802.11 Complexity

An introduction to 802.11 protocol chaos

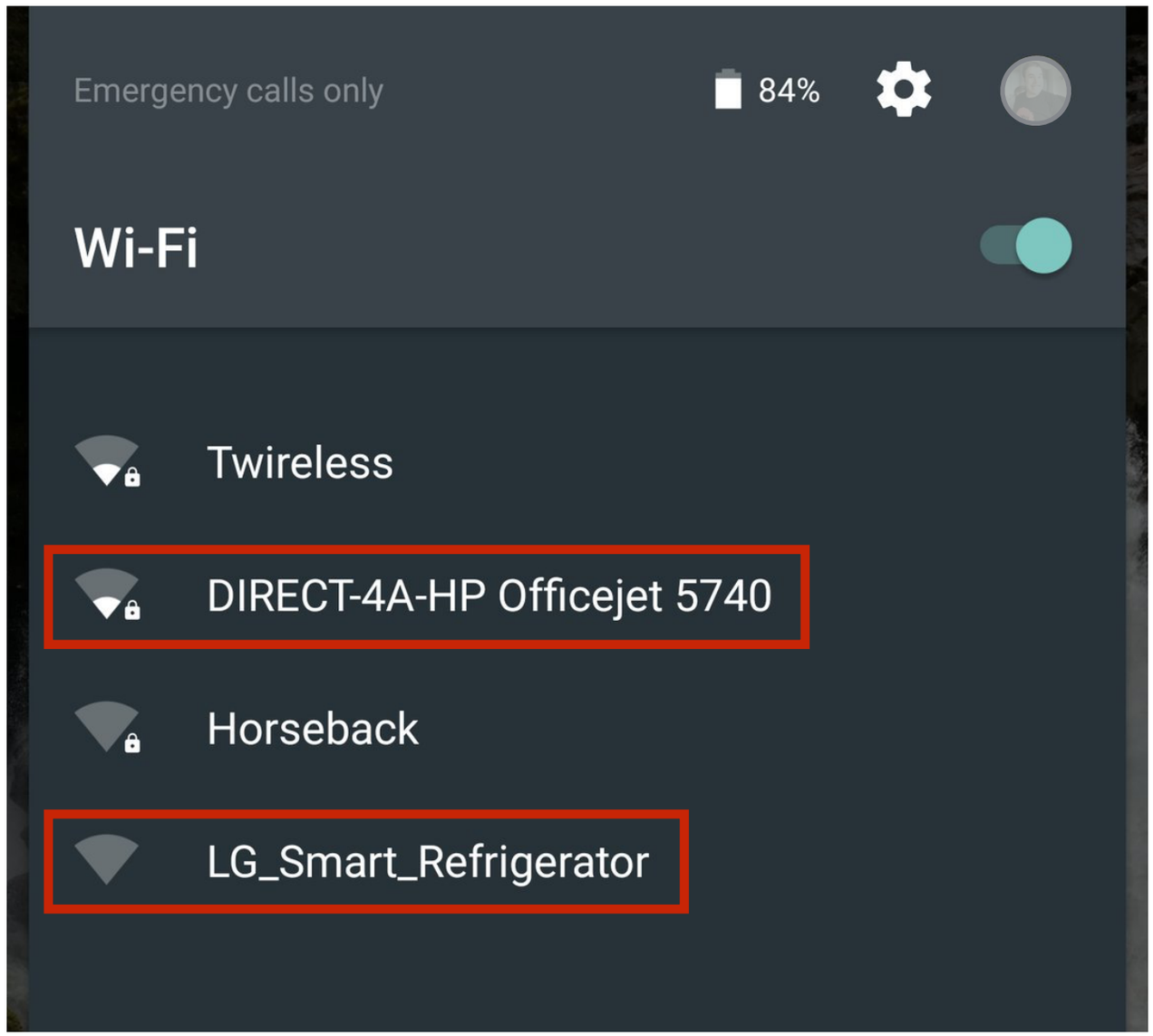
Andrés Blanco

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

- 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
- …

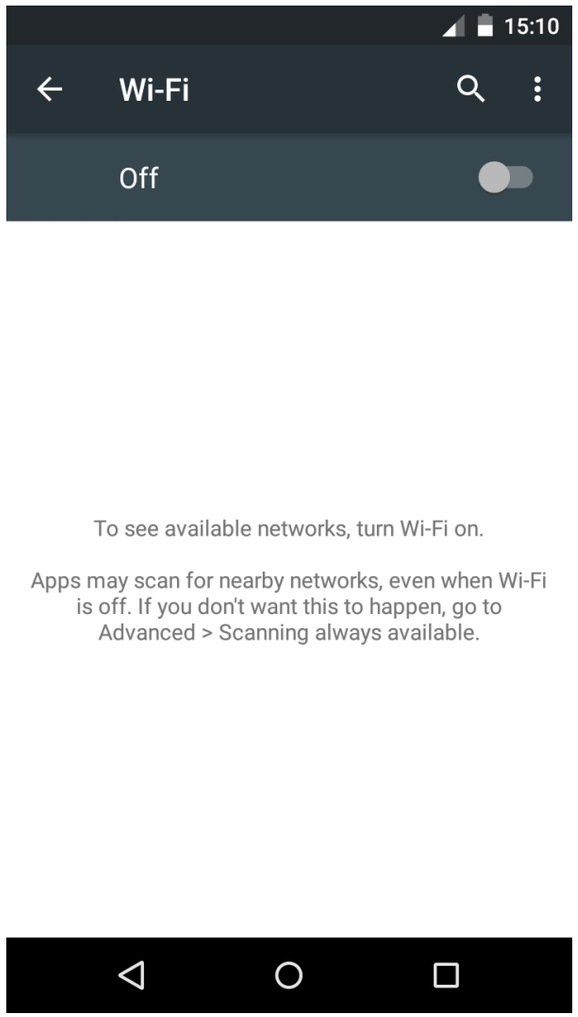
802.11 protocol is growing and constantly changing

Motivation

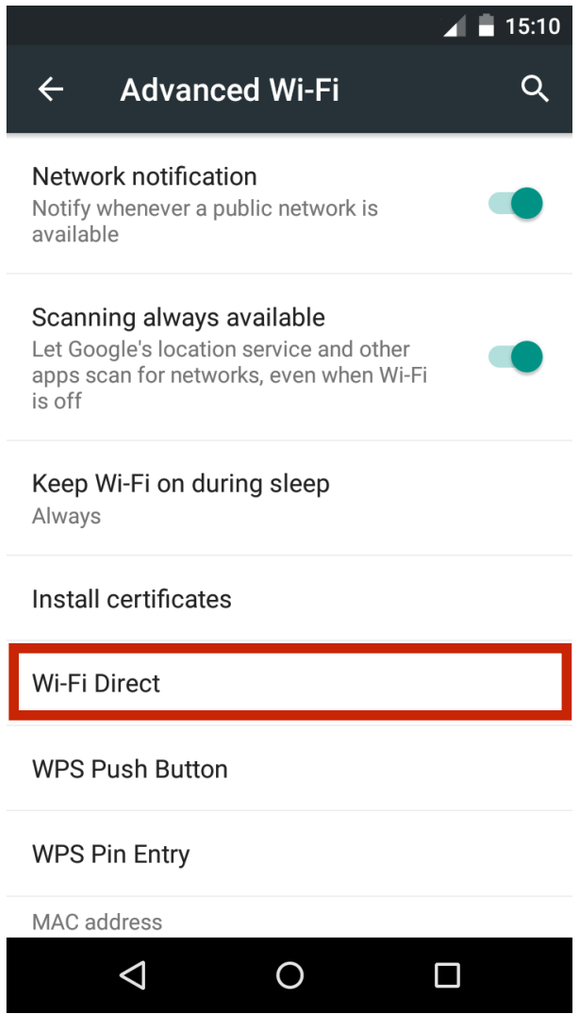
802.11 is growing and constantly changing

