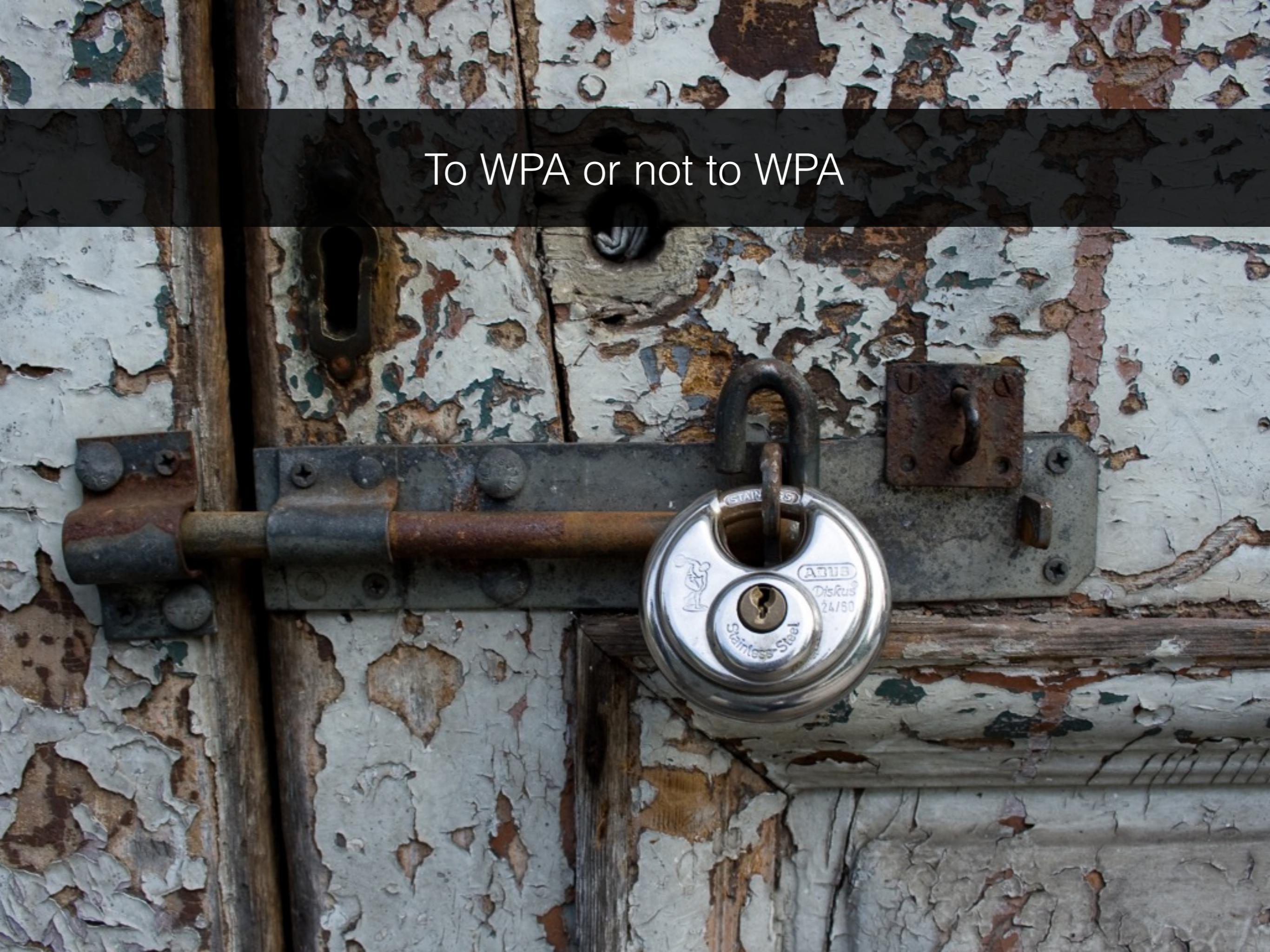




802.11 Protocol Chaos

Andrés Blanco

A close-up photograph of a weathered metal door. The surface is covered in white and brown peeling paint. A large, silver stainless steel padlock is attached to a metal handle. The door has a dark, textured background.

To WPA or not to WPA

IEEE 802.11 frame types and subtypes

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

Management frames are used for various link-layer maintenance functions

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



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



FullMAC is a term used to describe a type of Wireless NIC where the MAC is managed in hardware



Type	Length	Value
1 byte	1 byte	1-255 byte

Management frames use information elements structures to communicate information

Type 0x00	Length 0x00-0x20	Value
1 byte	1 byte	0-32 byte/s

SSID information element

Type 0x30	Length 0x00-0xff	Version 2 bytes	Group Cipher Suite 4 bytes	Pairwise Cipher Suite Count 2 bytes	Pairwise Cipher Suite 4 x N bytes	Auth. Suite Count 2 bytes	...
1 byte	1 byte	2 bytes	4 bytes	2 bytes	4 x N bytes	2 bytes	...
.....							
...	Auth. Suite 4 x N bytes	RSN Capa. 2 bytes	PMK Count 2 bytes	PMK List 16 x N bytes			
.....							

RSN information element

Wireshark

► Frame 1165: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface 0
► Radiotap Header v0, Length 36
► 802.11 radio information
▼ IEEE 802.11 Beacon frame, Flags:C
 Type/Subtype: Beacon frame (0x0008)
 ► Frame Control Field: 0x8000
 ..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: fa:fa:fa:fa:fa:fa (fa:fa:fa:fa:fa:fa)
 Source address: fa:fa:fa:fa:fa:fa (fa:fa:fa:fa:fa:fa)
 BSS Id: fa:fa:fa:fa:fa:fa
 0000 = Fragment number: 0
 0111 0011 1100 = Sequence number: 1852
 ► Frame check sequence: 0xc201c58e [correct]
▼ IEEE 802.11 wireless LAN management frame
 ► Fixed parameters (12 bytes)
 ▼ Tagged parameters (43 bytes)
 ► Tag: SSID parameter set:fafafa
 ► Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
 ► Tag: DS Parameter set: Current Channel: 6
 ▼ Tag: RSN Information
 Tag Number: RSN Information (48)
 Tag length: 20
 RSN Version: 1
 ► Group Cipher Suite: 00-0f-ac AES (CCM)
 Pairwise Cipher Suite Count: 1
 ► Pairwise Cipher Suite List 00-0f-ac AES (CCM)
 ► Auth Key Management (AKM) Suite Count: 65535
 ► Auth Key Management (AKM) List 00-0f-ac PSK
 ► RSN Capabilities: 0x0000

CVE-2012-2619

No.: 1165 · Time: 16.092353220 · Source: fa:fa:fa:fa:fa:fa · Deacon frame, SN=1852, FN=0, Flags=.....C, BI=100, SSID=fafafa

Close

Help



**FREE
AIR**

Free information

Cisco Client Extensions

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.

Wireshark ·

- ▶ Frame 6440: 253 bytes on wire (2024 bits), 253 bytes captured (2024 bits)
- ▶ IEEE 802.11 Beacon frame, Flags:
- ▼ IEEE 802.11 wireless LAN management frame
 - ▶ Fixed parameters (12 bytes)
 - ▼ Tagged parameters (217 bytes)
 - ▶ Tag: SSID parameter set: \000
 - ▶ 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 (241:1)
 - ▶ 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-DISASTER-AP
 - Clients: 17
 - Unknown2: 00003c
 - ▶ Tag: Vendor Specific: Aironet: Aironet DTPC Powerlevel 0x0B
 - ▶ Tag: Vendor Specific: Microsoft: WMM/WME: Parameter Element
 - ▶ Tag: Vendor Specific: Aironet: Aironet Unknown (1) (1)
 - ▶ Tag: Vendor Specific: Aironet: Aironet CCX version = 5
 - ▶ Tag: Vendor Specific: Aironet: Aironet Unknown (11) (11)
 - ▶ Tag: Vendor Specific: Aironet: Aironet Unknown (19)
 - ▶ Tag: Vendor Specific: Aironet: Aironet Client MFP Enabled

No.: 6440 · Time: 115.444978 · Source: CiscoInc_82:e7...ame, SN=2769, FN=0, Flags=....., BI=102, SSID=\000

