

Wireshark Developer and User Conference

Discovering WLAN 802.11n MIMO

June 14, 2011

Rolf Leutert

Network Consultant & Trainer | Leutert NetServices | Switzerland

SHARKFEST '11

Stanford University

June 13-16, 2011

Session Agenda

- 🦈 Design Goals for 802.11n
- 🦈 IEEE 802.11n physical layer improvements
- 🦈 IEEE 802.11n MAC layer improvements
- 🦈 Per-Packet Information Header
- 🦈 Analyzing 'Bad BAR' and 'Deadlock' problem
- 🦈 Bandwidth Measurement
- 🦈 Backwards compatibility to a/b/g
- 🦈 Future of 802.11n

SHARKFEST '11

Design Goals for 802.11n

- 🦈 IEEE 802.11n is a proposed amendment to the IEEE 802.11-2007 wireless networking standard
- 🦈 Significantly improve PHY layer transmission rate over previous standards, such as 802.11a and 802.11b/g with 'High Throughput' (HT) options
- 🦈 Increasing the MAC layer transfer rate to achieve a minimum of 100 Mbps data throughput
- 🦈 Maintain backward compatibility with existing IEEE WLAN legacy solutions (802.11a/b/g)

SHARKFEST

How the Goals are achieved

A combination of technical functions at PHY and MAC layers are added to the existing 802.11 standard:

- ✓ Increasing the physical transfer rate with new modulation scheme and timing up to **600Mbps**
- ✓ New multi-streaming modulation technique using **MIMO** (multiple input, multiple output antennas)
- ✓ Joining two adjacent channels with **Channel bonding**
- ✓ Support for frame aggregation **A-MPDU & A-MSDU**
- ✓ New **Block Acknowledgments**

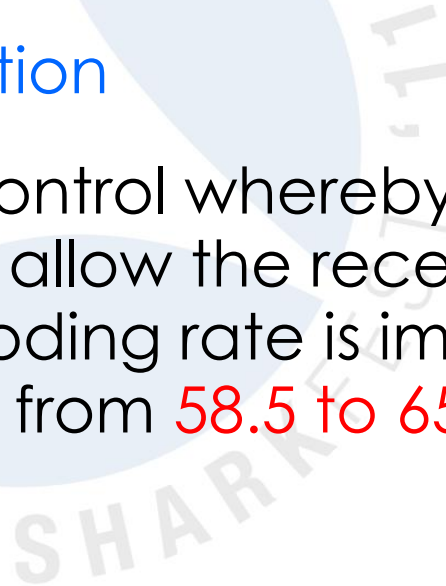
PHY layer improvements

Modified OFDM

The number of OFDM data sub-carriers is increased from 48 to 52 which improves the maximum throughput from **54 to 58.5 Mbps**

Forward Error Correction

FEC is a system of error control whereby the sender adds redundant data to allow the receiver to detect and correct errors. 3/4 coding rate is improved with 5/6 boosting the link rate from **58.5 to 65 Mbps**



PHY layer improvements (cont.)

Shorter Guard Interval (GI)

The GI between OFDM symbols is reduced from 800ns to 400ns and increases throughput from **65 to 72.2 Mbps**

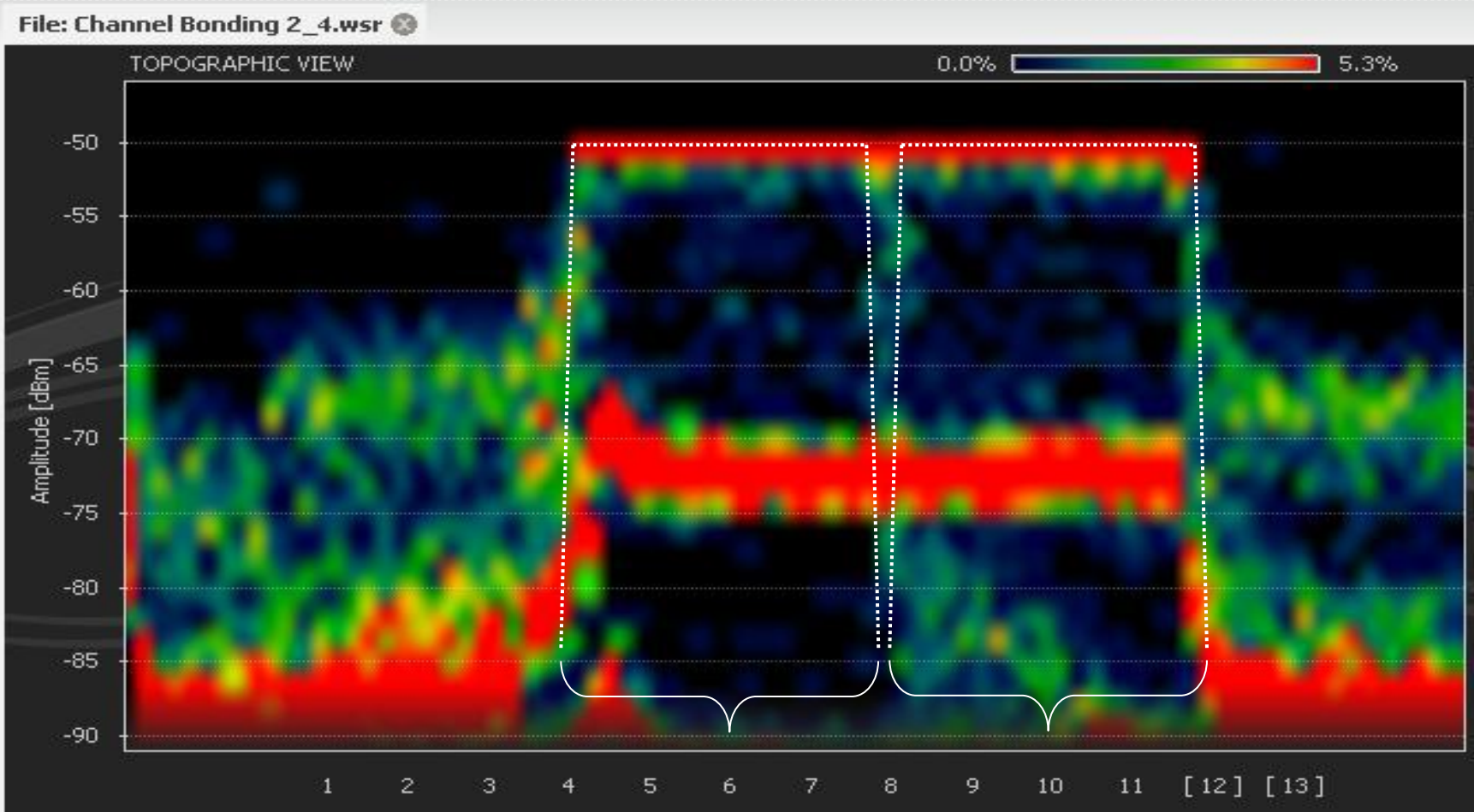
Channel Bonding

Doubling channel bandwidth from 20 to 40 MHz slightly more than doubles rate from **72.2 to 150 Mbps**

Spatial multiplexing

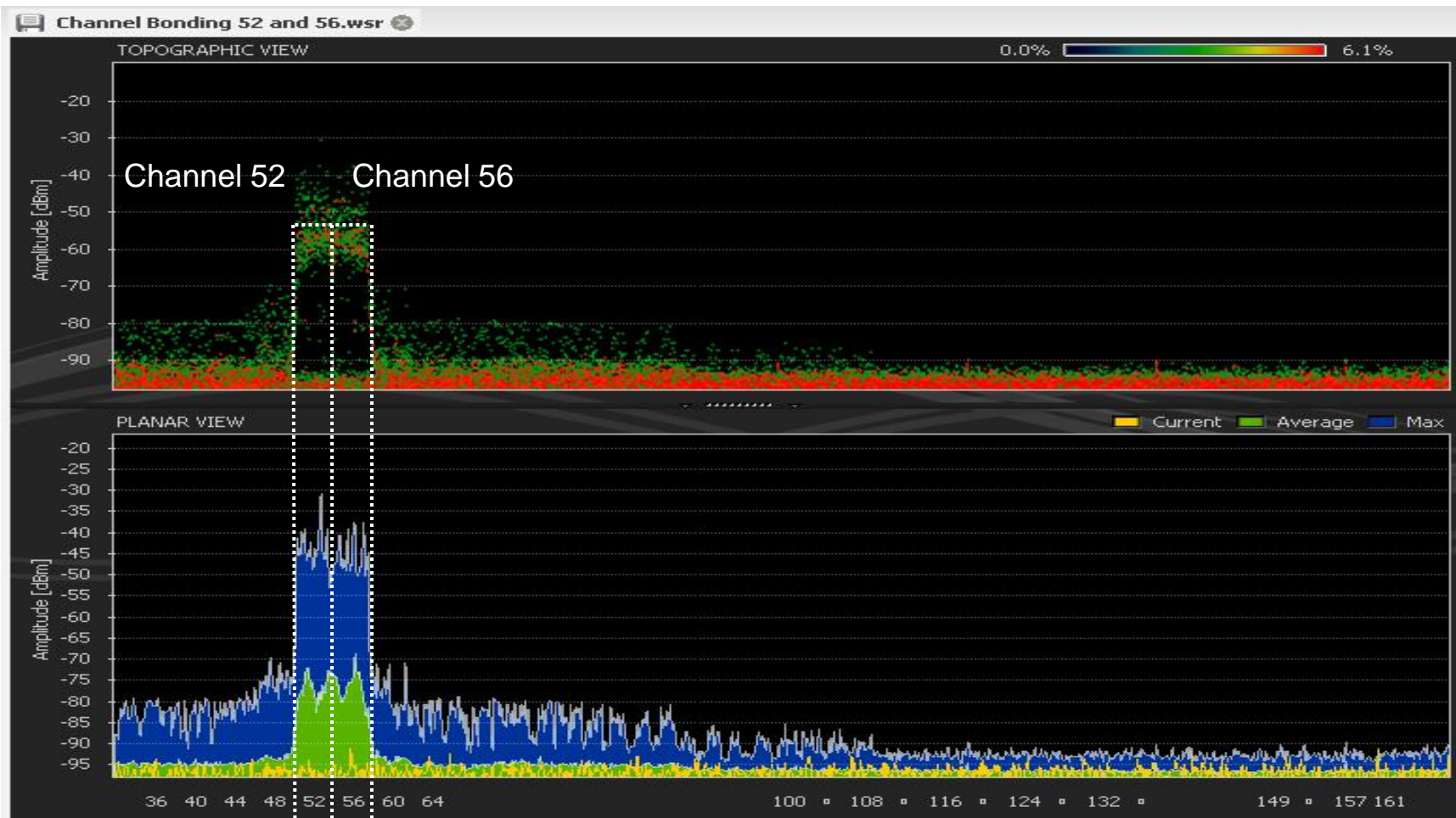
Support of up to four spatial streams (MIMO) increases throughput up to 4 times **150 to 600 Mbps**

