

Analyzing WLANs with Wireshark & AirPcap

Sessions BU-5

Rolf Leutert

Consultant & Trainer | Leutert NetServices, Switzerland









SHARKFEST '09

Stanford University

June 15-18, 2009

SHARKFEST '09

Agenda

-  Setting up Wireshark with AirPcap
-  Capturing WLAN data
-  WLAN Management, Control & Data Frames
-  WLAN Frame Formats
-  Analyzing: Client can not associate
-  Analyzing: Roaming problems
-  Analyzing: Throughput issues
-  Multiple-Input, Multiple-Output (MIMO)

Creating a WLAN profile

The screenshot shows the Wireshark Network Analyzer interface. The 'Edit' menu is open, and the 'Configuration Profiles...' option is selected. A dialog box titled 'Wireshark: Configuration Profiles' is open, showing a list of profiles with 'WLAN' selected. A 'New' button is highlighted, and the 'Profile name' field contains 'WLAN'. Three callout boxes provide instructions:

1. Click 'Edit' and 'Configuration profiles'
2. Select 'New' and enter name
3. Verify selected profile

The Wireless Toolbar

The screenshot shows the Wireshark interface with the 'View' menu open. The 'Wireless Toolbar' option is highlighted. The main display area shows a list of IEEE 802.11 Beacon frames. A red box highlights the 'FCS Filter' and 'Decryption Mode' fields in the top toolbar area.

View Menu:

- ✓ Main Toolbar
- ✓ Filter Toolbar
- ✓ **Wireless Toolbar**
- ✓ Statusbar
- ✓ Packet List
- ✓ Packet Details
- ✓ Packet Bytes
- Time Display Format
- Name Resolution
- ✓ Colorize Packet List
- ✓ Auto Scroll in Live Capture
- Zoom In (Ctrl++)
- Zoom Out (Ctrl+-)
- Normal Size (Ctrl+=)
- Resize All Columns
- Expand Subtrees
- Expand All
- Collapse All
- Coloring Rules...
- Show Packet in New Window
- Reload (Ctrl+R)

Packet List:

No.	Source	Destination	Protocol	Info
1	Ci	51 d	IEEE 802.11	Beacon frame, SN=9, FN=0, BI=100, SSID: "LNSWLAN", Name: "
2	Ci	50 d	IEEE 802.11	Beacon frame, SN=10, FN=0, BI=100, SSID: "LNSWLAN", Name: "
3	Ci	51 d	IEEE 802.11	Beacon frame, SN=11, FN=0, BI=100, SSID: "LNSWLAN", Name: "
4	Ci	49 d	IEEE 802.11	Beacon frame, SN=12, FN=0, BI=100, SSID: "LNSWLAN", Name: "
5	Ci	51 d	IEEE 802.11	Beacon frame, SN=13, FN=0, BI=100, SSID: "LNSWLAN", Name: "
6	Ci	49 d	IEEE 802.11	Beacon frame, SN=14, FN=0, BI=100, SSID: "LNSWLAN", Name: "
7	Ci	50 d	IEEE 802.11	Beacon frame, SN=15, FN=0, BI=100, SSID: "LNSWLAN", Name: "
8	Ci	49 d	IEEE 802.11	Beacon frame, SN=16, FN=0, BI=100, SSID: "LNSWLAN", Name: "
9	Ci	51 d	IEEE 802.11	Beacon frame, SN=17, FN=0, BI=100, SSID: "LNSWLAN", Name: "

Packet Details:

Not strictly ordered

cast (ff:ff:ff:ff:ff:ff)

f:60 (00:0f:24:11:1f:60)

BSS Id: Cisco 11:1f:60 (00:0f:24:11:1f:60)

The Wireless Toolbar

The screenshot shows the Wireshark interface for a capture named 'WLAN Beacon.pcap'. The 'AirPcap Interface' is set to '#00' and the '802.11 Channel' dropdown is open, displaying a list of channels from 1 to 14. The main packet list shows several IEEE 802.11 Beacon frames with SSID 'LNSWLAN'. A callout bubble points to the text '802.11 Channel number'.

No.	Source	Destination	SI	Protocol	Info
1	Cisco_11:1f:60 Bro				1 d IEEE 802.11 Beacon frame, SN=9, FN=0, BI=100, SSID: "LNSWLAN",
2	Cisco_11:1f:60 Bro				0 d IEEE 802.11 Beacon frame, SN=10, FN=0, BI=100, SSID: "LNSWLAN",
3	Cisco_11:1f:60 Bro				1 d IEEE 802.11 Beacon frame, SN=11, FN=0, BI=100, SSID: "LNSWLAN",
4	Cisco_11:1f:60 Bro				1 d IEEE 802.11 Beacon frame, SN=12, FN=0, BI=100, SSID: "LNSWLAN",
5	Cisco_11:1f:60 Bro				1 d IEEE 802.11 Beacon frame, SN=13, FN=0, BI=100, SSID: "LNSWLAN",
6	Cisco_11:1f:60 Bro				9 d IEEE 802.11 Beacon frame, SN=14, FN=0, BI=100, SSID: "LNSWLAN",
7	Cisco_11:1f:60 Bro				0 d IEEE 802.11 Beacon frame, SN=15, FN=0, BI=100, SSID: "LNSWLAN",
8	Cisco_11:1f:60 Bro				9 d IEEE 802.11 Beacon frame, SN=16, FN=0, BI=100, SSID: "LNSWLAN",
9	Cisco_11:1f:60 Bro				1 d IEEE 802.11 Beacon frame, SN=17, FN=0, BI=100, SSID: "LNSWLAN",

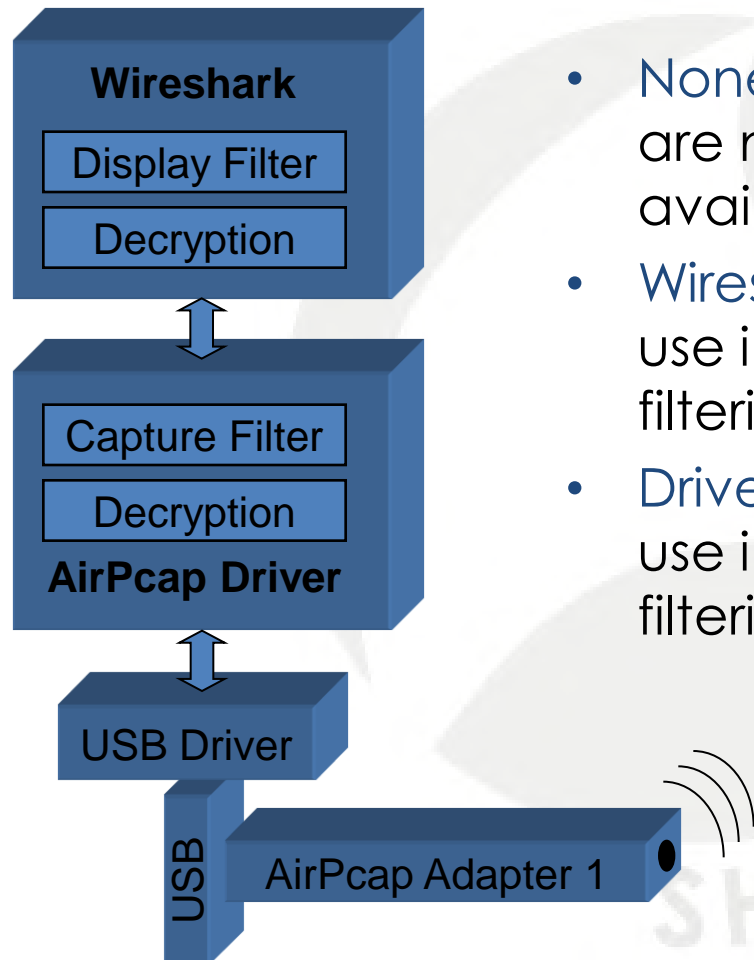
- Channel number can be changed during capturing

The Wireless Toolbar

The screenshot shows the Wireshark interface for a file named 'WLAN Beacon.pcap'. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. Below the menu is a toolbar with various icons for file operations and analysis. The 'Filter:' field is empty. The status bar at the top indicates 'AirPcap Interface: #00', '802.11 Channel: 1', 'FCS Filter: Valid Frame', 'Decryption Mode: Wireshark', and 'Wireless Settings... Decryption Keys...'. The main packet list pane shows a table of captured packets. A context menu is open over the first packet, with options: All Frames, Valid Frames, Invalid Frames, None, Wireshark, and Driver. A green callout bubble points to the 'Valid Frames' option with the text 'Show frames with or without FCS errors'. Another green callout bubble points to the 'Wireshark' and 'Driver' options with the text 'Decryption in Wireshark or in Driver'. The packet list shows several beacon frames from a Cisco source (11:1f:60) to a broadcast destination (ff:ff:ff:ff:ff:ff). The details pane at the bottom shows the following information:

0... .. = Order flag: Not strictly ordered
Duration: 0
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Source address: Cisco_11:1f:60 (00:0f:24:11:1f:60)
BSS Id: Cisco_11:1f:60 (00:0f:24:11:1f:60)
Fragment number: 0

Decryption Modes



- **None:** no decryption - use if packets are not encrypted or if key is not available
- **Wireshark:** decryption in Wireshark – use in combination with display filtering
- **Driver:** decryption in AirPcap driver – use in combination with capture filtering only

The Wireless Toolbar

The screenshot shows the Wireshark interface for a WLAN Beacon.pcap file. The main display area shows a list of captured packets, all of which are IEEE 802.11 Beacon frames from a Cisco 11:1f:60 source. The Advanced Wireless Settings dialog box is open, showing the 'Interface' as 'AirPcap Multi-Channel Aggregator' and the 'Basic Parameters' section. In the 'Basic Parameters' section, the 'Channel' is set to 2462 [BG 11], 'Channel Offset' is 0, and 'Capture Type' is set to '802.11 + Radio'. A callout bubble points to this selection with the text: 'Include Radio header to allow filtering on channel numbers'. The 'FCS Filter' is set to 'All Frames'.

No.	Source	Destination	RSSI	Protocol	Info
1	Cisco 11:1f:60	Broadcast	51	d IEEE 802.11	Beacon frame, SN=9, FN=0, BI=100, SSID: "LNSWLAN", M
2	Cisco 11:1f:60	Broadcast	50	d IEEE 802.11	Beacon frame, SN=10, FN=0, BI=100, SSID: "LNSWLAN",
3	Cisco 11:1f:60	Broadcast	51	d IEEE 802.11	Beacon frame, SN=11, FN=0, BI=100, SSID: "LNSWLAN",
4	Cis				12, FN=0, BI=100, SSID: "LNSWLAN",
5	Cis				13, FN=0, BI=100, SSID: "LNSWLAN",
6	Cis				14, FN=0, BI=100, SSID: "LNSWLAN",
7	Cis				15, FN=0, BI=100, SSID: "LNSWLAN",
8	Cis				16, FN=0, BI=100, SSID: "LNSWLAN",
9	Cis				17, FN=0, BI=100, SSID: "LNSWLAN",

The Wireless Toolbar

The screenshot shows the Wireshark interface with a WLAN Beacon.pcap file open. The main display area shows a list of 9 beacon frames, all from source Cisco_11:1f:60 to destination Broadcast. The frames are numbered 1 through 9, with varying RSSI values (51, 50, 51, 49, 51, 49, 50, 49, 51) and IEEE 802.11 Beacon frame details (SN, FN, BI). The SSID for all frames is "LNSWLAN".

A dialog box titled "Decryption Key Management" is open in the foreground. It contains a "Decryption Keys" table with the following entries:

Type	Key	SSID	
None	Select Decryption Mode		
WEP	1234abcdef		New
WEP	1234567890123456		Edit...
WPA-PWD	thisismypassword	LNSWLAN	Delete
WPA-PSK	1234567890ABCD		Up
			Down

Buttons for OK, Apply, and Cancel are at the bottom of the dialog.

Below the packet list, the packet details pane shows the following information for the selected packet:

- Order flag: Not started
- Duration: 0
- Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
- Source address: Cisco_11:1f:60 (00:0f:24:11:1f:60)
- BSS Id: Cisco_11:1f:60 (00:0f:24:11:1f:60)
- Fragment number: 0

Decryption Keys

- Wireshark supports decryption of WEP, WPA1 and WPA2 with static shared keys:
- WEP Key formats:

Keys

light * 5 ASCII Character $5 \times 8 \text{bit} = 40 + 24 \text{ bit IV} = 64 \text{ bit Key}$

1234ABCDEF 10 HEX Character $10 \times 4 \text{bit} = 40 + 24 \text{ bit IV} = 64 \text{ bit Key}$

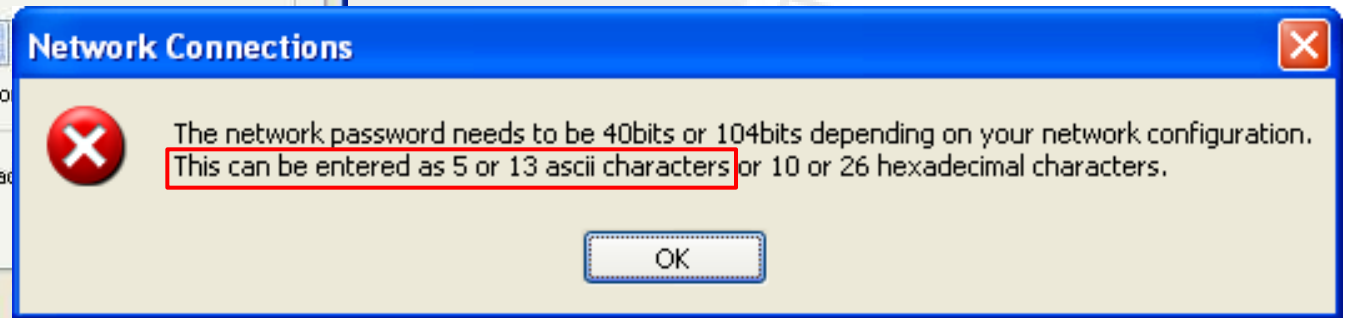
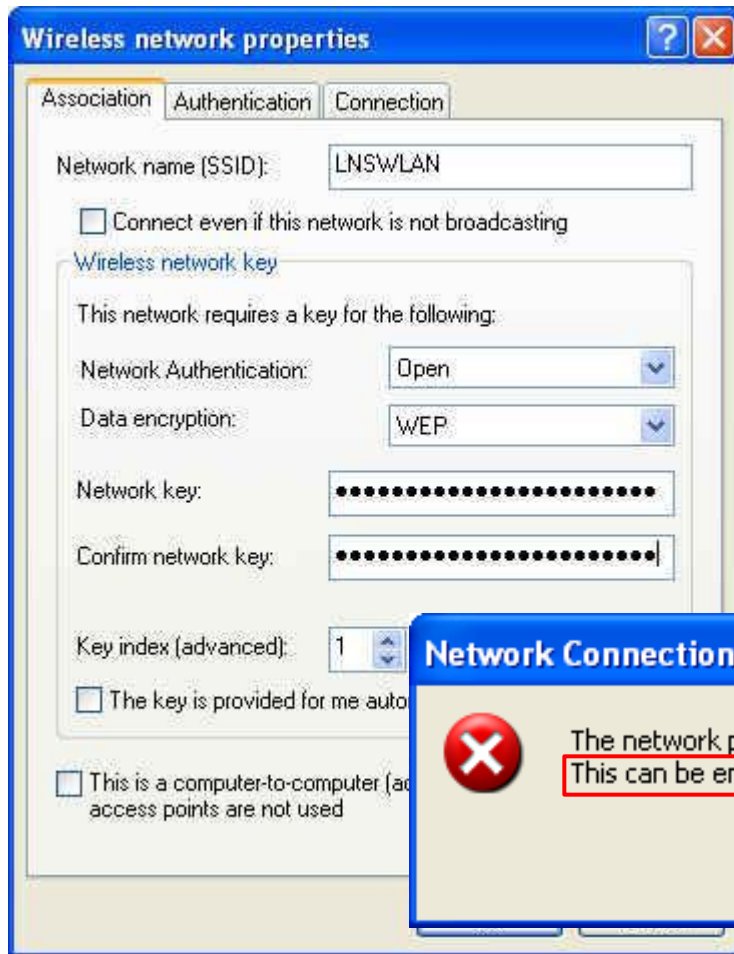
lightningstar * 13 ASCII Character $13 \times 8 \text{bit} = 104 + 24 \text{ bit IV} = 128 \text{ bit Key}$

