

SHARKFEST 2015

WIRESHARK DEVELOPER AND USER CONFERENCE



COMPUTER HISTORY MUSEUM

Discover WLAN with Wireshark, AirPcap and WiSpy
Rolf Leutert, Leutert NetServices

Discover WLAN with Wireshark, AirPcap and WiSpy

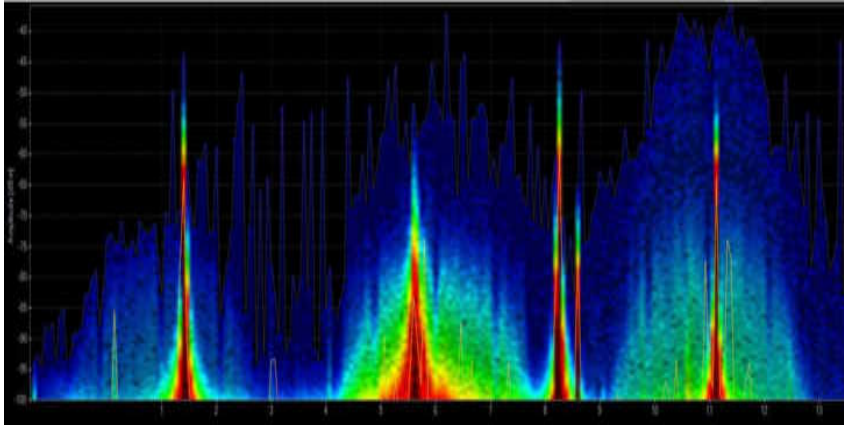
Session objectives:

- ▀ Learn what you can see on layer 1 and layer 2.
- ▀ Learn which tools can help you finding WLAN problems.
- ▀ Learn how Management- and Control frames assists you in root cause analysis.
- ▀ Learn how to customize Wireshark to show you specific WLAN information.



Discover WLAN with Wireshark, AirPcap and Wi-Spy

Troubleshooting WLANs comprises Layer 1 and Layer 2



Layer 1 - Physical Access

FH, DSSS, OFDM, coding, modulation, bands, channels, frequencies, noise, signal strength, interferences etc.

Clients: WiFi and non-WiFi devices like surveillance cameras, remote control, microwave, health gadgets etc.

Tools: Spectrum Analyser (e.g. Wi-Spy)

A screenshot of the Wireshark network protocol analyzer interface. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Signal, Noise, TX Speed, Channel, and Info. The selected packet (No. 111) is expanded to show details for the MAC layer (802.11), including fields like Frame Control, Duration, Address 1, Address 2, Address 3, Address 4, and Sequence Control. The Info pane shows the packet type as 'Probe Request, SN=265, PN=0'.

Layer 2 - Data Link Control

WiFi Standards 802.11 a/b/g/n/ac framing, management, access control, security, encryption etc.

Client: WiFi compatible devices only

Tools: Wireshark, AirPcap, Scanners

WLAN Layer 1 Analysis

- ▶ WLAN (WiFi) devices are working in the 2.4 GHz ISM* and 5 GHz UNII** bands
- ▶ But both bands are free for any use, WiFi as well as non-WiFi devices
- ▶ Especially the 2.4 GHz band is often crowded with non-WiFi devices
- ▶ The only limitation is max. radiated power according to country regulations
- ▶ Non-WiFi clients use any kind of modulation and may interfere with WiFi
- ▶ Layer 2 tools like Wireshark can not detect non-WiFi devices
- ▶ Spectrum analyzers scan the bands and show shape and strength of all signals

Wi-Spy® DBx spectrum scanner
and Chanalyzer® software displays
and records all layer 1 signals in
both 2.4 GHz and 5 GHz bands.

www.metageek.com

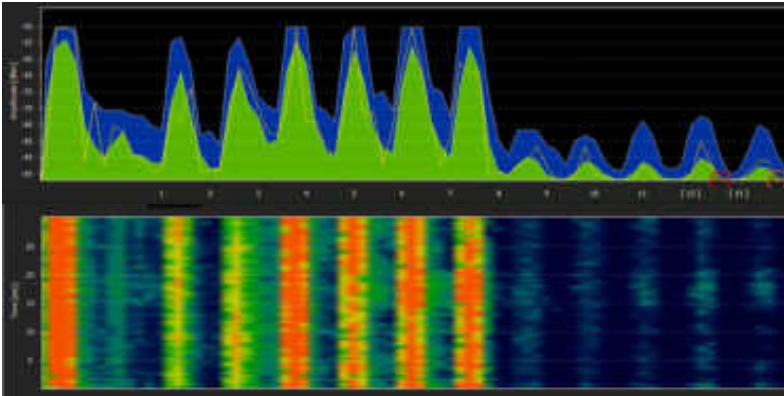
* ISM Industrial, Scientific and Medical