Channel Bonding (Channel 6 & 10)



Recorded with Wi-Spy® from MetaGeek

Channel Bonding (Channel 52 & 56)

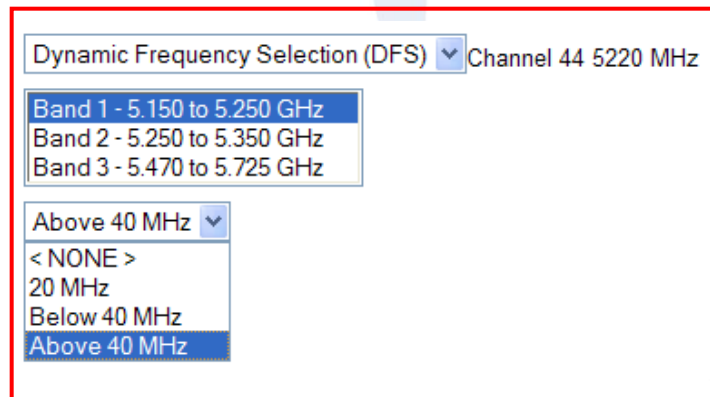


Recorded with Wi-Spy® from MetaGeek

Channel Bonding (configuration)

802.11n supports bundling of two 20 MHz channels

- 🐙 Select a control channel # and the channel offset
- 🐙 Both channels must fit inside allowed frequency range
- 🐙 A-band does not allow to select channel # manually



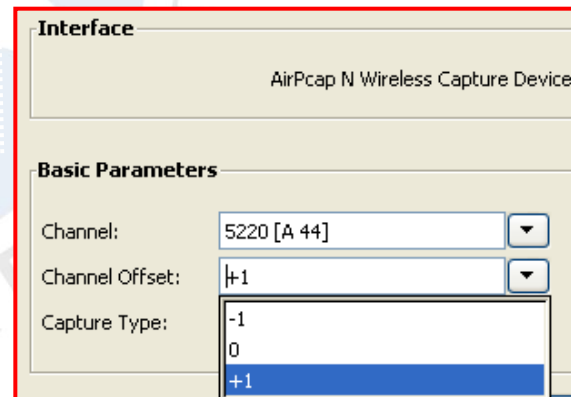
Dynamic Frequency Selection (DFS) Channel 44 5220 MHz

Band 1 - 5.150 to 5.250 GHz
Band 2 - 5.250 to 5.350 GHz
Band 3 - 5.470 to 5.725 GHz

Above 40 MHz

< NONE >
20 MHz
Below 40 MHz
Above 40 MHz

Configuration on Cisco AP1250



Interface
AirPcap N Wireless Capture Device

Basic Parameters

Channel: 5220 [A 44]

Channel Offset: +1

Capture Type:
-1
0
+1

Configuration on AirPcap N

Channel Allocation 5GHz 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 |
| Middle Band UNII-2 | 48 | 5.240 | 5.240 | -- |
| | 52 | 5.260* | 5.260 | 5.260 |
| | 56 | 5.280* | 5.280 | 5.280 |
| | 60 | 5.300* | 5.300 | 5.300 |
| High Band UNII-2 extended | 64 | 5.320* | 5.320 | 5.320 |
| | 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 |
| Upper Band UNII-3/ISM | 136 | 5.680* | 5.680 | 5.680 |
| | 140 | 5.700* | 5.700 | 5.700 |
| | 149 | 5.745 | -- | -- |
| | 153 | 5.765 | -- | -- |
| ISM | 157 | 5.785 | -- | -- |
| | 161 | 5.805 | -- | -- |
| | 165 | 5.825 | -- | -- |

| Available non-overlapping channels | |
|------------------------------------|---------|
| FCC (USA and Canada) | 24 20** |
| 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 |

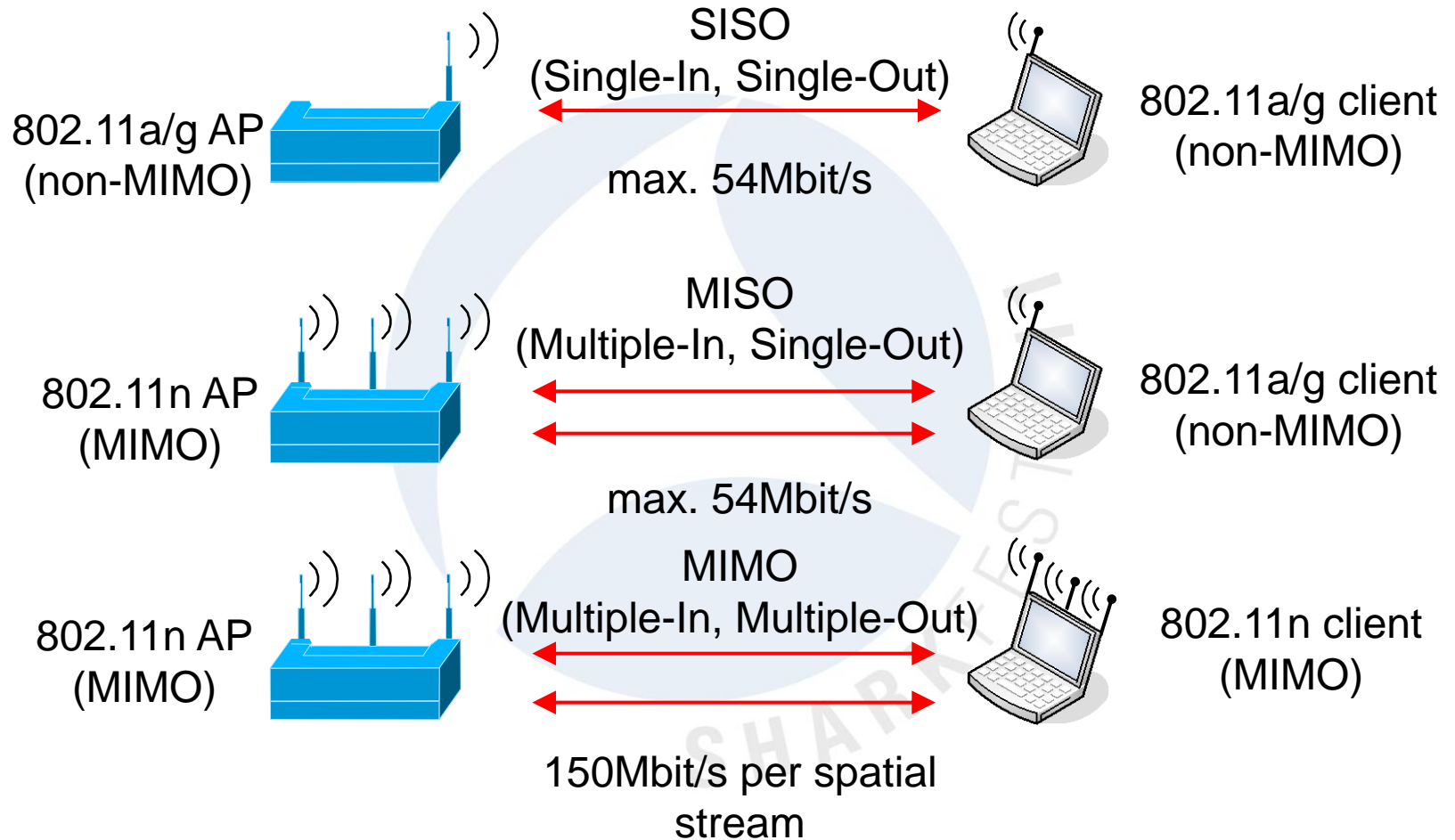
| Dynamic Frequency Selection (DFS) and 'Passive Scanning' required for | |
|---|-------------|
| FCC* (USA and Canada) | Band 2,2e |
| ETSI (Europe) | Band 1,2,2e |
| MKK (Japan) | Band 1,2,2e |

Some channels allowed for inhouse use only

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

** 4 Channels removed by FCC valid off October 5, 2009

Multi-Streaming Modulation



Modulation Coding Scheme (MCS)

802.11n introduces a new Modulation Coding Scheme

- 🦈 802.11 b/g adapts to channel conditions by selecting the highest of **12 possible rates** from 1 to 54 Mbps
- 🦈 The 802.11n standard will allow some **77 possible MCS'** - some compulsory, some optional
- 🦈 MCS selects, based on RF channel conditions, the best combination of **8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types**

SHARKFEST

MCS Configuration

Data Rates:

Best Range | Best Throughput | Default

| | | | |
|------------|--|------------------------------|-------------------------------|
| 6.0Mb/sec | <input checked="" type="radio"/> Require | <input type="radio"/> Enable | <input type="radio"/> Disable |
| 9.0Mb/sec | <input checked="" type="radio"/> Require | <input type="radio"/> Enable | <input type="radio"/> Disable |
| 12.0Mb/sec | <input checked="" type="radio"/> Require | <input type="radio"/> Enable | <input type="radio"/> Disable |
| 18.0Mb/sec | <input checked="" type="radio"/> Require | <input type="radio"/> Enable | <input type="radio"/> Disable |
| 24.0Mb/sec | <input checked="" type="radio"/> Require | <input type="radio"/> Enable | <input type="radio"/> Disable |
| 36.0Mb/sec | <input checked="" type="radio"/> Require | <input type="radio"/> Enable | <input type="radio"/> Disable |
| 48.0Mb/sec | <input checked="" type="radio"/> Require | <input type="radio"/> Enable | <input type="radio"/> Disable |
| 54.0Mb/sec | <input checked="" type="radio"/> Require | <input type="radio"/> Enable | <input type="radio"/> Disable |