Motivation

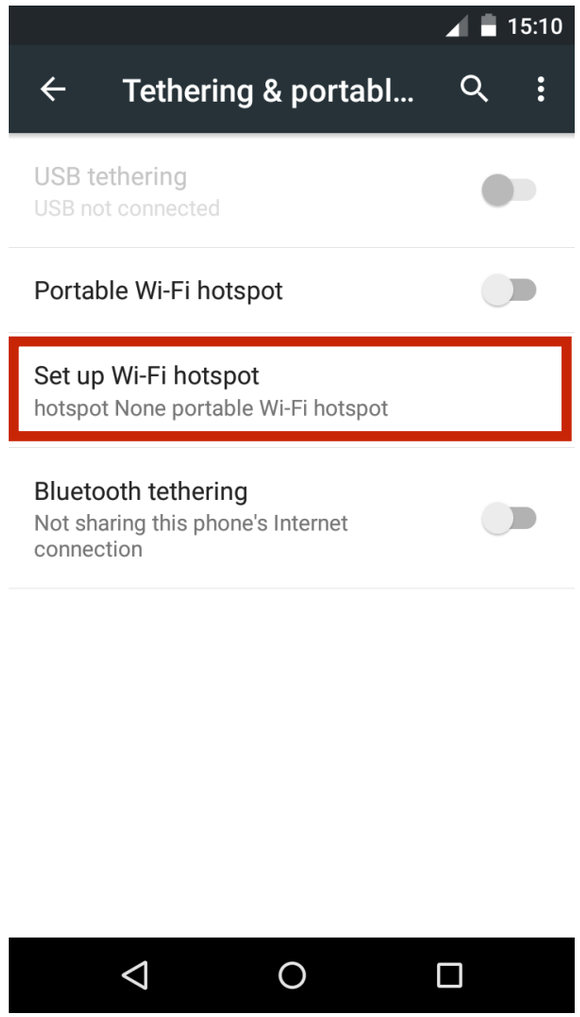
Managed



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

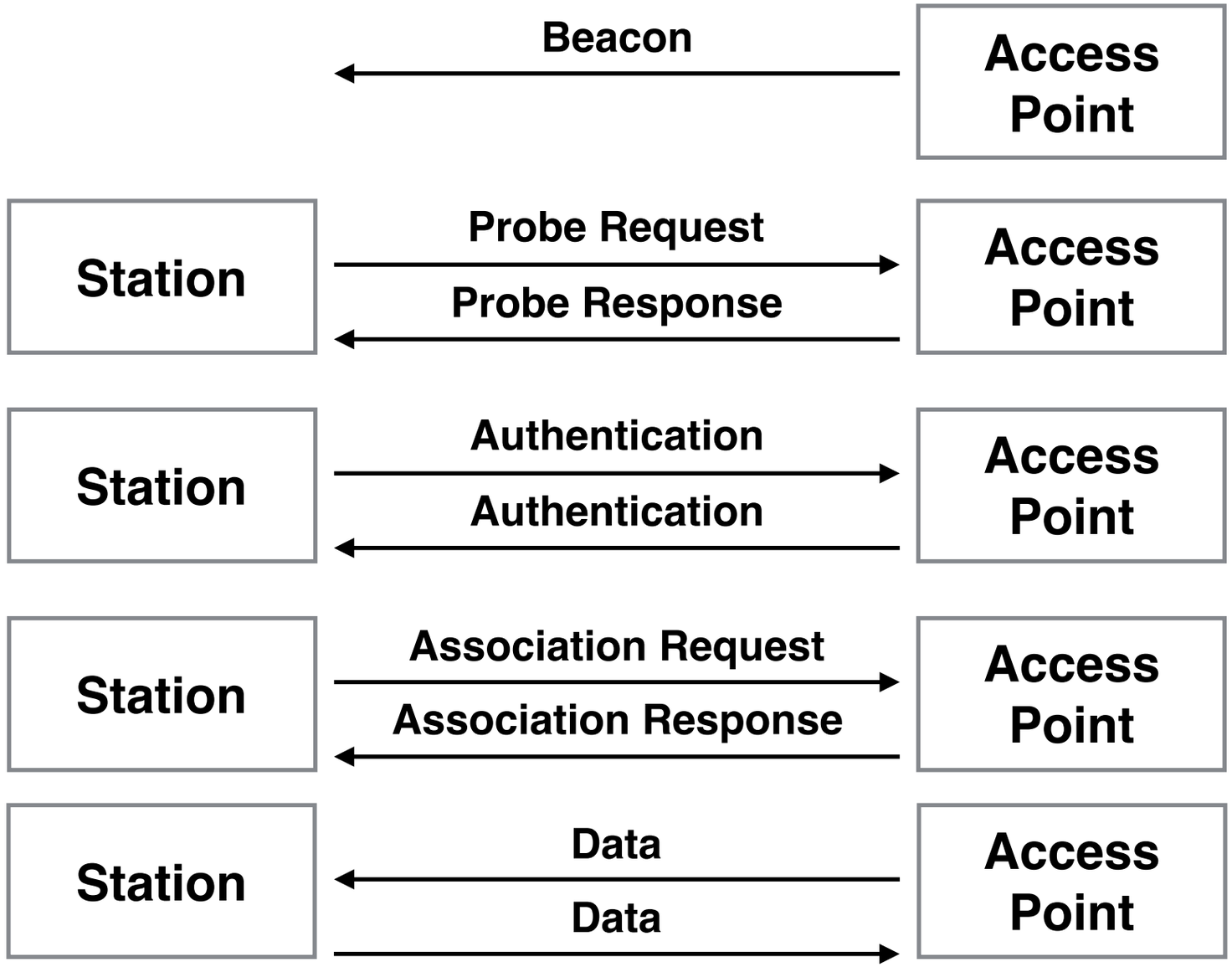
- Block ACK Request
- Block ACK
- PS-Poll
- RTS
- CTS
- ACK
- CF-End
- CF-End+CF-ACK

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

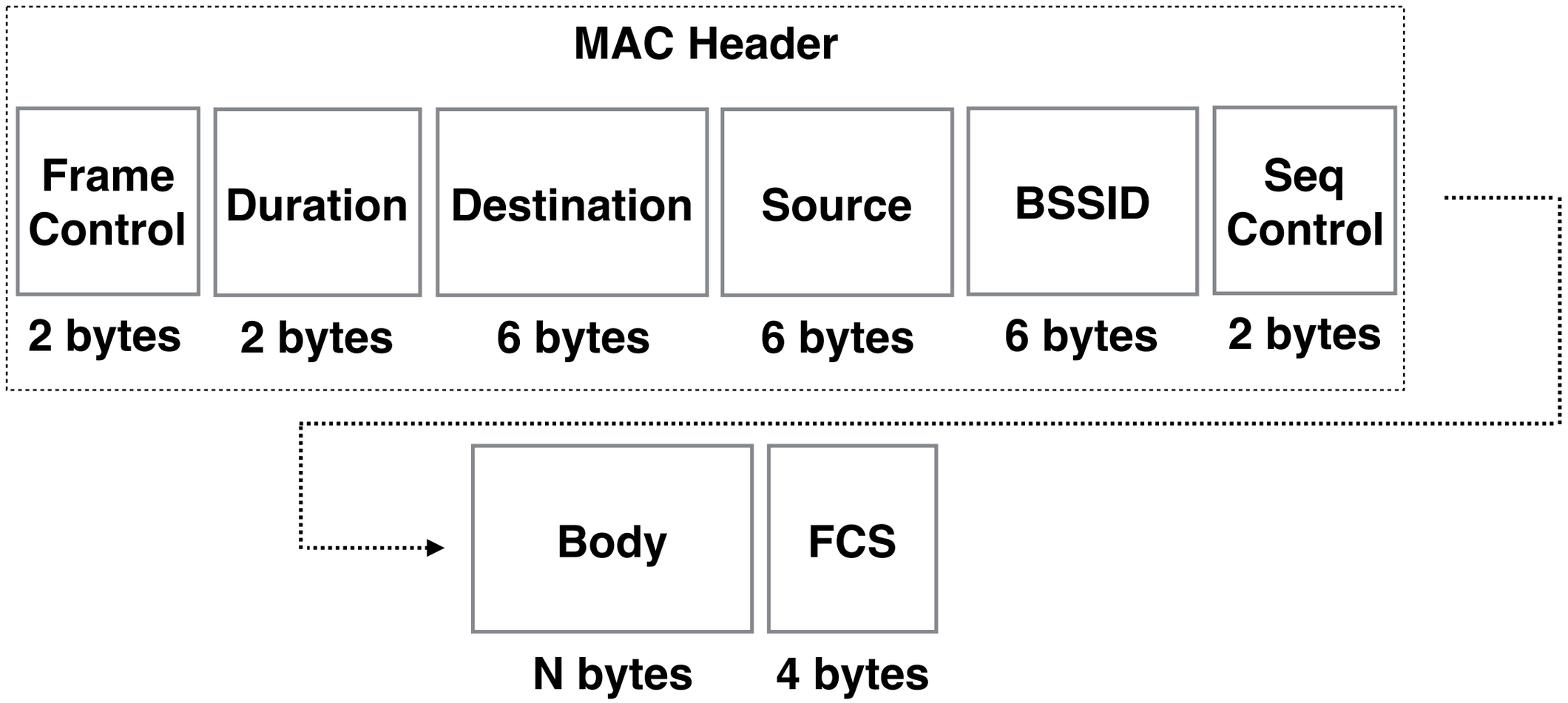
802.11 frame types and subtypes

Protocol Complexity



802.11 Association process

Protocol Complexity



Management frame structure

Protocol Complexity

Type	Length	Value
1 byte	1 byte	N bytes

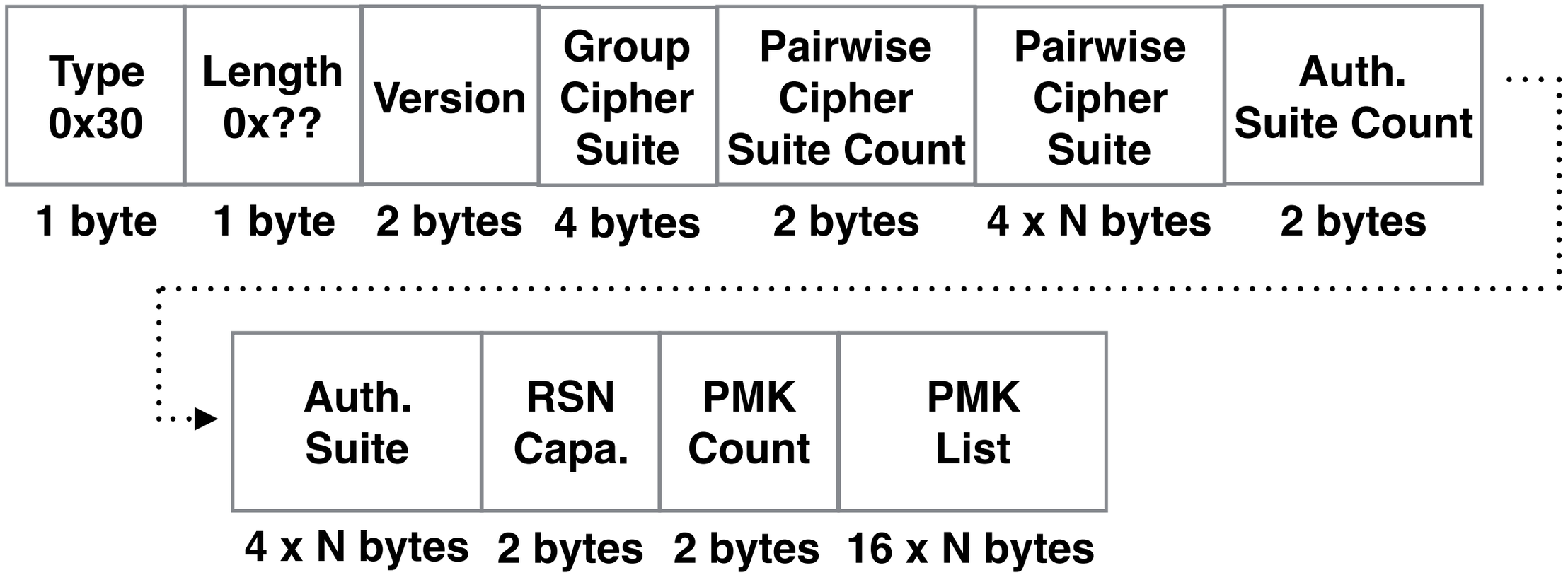
Information elements are variable-length components

