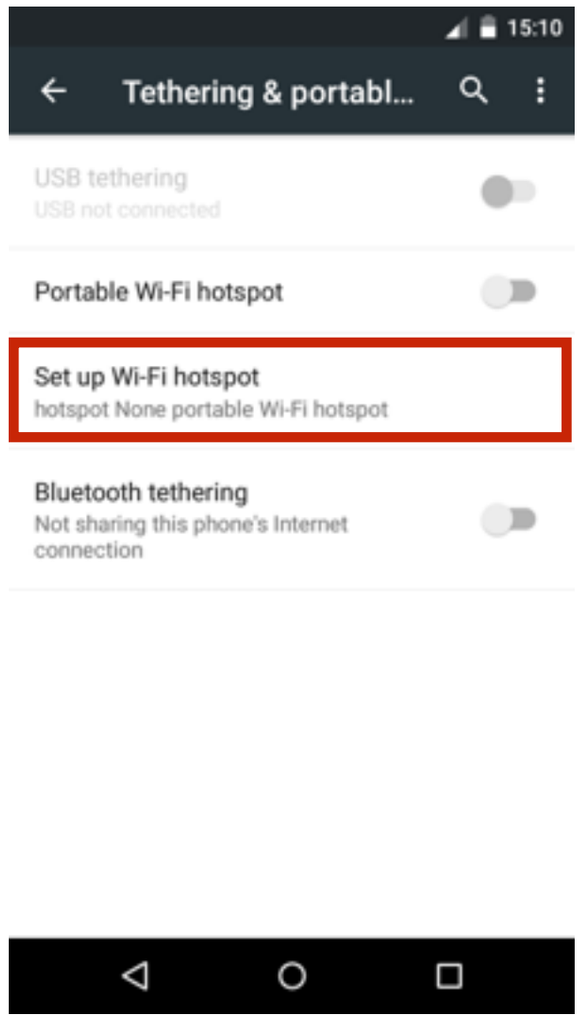
Managed



P2P



Master



Wireless NICs usually support more than one mode

Protocol Complexity

Management

- Association Request
- Association Response
- Reassociation Request
- Reassociation Response
- Probe Request
- Probe Response
- Beacon
- ATIM
- Disassociation
- Authentication
- Deauthentication
- Action

Control

- Block ACK Request
- Block ACK
- PS-Poll
- RTS
- CTS
- ACK
- CF-End
- CF-End+CF-ACK

Data

- Data
- Data+CF-ACK
- Data+CF-Poll
- Data+CF-ACK+CF-Poll
- Null
- CF-ACK
- CF-Poll
- CF-ACK+CF-Poll
- QoS data
- QoS data+CF-ACK
- QoS data+CF-Poll
- QoS data+CF-ACK+CF-Poll
- QoS Null
- QoS+CF-Poll
- QoS+CF-ACK

802.11 frame types and subtypes

Protocol Complexity

Management

- Association Request
- Association Response
- Reassociation Request
- Reassociation Response
- Probe Request
- Probe Response
- Beacon
- ATIM
- Disassociation
- Authentication
- Deauthentication
- Action

Control

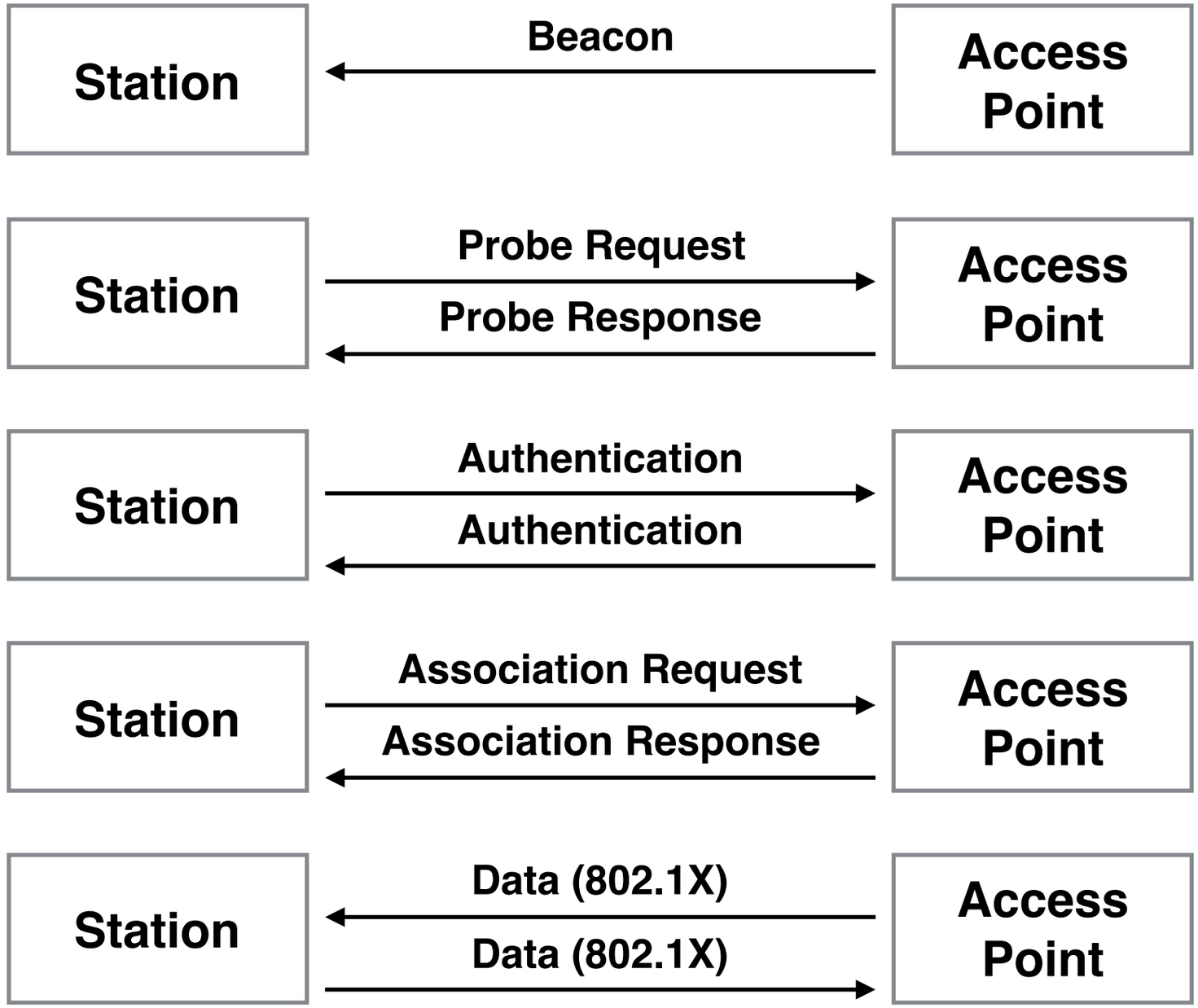
- Block ACK Request
- Block ACK
- PS-Poll
- RTS
- CTS
- ACK
- CF-End
- CF-End+CF-ACK

Data

- Data
- Data+CF-ACK
- Data+CF-Poll
- Data+CF-ACK+CF-Poll
- Null
- CF-ACK
- CF-Poll
- CF-ACK+CF-Poll
- QoS data
- QoS data+CF-ACK
- QoS data+CF-Poll
- QoS data+CF-ACK+CF-Poll
- QoS Null
- QoS+CF-Poll
- QoS+CF-ACK