MCS Rates:

| | | | | | | | | | | | | | | | | |
|----------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Enable | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> |
| Disable | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |



1 spatial stream

2 spatial streams

Screenshot Cisco AP1250




MCS Rate Chart

| MCS Rate Chart | | 20 MHz Channel | | | | | | | | 40 MHz Channel | | | | | | | |
|---------------------------------|----------|------------------------|------|------|------|---------------------|-------|------|-------|------------------------|------|-------|------|---------------------|------|------|------|
| | | 1 Stream (non MIMO) | | | | 2 Streams (MIMO) | | | | 1 Stream (non MIMO) | | | | 2 Streams (MIMO) | | | |
| 802.11n 2.4GHz GI = 800ns | MCS Rate | 0 | 1 | 2 | 3 | 8 | 9 | 10 | 11 | n.a. | n.a. | n.a. | n.a. | n.a. | n.a. | | |
| | Mbps | 6.5 | 13 | 19.5 | 26 | 13 | 26 | 39 | 52 | | | | | | | n.a. | n.a. |
| | | 39 | 52 | 58.5 | 65 | 78 | 104 | 117 | 130 | | | | | | | | |
| MCS Rate | 4 | 5 | 6 | 7 | 12 | 13 | 14 | 15 | | | | | | | | | |
| 802.11n 5GHz GI = 800ns | MCS Rate | 0 | 1 | 2 | 3 | 8 | 9 | 10 | 11 | 0 | 1 | 2 | 3 | 8 | 9 | 10 | 11 |
| | Mbps | 6.5 | 13 | 19.5 | 26 | 13 | 26 | 39 | 52 | 13.5 | 27 | 40.5 | 54 | 27 | 54 | 81 | 108 |
| | | 39 | 52 | 58.5 | 65 | 78 | 104 | 117 | 130 | 81 | 108 | 121.5 | 135 | 162 | 216 | 243 | 270 |
| MCS Rate | 4 | 5 | 6 | 7 | 12 | 13 | 14 | 15 | 4 | 5 | 6 | 7 | 12 | 13 | 14 | 15 | |
| 802.11n 5GHz GI = 400ns | MCS Rate | 0 | 1 | 2 | 3 | 8 | 9 | 10 | 11 | 0 | 1 | 2 | 3 | 8 | 9 | 10 | 11 |
| | Mbps | 7.2 | 14.4 | 21.7 | 28.9 | 14.4 | 28.9 | 43.3 | 57.8 | 15 | 30 | 45 | 60 | 30 | 60 | 90 | 120 |
| | | 43.3 | 57.8 | 65 | 72.2 | 86.7 | 115.6 | 130 | 144.4 | 90 | 120 | 135 | 150 | 180 | 240 | 270 | 300 |
| MCS Rate | 4 | 5 | 6 | 7 | 12 | 13 | 14 | 15 | 4 | 5 | 6 | 7 | 12 | 13 | 14 | 15 | |

SHARK

MAC layer improvements

Frame Aggregation Mechanisms

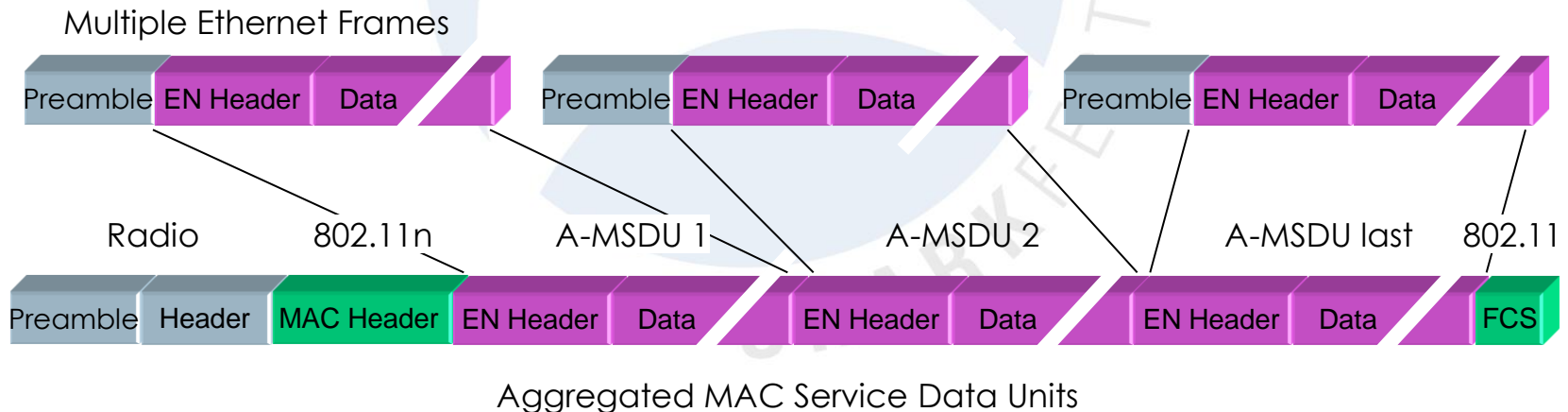
-  Aggregate-MAC Service Data Unit (A-MSDU) wraps multiple Ethernet frames in a .11n frame up to 8KB
-  Aggregate-MAC Protocol Data Unit (A-MPDU) allows bursting 802.11 frames up to 64KB
-  A-MPDU is performed in the software whereas A-MSDU is performed in the hardware

Block Acknowledgement

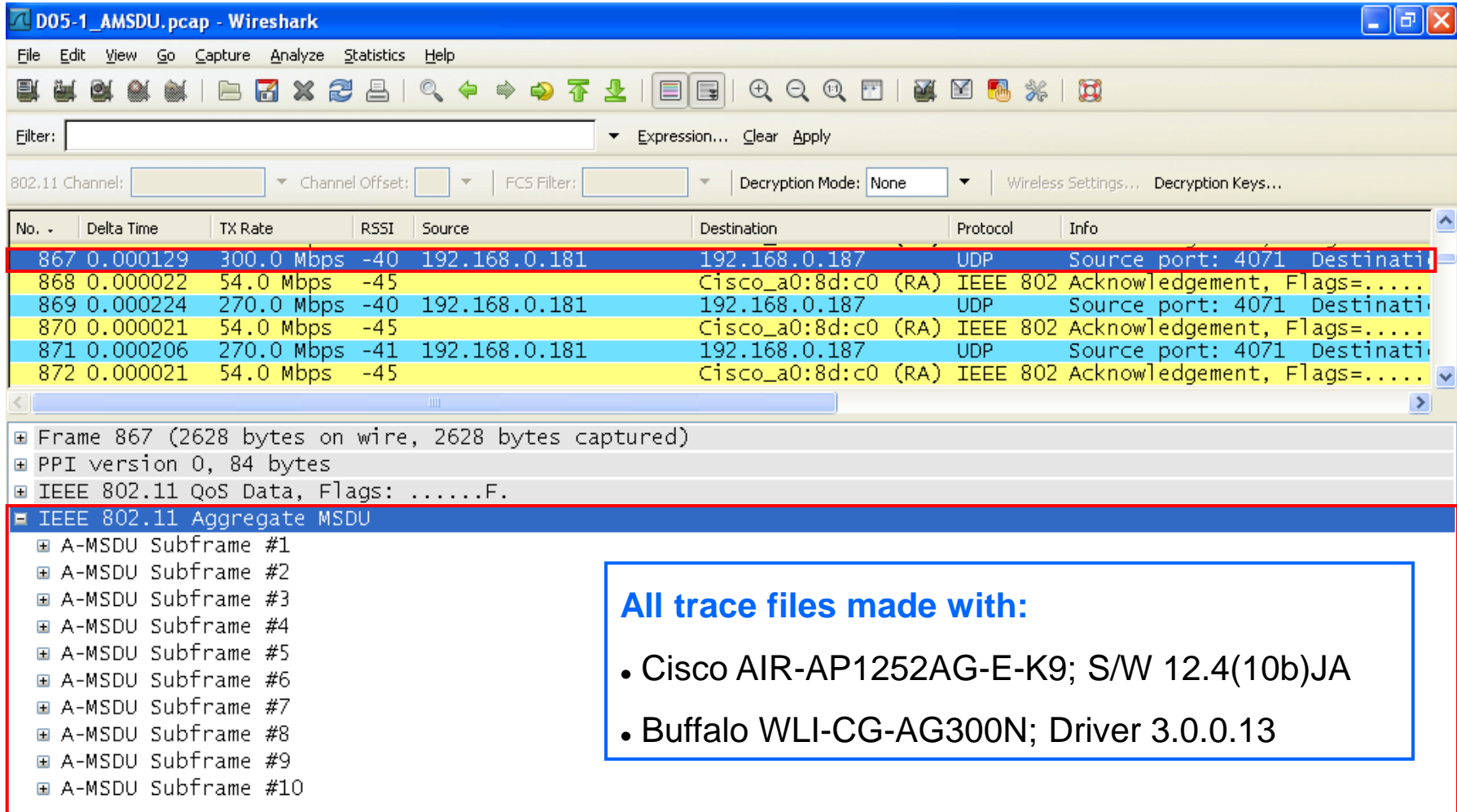
-  Block ACK effectively eliminates the need to initiate a new transfer for every MPDU

MSDU Aggregation

- Multiple Ethernet frames for a common destination are wrapped in a single 802.11 frame
- More efficient than A-MPDU as only one radio- and 802.11 MAC header is applied
- Whole frame must be retransmitted if no acknowledge



A-MSDU Analysis



The image shows a Wireshark capture of IEEE 802.11 frames. The main packet list table is as follows:

| 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 port: 4071 |
| 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 port: 4071 |
| 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 port: 4071 |
| 872 | 0.000021 | 54.0 Mbps | -45 | | Cisco_a0:8d:c0 (RA) | IEEE 802 | Acknowledgement, Flags=..... |

