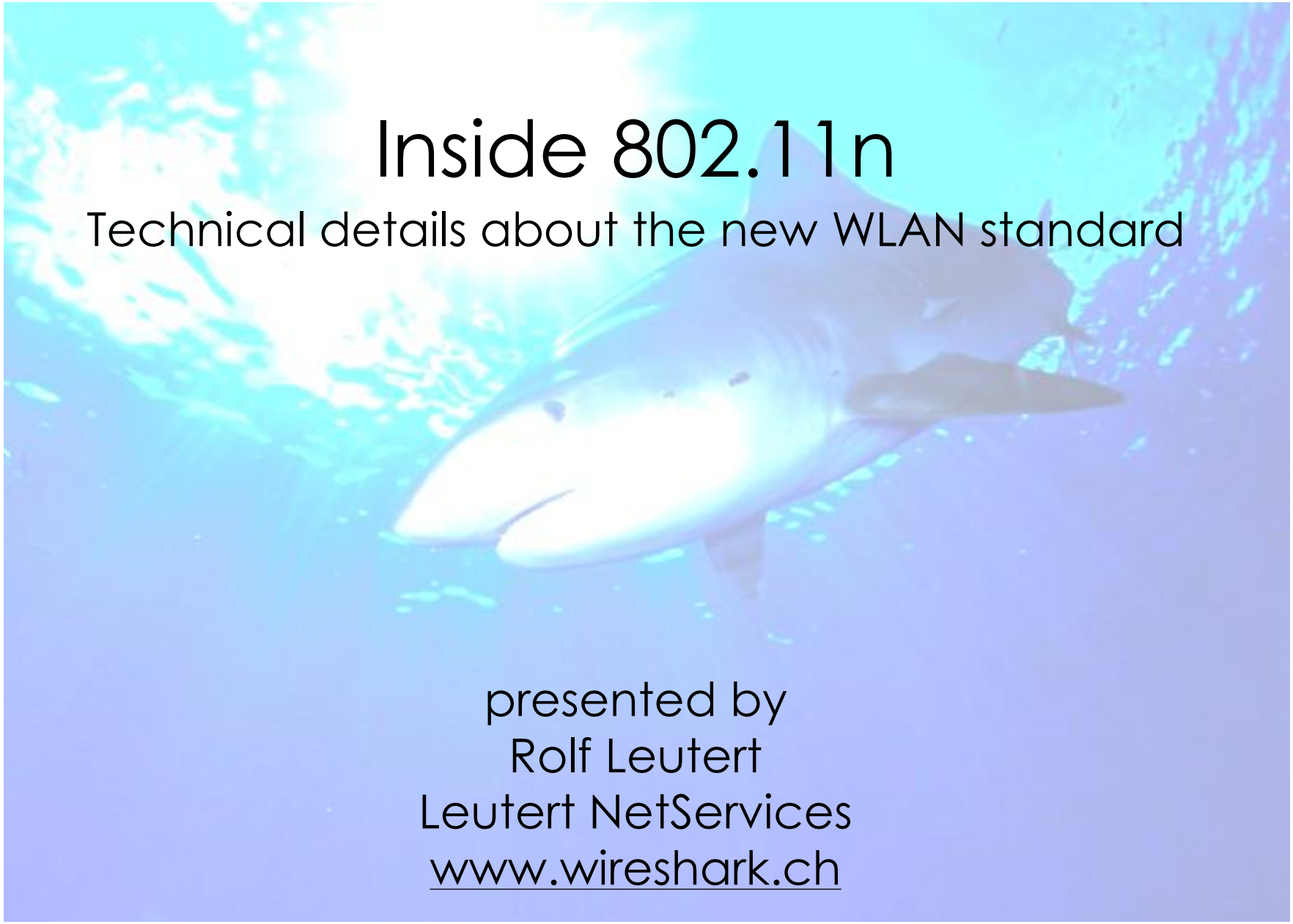


Inside 802.11n

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

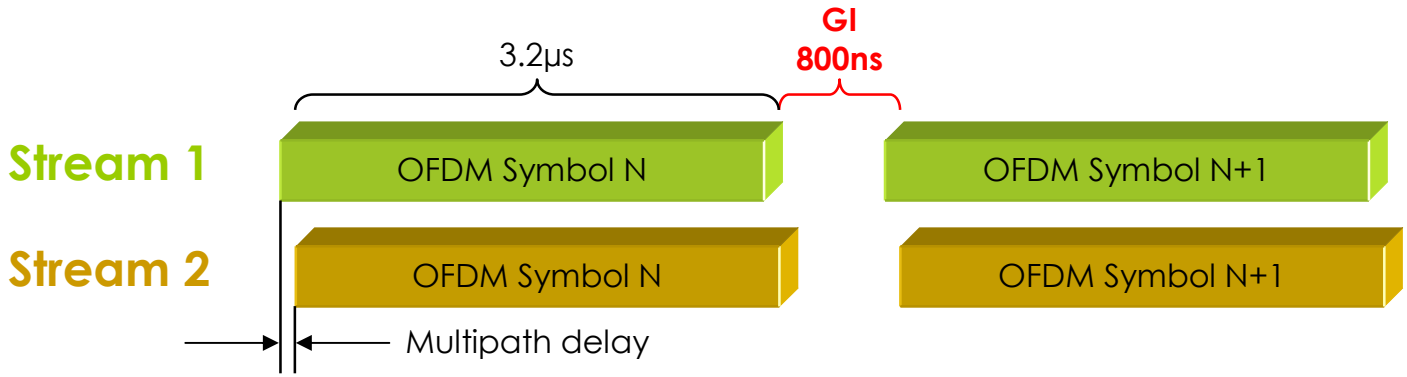
Doubling channel bandwidth from 20 to 40 MHz slightly more than doubles rate from 72.2 to 150 Mbps

Spatial Multiplexing

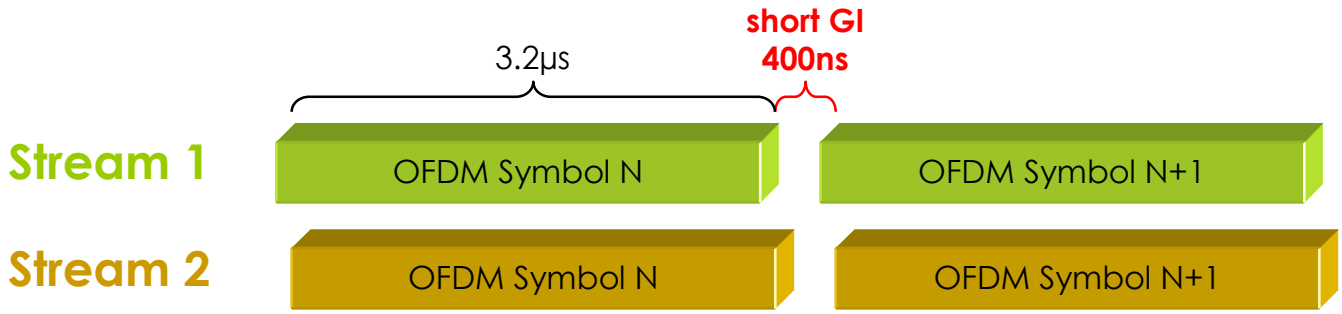
Support of up to four spatial streams (MIMO) increases throughput up to 4 times 150 to 600 Mbps

Short Guard Interval (GI)

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



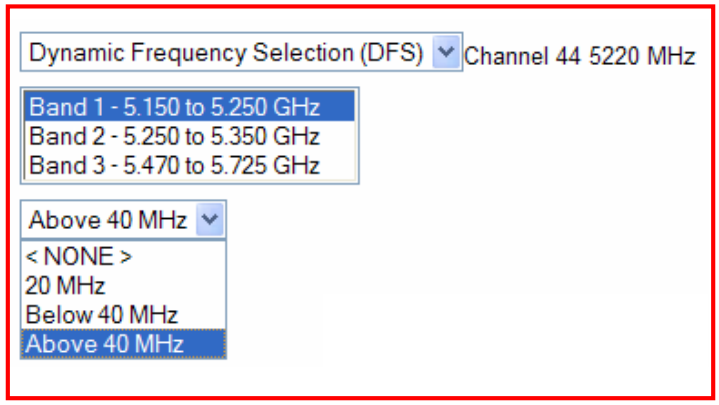
- Short Guard Interval can be used, if the multipath delay is low and symbols from streams do not interfere.