**UNII Unlicensed National Information Infrastructure

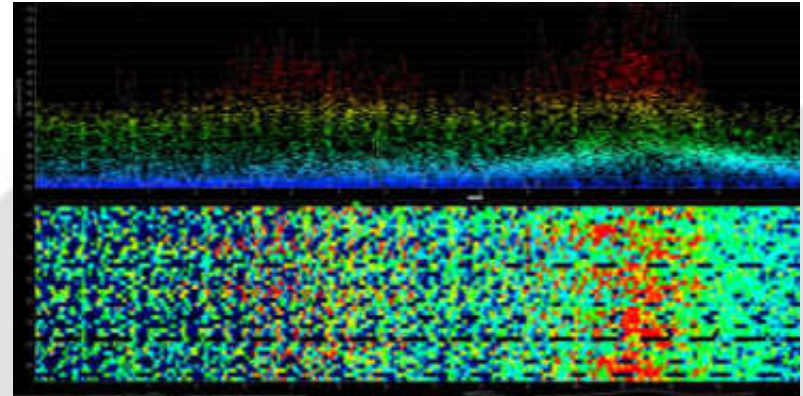


WLAN Layer 1 Analysis

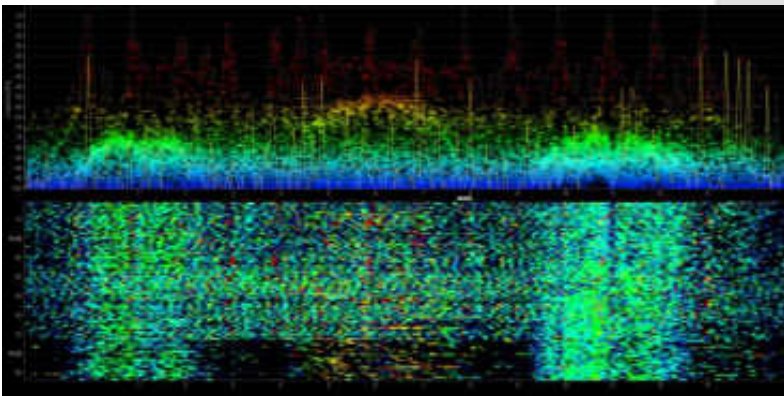
Non-WiFi Devices' Signatures



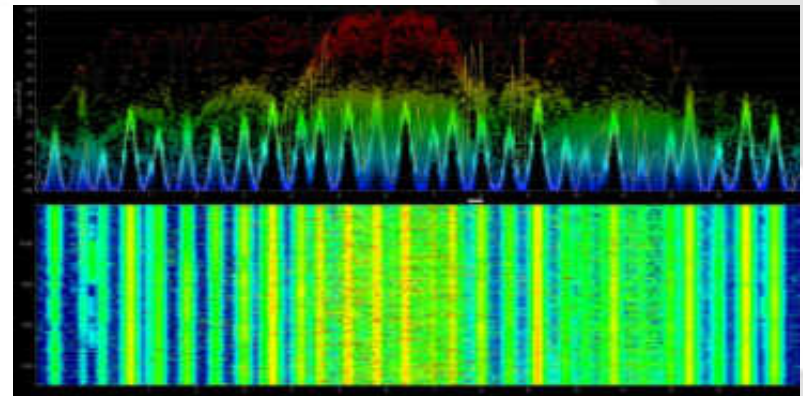
Home trainers in a fitness center



Microwave oven

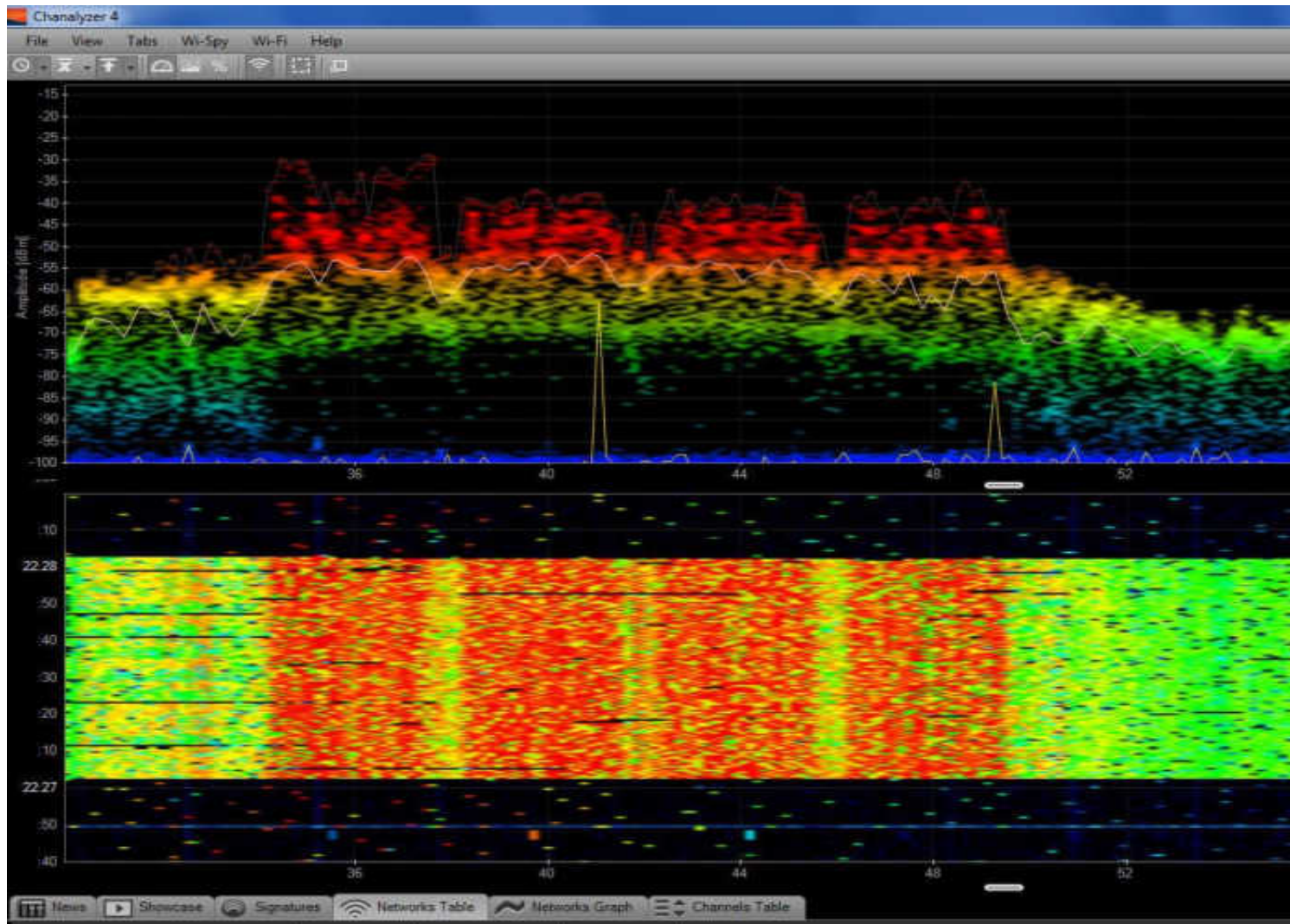


Remote control of model airplanes



Wireless guitar

WLAN Layer 1 Analysis



WiFi 802.11ac with four bonded channels

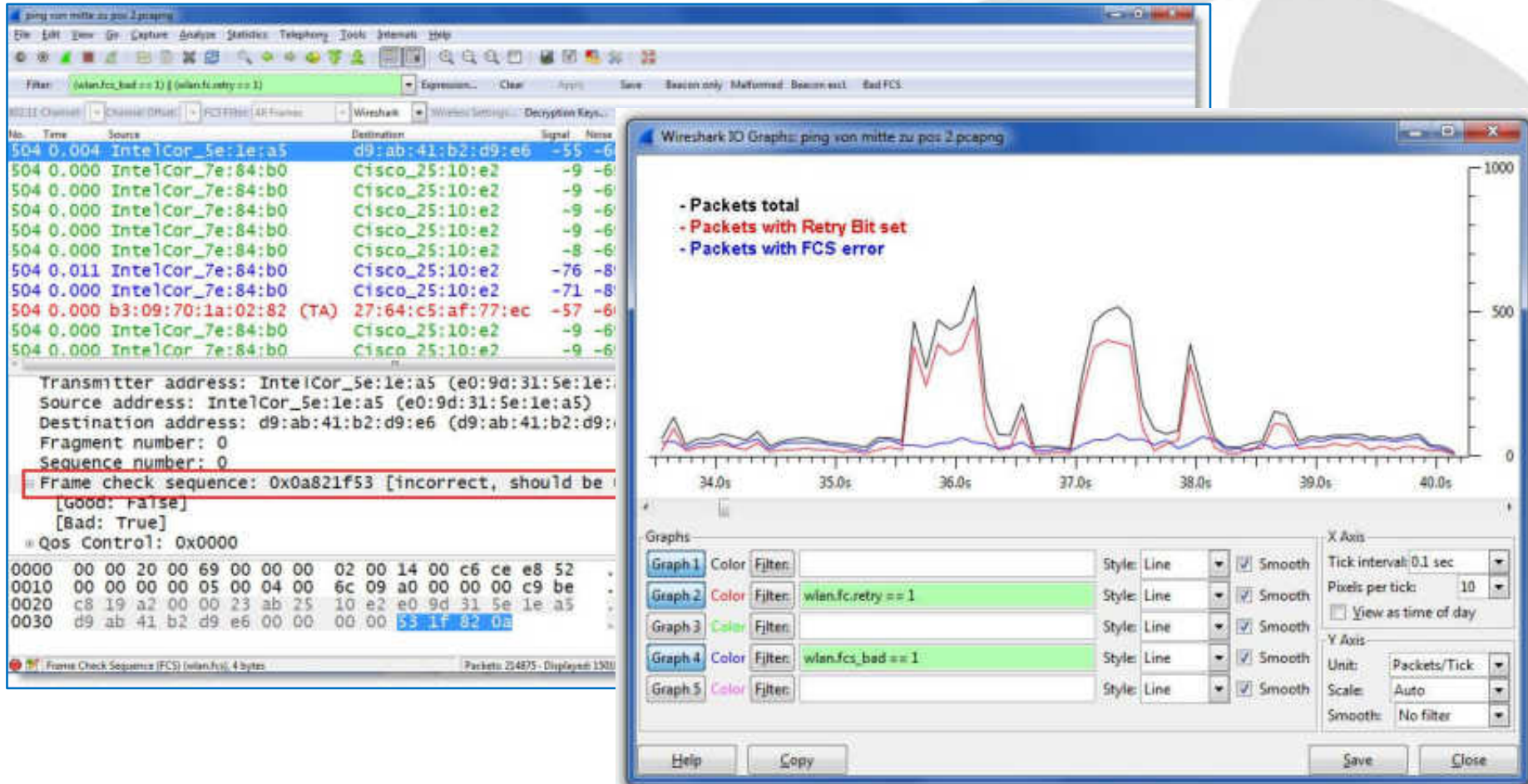
WLAN Layer 1 Analysis (Case one)

- Large logistic enterprise, **depending on WLAN** for day-to-day operations
- Two container cranes to load/unload trains require WLAN connections
- User complain about log-in **timeouts and disconnections** during operations
- Crane #2 is hardly usable due to **unreliable WLAN connection**
- Tech-Support has already changed WiFi channels and **added additional AP**



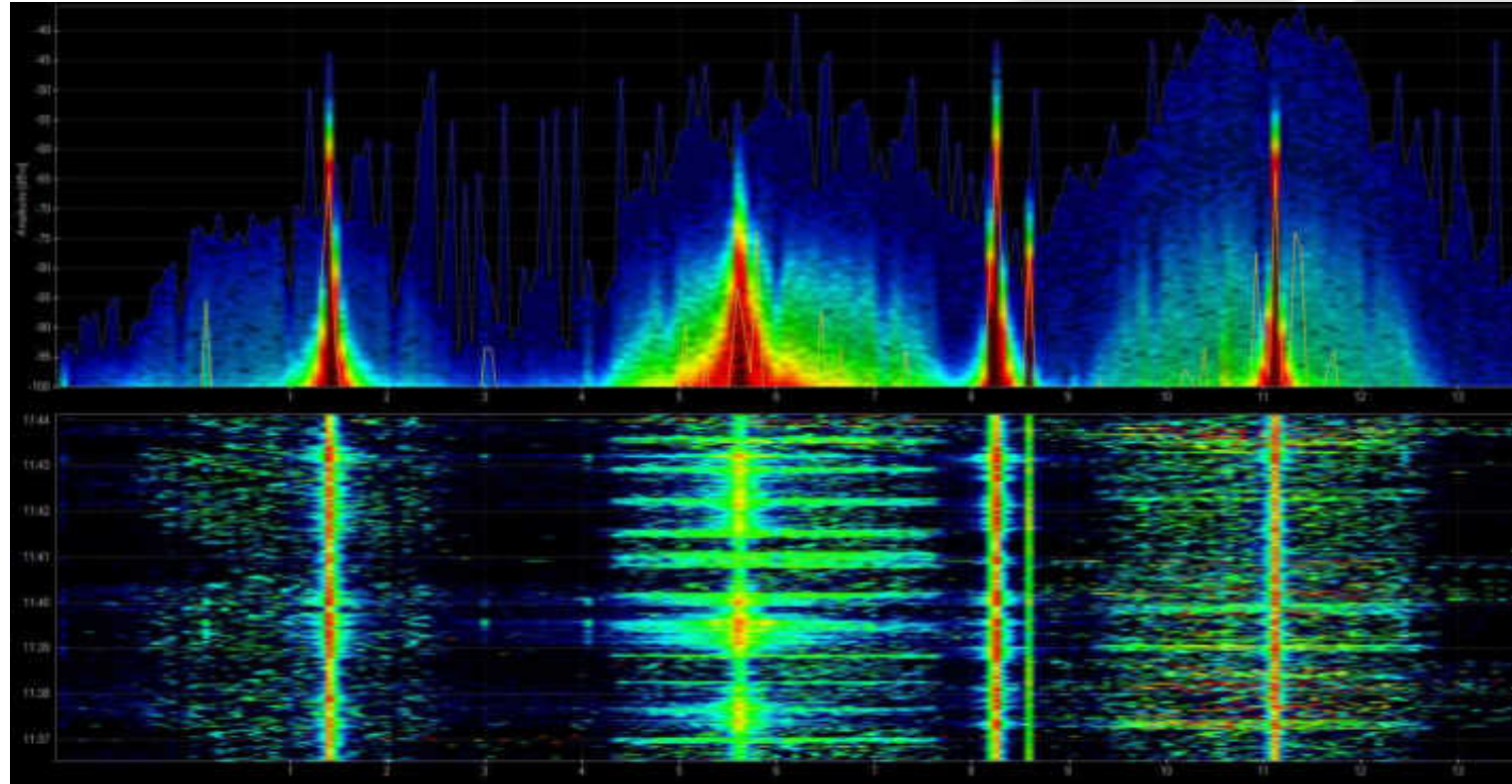
WLAN Layer 1 Analysis (Case one)

- Starting with **layer 2** analysis near crane #2 in channels 1, 6, and 11
- Wireshark shows up to **70%** of frames with **bad FCS** or the **Retry Flag** set



WLAN Layer 1 Analysis (Case one)

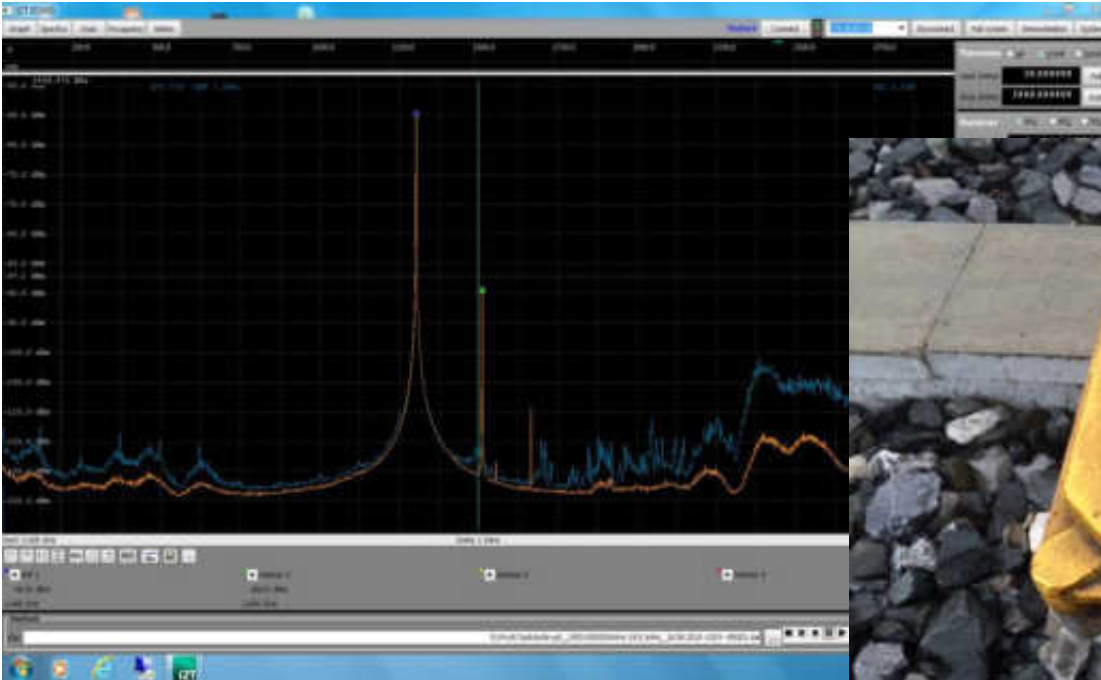
- Continuing with **layer 1** analysis near crane #2 in 2.4 GHz band
- Strong interference with **non-WiFi signals** on all three channels detected