123456..ABCDEF 26 HEX Character $26 \times 4 \text{bit} = 104 + 24 \text{ bit IV} = 128 \text{ bit Key}$

* Wireshark does not support text entries for WEP keys, use a Text-to-HEX converter like www.swingnote.com/tools/texttohex.php

Decryption Keys

- Some clients (like Windows XP or VISTA) allow WEP key entries in text (ASCII) format



Decryption Keys

- WPA-PWD (Password)

Key

SSID

thisismypassword LNSWLAN

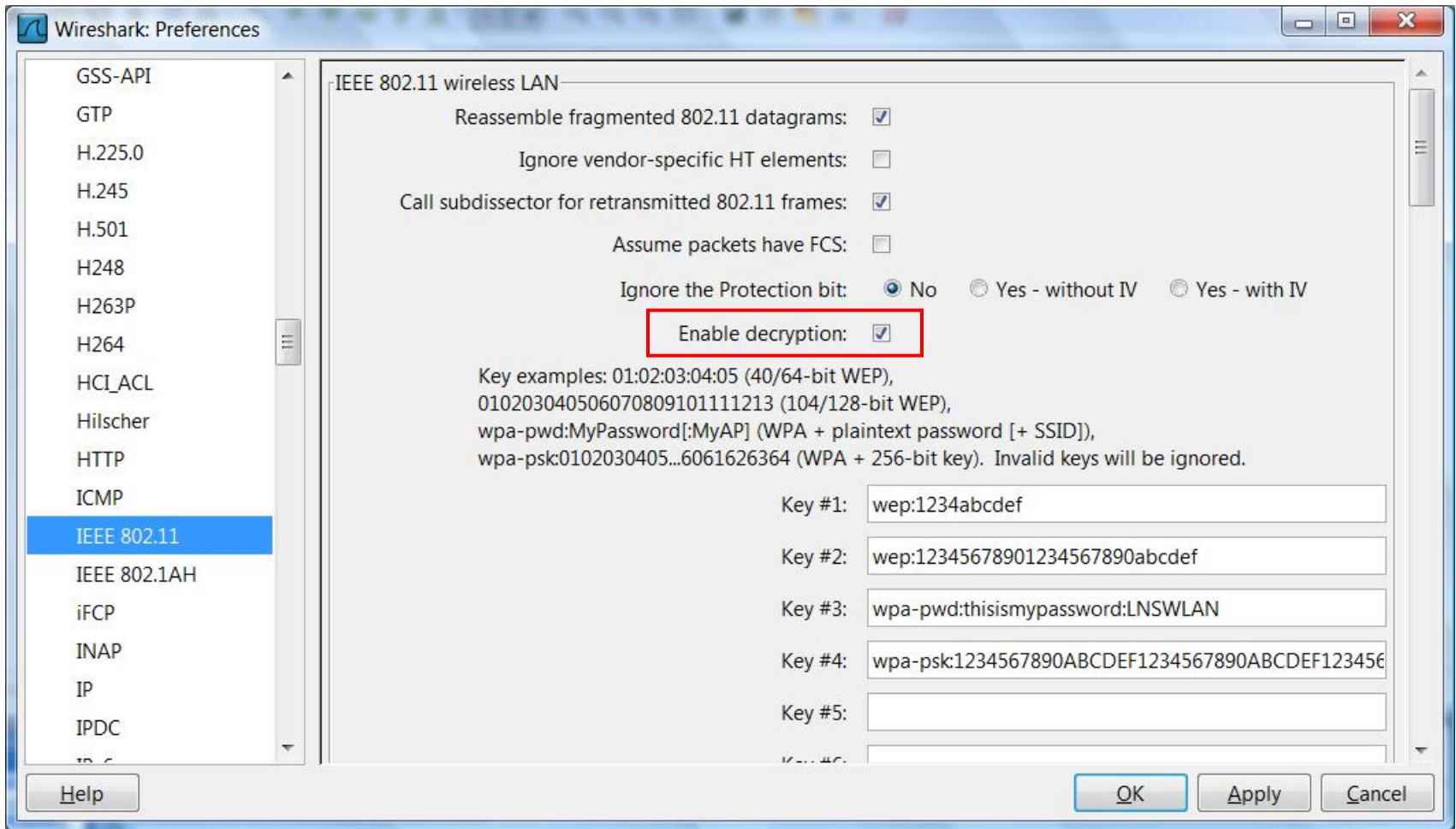
8 to 63 ASCII character password and SSID

- WPA-PSK (Pre-shared-key)

1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF

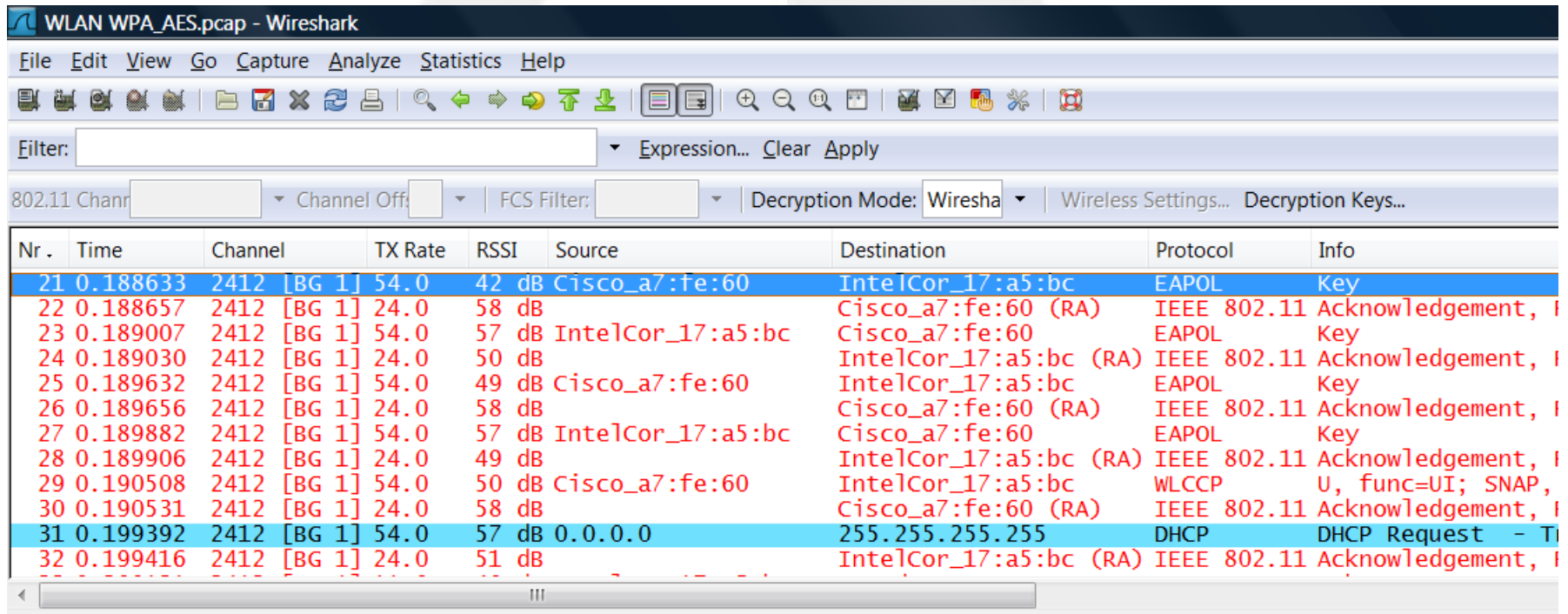
exact 64 long HEX character string

Decryption Keys



Decryption Keys

- In order to decrypt WPA, you also need to capture the key negotiation process during connection setup



WLAN WPA_AES.pcap - Wireshark

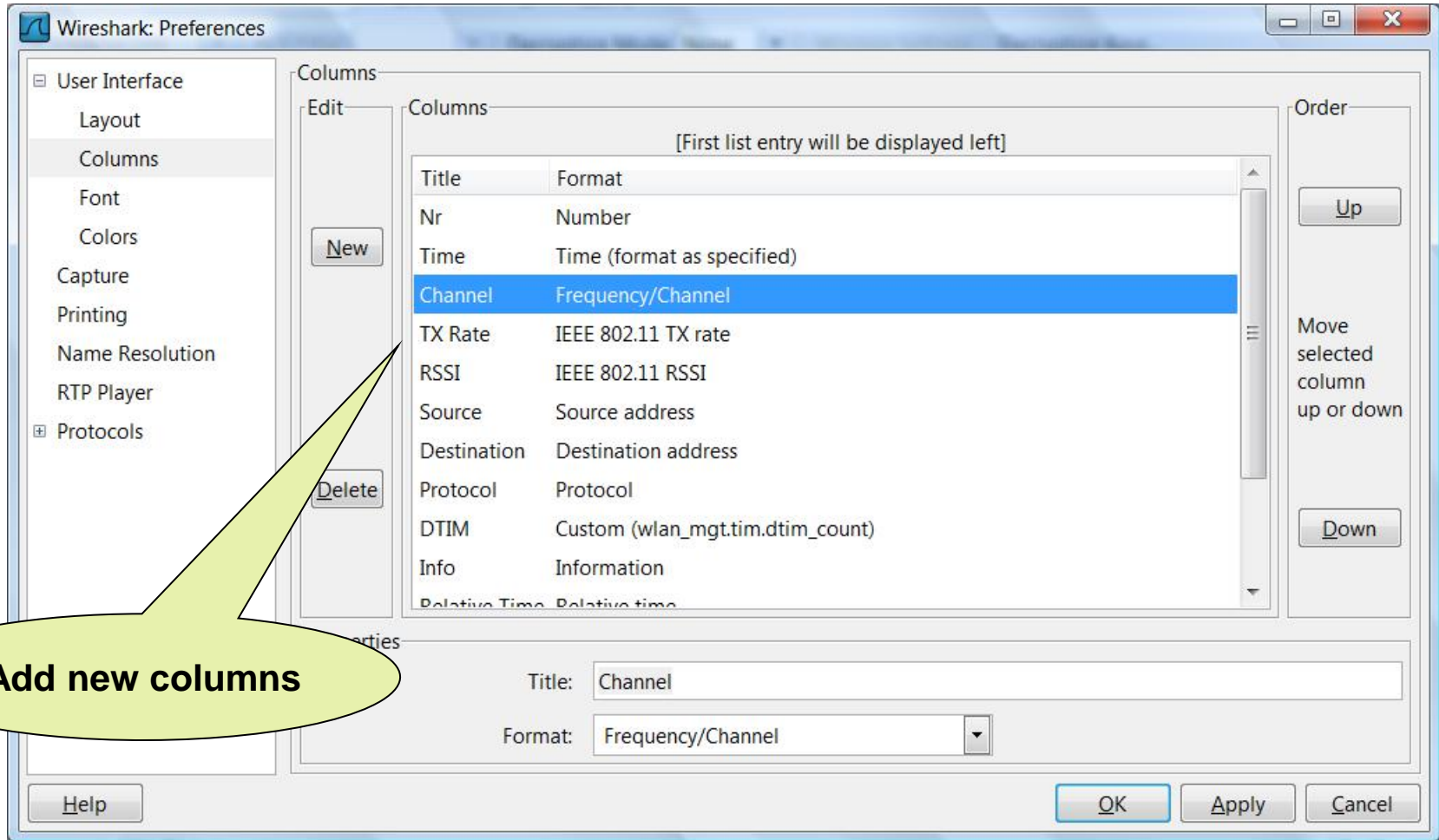
File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

802.11 Chanr Channel Off: FCS Filter: Decryption Mode: Wiresha Wireless Settings... Decryption Keys...

Nr.	Time	Channel	TX Rate	RSSI	Source	Destination	Protocol	Info
21	0.188633	2412 [BG 1]	54.0	42 dB	Cisco_a7:fe:60	IntelCor_17:a5:bc	EAPOL	Key
22	0.188657	2412 [BG 1]	24.0	58 dB		Cisco_a7:fe:60 (RA)	IEEE 802.11	Acknowledgement, F
23	0.189007	2412 [BG 1]	54.0	57 dB	IntelCor_17:a5:bc	Cisco_a7:fe:60	EAPOL	Key
24	0.189030	2412 [BG 1]	24.0	50 dB		IntelCor_17:a5:bc (RA)	IEEE 802.11	Acknowledgement, F
25	0.189632	2412 [BG 1]	54.0	49 dB	Cisco_a7:fe:60	IntelCor_17:a5:bc	EAPOL	Key
26	0.189656	2412 [BG 1]	24.0	58 dB		Cisco_a7:fe:60 (RA)	IEEE 802.11	Acknowledgement, F
27	0.189882	2412 [BG 1]	54.0	57 dB	IntelCor_17:a5:bc	Cisco_a7:fe:60	EAPOL	Key
28	0.189906	2412 [BG 1]	24.0	49 dB		IntelCor_17:a5:bc (RA)	IEEE 802.11	Acknowledgement, F
29	0.190508	2412 [BG 1]	54.0	50 dB	Cisco_a7:fe:60	IntelCor_17:a5:bc	WLCCP	U, func=UI; SNAP,
30	0.190531	2412 [BG 1]	24.0	58 dB		Cisco_a7:fe:60 (RA)	IEEE 802.11	Acknowledgement, F
31	0.199392	2412 [BG 1]	54.0	57 dB	0.0.0.0	255.255.255.255	DHCP	DHCP Request - T
32	0.199416	2412 [BG 1]	24.0	51 dB		IntelCor_17:a5:bc (RA)	IEEE 802.11	Acknowledgement, F