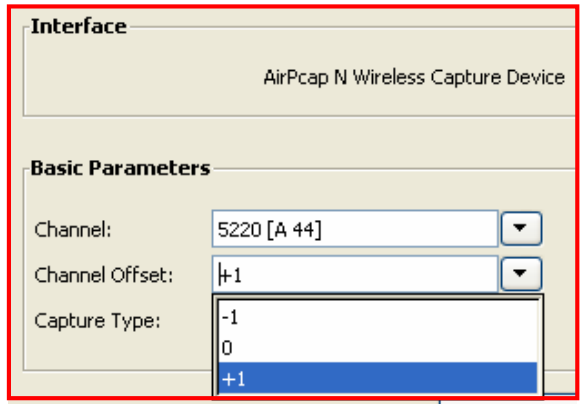
Channel Bonding

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

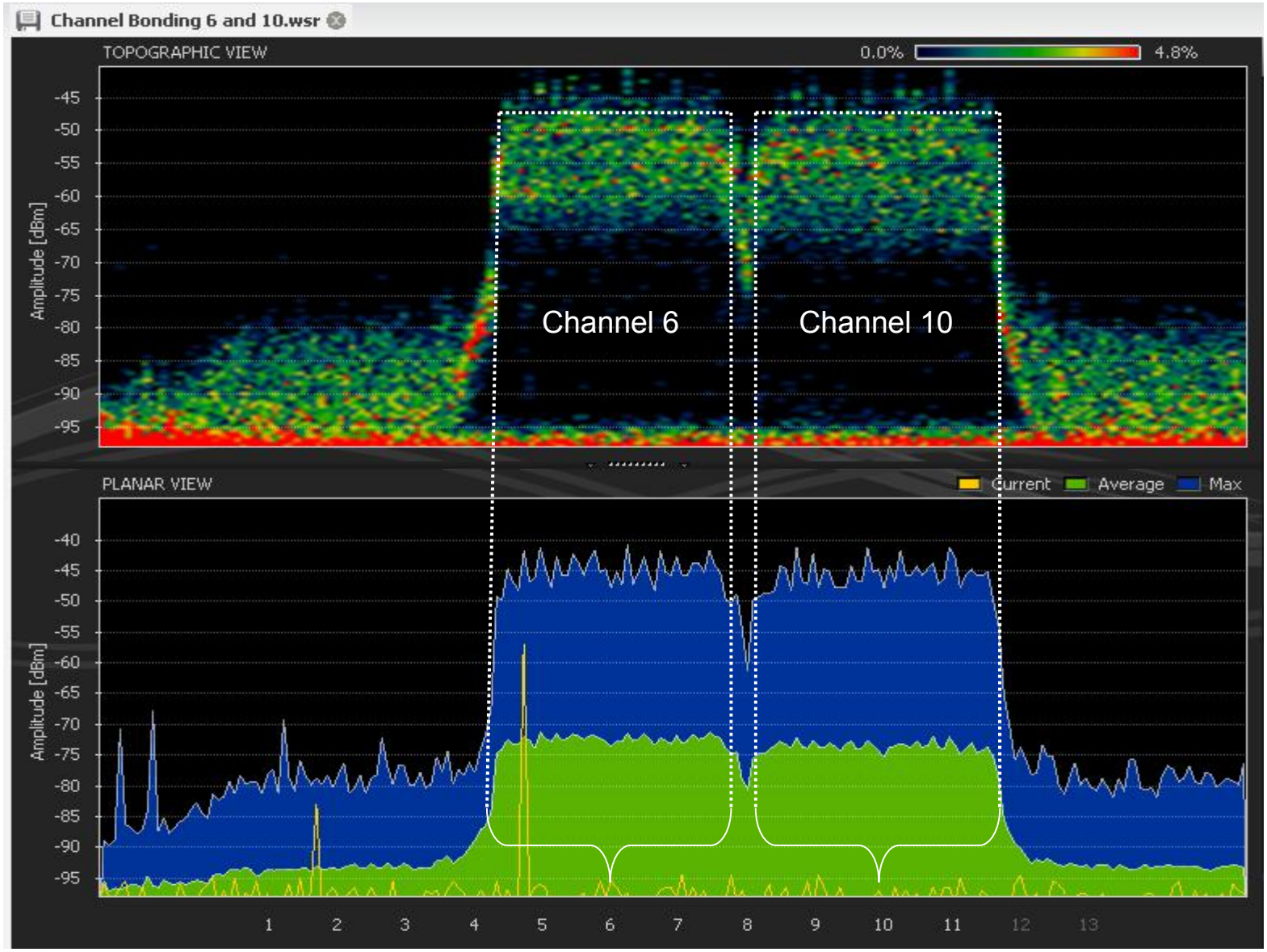


Configuration on Cisco AP1250

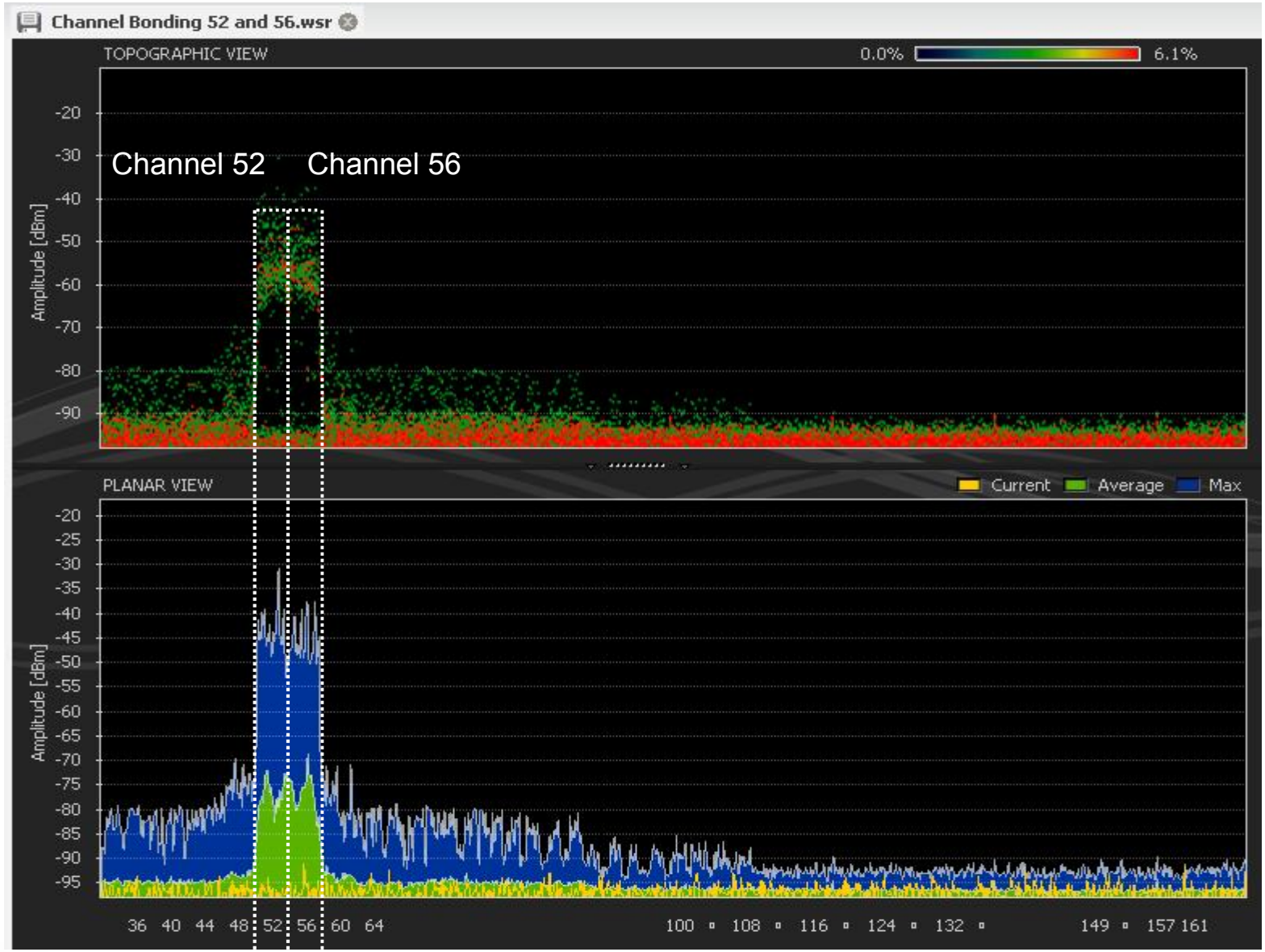


Configuration on AirPcap N

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

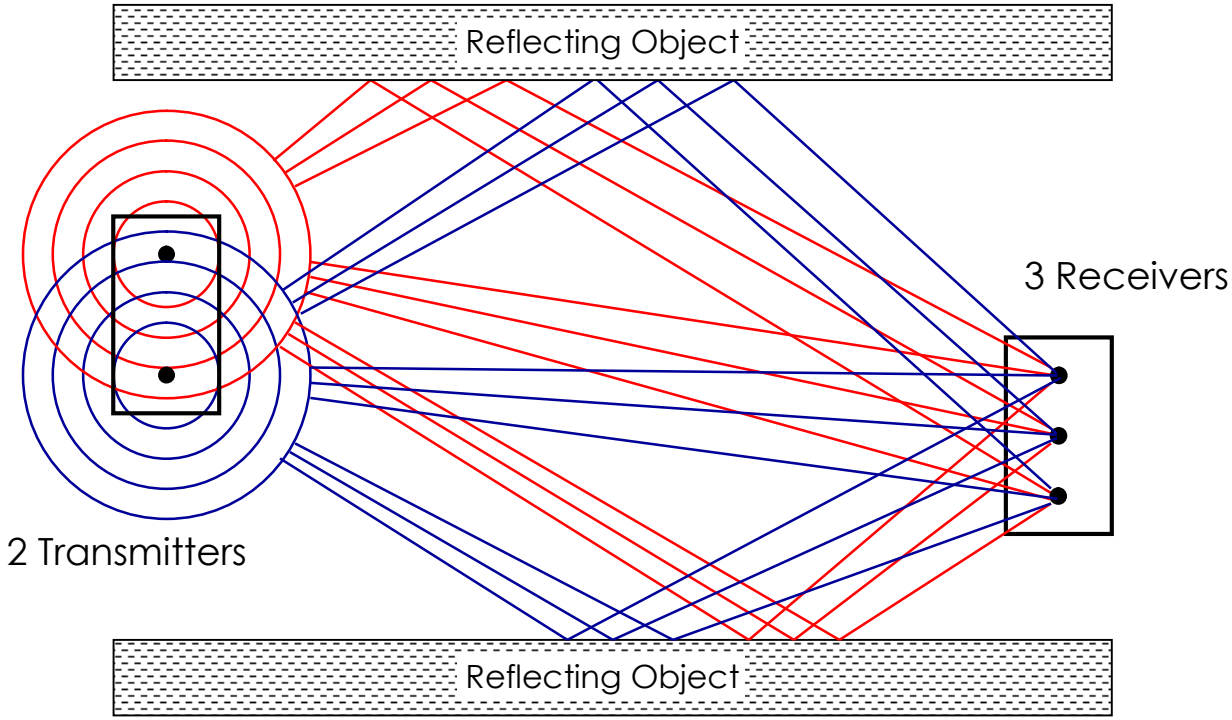
MIMO is the most difficult aspect of 802.11n to understand.

