











Inside 802.11n





Technical details about the new WLAN standard

presented by
Rolf Leutert
Leutert NetServices
www.wireshark.ch

Agenda Inside 802.11n

-  Design goals for 802.11n
-  802.11n physical layer improvements
-  802.11n MAC layer improvements
-  How to analyze 802.11n
-  Throughput measurement
-  Overview WLAN standards & frame types
-  Backwards compatibility to 802.11a/b/g
-  Future of 802.11n

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)

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**

Improved 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

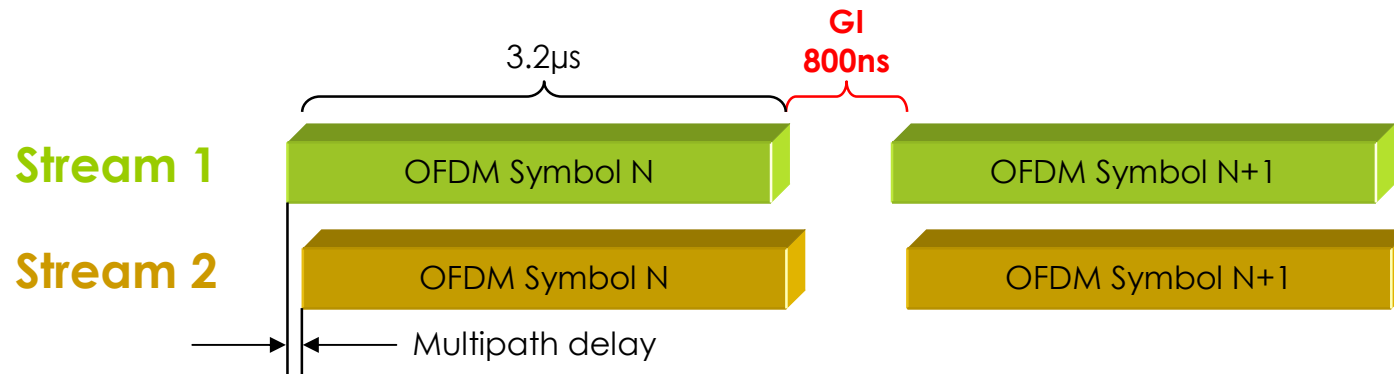
Doubling channel bandwidth from 20 to 40 MHz slightly more than doubles rate from **72.2 to 150 Mbps**

Spatial Multiplexing

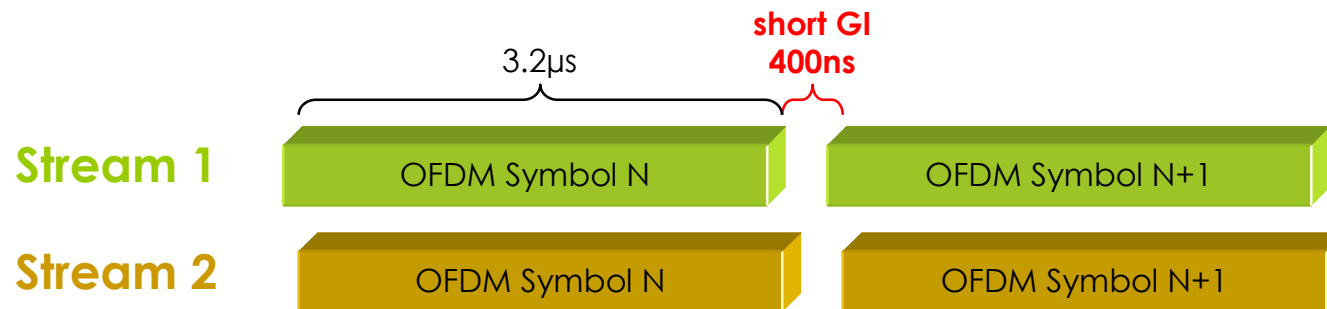
Support of up to four spatial streams (MIMO) increases throughput up to 4 times **150 to 600 Mbps**

Short Guard Interval (GI)

🐙 OFDM carries the bits in so called symbols, the gap between the symbols is the Guard Interval.



🐙 Short Guard Interval can be used, if the multipath delay is low and symbols from streams do not interfere.



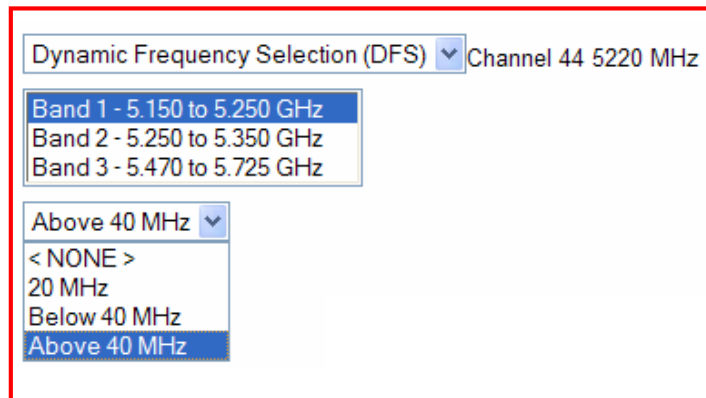
Channel Bonding

 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



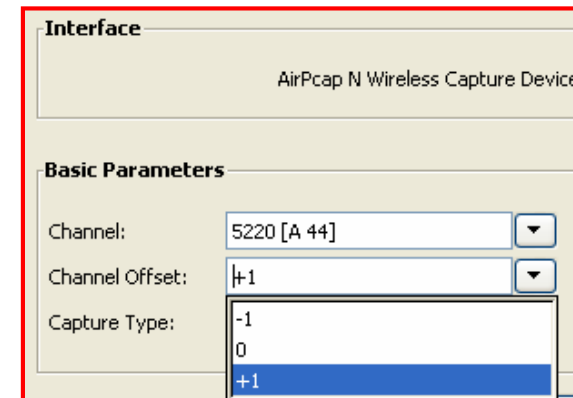
Dynamic Frequency Selection (DFS) Channel 44 5220 MHz