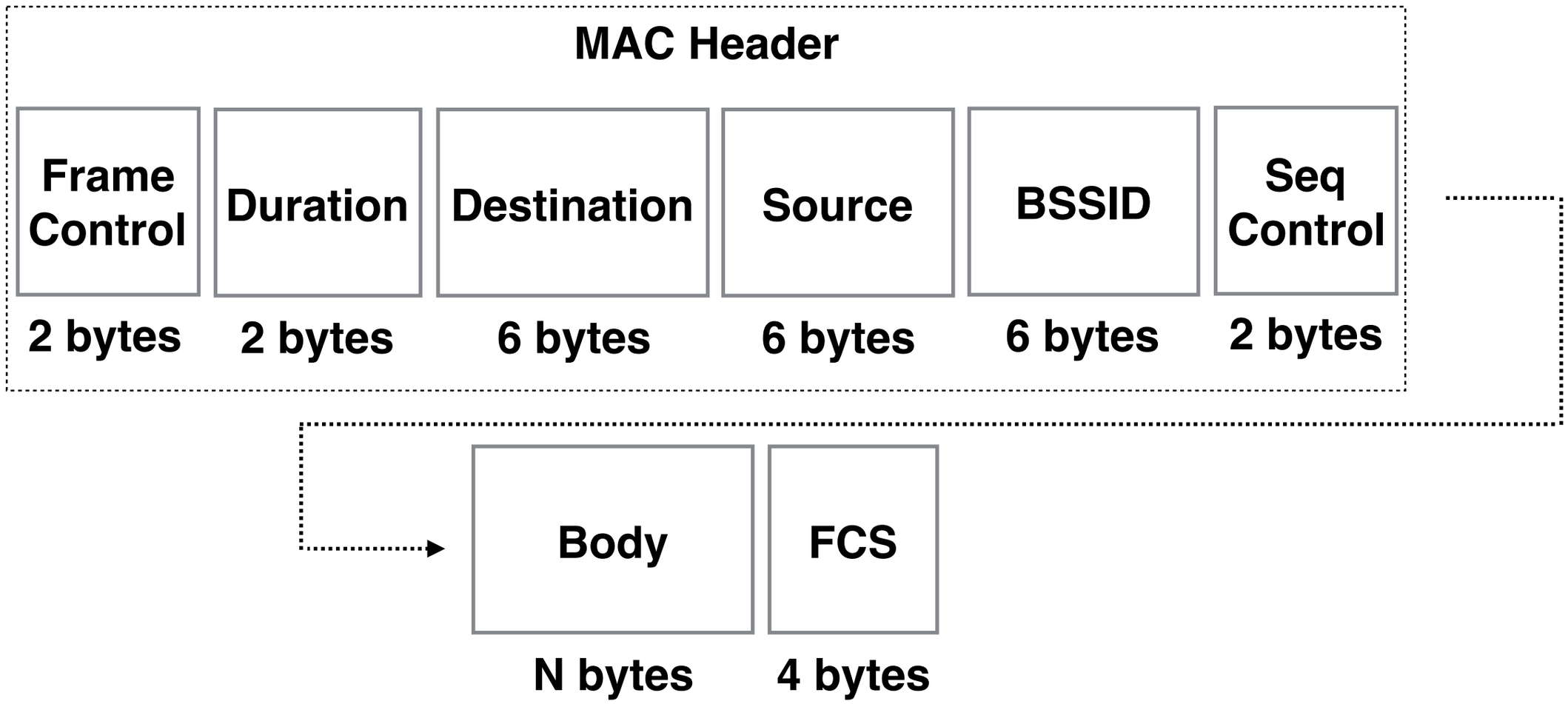
802.11 frame types and subtypes

Protocol Complexity



802.11 Association process

Protocol Complexity



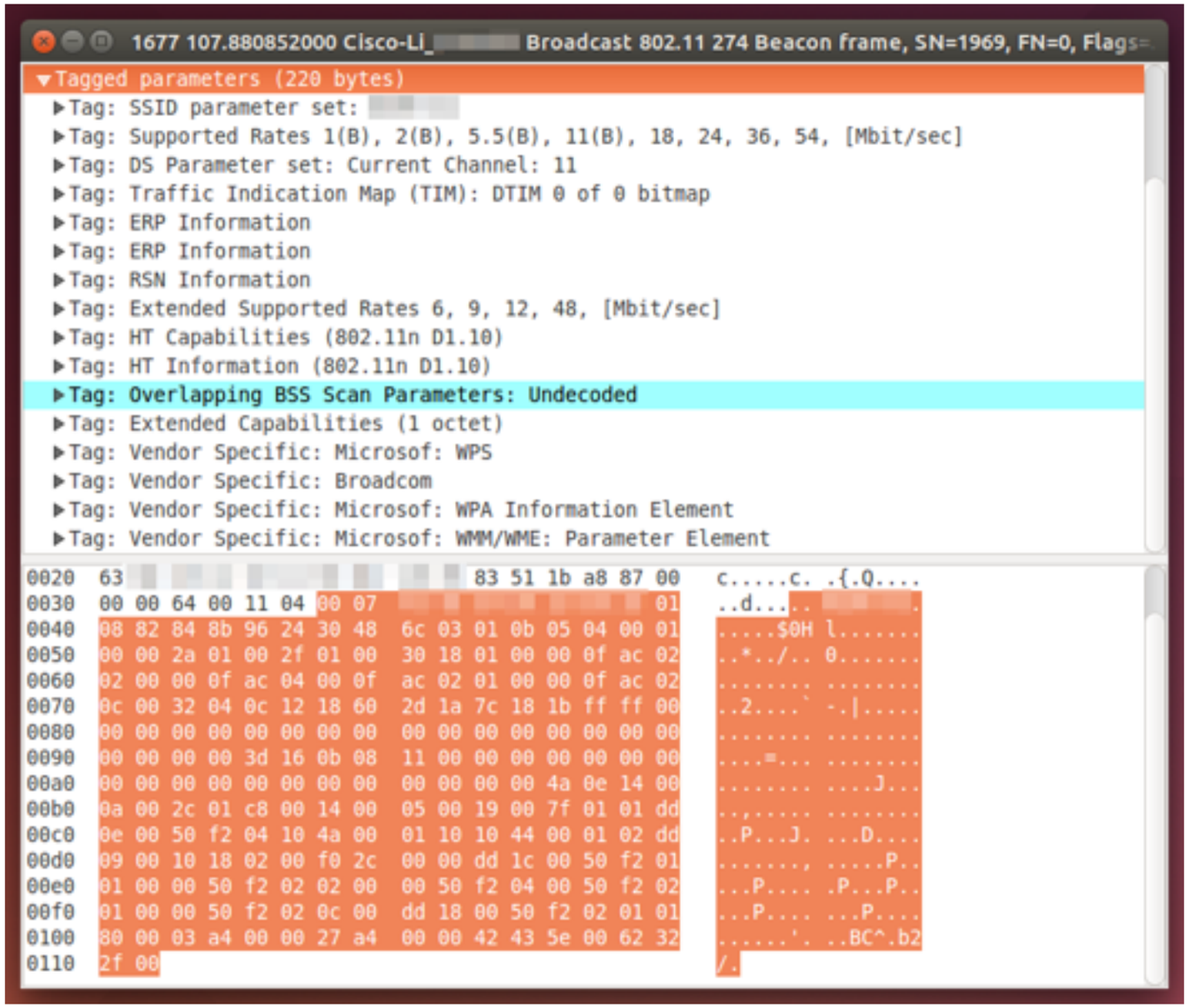
Management frame structure

Protocol Complexity

Type	Length	Value
1 byte	1 byte	N bytes

Information elements are variable-length components

Protocol Complexity



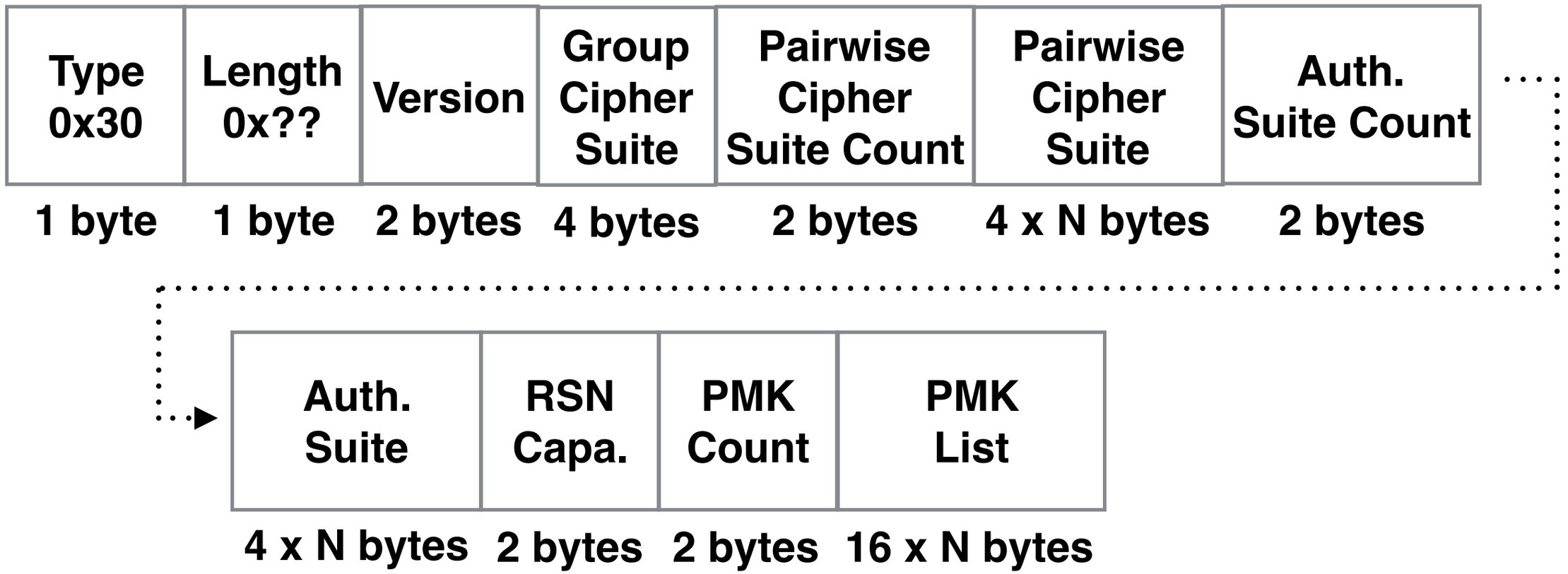
Information Elements on a beacon frame

Protocol Complexity

Type 0x00	Length 0x??	Value SSID
1 byte	1 byte	N bytes

SSID information element

Protocol Complexity



RSN information element

Protocol Complexity

Length Nonsense

39 5.659444 e0:cb:4e:[redacted] 94:71:ac:[redacted] 802.11 127 Probe Response, SN=2770, FN=0, Flag

```
▼Tag: Vendor Specific: 00:50:f2: WPA Information Element
   Tag Number: Vendor Specific (221)
   Tag length: 24
   OUI: 00-50-f2
   Vendor Specific OUI Type: 1
   Type: WPA Information Element (0x01)
   WPA Version: 1
 ▼Multicast Cipher Suite: 00-50-f2 TKIP
    Multicast Cipher Suite OUI: 00-50-f2
    Multicast Cipher Suite type: TKIP (2)
   Unicast Cipher Suite Count: 1
 ▶Unicast Cipher Suite List 00-50-f2 TKIP
   Auth Key Management (AKM) Suite Count: 1
 ▶Auth Key Management (AKM) List 00-50-f2 PSK
```

```
0000  00 00 12 00 2e 48 00 00  00 02 9e 09 a0 00 a7 01   .....H.. ........
0010  00 00 50 00 3a 01 94 71  ac [redacted] e0 cb 4e [redacted]   ..P.:..q .v.h..N`
0020  [redacted] e0 cb 4e [redacted] 20 ad 12 95 d1 c7 11 00   ....N`..  .......
0030  00 00 64 00 31 04 00 0c  46 69 62 65 72 74 65 6c   ..d.1... Fibertel
0040  20 36 33 39 01 08 82 84  8b 96 24 30 48 6c 03 01    639.... ..$0Hl..
0050  0b 2a 01 02 2f 01 02 32  04 0c 12 18 60 dd 06 00   .*../..2 ....`...
0060  10 18 02 02 00 dd 18 00  50 f2 01 01 00 00 50 f2   ........ P.....P.
0070  02 01 00 00 50 f2 02 01  00 00 50 f2 02 00 00      ....P... ..P....
```

