Laboratory of Nomadic Communication

Quick introduction to IEEE 802.11

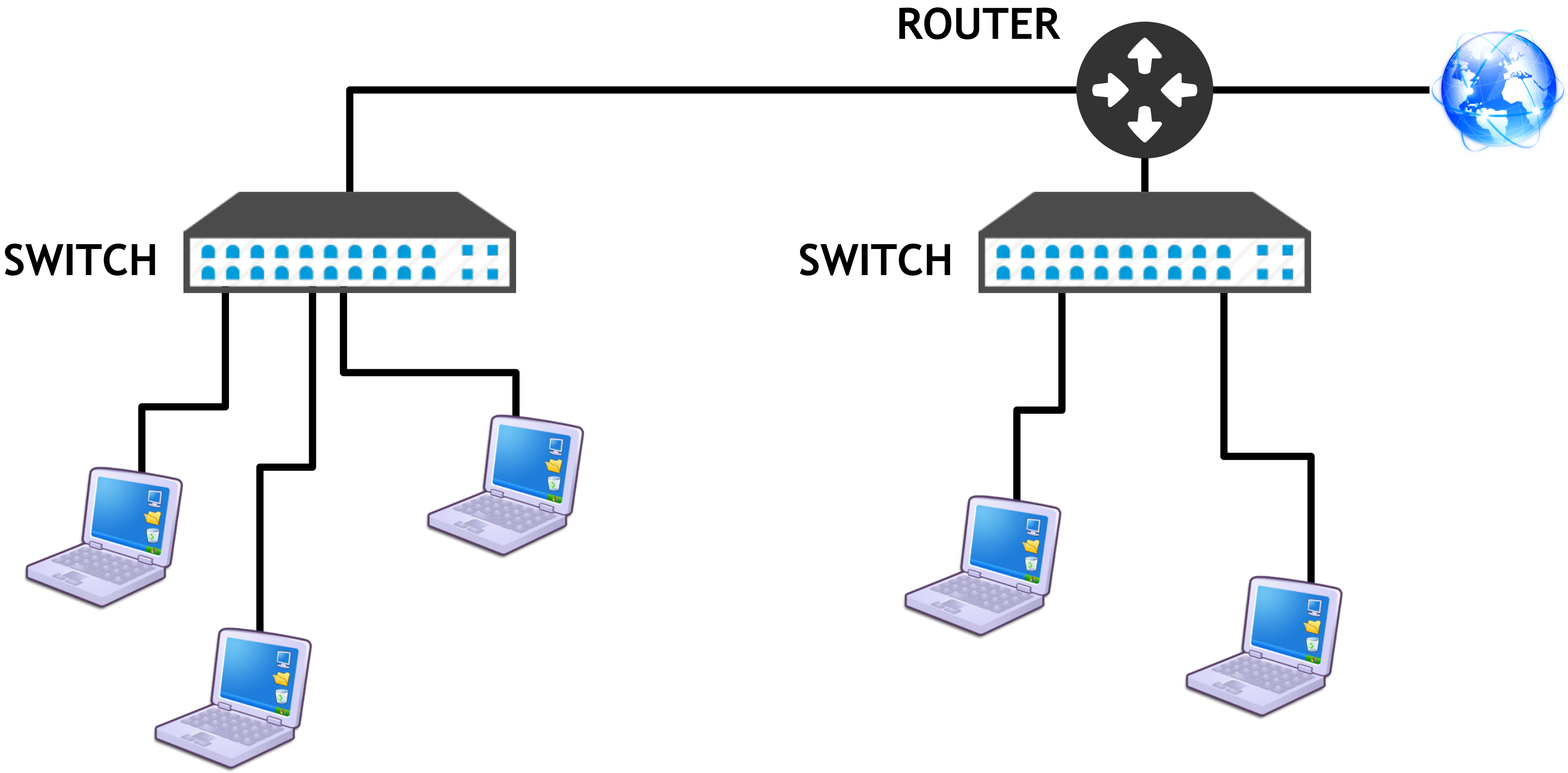
Wireless LAN Standard

A quick introduction to the IEEE 802.11 standard

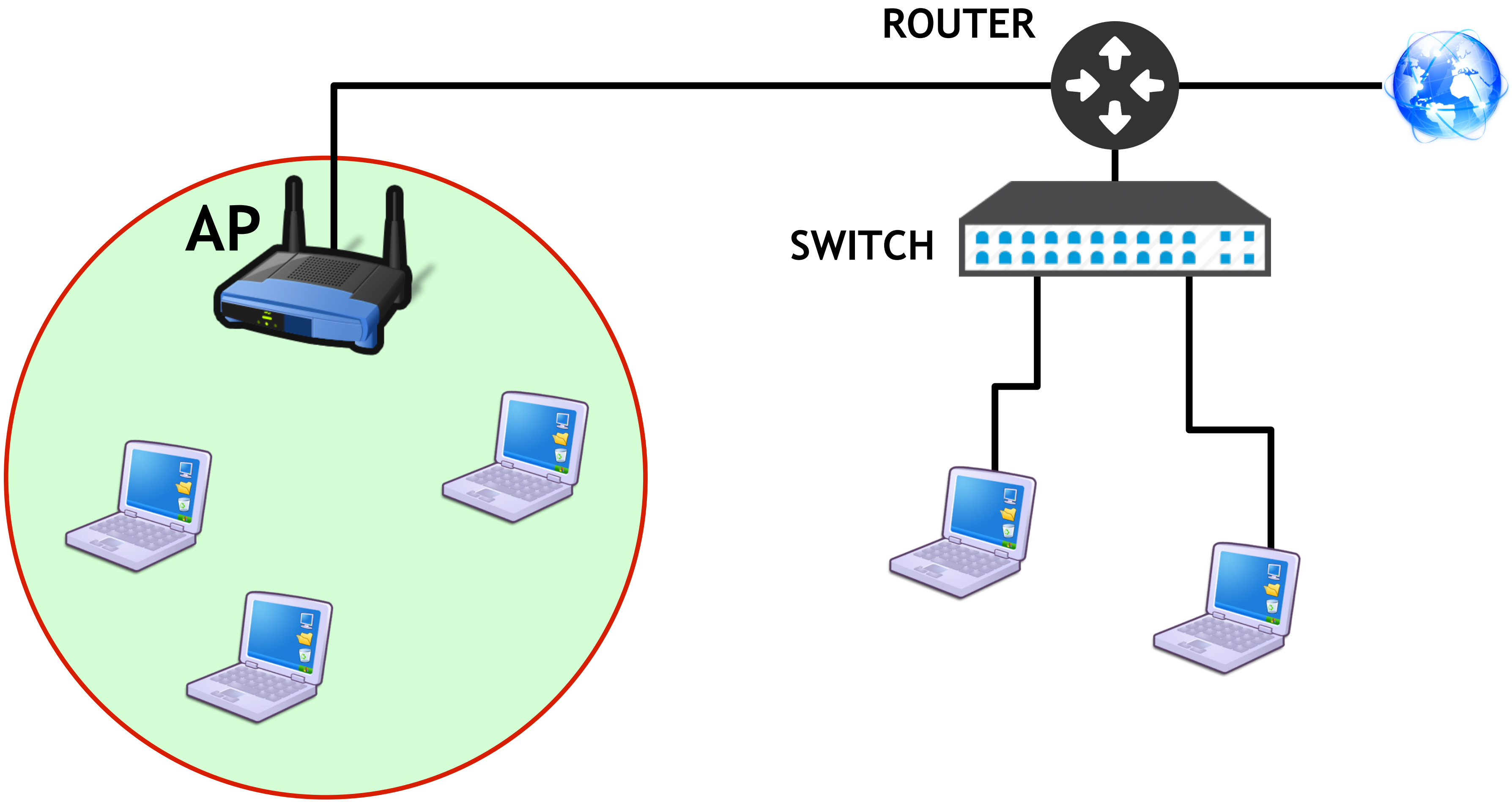
IEEE 802.11 standard

- Definition of wireless interface
  - between a client and a base station (aka: Access Point, AP)
  - between wireless clients (simply: stations)
- Two lower layers of the stack
  - 1-PHY - radio transmission: modulations, bands, frequency, energy
  - 2-MAC - medium access control: timings, retransmissions, signaling
- Many amendments published since ’97
  - Throughput improvements (e.g., 802.11ac up to multi Gb/s)
  - Security (802.11i), QoS (802.11e), reliable multicast (802.11aa)
- Very long standard: 2012 rel. (pre 11ac) is ~2800 pages!