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.

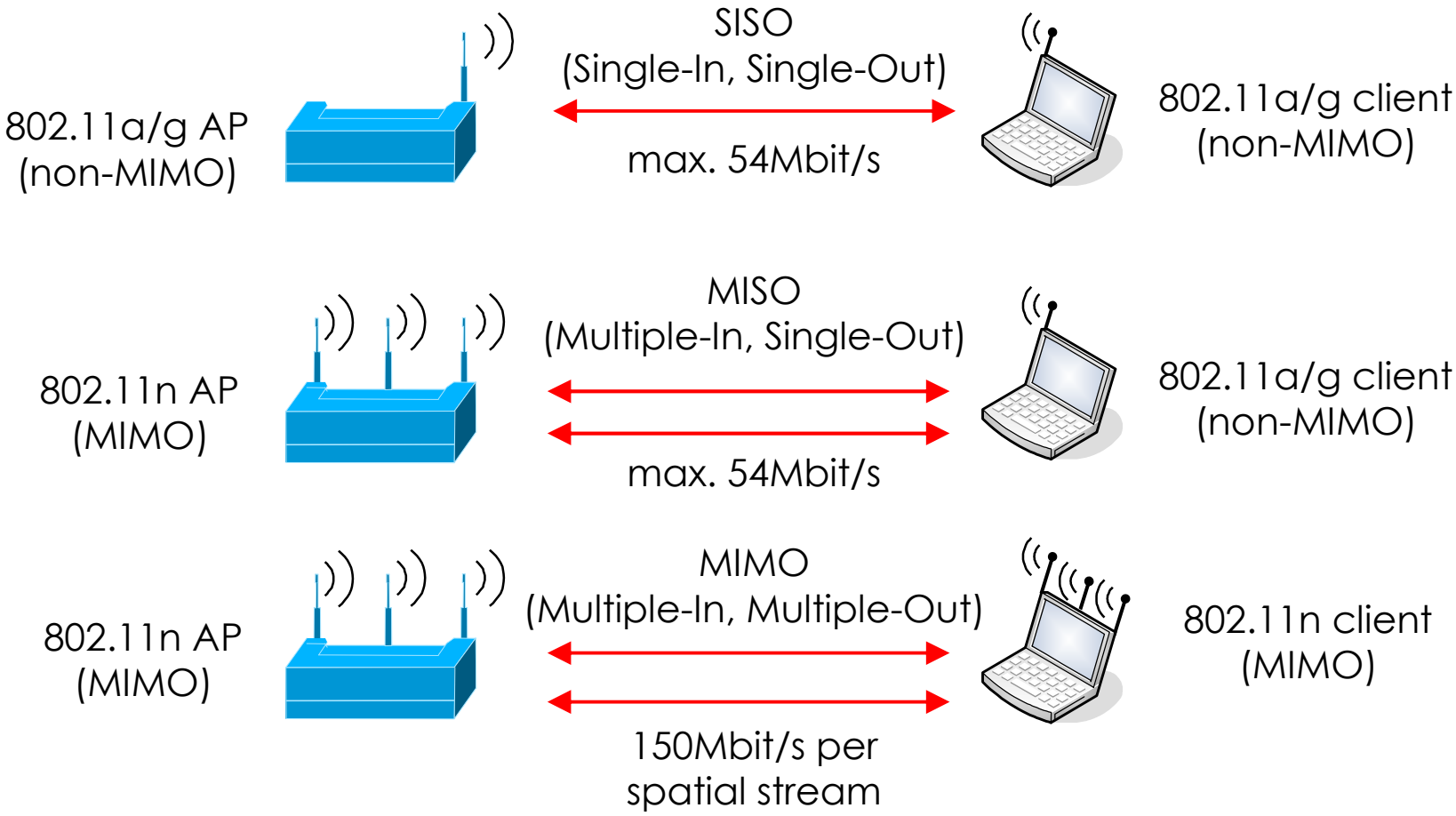
Multipath (RF signal reflection between transmitter and receiver) is normally the enemy of performance, but with MIMO it is used constructively.

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)

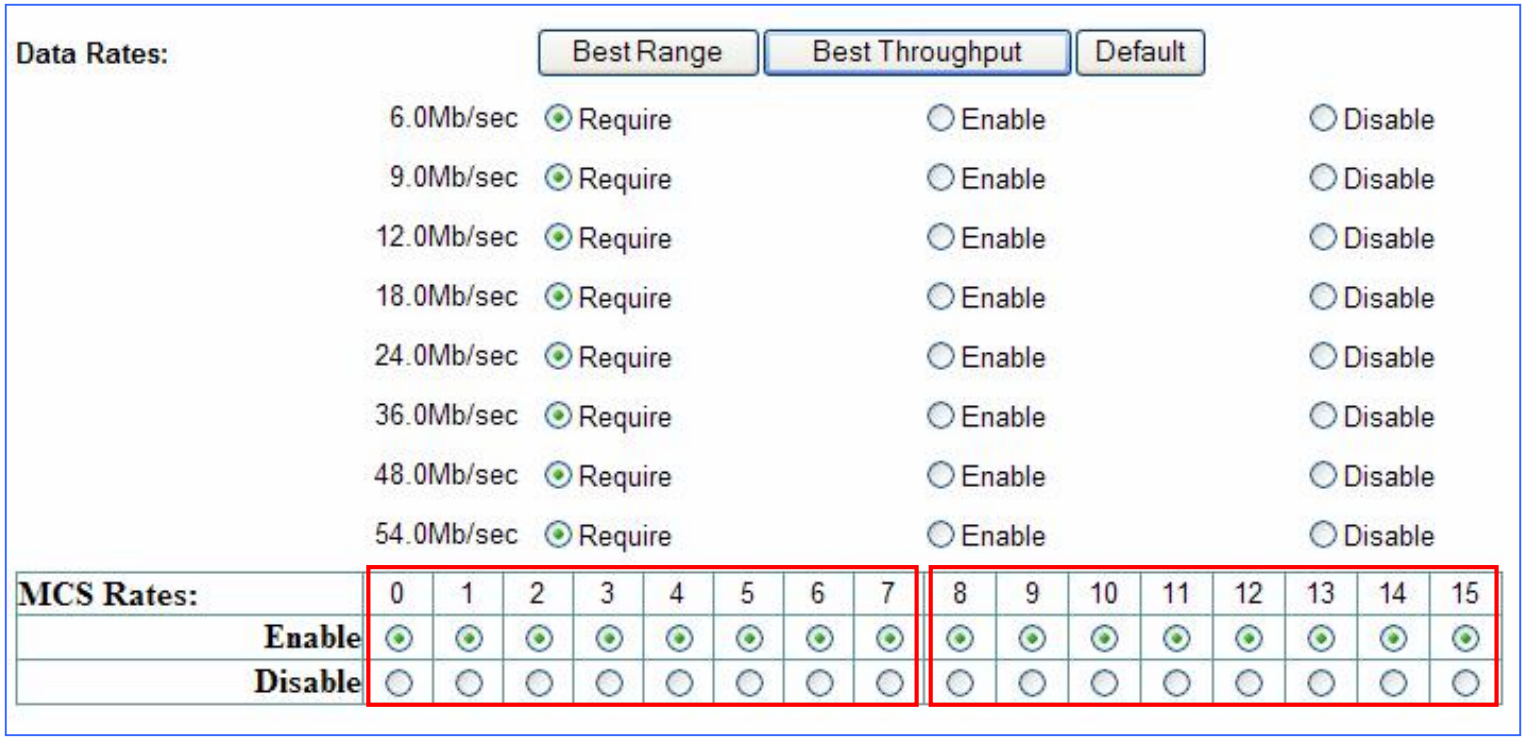
802.11n introduces a new MCS

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



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								
		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