- Signal source is outside of customers campus' → Swiss radio authority informed
- If this transmitting power is within legal limits → Change to 5 GHz band required

WLAN Layer 1 Analysis (Case one)

- Swiss radio authority (BAKOM) scanned the 2.4 GHz band with their own tool
- They detected a strongly interfering signal caused by a [railway induction loop](#)



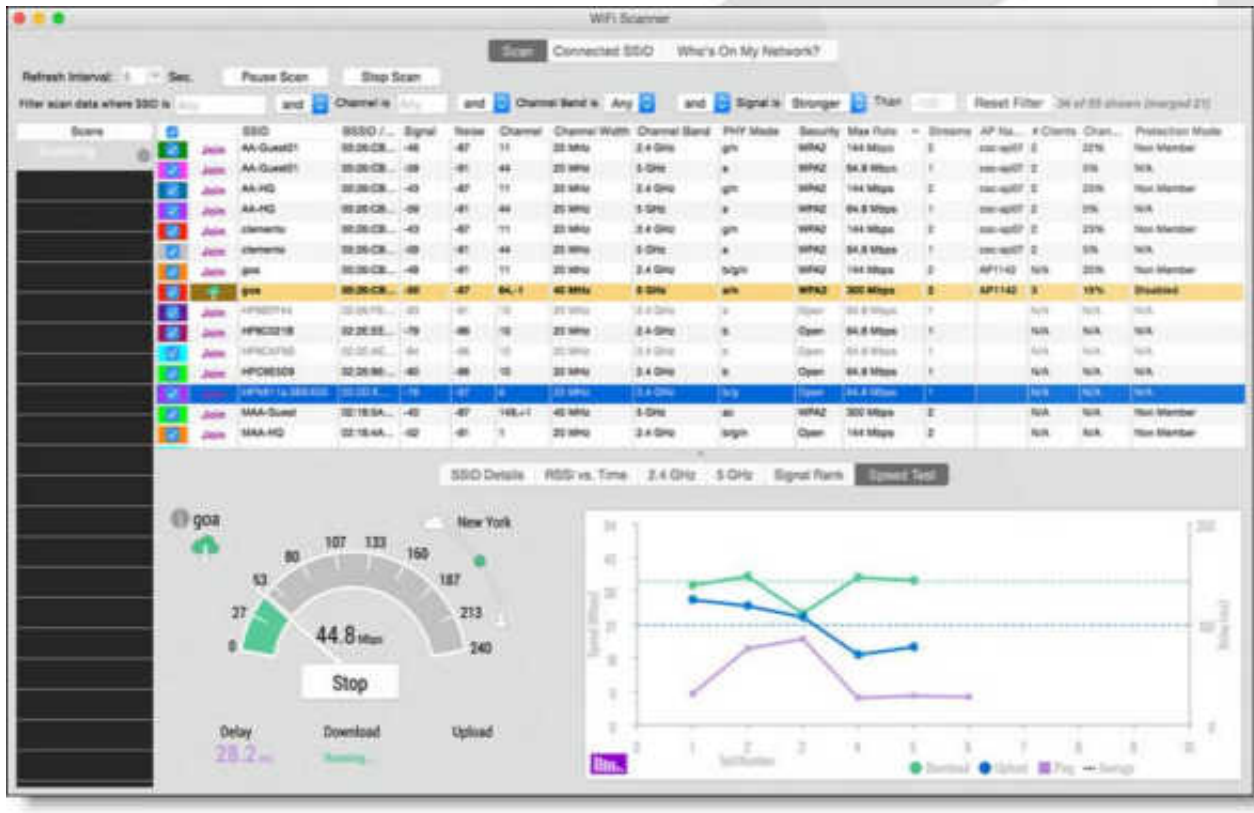
BAKOM scan result



Traffic monitoring induction loop

WiFi Scanners

- WiFi scanners show you available access points with lots of information like SSID, channel no, channel width, max. rate, security mode etc.
- Some tools are able to perform throughput simulations
- No adapter required, WiFi scanners are using internal WLAN cards



WiFi Scanners (just a few popular ones)



Acrylic WiFi scanner

www.acrylicwifi.com



Ekahau HeatMapper

www.ekahau.com



inSSIDer

www.metageek.com



NetStumbler

www.netstumbler.com



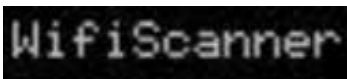
Wifi Analyzer (Android)

play.google.com



WifiInfoView

www.nirsoft.net



WifiScanner

wifiscanner.sourceforge.net



Wifi Scanner

www.apple.com/osx/apps/app-store

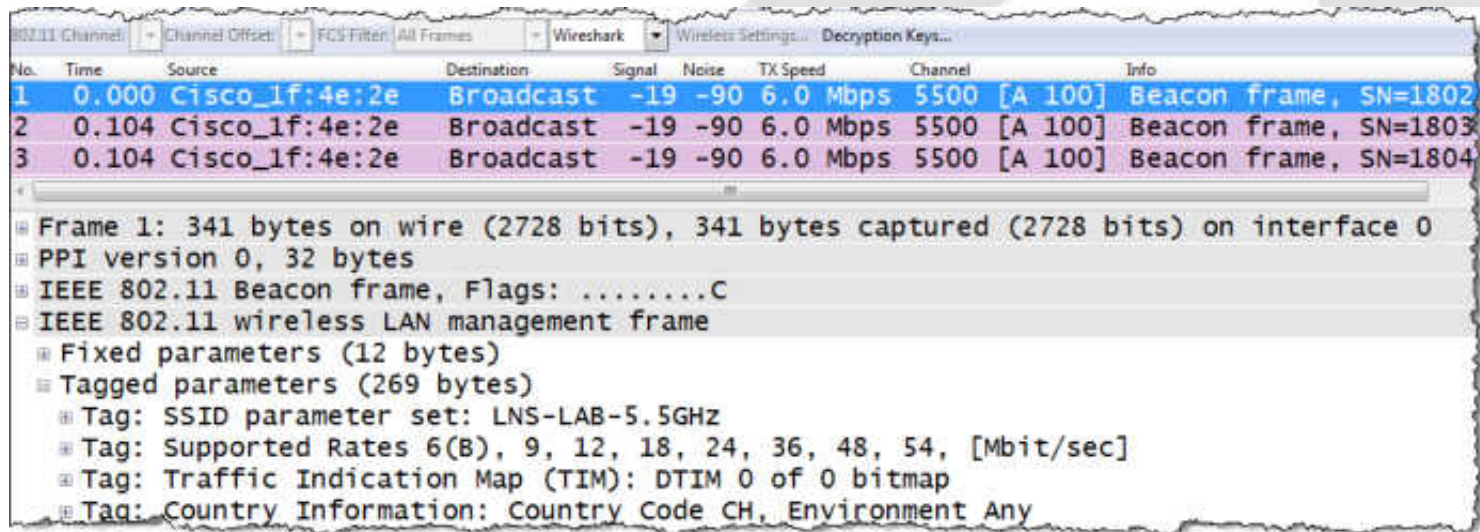


BTW: For iPhone/iPad, IOS Apple has locked direct access to the WiFi card for stability and other unknown reasons. Jailbreak is required to install and run WiFi Scanner apps on these devices.

WiFi Scanners

All these tools have the following **limitations** in common:

- Scanning on **layer 2**, therefore **only WiFi** devices can be detected.
- Non-802.11 sources like surveillance cameras etc. are **invisible**.
- WiFi scanners read data from **Beacon** and other **management frames**



The screenshot shows a Wireshark capture of three IEEE 802.11 Beacon frames. The interface includes a menu bar with options like 'Channel', 'Channel Offset', 'FCS Filter', 'All Frames', 'Wireshark', 'Wireless Settings...', and 'Decryption Keys...'. Below the menu is a table with columns: No., Time, Source, Destination, Signal, Noise, TX Speed, Channel, and Info. Three rows of data are visible, all from source 'Cisco_1f:4e:2e' to destination 'Broadcast' on channel 5500. The first row is highlighted in blue, the second in purple, and the third in pink. Below the table, the details pane for the first frame is expanded, showing fields like 'PPI version 0, 32 bytes', 'IEEE 802.11 Beacon frame, Flags:C', and 'IEEE 802.11 wireless LAN management frame' with its sub-parameters.

| No. | Time | Source | Destination | Signal | Noise | TX Speed | Channel | Info |
|-----|-------|----------------|-------------|--------|-------|----------|--------------|-----------------------|
| 1 | 0.000 | Cisco_1f:4e:2e | Broadcast | -19 | -90 | 6.0 Mbps | 5500 [A 100] | Beacon frame, SN=1802 |
| 2 | 0.104 | Cisco_1f:4e:2e | Broadcast | -19 | -90 | 6.0 Mbps | 5500 [A 100] | Beacon frame, SN=1803 |
| 3 | 0.104 | Cisco_1f:4e:2e | Broadcast | -19 | -90 | 6.0 Mbps | 5500 [A 100] | Beacon frame, SN=1804 |

Frame 1: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface 0

- PPI version 0, 32 bytes
- IEEE 802.11 Beacon frame, Flags:C
- IEEE 802.11 wireless LAN management frame
 - Fixed parameters (12 bytes)
 - Tagged parameters (269 bytes)
 - Tag: SSID parameter set: LNS-LAB-5.5GHZ
 - Tag: Supported Rates 6(B), 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
 - Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
 - Tag: Country Information: Country Code CH, Environment Any

WiFi Scanners will not provide any information if Beacon frames interfere with non 802.11 devices on layer 1!