Tuning display for WLAN



Add new columns

Tuning display for WLAN

WLAN Beacon.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

802.11 Chanr Channel Off: FCS Filter: Decryption Mode: None Wireless Settings... Decryption Keys...

Nr.	Time	Channel	TX Rate	RSSI	Source	Destination	Protocol	DTIM	Info
1	0.000000	2412 [BG 1]	1.0	51 dB	Cisco_11:1f:60	Broadcast IEEE 802.11	IEEE 802.11	0	Beacon frame
2	0.025722	2412 [BG 1]	1.0	50 dB	Cisco_11:1f:60	Broadcast IEEE 802.11	IEEE 802.11	1	Beacon frame
3	0.128057	2412 [BG 1]	1.0	51 dB	Cisco_11:1f:60	Broadcast IEEE 802.11	IEEE 802.11	0	Beacon frame
4	0.230379	2412 [BG 1]	1.0	49 dB	Cisco_11:1f:60	Broadcast IEEE 802.11	IEEE 802.11	1	Beacon frame
5	0.332965	2412 [BG 1]	1.0	51 dB	Cisco_11:1f:60	Broadcast IEEE 802.11	IEEE 802.11	0	Beacon frame
6	0.435215	2412 [BG 1]	1.0	49 dB	Cisco_11:1f:60	Broadcast IEEE 802.11	IEEE 802.11	1	Beacon frame
7	0.537539	2412 [BG 1]	1.0	50 dB	Cisco_11:1f:60	Broadcast IEEE 802.11	IEEE 802.11	0	Beacon frame
8	0.640087	2412 [BG 1]	1.0	49 dB	Cisco_11:1f:60	Broadcast IEEE 802.11	IEEE 802.11	1	Beacon frame
9	0.742412	2412 [BG 1]	1.0	51 dB	Cisco_11:1f:60	Broadcast IEEE 802.11	IEEE 802.11	0	Beacon frame
10	0.844743	2412 [BG 1]	1.0	50 dB	Cisco_11:1f:60	Broadcast IEEE 802.11	IEEE 802.11	1	Beacon frame
11	0.947133	2412 [BG 1]	1.0	49 dB	Cisco_11:1f:60	Broadcast IEEE 802.11	IEEE 802.11	0	Beacon frame
12	1.049602	2412 [BG 1]	1.0	50 dB	Cisco_11:1f:60	Broadcast IEEE 802.11	IEEE 802.11	1	Beacon frame
13	1.151959	2412 [BG 1]	1.0	50 dB	Cisco_11:1f:60	Broadcast IEEE 802.11	IEEE 802.11	0	Beacon frame

added columns

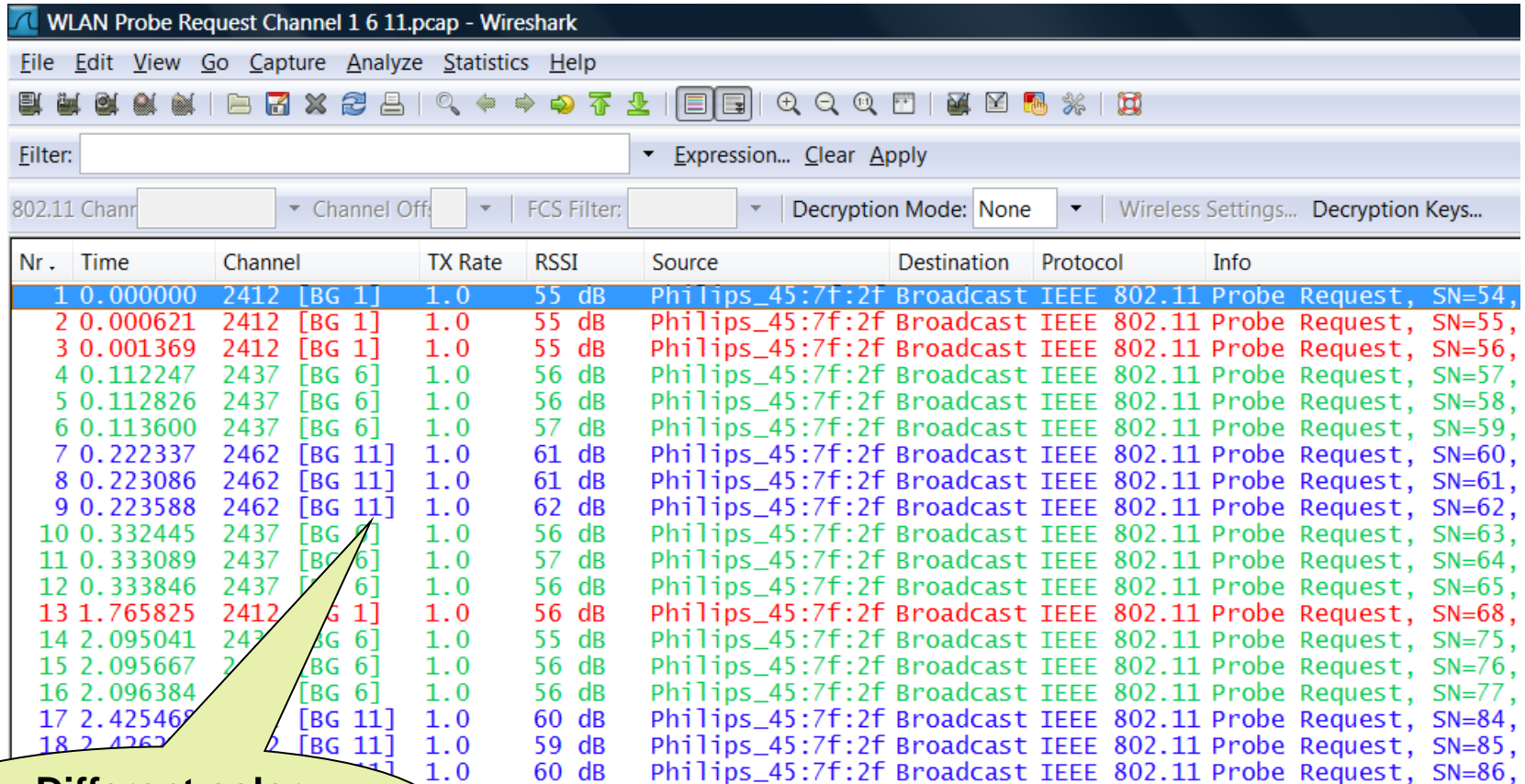
Tuning display for WLAN

The screenshot shows the Wireshark interface with a packet capture of WLAN Beacon frames. The main display area shows a list of packets with columns for Nr., Time, Channel, TX Rate, RSSI, Source, Destination, Protocol, DTIM, and Info. The packets are color-coded based on their type. A dialog box titled "Wireshark: Coloring Rules" is open, showing a list of rules with their names, strings, and colors. The rules are:

Name	String	Color
802.11 Channel 1	radiotap.channel.freq == 2412	Red
802.11 Channel 6	radiotap.channel.freq == 2437	Green
802.11 Channel 11	radiotap.channel.freq == 2462	Blue
802.11 A-MPDU	ppi.80211n-mac.flags.more_agg == 1	Red
802.11 Block-Ack	wlan.fc.type_subtype == 0x19	Yellow
802.11 Single Ack	wlan.fc.type_subtype == 0x1d	Yellow
802.11 Beacon	wlan.fc.type_subtype == 0x08	Green
802.11 Action	wlan.fc.type_subtype == 0x0d	Blue
802.11 Block Ack Request	wlan.fc.type_subtype == 0x18	Pink

A callout bubble points to the "802.11 Block-Ack" rule with the text "Adding new colors".

Tuning display for WLAN



WLAN Probe Request Channel 1 6 11.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

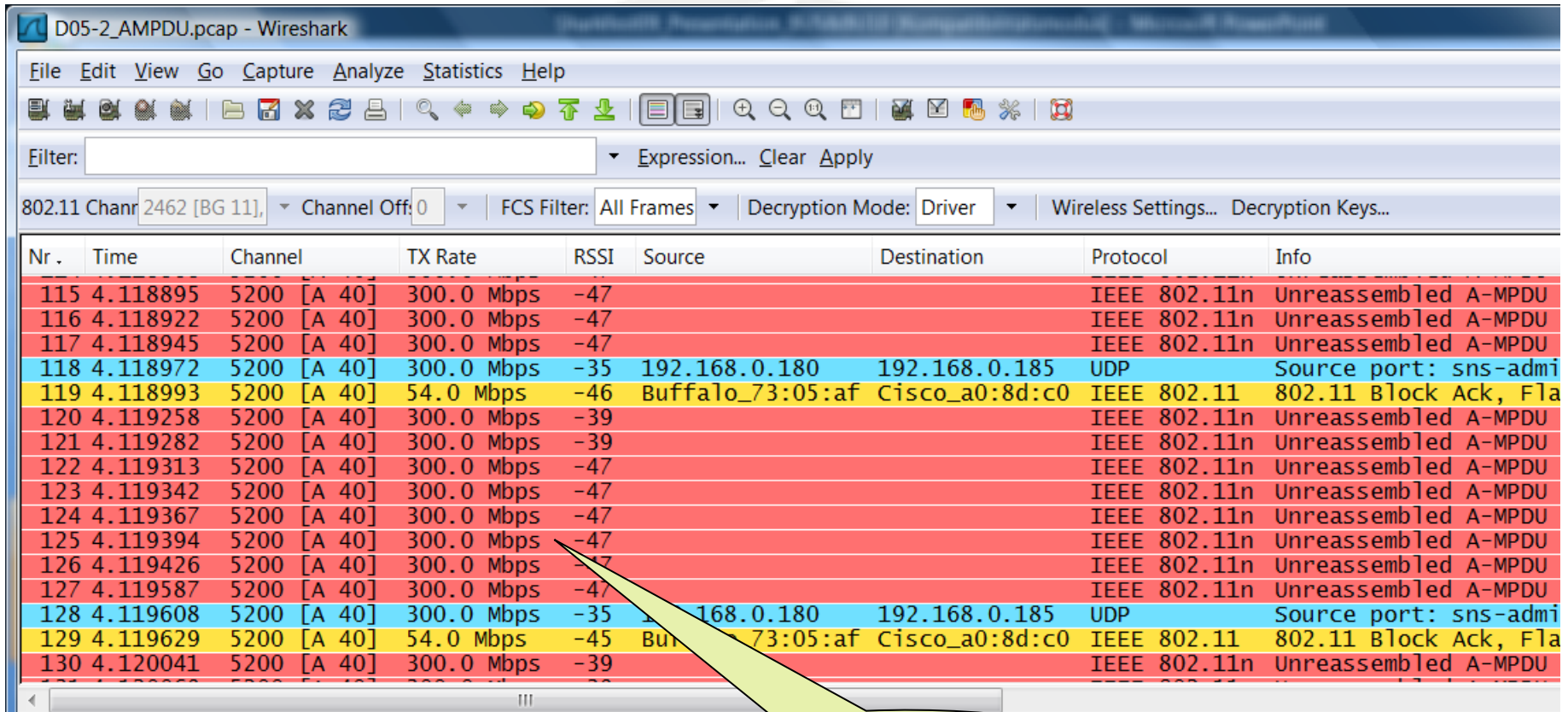
Filter: Expression... Clear Apply

802.11 Chanr Channel Off: FCS Filter: Decryption Mode: None Wireless Settings... Decryption Keys...

Nr.	Time	Channel	TX Rate	RSSI	Source	Destination	Protocol	Info
1	0.000000	2412 [BG 1]	1.0	55 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=54,
2	0.000621	2412 [BG 1]	1.0	55 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=55,
3	0.001369	2412 [BG 1]	1.0	55 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=56,
4	0.112247	2437 [BG 6]	1.0	56 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=57,
5	0.112826	2437 [BG 6]	1.0	56 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=58,
6	0.113600	2437 [BG 6]	1.0	57 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=59,
7	0.222337	2462 [BG 11]	1.0	61 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=60,
8	0.223086	2462 [BG 11]	1.0	61 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=61,
9	0.223588	2462 [BG 11]	1.0	62 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=62,
10	0.332445	2437 [BG 6]	1.0	56 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=63,
11	0.333089	2437 [BG 6]	1.0	57 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=64,
12	0.333846	2437 [BG 6]	1.0	56 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=65,
13	1.765825	2412 [BG 1]	1.0	56 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=68,
14	2.095041	2437 [BG 6]	1.0	55 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=75,
15	2.095667	2437 [BG 6]	1.0	56 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=76,
16	2.096384	2437 [BG 6]	1.0	56 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=77,
17	2.425468	2462 [BG 11]	1.0	60 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=84,
18	2.426217	2462 [BG 11]	1.0	59 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=85,
19	2.426966	2462 [BG 11]	1.0	60 dB	Philips_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=86,

Different color per channel

Tuning display for WLAN

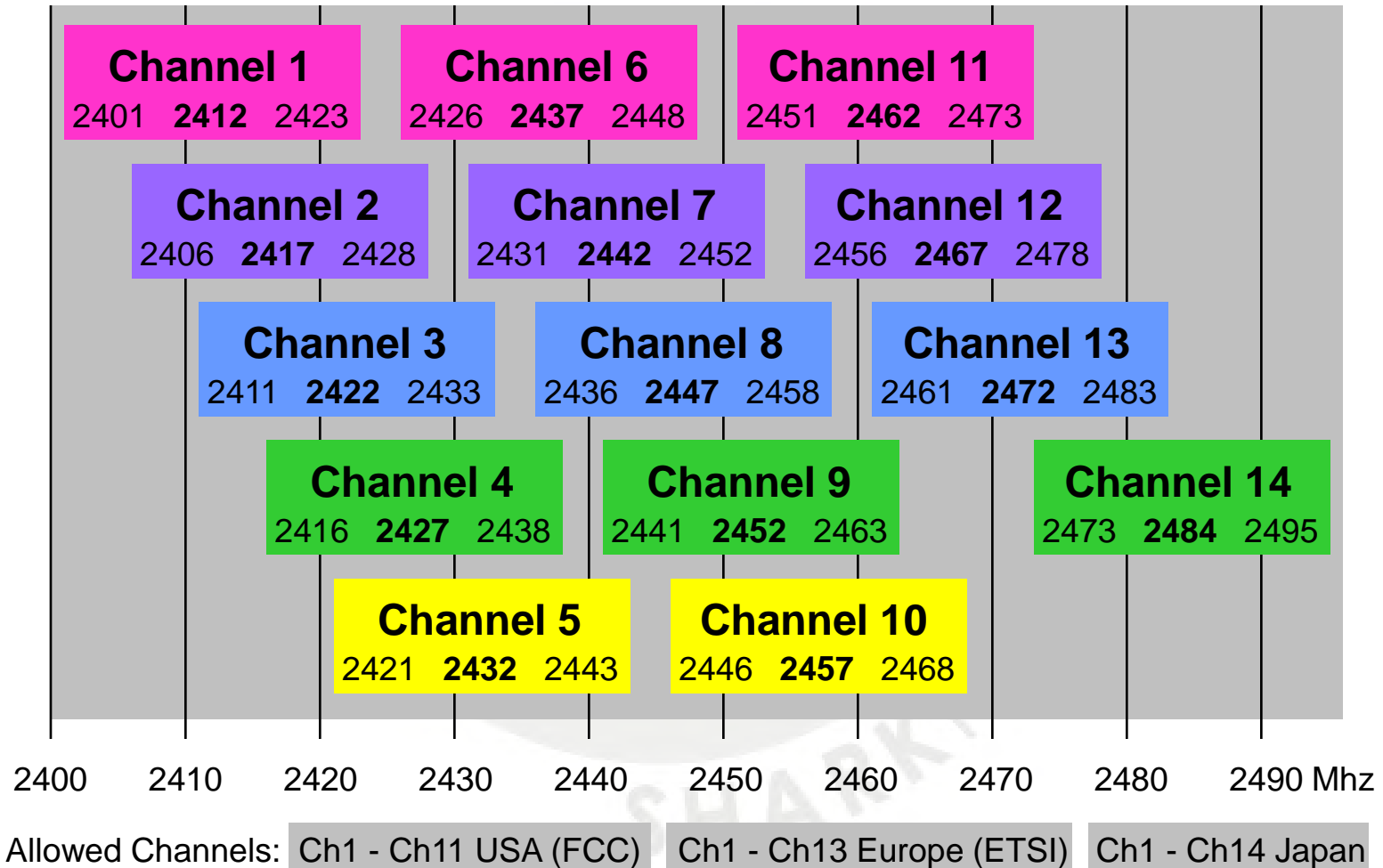


The image shows a Wireshark capture of WLAN traffic. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Help), a toolbar, a filter field, and a packet list table. The table columns are: Nr., Time, Channel, TX Rate, RSSI, Source, Destination, Protocol, and Info. The packets are color-coded based on their type: red for Unreassembled A-MPDU, yellow for 802.11 Block Ack, and cyan for UDP. A callout bubble points to the color coding.