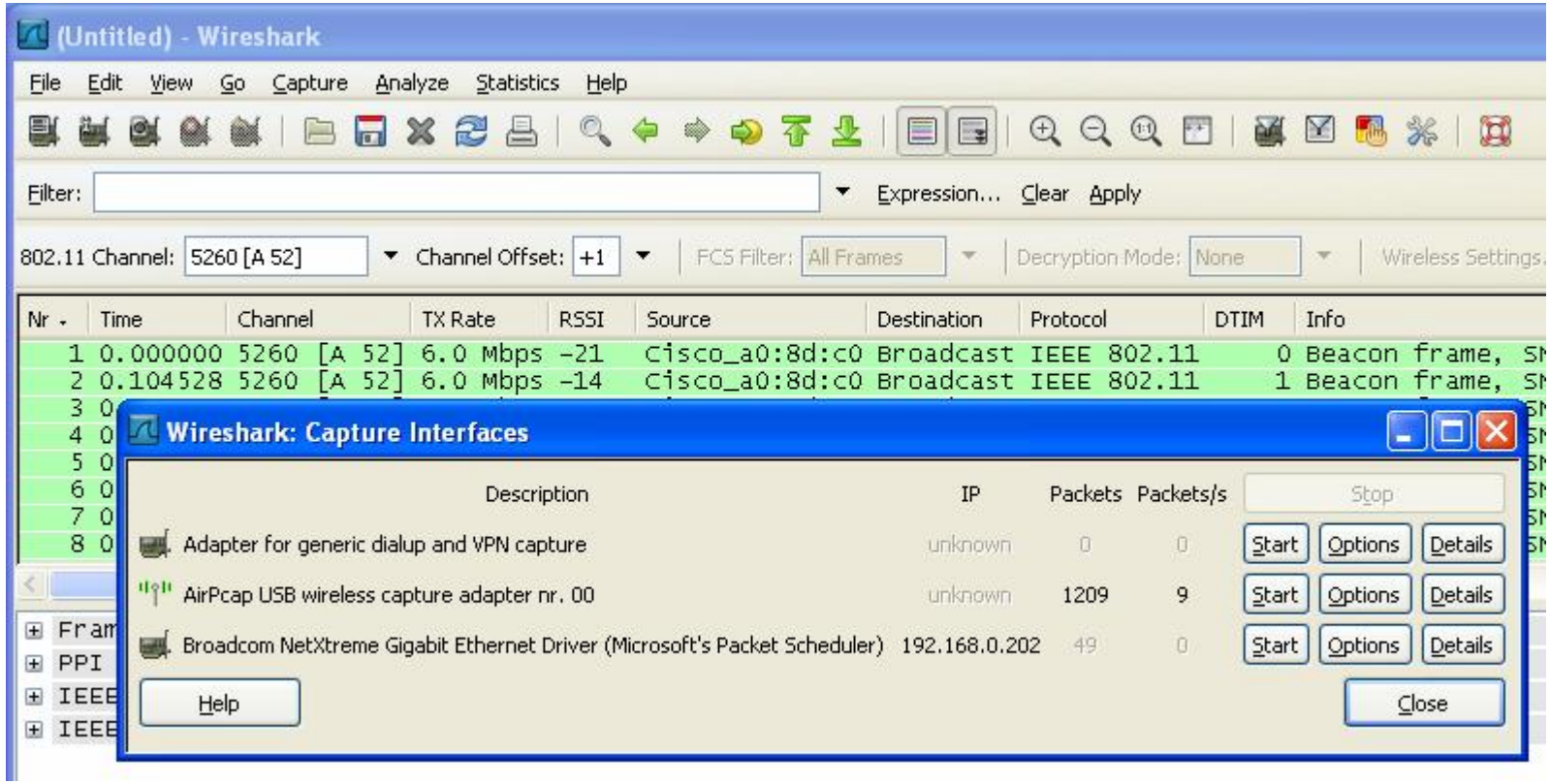
How to analyze 802.11n

CACE TECHNOLOGIES

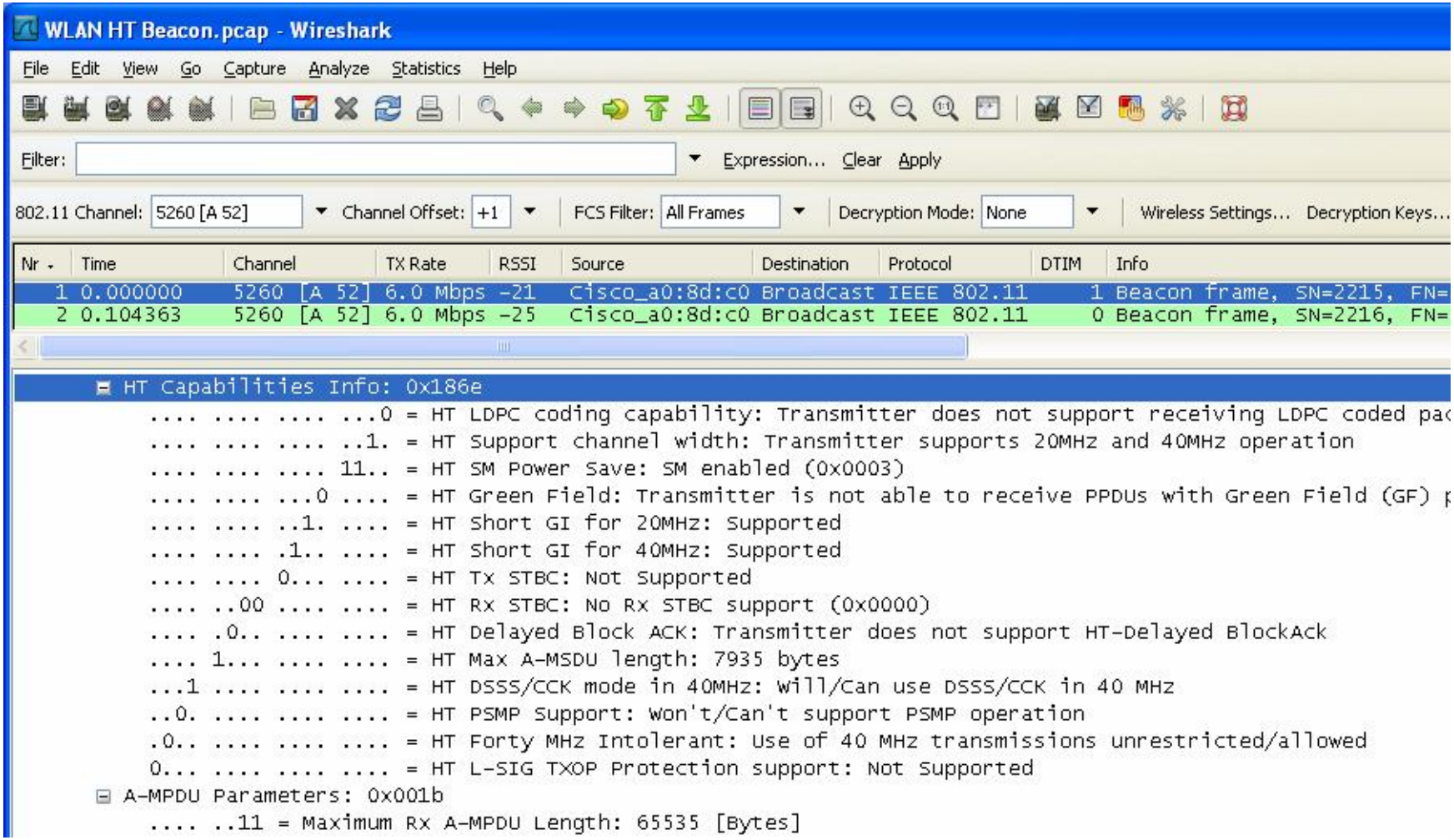
Home of WinPcap and Wireshark

AirPcap Nx

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



HT Capability Announcement in Beacons



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

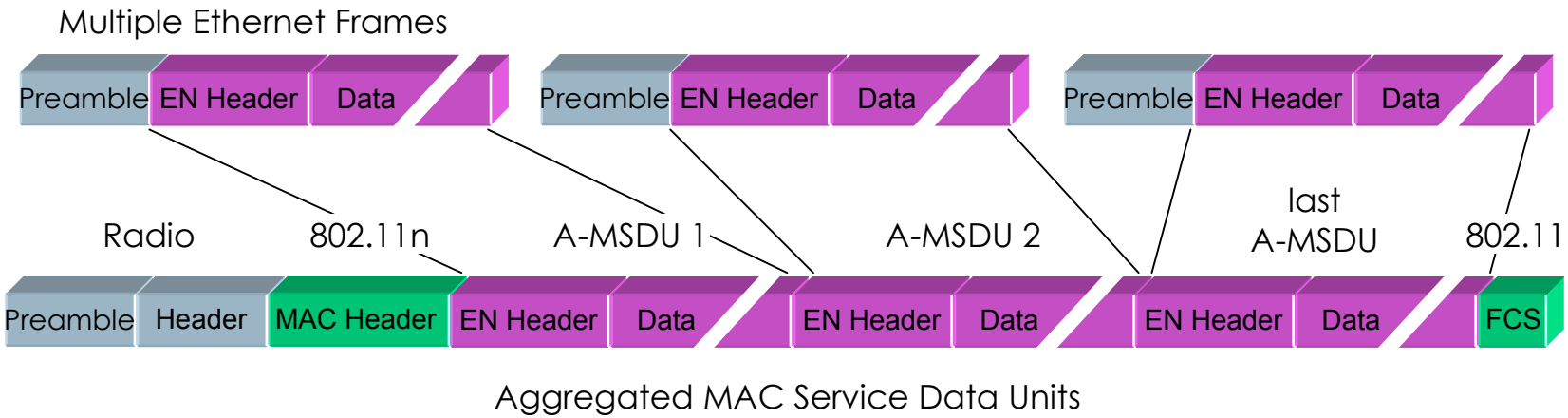
Block ACK effectively eliminates the need to initiate a new transfer for every MPDU