[Help](#) [Close](#)

Wireshark ·

▼ Tag: Cisco CCX1 CKIP + Device Name

Tag Number: Cisco CCX1 CKIP + Device Name (133)

Tag length: 30

Unknown: 05008f000f00ff035900

Name: B73-SIMPSON-AP0

Clients: 0

Unknown2: 00003c

CCX Information Elements

Help

Close

Wireshark ·

▼ Tag: Cisco CCX1 CKIP + Device Name

Tag Number: Cisco CCX1 CKIP + Device Name (133)

Tag length: 30

Unknown: 05008f000f00ff035900

Name: B69-BEETLEJUICE

Clients: 2

Unknown2: 00003c

No.: 328521 · Time: 3299.440884 · Source: CiscoInc...e, SN=3438, FN=0, Flags=....., BI=102, SSID=|000

Help

Close

Wireshark ·

▼ Tag: Cisco CCX1 CKIP + Device Name

Tag Number: Cisco CCX1 CKIP + Device Name (133)

Tag length: 30

Unknown: 01008f000f00ff035900

Name: B131-MIB-AP19oq

Clients: 5

Unknown2: 00003c

No.: 1134905 · Time: 9237.507955 · Source: CiscoInc...e, SN=3048, FN=0, Flags=....., BI=102, SSID=|000

Help

Close

Wireshark ·

- ▶ Frame 10458: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits)
- ▶ IEEE 802.11 Reassociation Response, Flags:
- ▼ IEEE 802.11 wireless LAN management frame
 - ▶ Fixed parameters (6 bytes)
 - ▼ Tagged parameters (143 bytes)
 - ▶ Tag: Supported Rates 36(B), 48, 54, [Mbit/sec]
 - ▶ Tag: Extended Supported Rates 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
 - ▶ Tag: HT Capabilities (802.11n D1.10)
 - ▶ 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: 004096000a0f03010000
 - Name: B67-DISASTER-AP
 - Clients: 0
 - Unknown2: 00003c
 - ▼ Tag: Cisco Unknown 95: Undecoded
 - ▶ Tag Number: Cisco Unknown 95 (149)
 - Tag length: 10
 - Tag Data: 004096000a0f03010000
 - ▶ Tag: Vendor Specific: Aironet: Aironet CCX version = 5
 - ▶ Tag: Vendor Specific: Microsoft: WMM/WME: Parameter Element

Wireless LAN Controller

No.: 10458 · Time: 134.577591 · Source: CiscoInc_82:e... Reassociation Response, SN=142, FN=0, Flags=.....

Help Close

0a 0f 03 01

Wireshark ·

Frame 166846: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)

IEEE 802.11 Reassociation Request, Flags:

Type/Subtype: Reassociation Request (0x0002)

Frame Control Field: 0x2000
.000 0000 0010 1000 = Duration: 40 microseconds

Receiver address: [REDACTED]

Destination address: [REDACTED]

Transmitter address: 00:de:ad:be:ef:00 (00:de:ad:be:ef:00)

Source address: 00:de:ad:be:ef:00 (00:de:ad:be:ef:00) **Selected**

BSS Id: CiscoInc_53:85:f7 (68:86:a7:53:85:f7)

..... 0000 = Fragment number: 0

0011 1001 0000 = Sequence number: 912

IEEE 802.11 wireless LAN management frame

Fixed parameters (10 bytes)

Tagged parameters (222 bytes)

Tag: SSID parameter set: Usuarios

Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]

Tag: DS Parameter set: Current Channel: 6

Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap

Tag: Country Information: Country Code AR, Environment Any

Tag: QBSS Load Element 802.11e CCA Version

Tag: ERP Information

Tag: HT Capabilities (802.11n D1.10)

Tag: RSN Capabilities

Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]

Tag: HT Information (802.11n D1.10)

Tag: Cisco CCX1 CKIP + Device Name

Tag: Vendor Specific: Aironet: Aironet DTPC Powerlevel 0x11

Tag: Vendor Specific: Microsoft: WMM/WME: Parameter Element

Tag: Vendor Specific: Aironet: Aironet Unknown (1) (1)

Tag: Vendor Specific: Aironet: Aironet CCX version = 5

Tag: Vendor Specific: Aironet: Aironet Unknown (11) (11)

No.: 166846 · Time: 1741.313941 · Source: 00:de:ad:be:ef:00 · Destination: 00:de:ad:be:ef:00 · Type/Subtype: Reassociation Request, SN=912, FN=0, Flags=....., SSID=Usuarios

Help Close

Wireshark

Frame 166851: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)

IEEE 802.11 Reassociation Response, Flags:R...

Type/Subtype: Reassociation Response (0x0003)

Frame Control Field: 0x3008

.000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: 00:de:ad:be:ef:00 (00:de:ad:be:ef:00)

Destination address: 00:de:ad:be:ef:00 (00:de:ad:be:ef:00)

Transmitter address:

Source address:

BSS Id:

.... 0000 = Fragment number: 0

1000 0011 1111 = Sequence number: 2111

IEEE 802.11 wireless LAN management frame

Fixed parameters (6 bytes)

Capabilities Information: 0x0431

Status code: Successful (0x0000)

..00 0000 1001 1101 = Association ID: 0x009d

Tagged parameters (81 bytes)

Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]

Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]

Tag: Cisco CCX1 CKIP + Device Name

Tag: Cisco Unknown 95: Undecoded

Tag Number: Cisco Unknown 95 (149)

Tag length: 10

Tag Data: 00409600ac1c11990000

Tag: Vendor Specific: Aironet: Aironet CCX version = 5

Tag: Vendor Specific: Aironet: Aironet Unknown (11) (11)

Tag: Vendor Specific: Aironet: Aironet Client MFP Enabled

No.: 166851 · Time: 1741.337402 · Source: ...nfo: Reassociation Response, SN=2111, FN=0, Flags=....R...

Help Close



WPS & WiFi-Direct

Wireshark

- ▶ Radiotap Header v0, Length 36
- ▶ 802.11 radio information
- ▶ IEEE 802.11 Probe Response, Flags:R...C
- ▶ IEEE 802.11 wireless LAN management frame
 - ▶ Fixed parameters (12 bytes)
 - ▶ Tagged parameters (319 bytes)
 - ▶ Tag: SSID parameter set: (T_T)
 - ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
 - ▶ Tag: DS Parameter set: Current Channel: 10
 - ▶ Tag: ERP Information
 - ▶ Tag: ERP Information
 - ▶ Tag: RSN Information
 - ▶ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
 - ▶ Tag: HT Capabilities (802.11n D1.10)
 - ▶ Tag: HT Information (802.11n D1.10)
 - ▶ Tag: Overlapping BS (Shorter Parameter) Unsupp. (Unsupp.)
 - ▶ Tag: Extended Capabilities (8 octets)
 - ▶ Tag: Vendor Specific: Microsoft WPS
 - Tag Number: Vendor Specific (221)
 - Tag length: 134
 - OUI: 00-50-f2
 - Vendor Specific OUI Type: 4
 - Type: WPS (0x04)
 - ▶ Version: 0x10
 - ▶ Wifi Protected Setup State: Configured (0x02)
 - ▶ Ap Setup Locked: 0x01
 - ▶ Response Type: AP (0x03)
 - ▶ UUID E
 - ▶ Manufacturer: NETGEAR, Inc.
 - ▶ Model Name: R6300v2
 - ▶ Model Number: R6300v2
 - ▶ Serial Number: 679
 - ▶ Primary Device Type
 - ▶ Device Name: R6300v2
 - ▶ Config Methods: 0x2008
 - ▶ RF Bands: 2.4 and 5 GHz (0x03)
 - ▶ Vendor Extension

No.: 102 · Time: 10.051742250 · Source: Netgear 03:84:64 · Destination: Response, SN=3467, FN=0, Flags=....R...C, BI=100, SSID=(T T)