CVE-2012-2619 affected at least 15 different vendors

Protocol Complexity

Too much information

Protocol Complexity

Too much information

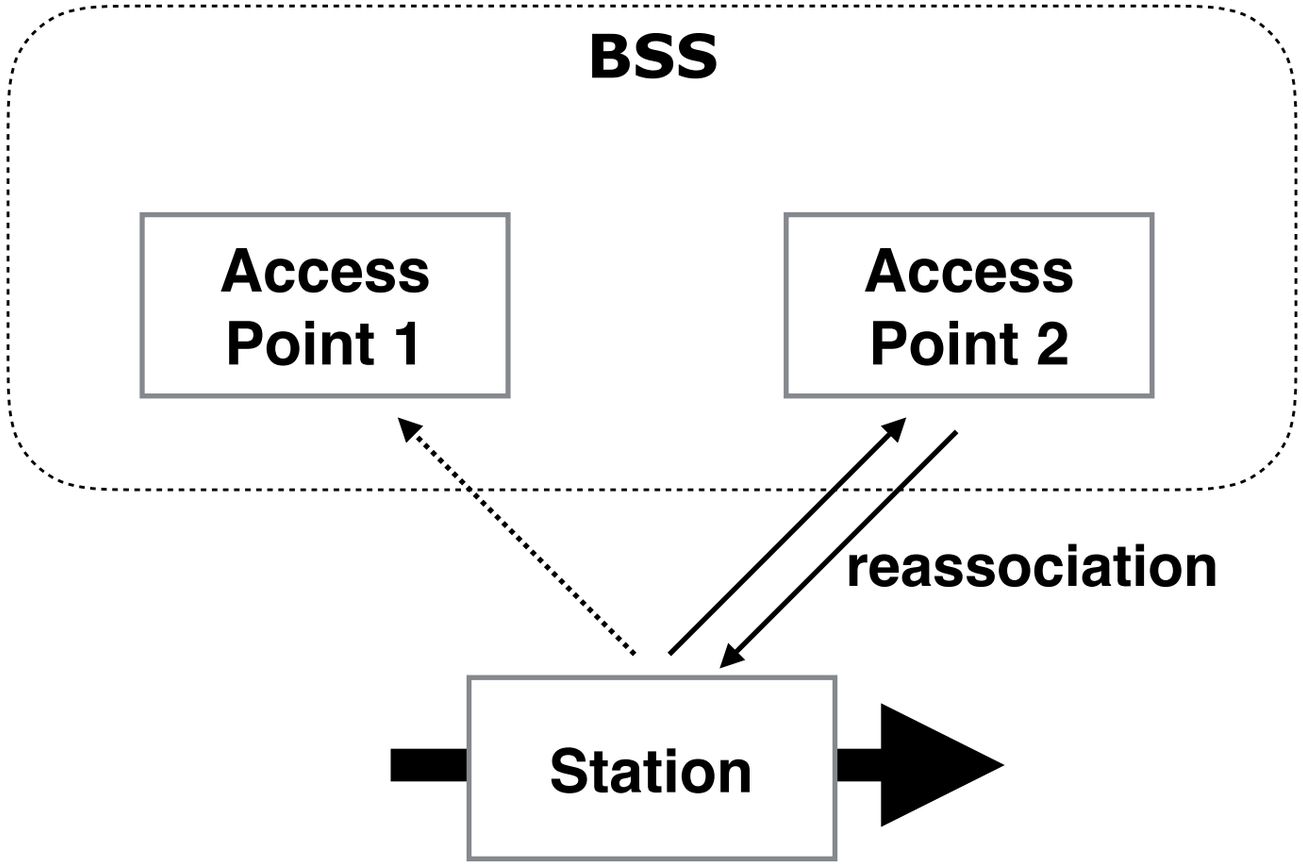
If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

CCX Cisco documentation

www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01011101.html

Protocol Complexity

Too much information



802.11 roaming

Protocol Complexity

Too much information

6440 115.444978 Cisco_[redacted] Broadcast 802.11 253 Beacon frame, SN=2769, FN=0, Flags=.....

```
▼Tagged parameters (217 bytes)
  ▶Tag: SSID parameter set: Broadcast
  ▶Tag: Supported Rates 36(B), 48, 54, [Mbit/sec]
  ▶Tag: DS Parameter set: Current Channel: 11
  ▶Tag: Traffic Indication Map (TIM): DTIM 0 of 4 bitmap
  ▶Tag: Country Information: Country Code US, Environment Any
  ▶Tag: QBSS Load Element 802.11e CCA Version
  ▶Tag: ERP Information
  ▶Tag: HT Capabilities (802.11n D1.10)
  ▶Tag: RSN Information
  ▶Tag: HT Information (802.11n D1.10)
  ▼Tag: Cisco CCX1 CKIP + Device Name
    Tag Number: Cisco CCX1 CKIP + Device Name (133)
    Tag length: 30
    Unknown: 07008f000f00ff035900
    Name: B67[redacted] AP
    Clients: 17
    Unknown2: 00003c
```

```
0000  80 00 00 00 ff ff ff ff  ff ff 70 10 5c [redacted]   ........ ..p.\..@
0010  70 10 5c [redacted] 10 ad  e6 6a c4 24 10 05 00 00   p.\..@.. .j.$....
0020  66 00 31 14 00 01 00 01  03 c8 60 6c 03 01 0b 05   f.1..... ..`l....
0030  07 00 01 04 08 00 00 00  07 06 55 53 20 01 0b 1e   ........ ..US ...
0040  0b 05 11 00 9c 8d 5b 2a  01 00 2d 1a ac 19 1b ff   ......[* ..-.....
0050  ff ff 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 30 14  01 00 00 0f ac 04 01 00   ......0. ........
0070  00 0f ac 04 01 00 00 0f  ac 01 28 00 3d 16 0b 00   ........ ..(.=...
0080  05 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Access Point name and number of associated clients

Protocol Complexity

Too much information

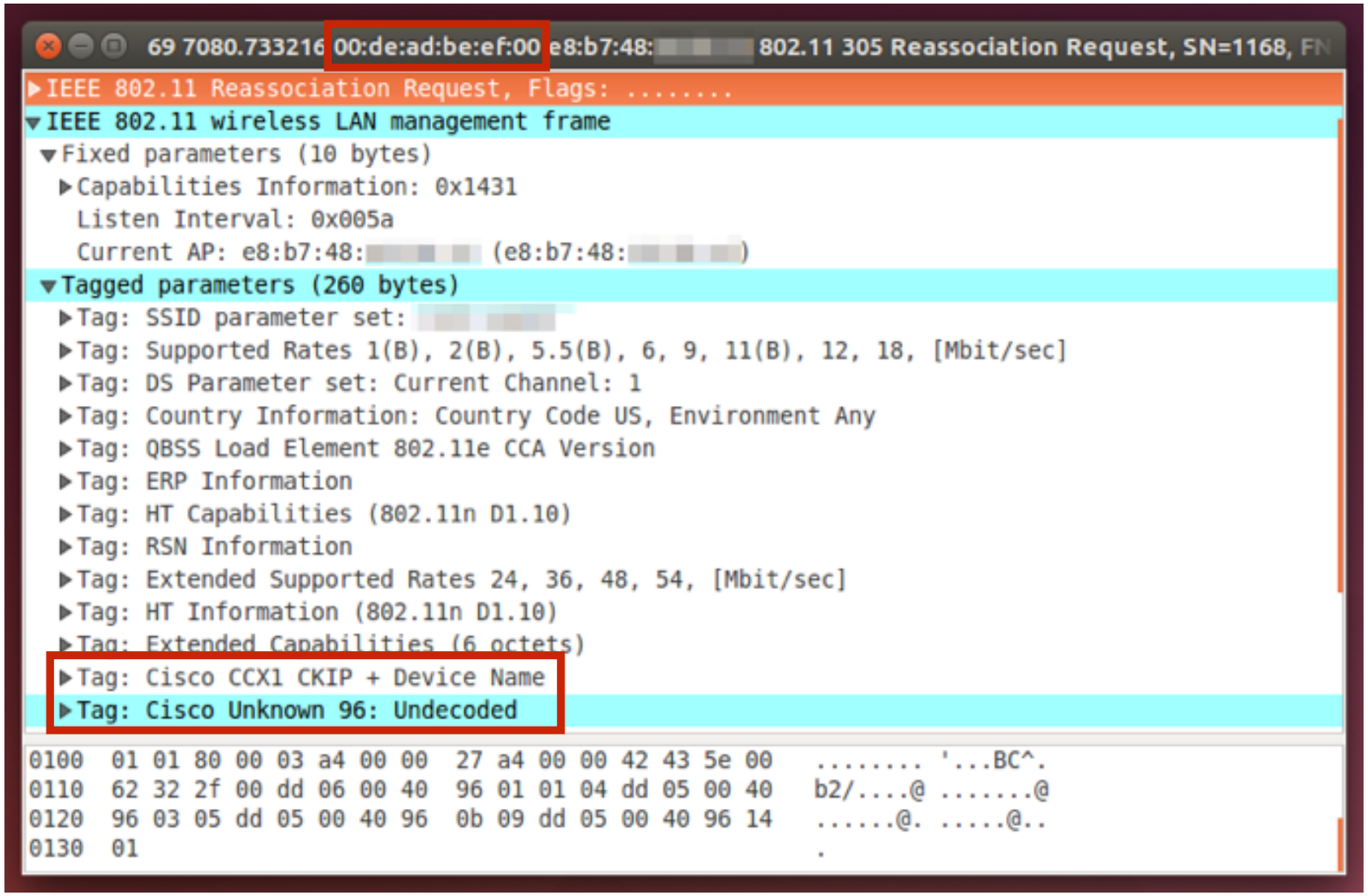
```
10458 134.577591 Cisco_      IntelCor_      802.11 173 Reassociation Response, SN=142,
  ▶Tag: HT Information (802.11n D1.10)
  ▼Tag: Cisco CCX1 CKIP + Device Name
    Tag Number: Cisco CCX1 CKIP + Device Name (133)
    Tag length: 30
    Unknown: 00008f0a0f00ff034000
    Name: B67      AP
    Clients: 0
    Unknown2: 00003c
  ▼Tag: Cisco Unknown 95: Undecoded
    ▶Tag Number: Cisco Unknown 95 (149)
    Tag length: 10
    Tag Data: 004096000a0f    0000