- 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

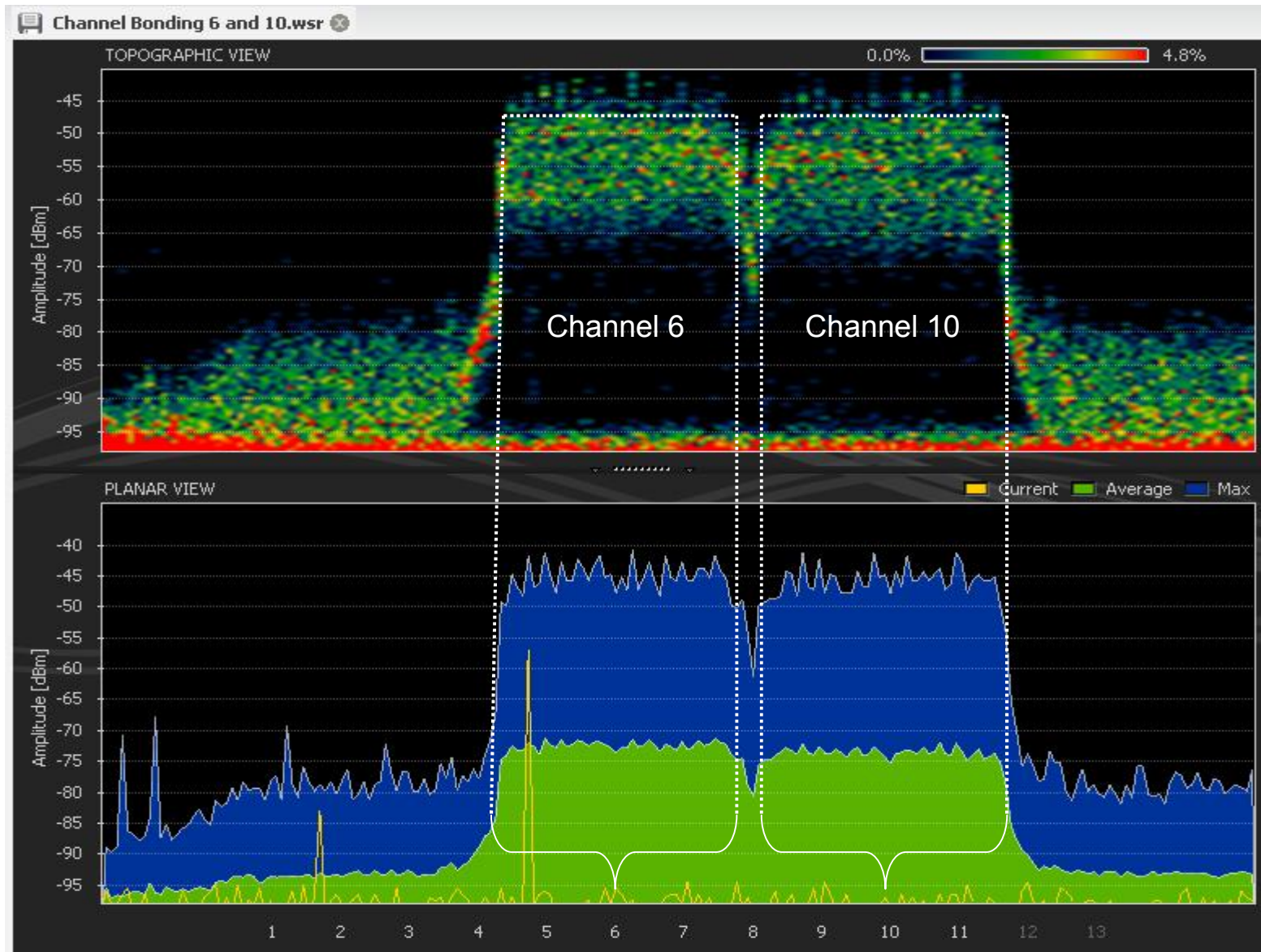
Channel: 5220 [A 44]

Channel Offset: +1

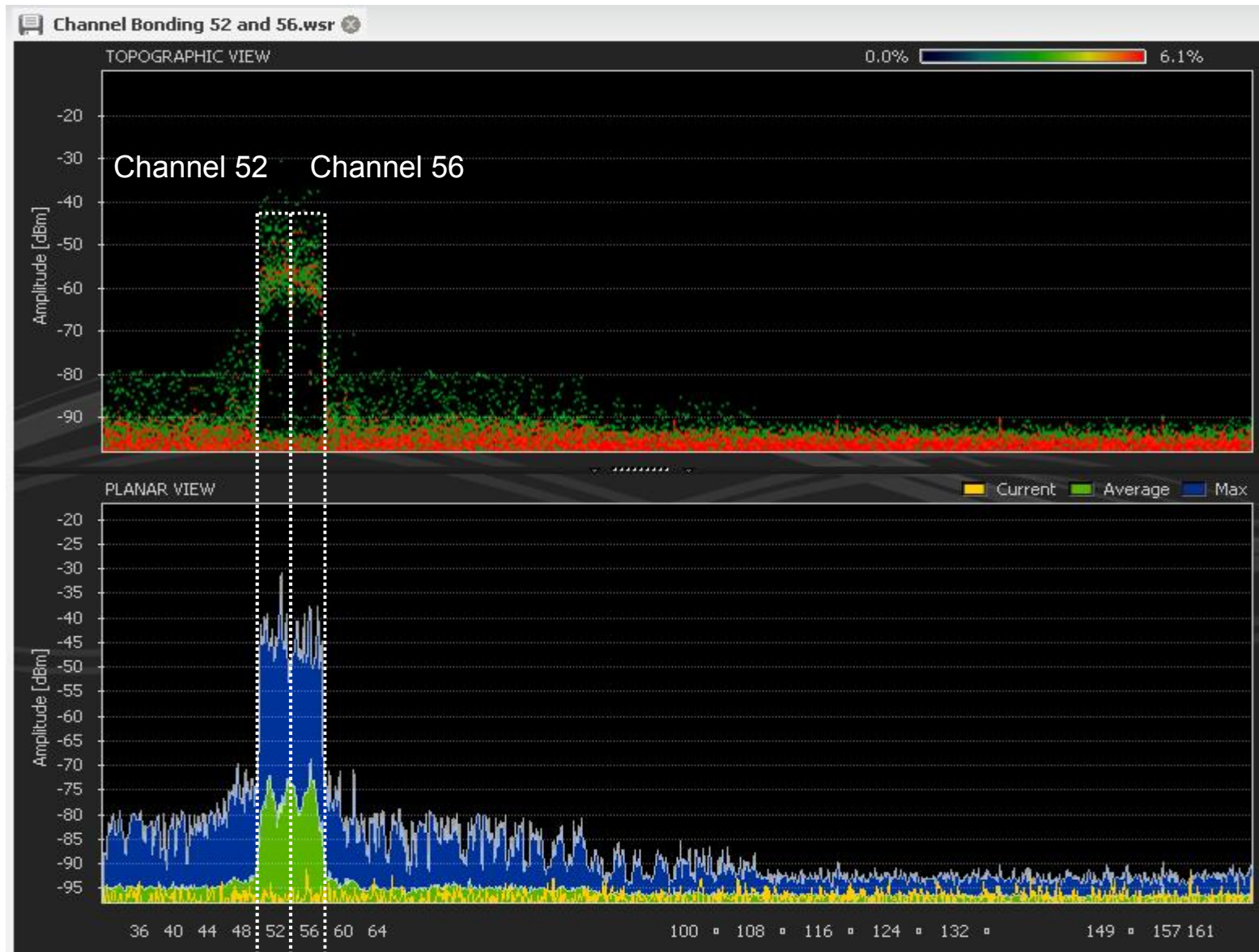
Capture Type: -1, 0, +1

Configuration on AirPcap N

Channel Bonding 2.4 GHz Band



Channel Bonding 5 GHz Band



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 supports Multi-Streaming Modulation