Close

Help

Wireshark

- ▶ Frame 4031: 334 bytes on wire (2672 bits), 334 bytes captured (2672 bits) on interface 0
- ▶ Radiotap Header v0, Length 36
- ▶ 802.11 radio information
- ▶ IEEE 802.11 Probe Response, Flags:
- ▶ IEEE 802.11 wireless LAN management frame
 - ▶ Fixed parameters (12 bytes)
 - ▶ Tagged parameters (258 bytes)
 - ▶ Tag: SSID parameter set: ciscosb
 - ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
 - ▶ Tag: DS Parameter set: Current Channel: 1
 - ▶ Tag: Country Information: Country Code US, Environment Any
 - ▶ Tag: ERP Information
 - ▶ Tag: ERP Information
 - ▶ Tag: RSN Information
 - ▶ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
 - ▶ Tag: Vendor Specific: Microsoft: WPS
 - Tag Number: Vendor Specific (221)
 - Tag length: 155
 - OUI: 00-50-f2
 - Vendor Specific OUI Type: 4
 - Type: WPS (0x04)
 - ▶ Version: 0x10
 - ▶ Wifi Protected Setup State: Not configured (0x01)
 - ▶ Response Type: AP (0x03)
 - ▶ UUID E
 - ▶ Manufacturer: Cisco Small Business
 - ▶ Model Name: WAP121
 - ▶ Model Number: SER192401TV
 - ▶ Serial Number: SER192401TV
 - ▶ Primary Device Type
 - ▶ Device Name: Cisco-AP :7B:40

WPS and serial numbers

No.: 403 ciscosb

Close Help

Wireshark

- ▶ Frame 154: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface wireless
- ▶ Radiotap Header v0, Length 36
- ▶ 802.11 radio information
- ▶ IEEE 802.11 Probe Response, Flags:C
- ▼ IEEE 802.11 wireless LAN management frame
 - ▶ Fixed parameters (12 bytes)
 - ▼ Tagged parameters (319 bytes)
 - ▶ Tag: SSID parameter set: (T_T)
 - ▶ Tag: Supported Rates 1(B), 2(B), 5.5, 11, 18, 24, 36, 54, [Mbit/sec]
 - ▶ Tag: DS Parameter set: Current Channel: 10
 - ▶ Tag: ERP Information
 - ▶ Tag: ERP Information
 - ▶ Tag: RSN Information
 - ▶ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
 - ▶ Tag: QBSS Load Element 802.11e CCA Version
 - ▶ Tag: HT Capabilities (802.11n D1.10)
 - ▶ Tag: HT Information (802.11n D1.10)
 - ▶ Tag: Overlapping BSS Scan Parameters: Undecoded
 - ▶ Tag: Extended Capabilities (8 octets)
 - ▼ Tag: Vendor Specific: Microsoft WPS
 - ▶ Tag Number: Vendor Specific (221)
 - ▶ Tag length: 134
 - ▶ OUI: 00-50-f2
 - ▶ Vendor Specific OUI Type: 4
 - ▶ Type: WPS (0x04)
 - ▶ Version: 0x10
 - ▶ Wifi Protected Setup State: Configured (0x02)
 - ▶ Ap Setup Locked: 0x01
 - ▶ Response Type: AP (0x03)
 - ▶ UUID E
 - ▶ Manufacturer: NETGEAR, Inc.
 - ▶ Model Name: R6300v2
 - ▶ Model Number: R6300v2
 - ▶ Serial Number: 679
 - ▶ Primary Device Type
 - ▶ Device Name: R6300v2
 - ▶ Config Methods: 0x2000

Is there any way to avoid this?

No.: 154 · Time: 14.948878043 · Source: Netgear 03:84:64 ...sponse, SN=3019, FN=0, Flags=.....C, BI=100, SSID=(T T)

[Close](#) [Help](#)

Disabling WPS?

The screenshot shows the NETGEAR Router R6300v2 configuration page in a Chromium browser window. The title bar reads "NETGEAR Router R6300v2 - Chromium". The main header features the "NETGEAR® genie" logo and the model "R6300v2". The navigation menu on the left includes links for "ADVANCED Home", "Setup Wizard", "WPS Wizard", "Setup", "USB Storage", "Security", "Administration", and "Advanced Setup". The "ADVANCED" tab is selected. The main content area displays "Wireless Settings (2.4GHz)" and "Wireless Settings (5GHz)". Both sections show the following parameters:

Name (SSID)	[Redacted]
Region	North America
Channel	10
Mode	Up to 450 Mbps
Wireless AP	On
Broadcast Name	On
Wi-Fi Protected Setup	Not Configured

Wireless Settings (5GHz)

Name (SSID)	[Redacted]
Region	North America
Channel	149 + 153(P) + 157 + 161
Mode	Up to 1300 Mbps
Wireless AP	On
Broadcast Name	On
Wi-Fi Protected Setup	Not Configured

Guest Network (2.4 GHz)

Name (SSID)	Guest
Wireless AP	Off

Guest Network (5 GHz)

Name (SSID)	Invitados
Wireless AP	On

Wireshark

- ▶ Fixed parameters (12 bytes)
- ▼ Tagged parameters (319 bytes)
 - ▶ Tag: SSID parameter set: (T_T)
 - ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
 - ▶ Tag: DS Parameter set: Current Channel: 10
 - ▶ Tag: ERP Information
 - ▶ Tag: ERP Information
 - ▶ Tag: RSN Information
 - ▶ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
 - ▶ Tag: QBSS Load Element 802.11e CCA Version
 - ▶ Tag: HT Capabilities (802.11n D1.10)
 - ▶ Tag: HT Information (802.11n D1.10)
 - ▶ Tag: Overlapping BSS Scan Parameters: Undecoded
 - ▶ Tag: Extended Capabilities (8 octets)
 - ▼ Tag: Vendor Specific: Microsoft: WPS
 - Tag Number: Vendor Specific (0x01)
 - Tag length: 134
 - OUI: 00-50-f2
 - Vendor Specific OUI Type: 4
 - Type: WPS (0x04)
 - ▶ Version: 0x10
 - ▶ Wifi Protected Setup State: Not configured (0x01)
 - ▶ Ap Setup Locked: 0x01
 - ▶ Response Type: AP (0x03)
 - ▶ UUID E
 - ▶ Manufacturer: NETGEAR, Inc.
 - ▶ Model Name: R6300v2
 - ▶ Model Number: R6300v2
 - ▶ Serial Number: 679
 - ▶ Primary Device Type
 - ▶ Device Name: R6300v2
 - ▶ Config Methods: 0x2008
 - ▶ RF Bands: 2.4 and 5 GHz (0x03)
 - ▶ Vendor Extension
 - ▶ Tag: Vendor Specific: Broadcom
 - ▶ Tag: Vendor Specific: Microsoft: WMM/WME: Parameter Element
 - ▶ Tag: RM Enabled Capabilities (5 octets)

Disabling WPS like a boss

No.: 4129 · Time: 47.808258270 · Source: Netgear 03:84:64 · Destin...Probe Response, SN=2216, FN=0, Flags=....R...C, BI=100, SSID=(T T)

Close

Help

Wireshark

- ▶ Fixed parameters (12 bytes)
- ▼ Tagged parameters (264 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: 10
 - ▼ Tag: Vendor Specific: Microsoft: WPS
 - Tag Number: Vendor Specific (221)
 - Tag length: 163
 - OUI: 00-50-f2
 - Vendor Specific OUI Type: 4
 - Type: WPS (0x04)
 - ▶ Version: 0x10
 - ▶ Wifi Protected Setup State: Not configured (0x01)
 - ▶ Device Password ID: PIN (default) (0x0000)
 - ▶ Response Type: Enrollee, Info only (0x00)
 - ▶ UUID E
 - ▶ Manufacturer: Western Digital Corporation
 - ▶ 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: Wi-FiAll: P2P
 - Tag Number: Vendor Specific (221)
 - Tag length: 41
 - OUI: 50-6f-9a
 - Vendor Specific OUI Type: 9
 - ▶ P2P Capability: Device 0x23 Group 0x0
 - ▶ P2P Device Info
- ▶ Tag: Vendor Specific: Wi-FiAll: Wi-Fi Display

No.: 716 · Time: 17.646745 · Source: 02:90:a9:67:7b:7e · Destin...be Response, SN=667, FN=0, Flags=....., BI=100, SSID=DIRECT-