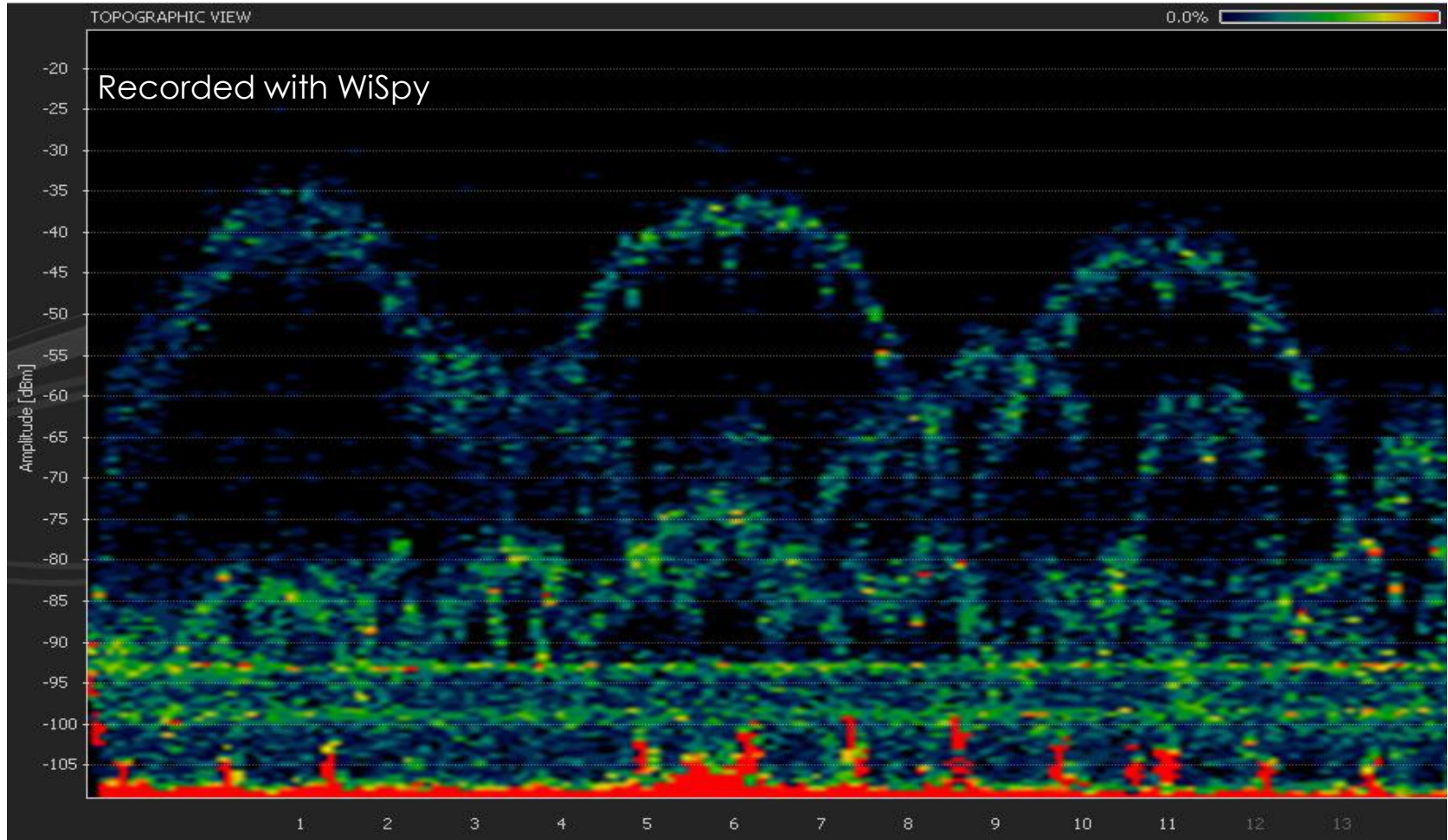
Nr.	Time	Channel	TX Rate	RSSI	Source	Destination	Protocol	Info
115	4.118895	5200 [A 40]	300.0 Mbps	-47			IEEE 802.11n	Unreassembled A-MPDU
116	4.118922	5200 [A 40]	300.0 Mbps	-47			IEEE 802.11n	Unreassembled A-MPDU
117	4.118945	5200 [A 40]	300.0 Mbps	-47			IEEE 802.11n	Unreassembled A-MPDU
118	4.118972	5200 [A 40]	300.0 Mbps	-35	192.168.0.180	192.168.0.185	UDP	Source port: sns-admi
119	4.118993	5200 [A 40]	54.0 Mbps	-46	Buffalo_73:05:af	Cisco_a0:8d:c0	IEEE 802.11	802.11 Block Ack, Fla
120	4.119258	5200 [A 40]	300.0 Mbps	-39			IEEE 802.11n	Unreassembled A-MPDU
121	4.119282	5200 [A 40]	300.0 Mbps	-39			IEEE 802.11n	Unreassembled A-MPDU
122	4.119313	5200 [A 40]	300.0 Mbps	-47			IEEE 802.11n	Unreassembled A-MPDU
123	4.119342	5200 [A 40]	300.0 Mbps	-47			IEEE 802.11n	Unreassembled A-MPDU
124	4.119367	5200 [A 40]	300.0 Mbps	-47			IEEE 802.11n	Unreassembled A-MPDU
125	4.119394	5200 [A 40]	300.0 Mbps	-47			IEEE 802.11n	Unreassembled A-MPDU
126	4.119426	5200 [A 40]	300.0 Mbps	-47			IEEE 802.11n	Unreassembled A-MPDU
127	4.119587	5200 [A 40]	300.0 Mbps	-47			IEEE 802.11n	Unreassembled A-MPDU
128	4.119608	5200 [A 40]	300.0 Mbps	-35	192.168.0.180	192.168.0.185	UDP	Source port: sns-admi
129	4.119629	5200 [A 40]	54.0 Mbps	-45	Buffalo_73:05:af	Cisco_a0:8d:c0	IEEE 802.11	802.11 Block Ack, Fla
130	4.120041	5200 [A 40]	300.0 Mbps	-39			IEEE 802.11n	Unreassembled A-MPDU

Different color per frame type

802.11b/g Channel Allocation



802.11b/g Channel Allocation



WLAN Management Frames

- Beacon
- Probe request and response
- Authentication
- Deauthentication
- Association request and response
- Reassociation request and response
- Disassociation

These frames are used to establish and maintain communications within a single radio cell (channel)

WLAN Control & Data Frames

Control Frames

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

These frames control the access to the shared media

Data Frames

- Data
- Null Function

These frames transport data or are use for keep alives

WLAN Management Frames

Beacon

- Marks the presence of an Access Point (AP)
- Sent 10 times / seconds (default)
- Carries BSSID, MAC address etc. of AP
- Indicates capabilities of AP (speeds etc.)
- Indicates type and need for encryption
- Keeps mobile clients time synchronized
- Carries optional vendor specific info
- and much more



WLAN Management Frames

Probe Request / Response

- Purpose is to find an Access Point
- Probe Request are always sent by client
- Probe Requests are sent in all channels
- Access Point replies with Probe Response
- Probe Response contains same info fields like Beacon



Remark: In 'Passive Mode' no Probe Request are sent by the client, channels are scanned for Beacons (saves power)

WLAN Management Frames

Authentication

- Initially two methods defined:
 - ‘Open Authentication’
 - ‘Shared Key Authentication’
- Obsolete methods (unsecure)
- 802.1x Authentication is mostly used today

Deauthentication

- Sent if a station or the Access Point wishes to terminate secure communications



WLAN Management Frames

Association Request

- A station is applying to be registered with an Access point
- A single station can only be associated with one Access Point

Association Response

- Reply from AP to confirm association

Dissassociation

- Sent to release an association



WLAN Management Frames

Reassociation Request

- Sent by a roaming station to the new Access Point
- Station lists the present Access Point in the Request as a reference

Reassociation Response

- Reply from the Access Point to confirm new association



WLAN Control Frames

Request to Send (RTS)

- Sent by a station or Access Point to reserve a time slot for transmission
- Used after a number of not acknowledged transmissions
- Used in mixed b/g/n cells and hidden node situations to prevent collisions



Clear to Send (CTS)

- Reply to confirm the requested time slot

WLAN Control Frames

Acknowledge

- Sent by a station or Access Point to confirm successful reception of a packet

Power Save Poll

- Sent by a station in sleep mode to fetch packets stored in Access Point



WLAN Data Frames

Data

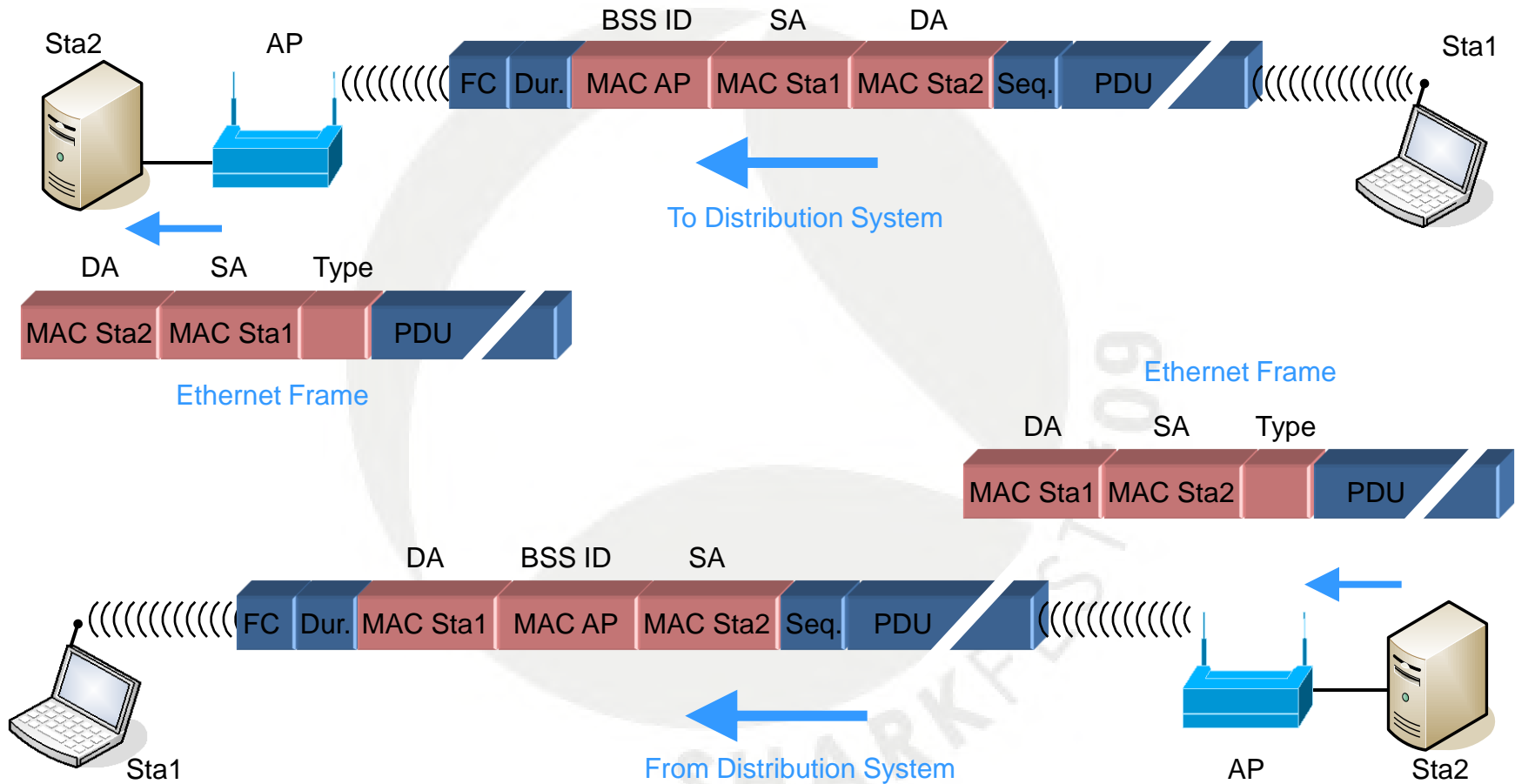
- Data frames may be encrypted or in clear text
- Data frames may contain 802.11 QOS control for Voice over WLAN

Null Function

- Data frame containing no data
- Used for keep-alives or signaling power save condition



WLAN Frame Formats



WLAN Frame Formats



Acknowledge, Clear to Send



Request to Send



Data Frame, Beacon, Probe Request, Probe Response, Authentication, Deauthentication, Association, Reassociation, Disassociation



Data Frame through repeater

FC = Frame Control, Dur. = Duration, RA = Receiver Address, TA = Transmitter Address;
DA = Destination Address, SA = Source Address, Seq. = Sequence, PDU = Protocol
Data Unit, FC = Frame Check Sequence

+

Client can not associate - Case one

WLAN No Connection_01.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

802.11 Chanr 2462 [BG 11] Channel Off: 0 FCS Filter: All Frames Decryption Mode: Wiresha Wireless Settings... Decryption Keys...

Nr.	Time	Channel	TX Rate	RSSI	Source	Destination	Protocol	Info
17	1.071215	2462 [BG 11]	6.0	57 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3016, FN=0, Flags=.....C,
18	1.775731	2462 [BG 11]	6.0	55 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3017, FN=0, Flags=.....C,
19	1.880076	2462 [BG 11]	6.0	57 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3018, FN=0, Flags=.....C,
20	1.984623	2462 [BG 11]	6.0	54 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3019, FN=0, Flags=.....C,
21	2.088968	2462 [BG 11]	6.0	56 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3020, FN=0, Flags=.....C,
22	2.193469	2462 [BG 11]	6.0	56 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3021, FN=0, Flags=.....C,
23	2.297962	2462 [BG 11]	6.0	57 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3022, FN=0, Flags=.....C,
24	2.402384	2462 [BG 11]	6.0	56 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3023, FN=0, Flags=.....C,
25	2.442603	2462 [BG 11]	1.0	67 dB	IntelCor_73:68:54	Broadcast	IEEE 802.11	Probe Request, SN=432, FN=0, Flags=.....C,
26	2.442956	2462 [BG 11]	6.0	56 dB	Cisco_a7:fe:60	IntelCor_73:68:54	IEEE 802.11	Probe Response, SN=1218, FN=0, Flags=....R...C
27	2.442957	2462 [BG 11]	6.0	65 dB	Cisco_a7:fe:60	Cisco_a7:fe:60 (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
28	2.443959	2462 [BG 11]	1.0	67 dB	IntelCor_73:68:54	Broadcast	IEEE 802.11	Probe Request, SN=433, FN=0, Flags=.....C,
29	2.444707	2462 [BG 11]	6.0	57 dB	Cisco_a7:fe:60	IntelCor_73:68:54	IEEE 802.11	Probe Response, SN=1219, FN=0, Flags=....R...C
30	2.444709	2462 [BG 11]	6.0	65 dB	Cisco_a7:fe:60	Cisco_a7:fe:60 (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
31	2.445579	2462 [BG 11]	1.0	67 dB	IntelCor_73:68:54	Broadcast	IEEE 802.11	Probe Request, SN=434, FN=0, Flags=.....C,
32	2.445954	2462 [BG 11]	6.0	56 dB	Cisco_a7:fe:60	IntelCor_73:68:54	IEEE 802.11	Probe Response, SN=1220, FN=0, Flags=....R...C
33	2.445956	2462 [BG 11]	6.0	65 dB	Cisco_a7:fe:60	Cisco_a7:fe:60 (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
34	2.447333	2462 [BG 11]	1.0	66 dB	IntelCor_73:68:54	Broadcast	IEEE 802.11	Probe Request, SN=435, FN=0, Flags=.....C,
35	2.447829	2462 [BG 11]	6.0	56 dB	Cisco_a7:fe:60	IntelCor_73:68:54	IEEE 802.11	Probe Response, SN=1221, FN=0, Flags=....R...C
36	2.447831	2462 [BG 11]	6.0	65 dB	Cisco_a7:fe:60	Cisco_a7:fe:60 (RA)	IEEE 802.11	Acknowledgement, Flags=.....C
37	2.506863	2462 [BG 11]	6.0	57 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3024, FN=0, Flags=.....C,
38	2.611338	2462 [BG 11]	6.0	56 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3025, FN=0, Flags=.....C,
39	2.715724	2462 [BG 11]	6.0	57 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3026, FN=0, Flags=.....C,
40	2.820227	2462 [BG 11]	6.0	56 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3027, FN=0, Flags=.....C,
41	2.924599	2462 [BG 11]	6.0	55 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3028, FN=0, Flags=.....C,
42	3.029104	2462 [BG 11]	6.0	56 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3029, FN=0, Flags=.....C,
43	3.133622	2462 [BG 11]	6.0	54 dB	Cisco_a7:fe:60	Broadcast	IEEE 802.11	Beacon frame, SN=3030, FN=0, Flags=.....C,
44	3.237975	2462 [BG 11]	6.0	57 dB	Cisco_a7:fe:60	Broadcast	TFFF 802.11	Beacon frame, SN=3031, FN=0, Flags=.....C,