0030  1b ff ff ff 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 00  3d 16 0b 00 05 00 00 00   ........ =.......
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  85 1e 00 00 8f 0a 0f 00  ff 03 40 00 42 36 37 ..   ........ ..@.B67.
0070  ..... ..... ..... ..... 41 50 00 00 00 00 3c      ..... ..... AP....<
0080  95 0a 00 40 96 00 0a 0f  ..... 00 00 dd 05 00 40   ...@.... .....   ...@
0090  96 03 05 dd 18 00 50 f2  02 01 01 80 00 03 a4 00   ......P. ........
00a0  00 27 a4 00 00 42 43 5e  00 62 32 2f 00           .'...BC^ .b2/.
```

Wireless LAN Controller IP Address

Protocol Complexity

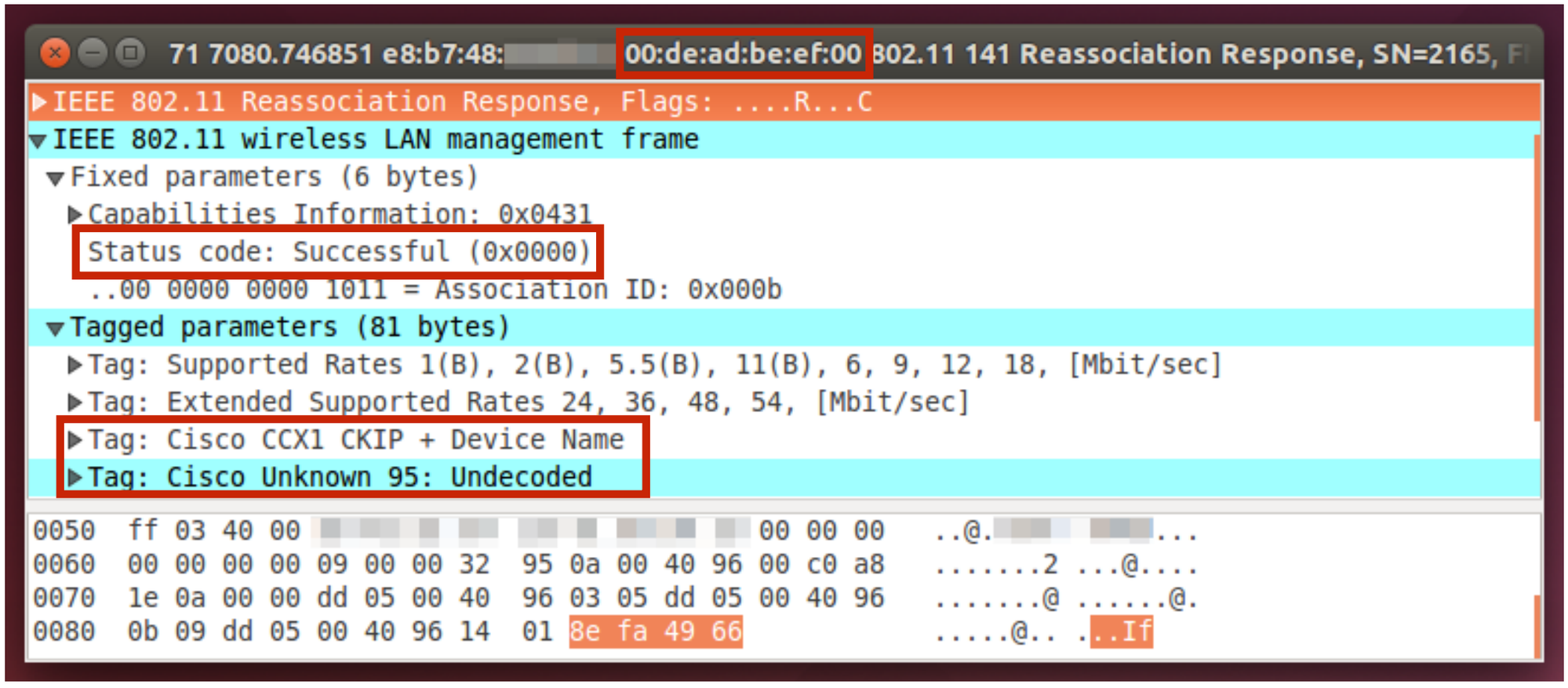
Too much information



Fake reassociation request frame

Protocol Complexity

Too much information



Reassociation response frame

Protocol Complexity

Too much information

Protocol Complexity

Too much information

Wi-Fi Protected Setup™ is an optional certification program based on technology designed to ease the setup of security-enabled Wi-Fi® networks in home and small office environments. Wi-Fi Protected Setup supports methods (pushing a button, entering a PIN, or using NFC) that are familiar to most consumers to configure a network and enable security.

http://www.wi-fi.org/discover-wi-fi/wi-fi-protected-setup

Protocol Complexity

Too much information

153614 1713.279543 Netgear_ 00:61:71: 802.11 397 Probe Response, SN=1865, FN=0, Flags=....., BI=10

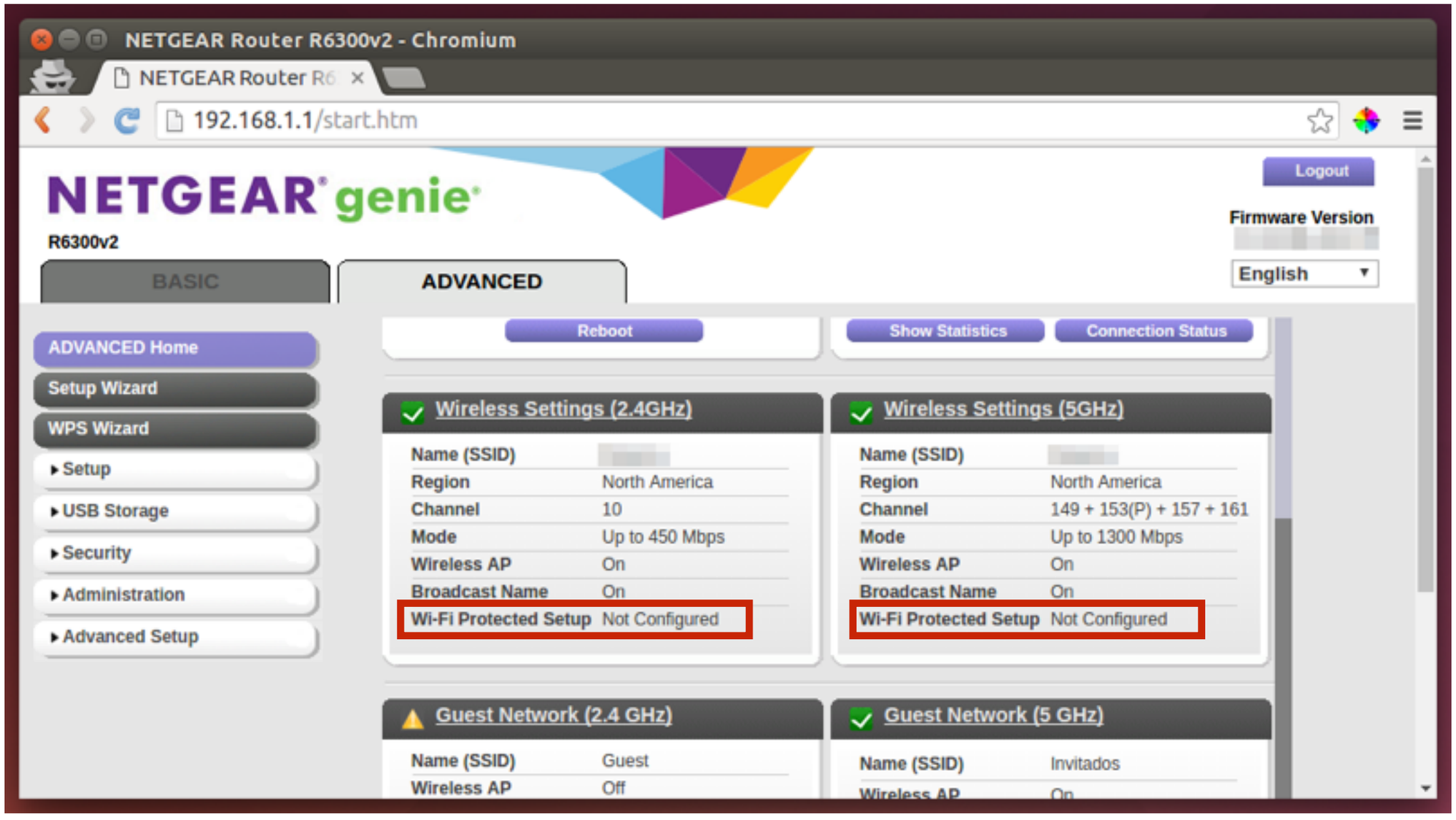
```
  ▶Manufacturer: NETGEAR, Inc.
  ▶Model Name: WGR614v10
  ▶Model Number: WGR614v10
  ▶Serial Number: 83258
  ▶Primary Device Type
  ▶Device Name: WGR614v10
  ▶Config Methods: 0x0084
 ▶Tag: Vendor Specific: Broadcom
```