Protocol Complexity

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

SSID information element

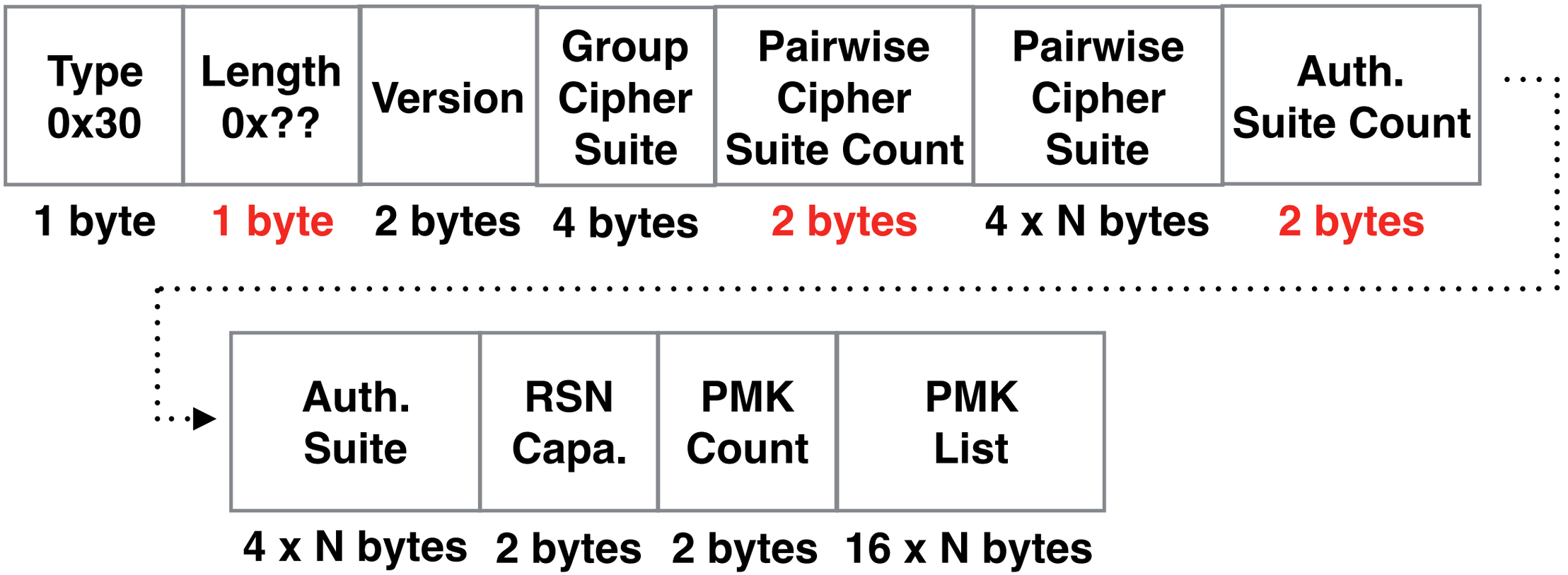
Protocol Complexity



RSN information element

Protocol Complexity

Length Nonsense



CVE-2012-2619 affected at least 15 different vendors

Protocol Complexity

Cisco

Protocol Complexity

Cisco

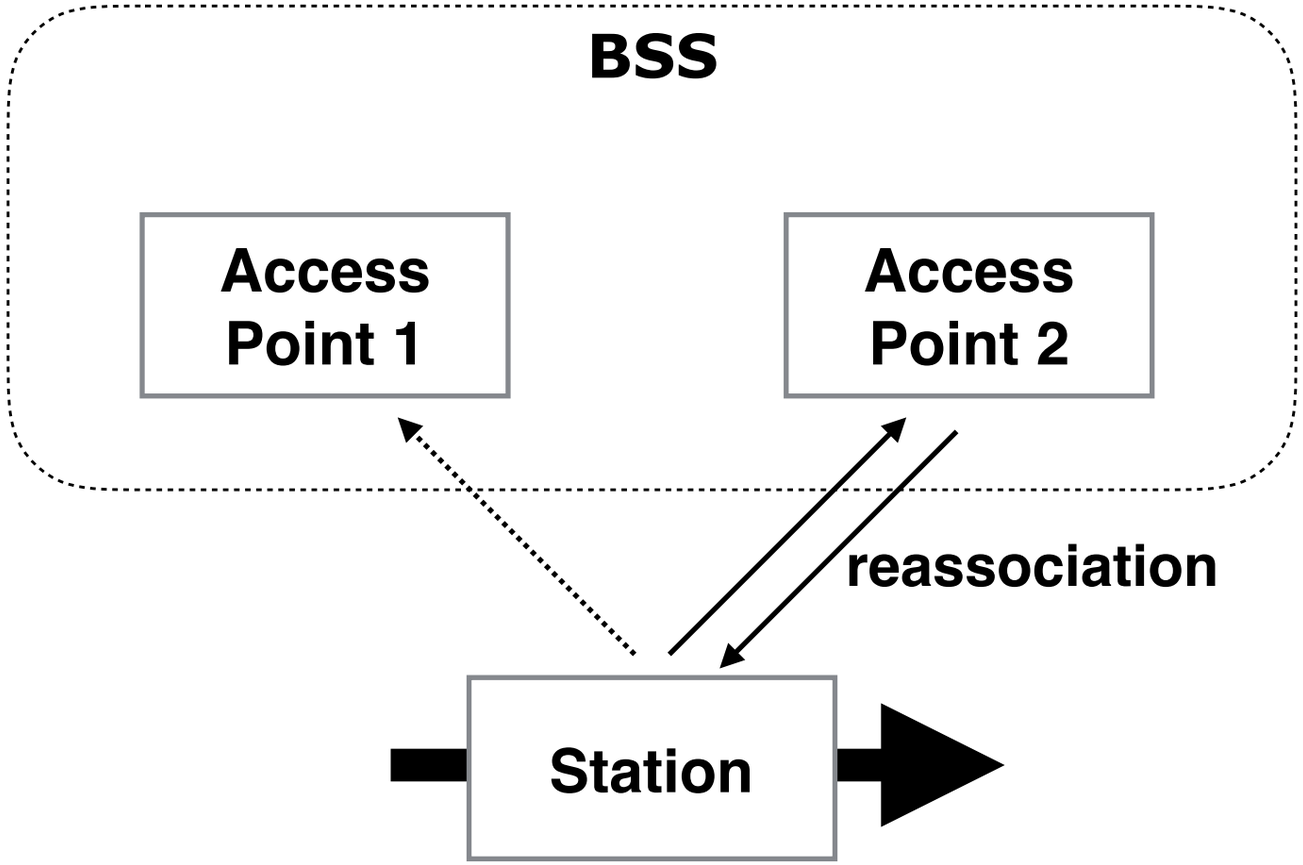
If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address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