Client can not associate - Case one

The image shows a Wireshark capture of WLAN traffic. The main display area shows a list of frames. Frame 26 is highlighted, showing an IEEE 802.11 Probe Response from Cisco_a7:fe:60 to IntelCor_73:68:54. The details pane below shows the structure of this frame, including a Vendor Specific tag (Tag 221) for WPA. The WPA tag details are:

- Tag Number: 221 (Vendor Specific)
- Tag length: 24
- Vendor: Microsoft
- Tag interpretation: WPA IE, type 1, version 1
- Tag interpretation: Multicast cipher suite: TKIP
- Tag interpretation: # of unicast cipher suites: 1
- Tag interpretation: Unicast cipher suite 1: TKIP
- Tag interpretation: # of auth key management suites: 1
- Tag interpretation: auth key management suite 1: PSK
- Tag interpretation: Not interpreted

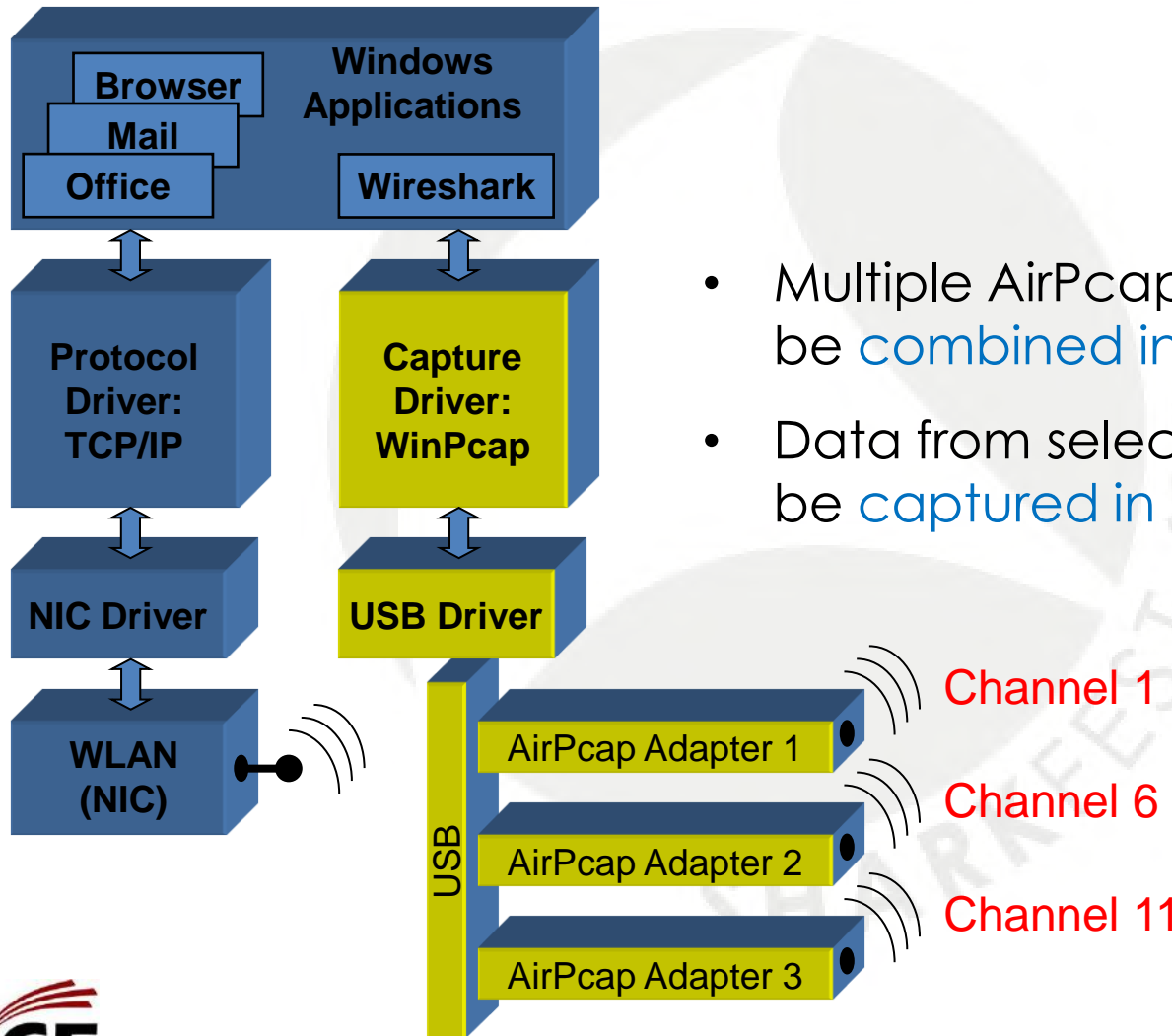
Other frames in the capture include Beacon frames and other Probe Requests and Responses.

Client can not associate - Case two

The image shows a Wireshark capture of a WLAN connection attempt. The capture is titled "WLAN No Connection_02.pcap - Wireshark". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Help) and a toolbar with various icons. A filter bar is set to "Expression... Clear Apply". The main display area shows a list of network packets with columns for Nr., Time, Channel, TX Rate, RSSI, Source, Destination, Protocol, and Info. The packets are listed in a table format, with the 62nd packet highlighted in blue. The 62nd packet is a Deauthentication frame from Cisco_11:1f:60 to Philips_45:7f:2f, with SN=4085 and FN=0. The 63rd packet is an Acknowledgement frame from Philips_45:7f:2f to Cisco_11:1f:60. The 64th packet is a Beacon frame from Cisco_11:1f:60 to Broadcast, with SN=4086 and FN=0.

Nr.	Time	Channel	TX Rate	RSSI	Source	Destination	Protocol	Info
36	2.457484	2412 [BG 1]	1.0	51 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4074, FN=0, Flags=.....
37	2.559947	2412 [BG 1]	1.0	49 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4075, FN=0, Flags=.....
38	2.662303	2412 [BG 1]	1.0	50 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4076, FN=0, Flags=.....
39	2.764635	2412 [BG 1]	1.0	52 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4077, FN=0, Flags=.....
40	2.765481	2412 [BG 1]	1.0	56 dB	Philips_45:7f:2f	Cisco_11:1f:60	IEEE 802.11	Authentication, SN=22, FN=0, Flags=.....
41	2.765729	2412 [BG 1]	1.0	52 dB	Philips_45:7f:2f	Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags=.....
42	2.766162	2412 [BG 1]	1.0	51 dB	Cisco_11:1f:60	Philips_45:7f:2f	IEEE 802.11	Authentication, SN=4078, FN=0, Flags=.....
43	2.766480	2412 [BG 1]	1.0	76 dB	Cisco_11:1f:60	Cisco_11:1f:60 (RA)	IEEE 802.11	Acknowledgement, Flags=.....
44	2.767855	2412 [BG 1]	1.0	55 dB	Philips_45:7f:2f	Cisco_11:1f:60	IEEE 802.11	Association Request, SN=23, FN=0, Flags=.....
45	2.768045	2412 [BG 1]	1.0	50 dB	Philips_45:7f:2f	Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags=.....
46	2.768518	2412 [BG 1]	54.0	44 dB	Cisco_11:1f:60	Philips_45:7f:2f	IEEE 802.11	Association Response, SN=4079, FN=0, Flags=..
47	2.768598	2412 [BG 1]	24.0	74 dB	Cisco_11:1f:60	Cisco_11:1f:60 (RA)	IEEE 802.11	Acknowledgement, Flags=.....
48	2.769079	2412 [BG 1]	54.0	44 dB	Cisco_11:1f:60	Philips_45:7f:2f	EAPOL	Key
49	2.769131	2412 [BG 1]	24.0	75 dB	Cisco_11:1f:60	Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags=.....
50	2.772431	2412 [BG 1]	54.0	51 dB	Philips_45:7f:2f	Cisco_11:1f:60	EAPOL	Key
51	2.772529	2412 [BG 1]	24.0	45 dB	Philips_45:7f:2f	Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags=.....
52	2.776426	2412 [BG 1]	54.0	50 dB	Philips_45:7f:2f	Cisco_11:1f:60	EAPOL	Start
53	2.776521	2412 [BG 1]	24.0	46 dB	Philips_45:7f:2f	Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags=.....
54	2.867071	2412 [BG 1]	1.0	52 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4081, FN=0, Flags=.....
55	2.868717	2412 [BG 1]	54.0	45 dB	Cisco_11:1f:60	Philips_45:7f:2f	EAPOL	Key
56	2.870177	2412 [BG 1]	54.0	50 dB	Philips_45:7f:2f	Cisco_11:1f:60	EAPOL	Key
57	2.870255	2412 [BG 1]	24.0	45 dB	Philips_45:7f:2f	Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags=.....
58	2.969425	2412 [BG 1]	1.0	49 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4083, FN=0, Flags=.....
59	2.969572	2412 [BG 1]	54.0	44 dB	Cisco_11:1f:60	Philips_45:7f:2f	EAPOL	Key
60	3.005391	2412 [BG 1]	54.0	51 dB	Philips_45:7f:2f	Cisco_11:1f:60	EAPOL	Key
61	3.005511	2412 [BG 1]	24.0	45 dB	Philips_45:7f:2f	Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags=.....
62	3.068956	2412 [BG 1]	1.0	49 dB	Cisco_11:1f:60	Philips_45:7f:2f	IEEE 802.11	Deauthentication, SN=4085, FN=0, Flags=.....
63	3.071272	2412 [BG 1]	1.0	76 dB	Cisco_11:1f:60	Cisco_11:1f:60 (RA)	IEEE 802.11	Acknowledgement, Flags=.....
64	3.071816	2412 [BG 1]	1.0	49 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4086, FN=0, Flags=.....

Analyzing Roaming Problems



- Multiple AirPcap adapters can be combined in one logical I/F
- Data from selected channels will be captured in one trace file

Analyzing Roaming Problems

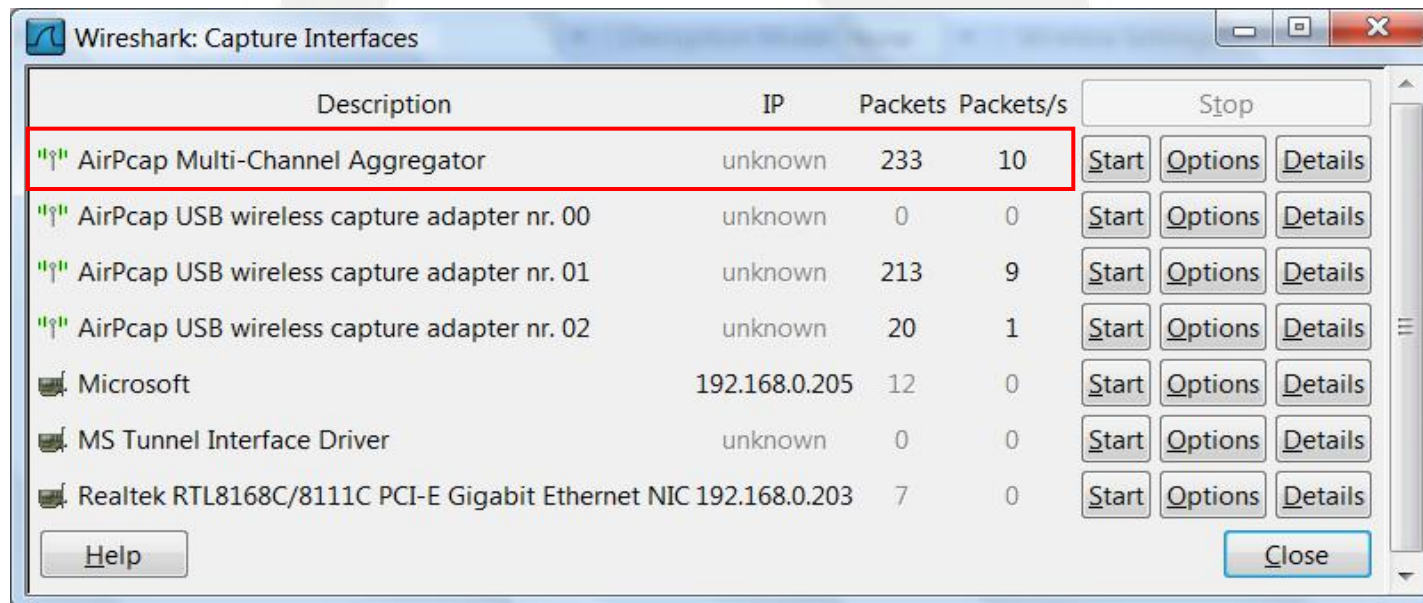
- Mounting USB hub and AirPcap adapters on a notebook gives you a **mobile solution** to capture **roaming processes**



- Roaming problems are quite **complex to analyze**
- In order to capture the roaming event, you have to **follow the roaming client** as close as possible
- Set a **display filter** to BEACONs and MAC address of roaming client

Combining multiple Airpcap adapters

- More than one AirPcap adapter will be automatically combined in the [AirPcap Multi-Channel Aggregator](#)
- Channel numbers must be configured individually on each adapter



Roaming Client

WLAN Roaming_01.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Nr.	Time	Channel	TX Rate	RSSI	Source	Destination	Protocol	Info
183	6.936186	2412 [BG 1]	11.0	74 dB	192.168.0.203	192.168.0.1	ICMP	Echo (ping) request
184	6.936279	2412 [BG 1]	2.0	25 dB		Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags
185	6.937318	2412 [BG 1]	11.0	25 dB	192.168.0.1	192.168.0.203	ICMP	Echo (ping) reply
186	6.937418	2412 [BG 1]	2.0	74 dB		Cisco_11:1f:60 (RA)	IEEE 802.11	Acknowledgement, Flags
187	6.962979	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=746,
188	7.019684	2412 [BG 1]	1.0	23 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=2028,
189	7.065378	2462 [BG 11]	1.0	71 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=747,
190	7.066325	2462 [BG 11]	1.0	66 dB	Philips_45:7f:2f	Cisco_92:ad:21	IEEE 802.11	Authentication, SN=284,
191	7.066485	2462 [BG 11]	1.0	72 dB		Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags
192	7.067208	2462 [BG 11]	2.0	73 dB	Cisco_92:ad:21	Philips_45:7f:2f	IEEE 802.11	Authentication, SN=749,
193	7.067552	2462 [BG 11]	2.0	76 dB		Cisco_92:ad:21 (RA)	IEEE 802.11	Acknowledgement, Flags
194	7.068675	2462 [BG 11]	1.0	69 dB	Philips_45:7f:2f	Cisco_92:ad:21	IEEE 802.11	Reassociation Request
195	7.068984	2462 [BG 11]	1.0	71 dB		Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags
196	7.070590	2462 [BG 11]	11.0	71 dB	Cisco_92:ad:21	Philips_45:7f:2f	IEEE 802.11	Reassociation Response
197	7.070656	2462 [BG 11]	2.0	77 dB		Cisco_92:ad:21 (RA)	IEEE 802.11	Acknowledgement, Flags
198	7.122311	2412 [BG 1]	1.0	24 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=2029,
199	7.167782	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=748,
200	7.167882	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=749,
201	7.167982	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=750,
202	7.168082	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=751,
203	7.168182	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=752,
204	7.168282	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=753,
205	7.168382	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=754,
206	7.168482	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=755,
207	7.168582	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=756,
208	7.168682	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=757,
209	7.168782	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=758,
210	7.168882	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=759,
211	7.168982	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=760,
212	7.169082	2462 [BG 11]	1.0	72 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=761,
213	7.884651	2462 [BG 11]	1.0	73 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=757,
214	7.937562	2462 [BG 11]	11.0	70 dB	192.168.0.203	192.168.0.1	ICMP	Echo (ping) request
215	7.937685	2462 [BG 11]	2.0	71 dB		Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags
216	7.939356	2462 [BG 11]	11.0	72 dB	192.168.0.1	192.168.0.203	ICMP	Echo (ping) reply
217	7.939454	2462 [BG 11]	2.0	74 dB		Cisco_92:ad:21 (RA)	IEEE 802.11	Acknowledgement, Flags
218	7.941290	2412 [BG 1]	1.0	25 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=2037,
219	7.986943	2462 [BG 11]	1.0	70 dB	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=758,