WLAN Layer 2 Analysis

Key features:

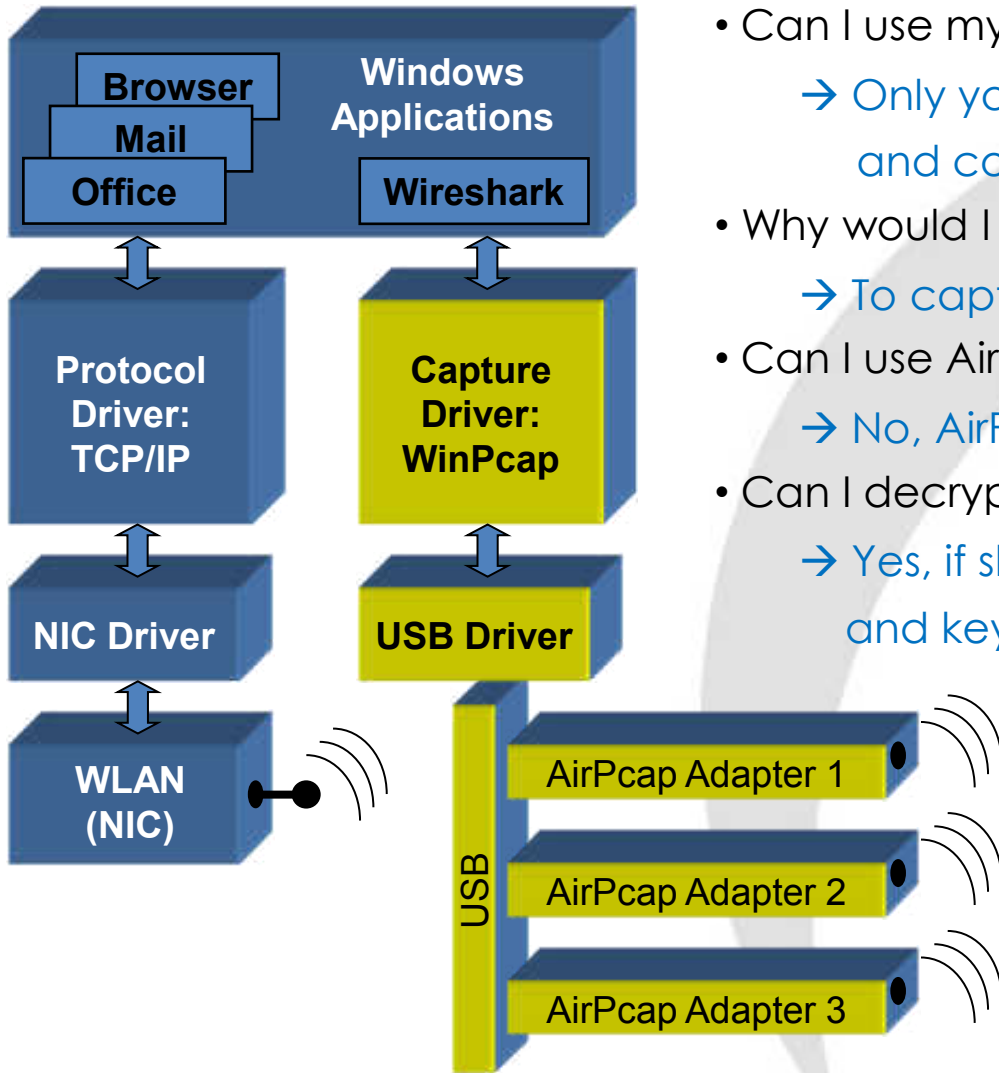
- ▶ Radio cells use **one or multiple 20 MHz channels** (n/ac) to increase throughput
- ▶ Each radio cell is a **shared media** and is controlled by an Access Point (AP)
- ▶ A mobile client can be associated with **only one AP** at the time
- ▶ Radio cell access is controlled by **managements and control frames**
- ▶ Wireshark with AirPcap can **capture and analyze** these frames
- ▶ Understanding of these frames is crucial for **WLAN troubleshooting**

AirPcap Nx 802.11a/b/g/n USB - adapter works with **Wireshark** and captures WiFi packets in both 2.4 GHz and 5 GHz bands.

www.riverbed.com/products/



WLAN Layer 2 Analysis



Frequently Asked Questions:

- Can I use my built-in WLAN NIC with Wireshark?
 - Only your own traffic and no management and control frames will be captured
- Why would I need multiple AirPcaps?
 - To capture roaming processes
- Can I use AirPcaps to join a WLAN?
 - No, AirPcaps are monitoring devices only.
- Can I decrypt data with AirPcap adapter?
 - Yes, if shared keys are used, key is available and key negotiation is captured

WLAN Layer 2 Analysis

- ▶ Capturing with the **built-in** WLAN NIC will display **Ethernet-like** frames
- ▶ Only **Data** frames and no **Radio** or **WLAN header** will be seen

The screenshot shows the Wireshark interface with a capture of network traffic. The packet list pane contains the following data:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|-----------------|----------|--------|----------------|
| 1 | 0.000000 | 192.168.0.217 | 192.168.0.255 | NBNS | 92 | Name query NB |
| 2 | 0.258232 | 192.168.0.201 | 192.168.0.255 | NBNS | 92 | Name query NB |
| 3 | 0.069601 | 192.168.0.217 | 239.255.255.250 | SSDP | 175 | M-SEARCH * HTT |
| 4 | 0.237969 | 192.168.0.201 | 239.255.255.250 | SSDP | 175 | M-SEARCH * HTT |
| 5 | 0.199400 | 192.168.0.217 | 224.0.0.252 | LLMNR | 66 | Standard query |
| 6 | 0.107298 | 192.168.0.201 | 224.0.0.252 | LLMNR | 66 | Standard query |
| 7 | 0.001103 | 192.168.0.217 | 224.0.0.252 | LLMNR | 66 | Standard query |
| 8 | 0.203786 | 192.168.0.217 | 192.168.0.255 | NBNS | 92 | Name query NB |
| 9 | 0.102408 | 192.168.0.201 | 224.0.0.252 | LLMNR | 66 | Standard query |
| 10 | 0.002094 | 192.168.0.201 | 192.168.0.255 | NBNS | 92 | Name query NB |
| 11 | 0.659450 | 192.168.0.217 | 192.168.0.255 | NBNS | 92 | Name query NB |

The packet details pane for the first packet shows the following structure:

- Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
- Ethernet II, Src: IntelCor_73:68:54 (00:21:6b:73:68:54), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 192.168.0.217 (192.168.0.217), Dst: 192.168.0.255
- User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
- NetBIOS Name Service

WLAN Layer 2 Analysis

- AirPcap is adding a **Radio Tap** or **PPI (Per Packet Information)** pseudo header
- The **Pseudo-Header** contains helpful infos like **channel no, signal strength** etc.

The image shows a Wireshark capture of a NetBIOS Name Service query over a wireless network. The capture filter is `wlan.fc.type_subtype == 0x0020`. Two frames are visible: Frame 106 (blue) and Frame 110 (yellow), both of length 146 bytes. The details pane for Frame 106 is expanded, showing a PPI pseudo header (32 bytes) and the underlying IEEE 802.11 data, Logical-Link Control, and Internet Protocol Version 4 (IP) packet. The PPI header contains the following information:

- Version: 0
- Flags: 0x00
- Header length: 32
- DLT: 105
- 802.11-Common
 - Field type: 802.11-Common (2)
 - Field length: 20
 - TSFT: 3091835552
 - Flags: 0x0001
 - Rate: 6.0 Mbps
 - Channel frequency: 5200 [A 40]
 - Channel type: 802.11a (0x0140)
 - FHSS hopset: 0x00
 - FHSS pattern: 0x00
 - dBm antenna signal: -19
 - dBm antenna noise: -89

The IP packet details show: IEEE 802.11 Data, Flags:F.C; Logical-Link Control; Internet Protocol Version 4, Src: 192.168.0.233 (192.168.0.233), Dst: 192.168.0.255 (192.168.0.255); User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137); NetBIOS Name Service.

← PPI Pseudo Header added by AirPcap

Customize Wireshark for WLAN Analysis

- Create a **new profile** and **customize your Wireshark** before analyzing WLANs
- Turn on **Wireless Toolbar** and **add columns** with useful layer 1 information
- Configure **AirPcap** to add a **Pseudo Header (PPI)** to each frame at reception

Add Quick Filter buttons

Open the Per Packet Information pseudo header

Select Capture Type to include PPI

Use these fields and Apply as Column

| No. | Time | Source | Destination | Signal | Noise | Tx Speed | Channel | Info |
|-----|-------|----------------|-------------|--------|-------|----------|--------------|-------------------------------|
| 1 | 0.000 | Cisco_1f:4e:2e | Broadcast | -19 | -90 | 6.0 Mbps | 5500 [A 100] | Beacon frame, SN=1802, FN=... |
| 2 | 0.104 | Cisco_1f:4e:2e | Broadcast | -19 | -90 | 6.0 Mbps | 5500 [A 100] | Beacon frame, SN=1803, FN=... |
| 3 | 0.104 | Cisco_1f:4e:2e | Broadcast | -19 | -90 | 6.0 Mbps | 5500 [A 100] | Beacon frame, SN=1804, FN=... |
| 4 | 0.104 | Cisco_1f:4e:2e | Broadcast | -19 | -90 | 6.0 Mbps | 5500 [A 100] | Beacon frame, SN=1805, FN=... |

Frame 1: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface 0

PPI version 0, 32 bytes

```

Version: 0
Flags: 0x00
Header length: 32
DLT: 105
802.11-Common
  Field type: 802.11-Common (2)
  Field length: 20
  TSFT: 3313588701
  Flags: 0x0001
  Rate: 6.0 Mbps
  Channel frequency: 5500 [A 100]
  Channel type: 802.11a (0x0140)
  FHSS hopset: 0x00
  FHSS pattern: 0x00
  dBm antenna signal: -19
  dBm antenna noise: -90
IEEE 802.11 Beacon frame, Flags: .....C
IEEE 802.11 wireless LAN management frame
    
```