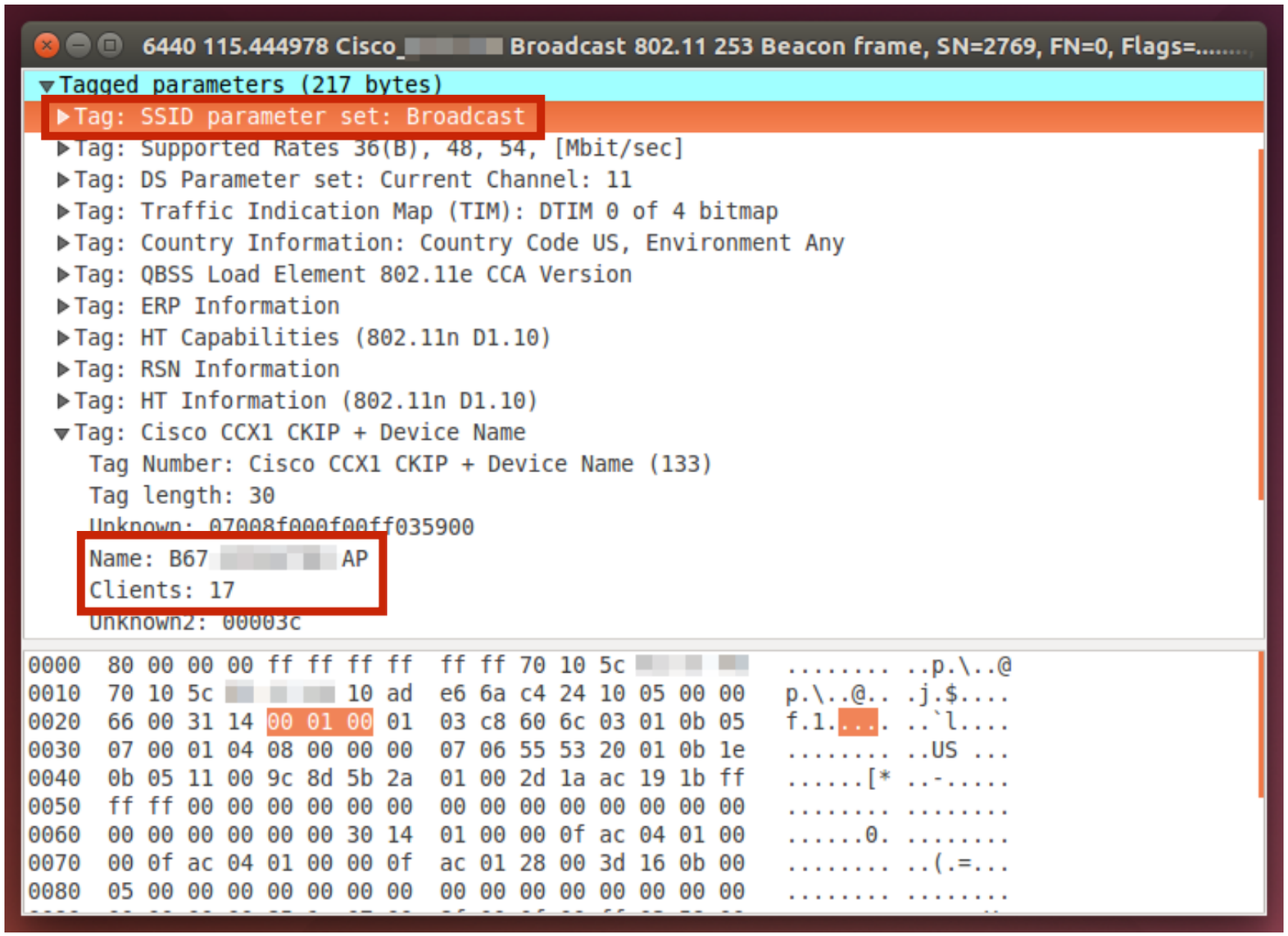
Cisco



802.11 roaming

Protocol Complexity

Cisco



Access Point name and number of associated clients

Protocol Complexity

Cisco

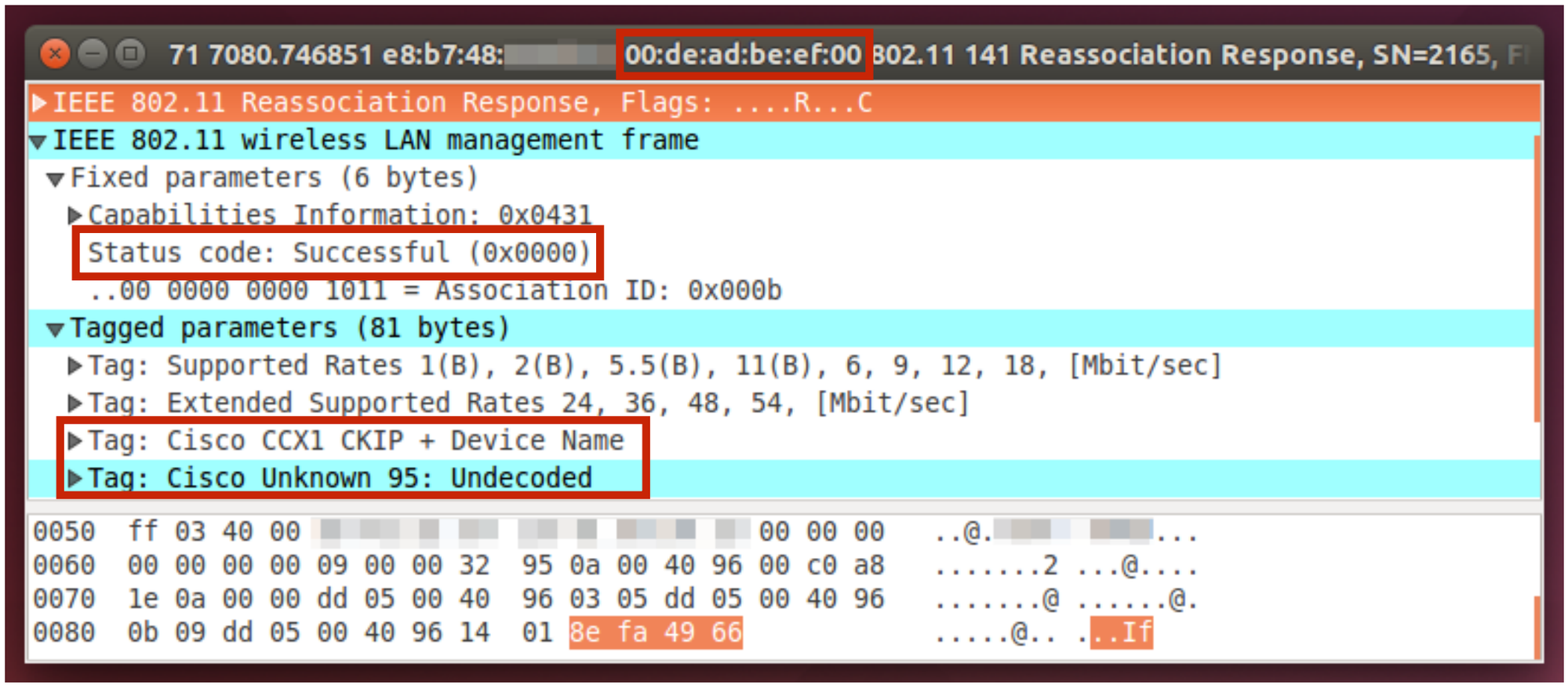
```
69 7080.733216 00:de:ad:be:ef:00 e8:b7:48:[redacted] 802.11 305 Reassociation Request, SN=1168, FN
▶IEEE 802.11 Reassociation Request, Flags: ........
▼IEEE 802.11 wireless LAN management frame
 ▼Fixed parameters (10 bytes)
  ▶Capabilities Information: 0x1431
   Listen Interval: 0x005a
   Current AP: e8:b7:48:[redacted] (e8:b7:48:[redacted])
 ▼Tagged parameters (260 bytes)
  ▶Tag: SSID parameter set: [redacted]
  ▶Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
  ▶Tag: DS Parameter set: Current Channel: 1
  ▶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: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
  ▶Tag: HT Information (802.11n D1.10)
  ▶Tag: Extended Capabilities (6 octets)
  ▶Tag: Cisco CCX1 CKIP + Device Name
  ▶Tag: Cisco Unknown 96: Undecoded

0100  01 01 80 00 03 a4 00 00  27 a4 00 00 42 43 5e 00   ........ '...BC^.
0110  62 32 2f 00 dd 06 00 40  96 01 01 04 dd 05 00 40   b2/....@ .......@
0120  96 03 05 dd 05 00 40 96  0b 09 dd 05 00 40 96 14   ......@. .....@..
0130  01                                                .
```

Fake reassociation request frame

Protocol Complexity

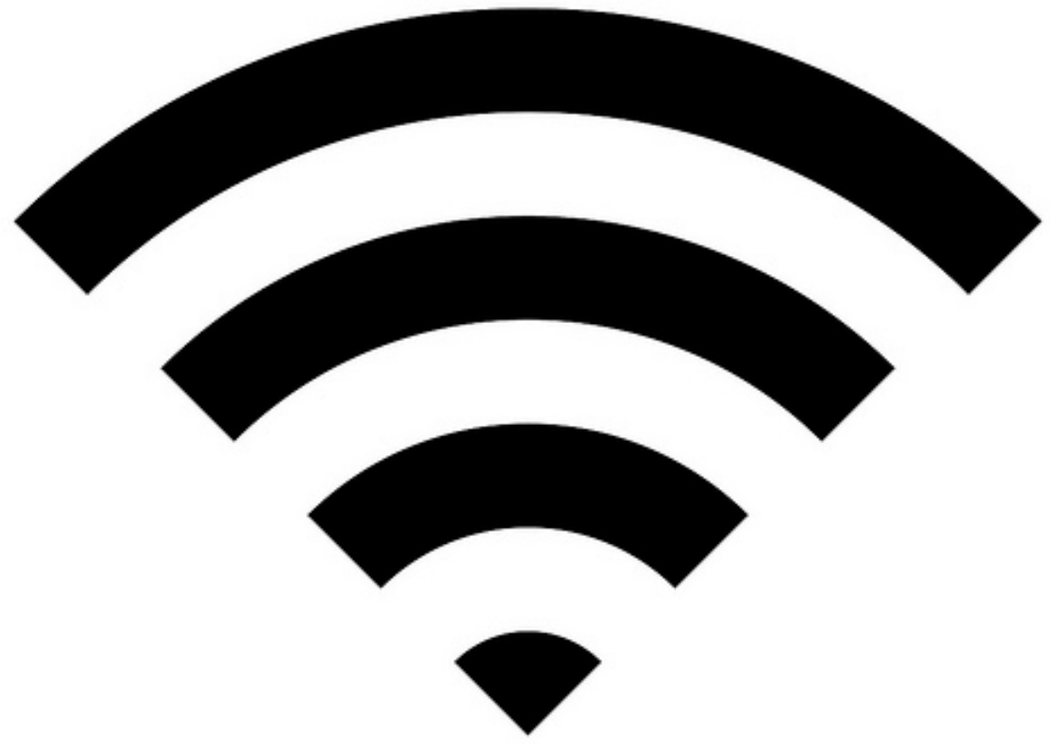
Cisco



Reassociation response frame

Protocol Complexity

Cisco



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

WiFi Alliance

Protocol Complexity

WiFi Alliance

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

WiFi Alliance

153614 1713.279543 Netgear_ 00:61:71: 802.11 397 Probe Response, SN=1865, FN=0, Flags=....., BI=100