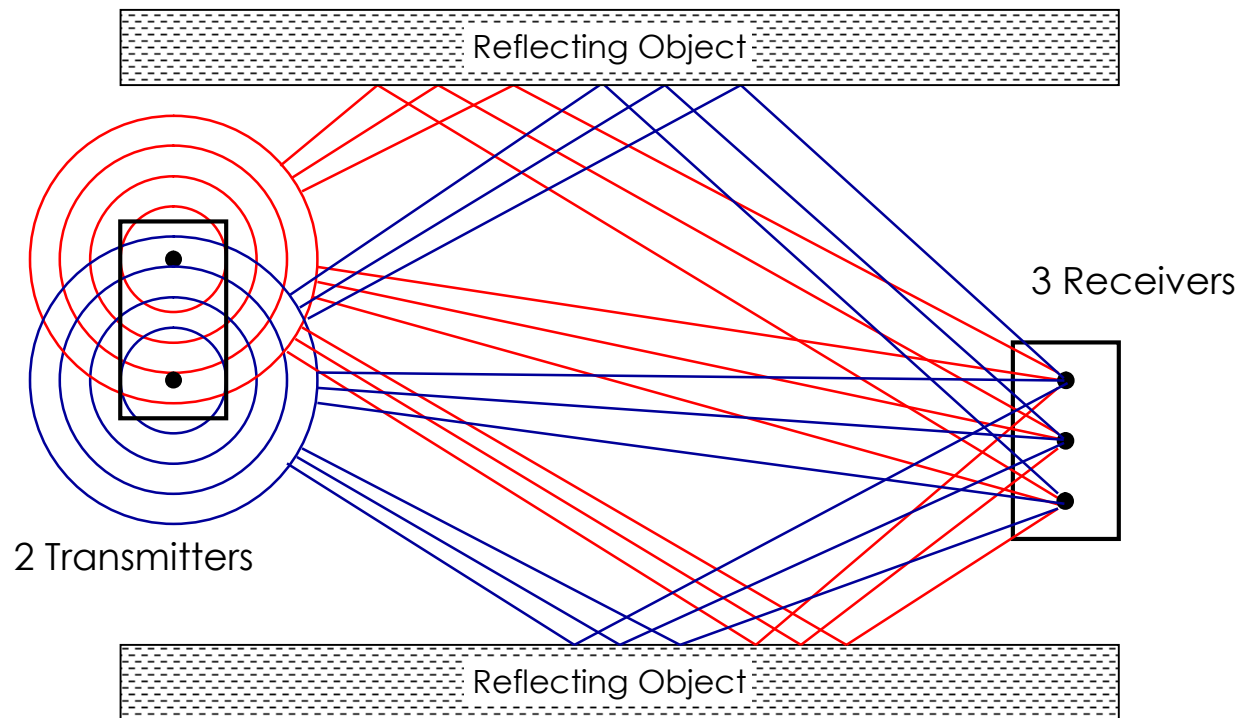
MIMO is the most difficult aspect of 802.11n to understand.

In MIMO, the transmitting and receiving stations each have **multiple RF chains** with multiple antennas. The 802.11n standard mandates at least two and up to four spatial streams.

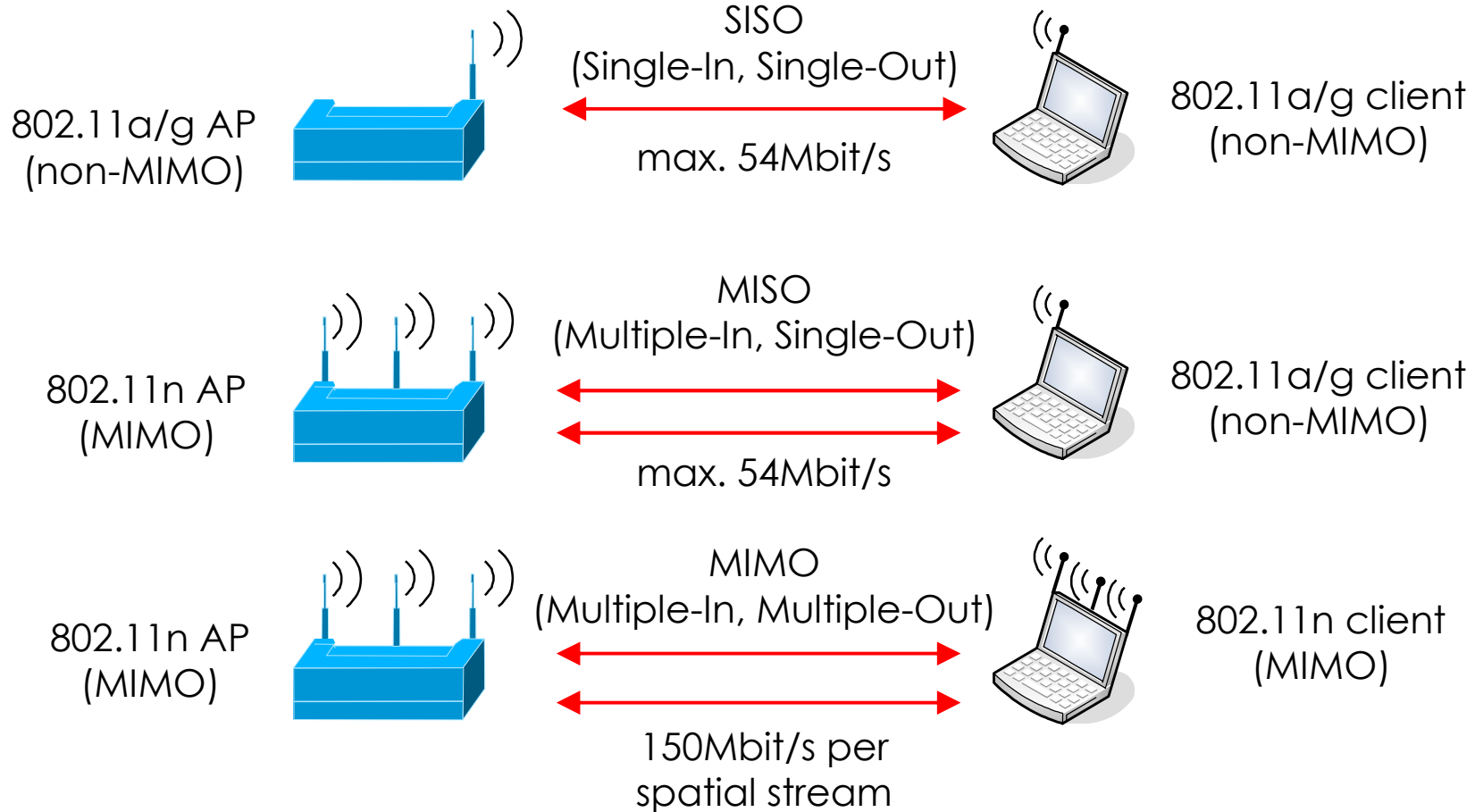
Multipath (RF signal reflection between transmitter and receiver) is normally the enemy of performance, but with MIMO it is used **constructively**.