The details pane for frame 867 shows the following structure:

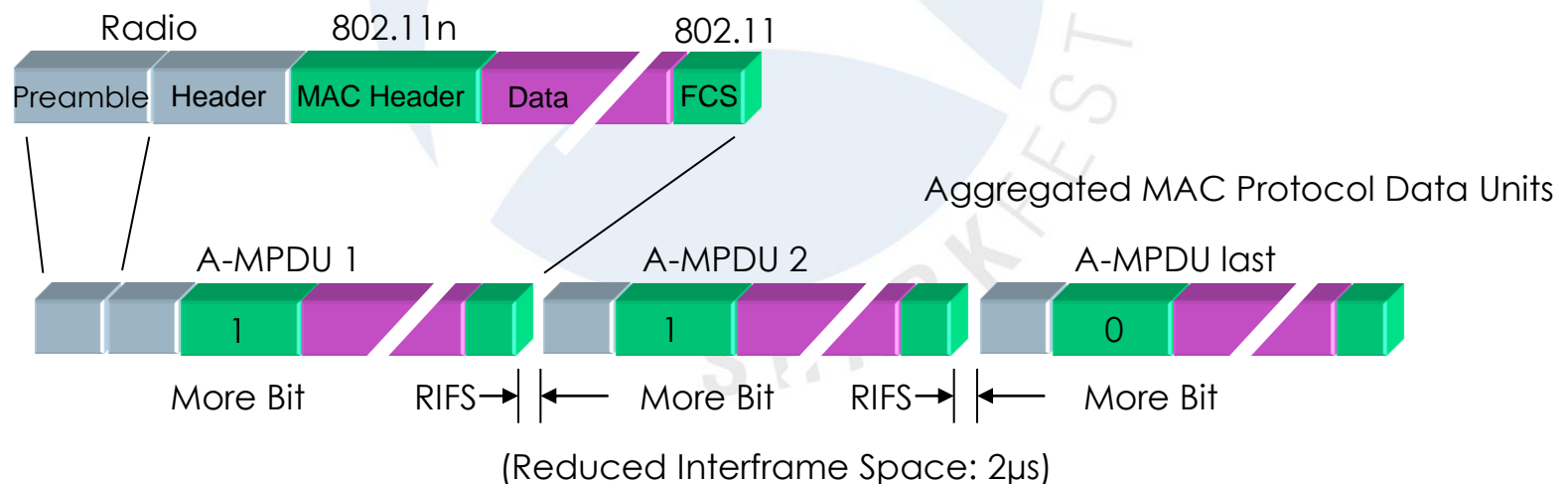
- Frame 867 (2628 bytes on wire, 2628 bytes captured)
- PPI version 0, 84 bytes
- IEEE 802.11 QoS Data, Flags:F.
- IEEE 802.11 Aggregate MSDU
 - A-MSDU Subframe #1
 - A-MSDU Subframe #2
 - A-MSDU Subframe #3
 - A-MSDU Subframe #4
 - A-MSDU Subframe #5
 - A-MSDU Subframe #6
 - A-MSDU Subframe #7
 - A-MSDU Subframe #8
 - A-MSDU Subframe #9
 - A-MSDU Subframe #10

All trace files made with:

- Cisco AIR-AP1252AG-E-K9; S/W 12.4(10b)JA
- Buffalo WLI-CG-AG300N; Driver 3.0.0.13

MPDU Aggregation

- Multiple Ethernet frames for a common destination are translated to 802.11 format and sent as burst
- Elements of an A-MPDUs burst can be acknowledged individually with one single Block-Acknowledge
- Only not-acknowledged A-MPDUs are retransmitted



A-MPDU Analysis

D05-2_AMPDU.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

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

| 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 Destinati |
| 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 Destinati |
| 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)

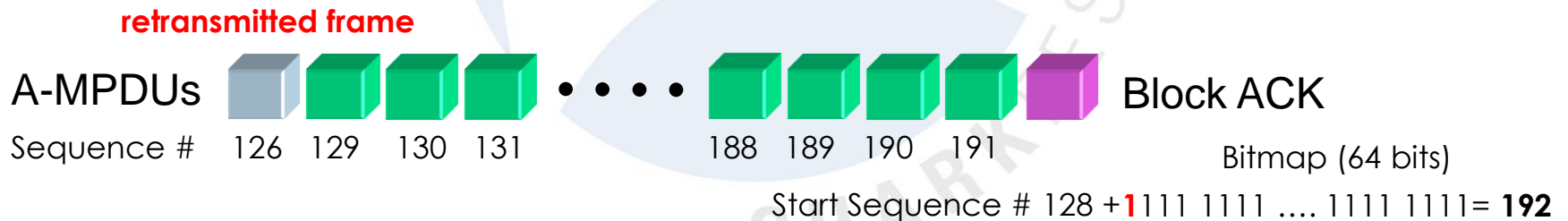
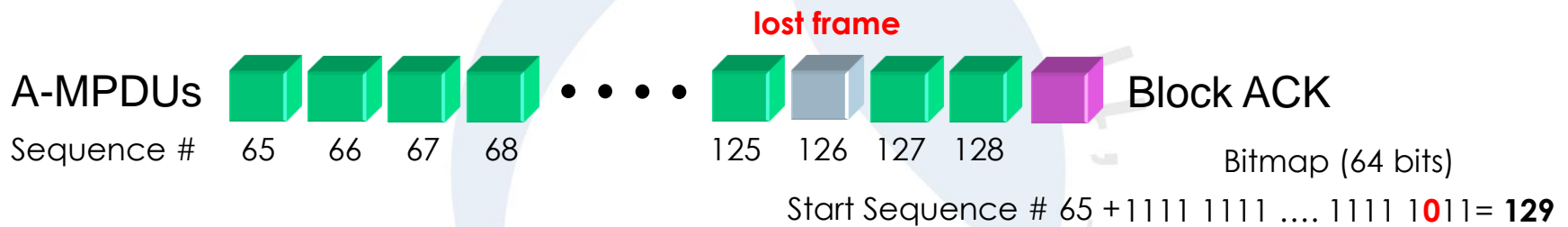
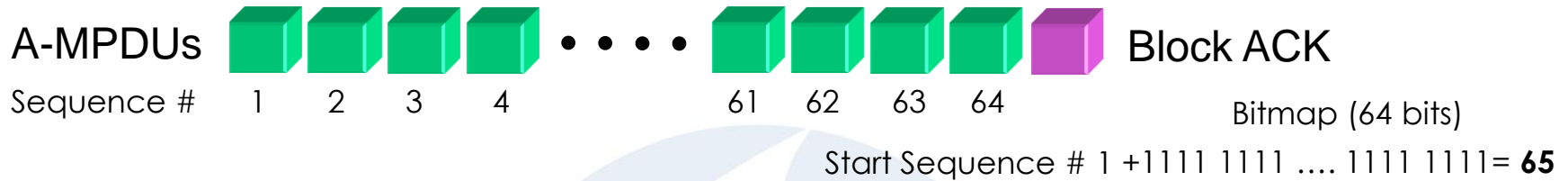
- PPI version 0, 84 bytes
- IEEE 802.11 Aggregate MPDU
 - MPDU #1
 - MPDU #2
 - MPDU #3
 - MPDU #4
 - MPDU #5
 - MPDU #6
 - MPDU #7
 - MPDU #8

Block-ACK Mechanism

- 🦈 Rather than sending an individual acknowledge following each data frame, 802.11n introduces the technique of confirming a burst of up to 64 frames with a single **Block ACK** (BA) frame
- 🦈 The Block ACK even contains a bitmap to **selectively acknowledge** individual frames of a burst (comparable to selective acknowledges of TCP)
- 🦈 The use of combined acknowledges can be requested by sending a **Block ACK Request** (BAR)

SHARKFEST

Block-ACK Mechanism (cont.)