Customize Wireshark for WLAN Analysis

Adding a coloring rule **per channel** enhances readability

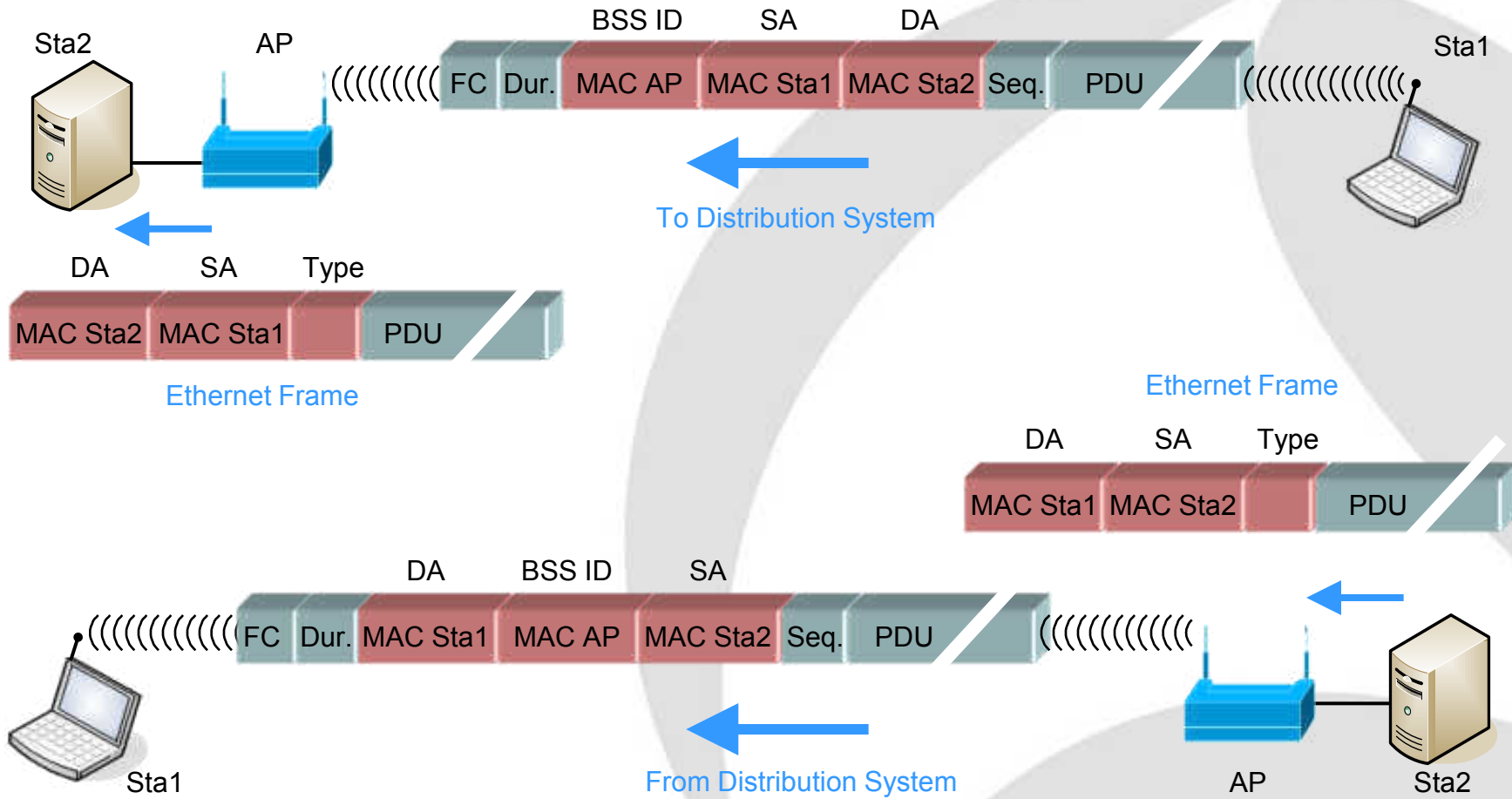
The screenshot shows the Wireshark interface with a packet capture of WLAN probe requests. The main pane displays a list of packets with columns for No., Time, Channel, TX Speed, SNR, Source, Destination, Protocol, and Info. The packets are color-coded based on their channel: Channel 11 (2462 MHz) is blue, Channel 6 (2437 MHz) is green, and Channel 1 (2412 MHz) is red.

The 'Wireshark: Coloring Rules' dialog box is open, showing a list of rules. The rules are processed in order until a match is found. The rules are:

| Name | Filter |
|--------------|---------------------------------------------------------------------|
| Low TTL | ip.ttl < 5 |
| Checksum Err | edp.checksum_bad==1 ip.checksum_bad==1 tcp.checksum_bad |
| SMB | smb nbss nbns nbpx ipxsap netbios |
| HTTP | http tcp.port == 80 |
| IPX | ipx spx |
| DCERPC | dcerpc |
| Routing | hsrp eigrp ospf bgp cdp vrrp gvrp igmp ismp |
| TCP SYN/FIN | tcp.flags & 0x02 tcp.flags.fin == 1 |
| TCP | tcp |
| UDP | udp |
| Broadcast | eth[0] & 1 |
| Channel 1 | radiotap.channel.freq == 2412 |
| Channel 6 | radiotap.channel.freq == 2437 |
| Channel 11 | radiotap.channel.freq == 2462 |

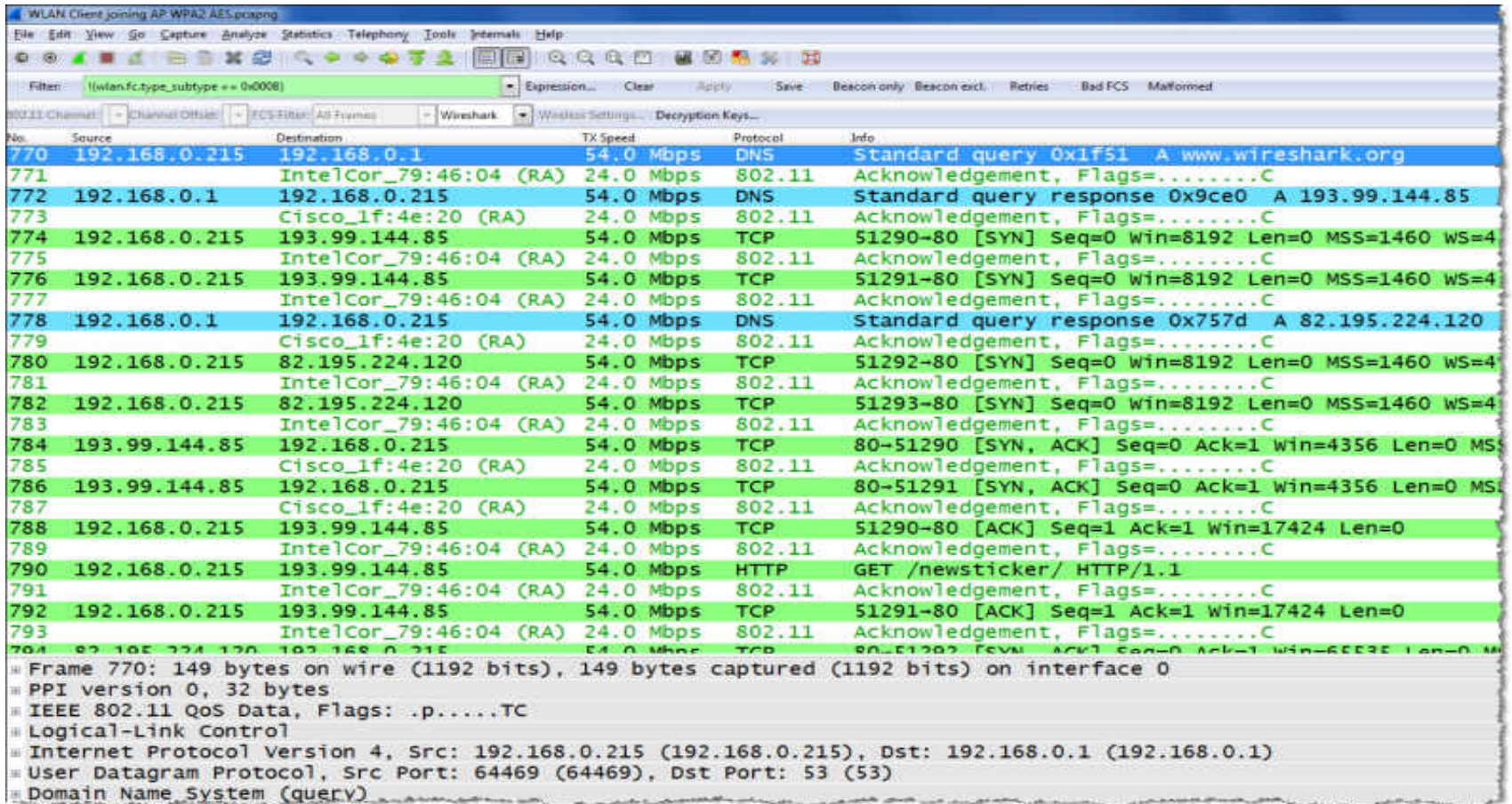
WLAN Layer 2 Analysis

- 802.11 frames look different from Ethernet frames
- WLAN frames have from one to four MAC addresses



WLAN Layer 2 Analysis

Data Transmission (single packets)



| No. | Source | Destination | Tx Speed | Protocol | Info |
|-----|----------------|------------------------|-----------|----------|----------------------------------------------------|
| 770 | 192.168.0.215 | 192.168.0.1 | 54.0 Mbps | DNS | Standard query 0x1f51 A www.wireshark.org |
| 771 | | IntelCor_79:46:04 (RA) | 24.0 Mbps | 802.11 | Acknowledgement, Flags=.....C |
| 772 | 192.168.0.1 | 192.168.0.215 | 54.0 Mbps | DNS | Standard query response 0x9ce0 A 193.99.144.85 |
| 773 | | Cisco_1f:4e:20 (RA) | 24.0 Mbps | 802.11 | Acknowledgement, Flags=.....C |
| 774 | 192.168.0.215 | 193.99.144.85 | 54.0 Mbps | TCP | 51290-80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 |
| 775 | | IntelCor_79:46:04 (RA) | 24.0 Mbps | 802.11 | Acknowledgement, Flags=.....C |
| 776 | 192.168.0.215 | 193.99.144.85 | 54.0 Mbps | TCP | 51291-80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 |
| 777 | | IntelCor_79:46:04 (RA) | 24.0 Mbps | 802.11 | Acknowledgement, Flags=.....C |
| 778 | 192.168.0.1 | 192.168.0.215 | 54.0 Mbps | DNS | Standard query response 0x757d A 82.195.224.120 |
| 779 | | Cisco_1f:4e:20 (RA) | 24.0 Mbps | 802.11 | Acknowledgement, Flags=.....C |
| 780 | 192.168.0.215 | 82.195.224.120 | 54.0 Mbps | TCP | 51292-80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 |
| 781 | | IntelCor_79:46:04 (RA) | 24.0 Mbps | 802.11 | Acknowledgement, Flags=.....C |
| 782 | 192.168.0.215 | 82.195.224.120 | 54.0 Mbps | TCP | 51293-80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 |
| 783 | | IntelCor_79:46:04 (RA) | 24.0 Mbps | 802.11 | Acknowledgement, Flags=.....C |
| 784 | 193.99.144.85 | 192.168.0.215 | 54.0 Mbps | TCP | 80-51290 [SYN, ACK] Seq=0 Ack=1 win=4356 Len=0 MS |
| 785 | | Cisco_1f:4e:20 (RA) | 24.0 Mbps | 802.11 | Acknowledgement, Flags=.....C |
| 786 | 193.99.144.85 | 192.168.0.215 | 54.0 Mbps | TCP | 80-51291 [SYN, ACK] Seq=0 Ack=1 win=4356 Len=0 MS |
| 787 | | Cisco_1f:4e:20 (RA) | 24.0 Mbps | 802.11 | Acknowledgement, Flags=.....C |
| 788 | 192.168.0.215 | 193.99.144.85 | 54.0 Mbps | TCP | 51290-80 [ACK] Seq=1 Ack=1 Win=17424 Len=0 |
| 789 | | IntelCor_79:46:04 (RA) | 24.0 Mbps | 802.11 | Acknowledgement, Flags=.....C |
| 790 | 192.168.0.215 | 193.99.144.85 | 54.0 Mbps | HTTP | GET /newsticker/ HTTP/1.1 |
| 791 | | IntelCor_79:46:04 (RA) | 24.0 Mbps | 802.11 | Acknowledgement, Flags=.....C |
| 792 | 192.168.0.215 | 193.99.144.85 | 54.0 Mbps | TCP | 51291-80 [ACK] Seq=1 Ack=1 Win=17424 Len=0 |
| 793 | | IntelCor_79:46:04 (RA) | 24.0 Mbps | 802.11 | Acknowledgement, Flags=.....C |
| 794 | 82.195.224.120 | 192.168.0.215 | 54.0 Mbps | TCP | 80-51292 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MS |