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.



MIMO Combinations



Modulation Coding Scheme (MCS)

 802.11n introduces a new MCS

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**

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.						
	Mbps	6.5	13	19.5	26	13	26	39	52								
	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
	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
	MCS Rate	4	5	6	7	12	13	14	15	4	5	6	7	12	13	14	15

How to analyze 802.11n



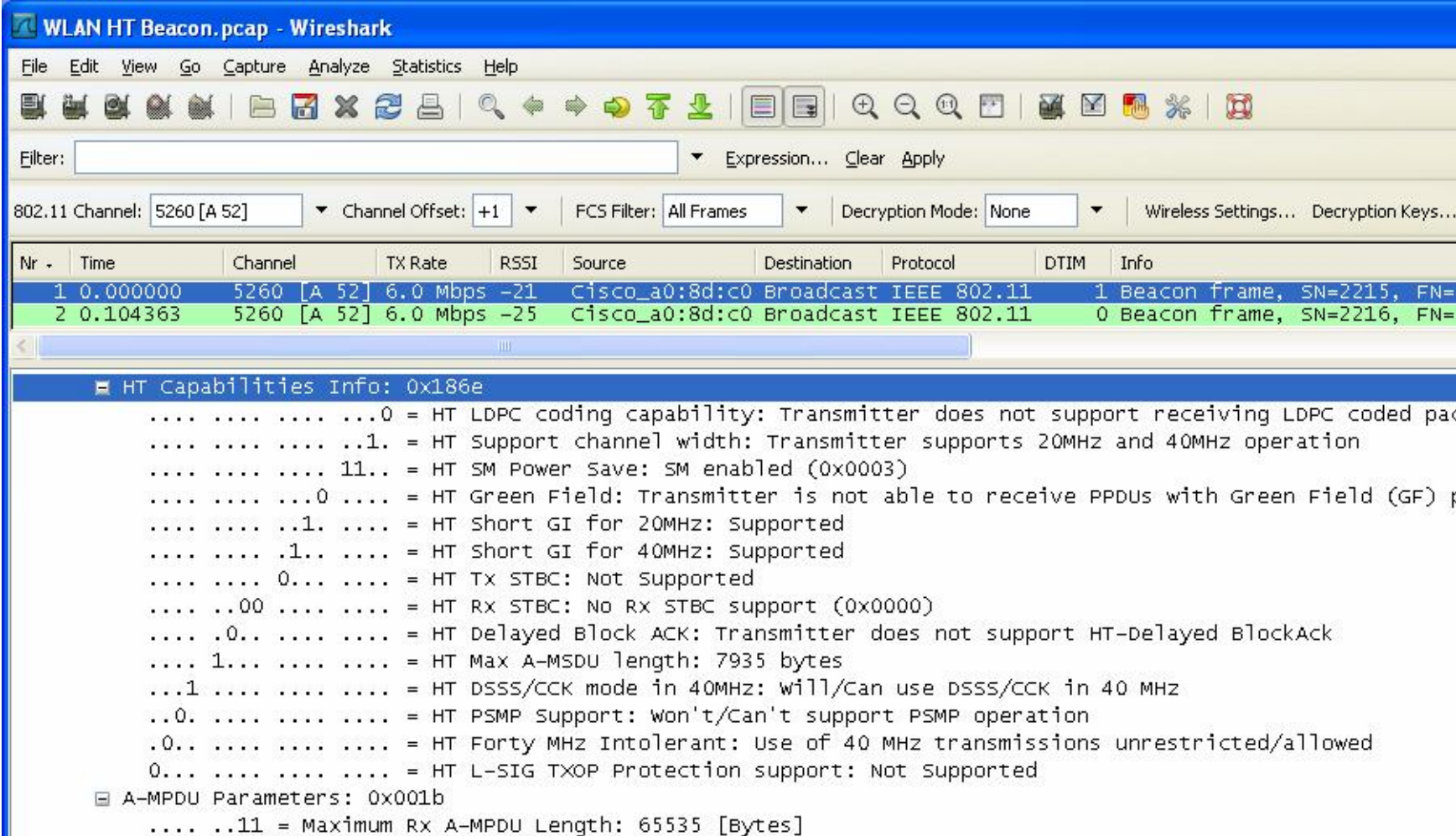
802.11a/b/g/n USB wireless Adapter with two external antennas

802.11 Channel: 5260 [A 52] Channel Offset: +1 FCS Filter: All Frames Decryption Mode: None

Nr	Time	Channel	TX Rate	RSSI	Source	Destination	Protocol	DTIM	Info
1	0.000000	5260 [A 52]	6.0 Mbps	-21	Cisco_a0:8d:c0	Broadcast	IEEE 802.11	0	Beacon frame, ST...
2	0.104528	5260 [A 52]	6.0 Mbps	-14	Cisco_a0:8d:c0	Broadcast	IEEE 802.11	1	Beacon frame, ST...

Description	IP	Packets	Packets/s	Stop
Adapter for generic dialup and VPN capture	unknown	0	0	Start Options Details
AirPcap USB wireless capture adapter nr. 00	unknown	1209	9	Start Options Details
Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler)	192.168.0.202	49	0	Start Options Details

HT Capability Announcement in Beacons



WLAN HT Beacon.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

802.11 Channel: 5260 [A 52] Channel Offset: +1 FCS Filter: All Frames Decryption Mode: None Wireless Settings... Decryption Keys...