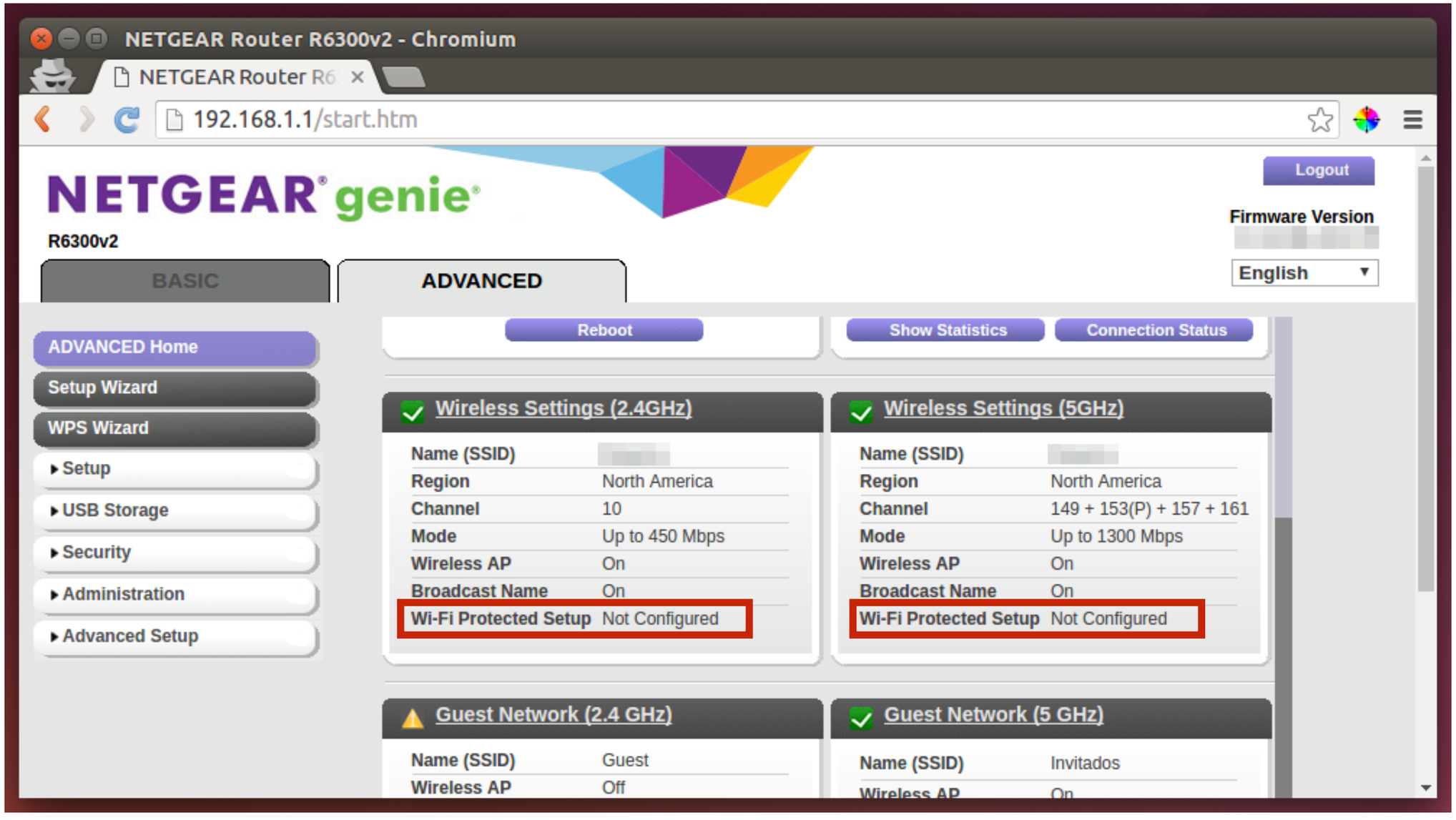
```
  ▶Manufacturer: NETGEAR, Inc.
  ▶Model Name: WGR614v10
  ▶Model Number: WGR614v10
  ▶Serial Number: 83258
  ▶Primary Device Type
  ▶Device Name: WGR614v10
  ▶Config Methods: 0x0084
▶Tag: Vendor Specific: Broadcom
```

```
0000  50 00 3a 01 00 61 71 [redacted] a0 21 b7 [redacted]   P.:..aq. u..!.a.8
0010  a0 21 b7 [redacted] 90 74  bf 1f 55 9c 00 00 00 00   .!.a.8.t ..U.....
0020  64 00 11 04 00 0f [redacted] 70 6f 6b 65   d.....[redacted]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

WiFi Alliance



Disabling WPS can protect a device from some know attacks

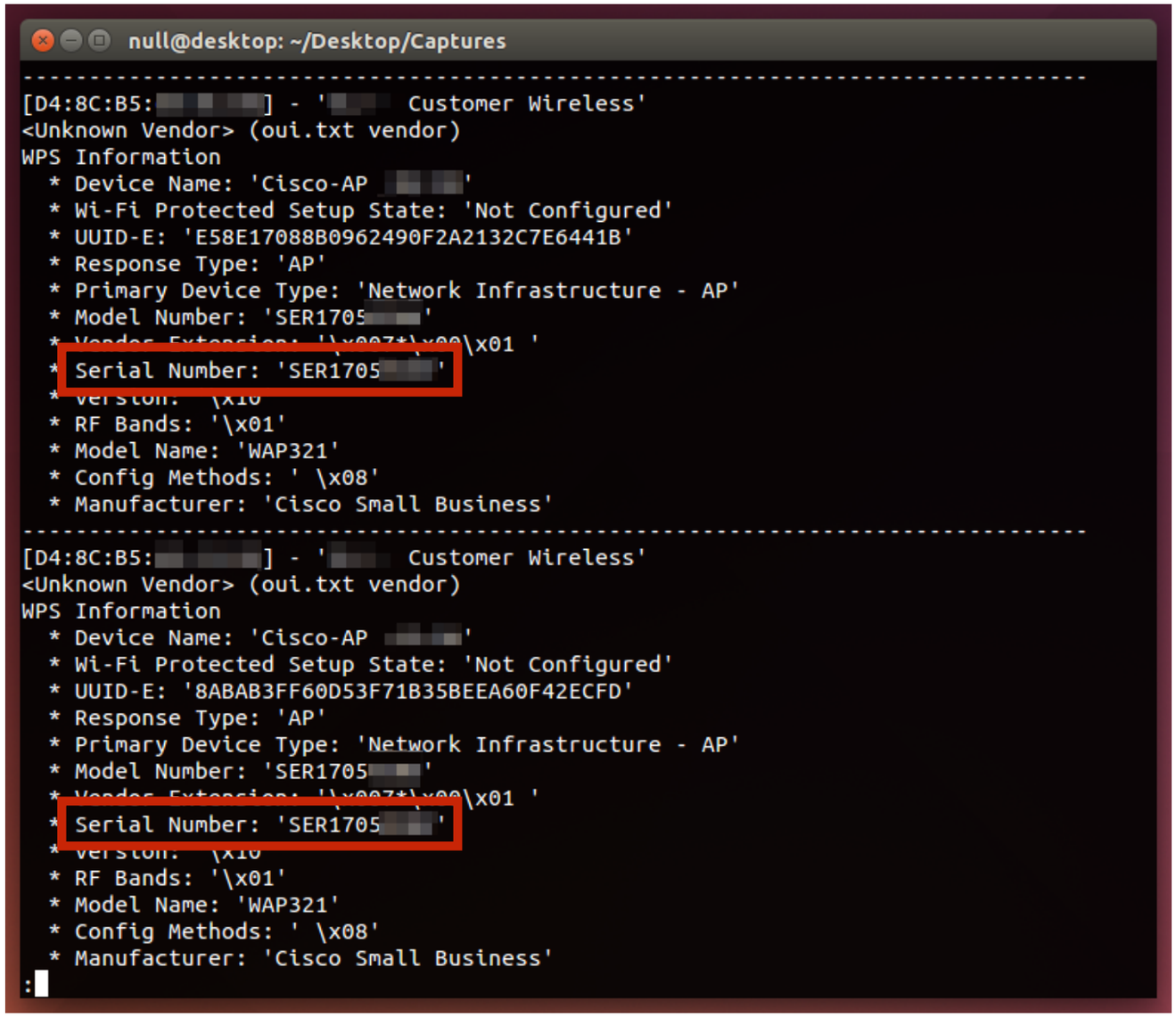
Protocol Complexity

WiFi Alliance