MSDU Aggregation

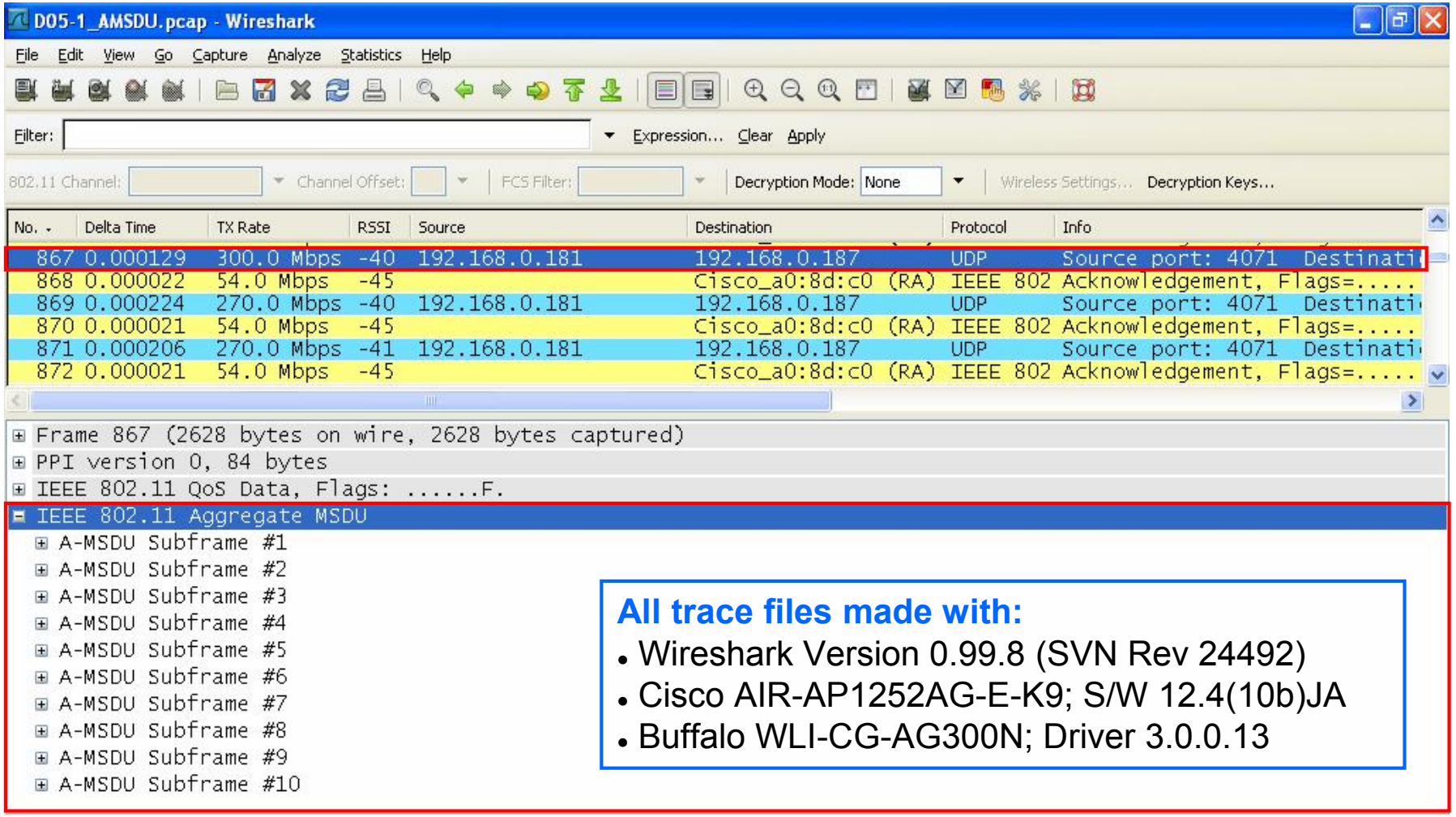
Multiple Ethernet frames for a common destination are wrapped in a single 802.11 frame

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



All trace files made with:

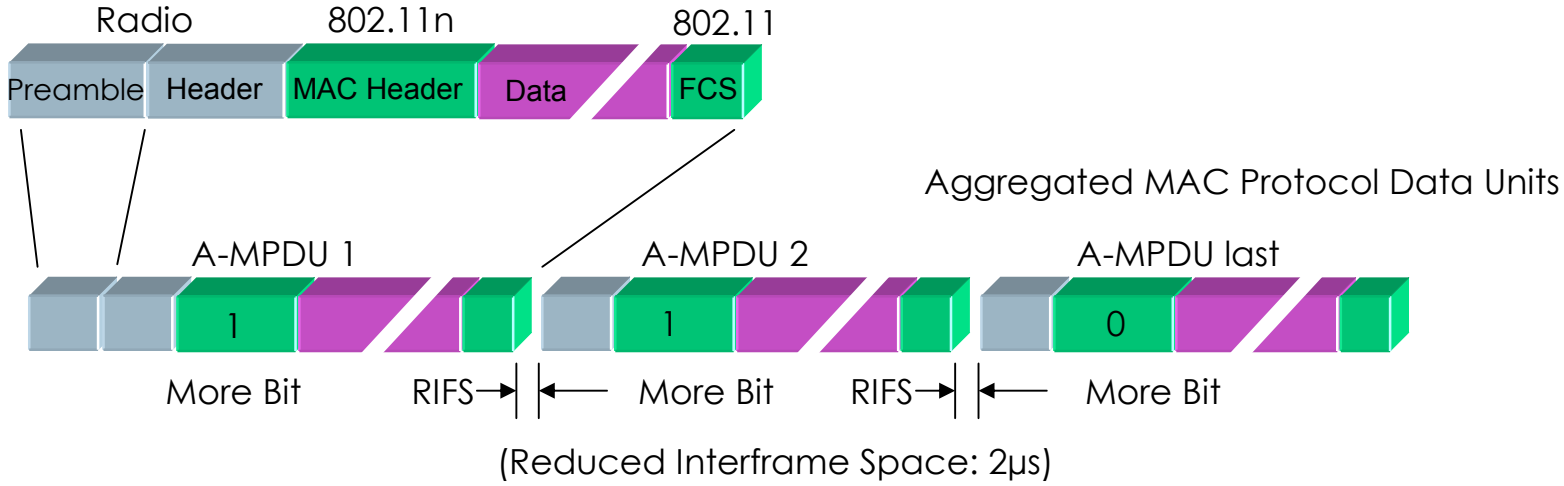
- Wireshark Version 0.99.8 (SVN Rev 24492)
- Cisco AIR-AP1252AG-E-K9; S/W 12.4(10b)JA
- Buffalo WLI-CG-AG300N; Driver 3.0.0.13