Nr	Time	Channel	TX Rate	RSSI	Source	Destination	Protocol	DTIM	Info
1	0.000000	5260 [A 52]	6.0 Mbps	-21	Cisco_a0:8d:c0	Broadcast	IEEE 802.11	1	Beacon frame, SN=2215, FN=
2	0.104363	5260 [A 52]	6.0 Mbps	-25	Cisco_a0:8d:c0	Broadcast	IEEE 802.11	0	Beacon frame, SN=2216, FN=

HT Capabilities Info: 0x186e

-0 = HT LDPC coding capability: Transmitter does not support receiving LDPC coded packets
-1. = HT Support channel width: Transmitter supports 20MHz and 40MHz operation
-11.. = HT SM Power save: SM enabled (0x0003)
-0 = HT Green Field: Transmitter is not able to receive PPDUs with Green Field (GF) protection
-1. = HT short GI for 20MHz: Supported
-1.. = HT short GI for 40MHz: Supported
-0... = HT Tx STBC: Not Supported
-00 = HT Rx STBC: No Rx STBC support (0x0000)
-0.. = HT Delayed Block ACK: Transmitter does not support HT-Delayed BlockAck
- 1... = HT Max A-MSDU length: 7935 bytes
-1 = HT DSSS/CCK mode in 40MHz: will/Can use DSSS/CCK in 40 MHz
-0. = HT PSMP Support: won't/Can't support PSMP operation
-0.. = HT Forty MHz Intolerant: Use of 40 MHz transmissions unrestricted/allowed
- 0... = HT L-SIG TXOP Protection support: Not Supported

A-MPDU Parameters: 0x001b

-11 = Maximum Rx A-MPDU Length: 65535 [Bytes]

MAC layer improvements

Frame Aggregation Mechanisms

Aggregate-MAC Service Data Unit (**A-MSDU**) wraps multiple Ethernet frames in a 802.11 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

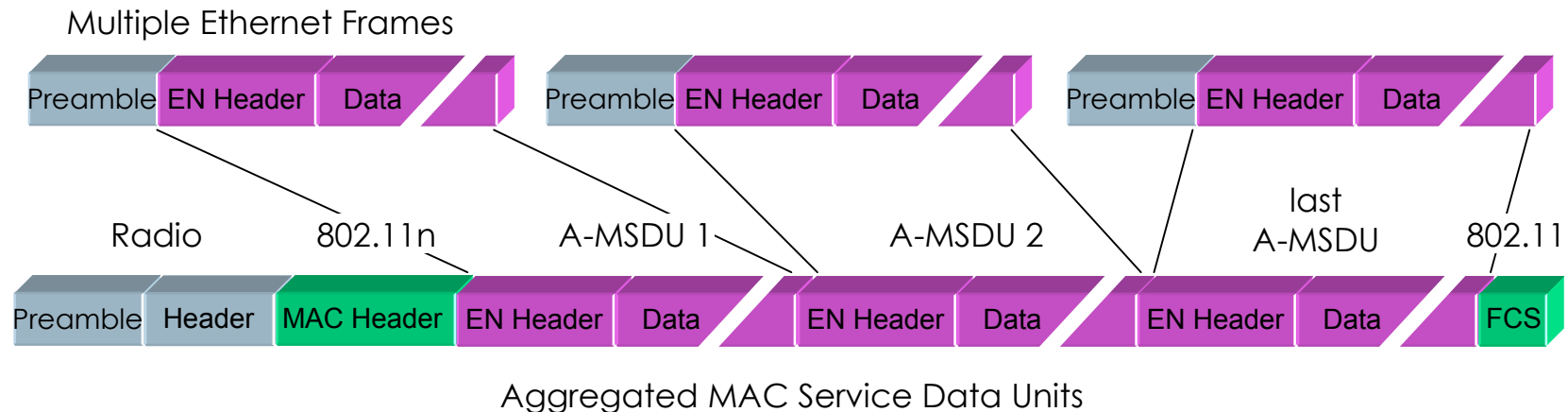
Block ACK effectively eliminates the need to initiate a new transfer for every MPDU

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

D05-1_AMSDU.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
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=.....

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:

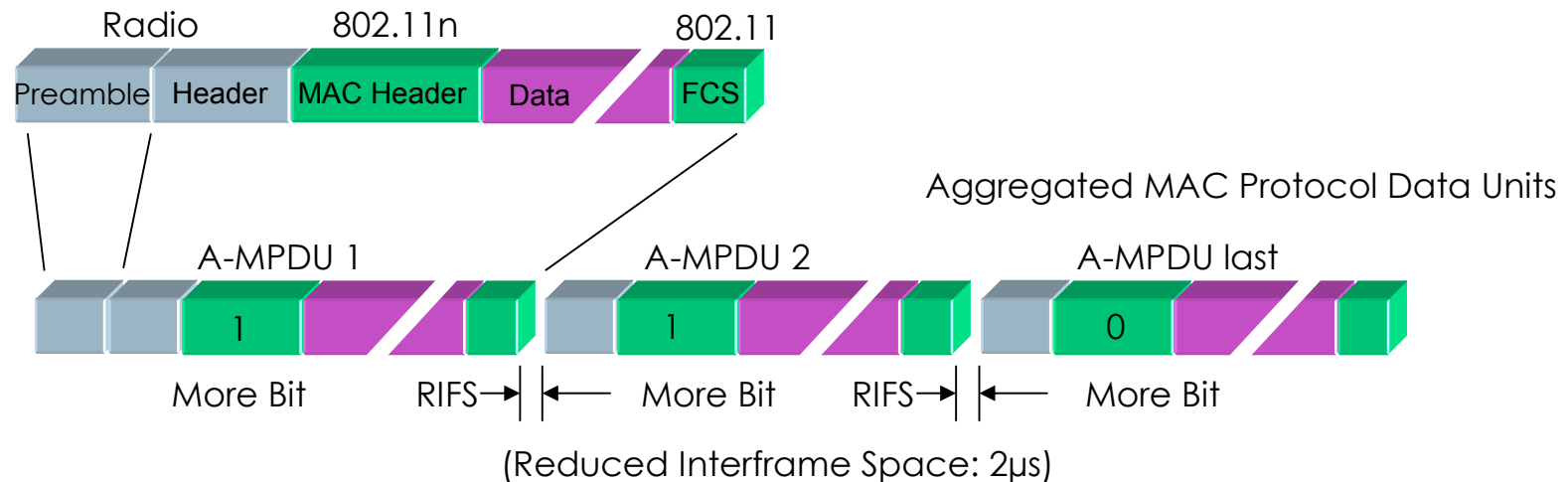
- Wireshark Version 0.99.8 (SVN Rev 24492)
- Cisco AIR-AP1252AG-E-K9; S/W 12.4(10b)JA
- Buffalo WLI-CG-AG300N; Driver 3.0.0.13

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




The screenshot shows a Wireshark capture of an A-MPDU analysis. The main pane displays a list of frames with the following data:

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 802.11	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 802.11	Block Ack, Flags=...