```
root@desktop: ~/Desktop/wig
------------------------------------------------------------------------
BSSID: c4:04:15:
SSID:
--------------------
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:
SSID:
--------------------
device name: 'VMG1312-B10B'
primary device type: 'Network Infrastructure'
```

Even disabling WPS doesn't disable completely

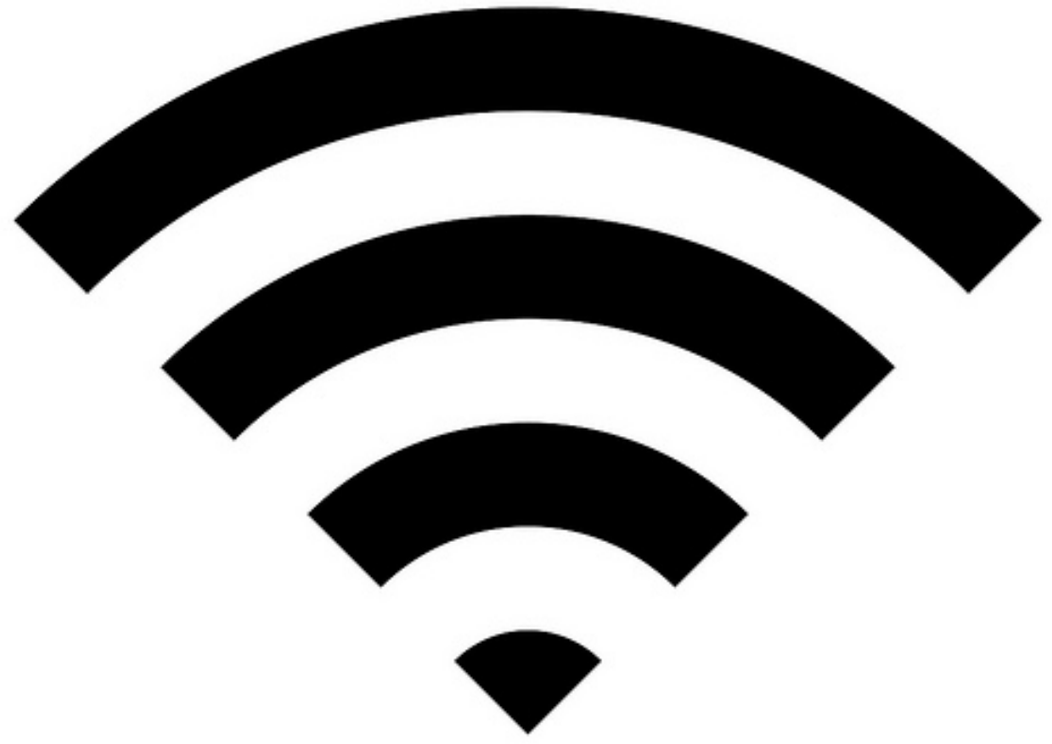
Protocol Complexity



WPS serial numbers

Protocol Complexity

WiFi Alliance



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

WiFi Alliance

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

WiFi Alliance

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

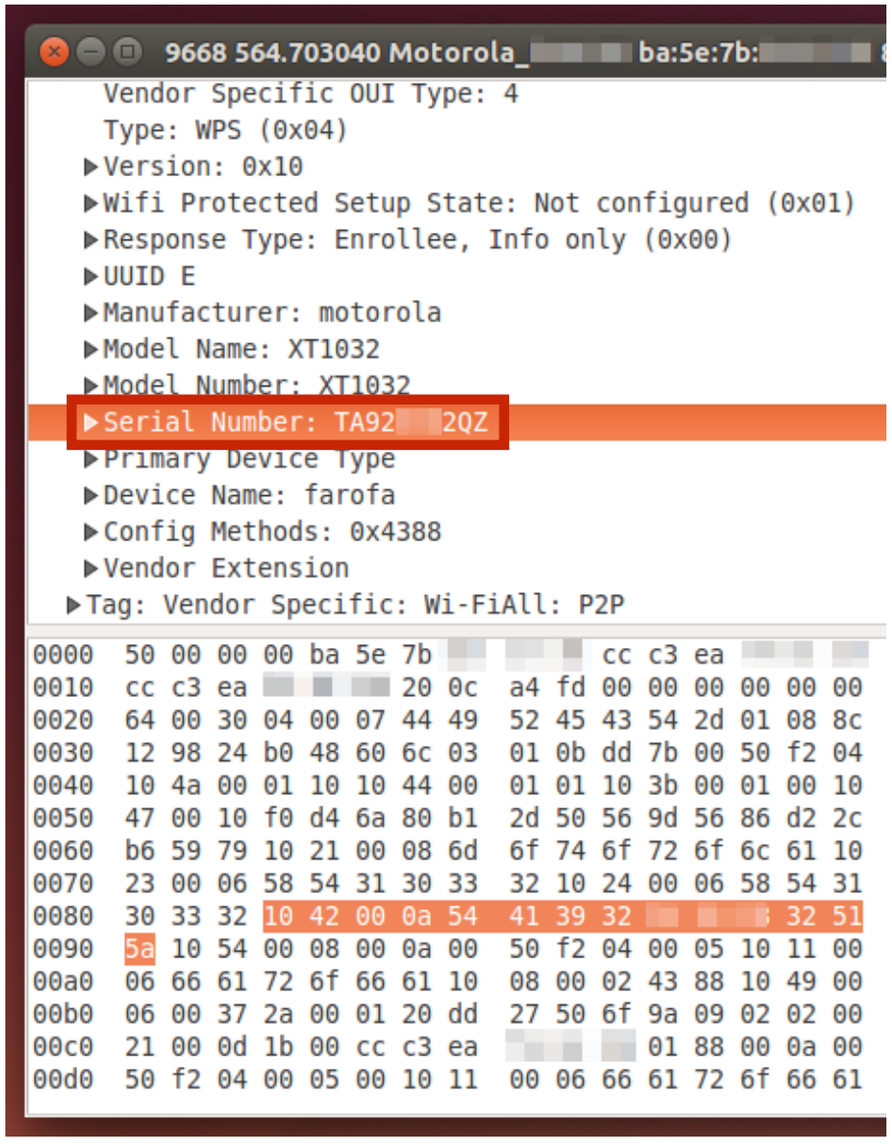
```
▶Frame 76656: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface 0
▶Radiotap Header v0, Length 26
▶IEEE 802.11 Probe Response, Flags: ........C
▼IEEE 802.11 wireless LAN management frame
 ▶Fixed parameters (12 bytes)
 ▼Tagged parameters (230 bytes)
  ▶Tag: SSID parameter set: 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
```

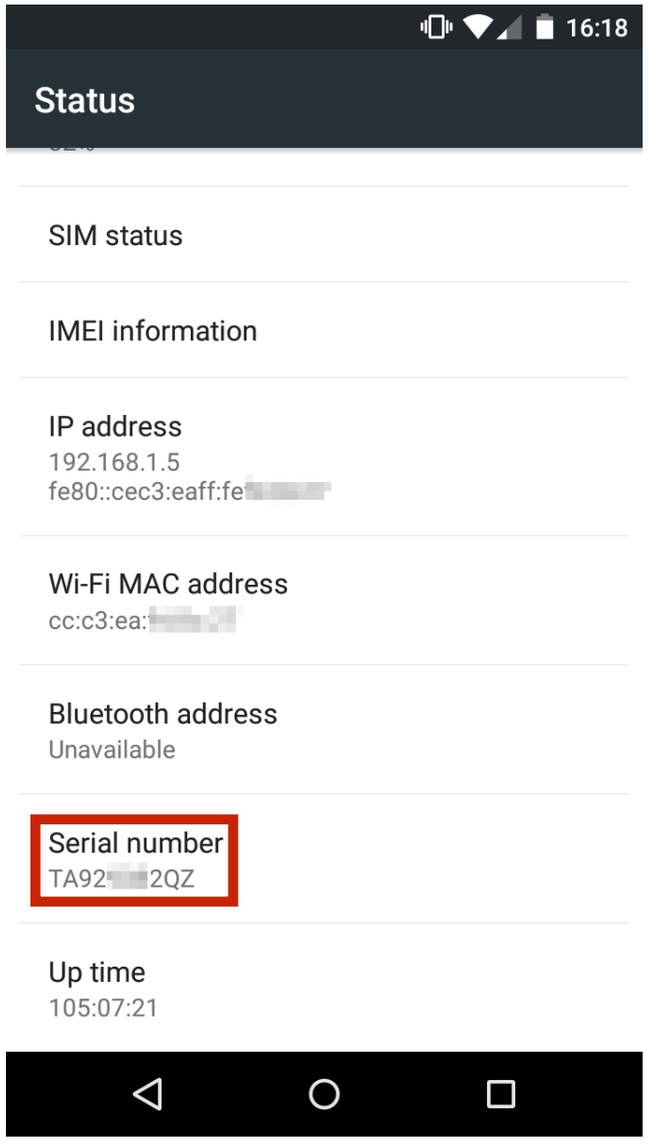
```
0000  00 00 1a 00 2f 48 00 00  32 10 f3 84 00 00 00 00   ..../H.. 2.......
0010  10 0c 6c 09 c0 00 e8 01  00 00 50 00 3c 00 cc c3   ..l..... ..P.<...
0020  ea [redacted] 02 90 a9 [redacted] 02 90 a9 [redacted]   . ... ... ...
0030  f0 54 48 6d 49 07 00 00  00 00 64 00 20 04 00 07   .THmI... ..d. ...
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