Throughput Analysis

- Throughput will always be an issue in WLANs
- A radio cell is a **shared media** with **half duplex** conversation
- Indicated throughput (i.e. 54Mbps) are **maximum** values and are only achieved under **optimal conditions**
- Data throughput is around **50%** of cell throughput
- Presence of old 802.11b-only client will **reduce** cell throughput significantly



Overview WLAN Standards



Mbps	Coding	Modulation	Description	
1 2	Barker Barker	DBPSK	802.11 DSSS (Clause 15) with ,Long Preamble'	
5.5 11	CCK CCK	DQPSK	802.11b HR/DSSS (Clause 18) with ,Short Preamble'	
6, 9 12, 18 24, 36 48, 54	OFDM OFDM OFDM OFDM	BPSK QPSK 16-QAM 64-QAM	802.11g Extended Rate PHY (ERP)	802.11a
7.2-72.2 14.4-144.4	OFDM OFDM	MCS 0-7 MCS 8-15	1 Stream 2 Streams	802.11n High Throughput (HT) Extensions
2.4 GHz				5 GHz

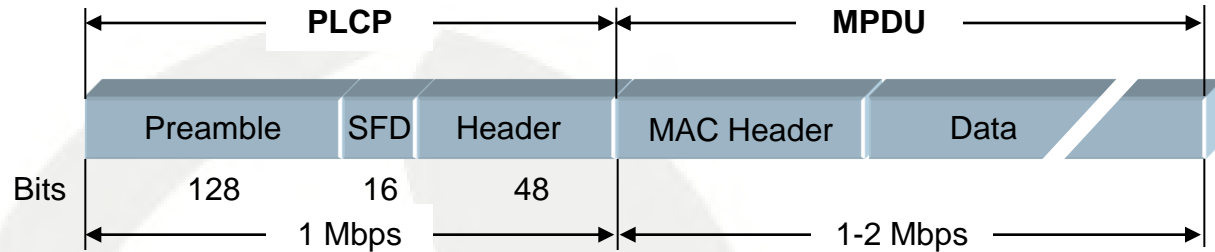
CCK = Complementary Code Keying
 DBPSK = Differential Binary Phase-Shift Keying
 DQPSK = Differential Quadrature Phase-Shift Keying
 OFDM = Orthogonal Frequency Division Multiplexing

BPSK = Binary Phase-Shift Keying
 QPSK = Quadrature Phase-Shift Keying
 QAM = Quadrature Amplitude Modul.
 MCS = Modulation Coding Scheme

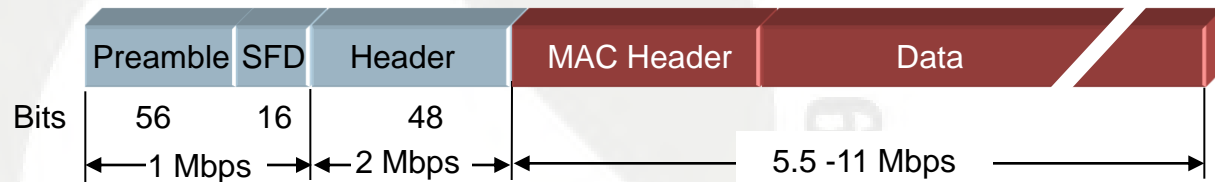
Overview Frame Types (2.4 GHz)



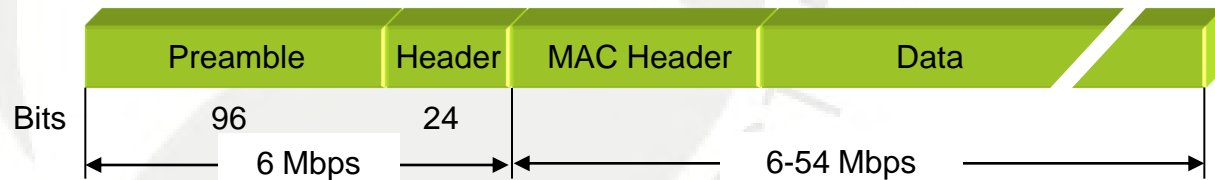
802.11 DSSS with
,Long Preamble'
Barker Code



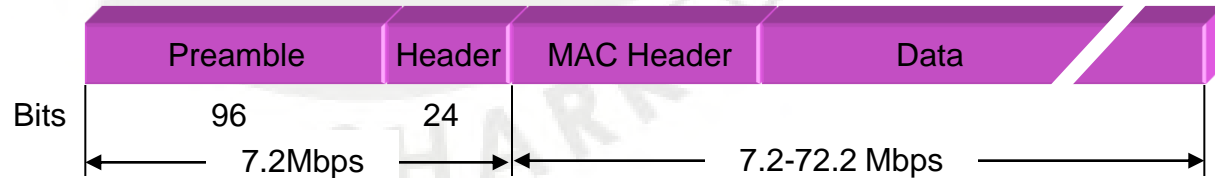
802.11b HR/DSSS with
,Short Preamble'
Barker / CCK



802.11g (ERP)
Extended Rate PHY
OFDM

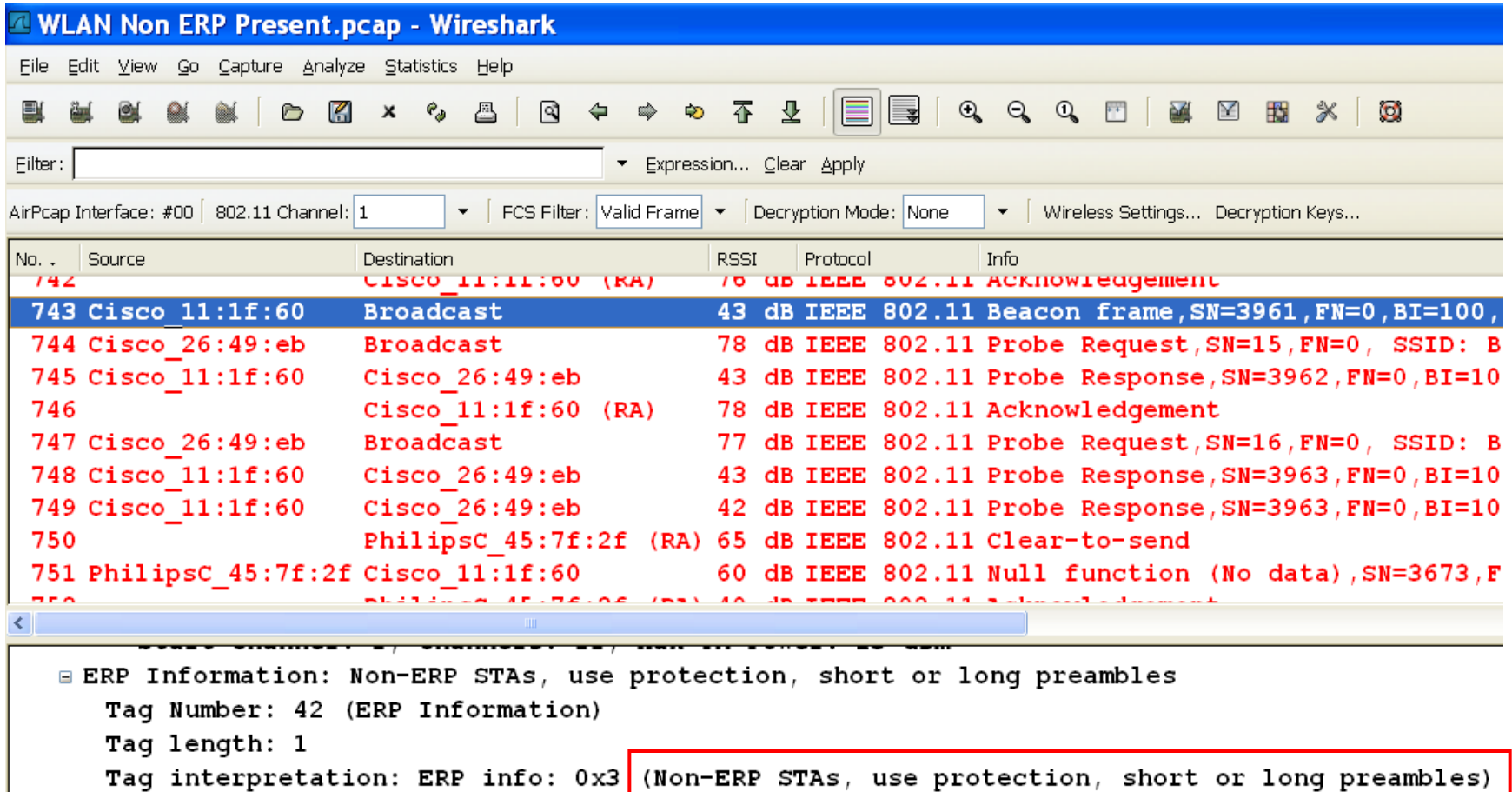


802.11n (HT)
High Throughput
extended OFDM



PLCP = Physical Layer Convergence Protocol
MPDU = MAC Layer Protocol Data Unit

Throughput Analysis



WLAN Non ERP Present.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

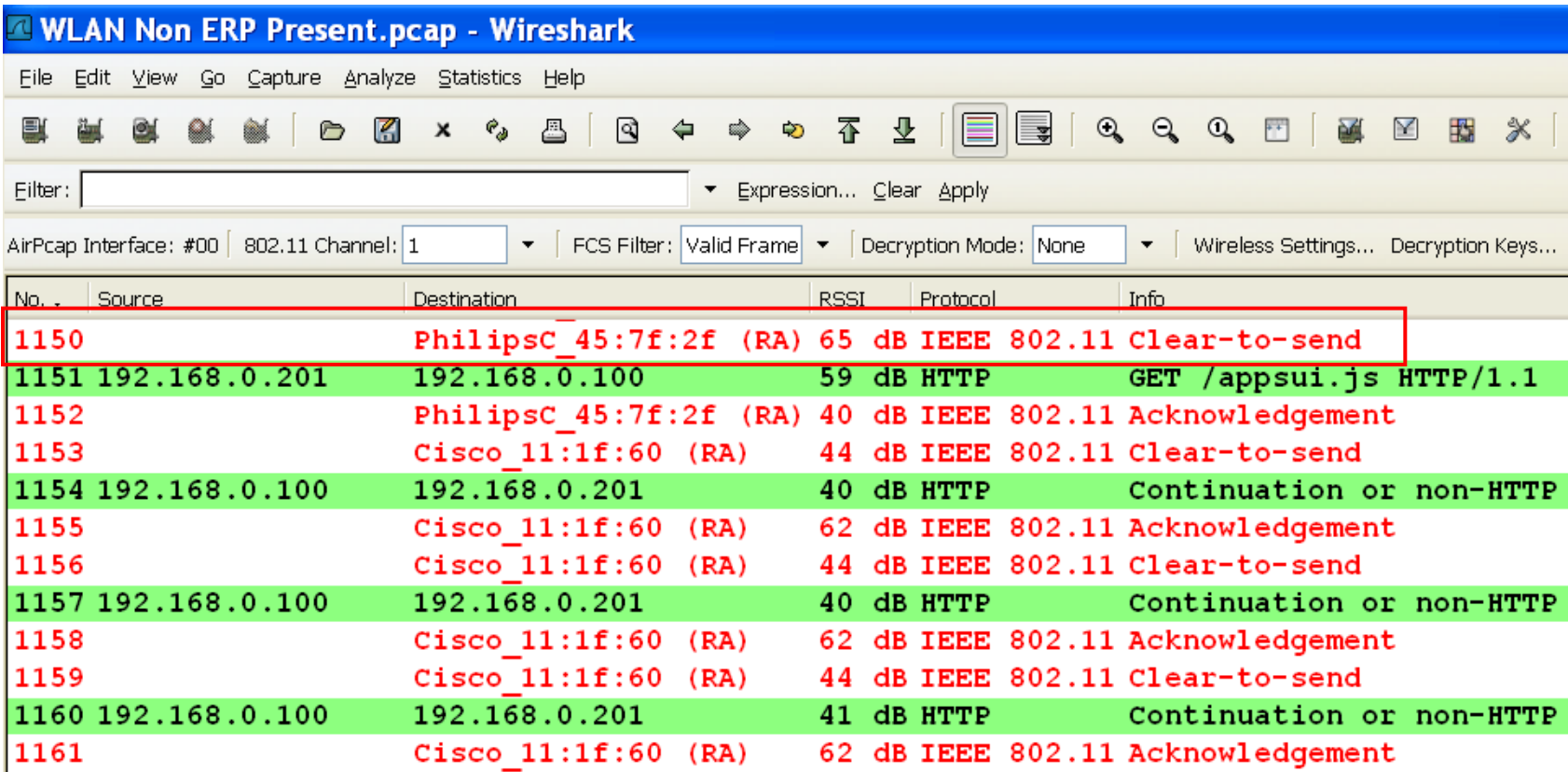
Filter: Expression... Clear Apply

AirPcap Interface: #00 802.11 Channel: 1 FCS Filter: Valid Frame Decryption Mode: None Wireless Settings... Decryption Keys...