```
0000  50 00 3a 01 00 61 71 __ __ __ a0 21 b7 __ __ __   P.:..aq. u..!.a.8
0010  a0 21 b7 __ __ __ 90 74  bf 1f 55 9c 00 00 00 00   .!.a.8.t ..U.....
0020  64 00 11 04 00 0f __ __ __ __ __ __ 70 6f 6b 65   d.....  ....poke
0030  72 72 6f 6f 6d 01 08 82  84 8b 96 24 30 48 6c 03   rroom... ...$0Hl.
0040  01 08 2a 01 04 2f 01 04  30 14 01 00 00 0f ac 04   ..*../.. 0.......
0050  01 00 00 0f ac 04 01 00  00 0f ac 02 0c 00 32 04   ........ ......2.
0060  0c 12 18 60 2d 1a 6c 18  1b ff 00 00 00 00 00 00   ...`-.l. ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  3d 16 08 08 04 00 00 00  00 00 00 00 00 00 00 00   =....... ........
0090  00 00 00 00 00 00 00 00  4a 0e 14 00 0a 00 2c 01   ........ J.....,.
00a0  c8 00 14 00 05 00 19 00  7f 01 01 dd 7f 00 50 f2   ........ ......P.
00b0  04 10 4a 00 01 10 10 44  00 01 02 10 41 00 01 00   ..J....D ....A...
00c0  10 3b 00 01 03 10 47 00  10 4f 7e e6 6d a0 12 ee   .;....G. .O~.m...
00d0  42 83 ed e1 b7 8a 20 ad  bc 10 21 00 0d 4e 45 54   B..... . ..!..NET
00e0  47 45 41 52 2c 20 49 6e  63 2e 10 23 00 09 57 47   GEAR, In c..#..WG
00f0  52 36 31 34 76 31 30 10  24 00 09 57 47 52 36 31   R614v10. $..WGR61
0100  34 76 31 30 10 42 00 05  38 33 32 35 38 10 54 00   4v10.B.. 83258.T.
0110  08 00 06 00 50 f2 04 00  01 10 11 00 09 57 47 52   ....P... .....WGR
0120  36 31 34 76 31 30 10 08  00 02 00 84 dd 09 00 10   614v10.. ........
0130  18 02 06 f0 05 00 00 dd  18 00 50 f2 02 01 01 80   ........ ..P.....
0140  00 03 a4 00 00 27 a4 00  00 42 43 5e 00 62 32 2f   .....'.. .BC^.b2/
0150  00 dd 1e 00 90 4c 33 6c  18 1b ff 00 00 00 00 00   .....L3l ........
0160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0170  00 dd 1a 00 90 4c 34 08  08 04 00 00 00 00 00 00   .....L4. ........
0180  00 00 00 00 00 00 00 00  00 00 00 00 00           ........ .....
```

Probe Response with WPS information element

Protocol Complexity

Too much information



Disabling WPS can protect a device from some know attacks

Protocol Complexity

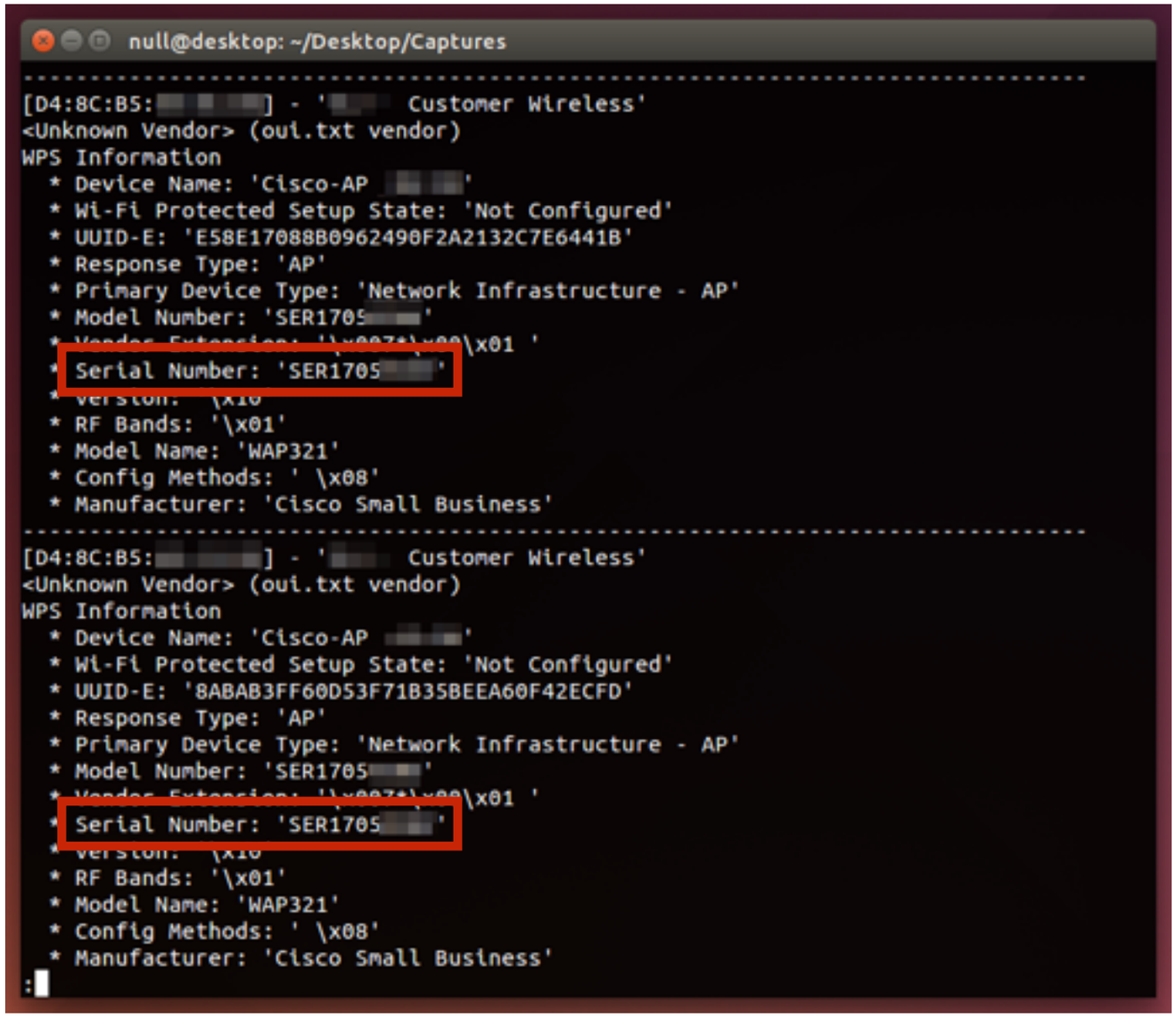
Too much information