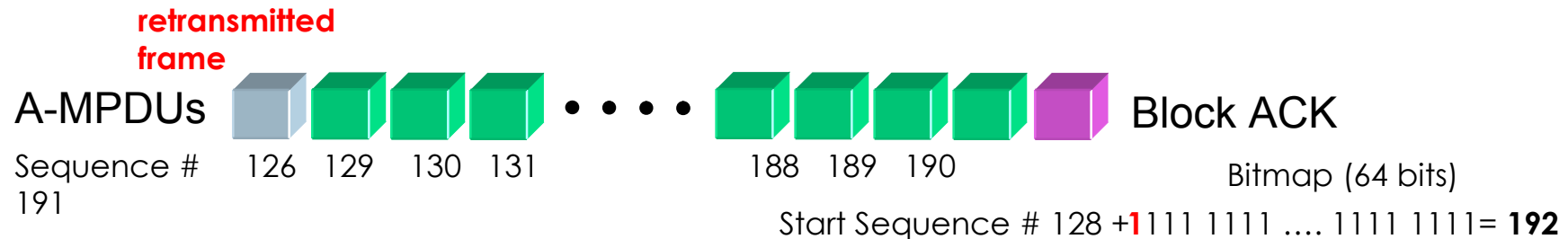
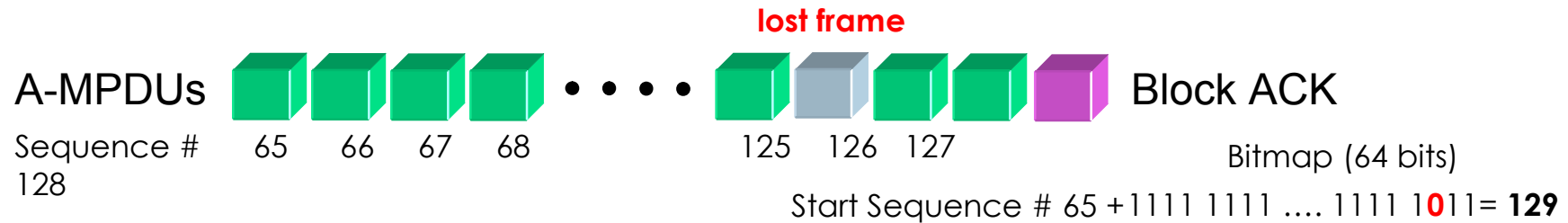
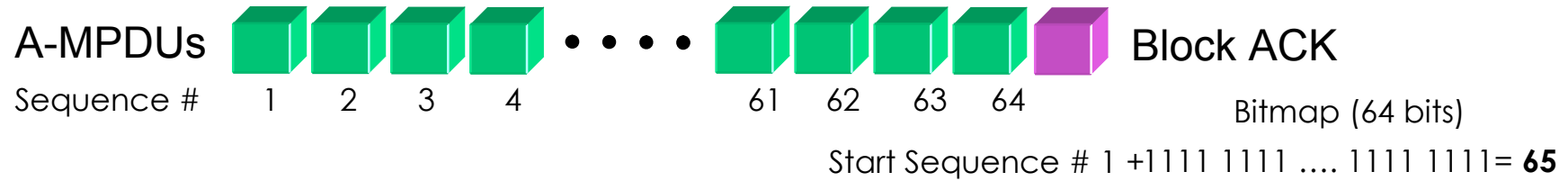
The packet details pane for frame 75 shows the following structure:

- 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-Acknowledge 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)

Block-Ack Mechanism (cont.)



Block-ACK Bitmap Analysis

Wireshark capture showing an IEEE 802.11 Block Ack frame (No. 4588). The packet details pane highlights the Block Ack Bitmap field.

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=...

Packet Details for 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]

```

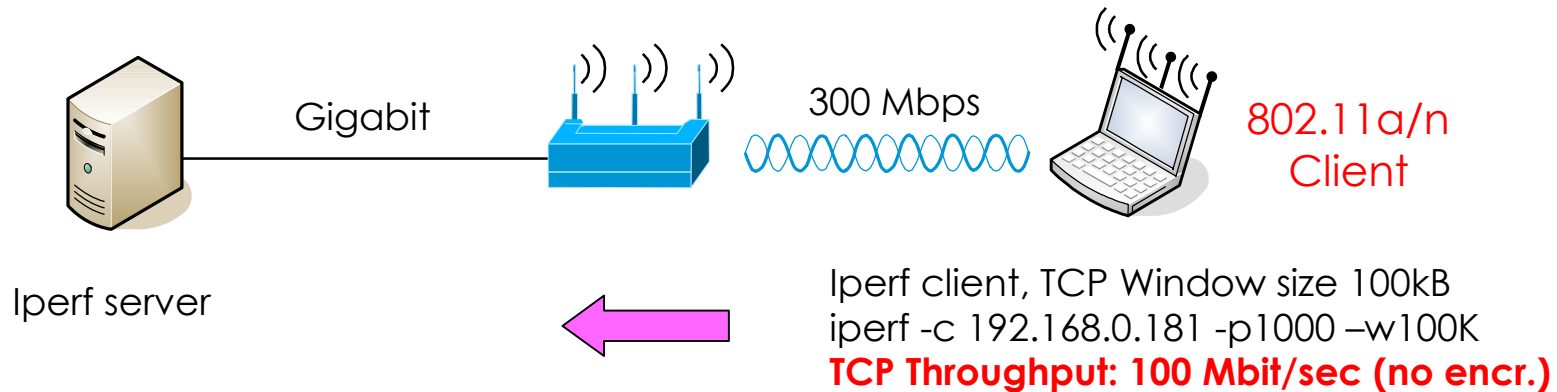
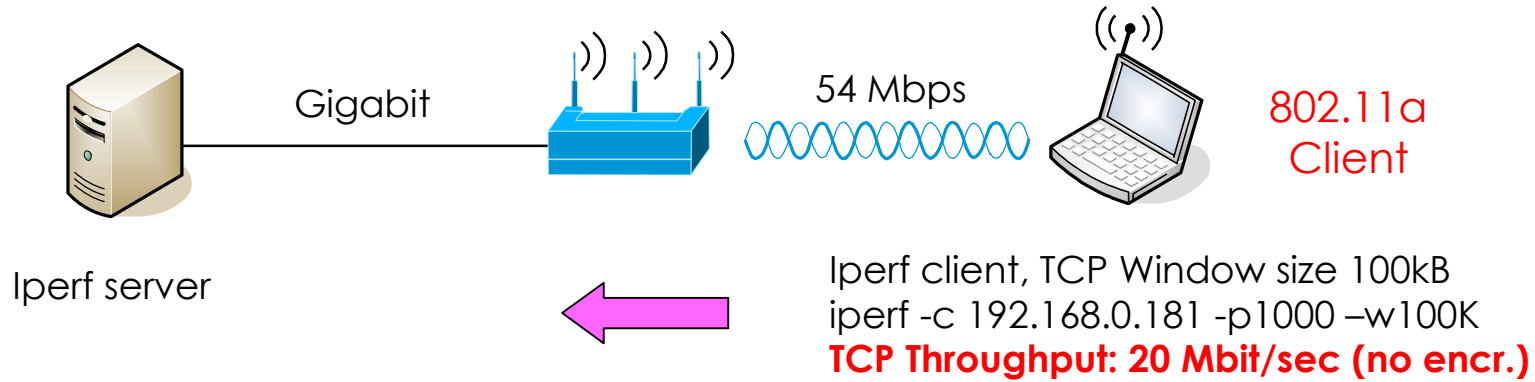
0000  00 00 20 00 69 00 00 00 02 00 14 00 56 f0 08 c6  .. .i... ..V...
0010  01 00 00 00 01 00 6c 00 50 14 40 01 00 00 d1 a0  .....l. P.@....
0020  94 00 00 00 00 17 df a0 8d c0 00 16 01 73 05 af  .....s.....
0030  04 00 d0 56 ff ff ff ff ff ff ff ff f4 7e a4 d2  ...V.....~..
    
```