Help WiFi-Direct Close

Wireshark

► Frame 244847: 417 bytes on wire (3336 bits), 417 bytes captured (3336 bits)
► IEEE 802.11 Beacon frame, Flags:,
▼ IEEE 802.11 wireless LAN management frame
 ► Fixed parameters (12 bytes)
 ▼ Tagged parameters (381 bytes)
 ► Tag: SSID parameter set: DIRECT-24-HP DeskJet 3630 series
 ► Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
 ► Tag: DS Parameter set: Current Channel: 1
 ► Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
 ► Tag: Power Constraint: 0
 ► Tag: TPC Report Transmit Power: 17, Link Margin: 0
 ► Tag: ERP Information
 ► Tag: ERP Information
 ► Tag: RSN Information
 ► Tag: HT Capabilities (802.11n D1.10)
 ► Tag: HT Information (802.11n D1.10)
 ► Tag: Vendor Specific: Broadcom
 ► Tag: Vendor Specific: Microsoft WMM/WME: Parameter Element
 ► Tag: Vendor Specific: Wi-FiAll: P2P
 ► Tag: Vendor Specific: Microsoft: WPS
 ▼ Tag: Vendor Specific: HP
 Tag Number: Vendor Specific (221)
 Tag length: 98
 OUI: 08-00-09
 Vendor Specific OUI Type: 0
 Vendor Specific Data: 0004000000170102010003144465736b4a65742033363330...

No.: 244847 · Time: 3677.236609 · Source: ...gs=....., BI=100, SSID=DIRECT-24-HP DeskJet 3630 series

Help

Close

Information Elements for everyone

```
root@null-vm:~$ 

SSID: FC:3F:DB:98:9D:42
0000  00 04 00 00 00 17 01 02 01 00 03 14 44 65 73 6b      .....Desk
0010  4a 65 74 20 33 36 33 30 20 73 65 72 69 65 73 00      Jet 3630 series.
0020  04 05 33 36 33 30 00 05 10 43 4e 36 33 37 33 4e      ..3630...CN6373N
0030  32 35 51 30 36 37 50 00 00 06 10 1c 85 2a 4d b8      25Q067P.....*M.
0040  00 1f 08 ab cd fc 3f db 98 5f 24 07 04 c0 a8 00      .....?...$_.....
0050  99 08 02 00 c4 09 02 00 08 0a 04      .....

Status Bitfield: '\x00\x00\x00\x17' - 23
- Station is on.
- Station is configured.
- Station is connected.
- Station doesn't support 5GHz.
- USB connected to host.
AWC version: 1.0
Model Name: DeskJet 3630 series
Product SKU: 3630
Serial Number: CN6373N25Q067P
UUID: 1C852A4DB8001F08ABCDFA3FDB985F24
IPv4 Address: 192.168.0.153
```

Information Elements for everyone

```
► Frame 600: 815 bytes on wire (6520 bits), 815 bytes captured (6520 bits)
  ► Radiotap Header v0, Length 36
  ► 802.11 radio information
  ▼ IEEE 802.11 Action, 51 bytes
    Type/Subtype: Action (0x0000)
    ► Frame Control Field: 0xd000
      .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: 9e:ae:17:fd:e4:3b (9e:ae:17:fd:e4:3b)
      Source address: 9e:ae:17:fd:e4:3b (9e:ae:17:fd:e4:3b)
      BSS Id: Apple_ff:94:73 (00:25:00:ff:94:73)
      .... .... 0000 = Fragment number: 0
      1100 1001 1001 .... = Sequence number: 3225
    ► Frame check sequence: 0xf3580425 [correct]
  ► IEEE 802.11 wireless LAN management frame
  ► [Malformed Packet: IEEE 802.11]
```

01c0	46 46 37 2c 30 78 45 08 6d 64 3d 30 2c 31 2c 32	FF7, 0xE. md=0,1,2
01d0	0d 61 6d 3d 41 70 70 6c 65 54 56 33 2c 31 43 70	.am=Appl eTV3,1Cp
01e0	6b 3d 37 62 36 33 33 37 61 38 37 64 62 62 36 30	k=7b6337 a87dbb60
01f0	30 36 66 65 63 66 30 30 37 30 30 34 66 33 62 30	06fecf00 7004f3b0
0200	62 31 34 65 32 38 65 31 66 64 39 31 30 64 36 62	b14e28e1 fd910d6b
0210	63 33 33 39 64 39 31 34 39 30 39 34 65 63 62 61	c339d914 9094ecba
0220	65 64 06 73 66 3d 30 78 34 06 74 70 3d 55 44 50	ed.sf=0x 4.tp=UDP
0230	08 76 6e 3d 36 35 35 33 37 09 76 73 3d 32 32 30	.vn=6553 7.vs=220
0240	2e 36 38 04 76 76 3d 32 02 e0 00 0c 00 08 61 70	.68.vv=2ap
0250	70 6c 65 20 74 76 c0 01 10 ce 00 00 00 1a 64 65	ple tv..de
0260	76 69 63 65 69 64 3d 37 43 3a 44 31 3a 43 33 3a	viseid=7 C:D1:C3:
0270	32 36 3a 35 34 3a 44 31 17 66 65 61 74 75 72 65	26:54:D1 .feature
0280	73 3d 30 78 35 41 37 46 46 46 46 37 2c 30 78 45	s=0x5A7F FFF7, 0xE
0290	09 66 6c 61 67 73 3d 30 78 34 10 6d 6f 64 65 6c	.flags=0 x4.model
02a0	3d 41 70 70 6c 65 54 56 33 2c 31 43 70 6b 3d 37	=AppleTV 3,1Cpk=7
02b0	62 36 33 33 37 61 38 37 64 62 62 36 30 30 36 66	b6337a87 dbb6006f
02c0	65 63 66 30 30 37 30 30 34 66 33 62 30 62 31 34	ecf00700 4f3b0b14

Wireshark ·

► Frame 342226: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits)

► IEEE 802.11 Probe Response, Flags:

▼ IEEE 802.11 IEEE 802.11 management frame

► Fixed parameters (12 bytes)

▼ Tagged parameters (408 bytes)

► Tag: SSID parameter set: DIRECT-R3Samsung Wireless Audio

► Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]

► Tag: DS Parameter set: Current Channel: 11

► Tag: ERP Information

► Tag: HT Capabilities (802.11n D1.10)

► Tag: HT Information (802.11n D1.10)

► Tag: RSN Information

► Tag: Vendor Specific: Microsoft WMM/WME: Parameter Element

► Tag: Vendor Specific: Microsoft WPS

▼ Tag: Vendor Specific: 00:2d:25

 Tag Number: Vendor Specific (221)

 Tag length: 56

 OUI: 00-2d-25 ()

 Vendor Specific OUI Type: 32

 Vendor Specific Data: 2000310010c0a80103244b0378f417264b0378f417c0ffd4...