```
root@desktop: ~/Desktop/wig
------------------------------------------------------------------------
BSSID: c4:04:15:[redacted]
SSID: [redacted]
--------------------
device name: 'R6300v2'
primary device type: 'Network Infrastructure'
response type: '\x03'
vendor extension: '\x007*\x00\x01 '
model number: 'R6300v2'
ap setup locked: '\x01'
serial number: '679'
version: '1.0'
rf bands: '\x03'
model name: 'R6300v2'
wifi protected setup state: 'Not-Configured'
config methods: 'Display'
uuid e: 'A479F20D63EDA69A99568F8199D39254'
manufacturer: 'NETGEAR, Inc.'
------------------------------------------------------------------------
BSSID: a0:e4:cb:[redacted]
SSID: [redacted]
--------------------
device name: 'VMG1312-B10B'
primary device type: 'Network Infrastructure'
```

Even disabling WPS doesn't disable completely

Protocol Complexity

Too much information



WPS serial numbers

Protocol Complexity

Too much information

Wi-Fi Direct, initially called Wi-Fi P2P, is a Wi-Fi standard enabling devices to easily connect with each other without requiring a wireless access point.

https://en.wikipedia.org/wiki/Wi-Fi_Direct

Protocol Complexity

Too much information

76656 2179.903890000 02:90:a9:[redacted] Motorola_[redacted] 802.11 296 Probe Response, SN=1359, FN=0, Flag

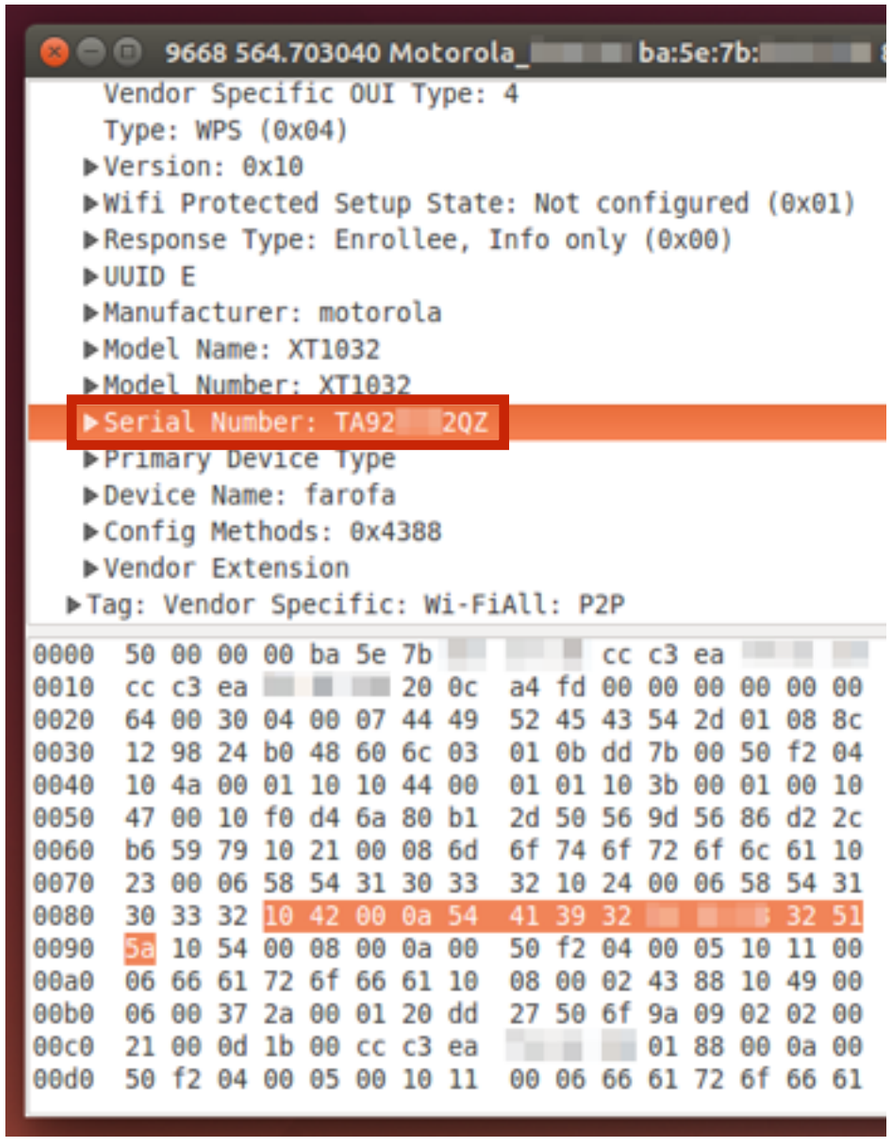
```
▶Frame 76656: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface 0
▶Radiotap Header v0, Length 26
▶IEEE 802.11 Probe Response, Flags: ........C
▼IEEE 802.11 wireless LAN management frame
 ▶Fixed parameters (12 bytes)
 ▼Tagged parameters (230 bytes)
  ▶Tag: SSID parameter set: DIRECT-
  ▶Tag: Supported Rates 6(B), 9(B), 12, 18, 24, 36, 48, 54, [Mbit/sec]
  ▶Tag: DS Parameter set: Current Channel: 1
  ▶Tag: Vendor Specific: Microsof: WPS
  ▶Tag: Vendor Specific: Wi-FiAll: P2P
```

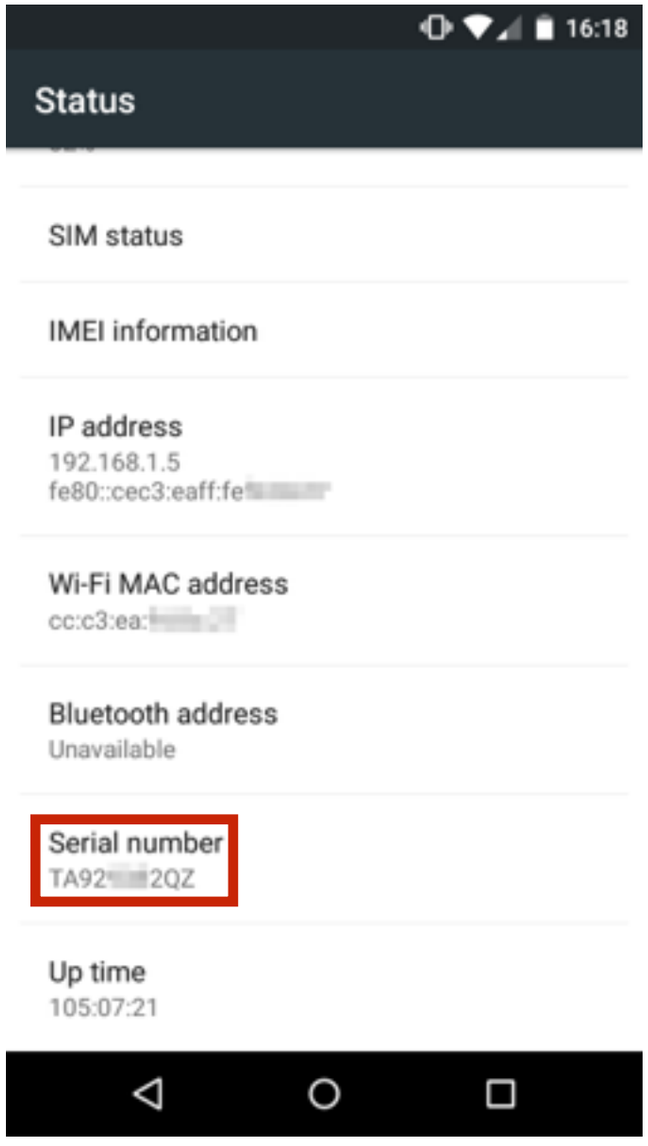
```
0000  00 00 1a 00 2f 48 00 00  32 10 f3 84 00 00 00 00   ..../H.. 2.......
0010  10 0c 6c 09 c0 00 e8 01  00 00 50 00 3c 00 cc c3   ..l..... ..P.<...
0020  ea [redacted] 02 90 a9 [redacted] 02 90 a9 [redacted]   . ... ... ...
0030  f0 54 48 6d 49 07 00 00  00 00 64 00 20 04 00 07   .THmI... ..d. ...
0040  44 49 52 45 43 54 2d 01  08 8c 92 18 24 30 48 60   DIRECT-. ....$0H`
0050  6c 03 01 01 dd a3 00 50  f2 04 10 4a 00 01 10 10   l......P ...J....
0060  44 00 01 01 10 12 00 02  00 00 10 3b 00 01 00 10   D....... ...;....
0070  47 00 10 ae 6e 76 80 00  90 a9 [redacted] f4 53 d8   G...nv.. . ..S.
0080  b8 02 a6 10 21 00 1b 57  65 73 74 65 72 6e 20 44   ....!..W estern D
0090  69 67 69 74 61 6c 20 43  6f 72 70 6f 72 61 74 69   igital C orporati
00a0  6f 6e 10 23 00 0a 57 44  20 54 56 20 4c 69 76 65   on.#..WD  TV Live
00b0  10 24 00 0d 57 44 42 48  47 37 30 30 30 30 4e 42   .$..WDBH G70000NB
00c0  4b 10 42 00 0c 57 4e 43  34 34 31 32 30 33 35 32   K.B..WNC 44120352
00d0  37 10 54 00 08 00 07 00  50 f2 04 00 01 10 11 00   7.T..... P.......
00e0  08 57 44 54 56 4c 69 76  65 10 08 00 02 23 88 10   .WDTVLiv e....#..
00f0  49 00 06 00 37 2a 00 01  20 dd 29 50 6f 9a 09 02   I...7*..  .)Po...
0100  02 00 23 00 0d 1d 00 02  90 a9 [redacted] 01 88 00   ..#..... .. ...
0110  07 00 50 f2 04 00 01 00  10 11 00 08 57 44 54 56   ..P..... ....WDTV
0120  4c 69 76 65 40 f8 fa 35                           Live@..5
```

Wi-Fi Direct information element on Probe Response frame

Protocol Complexity

Too much information

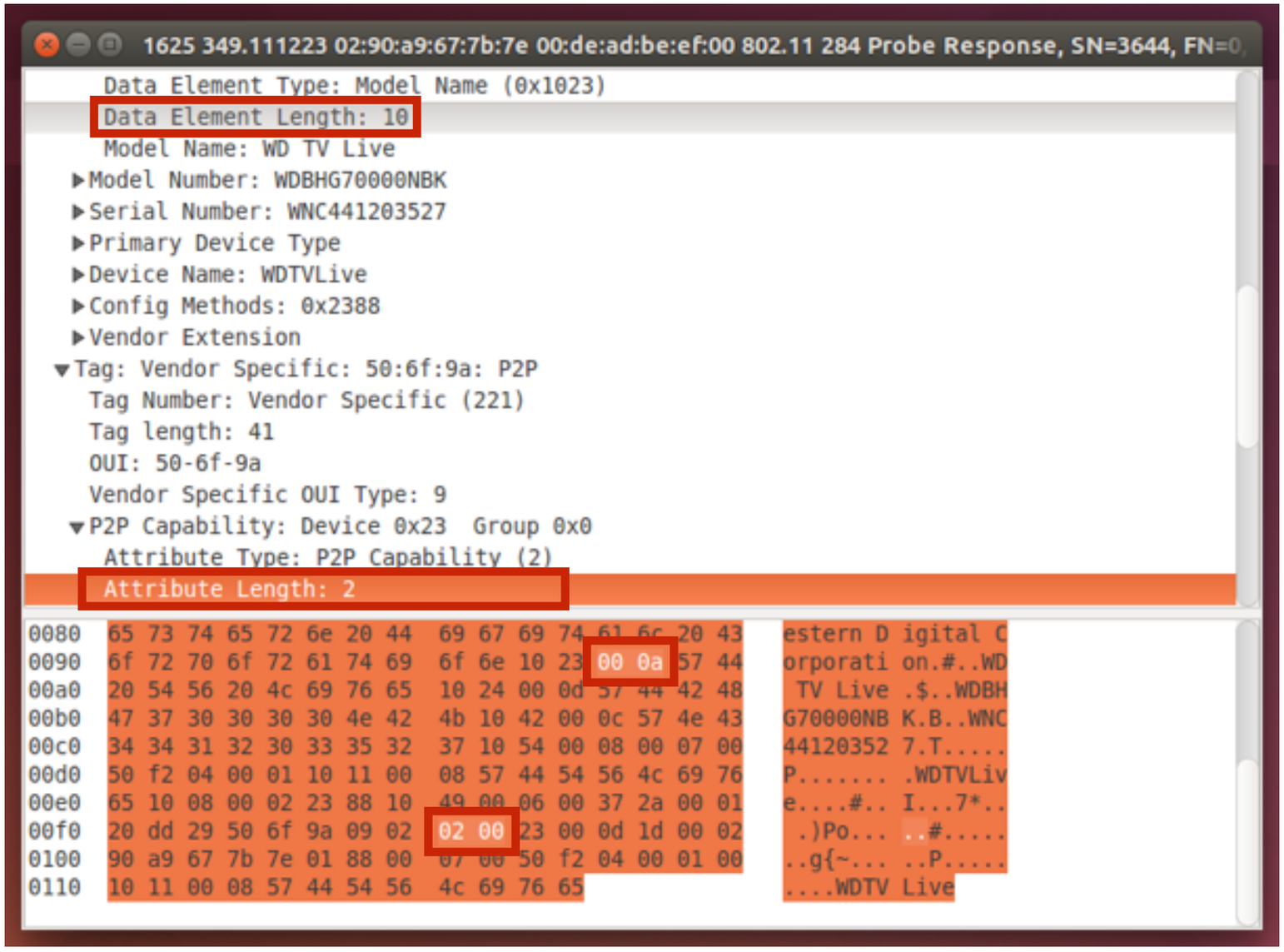




Sharing serial numbers

Protocol Complexity

Endianness Nonsense



Big-endian is the most common format in data networking

Protocol Complexity

Too much information

Protocol Complexity

Too much information

With AirPlay, you can stream music, photos, and videos to your Apple TV, or stream music to your AirPort Express or AirPlay-enabled speakers. And with AirPlay Mirroring, you can display your iOS screen on your Apple TV.

https://support.apple.com/en-gb/HT204289

Protocol Complexity

Too much information

160 153.087073000 de:63:aa:18:8c:16 Broadcast 802.11 797 Action, SN=4020, FN=0, Flags=.....