MPDU Aggregation

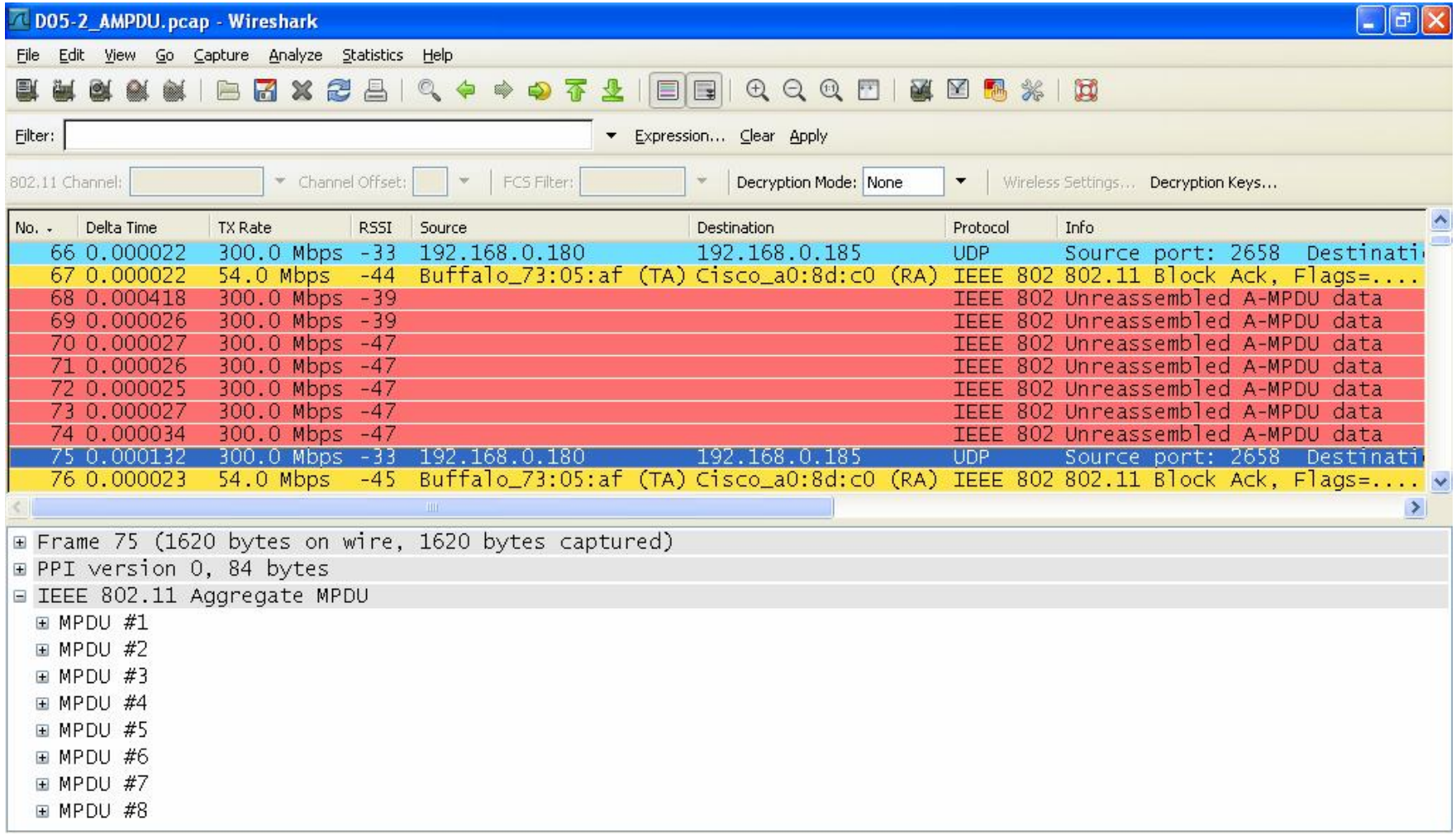
Multiple Ethernet frames for a common destination are translated to 802.11 format and sent as burst

Elements of an A-MPDUs burst can be acknowledged individually with one single Block-Acknowledge

Only not-acknowledged A-MPDUs are retransmitted



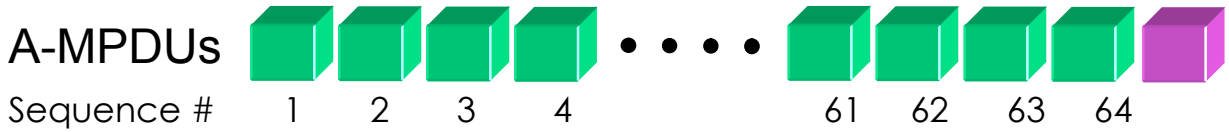
A-MPDU Analysis



Block-Acknowledge Mechanism

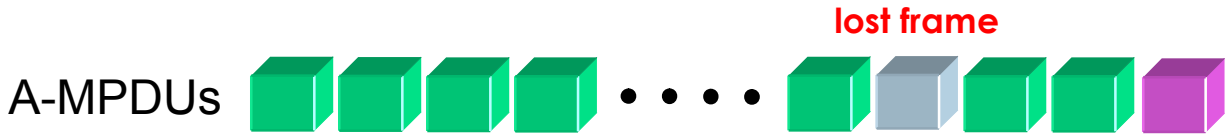
- Rather than sending an individual acknowledge following each data frame, 802.11n introduces the technique of confirming a burst of up to 64 frames with a single Block ACK (BA) frame
- The Block ACK even contains a bitmap to selectively acknowledge individual frames of a burst (comparable to selective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

Block-Ack Mechanism (cont.)



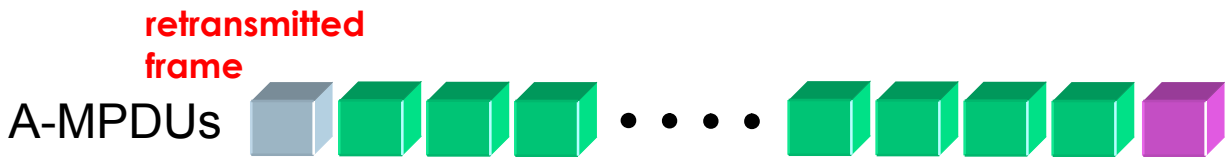
Bitmap (64 bits)

Start Sequence # 1 +1111 1111 …. 1111 1111= **65**



Bitmap (64 bits)

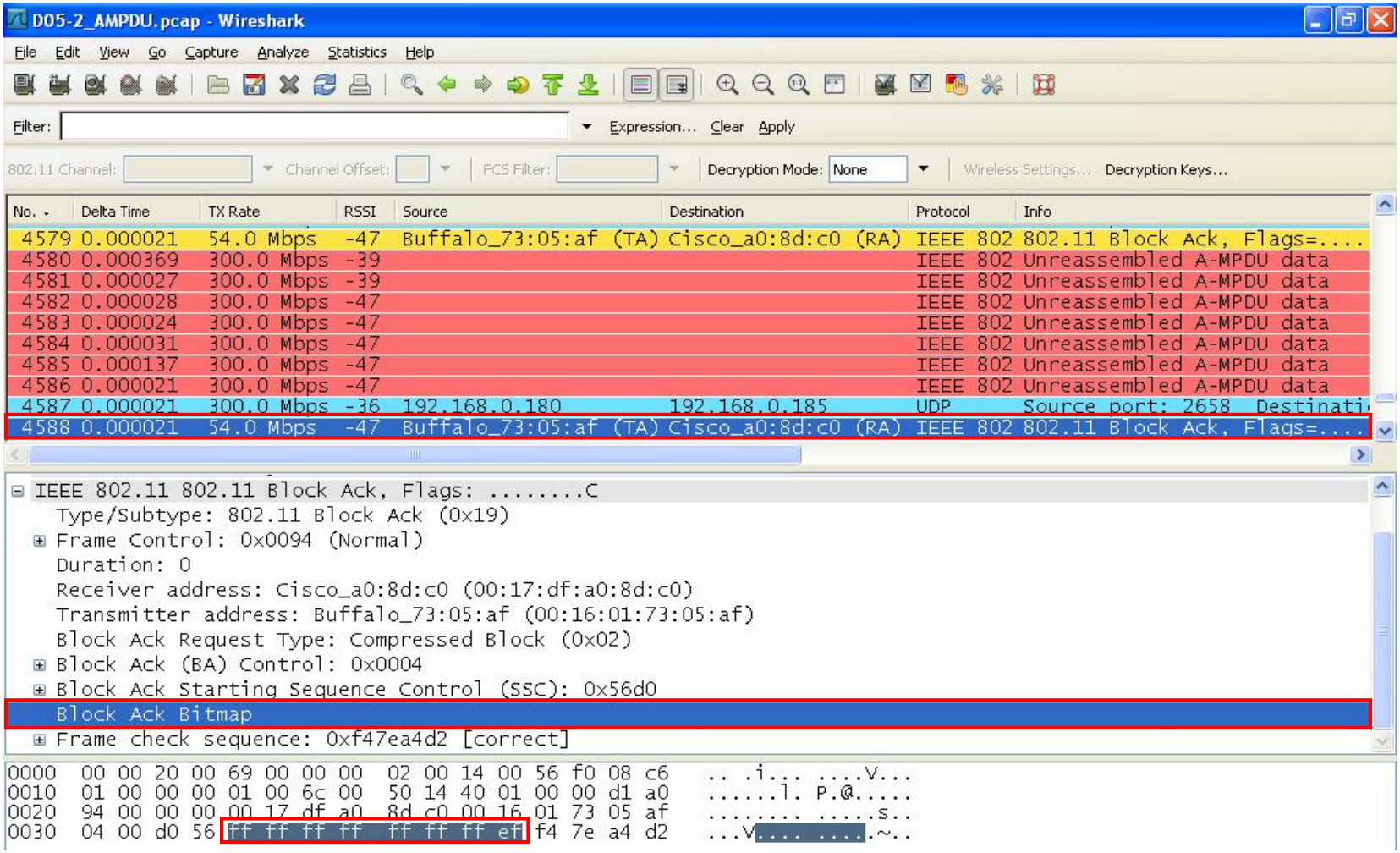
Start Sequence # 65 +1111 1111 …. 1111 1**0**11= **129**



Bitmap (64 bits)