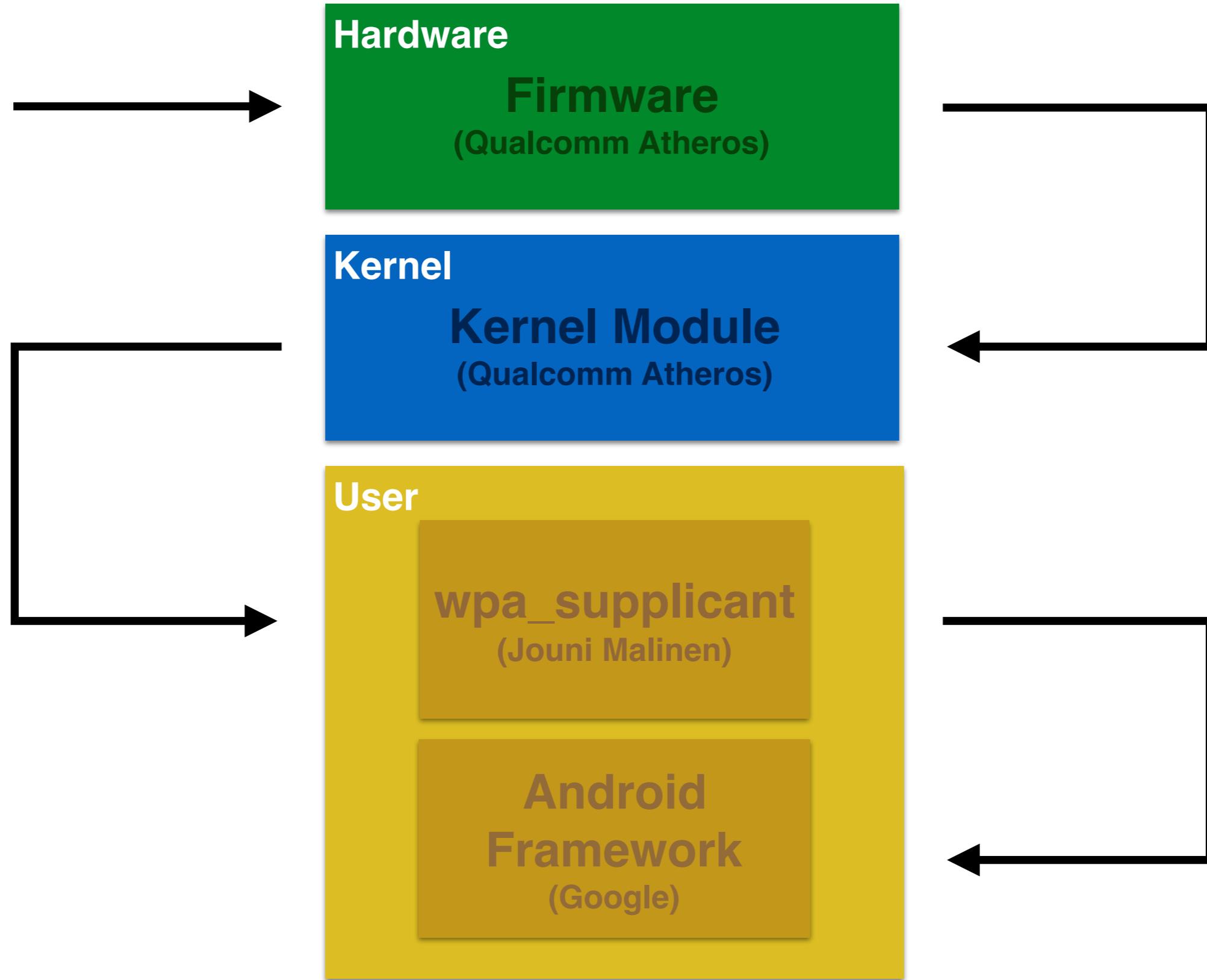
► Tag: Vendor Specific: Wi-FiAll: P2P

No.: 342226 · Time: 4767.736327 · Source: ...lags=....., BI=100, SSID=DIRECT-R3Samsung Wireless Audio