```
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: de:63:aa:18:8c:16 (de:63:aa:18:8c:16)
Source address: de:63:aa:18:8c:16 (de:63:aa:18:8c:16)
```

```
01c0  32 0d 61 6d 3d 41 70 70  6c 65 54 56 33 2c 32 43   2.am=App leTV3,2C
01d0  70 6b 3d 33 30 35 38 39  35 36 32 36 34 61 61 38   pk=30589 56264aa8
01e0  61 61 39 33 35 61 64 30  30 33 63 63 37 31 65 31   aa935ad0 03cc71e1
01f0  33 32 65 38 37 31 30 63  38 62 36 34 64 30 63 61   32e8710c 8b64d0ca
0200  36 37 61 34 30 34 38 66  30 33 63 35 31 33 61 65   67a4048f 03c513ae
0210  39 65 32 06 73 66 3d 30  78 34 06 74 70 3d 55 44   9e2.sf=0 x4.tp=UD
0220  50 08 76 6e 3d 36 35 35  33 37 09 76 73 3d 32 32   P.vn=655 37.vs=22
0230  30 2e 36 38 04 76 76 3d  32 02 e1 00 0c 00 08 61   0.68.vv= 2......a
0240  70 70 6c 65 20 74 76 c0  01 10 cf 00 00 00 1a 64   pple tv. .......d
0250  65 76 69 63 65 69 64 3d  36 38 3a 36 34 3a 34 42   eviceid= 68:64:4B
0260  3a [redacted]  18 66 65 61 74 75 72   :[redacted].featur
0270  65 73 3d 30 78 35 41 37  46 46 46 46 37 2c 30 78   es=0x5A7 FFFF7,0x
0280  31 45 09 66 6c 61 67 73  3d 30 78 34 10 6d 6f 64   1E.flags =0x4.mod
0290  65 6c 3d 41 70 70 6c 65  54 56 33 2c 32 43 70 6b   el=Apple TV3,2pk
02a0  3d 33 30 35 38 39 35 36  32 36 34 61 61 38 61 61   =3058956 264aa8aa
02b0  39 33 35 61 64 30 30 33  63 63 37 31 65 31 33 32   935ad003 cc71e132
02c0  65 38 37 31 30 63 38 62  36 34 64 30 63 61 36 37   e8710c8b 64d0ca67
02d0  61 34 30 34 38 66 30 33  63 35 31 33 61 65 39 65   a4048f03 c513ae9e
```

AirPlay action frame from an AppleTV 3rd Generation

Protocol Complexity

Too much information

With AirDrop, you can wirelessly send photos, videos, websites, locations, and more to a nearby iPhone, iPad, iPod touch, or Mac.

https://support.apple.com/en-us/HT203106

Protocol Complexity

Too much information

91637 1554.173064 d6:7a:41:[redacted] Broadcast 802.11 196 Action, SN=2283, FN=0, Flags=....., S

```
▶Frame 91637: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits)
▶IEEE 802.11 Action, Flags: ........
▶IEEE 802.11 wireless LAN management frame
▶[Malformed Packet: IEEE 802.11]
```