Frame 770: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0

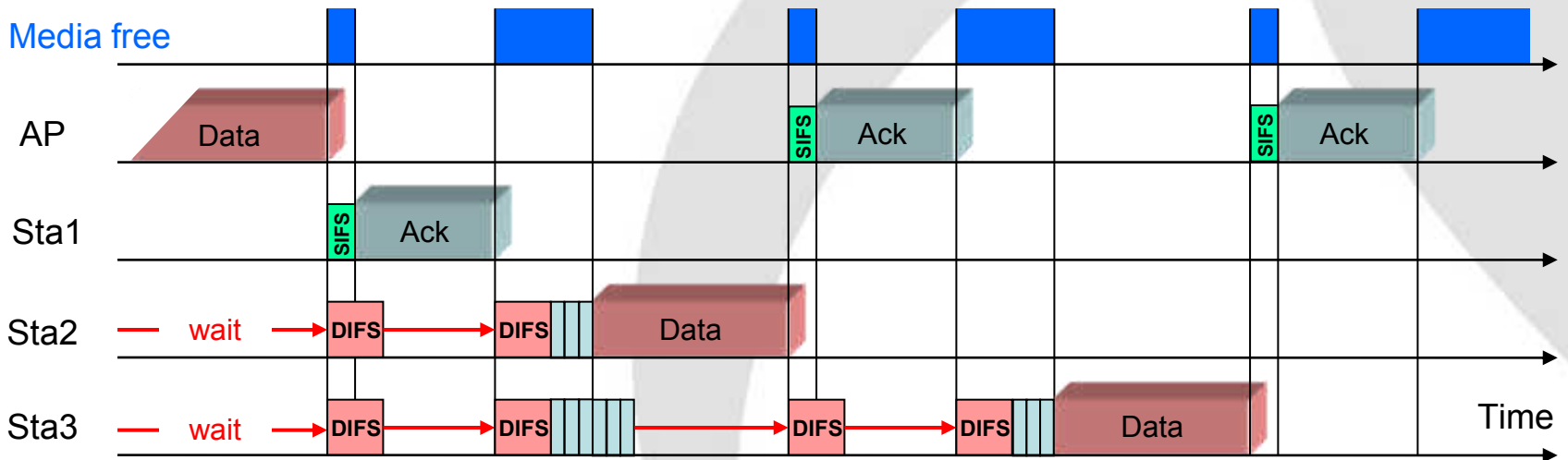
- PPID version 0, 32 bytes
- IEEE 802.11 QoS Data, Flags: .p.....TC
- Logical-Link Control
- Internet Protocol Version 4, Src: 192.168.0.215 (192.168.0.215), Dst: 192.168.0.1 (192.168.0.1)
- User Datagram Protocol, Src Port: 64469 (64469), Dst Port: 53 (53)
- Domain Name System (query)

Acks must follow immediately after a Data frame and have no source address.

WLAN Layer 2 Analysis

- Access method Carrier Sense, Multiple Access w. Collision Avoidance CSMA/CA
- Different time spaces control the access to the shared media

| | | |
|-----------------------------------------------------------|---------------------------------------------------------|---------------------------------------|
| SIFS (Short Inter Frame Space) | 802.11b/g = 10 μ s | 802.11a = 16 μ s |
| DIFS (DCF Inter Frame Space) (2x Slot time + SIFS) | 802.11b=50 μ s | 802.11g=28 μ s 802.11a=34 μ s |
| Slot Time 802.11b = 20 μ s (max. 31x) | Short Slot Time 802.11a/g = 9 μ s (max. 15x) | |



- If media is free, each station waits **DIFS** and a random number of **Slot Times**

WLAN Layer 2 Analysis

Frame Types Overview

Management Frames:

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

Control Frames:

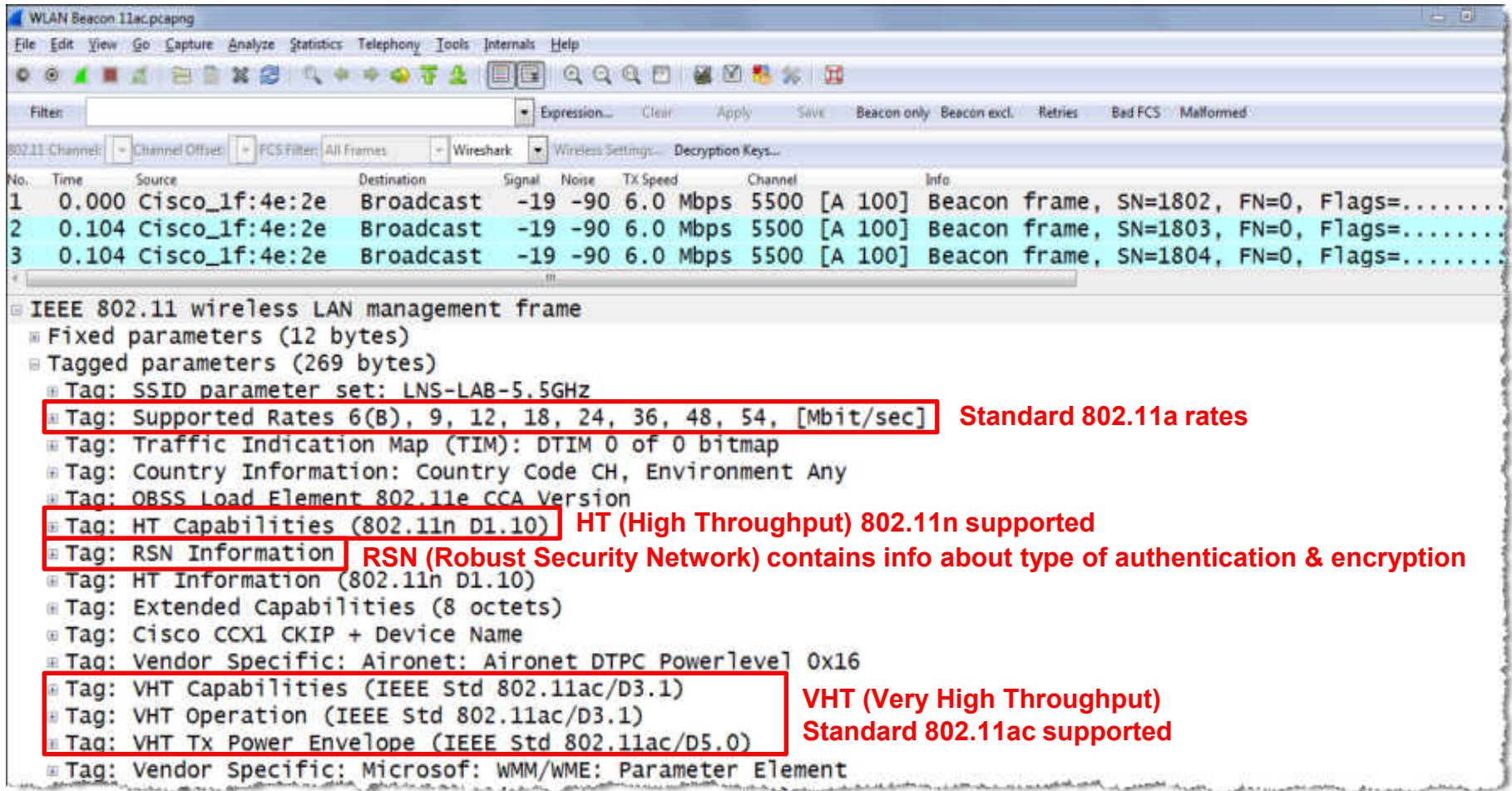
- Request to Send (RTS)
- Clear to Send (CTS)
- Acknowledge / Block Acknowledge Request / Block Acknowledge
- Power Save Poll

Data Frames:

- Data
- Null Function

WLAN Layer 2 Analysis

Beacon Tags



The image shows a Wireshark capture of three IEEE 802.11 Beacon frames. The packet list pane shows the following details:

| No. | Time | Source | Destination | Signal | Noise | TX Speed | Channel | Info |
|-----|-------|----------------|-------------|--------|-------|----------|--------------|------------------------------------------|
| 1 | 0.000 | Cisco_1f:4e:2e | Broadcast | -19 | -90 | 6.0 Mbps | 5500 [A 100] | Beacon frame, SN=1802, FN=0, Flags=..... |
| 2 | 0.104 | Cisco_1f:4e:2e | Broadcast | -19 | -90 | 6.0 Mbps | 5500 [A 100] | Beacon frame, SN=1803, FN=0, Flags=..... |
| 3 | 0.104 | Cisco_1f:4e:2e | Broadcast | -19 | -90 | 6.0 Mbps | 5500 [A 100] | Beacon frame, SN=1804, FN=0, Flags=..... |

The packet details pane for the selected frame shows the following tags:

- Tag: SSID parameter set: LNS-LAB-5.5GHZ
- Tag: Supported Rates 6(B), 9, 12, 18, 24, 36, 48, 54, [Mbit/sec] **Standard 802.11a rates**
- Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
- Tag: Country Information: Country Code CH, Environment Any
- Tag: OBSS Load Element 802.11e CCA Version
- Tag: HT Capabilities (802.11n D1.10) **HT (High Throughput) 802.11n supported**
- Tag: RSN Information **RSN (Robust Security Network) contains info about type of authentication & encryption**
- Tag: HT Information (802.11n D1.10)
- Tag: Extended Capabilities (8 octets)
- Tag: Cisco CCX1 CKIP + Device Name
- Tag: Vendor Specific: Aironet: Aironet DTPC Powerlevel 0x16
- Tag: VHT Capabilities (IEEE Std 802.11ac/D3.1) **VHT (Very High Throughput) Standard 802.11ac supported**
- Tag: VHT Operation (IEEE Std 802.11ac/D3.1)
- Tag: VHT Tx Power Envelope (IEEE Std 802.11ac/D5.0)
- Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element