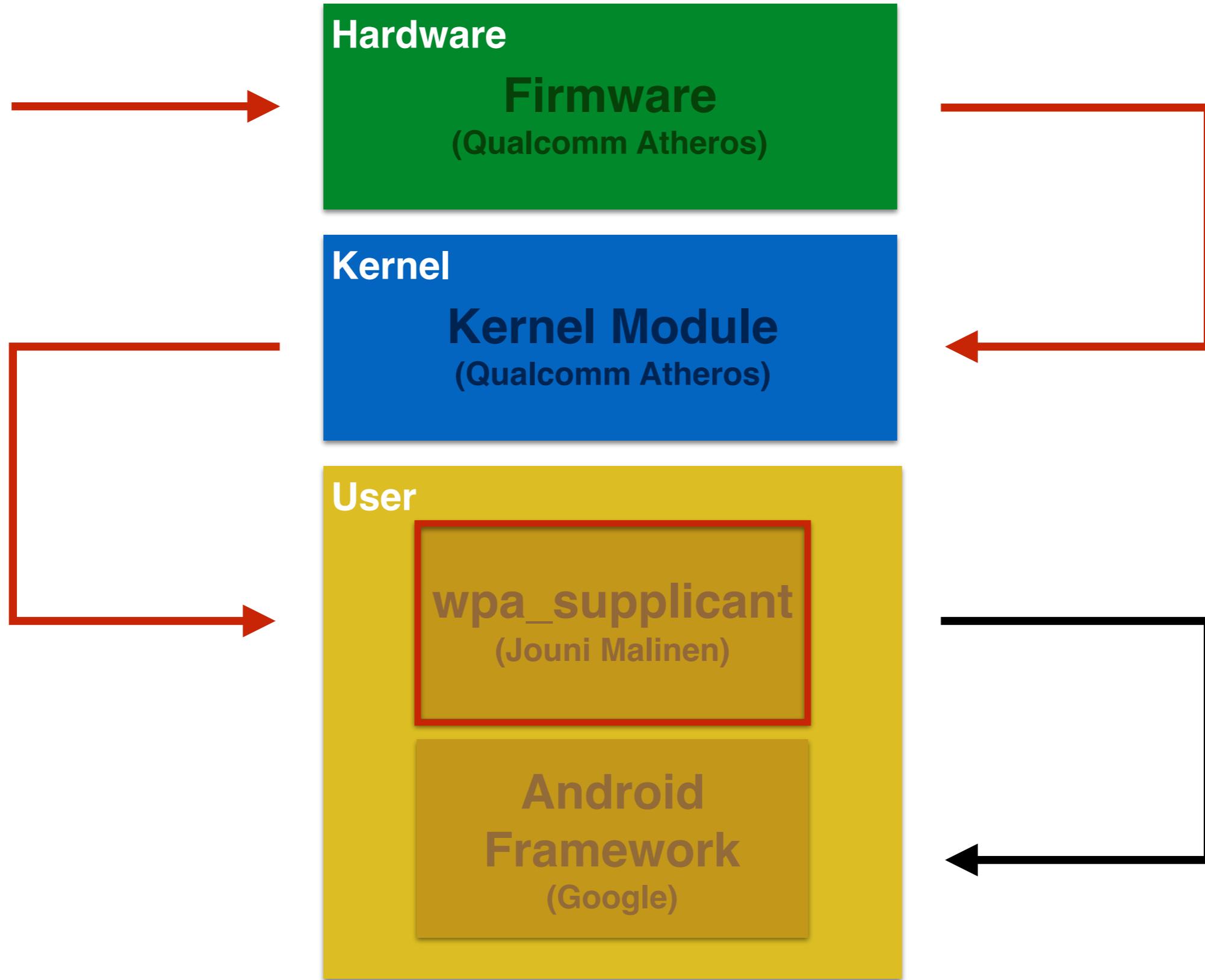
Help Close

c0 a8 01 03





802.11 Android architecture



802.11 Android architecture

D/TCMD (519): Listening for incoming client connection request
I/wpa_supplicant(3482): P2P-DEVICE-FOUND 70:5a:0f:16:ed:54 p2p_dev_addr=72:5a:0f:16:b4:66 pri_de
name='DIRECT-66-HP OfficeJet Pro 8710' config_methods=0x5a88 dev_capab=0x4 group_capab=0x1 level
I/wpa_supplicant(3482): P2P-DEVICE-FOUND 00:de:ad:fa:fa:fa p2p_dev_addr=00:de:ad:fa:fa:fa pri_de
5 name='fafa<FA><FA>' config_methods=0x188 dev_capab=0x21 group_capab=0x0 level=-27
D/MDMCTBK (267): reply_len: 40 reply is = <3>P2P-DEVICE-FOUND 70:5a:0f:16:ed:54 p2
D/MDMCTBK (267): Event received = P2P-DEVICE-FOUND 70:5a:0f:16:ed:54 p2
D/MDMCTBK (267): reply_len: 40 reply is = <3>P2P-DEVICE-FOUND 00:de:ad:fa:fa:fa p2
D/MDMCTBK (267): Event received = P2P-DEVICE-FOUND 00:de:ad:fa:fa:fa p2
D/WifiP2pService(1024): InactiveState{ when=-1ms what=147477 obj=Device: DIRECT-66-HP OfficeJet
D/WifiP2pService(1024): deviceAddress: 72:5a:0f:16:b4:66
D/WifiP2pService(1024): primary type: 3-0050F204-1
D/WifiP2pService(1024): secondary type: null
D/WifiP2pService(1024): wps: 23176
D/WifiP2pService(1024): grpcapab: 1
D/WifiP2pService(1024): devcapab: 4
D/WifiP2pService(1024): status: 3
D/WifiP2pService(1024): wfdInfo: null
D/WifiP2pService(1024): level: -49 target=com.android.internal.util.StateMachine\$SmHandler }
D/WifiP2pService(1024): P2pEnabledState{ when=-1ms what=147477 obj=Device: DIRECT-66-HP OfficeJe
D/WifiP2pService(1024): deviceAddress: 72:5a:0f:16:b4:66
D/WifiP2pService(1024): primary type: 3-0050F204-1
D/WifiP2pService(1024): secondary type: null
D/WifiP2pService(1024): wps: 23176
D/WifiP2pService(1024): grpcapab: 1
D/WifiP2pService(1024): devcapab: 4
D/WifiP2pService(1024): status: 3
D/WifiP2pService(1024): wfdInfo: null
D/WifiP2pService(1024): level: -49 target=com.android.internal.util.StateMachine\$SmHandler }
W/dalvikvm(1024): threadid=71: thread exiting with uncaught exception (group=0x4171bd40)
E/AndroidRuntime(1024): *** FATAL EXCEPTION IN SYSTEM PROCESS: WifiMonitor
E/AndroidRuntime(1024): java.lang.IllegalArgumentException: Malformed supplicant event
E/AndroidRuntime(1024): at android.net.wifi.p2p.WifiP2pDevice.<init>(WifiP2pDevice.java:2
E/AndroidRuntime(1024): at android.net.wifi.WifiMonitor\$MonitorThread.handleP2pEvents(Wif
E/AndroidRuntime(1024): at android.net.wifi.WifiMonitor\$MonitorThread.dispatchEvent(WifiM
E/AndroidRuntime(1024): at android.net.wifi.WifiMonitor\$MonitorThread.run(WifiMonitor.jav
I/Process (1024): Sending signal. PID: 1024 SIG: 9
I/ServiceManager(255): service 'package' died
I/ServiceManager(255): service 'sensorservice' died

CVE-2014-0997



WD TV Live



Default?



Network Setup

Check Connection

Auto Detect Wi-Fi Direct Setup

On

Wireless Display (Miracast™)

Device Name

WDTVLive



Completed SYN Stealth Scan at 22:04, 4.61s elapsed (1000 total ports)
Initiating Service scan at 22:04
Scanning 5 services on 192.168.69.61
Completed Service scan at 22:04, 26.03s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against 192.168.69.61
Retrying OS detection (try #2) against 192.168.69.61
NSE: Script scanning 192.168.69.61.
Initiating NSE at 22:04
Completed NSE at 22:05, 66.34s elapsed
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed
Nmap scan report for 192.168.69.61
Host is up (0.0033s latency).
Not shown: 995 closed ports

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Apache httpd (PHP 5.2.17)
139/tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
443/tcp	open	ssl/http	Apache httpd (PHP 5.2.17)
445/tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
30000/tcp	open	unknown	

MAC Address: 02:90:A9:67:7B:7E (Unknown)
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -
No OS matches for host
Network Distance: 1 hop

TRACEROUTE

HOP	RTT	ADDRESS
1	3.34 ms	192.168.69.61

NSE: Script Post-scanning.
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed

Services





HP WiFi Printers

66 17:14

NESES0-2017-0111 PoC



HP-Print-B2-Deskjet 5520 series
[REDACTED] OPEN

HP-Print-6B-LaserJet 1025
[REDACTED] OPEN

HP-Print-35-Deskjet 4640 series
[REDACTED] WPA2

HP-Print-10-LaserJet 1102
[REDACTED] OPEN

HP-Print-7e-LaserJet Pro M201dw
[REDACTED] WPA2

HP-Print-34-LaserJet 1025
[REDACTED] OPEN

HP-Print-34-Officejet Pro 8620
[REDACTED] OPEN

Bad Choice





NETWORK

- General

[Network Summary](#)

Network Identification

Network Protocols

Proxy Settings

+ Wired (802.3)

+ Wireless (802.11)

+ Wi-Fi Direct

+ AirPrint™

+ Google Cloud Print

+ Internet Printing Protocol

+ Advanced Settings

General

Network Summary

Wired (802.3)



Status: Not connected

Host Name: HP16B465

IP Address:

Hardware (MAC) Address: 705A0F16B465

Wireless (802.11)



Status: Connected

Host Name: HP16B465

IP Address: 192.168.0.104

Hardware (MAC) Address: 705A0F16B466

SSID: ██████████

Wi-Fi Direct



Security by default

Wi-Fi Direct Name: DIRECT-66-HP OfficeJet Pro 8710

```
Initiating SYN Stealth Scan at 22:31
Scanning 192.168.223.1 [1000 ports]
Discovered open port 443/tcp on 192.168.223.1
Discovered open port 8080/tcp on 192.168.223.1
Discovered open port 80/tcp on 192.168.223.1
Discovered open port 9220/tcp on 192.168.223.1
Increasing send delay for 192.168.223.1 from 0 to 5 due to 34 out of 113 dropped probe
increase.
Increasing send delay for 192.168.223.1 from 5 to 10 due to 34 out of 111 dropped probe
t increase.
Discovered open port 515/tcp on 192.168.223.1
Increasing send delay for 192.168.223.1 from 10 to 20 due to 19 out of 61 dropped probe
t increase.
Increasing send delay for 192.168.223.1 from 20 to 40 due to 11 out of 26 dropped probe
t increase.
Increasing send delay for 192.168.223.1 from 40 to 80 due to 11 out of 33 dropped probe
t increase.
Discovered open port 9100/tcp on 192.168.223.1
Discovered open port 631/tcp on 192.168.223.1
Completed SYN Stealth Scan at 22:33, 84.01s elapsed (1000 total ports)
Nmap scan report for 192.168.223.1      Services
Host is up (0.0020s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
515/tcp   open  printer
631/tcp   open  ipp
8080/tcp  open  http-proxy
9100/tcp  open  jetdirect
9220/tcp  open  unknown
MAC Address: 70:5A:0F:16:ED:54 (Hewlett Packard)
Read data files from: /usr/bin/../share/nmap
```



They've got no idea I used my phone

Samsung Smart TVs



The background of the screen shows a sunset or sunrise over a dense forest of tall evergreen trees. The sky is a gradient from light blue to orange and yellow near the horizon. A small portion of the sun is visible on the right side.

Tablet is attempting to connect to
your TV. To allow the connection,
press Allow within 120 seconds.

Remaining Time :114sec

You can manage allowed devices
later by selecting Network > Wi-Fi
Direct.