No.	Source	Destination	RSSI	Protocol	Info
742		CISCO_11:11:60 (RA)	76 dB	IEEE 802.11	Acknowledgement
743	Cisco_11:1f:60	Broadcast	43 dB	IEEE 802.11	Beacon frame, SN=3961, FN=0, BI=100,
744	Cisco_26:49:eb	Broadcast	78 dB	IEEE 802.11	Probe Request, SN=15, FN=0, SSID: B
745	Cisco_11:1f:60	Cisco_26:49:eb	43 dB	IEEE 802.11	Probe Response, SN=3962, FN=0, BI=10
746		Cisco_11:1f:60 (RA)	78 dB	IEEE 802.11	Acknowledgement
747	Cisco_26:49:eb	Broadcast	77 dB	IEEE 802.11	Probe Request, SN=16, FN=0, SSID: B
748	Cisco_11:1f:60	Cisco_26:49:eb	43 dB	IEEE 802.11	Probe Response, SN=3963, FN=0, BI=10
749	Cisco_11:1f:60	Cisco_26:49:eb	42 dB	IEEE 802.11	Probe Response, SN=3963, FN=0, BI=10
750		PhilipsC_45:7f:2f (RA)	65 dB	IEEE 802.11	Clear-to-send
751	PhilipsC_45:7f:2f	Cisco_11:1f:60	60 dB	IEEE 802.11	Null function (No data), SN=3673, F
752		PhilipsC_45:7f:2f (RA)	40 dB	IEEE 802.11	Acknowledgement

ERP Information: Non-ERP STAs, use protection, short or long preambles
Tag Number: 42 (ERP Information)
Tag length: 1
Tag interpretation: ERP info: 0x3 (Non-ERP STAs, use protection, short or long preambles)

Throughput Analysis



The image shows a Wireshark capture of WLAN traffic. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Help), a toolbar with various icons, and a filter field. The capture settings show 'AirPcap Interface: #00', '802.11 Channel: 1', 'FCS Filter: Valid Frame', and 'Decryption Mode: None'. The packet list table below shows a sequence of frames:

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
1159		Cisco_11:1f:60 (RA)	44 dB	IEEE 802.11	Clear-to-send
1160	192.168.0.100	192.168.0.201	41 dB	HTTP	Continuation or non-HTTP
1161		Cisco_11:1f:60 (RA)	62 dB	IEEE 802.11	Acknowledgement

OFDM (ERP) stations are sending control frames ,**Clear-to send to self**' (CTS-to-self) before each data frame to reserve time slot

Throughput Analysis

- Reduced data throughput in mixed environment

	Data Rate (Mbps)	Approximate Throughput (Mbps)	Throughput as a Percentage of 802.11b Throughput
802.11b	11	6	100%
802.11g—with 802.11b clients in cell (CTS/RTS)	54	8	133%
802.11g—with 802.11b clients in cell (CTS-to-self)	54	13	217%
802.11g (no 802.11b clients in cell)	54	22	367%
802.11a	54	25	417%

Source: Cisco Systems

Throughput improvement:
Upgrade of all 802.11b stations to 802.11g

Channel Allocation 5 GHz Band

Frequency Band	Channel ID	FCC (GHz)	ETSI (GHz)	MKK (GHz)
Lower Band UNII-1	34	--	--	5.170
	36	5.180	5.180	--
	38	--	--	5.190
	40	5.200	5.200	--
	42	--	--	5.210
	44	5.220	5.220	--
	46	--	--	5.230
	48	5.240	5.240	--
Middle Band UNII-2	52	5.260*	5.260	5.260
	56	5.280*	5.280	5.280
	60	5.300*	5.300	5.300
	64	5.320*	5.320	5.320
High Band UNII-2 extended	100	5.500*	5.500	5.500
	104	5.520*	5.520	5.520
	108	5.540*	5.540	5.540
	112	5.560*	5.560	5.560
	116	5.580*	5.580	5.580
	120	5.600*	5.600	5.600
	124	5.620*	5.620	5.620
	128	5.640*	5.640	5.640
	132	5.660*	5.660	5.660
	136	5.680*	5.680	5.680
	140	5.700*	5.700	5.700
Upper Band UNII-3/ISM	149	5.745	--	--
	153	5.765	--	--
	157	5.785	--	--
	161	5.805	--	--
ISM	165	5.825	--	--

Available non-overlapping channels	
FCC (USA and Canada)	24
ETSI (Europe)	19
MKK (Japan)	19

Transmit Power Control (TPC) required for	
FCC (USA and Canada)	Band 2,2e
ETSI (Europe)	Band 1,2,2e
MKK (Japan)	Band 1,2,2e

Dynamic Frequency Selection (DFS) required for	
FCC* (USA and Canada)	Band 2,2e
ETSI (Europe)	Band 1,2,2e
MKK (Japan)	Band 1,2,2e

Some channels only allowed for inhouse use

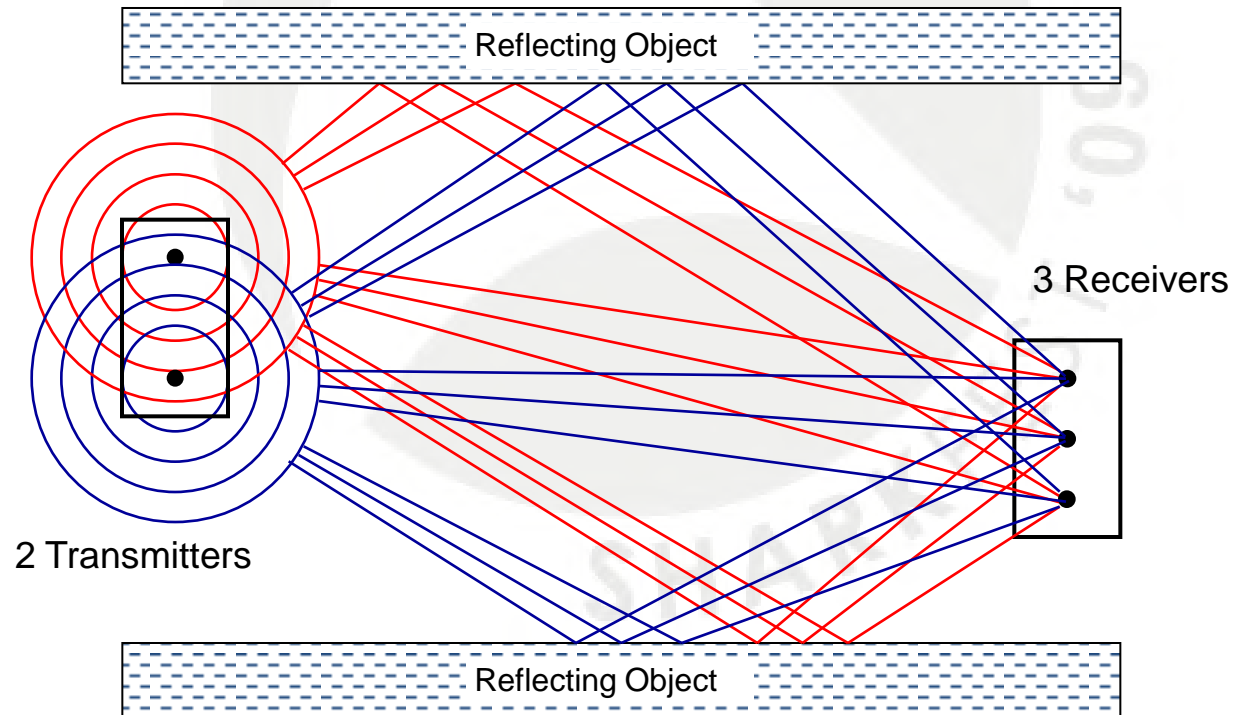
*New stricter FCC DFS2 rules valid off July 20, 2007

Multiple-Input, Multiple-Output (MIMO)

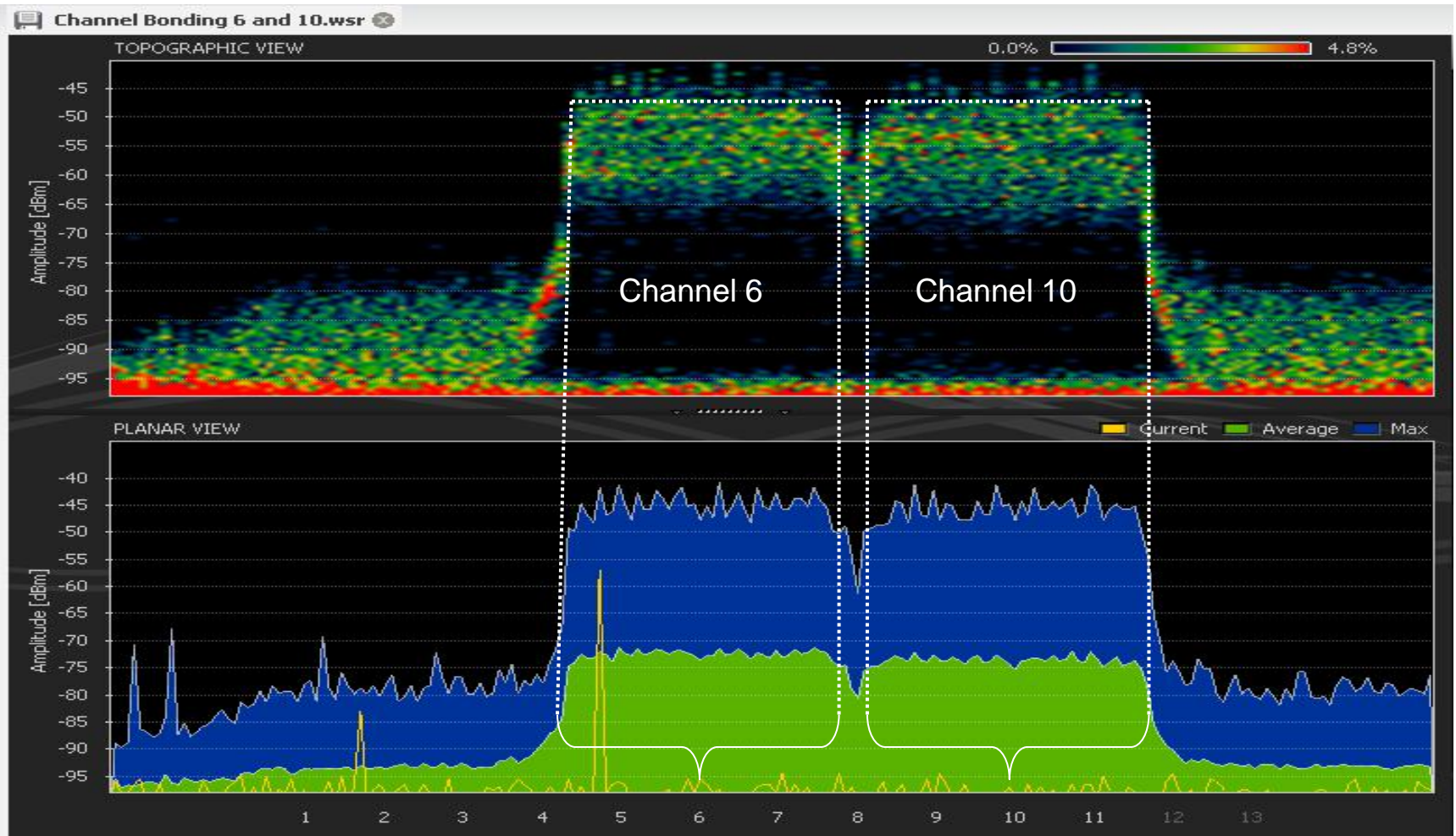
-  802.11n introduces lots of new WLAN technologies
-  Physical layer improvements with new OFDM
-  MIMO supports multiple streams within one channel
-  Channel bonding combines two adjacent channels
-  Frame aggregation allows large frames or streaming packets
-  Block acknowledges replaces ping pong procedure
-  With two streams and two channels up to 300 Mbps
-  Future product will support four streams and up to 600 Mbps

Multiple Streams (Spatial Multiplexing)

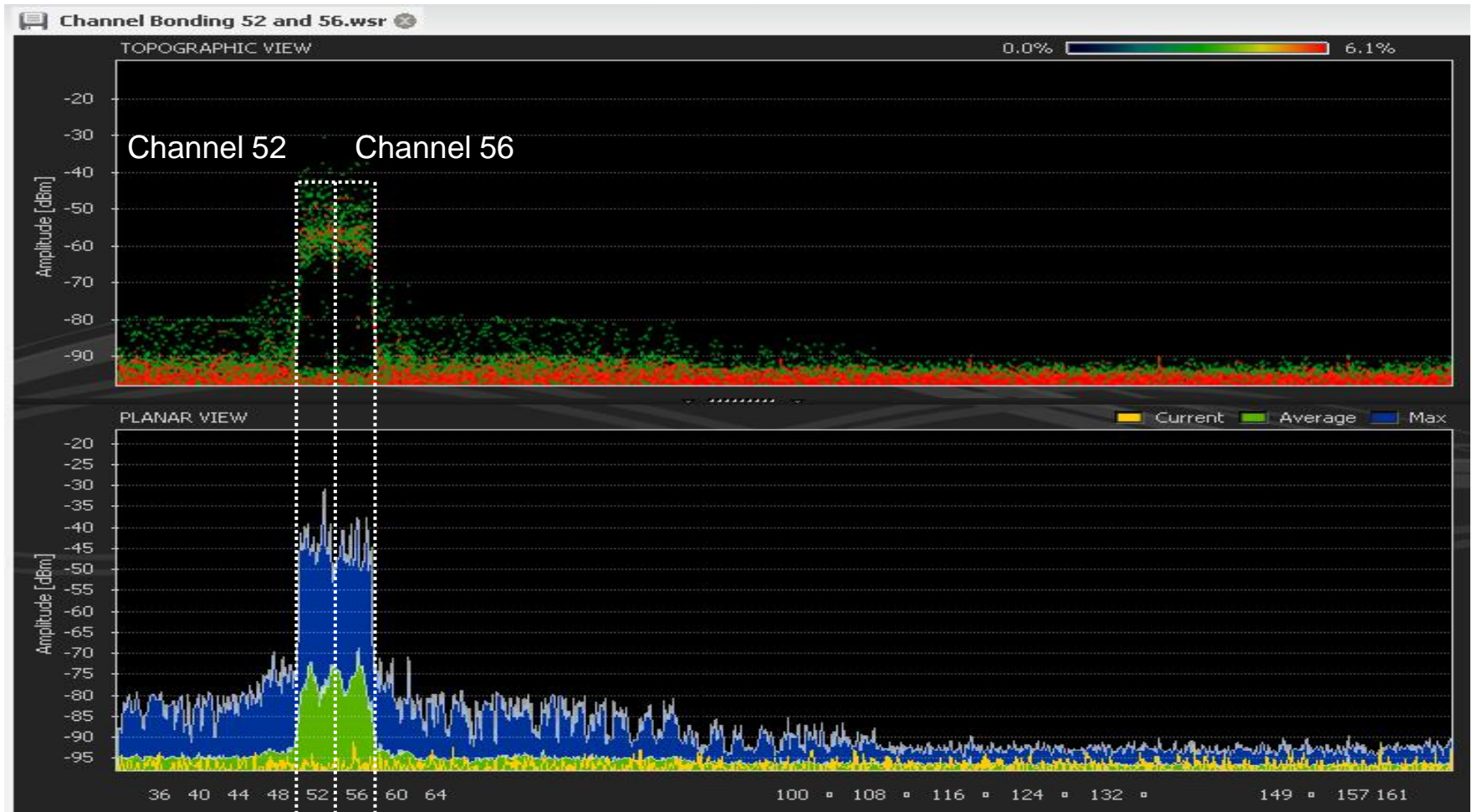
- A signal stream is broken down into **multiple signal streams**, each is transmitted from a different antenna.
- Each of these “spatial” streams arrives at the receiver with different amplitude (signal strength) and phase.



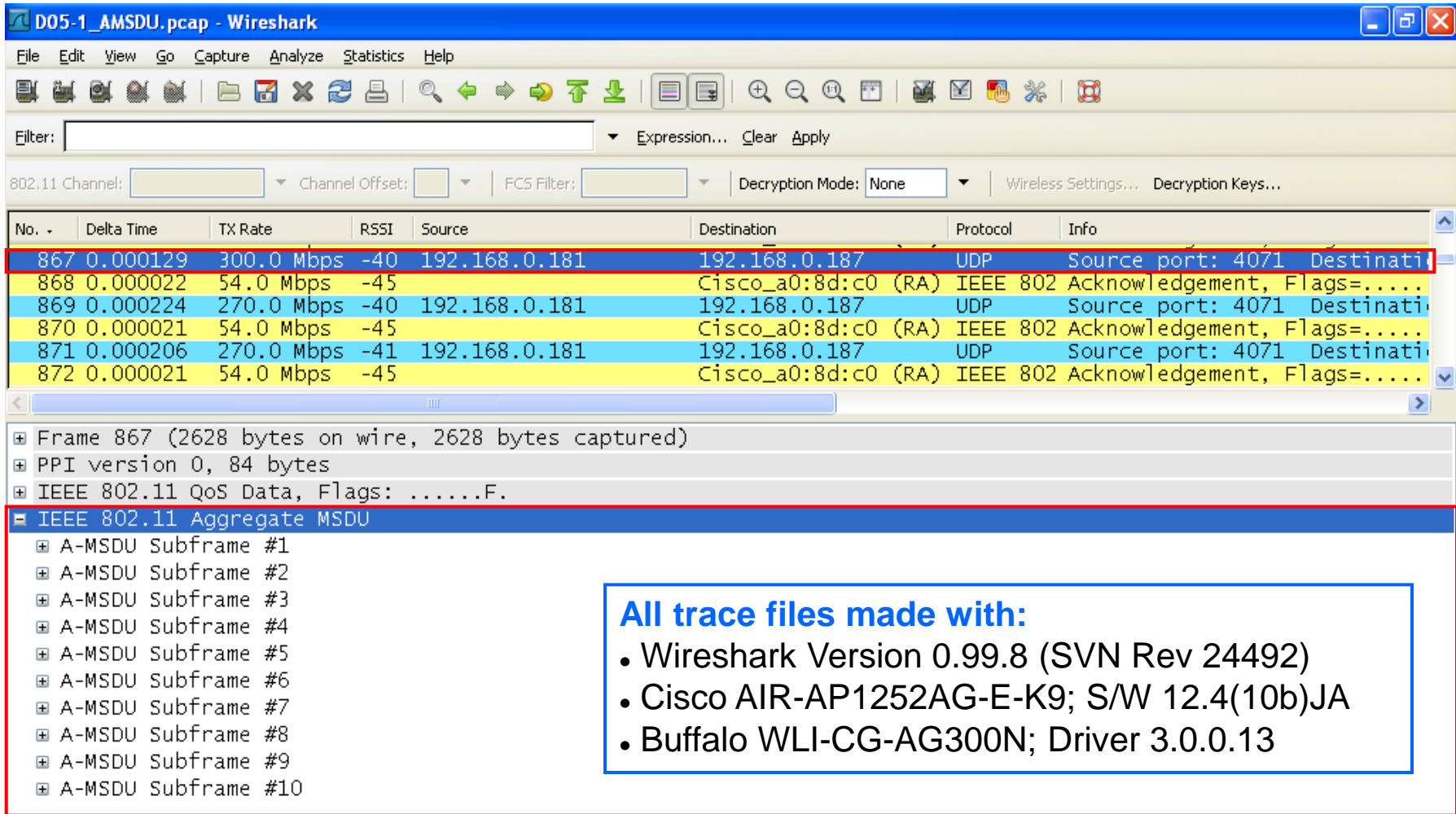
Channel Bonding 2.4 GHz Band



Channel Bonding 5 GHz Band



Aggregate-MAC Service Data Unit (A-MSDU)



The image shows a Wireshark capture of an IEEE 802.11 Aggregate MSDU frame. The packet list pane shows several packets, with packet 867 highlighted in red. The packet details pane shows the structure of the frame, including the IEEE 802.11 Aggregate MSDU subframes.