Block-ACK Bitmap Analysis

The image shows a Wireshark capture of an IEEE 802.11 Block Ack frame. The packet list pane shows several packets, with packet 4588 selected. The packet details pane shows the structure of the Block Ack frame, with the Block Ack Bitmap field highlighted in red. 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.....~..
```


Block-ACK Bitmap Analysis (cont.)

| Frame # | Type | Sequence # | Bitmap (64 bits) |
|---------|-----------|-------------------------------------|-------------------------|
| 4579 | Block ACK | Start Sequence # $1381 + 64 = 1445$ | FF FF FF FF |
| 4580 | MPDU #1 | 1445 | |
| 4581 | MPDU #2 | 1446 | |
| 4582 | MPDU #3 | 1447 | |
| 4583 | MPDU #4 | 1448 | |
| 4584 | MPDU #5 | 1449 lost frame | |
| 4585 | MPDU #6 | 1450 | |
| 4586 | MPDU #7 | 1451 | |
| 4587 | MPDU #8 | 1452 | |
| 4588 | Block ACK | Start Sequence # $1389 + 64 = 1453$ | FF FF FF EF |
| 4589 | MPDU #1 | 1449 retransmitted frame | |
| 4590 | MPDU #2 | 1453 | |
| 4591 | MPDU #3 | 1454 | |
| 4592 | MPDU #4 | 1455 | |
| 4593 | MPDU #5 | 1456 | |
| 4594 | MPDU #6 | 1457 | |
| 4595 | MPDU #7 | 1458 | |
| 4596 | MPDU #8 | 1459 | |
| 4597 | MPDU #9 | 1460 | |
| 4598 | MPDU #10 | 1461 | |
| 4599 | Block ACK | Start Sequence # $1398 + 64 = 1462$ | FF FF FF FF |

Trace file: [D05_AMPDU.pcap](#)

Block-ACK negotiation/activation

- 🦈 The Block-ACK options are negotiated and confirmed with **'Action' frames** defined in 802.11e (WLAN QoS)
- 🦈 'Action' frames are used to negotiate other options too
 - Category Code 0 = Spectrum management
 - Category Code 1 = QoS options
 - Category Code 2 = DLS (Direct Link Setup)
 - Category Code 3 = Block Ack
- 🦈 The use of combined acknowledges can be requested by sending a **Block ACK Request** (BAR)

Block-ACK negotiation/activation (cont.)

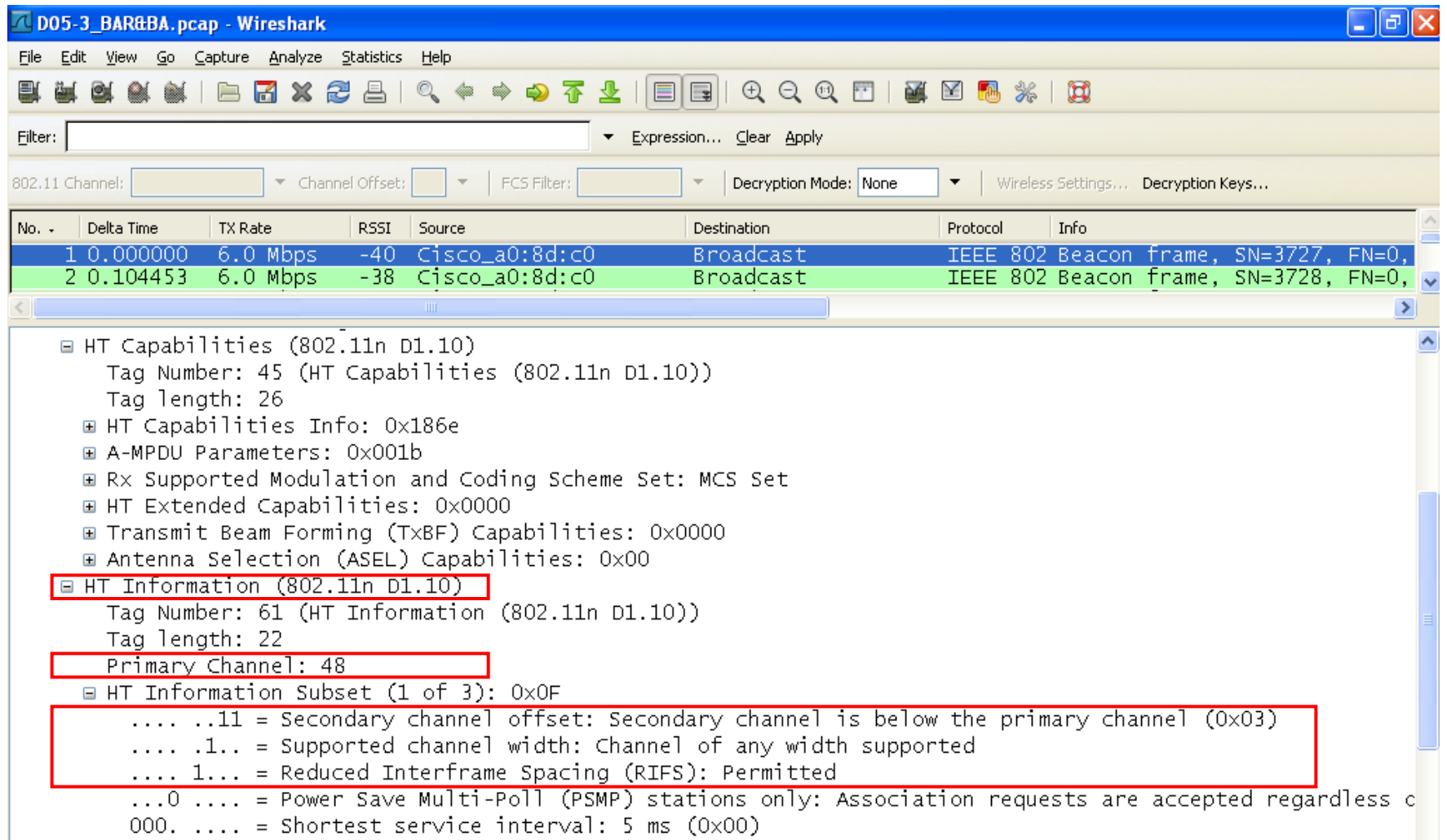
The image shows a Wireshark capture window titled "D05-3_BAR&BA.pcap - Wireshark". The main pane displays a list of captured frames. The following table summarizes the frames shown in the main pane:

| No. | Delta Time | TX Rate | RSSI | Source | Destination | Protocol | Info |
|-----|------------|---------|------|-----------------------|-----------------------|----------|--|
| 140 | 0.000022 | 54.0 Mb | -35 | | Cisco_a0:8d:c0 (RA) | IEEE 802 | Acknowledgement, Flags=.....C |
| 141 | 0.000024 | 300.0 M | -37 | Cisco_a0:8d:c0 | Buffalo_73:05:af | IEEE 802 | Action, SN=3837, FN=0, Flags=.....C |
| 142 | 0.000021 | 54.0 Mb | -35 | | Cisco_a0:8d:c0 (RA) | IEEE 802 | Acknowledgement, Flags=.....C |
| 143 | 0.001046 | 6.0 Mbp | -33 | Buffalo_73:05:af | Cisco_a0:8d:c0 | IEEE 802 | Action, SN=79, FN=0, Flags=.....C |
| 144 | 0.000021 | 6.0 Mbp | -41 | | Buffalo_73:05:af (RA) | IEEE 802 | Acknowledgement, Flags=.....C |
| 145 | 0.000145 | 54.0 Mb | -37 | Cisco_a0:8d:c0 (TA) | Buffalo_73:05:af (RA) | IEEE 802 | 802.11 Block Ack Req, Flags=.....C |
| 146 | 0.000019 | 54.0 Mb | -33 | Buffalo_73:05:af (TA) | Cisco_a0:8d:c0 (RA) | IEEE 802 | 802.11 Block Ack, Flags=.....C |
| 147 | 0.097038 | 6.0 Mbp | -41 | Cisco_a0:8d:c0 | Broadcast | IEEE 802 | Beacon frame, SN=3838, FN=0, Flags=..... |
| 148 | 0.104498 | 6.0 Mbp | -38 | Cisco_a0:8d:c0 | Broadcast | IEEE 802 | Beacon frame, SN=3839, FN=0, Flags=..... |

The packet details pane for frame 141 is expanded, showing the following structure:

- Frame 141 (121 bytes on wire, 121 bytes captured)
- PPI version 0, 84 bytes
- IEEE 802.11 Action, Flags:
- IEEE 802.11 wireless LAN management frame
 - Fixed parameters
 - Action: 0x03
 - Category code: Block Ack (3)
 - Action code: Add Block Ack Request (0x00)
 - Dialog token: 0x01
 - Block Ack Parameters: 0x1002
 - = A-MSDUs: Not Permitted
 - = Block Ack Policy: Immediate Block Ack
 - ..00 00.. = Traffic Identifier: 0x00
 - 0001 0000 00.. = Number of Buffers (1 Buffer = 2304 Bytes): 64
 - Block Ack Timeout: 0x0000
 - Block Ack Starting Sequence Control (SSC): 0x0010

New HT Capabilities in Beacon Frame



The image shows a Wireshark capture window titled "D05-3_BAR&BA.pcap - Wireshark". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Help), a toolbar with various icons, and a filter field. Below the filter, there are fields for "802.11 Channel", "Channel Offset", "FCS Filter", "Decryption Mode" (set to None), and "Wireless Settings...".

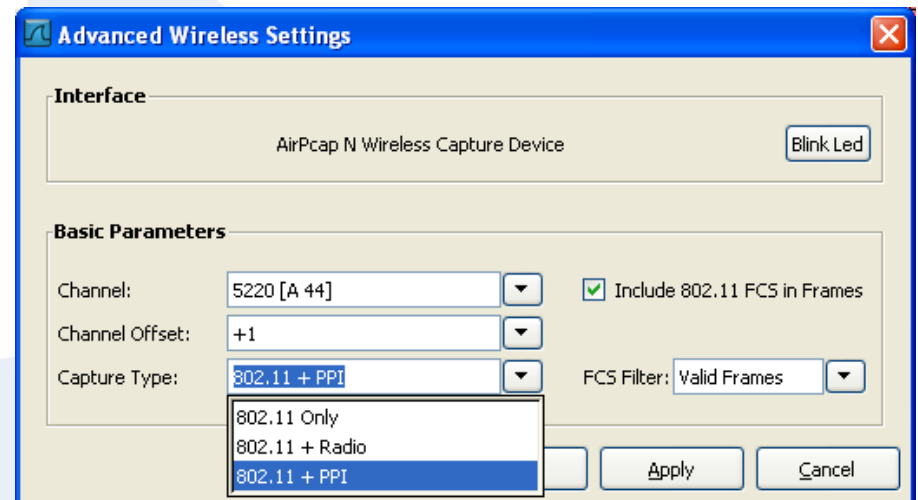
| No. | Delta Time | TX Rate | RSSI | Source | Destination | Protocol | Info |
|-----|------------|----------|------|----------------|-------------|-----------------------|----------------|
| 1 | 0.000000 | 6.0 Mbps | -40 | Cisco_a0:8d:c0 | Broadcast | IEEE 802 Beacon frame | SN=3727, FN=0, |
| 2 | 0.104453 | 6.0 Mbps | -38 | Cisco_a0:8d:c0 | Broadcast | IEEE 802 Beacon frame | SN=3728, FN=0, |

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

- HT Capabilities (802.11n D1.10)
 - Tag Number: 45 (HT Capabilities (802.11n D1.10))
 - Tag length: 26
 - HT Capabilities Info: 0x186e
 - A-MPDU Parameters: 0x001b
 - Rx Supported Modulation and Coding Scheme Set: MCS Set
 - HT Extended Capabilities: 0x0000
 - Transmit Beam Forming (TxBF) Capabilities: 0x0000
 - Antenna Selection (ASEL) Capabilities: 0x00
 - HT Information (802.11n D1.10)
 - Tag Number: 61 (HT Information (802.11n D1.10))
 - Tag length: 22
 - Primary Channel: 48
 - HT Information Subset (1 of 3): 0x0F
 -11 = Secondary channel offset: Secondary channel is below the primary channel (0x03)
 -1.. = Supported channel width: Channel of any width supported
 - ... 1.. = Reduced Interframe Spacing (RIFS): Permitted
 - ...0 = Power Save Multi-Poll (PSMP) stations only: Association requests are accepted regardless c
 - 000. = Shortest service interval: 5 ms (0x00)

Per-Packet Information Header (PPI)

- 🦈 New PPI header replaces the radiotap header used in 802.11 a/b/g with additional 802.11n radio information
- 🦈 PPI adds a pseudo-header to each packet and provides Meta data about RF signal strength, timing, options etc.



References

Radiotap manual: http://netbsd.gw.com/cgi-bin/man-cgi?ieee80211_radiotap+9+NetBSD-current

PPI manual: http://www.cacotech.com/documents/PPI_Header_format_1.0.1.pdf

Per-Packet Information Header (cont.)

Wireshark interface showing packet capture details for frame 60. The PPI version 0 header is expanded, showing fields like DLT: 105, 802.11-Common, 802.11n MAC+PHY, and [A-MPDU (9244 bytes w/hdrs): #55(1536), #56(1536), #57(1536), #58(1536), #59(1536), #60(1536)]. Red arrows point to these fields with explanatory text.

| No. | Delta Time | TX Rate | RSSI | Source | Destination | Protocol | Info |
|-----|------------|------------|------|-----------------------|---------------------|----------|----------------------------------|
| 54 | 0.000021 | 54.0 Mbps | -44 | Buffalo_73:05:af (TA) | Cisco_a0:8d:c0 (RA) | IEEE 802 | 802.11 Block Ack, Flags=... |
| 55 | 0.000187 | 300.0 Mbps | -39 | | | IEEE 802 | Unreassembled A-MPDU data |
| 56 | 0.000025 | 300.0 Mbps | -39 | | | IEEE 802 | Unreassembled A-MPDU data |
| 57 | 0.000026 | 300.0 Mbps | -47 | | | IEEE 802 | Unreassembled A-MPDU data |
| 58 | 0.000026 | 300.0 Mbps | -47 | | | IEEE 802 | Unreassembled A-MPDU data |
| 59 | 0.000026 | 300.0 Mbps | -47 | | | IEEE 802 | Unreassembled A-MPDU data |
| 60 | 0.000028 | 300.0 Mbps | -34 | 192.168.0.180 | 192.168.0.185 | UDP | Source port: 2658 Destination... |
| 61 | 0.000024 | 54.0 Mbps | -44 | Buffalo_73:05:af (TA) | Cisco_a0:8d:c0 (RA) | IEEE 802 | 802.11 Block Ack, Flags=... |

Frame 60 (1620 bytes on wire, 1620 bytes captured)

PPI version 0, 84 bytes

- Version: 0
- Flags: 0x00
- Header length: 84
- DLT: 105 ← Data-link level type (105=IEEE 802.11 wireless)
- 802.11-Common ← Contains data common to both pre-n and 802.11n
- 802.11n MAC+PHY ← Extension field contains radio information specific to 802.11n
- [A-MPDU (9244 bytes w/hdrs): #55(1536), #56(1536), #57(1536), #58(1536), #59(1536), #60(1536)]
- IEEE 802.11 Aggregate MPDU

Per-Packet Information Header (cont.)