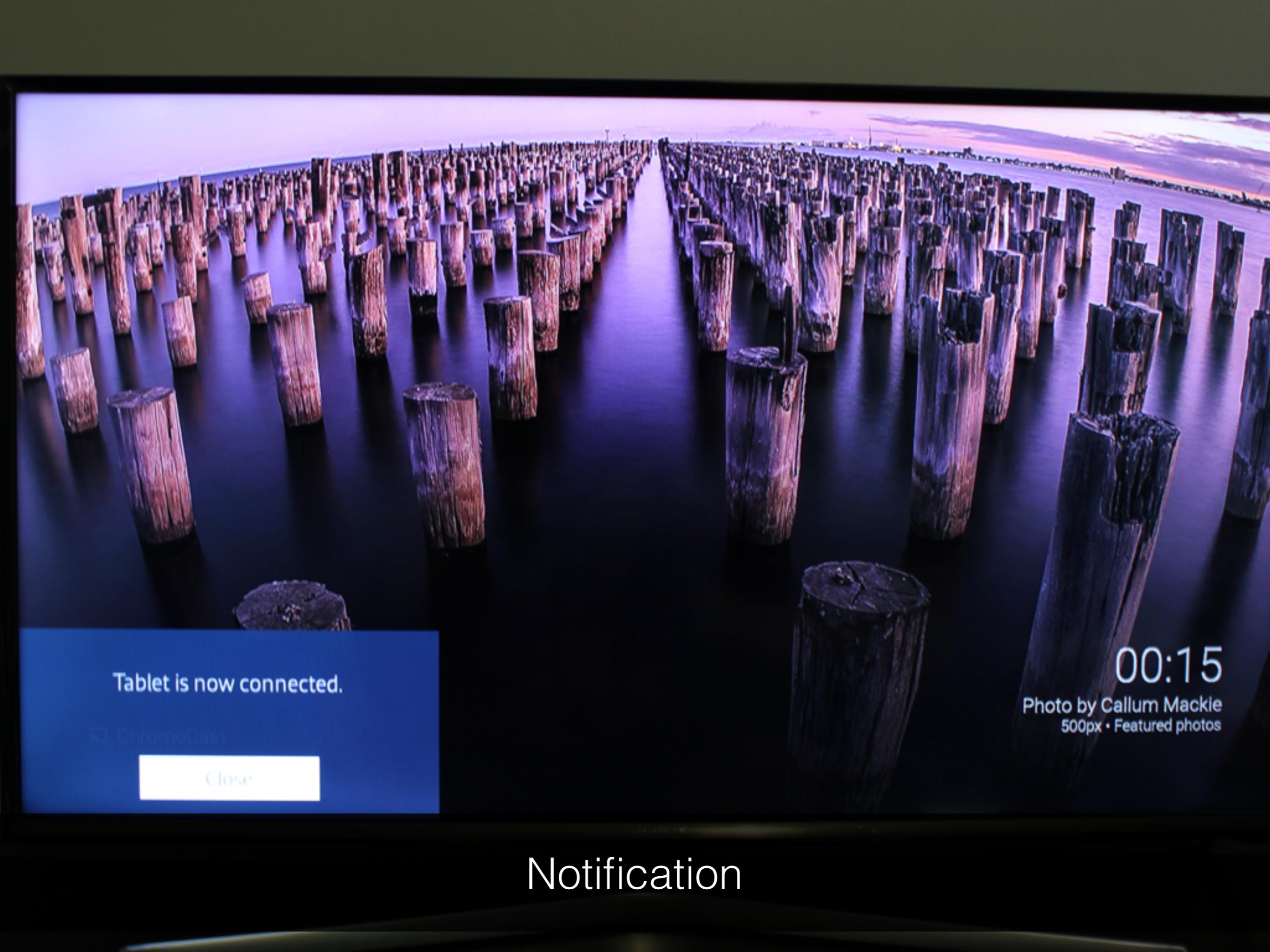
Allow

Deny

00:14

Photo by Raimund Linke
Getty Images • Featured photos

Authentication



Tablet is now connected.

[Close](#)

00:15

Photo by Callum Mackie
500px • Featured photos

Notification

HDMI

Multimedia Device Manager

■ Tablet

Allowed

□ Phone

Denied

Allow other devices on
your network like smart
phones and tablets, to
share content with your
TV.

Close

Wi-Fi Direct

Multimedia Device Manager

Screen Mirroring

Device Name

[TV] UN32J5500

00:13

□ Chromecast

Photo by Patrick Smith

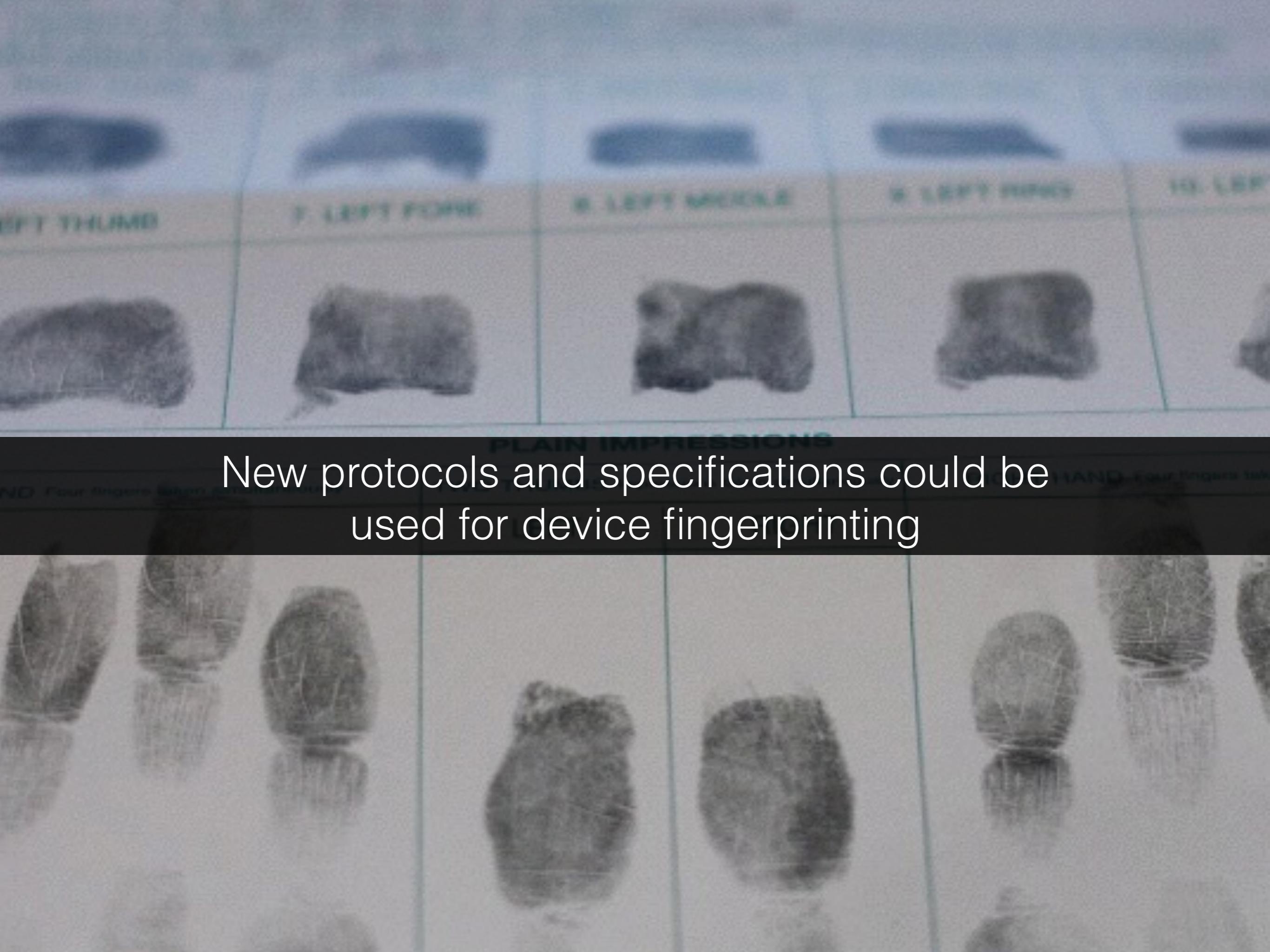
Device Manager

```
Initiating SYN Stealth Scan at 22:42
Scanning 192.168.49.1 [1000 ports]
Discovered open port 8080/tcp on 192.168.49.1
Discovered open port 7676/tcp on 192.168.49.1
Discovered open port 8002/tcp on 192.168.49.1
Increasing send delay for 192.168.49.1 from 0 to 5 due to 113 out of 376 dropped probe
increase.
Increasing send delay for 192.168.49.1 from 5 to 10 due to 145 out of 481 dropped prob
t increase.
Increasing send delay for 192.168.49.1 from 10 to 20 due to 12 out of 39 dropped probe
increase.
Increasing send delay for 192.168.49.1 from 20 to 40 due to max_successful_tryno incre
Increasing send delay for 192.168.49.1 from 40 to 80 due to 11 out of 34 dropped probe
increase.
Discovered open port 8001/tcp on 192.168.49.1
Increasing send delay for 192.168.49.1 from 80 to 160 due to 48 out of 159 dropped probe
st increase.
Discovered open port 8000/tcp on 192.168.49.1
Discovered open port 9999/tcp on 192.168.49.1
Completed SYN Stealth Scan at 22:43, 66.01s elapsed (1000 total ports)
Nmap scan report for 192.168.49.1
Host is up (0.062s latency).
Not shown: 994 closed ports
Services
PORT      STATE SERVICE
7676/tcp  open  imqbrokerd
3000/tcp  open  http-alt
3001/tcp  open  vcom-tunnel
3002/tcp  open  teradataordbms
3080/tcp  open  http-proxy
9999/tcp  open  abyss
MAC Address: CE:B1:1A:F4:B7:F5 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 79.32 seconds
```