No.	Delta Time	TX Rate	RSSI	Source	Destination	Protocol	Info
867	0.000129	300.0 Mbps	-40	192.168.0.181	192.168.0.187	UDP	Source port: 4071 Destination...
868	0.000022	54.0 Mbps	-45		Cisco_a0:8d:c0 (RA)	IEEE 802	Acknowledgement, Flags=.....
869	0.000224	270.0 Mbps	-40	192.168.0.181	192.168.0.187	UDP	Source port: 4071 Destination...
870	0.000021	54.0 Mbps	-45		Cisco_a0:8d:c0 (RA)	IEEE 802	Acknowledgement, Flags=.....
871	0.000206	270.0 Mbps	-41	192.168.0.181	192.168.0.187	UDP	Source port: 4071 Destination...
872	0.000021	54.0 Mbps	-45		Cisco_a0:8d:c0 (RA)	IEEE 802	Acknowledgement, Flags=.....

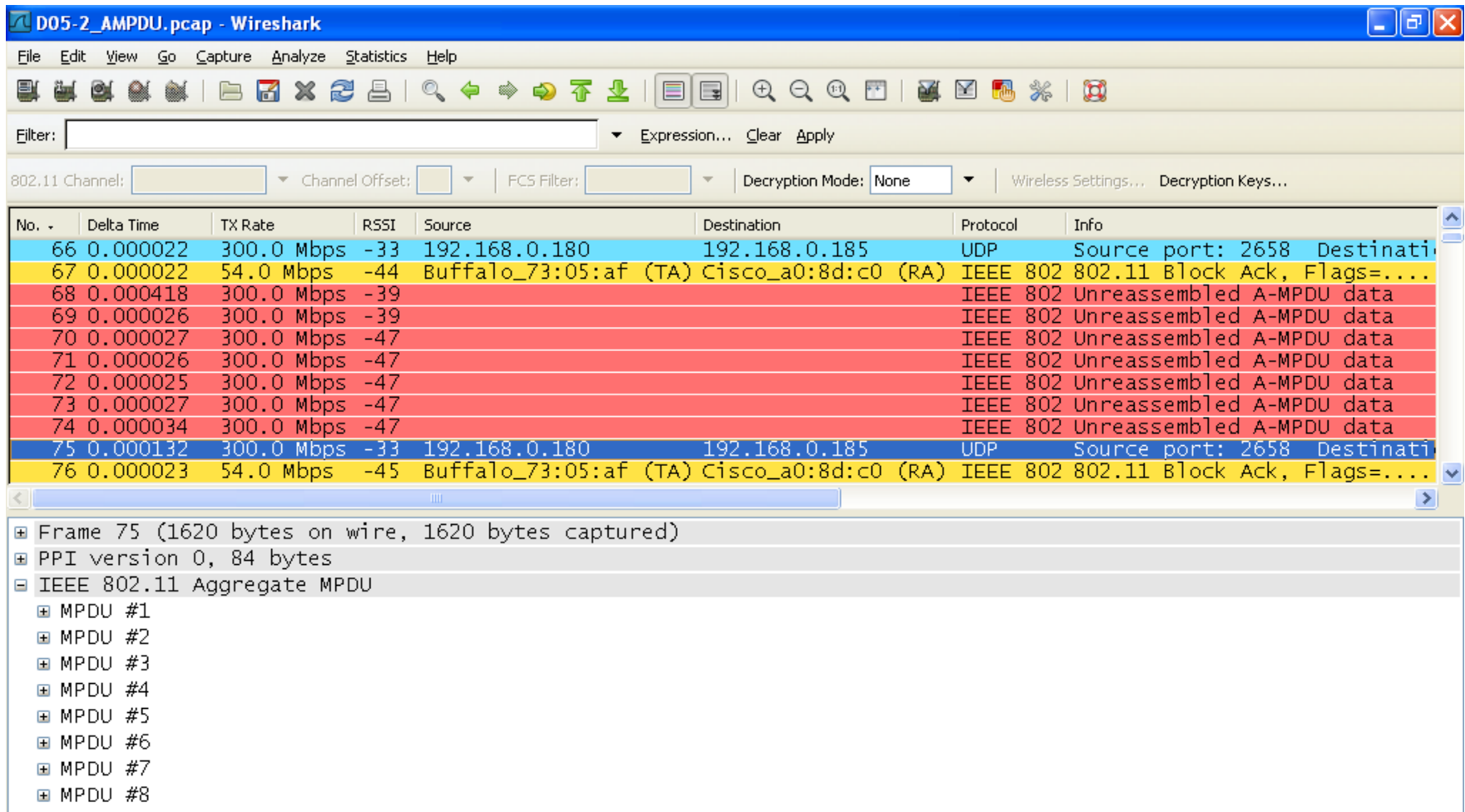
Frame 867 (2628 bytes on wire, 2628 bytes captured)

- PPI version 0, 84 bytes
- IEEE 802.11 QoS Data, Flags:F.
- IEEE 802.11 Aggregate MSDU**
 - A-MSDU Subframe #1
 - A-MSDU Subframe #2
 - A-MSDU Subframe #3
 - A-MSDU Subframe #4
 - A-MSDU Subframe #5
 - A-MSDU Subframe #6
 - A-MSDU Subframe #7
 - A-MSDU Subframe #8
 - A-MSDU Subframe #9
 - A-MSDU Subframe #10

All trace files made with:

- Wireshark Version 0.99.8 (SVN Rev 24492)
- Cisco AIR-AP1252AG-E-K9; S/W 12.4(10b)JA
- Buffalo WLI-CG-AG300N; Driver 3.0.0.13

Aggregate-MAC Protocol Data Unit (A-MPDU)



The image shows a Wireshark capture of an IEEE 802.11 A-MPDU. The main packet list shows frame 75 as a UDP packet from 192.168.0.180 to 192.168.0.185. The packet details pane shows the structure of the A-MPDU, including the PPI version and the IEEE 802.11 Aggregate MPDU containing eight individual MPDUs.

No.	Delta Time	TX Rate	RSSI	Source	Destination	Protocol	Info
66	0.000022	300.0 Mbps	-33	192.168.0.180	192.168.0.185	UDP	Source port: 2658 Destination...
67	0.000022	54.0 Mbps	-44	Buffalo_73:05:af (TA)	Cisco_a0:8d:c0 (RA)	IEEE 802	802.11 Block Ack, Flags=...
68	0.000418	300.0 Mbps	-39			IEEE 802	Unreassembled A-MPDU data
69	0.000026	300.0 Mbps	-39			IEEE 802	Unreassembled A-MPDU data
70	0.000027	300.0 Mbps	-47			IEEE 802	Unreassembled A-MPDU data
71	0.000026	300.0 Mbps	-47			IEEE 802	Unreassembled A-MPDU data
72	0.000025	300.0 Mbps	-47			IEEE 802	Unreassembled A-MPDU data
73	0.000027	300.0 Mbps	-47			IEEE 802	Unreassembled A-MPDU data
74	0.000034	300.0 Mbps	-47			IEEE 802	Unreassembled A-MPDU data
75	0.000132	300.0 Mbps	-33	192.168.0.180	192.168.0.185	UDP	Source port: 2658 Destination...
76	0.000023	54.0 Mbps	-45	Buffalo_73:05:af (TA)	Cisco_a0:8d:c0 (RA)	IEEE 802	802.11 Block Ack, Flags=...

Frame 75 (1620 bytes on wire, 1620 bytes captured)

- PPI version 0, 84 bytes
- IEEE 802.11 Aggregate MPDU
 - MPDU #1
 - MPDU #2
 - MPDU #3
 - MPDU #4
 - MPDU #5
 - MPDU #6
 - MPDU #7
 - MPDU #8

Block Acknowledges

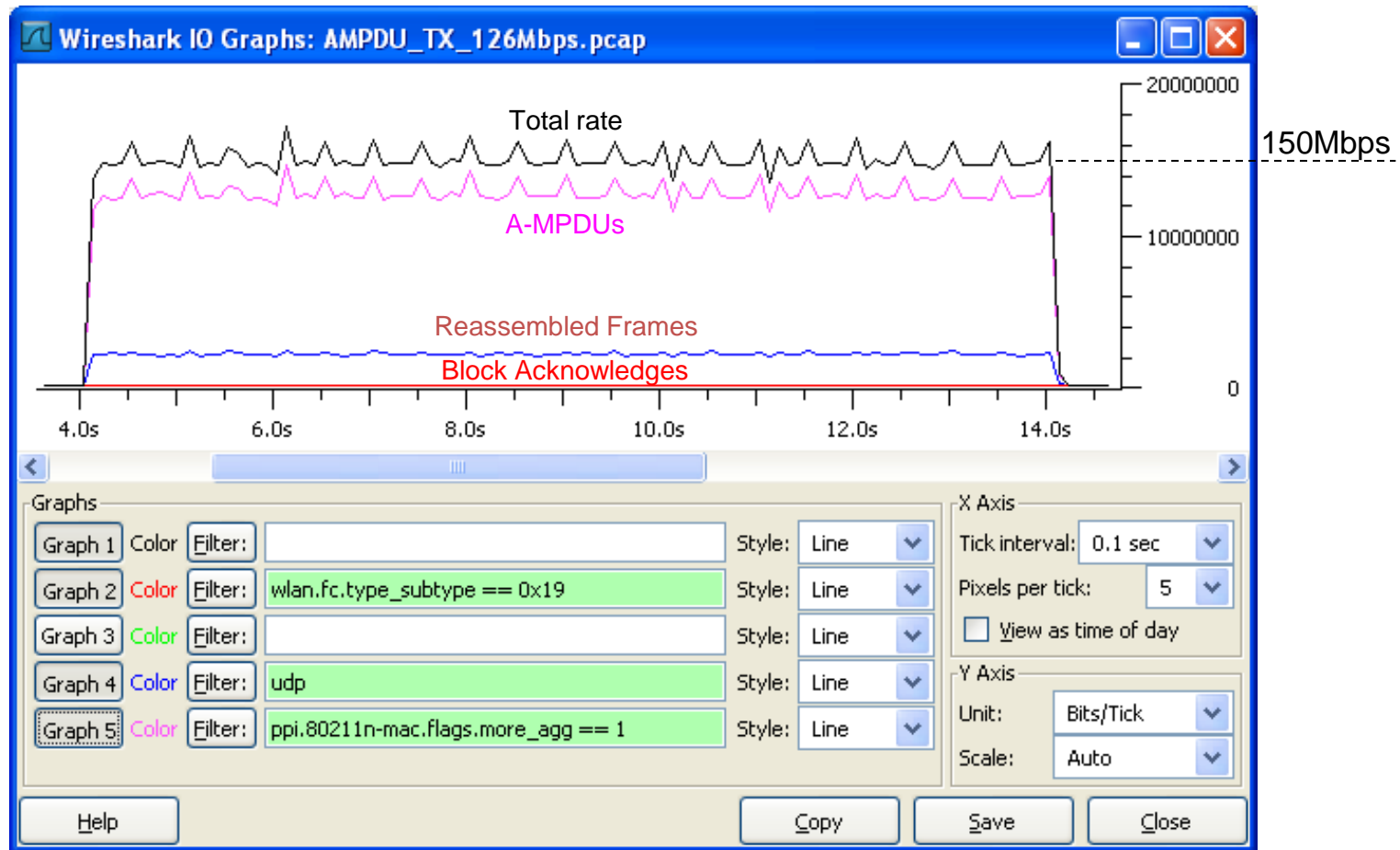
The image shows a Wireshark capture of a network packet. The packet list pane shows a Block Ack frame (No. 4588) from Buffalo_73:05:af (TA) to Cisco_a0:8d:c0 (RA). The packet details pane shows the structure of the IEEE 802.11 Block Ack frame, including Frame Control, Duration, Receiver and Transmitter addresses, Block Ack Request Type, Block Ack (BA) Control, Block Ack Starting Sequence Control (SSC), Block Ack Bitmap, and Frame check sequence. The packet bytes pane shows the raw data of the frame, with the Block Ack Bitmap field highlighted in red.

No.	Delta Time	TX Rate	RSSI	Source	Destination	Protocol	Info
4579	0.000021	54.0 Mbps	-47	Buffalo_73:05:af (TA)	Cisco_a0:8d:c0 (RA)	IEEE 802	802.11 Block Ack, Flags=...
4580	0.000369	300.0 Mbps	-39			IEEE 802	Unreassembled A-MPDU data
4581	0.000027	300.0 Mbps	-39			IEEE 802	Unreassembled A-MPDU data
4582	0.000028	300.0 Mbps	-47			IEEE 802	Unreassembled A-MPDU data
4583	0.000024	300.0 Mbps	-47			IEEE 802	Unreassembled A-MPDU data
4584	0.000031	300.0 Mbps	-47			IEEE 802	Unreassembled A-MPDU data
4585	0.000137	300.0 Mbps	-47			IEEE 802	Unreassembled A-MPDU data
4586	0.000021	300.0 Mbps	-47			IEEE 802	Unreassembled A-MPDU data
4587	0.000021	300.0 Mbps	-36	192.168.0.180	192.168.0.185	UDP	Source port: 2658 Destination...
4588	0.000021	54.0 Mbps	-47	Buffalo_73:05:af (TA)	Cisco_a0:8d:c0 (RA)	IEEE 802	802.11 Block Ack, Flags=...

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]

```
0000 00 00 20 00 69 00 00 00 02 00 14 00 56 f0 08 c6  ..i... ..V...
0010 01 00 00 00 01 00 6c 00 50 14 40 01 00 00 d1 a0  ....l.P.@...
0020 94 00 00 00 00 17 df a0 8d c0 00 16 01 73 05 af  ....s...
0030 04 00 d0 56 ff ff ff ff ff ff ff ef f4 7e a4 d2  ...V.....~..
```

802.11n Throughput analysis



UDP bandwidth measurement with **IPerf**
indicates throughput of 126Mbps

Thank you for your attention

Please fill in the evals

Trace files are available on
request from:

Rolf Leutert
Leutert NetServices
leutert@wireshark.ch