TCP Throughput Measurements with Iperf

IBM TP T41p Win XP
192.168.0.181

Cisco 1250
AIR-AP1252AG-E-K9

HP2230 Win Vista
INTEL WiFi 5100AGN
192.168.0.204



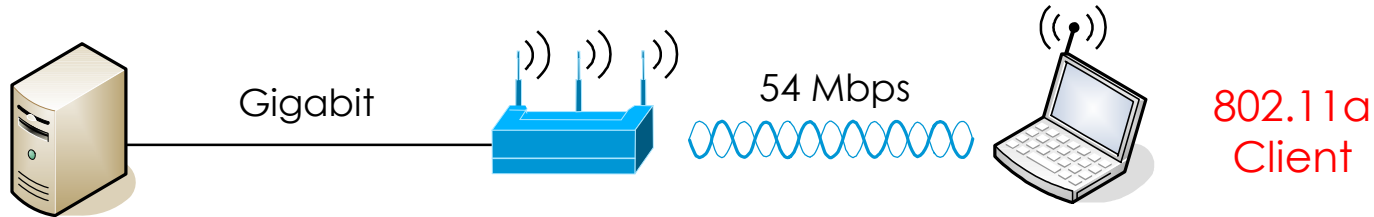
5 - 15% throughput reduction with WPA2 Encryption

TCP Throughput Measurements with Iperf

IBM TP T41p Win XP
192.168.0.181

Cisco 1250
AIR-AP1252AG-E-K9

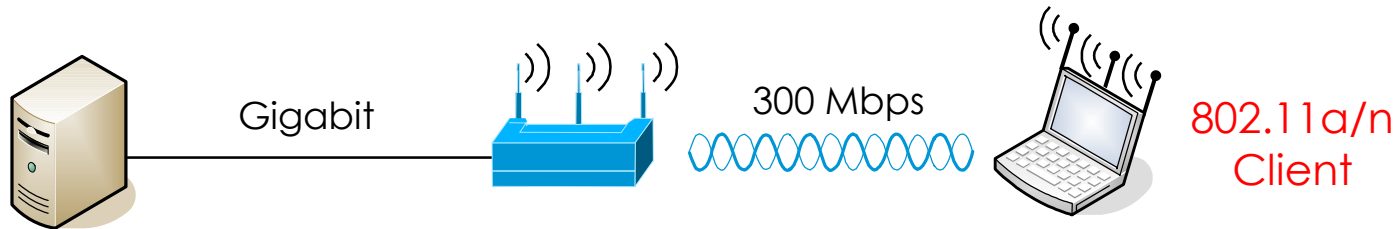
HP2230 Win Vista
INTEL WiFi 5100AGN
192.168.0.204



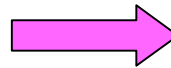
Iperf client, TCP Window size 100kB
iperf -c 192.168.0.204 -p1000 -w100K
Throughput: 21 Mbit/sec (no encr.)



Iperf server



Iperf client, TCP Window size 100kB
iperf -c 192.168.0.204 -p1000 -w100K
Throughput: 120 Mbit/sec (no encr.)



Iperf server

5 - 15% throughput reduction with WPA2 Encryption

Overview WLAN Standards



Mbps	Coding	Modulation	Description	
1 2	Barker Barker	DBPSK	802.11 DSSS (Clause 15) with ,Long Preamble'	<div style="background-color: #FFD700; width: 100%; height: 100%; display: flex; align-items: center; justify-content: center;"> <div style="background-color: #4682B4; width: 100%; height: 100%; display: flex; align-items: center; justify-content: center;"> <div style="background-color: #FFD700; width: 100%; height: 100%; display: flex; align-items: center; justify-content: center;"> 802.11a </div> </div> </div>
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

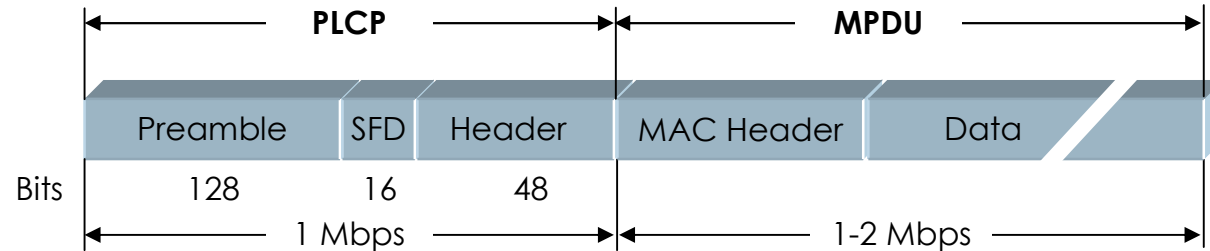
CCK = Complementary Code Keying
 DBPSK = Differential Binary Phase-Shift Keying
 DQPSK = Differential Quadrature Phase-Shift Keying
 OFDM = Orthogonal Frequency Division Multiplexing