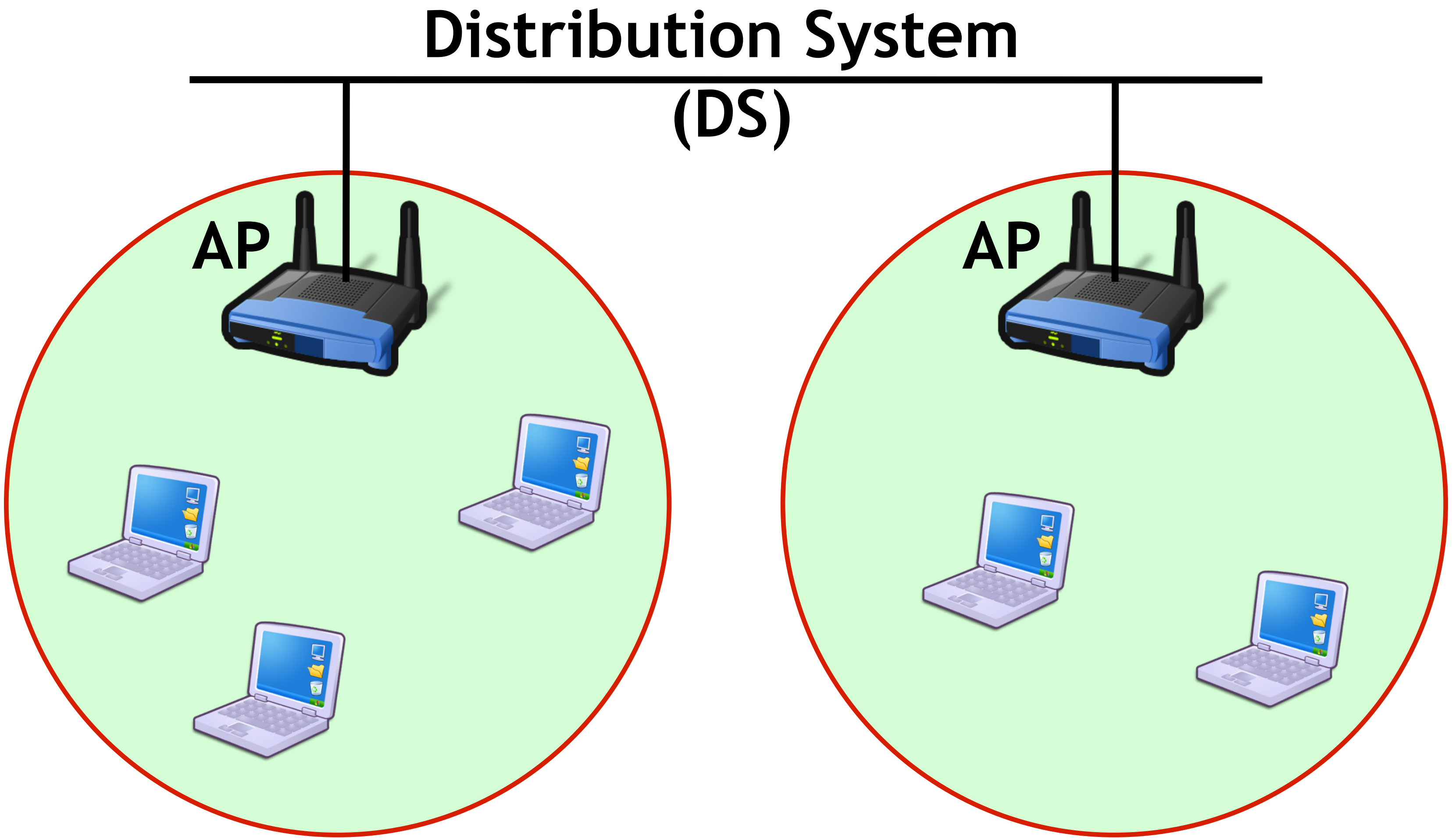
A LAN goes WIRELESS



A LAN goes WIRELESS/2

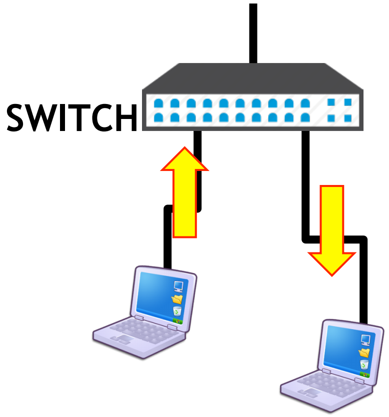


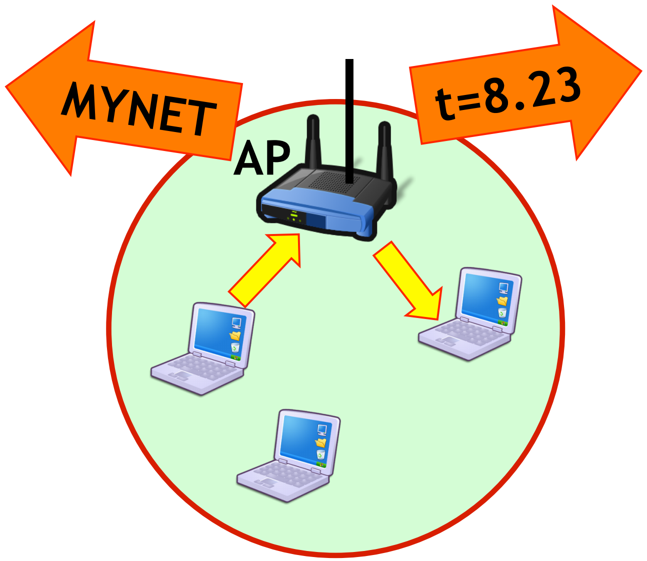
A LAN goes WIRELESS/3



Wireless-LAN vs Wired-Lan

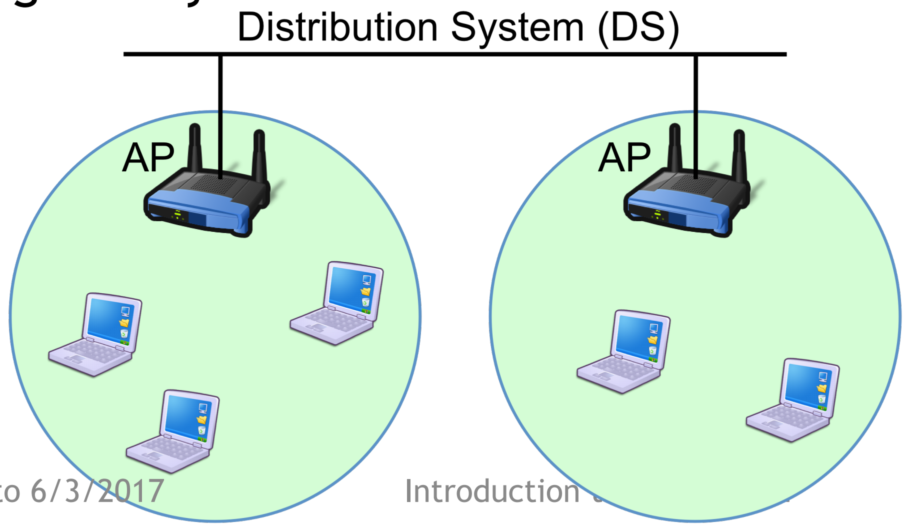
- ❑ Apparently: AP replaces the switch, air replaces cables
- ❑ AP, in fact,
  - forwards inter-stations frames (no direct communication)
  - rules stations access to the network (e.g, by authenticating)
  - manages even more issues than the switch has to, i.e.,