Start Sequence # 128 +**1**111 1111 …. 1111 1111= **192**

Block-ACK Bitmap Analysis

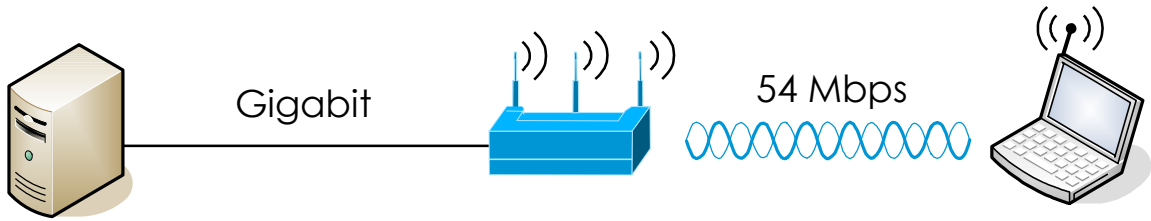


TCP Throughput Measurements with Iperf

IBM TP T41p Win XP
192.168.0.181

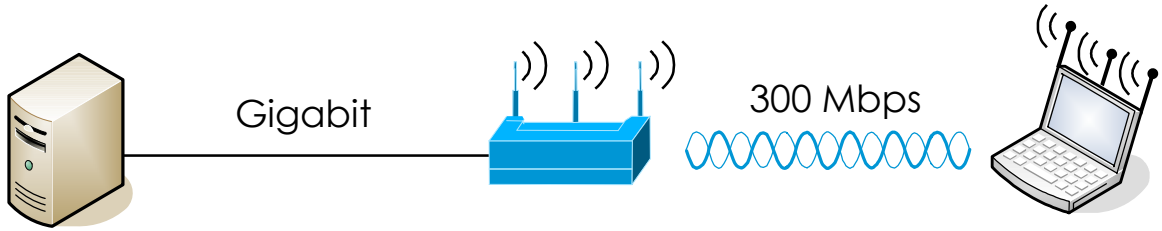
Cisco 1250
AIR-AP1252AG-E-K9

HP2230 Win Vista
INTEL WiFi 5100AGN
192.168.0.204



Iperf server

Iperf client, TCP Window size 100kB
iperf -c 192.168.0.181 -p1000 –w100K
TCP Throughput: 20 Mbit/sec (no encr.)



Iperf server

Iperf client, TCP Window size 100kB
iperf -c 192.168.0.181 -p1000 –w100K
TCP Throughput: 100 Mbit/sec (no encr.)

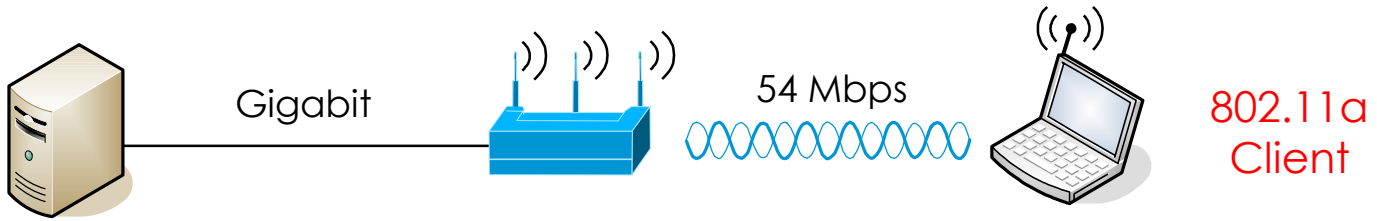
5 - 15% throughput reduction with WPA2 Encryption

TCP Throughput Measurements with Iperf

IBM TP T41p Win XP
192.168.0.181

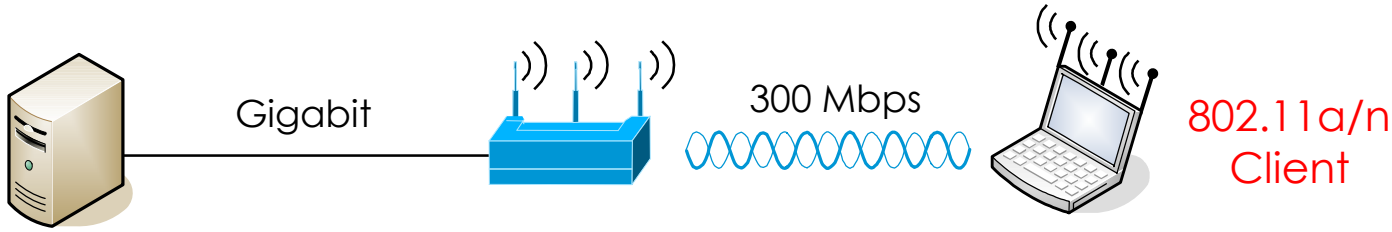
Cisco 1250
AIR-AP1252AG-E-K9

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'	
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 Troughput (HT) Extensions**

2.4 GHz

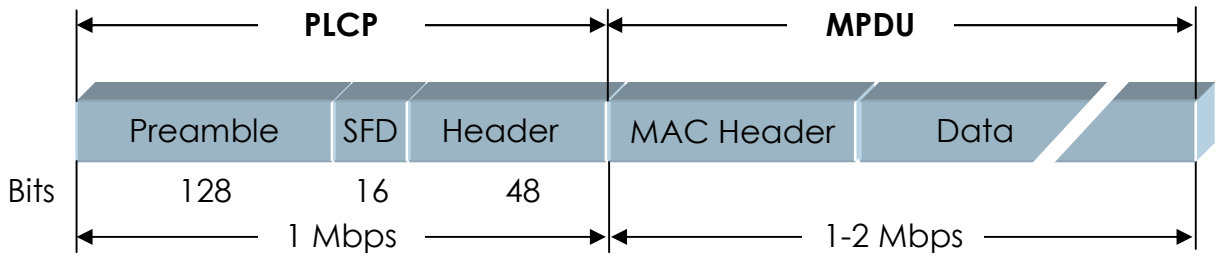
5 GHz

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

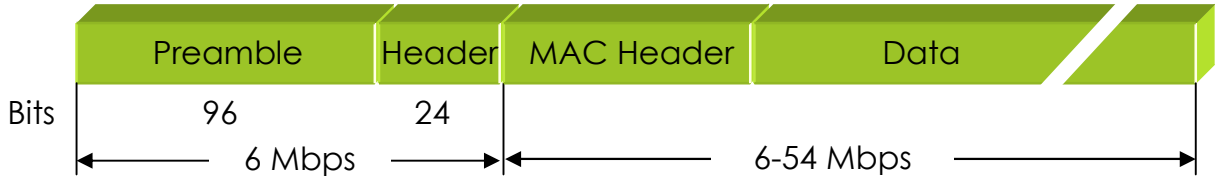
Overview Frame Types (2.4 GHz)

802.11 DSSS with
‚Long Preamble'
Barker Code

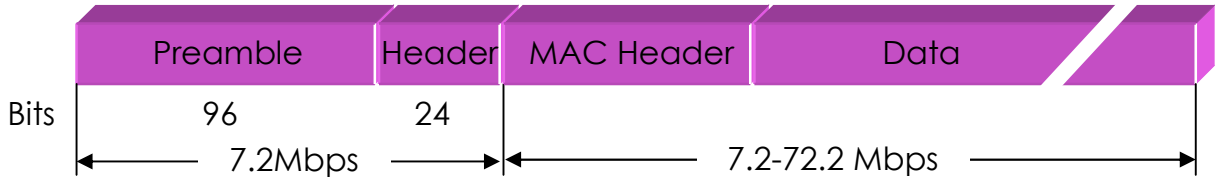


802.11b HR/DSSS with
‚Short Preamble'
Barker / CCK

802.11g (ERP)
Extended Rate PHY
OFDM



802.11n (HT)
High Throughput
extended OFDM

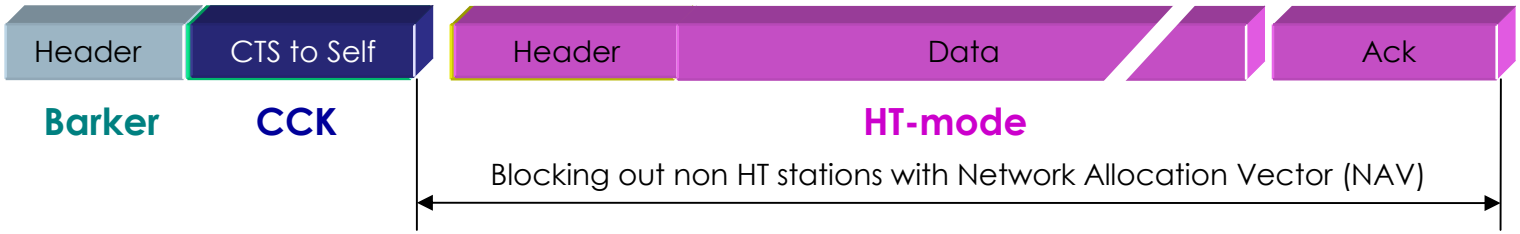


PLCP = Physical Layer Convergence Protocol
MPDU = MAC Layer Protocol Data Unit (decodiert by Wireshark)