```
0000  d0 00 00 00 ff ff ff ff  ff ff d6 7a 41 [redacted]   ........ ...zA...
0010  00 25 00 ff 94 73 b0 8e  7f 00 17 f2 08 10 00 00   .%...s.. ........
0020  b8 6f 5e 00 3c 6e 5e 00  04 39 00 06 39 00 06 00   .o^.<n^. .9..9...
0030  10 00 6e 00 00 18 10 00  10 00 09 00 03 00 00 00   ..n..... ........
0040  d6 7a 41 86 ee c7 04 00  80 01 00 00 0f 00 00 03   .zA..... ........
0050  ff ff 06 00 06 00 00 00  06 06 06 00 06 00 00 00   ........ ........
0060  06 06 00 00 05 15 00 00  00 00 00 00 d6 7a 41 86   ........ .....zA.
0070  ee c7 72 00 00 00 72 00  00 00 00 00 06 0a 00 00   ..r...r. ........
0080  00 00 02 00 00 04 00 00  40 0c 15 00 23 03 55 53   ........ @...#.US
0090  00 06 00 70 10 5c 83 f5  c4 06 00 b0 34 95 c4 44   ...p.\.. ....4..D
00a0  1e 07 06 00 00 00 6c 01  19 ff 10 17 00 03 13 4a   ......l. .......J
00b0  65 66 66 72 65 79 73 2d  69 50 6f 64 2d 74 6f 75   effreys- iPod-tou
00c0  63 68 c0 0c                                       ch..
```

AirDrop action frame from an iPod touch

Protocol Complexity

Too much information

Wireless Network Traffic could be displayed during the demo.
Please disable Wi-Fi if you don’t want to be part of it.

Protocol Complexity

Messy Implementations

WD TV Live Media Player

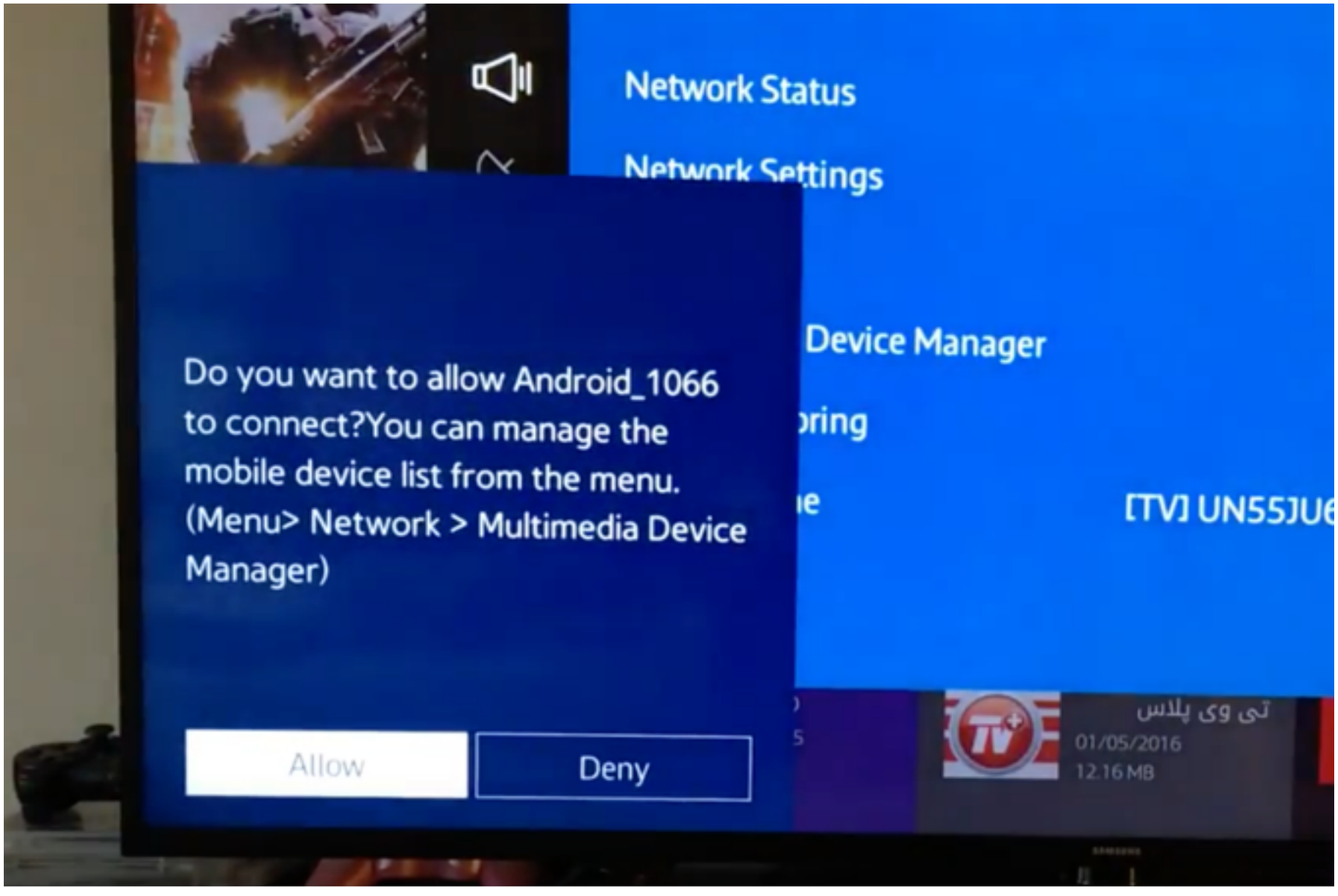
Protocol Complexity

Messy Implementations

WD TV Live Media Player has WiFi Direct enabled by default

Protocol Complexity

Messy Implementations



Samsung TV authenticating a WiFi Direct connection request

Protocol Complexity

Messy Implementations

Wireless Network Traffic could be displayed during the demo.
Please disable Wi-Fi if you don’t want to be part of it.

Platform Complexity

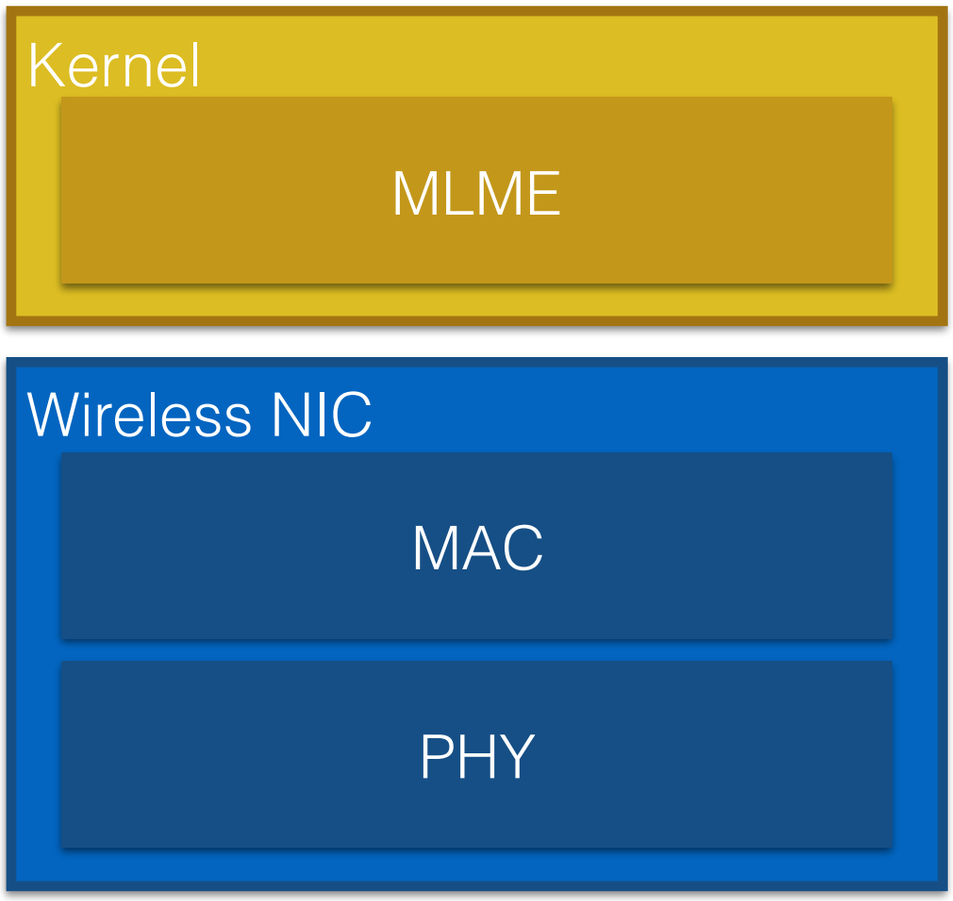
MLME stands for MAC Layer Management Entity. Examples of states a MLME may assist in reaching:

- Authenticate
- Deauthenticate
- Associate
- Disassociate
- Reassociate
- Beacon
- Probe
- Timing Synchronization Function (TSF)

http://linuxwireless.org/en/developers/Documentation/Glossary/#MLME

Platform Complexity

SoftMAC is a term used to describe a type of Wireless NIC where the MLME is expected to be managed in software.



http://linuxwireless.org/en/developers/Documentation/Glossary/#SoftMAC

Platform Complexity

FullMAC is a term used to describe a type of wireless card where the MLME is managed in hardware.

http://linuxwireless.org/en/developers/Documentation/Glossary/#FullMAC

Platform Complexity

Hardware

Firmware
(Broadcom)

Kernel

Kernel Module
(Broadcom)

User

wpa_supplicant
(Jouni Malinen)

Android Framework
(Google)

Platform Complexity

- Firmware
  - chipset rom
  - /system/etc/wifi/
- Kernel module
  - /system/lib/modules/
  - Builtin into the kernel
- wpa_supplicant
  - /system/bin/wpa_supplicant
- Android Framework
  - /system/framework

Platform Complexity

Firmware

- No source code available.
- No symbols.
- IDA Pro doesn’t have a loader.
- Firmware is divided into 2 segments.
- Some dynamic analysis by firmware modification.
- Runs on the Wireless NIC chipset.
- Shared code with kernel modules.

Platform Complexity

Kernel Module

- Some of them are open source.
- Kernel debugging.
- Kernel Module debug level.

Platform Complexity

wpa_supplicant & hostapd

- Open Source.
- wpa_cli to interact with supplicant.
- User space application.

Platform Complexity

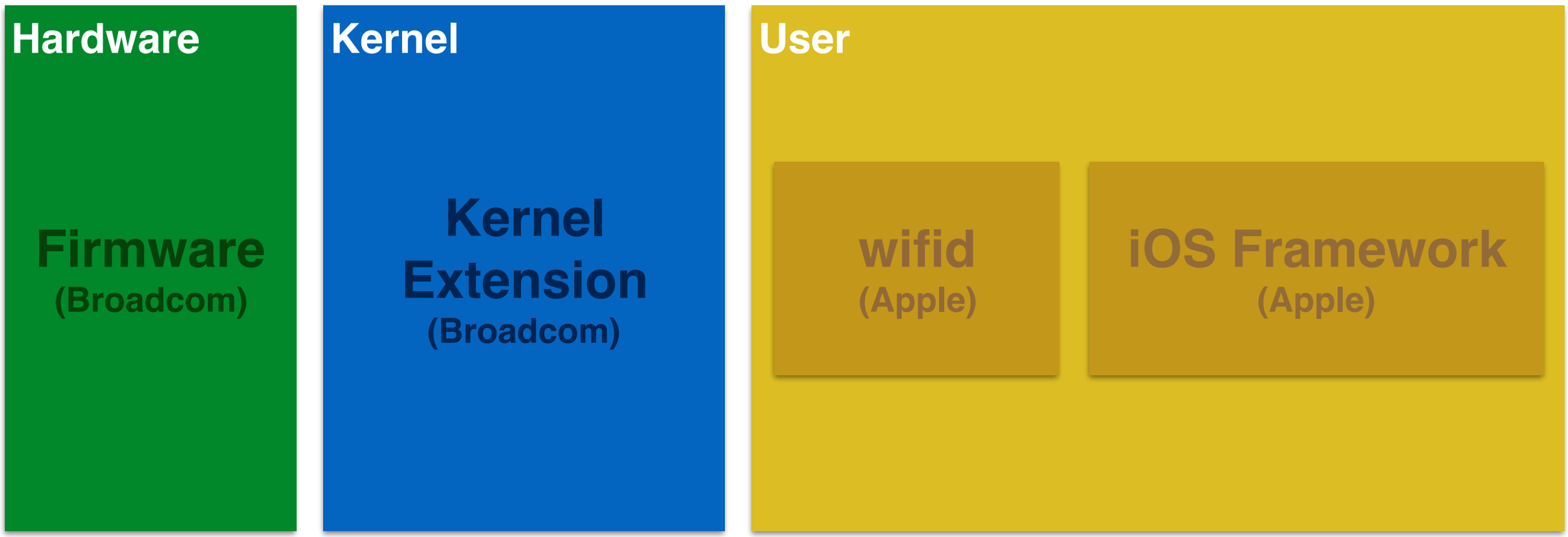
Android Framework

- Open Source.
- Use adb logcat to see information.
- Debug using Android SDK tools.

Protocol Complexity

Wireless Network Traffic could be displayed during the demo.
Please disable Wi-Fi if you don’t want to be part of it.

Platform Complexity



Platform Complexity

- Firmware
  - chipset rom
  - /system/etc/wifi/
- Kernel extension
  - /System/Library/Caches/com.apple.kernelcaches/kernelcache
- wifid
  - /usr/sbin/wifid
- iOS Framework
  - /System/Library/Frameworks/

Platform Complexity

Firmware

- No source code available.
- No symbols.
- IDA Pro doesn’t have a loader.
- Firmware is divided into 2 sections.
- Pseudo dynamic analysis by firmware modification. [4] [5]
- Runs on the Wireless NIC chipset.
- Shared code with kernel modules and chipset models (4329, 4330, etc).

Same as Android Platform

Platform Complexity

Kernel extensions

- Encrypted kernel**.
- Static analysis.
- Shared code between OS X and iOS.
- Extensions targets:
  - AppleBCMWLANCore
  - IO80211Family

Platform Complexity

wifid

- Closed Source.
- Not only handles Wi-Fi tasks but also Bluetooth.
- Can use GDB for debugging.

Platform Complexity

Framework

- Private framework.
- Static analysis.
- Shared code between OS X and iOS.

Conclusions

Protocol Complexity

- WPS, WiFi Direct, CCX, AirPlay and AirDrop specifications could help device fingerprinting.

- iOS MAC address randomization privacy feature could be evaded when using AirDrop or AirPlay specifications.

- Specifications such as AirPlay or WiFi Direct could expose devices to unauthenticated connections.

Conclusions

- WPS Pin brute force attack (**CVE-2011-5053**)
  - Brute forcing Wi-Fi Protected Setup [8]
  - Pixie Dust Attack [9]

- MalwAirDrop
  http://2015.ruxcon.org.au/assets/2015/slides/ruxcon-2016-dowd.pptx

- WD TV Live Streaming Media Player Wi-Fi Direct Unauthenticated Access
  http://neseso.com/advisories/NESESO-2016-0910.pdf

Conclusions

Frames are parsed by different layers and some of these frames contain complex structures.

- Broadcom BCM4325 and BCM4329 wireless chipset denial-of-service vulnerability (**CVE-2012-2619**)
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-2619
- Android WiFi-Direct DoS (**CVE-2014-0997**)
  http://www.coresecurity.com/advisories/android-wifi-direct-denial-service
- Long WPS_ID_DEVICE_NAME in WPS info elements. (**CVE-2016-0801**, **CVE-2016-0802**)
  https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0801
- A frame validation and memory corruption issue existed for a given ethertype. (**CVE-2016-0801**, **CVE-2016-0802**)
  https://support.apple.com/en-us/HT206166

Conclusions

Future Work

- Extend analysis on other platforms and vendors.
- Implement the Bluetooth LE Apple scanning protocol not the Ubertooth firmware and extend WIG tool to support it.
- Extend the RE work on Apple proprietary protocols.
- Continue extending and fixing bug on WIG tool.

Questions

WIG Project Repository

https://github.com/6e726d/WIG

Email: 6e726d@gmail.com **Twitter:** @6e726d

References

- Abusing Windows WiFi Native API to create a Cover Channel, Andrés Blanco &Ezequiel Gutesman
  http://www.coresecurity.com/corelabs-research/publications/abusing-windows-wifi-native-api-create-covert-channel

- Wi-Door - Bind/Rev Shells for your Wi-Fi, Vivek Ramachandran
  https://www.youtube.com/watch?v=T6yc0Toyt2A

- Broadcom BCM4325 and BCM4329 DoS
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-2619

- One firmware to monitor 'em all, Andrés Blanco & Matías Eissler
  http://archive.hack.lu/2012/Hacklu-2012-one-firmware-Andres-Blanco-Matias-Eissler.pdf

- Apple80211 reversed, Jonathan Levin
  http://newosxbook.com/articles/11208ellpA.html

- Brute forcing Wi-Fi Protected Setup
  https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

- Offline bruteforce attack on WiFi Protected Setup
  http://archive.hack.lu/2014/Hacklu2014_offline_bruteforce_attack_on_wps.pdf

- Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms
  http://papers.mathyvanhoef.com/asiaccs2016.pdf