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

Overview Frame Types (2.4 GHz)



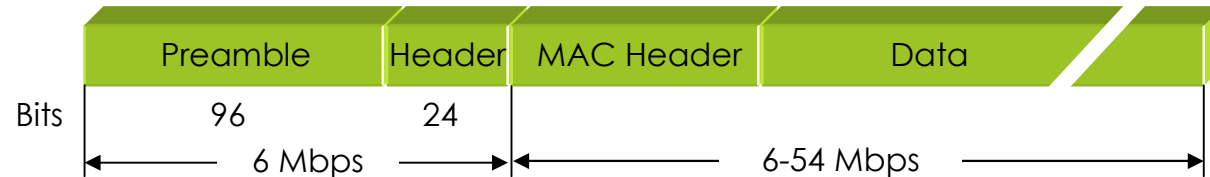
802.11 DSSS with
'Long Preamble'
Barker Code



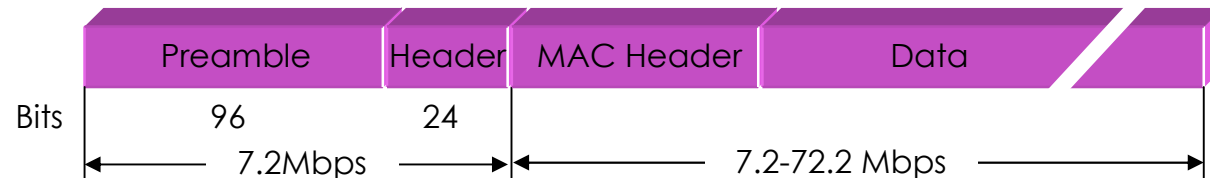
802.11b HR/DSSS with
'Short Preamble'
Barker / CCK



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 (decodiert by Wireshark)

Backwards compatibility to a/b/g

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.)

Access point indicates in 'Beacon' if 'b-only' stations are present

The image shows a Wireshark capture of WLAN traffic. The main pane displays a list of frames. Frame 743 is highlighted, showing a Beacon frame from Cisco_11:1f:60 to Broadcast. The details pane for this frame shows ERP information: Non-ERP STAs, use protection, short or long preambles. The tag number is 42, the tag length is 1, and the tag interpretation is ERP info: 0x3 (Non-ERP STAs, use protection, short or long preambles).

No.	Source	Destination	RSSI	Protocol	Info
742	Cisco_11:1f: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)

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

OFDM stations changes to 'Protected Mode'

The image shows a Wireshark capture of WLAN traffic. The interface is titled 'WLAN Non ERP Present.pcap - Wireshark'. The capture is filtered for 'Valid Frame'. The table below shows the captured packets, with a red box highlighting packet 1150, which is a 'Clear-to-send' frame from PhilipsC_45:7f:2f (RA) to itself.

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

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

Reduced data throughput in mixed environments

	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

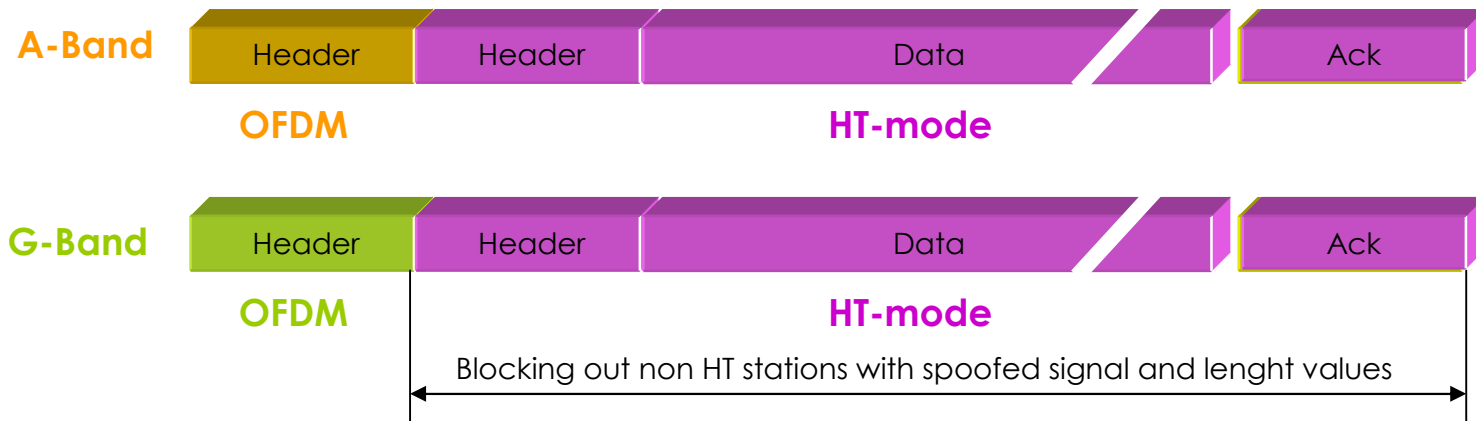
Throughput improvement:

Upgrade of all 802.11b stations to 802.11g

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

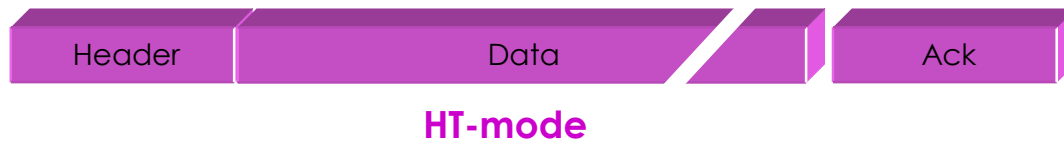
Mixed mode

802.11n to a/g compatibility with Legacy header



Greenfield mode

No backwards compatibility to a/b/g



Future of 802.11n

- 🐳 Standard ratification in January 2010?
- 🐳 The Australian Commonwealth Scientific and Industrial Research Organization (CSIRO) holds OFDM patent and may delay ratification of 802.11n
- 🐳 Interoperability remains a question mark for pre-N products
- 🐳 New products supporting technical features like:
 - Up to four spatial streams
 - Transmit Beam forming
 - Direct Link Setup ... and many more

The End

Thank you for your attention

I would enjoy to meet you
again in one of our trainings

Rolf Leutert
Leutert NetServices
leutert@wireshark.ch
www.wireshark.ch