WiFi Alliance

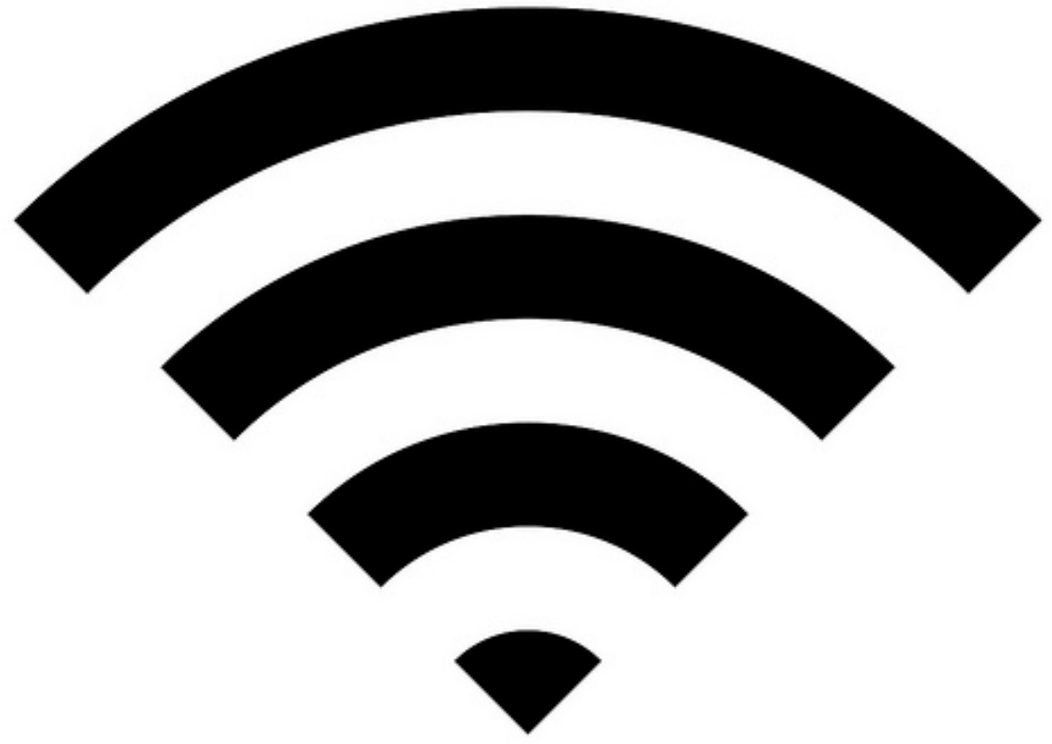




Sharing serial numbers

Protocol Complexity

WiFi Alliance



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

Endianness Nonsense

1625 349.111223 02:90:a9:67:7b:7e 00:de:ad:be:ef:00 802.11 284 Probe Response, SN=3644, FN=0,

```
    Data Element Type: Model Name (0x1023)
    Data Element Length: 10
    Model Name: WD TV Live
  ▶ Model Number: WDBHG70000NBK
  ▶ Serial Number: WNC441203527
  ▶ Primary Device Type
  ▶ Device Name: WDTVLive
  ▶ Config Methods: 0x2388
  ▶ Vendor Extension
  ▼ Tag: Vendor Specific: 50:6f:9a: P2P
    Tag Number: Vendor Specific (221)
    Tag length: 41
    OUI: 50-6f-9a
    Vendor Specific OUI Type: 9
  ▼ P2P Capability: Device 0x23  Group 0x0
    Attribute Type: P2P Capability (2)
    Attribute Length: 2
```

```
0080  65 73 74 65 72 6e 20 44  69 67 69 74 61 6c 20 43   estern D igital C
0090  6f 72 70 6f 72 61 74 69  6f 6e 10 23 00 0a 57 44   orporati on.#..WD
00a0  20 54 56 20 4c 69 76 65  10 24 00 0d 57 44 42 48    TV Live .$..WDBH
00b0  47 37 30 30 30 30 4e 42  4b 10 42 00 0c 57 4e 43   G70000NB K.B..WNC
00c0  34 34 31 32 30 33 35 32  37 10 54 00 08 00 07 00   44120352 7.T.....
00d0  50 f2 04 00 01 10 11 00  08 57 44 54 56 4c 69 76   P....... .WDTVLiv
00e0  65 10 08 00 02 23 88 10  49 00 06 00 37 2a 00 01   e....#.. I...7*..
00f0  20 dd 29 50 6f 9a 09 02  02 00 23 00 0d 1d 00 02    .)Po... ..#.....
0100  90 a9 67 7b 7e 01 88 00  07 00 50 f2 04 00 01 00   ..g{~... ..P.....
0110  10 11 00 08 57 44 54 56  4c 69 76 65               ....WDTV Live
```