Backwards compatibility to a/b/g

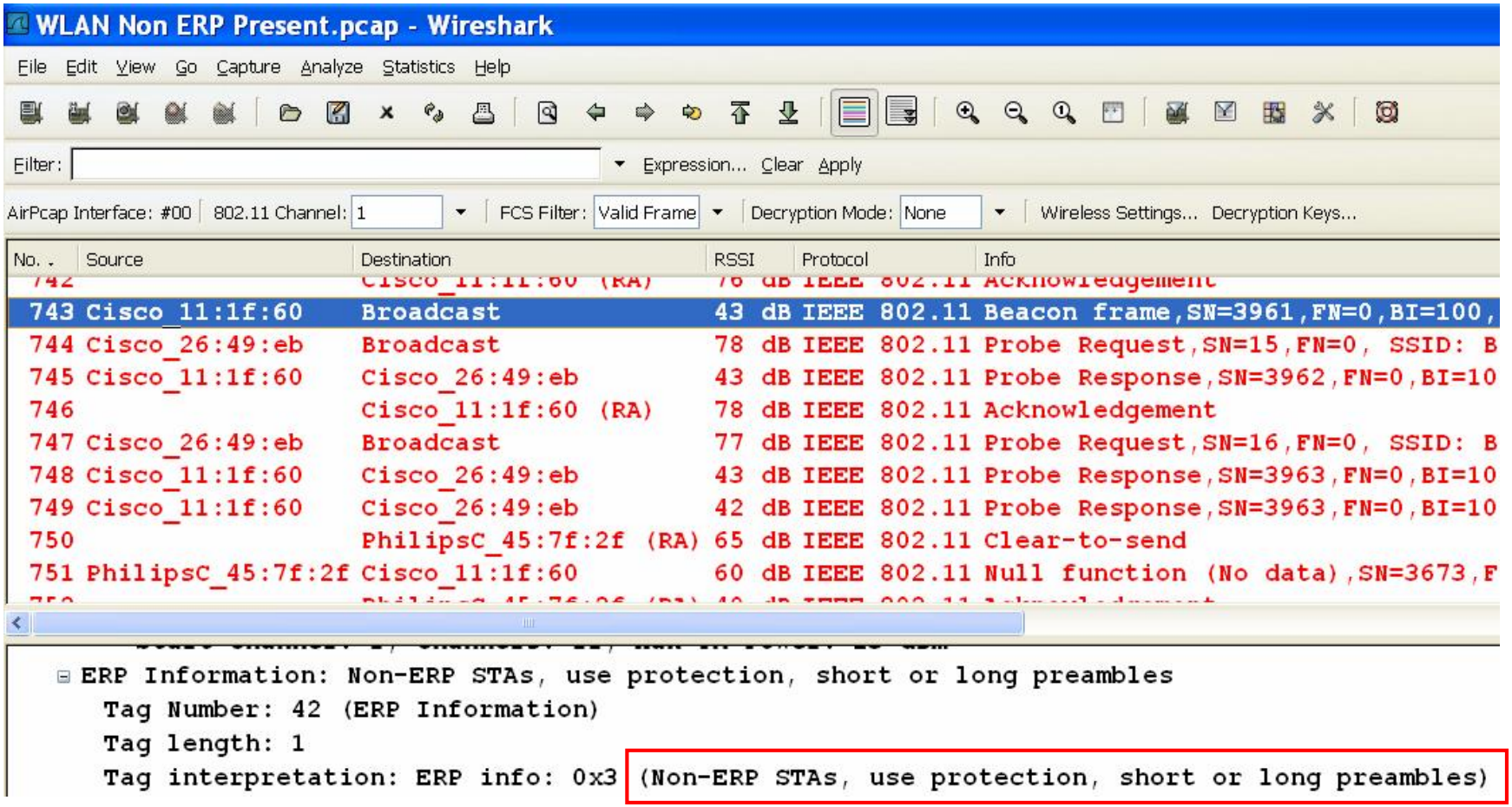
- 802.11n supports three compatibility modes
  - Legacy mode
  - Mixed mode
  - Greenfield mode
- Legacy mode

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



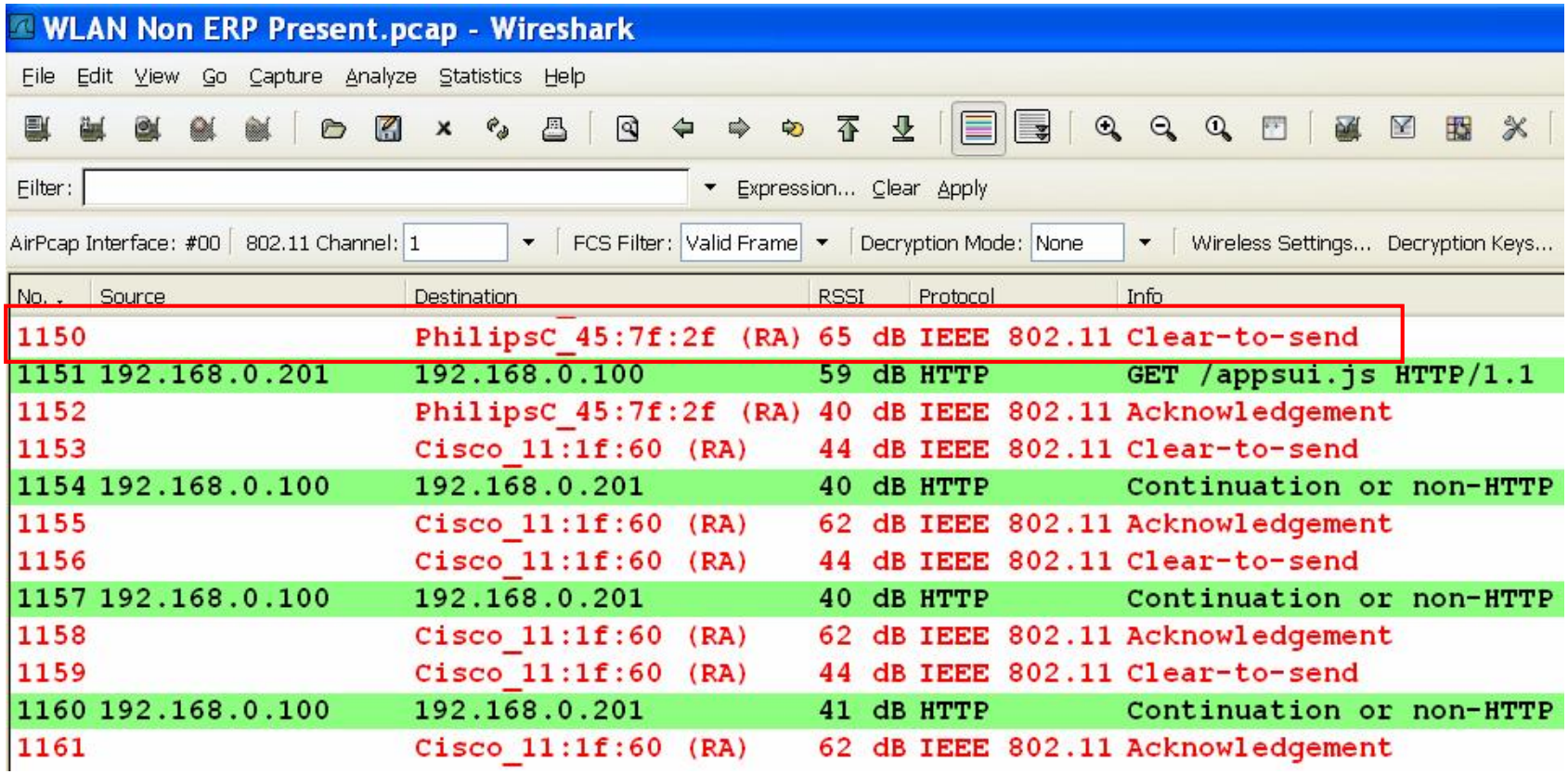
Backwards compatibility to a/b/g (cont.)

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



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

OFDM stations changes to 'Protected Mode'



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

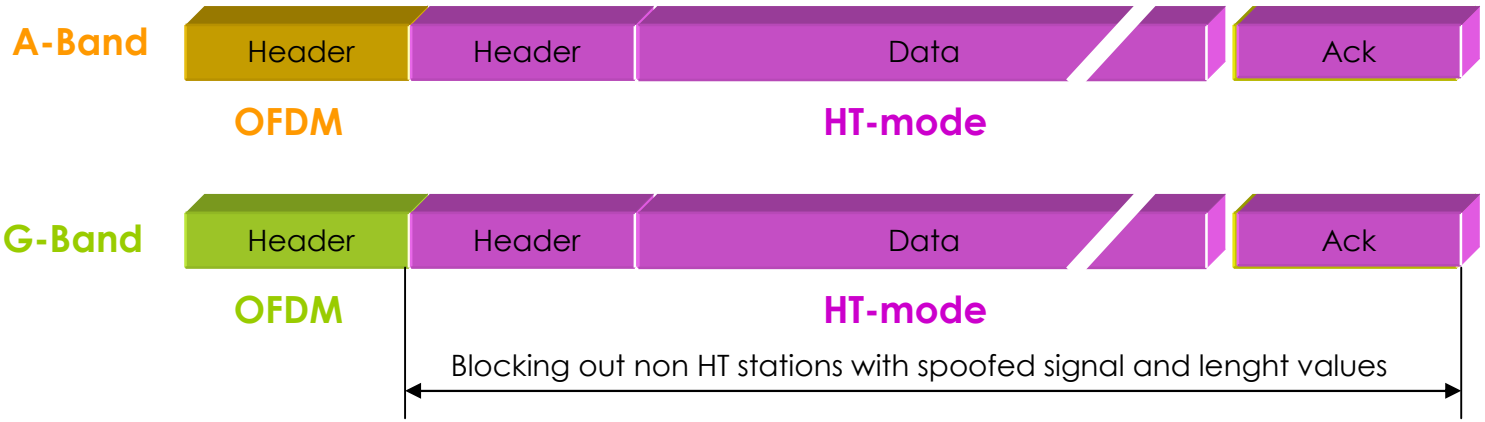
Throughput improvement:

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