Beacons tags contain information about supported and required features

WLAN Layer 2 Analysis

Probe Request / Probe Response

The image shows a Wireshark capture of WLAN traffic. The filter is set to `(wlan.fc.type_subtype == 0x0008)`. The capture shows several frames:

| Source | Destination | Info |
|---------------------|-------------------|----------------------------------------------------------------------------|
| IntelCor_79:46:04 | Broadcast | Probe Request, SN=182, FN=0, Flags=.....C, SSID=Broadcast |
| Cisco_1f:4e:2e | IntelCor_79:46:04 | Probe Response, SN=2346, FN=0, Flags=...R...C, BI=102, SSID=LNS-LAB-5.5GHZ |
| Cisco_1f:4e:2e (RA) | | Acknowledgement, Flags=.....C |
| IntelCor_79:46:04 | Broadcast | Probe Request, SN=183, FN=0, Flags=.....C, SSID=LNS WLAN |
| IntelCor_79:46:04 | Broadcast | Probe Request, SN=184, FN=0, Flags=.....C, SSID=Broadcast |
| Cisco_1f:4e:2e | IntelCor_79:46:04 | Probe Response, SN=2347, FN=0, Flags=...R...C, BI=102, SSID=LNS-LAB-5.5GHZ |
| Cisco_1f:4e:2e (RA) | | Acknowledgement, Flags=.....C |
| 00:00:00_00:00:00 | 76:26:ac:1f:7f:f0 | I, N(R)=0, N(S)=0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command |
| IntelCor_79:46:04 | Broadcast | Probe Request, SN=221, FN=0, Flags=.....C, SSID=Broadcast |
| Cisco_1f:4e:2e | IntelCor_79:46:04 | Probe Response, SN=2348, FN=0, Flags=...R...C, BI=102, SSID=LNS-LAB-5.5GHZ |
| Cisco_1f:4e:2e (RA) | | Acknowledgement, Flags=.....C |
| IntelCor_79:46:04 | Broadcast | Probe Request, SN=222, FN=0, Flags=.....C, SSID=LNS WLAN |
| IntelCor_79:46:04 | Broadcast | Probe Request, SN=223, FN=0, Flags=.....C, SSID=Broadcast |

Frame 31 details:

- Frame 31: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
- PPI version 0, 32 bytes
- IEEE 802.11 Probe Request, Flags:C
- IEEE 802.11 wireless LAN management frame
 - Tagged parameters (54 bytes)
 - Tag: SSID parameter set: Broadcast
 - Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
 - Tag: HT Capabilities (802.11n D1.10)
 - Tag: VHT Capabilities (IEEE Std 802.11ac/D3.1)

Client supports 802.11a/n/ac

- Clients scan for Access Points through all channels using **Probe Request**
- Probe Request contains client features and **specific or broadcast SSID**
- Access Points reply with **Probe Response**, containing same fields as **Beacon**

WLAN Layer 2 Analysis

Following a roaming client with two AirPcap adapters

The image shows a Wireshark capture of WLAN traffic. The interface includes a menu bar, a toolbar, a filter field, and a packet list table. The table displays 200 packets, with columns for No., Time, Channel, Source, Destination, Length, Protocol, and Info. The traffic shows a client (192.168.0.203) moving between two access points (Cisco_11:1f:60 and Cisco_92:ad:21). Key events include an ICMP ping request and reply, and several 802.11 Beacon frames and authentication/association frames.

| No. | Time | Channel | Source | Destination | Length | Protocol | Info |
|-----|-------|--------------|------------------|-------------------|--------|----------|------------------------|
| 178 | 0.056 | 2412 [BG 1] | Cisco_11:1f:60 | Broadcast | 197 | 802.11 | Beacon frame, SN=2024, |
| 179 | 0.045 | 2462 [BG 11] | Cisco_92:ad:21 | Broadcast | 152 | 802.11 | Beacon frame, SN=744, |
| 180 | 0.056 | 2412 [BG 1] | Cisco_11:1f:60 | Broadcast | 197 | 802.11 | Beacon frame, SN=2025, |
| 181 | 0.045 | 2462 [BG 11] | Cisco_92:ad:21 | Broadcast | 152 | 802.11 | Beacon frame, SN=745, |
| 182 | 0.056 | 2412 [BG 1] | Cisco_11:1f:60 | Broadcast | 197 | 802.11 | Beacon frame, SN=2026, |
| 183 | 0.018 | 2412 [BG 1] | 192.168.0.203 | 192.168.0.1 | 120 | ICMP | Echo (ping) request |
| 184 | 0.000 | 2412 [BG 1] | | Philips_45:7f:2f | 38 | 802.11 | Acknowledgement, Flags |
| 185 | 0.001 | 2412 [BG 1] | 192.168.0.1 | 192.168.0.203 | 120 | ICMP | Echo (ping) reply |
| 186 | 0.000 | 2412 [BG 1] | | Cisco_11:1f:60 (f | 38 | 802.11 | Acknowledgement, Flags |
| 187 | 0.025 | 2462 [BG 11] | Cisco_92:ad:21 | Broadcast | 152 | 802.11 | Beacon frame, SN=746, |
| 188 | 0.056 | 2412 [BG 1] | Cisco_11:1f:60 | Broadcast | 197 | 802.11 | Beacon frame, SN=2028, |
| 189 | 0.045 | 2462 [BG 11] | Cisco_92:ad:21 | Broadcast | 152 | 802.11 | Beacon frame, SN=747, |
| 190 | 0.000 | 2462 [BG 11] | Philips_45:7f:2f | Cisco_92:ad:21 | 58 | 802.11 | Authentication, SN=284 |
| 191 | 0.000 | 2462 [BG 11] | | Philips_45:7f:2f | 38 | 802.11 | Acknowledgement, Flags |
| 192 | 0.000 | 2462 [BG 11] | Cisco_92:ad:21 | Philips_45:7f:2f | 58 | 802.11 | Authentication, SN=749 |
| 193 | 0.000 | 2462 [BG 11] | | Cisco_92:ad:21 (f | 38 | 802.11 | Acknowledgement, Flags |
| 194 | 0.001 | 2462 [BG 11] | Philips_45:7f:2f | Cisco_92:ad:21 | 107 | 802.11 | Reassociation Request |
| 195 | 0.000 | 2462 [BG 11] | | Philips_45:7f:2f | 38 | 802.11 | Acknowledgement, Flags |
| 196 | 0.001 | 2462 [BG 11] | Cisco_92:ad:21 | Philips_45:7f:2f | 108 | 802.11 | Reassociation Response |
| 197 | 0.000 | 2462 [BG 11] | | Cisco_92:ad:21 (f | 38 | 802.11 | Acknowledgement, Flags |
| 198 | 0.051 | 2412 [BG 1] | Cisco_11:1f:60 | Broadcast | 197 | 802.11 | Beacon frame, SN=2029, |
| 199 | 0.045 | 2462 [BG 11] | Cisco_92:ad:21 | Broadcast | 152 | 802.11 | Beacon frame, SN=748, |
| 200 | 0.056 | 2412 [BG 1] | Cisco_11:1f:60 | Broadcast | 197 | 802.11 | Beacon frame, SN=2030, |

WLAN Layer 2 Analysis

Association Request / Association Response

| Source | Destination | Info |
|------------------------|---------------------|---------------------------------------------------|
| IntelCor_79:46:04 | Cisco_1f:4e:20 | Authentication, SN=15, FN=0, Flags=.....C |
| IntelCor_79:46:04 (RA) | IntelCor_79:46:04 | Acknowledgement, Flags=.....C |
| Cisco_1f:4e:20 | IntelCor_79:46:04 | Authentication, SN=1598, FN=0, Flags=.....C |
| Cisco_1f:4e:20 (RA) | Cisco_1f:4e:20 | Acknowledgement, Flags=.....C |
| IntelCor_79:46:04 | Cisco_1f:4e:20 | Association Request, SN=16, FN=0, Flags=.....C, |
| IntelCor_79:46:04 (RA) | IntelCor_79:46:04 | Acknowledgement, Flags=.....C |
| Cisco_1f:4e:20 | IntelCor_79:46:04 | Association Response, SN=1600, FN=0, Flags=.....C |
| Cisco_1f:4e:20 (RA) | Cisco_1f:4e:20 | Acknowledgement, Flags=.....C |
| Cisco_1f:4e:20 | IntelCor_79:46:04 | Key (Message 1 of 4) ← |
| Cisco_1f:4e:20 | IntelCor_79:46:04 | Key (Message 1 of 4) ← |
| IntelCor_79:46:04 | Cisco_1f:4e:20 (RA) | Acknowledgement, Flags=.....C |
| IntelCor_79:46:04 | Cisco_1f:4e:20 | Key (Message 2 of 4) ← |
| IntelCor_79:46:04 (RA) | IntelCor_79:46:04 | Acknowledgement, Flags=.....C |
| Cisco_1f:4e:20 | IntelCor_79:46:04 | Key (Message 3 of 4) ← |
| Cisco_1f:4e:20 (RA) | IntelCor_79:46:04 | Acknowledgement, Flags=.....C |
| IntelCor_79:46:04 | Cisco_1f:4e:20 | Key (Message 4 of 4) ← |
| IntelCor_79:46:04 (RA) | IntelCor_79:46:04 | Acknowledgement, Flags=.....C |
| 0.0.0.0 | 255.255.255.255 | DHCP Request - Transaction ID 0x86dfddf2 |
| IntelCor_79:46:04 (RA) | IntelCor_79:46:04 | Acknowledgement, Flags=.....C |
| IntelCor_79:46:04 | Broadcast | who has 192.168.0.1? Tell 192.168.0.215 |

Key messages 1 - 4 must be captured to enable Wireshark to encrypt data

- Authentication is old WEP legacy stuff; still there, but has no function.
- Clients associates with Access Point and negotiates WPA session key.
- All frames are acknowledged or retransmitted by the sender.