New protocols and specifications could be used for device fingerprinting



Too Many Hands in the Pot

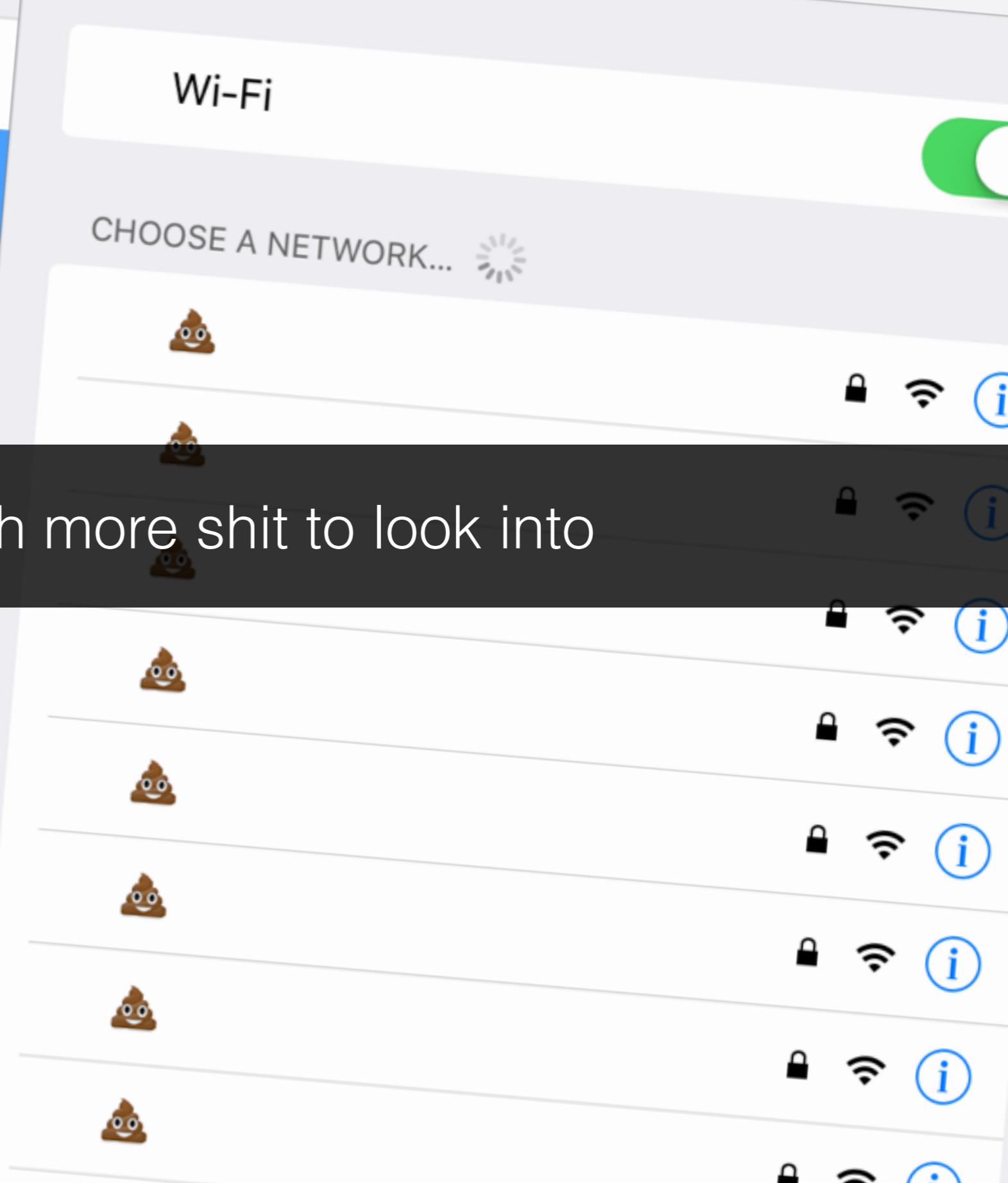
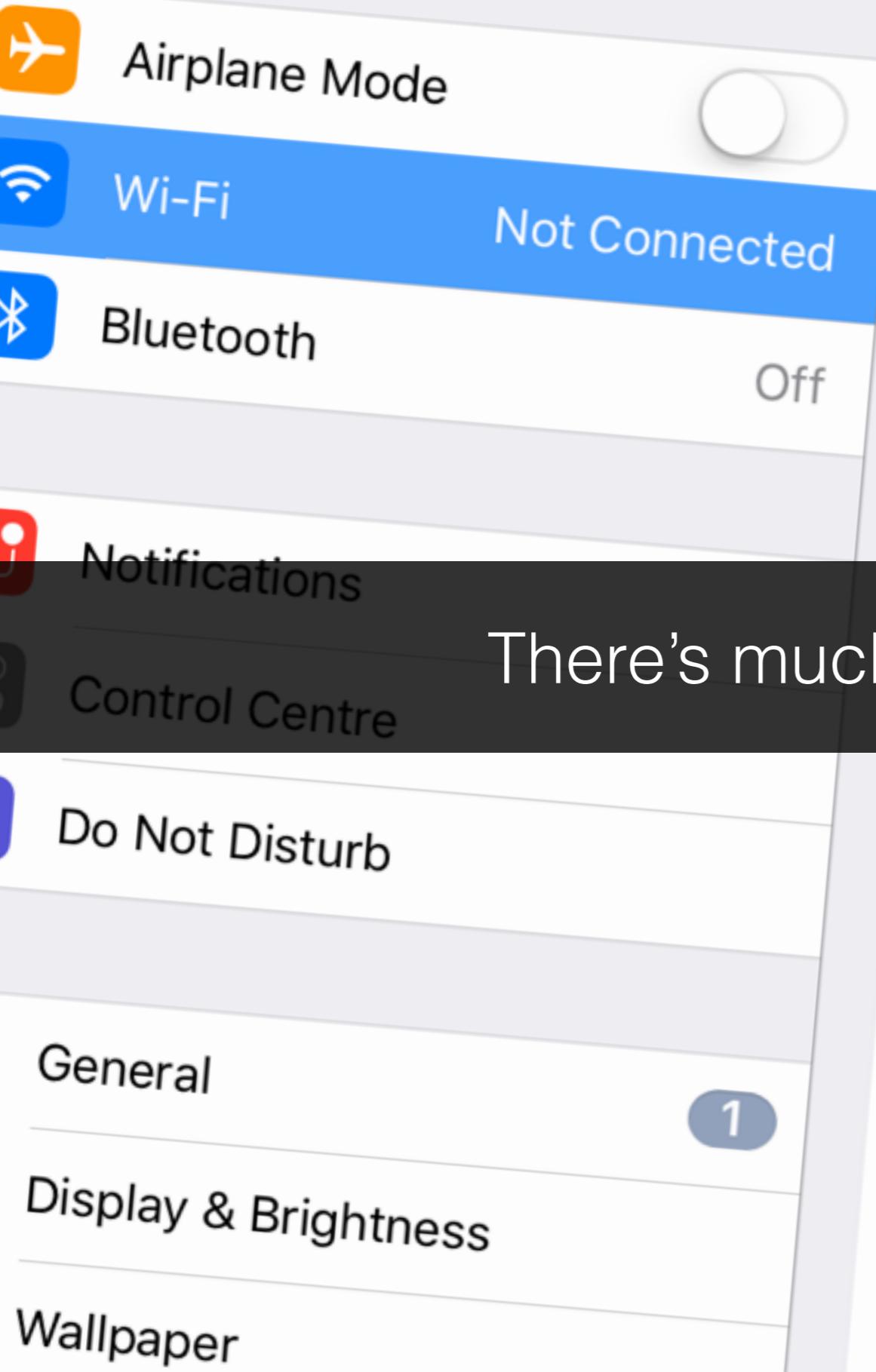
Bad Implementations





Network Access

Wi-Fi



Questions

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

Email: 6e726d@gmail.com

Twitter: @6e726d