Big-endian is the most common format in data networking

Protocol Complexity

Apple

Protocol Complexity

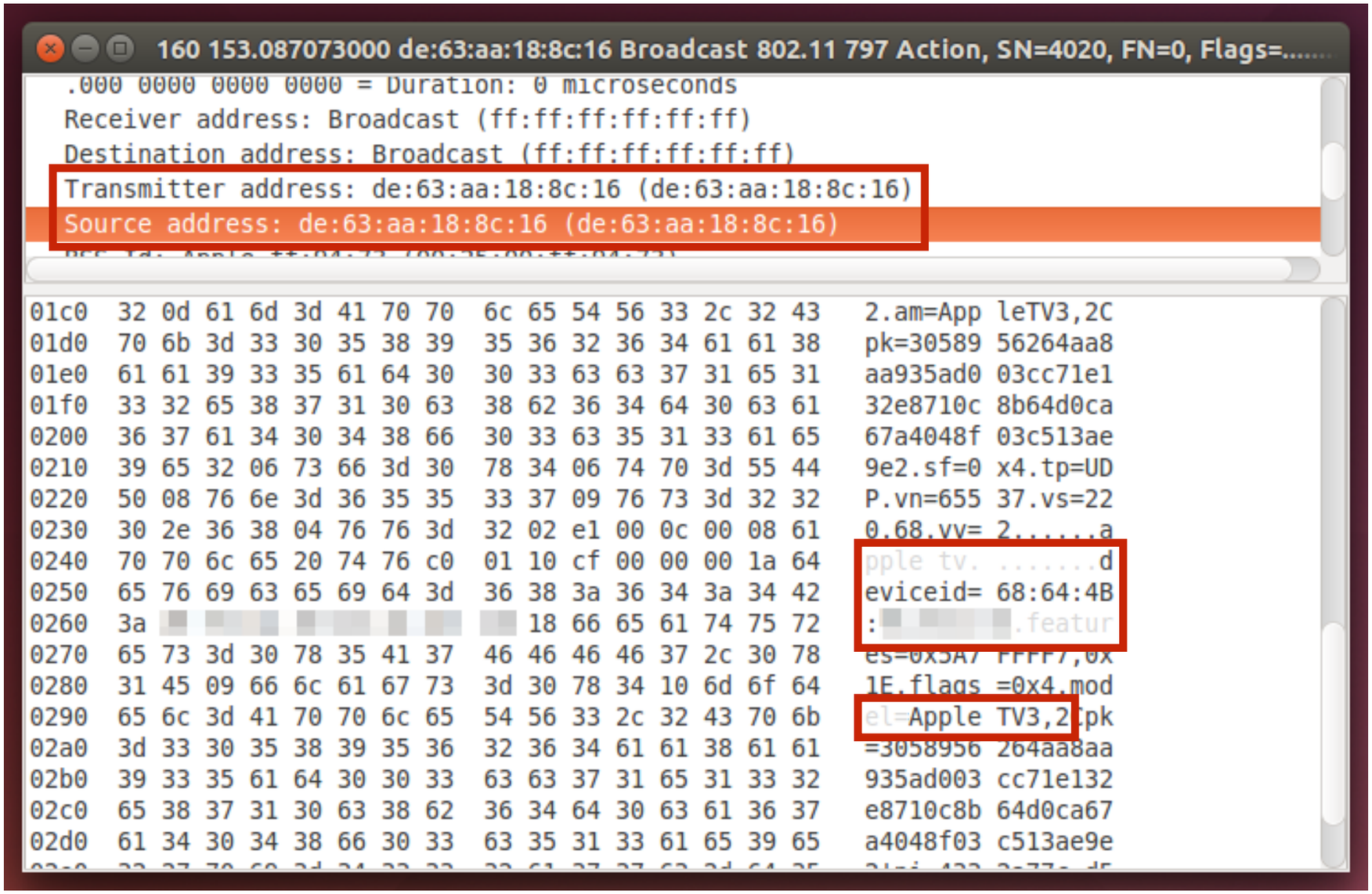
Apple

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

Apple



AirPlay action frame from an AppleTV 3rd Generation

Protocol Complexity

Apple

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

Apple

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

```
▶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

Messy Implementations

WD TV Live Media Player

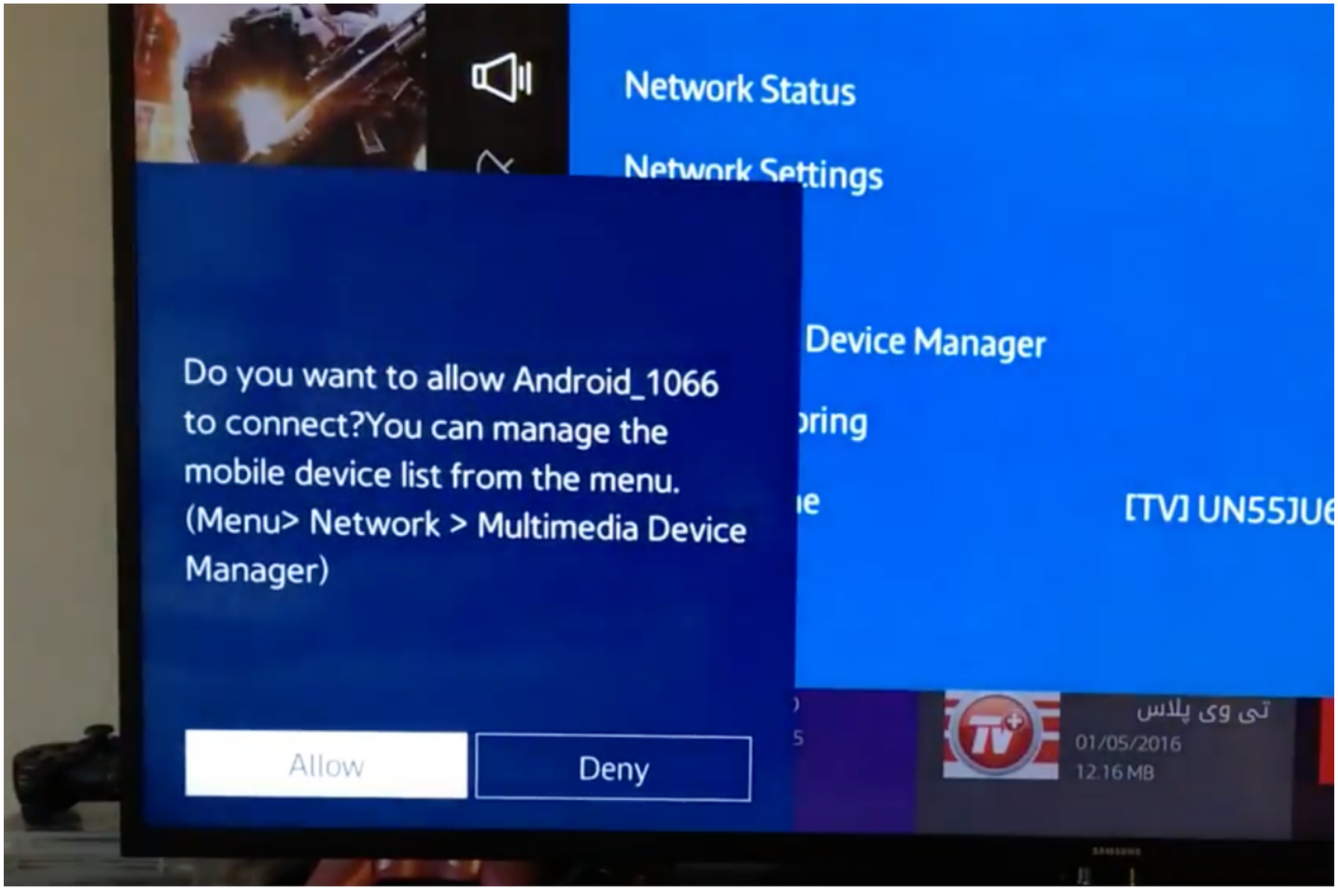
Protocol Complexity

Messy Implementations

WD TV Live Media Player has WiFi Direct enabled by default

Protocol Complexity

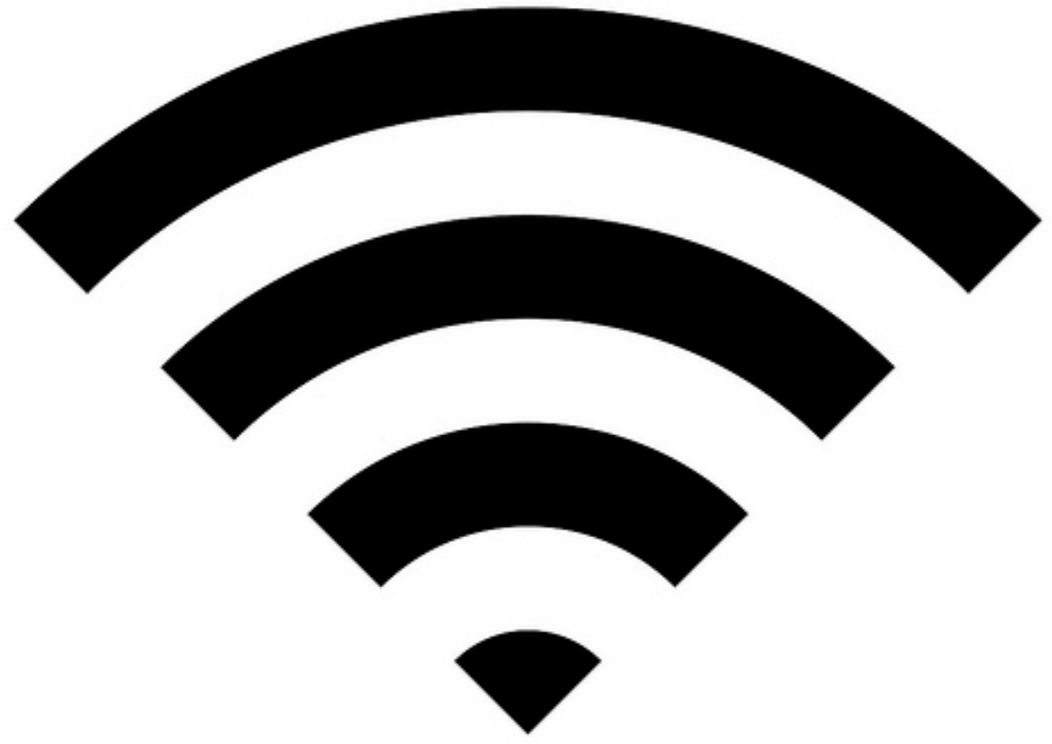
Messy Implementations



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

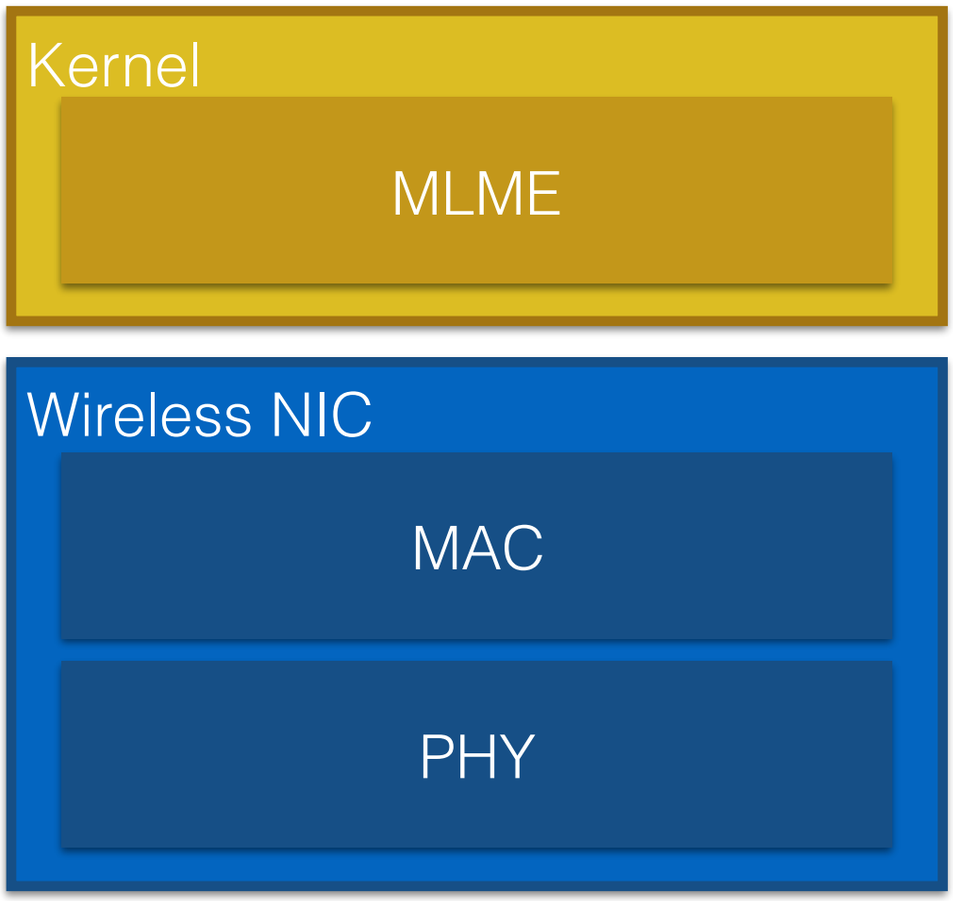
MLME stands for MAC Layer Management Entity. Examples of states a MLME may assist in reaching:

- 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

- No symbols, bare metal binary.
- Shared code with some kernel modules.
- Segment on chipset ROM.

Kernel modules

- Open Source. **
- Kernel debugging & debug parameters.

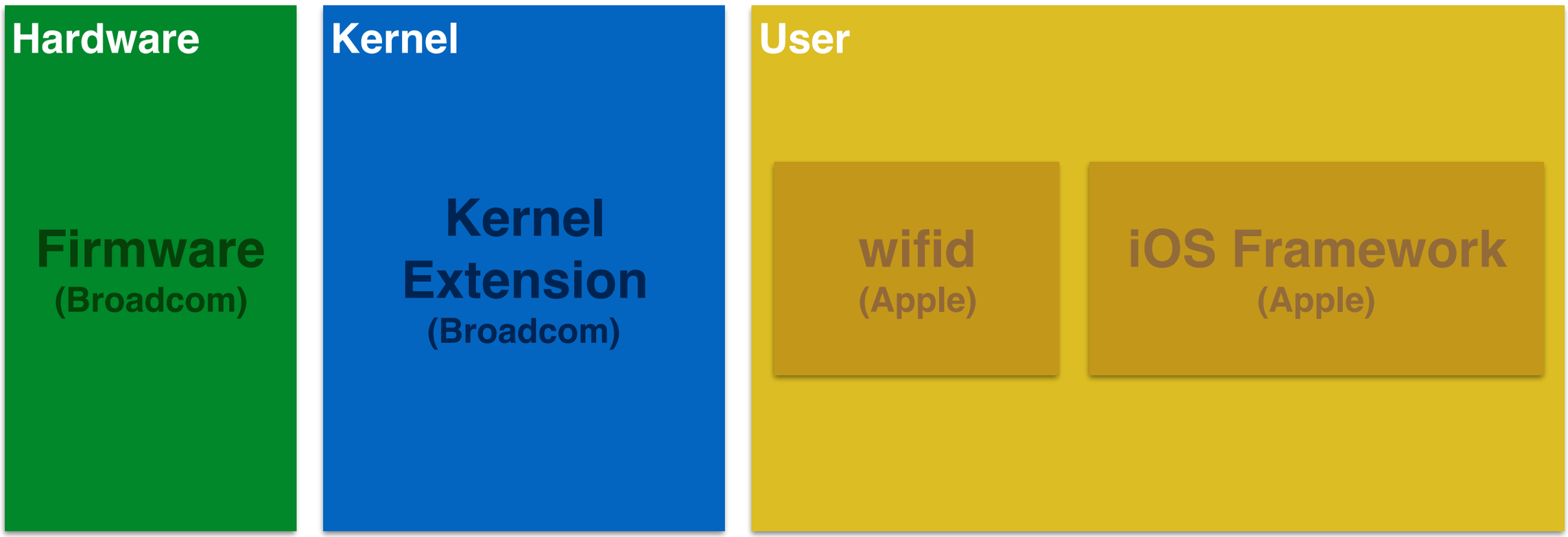
wpa_supplicant & hostapd

- Open Source.
- Debugging & client interaction.

Framework

- Open Source.
- Debugging & Log analysis.

Platform Complexity



Platform Complexity

Firmware

- No symbols, bare metal binary.
- Shared code with OS X kernel extension.
- Segment on chipset ROM.

Kernel extensions

- Encrypted kernel. **
- Shared code between OS X and iOS.

wifid

- Handles more than 802.11 functionality.

Framework

- Private framework.

Conclusions

- Specifications or proprietary protocols could help device fingerprinting.
- Specifications or proprietary protocols could break privacy features such as MAC address randomization.
- Bad implementations could expose devices to unauthenticated access.
  - WD TV Live Streaming Media Player Wi-Fi Direct Unauthenticated Access - http://neseso.com/advisories/NESESO-2016-0910.pdf
- Protocol and platform complexity could lead to vulnerabilities.
  - Broadcom BCM4325 and BCM4329 wireless chipset denial-of-service vulnerability - CVE-2012-2619
  - Android WiFi-Direct DoS - CVE-2014-0997

Future Work

- Research other platforms and vendors.

- Implement Apple Bluetooth Low Energy scanning protocol on Ubertooth and extend the reverse engineering on Apple proprietary protocols.

- Develop a 802.11 information gathering tool.

Questions

WIG Project Repository

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

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