WLAN Layer 2 Analysis

Data Transmission (multiple packets in aggregation mode)

The image shows a Wireshark capture of an IEEE 802.11 Block Acknowledgment frame. The packet list pane shows a sequence of packets: a Block Ack (No. 4579), followed by several Unreassembled A-MPDU data packets (Nos. 4580-4586), a UDP packet (No. 4587), and another Block Ack (No. 4588). The details pane for the selected Block Ack (No. 4579) shows the following structure:

- IEEE 802.11 802.11 Block Ack, Flags:C
 - Type/Subtype: 802.11 Block Ack (0x19)
 - Frame Control: 0x0094 (Normal)
 - Duration: 0
 - Receiver address: Cisco_a0:8d:c0 (00:17:df:a0:8d:c0)
 - Transmitter address: Buffalo_73:05:af (00:16:01:73:05:af)
 - Block Ack Request Type: Compressed Block (0x02)
 - Block Ack (BA) Control: 0x0004
 - Block Ack Starting Sequence Control (SSC): 0x56d0
 - Block Ack Bitmap
 - Frame check sequence: 0xf47ea4d2 [correct]

The hex dump at the bottom shows the raw bytes of the frame, with the Block Ack Bitmap field (0010) containing the value 0100000001006c00501440010000d1a0.

- 802.11n/ac supports up to 64 packet in a burst with a single **Block Acknowledge**.
- Block Ack contains **Bitmap** to ack only good packets, other will be sent again.

WLAN Layer 2 Analysis

Interoperability between WLAN generations

- Interoperability between 802.11b/g/n and 802.11a/n/ac is granted.
- Mixed operations come at a cost: lower throughput.
- Indicated throughput values are valid for non-mixed environment and small cells.
- Clients at the border of cells transmit at low speed and use longer airtime.
- Shrink your cell size and gain bandwidth by disabling lower rates in Access Points.
- Try to get rid of old clients (especially B-only) before upgrading your APs.

| No. . | Source | Destination | RSSI | Protocol | Info |
|-------|---------------|------------------------|-------|-------------|--------------------------|
| 1150 | | PhilipsC_45:7f:2f (RA) | 65 dB | IEEE 802.11 | Clear-to-send |
| 1151 | 192.168.0.201 | 192.168.0.100 | 59 dB | HTTP | GET /appsui.js HTTP/1.1 |
| 1152 | | PhilipsC_45:7f:2f (RA) | 40 dB | IEEE 802.11 | Acknowledgement |
| 1153 | | Cisco_11:1f:60 (RA) | 44 dB | IEEE 802.11 | Clear-to-send |
| 1154 | 192.168.0.100 | 192.168.0.201 | 40 dB | HTTP | Continuation or non-HTTP |
| 1155 | | Cisco_11:1f:60 (RA) | 62 dB | IEEE 802.11 | Acknowledgement |
| 1156 | | Cisco_11:1f:60 (RA) | 44 dB | IEEE 802.11 | Clear-to-send |
| 1157 | 192.168.0.100 | 192.168.0.201 | 40 dB | HTTP | Continuation or non-HTTP |
| 1158 | | Cisco_11:1f:60 (RA) | 62 dB | IEEE 802.11 | Acknowledgement |

- Old clients must be silenced with Request-to-Send / Clear-to-send (RTS/CTS) or Clear-to-Send-Self (CTS-Self) frames sent before each data frame.
- This process will significantly reduce the total cell throughput.

WLAN Layer 2 Analysis (Case two)

Customer problem analyzed and solved with Wireshark and AirPcap

- ▶ User is complaining about **sporadic hangers** in bar code scanners, up to minutes
- ▶ Vendors of **mobile clients** and **access points** are finger pointing, since month.
- ▶ Problem could be assigned to **bar code vendor** by analyzing trace files.

| No. | Time | Source | Destination | Channel | Protocol | Info |
|-----|--------|-------------------|------------------------|-------------|----------|-----------------------------------|
| 1 | 0.000 | ZebraTec_fb:c4:57 | Cisco_a9:3b:c0 | 5200 [A 40] | 802.11 | Null function (No data), SN=903, |
| 2 | 0.000 | ZebraTec_fb:c4:57 | Cisco_a9:3b:c0 | 5200 [A 40] | 802.11 | Null function (No data), SN=903, |
| 3 | 0.000 | ZebraTec_fb:c4:57 | ZebraTec_fb:c4:57 (RA) | 5200 [A 40] | 802.11 | Acknowledgement, Flags=.....C |
| 4 | 1.846 | ZebraTec_fb:c4:57 | All-HSRP-routers_00 | 5200 [A 40] | 802.11 | U, func=Unknown; DSAP Nestar Indi |
| 5 | 0.000 | ZebraTec_fb:c4:57 | ZebraTec_fb:c4:57 (RA) | 5200 [A 40] | 802.11 | Acknowledgement, Flags=.....C |
| 6 | 0.006 | ZebraTec_fb:c4:57 | Cisco_a9:3c:60 | 5180 [A 36] | 802.11 | Authentication, SN=911, FN=0, Fla |
| 7 | 0.000 | ZebraTec_fb:c4:57 | ZebraTec_fb:c4:57 (RA) | 5180 [A 36] | 802.11 | Acknowledgement, Flags=.....C |
| 8 | 0.000 | Cisco_a9:3c:60 | ZebraTec_fb:c4:57 | 5180 [A 36] | 802.11 | Authentication, SN=502, FN=0, Fla |
| 9 | 0.000 | Cisco_a9:3c:60 | Cisco_a9:3c:60 (RA) | 5180 [A 36] | 802.11 | Acknowledgement, Flags=.....C |
| 10 | 0.003 | ZebraTec_fb:c4:57 | Cisco_a9:3c:60 | 5180 [A 36] | 802.11 | Reassociation Request, SN=912, FN |
| 11 | 0.000 | ZebraTec_fb:c4:57 | ZebraTec_fb:c4:57 (RA) | 5180 [A 36] | 802.11 | Acknowledgement, Flags=.....C |
| 12 | 0.000 | Cisco_a9:3c:60 | ZebraTec_fb:c4:57 | 5180 [A 36] | 802.11 | Reassociation Response, SN=503, F |
| 13 | 0.000 | Cisco_a9:3c:60 | Cisco_a9:3c:60 (RA) | 5180 [A 36] | 802.11 | Acknowledgement, Flags=.....C |
| 14 | 0.000 | Cisco_a9:3c:60 | ZebraTec_fb:c4:57 | 5180 [A 36] | EAP | Request, Identity |
| 15 | 0.000 | Cisco_a9:3c:60 | Cisco_a9:3c:60 (RA) | 5180 [A 36] | 802.11 | Acknowledgement, Flags=.....C |
| 16 | 30.438 | Cisco_a9:3c:60 | ZebraTec_fb:c4:57 | 5180 [A 36] | 802.11 | Deauthentication, SN=849, FN=0, F |
| 17 | 0.000 | Cisco_a9:3c:60 | Cisco_a9:3c:60 (RA) | 5180 [A 36] | 802.11 | Acknowledgement, Flags=.....C |
| 18 | 1.289 | ZebraTec_fb:c4:57 | Cisco_a9:3c:60 | 5180 [A 36] | 802.11 | Authentication, SN=919, FN=0, Fla |
| 19 | 0.000 | ZebraTec_fb:c4:57 | ZebraTec_fb:c4:57 (RA) | 5180 [A 36] | 802.11 | Acknowledgement, Flags=.....C |
| 20 | 0.000 | Cisco_a9:3c:60 | ZebraTec_fb:c4:57 | 5180 [A 36] | 802.11 | Authentication, SN=866, FN=0, Fla |
| 21 | 0.000 | Cisco_a9:3c:60 | Cisco_a9:3c:60 (RA) | 5180 [A 36] | 802.11 | Acknowledgement, Flags=.....C |

WLAN technology coming soon...



| 802.11n/ac Physical Rate Table (Mbps) | | | | | | | | |
|---------------------------------------|------------|---------------------|--------------------|---------------------|-------|-------|-------|--------------|
| Number of Streams | Modulation | Antennas Tx x Rx | Spatial Streams | Maximum Rate (Mbps) | | | | Band Support |
| | | | | 1 Ch. | 2 Ch. | 4 Ch. | 8 Ch. | |
| One Stream* | 64-QAM | 1 x 1 | 1 | 72 | 150 | n.a. | n.a. | 2.4 & 5 GHz |
| Two Streams* | 64-QAM | 2 x 2 | 2 | 144 | 300 | n.a. | n.a. | 2.4 & 5 GHz |
| Three Streams | 64-QAM | 3 x 3 | 3 | 216 | 450 | n.a. | n.a. | 2.4 & 5 GHz |
| Four Streams | 64-QAM | 4 x 4 | 4 | 288 | 600 | n.a. | n.a. | 2.4 & 5 GHz |

* AirPcap Nx supports 802.11n with up to two Spatial Streams (2x2:2) in Legacy, HT20 or HT40 mode (no SGI & Greenfield mode)



| | | | | | | | | |
|---------------|---------|-------|---|-----|-----|------|------|-------|
| One Stream | 256-QAM | 1 x 1 | 1 | 86 | 200 | 433 | n.a. | 5 GHz |
| Two Streams | 256-QAM | 2 x 2 | 2 | 173 | 400 | 866 | n.a. | 5 GHz |
| Three Streams | 256-QAM | 3 x 3 | 3 | 289 | 600 | 1300 | n.a. | 5 GHz |



| | | | | | | | | |
|---------------|---------|-------|---|-----|------|------|------|-------|
| One Stream | 256-QAM | 1 x 1 | 1 | 86 | 200 | 433 | 866 | 5 GHz |
| Two Streams | 256-QAM | 2 x 2 | 2 | 173 | 400 | 866 | 1730 | 5 GHz |
| Three Streams | 256-QAM | 3 x 3 | 3 | 289 | 600 | 1300 | 2600 | 5 GHz |
| Four Streams | 256-QAM | 4 x 4 | 4 | 385 | 800 | 1730 | 3470 | 5 GHz |
| Eight Streams | 256-QAM | 8 x 8 | 8 | 770 | 1600 | 3470 | 6930 | 5 GHz |

WLAN technology coming soon...

Unofficially announced: A new **AirPcap adapter** from **riverbed**

Supporting Short Guard Interval (SGI), 3x3 MIMO, AC and more...
Planned availability: early 2016

| Product Requirements | Atheros AR9342 with Qualcomm/Atheros QCA9880 |
|--------------------------------------------------------------------------------|----------------------------------------------|
| 3x3 MIMO | X |
| USB 3.0 (5Gbps or 640MB/s) | USB 2.0 (480Mbps or 60MB/s) |
| 802.11ac (Theoretical max. 6,933Mbps or 900MB/s - Up to 8x 866.7Mbps channels) | X |
| 802.11abgn (802.11n max. 600MB/s) | X |
| Win8 | |
| External Antenna | 3 |
| USB stick form factor | External USB Enclosure |
| Short Guard Interval | X |
| Channel Support | 2.412-2.472Ghz, 5.180-5.825Ghz, TBD |

Source: Riverbed Technology (specs. without commitment)

Thank you for your attention



Rolf Leutert, Leutert NetServices, www.wireshark.ch