```
802.11n MAC+PHY
Field type: 802.11n MAC+PHY Extensions (4)
Field length: 48
MAC flags: 0x00000016
.....0 = Greenfield flag: False
.....1. = HT20/HT40 flag: HT40
.....1.. = RX Short Guard Interval (SGI) flag: True
.....0... = Duplicate RX flag: False
.....1.... = Aggregate flag: True
.....0. .... = More aggregates flag: False
.....0.. .... = A-MPDU Delimiter CRC error after this frame flag: False
0..... = Debug Flag (more desc): False
AMPDU-ID: 0x000131cd
Num-Delimiters: 0
MCS: 15
Number of spatial streams: 2
RSSI combined: 62
Antenna 0 control RSSI: 53
Antenna 1 control RSSI: 58
Antenna 2 control RSSI: 58
Antenna 3 control RSSI: 255 [invalid]
Antenna 0 extension RSSI: 55
```


AirPcap Nx and Wireshark

AirPcap Nx and Wireshark, the perfect combination for:

- 🦈 Learning about how things are functioning
- 🦈 Finding out what 802.11n options and capabilities are offered and negotiated in the air
- 🦈 Verifying vendor specifications (like throughput etc.)
- 🦈 Investigating compatibility issues between vendors
- 🦈 Training technical people
- 🦈 and much more...



Frame Aggregation (config. examples)

Cisco's 802.11abgn AP1250

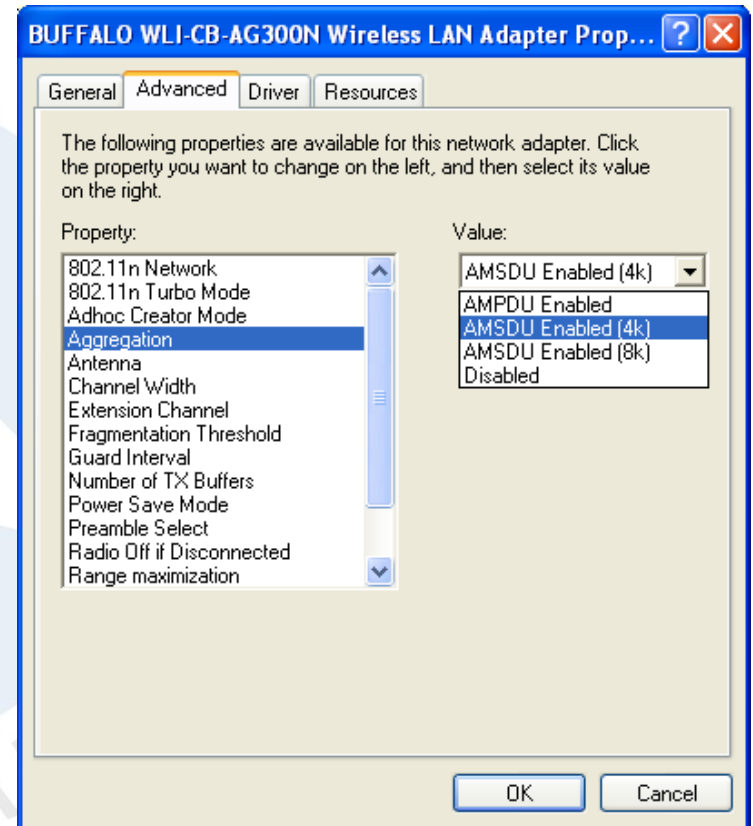


By disabling **A-MPDU** with the 'no' command, the traffic associated with that priority level uses **A-MSDU** transmission

Command line interface:

```
ap1250(config)#interface dot11Radio 1  
ap1250(config-if)#no ampdu transmit priority 0
```

Buffalo's 802.11abgn PC-Card



Analyzing 'Bad BAR' problem

D05-4_Bad_BAR.pcap - Wireshark

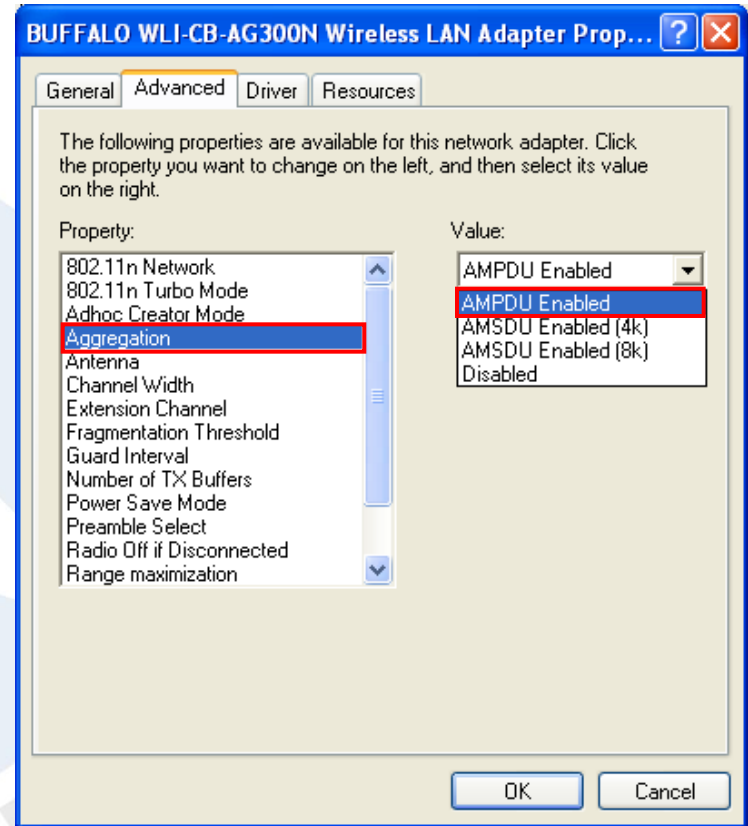
Filter: Expression... Clear Apply

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

| No. | Delta Time | TX Rate | RSSI | Source | Destination | Protocol | Info |
|-----|------------|------------|------|--------------------------------------|---------------------|-------------|--|
| 582 | 0.000027 | 243.0 Mbps | -45 | 195.186.6.80 | 192.168.0.187 | TCP | [TCP segment of a (re)assembled flow] |
| 583 | 0.000022 | 54.0 Mbps | -45 | Buffalo_73:05:af | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 584 | 0.000260 | 300.0 Mbps | 20 | 192.168.0.187 | 195.186.6.80 | TCP | 2823 > 80 [ACK] Seq=302 Ack=10881 win=65 |
| 585 | 0.000141 | 54.0 Mbps | -44 | 18:f0:9f:e5:18:f0 | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack Req, Flags=.....C |
| 586 | 0.000020 | 54.0 Mbps | -38 | Cisco_a0:8d:c0 (T 18:f0:9f:e5:18:f0) | (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 587 | 0.000174 | 54.0 Mbps | -44 | 18:f0:9f:e5:18:f0 | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack Req, Flags=....R...C |
| 588 | 0.000021 | 54.0 Mbps | -38 | Cisco_a0:8d:c0 (T 18:f0:9f:e5:18:f0) | (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 589 | 0.000126 | 243.0 Mbps | 19 | 195.186.6.80 | 192.168.0.187 | TCP | 80 > 2824 [SYN, ACK] Seq=0 Ack=1 win=584 |
| 590 | 0.000256 | 6.0 Mbps | -43 | 18:f0:9f:e5:18:f0 | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack Req, Flags=....R...C |
| 591 | 0.000020 | 6.0 Mbps | -37 | Cisco_a0:8d:c0 (T 18:f0:9f:e5:18:f0) | (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 592 | 0.000021 | 54.0 Mbps | -39 | Cisco_a0:8d:c0 | 18:f0:9f:e5:18:f0 | IEEE 802.11 | Deauthentication, SN=1287, FN=0, Flags=. |
| 593 | 0.000257 | 54.0 Mbps | -39 | Cisco_a0:8d:c0 | 18:f0:9f:e5:18:f0 | IEEE 802.11 | Deauthentication, SN=1287, FN=0, Flags=. |
| 594 | 0.000196 | 54.0 Mbps | -38 | Cisco_a0:8d:c0 | 18:f0:9f:e5:18:f0 | IEEE 802.11 | Deauthentication, SN=1287, FN=0, Flags=. |
| 595 | 0.000268 | 243.0 Mbps | -71 | 195.186.6.80 | 192.168.0.187 | TCP | 80 > 2824 [SYN, ACK] Seq=0 Ack=1 win=584 |
| 596 | 0.000020 | 54.0 Mbps | -44 | Buffalo_73:05:af | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 597 | 0.000218 | 6.0 Mbps | -43 | 18:f0:9f:e5:18:f0 | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack Req, Flags=....R...C |
| 598 | 0.000020 | 6.0 Mbps | -36 | Cisco_a0:8d:c0 (T 18:f0:9f:e5:18:f0) | (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 599 | 0.000212 | 6.0 Mbps | -43 | 18:f0:9f:e5:18:f0 | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack Req, Flags=....R...C |
| 600 | 0.000019 | 6.0 Mbps | -36 | Cisco_a0:8d:c0 (T 18:f0:9f:e5:18:f0) | (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 601 | 0.000523 | 6.0 Mbps | -43 | 18:f0:9f:e5:18:f0 | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack Req, Flags=....R...C |
| 602 | 0.000020 | 6.0 Mbps | -36 | Cisco_a0:8d:c0 (T 18:f0:9f:e5:18:f0) | (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 603 | 0.000307 | 6.0 Mbps | -42 | 18:f0:9f:e5:18:f0 | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack Req, Flags=....R...C |
| 604 | 0.000021 | 6.0 Mbps | -35 | Cisco_a0:8d:c0 (T 18:f0:9f:e5:18:f0) | (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 605 | 0.000707 | 6.0 Mbps | -41 | 18:f0:9f:e5:18:f0 | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack Req, Flags=....R...C |
| 606 | 0.000021 | 6.0 Mbps | -35 | Cisco_a0:8d:c0 (T 18:f0:9f:e5:18:f0) | (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 607 | 0.000166 | 6.0 Mbps | -41 | 18:f0:9f:e5:18:f0 | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack Req, Flags=....R...C |
| 608 | 0.000020 | 6.0 Mbps | -35 | Cisco_a0:8d:c0 (T 18:f0:9f:e5:18:f0) | (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 609 | 0.000224 | 6.0 Mbps | -41 | 18:f0:9f:e5:18:f0 | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack Req, Flags=....R...C |
| 610 | 0.000020 | 6.0 Mbps | -36 | Cisco_a0:8d:c0 (T 18:f0:9f:e5:18:f0) | (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 611 | 0.000119 | 6.0 Mbps | -42 | 18:f0:9f:e5:18:f0 | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack Req, Flags=....R...C |

Analyzing 'Bad BAR' problem (cont.)

- 🦈 Buffalo WLI-CB-AG300N is using strange SRC MAC address when sending BAR
- 🦈 Problem occurs only when A-MPDU is activated
- 🦈 Problem seems to be related to retransmissions
- 🦈 Possibly a driver issue as A-MPDU is done in software
- 🦈 A-MSDU works fine



SHARK

Analyzing 'Deadlock' problem

The image shows a Wireshark packet capture window titled "D05-5_DeadLock.pcap - Wireshark". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Help), a toolbar with various icons, and a filter field. Below the filter, there are settings for the capture channel (802.11), channel offset, FCS filter, decryption mode (None), and wireless settings. The main display area shows a list of network packets with columns for No., Delta Time, TX Rate, RSSI, Source, Destination, Protocol, and Info.

| No. | Delta Time | TX Rate | RSSI | Source | Destination | Protocol | Info |
|-------|------------|------------|------|-----------------------|-----------------------|-------------|---|
| 22105 | 0.000022 | 6.0 Mbps | -39 | Buffalo_73:05:af (TA) | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 22106 | 0.001719 | 216.0 Mbps | 78 | 195.186.8.35 | 192.168.0.187 | TCP | 1935 > 2604 [ACK] Seq=3788779 Ack=3803 |
| 22107 | 0.000022 | 6.0 Mbps | -40 | Buffalo_73:05:af (TA) | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 22108 | 0.000243 | 6.0 Mbps | -45 | 195.186.8.35 | Buffalo_73:05:af (RA) | IEEE 802.11 | Acknowledgement, Flags=.....C |
| 22109 | 0.001525 | 216.0 Mbps | -97 | 195.186.8.35 | 192.168.0.187 | TCP | 1935 > 2604 [ACK] Seq=3789303 Ack=3803 |
| 22110 | 0.000252 | 216.0 Mbps | -50 | 195.186.8.35 | 192.168.0.187 | TCP | [TCP out-of-order] 1935 > 2604 [ACK] |
| 22111 | 0.000020 | 6.0 Mbps | -40 | Buffalo_73:05:af (TA) | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 22112 | 0.000276 | 216.0 Mbps | -44 | 195.186.8.35 | 192.168.0.187 | RTMP | Audio Data[Malformed Packet] |
| 22113 | 0.000021 | 6.0 Mbps | -40 | Buffalo_73:05:af (TA) | Cisco_a0:8d:c0 (RA) | IEEE 802.11 | 802.11 Block Ack, Flags=.....C |
| 22114 | 0.000122 | 300.0 Mbps | -39 | 192.168.0.187 | 195.186.8.35 | TCP | 2604 > 1935 [ACK] Seq=3803 Ack=378989 |
| 22115 | 0.000115 | 6.0 Mbps | -45 | 195.186.8.35 | Buffalo_73:05:af (RA) | IEEE 802.11 | Acknowledgement, Flags=.....C |
| 22116 | 0.001367 | 216.0 Mbps | -96 | 195.186.8.35 | 192.168.0.187 | RTMP | Audio Data[Malformed Packet] |
| 22117 | 0.000942 | 216.0 Mbps | 107 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP out-of-order] Audio Data[Malformed Packet] |
| 22118 | 0.000213 | 216.0 Mbps | -35 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP out-of-order] Audio Data[Malformed Packet] |
| 22119 | 0.000223 | 216.0 Mbps | -60 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP out-of-order] Audio Data[Malformed Packet] |
| 22120 | 0.000346 | 162.0 Mbps | -60 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP out-of-order] Audio Data[Malformed Packet] |
| 22121 | 0.000223 | 162.0 Mbps | -96 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP out-of-order] Audio Data[Malformed Packet] |
| 22122 | 0.000307 | 108.0 Mbps | -96 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP out-of-order] Audio Data[Malformed Packet] |
| 22123 | 0.000233 | 108.0 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP out-of-order] Audio Data[Malformed Packet] |
| 22124 | 0.000363 | 54.0 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP out-of-order] Audio Data[Malformed Packet] |

Problem starts at frame # 22116 which is not acknowledged by receiver

Analyzing 'Deadlock' problem (cont.)

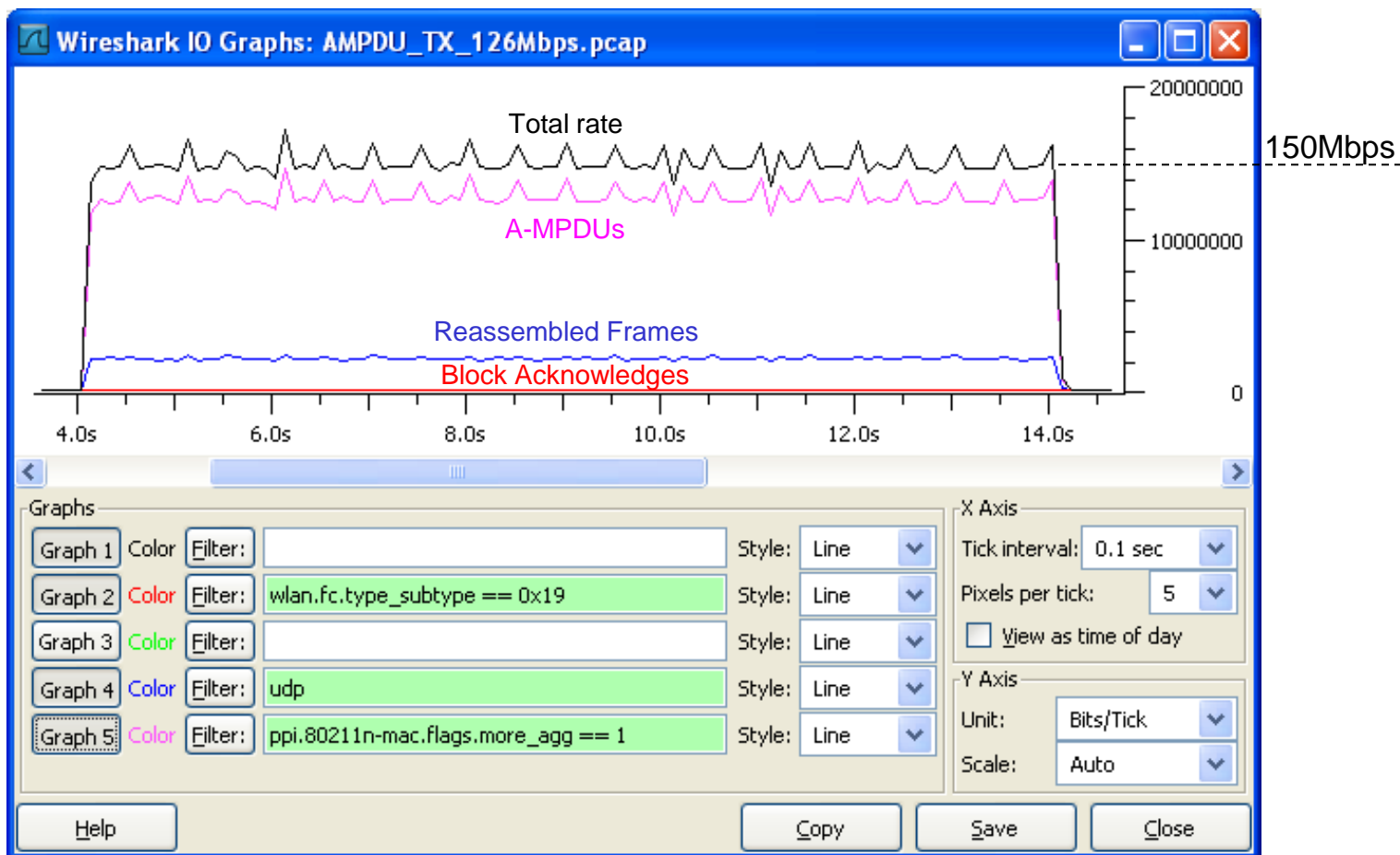
Wireshark interface showing a capture of network traffic. The filter is set to 'Expression...'. The capture shows a series of RTMP packets from 195.186.8.35 to 192.168.0.187, followed by a deauthentication frame (IEEE 802.11) from Cisco_a0:8d:c0 to Buffalo_73:05:af (packet 22247), and then several beacon frames (IEEE 802.11) from Cisco_a0:8d:c0 to Broadcast.

| No. | Delta Time | TX Rate | RSSI | Source | Destination | Protocol | Info |
|-------|------------|----------|------|----------------|------------------|-------------|--|
| 22227 | 0.001221 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22228 | 0.001110 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22229 | 0.001212 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22230 | 0.001186 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22231 | 0.001169 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22232 | 0.001131 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22233 | 0.001169 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22234 | 0.001111 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22235 | 0.001168 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22236 | 0.001111 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22237 | 0.001194 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22238 | 0.001250 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22239 | 0.001219 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22240 | 0.001111 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22241 | 0.001169 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22242 | 0.001265 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22243 | 0.001241 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22244 | 0.001108 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22245 | 0.001170 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22246 | 0.001158 | 6.5 Mbps | -125 | 195.186.8.35 | 192.168.0.187 | RTMP | [TCP Retransmission] Audio Data [Malformed Packe |
| 22247 | 0.000970 | 6.0 Mbps | -41 | Cisco_a0:8d:c0 | Buffalo_73:05:af | IEEE 802.11 | Deauthentication, SN=1530, FN=0, Flags=..... |
| 22248 | 0.000225 | 6.0 Mbps | -41 | Cisco_a0:8d:c0 | Buffalo_73:05:af | IEEE 802.11 | Deauthentication, SN=1530, FN=0, Flags=...R... |
| 22249 | 0.000235 | 6.0 Mbps | -41 | Cisco_a0:8d:c0 | Buffalo_73:05:af | IEEE 802.11 | Deauthentication, SN=1530, FN=0, Flags=...R... |
| 22250 | 0.000232 | 6.0 Mbps | -41 | Cisco_a0:8d:c0 | Buffalo_73:05:af | IEEE 802.11 | Deauthentication, SN=1530, FN=0, Flags=...R... |
| 22251 | 0.009058 | 6.0 Mbps | -41 | Cisco_a0:8d:c0 | Broadcast | IEEE 802.11 | Beacon frame, SN=1531, FN=0, Flags=.....C, E |
| 22252 | 0.104451 | 6.0 Mbps | -42 | Cisco_a0:8d:c0 | Broadcast | IEEE 802.11 | Beacon frame, SN=1532, FN=0, Flags=.....C, E |
| 22253 | 0.104450 | 6.0 Mbps | -39 | Cisco_a0:8d:c0 | Broadcast | IEEE 802.11 | Beacon frame, SN=1533, FN=0, Flags=.....C, E |
| 22254 | 0.104446 | 6.0 Mbps | -42 | Cisco_a0:8d:c0 | Broadcast | IEEE 802.11 | Beacon frame, SN=1534, FN=0, Flags=.....C, E |

Analyzing 'Deadlock' problem (cont.)

- 🦈 Access point retransmits frame 128 times up to frame # 22246 (value of Max. Data Retries counter)
- 🦈 As the mobile station does not acknowledge, access point sends 'Deauthentication' in frame # 22247 and removes station from association list
- 🦈 As mobile station does not acknowledge again, access point retransmits in frames # 22248 to 22250
- 🦈 Mobile station does not acknowledge, assumes to be still associated with access point and keeps sending frames (# 22298, 22315 etc.) → Deadlock situation

Bandwidth Measurement



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

Backwards compatibility to a/b/g

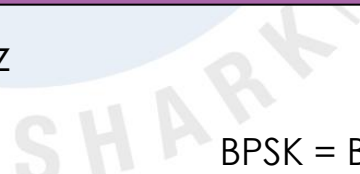


| Mbps | Coding | Modulation | Description | |
|------------------------------------|------------------------------|----------------------------------|---|----------------|
| 1 2 | Barker Barker | DBPSK | 802.11 DSSS (Clause 15) with ,Long Preamble' | 802.11a |
| 5.5 11 | CCK CCK | DQPSK | 802.11b HR/DSSS (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) | |
| 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

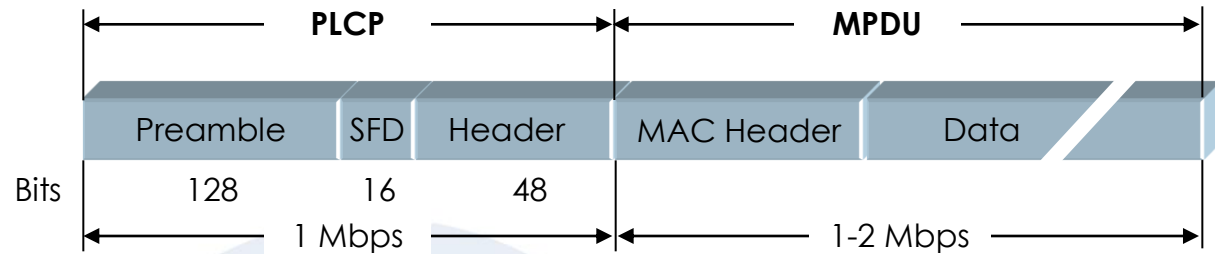
CCK = Complementary Code Keying
 DBPSK = Differential Binary Phase-Shift Keying
 DQPSK = Differential Quadrature Phase-Shift Keying
 OFDM = Orthogonal Frequency Division Multiplexing

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



Backwards compatibility to a/b/g (cont.)

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 (decodiert by Wireshark)

Backwards compatibility to a/b/g (cont.)

802.11n supports three compatibility modes

Legacy mode

Mixed mode

Greenfield mode

Legacy mode

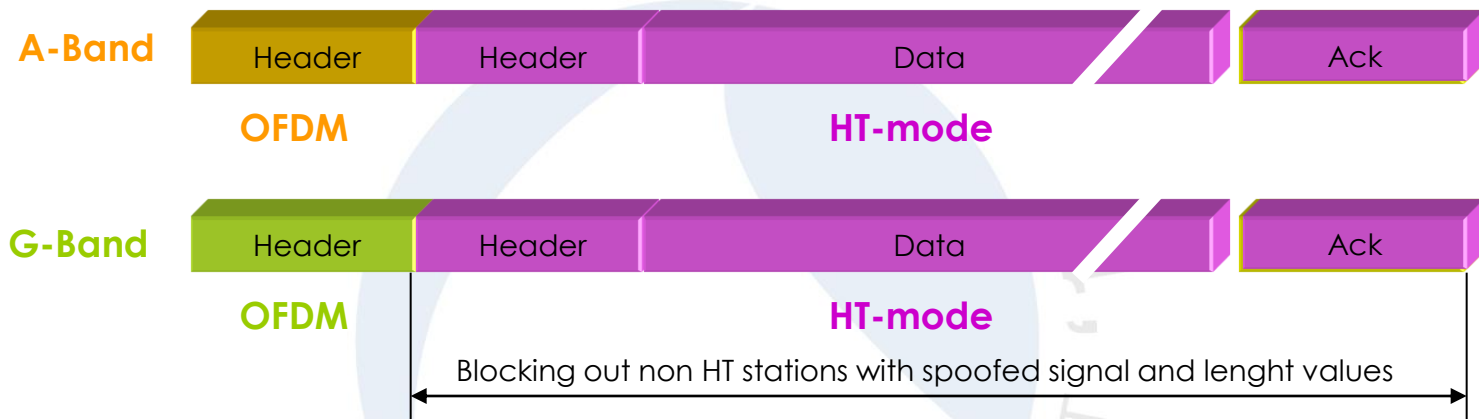
802.11n to b/g compatibility with Clear-to-send to self



Backwards compatibility to a/b/g (cont.)

Mixed mode

802.11n to a/g compatibility with Legacy header



Greenfield mode

No backwards compatibility to a/b/g



Future of 802.11n

- 🦈 Standard has been ratified September 2009 after years of discussions. (IEEE 802.11n-2009)
- 🦈 Standard is based on 802.11n Draft 2 specifications with two streams, all other functions are optional.
- 🦈 Interoperability remains a question mark for pre-N products
- 🦈 New products supporting technical features like:
 - Up to four spatial streams
 - Transmit Beamforming
 - Direct Link Setup ... and many more

Thanks for visiting



Rolf Leutert, Leutert NetServices, www.wireshark.ch