    - **advertizes the network**
    - **synchronizes time etc**





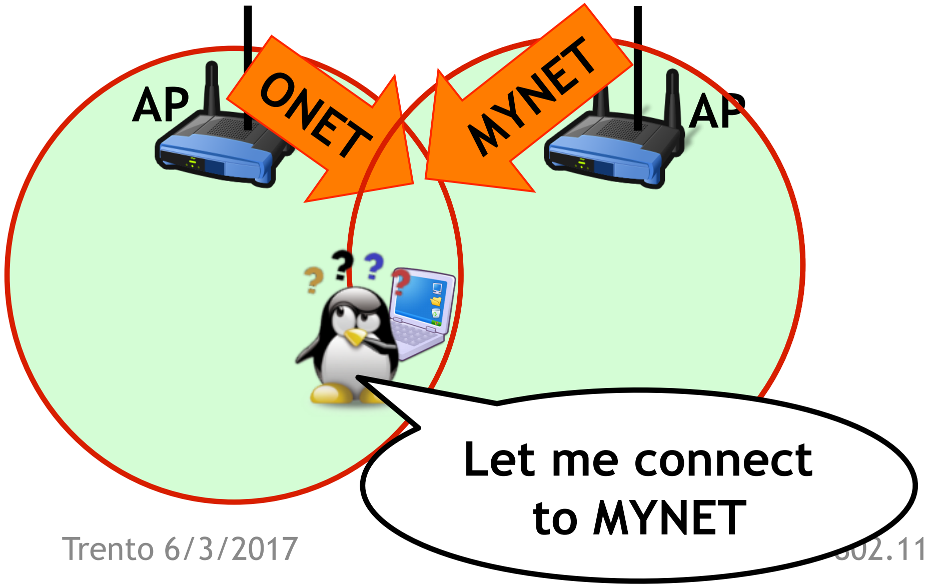
802.11 Wireless-Lan: Infrastructure Mode Basic

- Each cell is an Infrastructure "Basic Service Set" (BSS)
  - The Access Point (AP) "creates" and maintain the BSS
  - Time sync, BSS name and capabilities inside "Beacons" frame
  - All BSS traffic goes through the AP
- More cells build an "Extended Service Set" (ESS)
  - A Distribution System (DS, wired or wireless) connects all APs
  - DS may connect to an Internet gateway



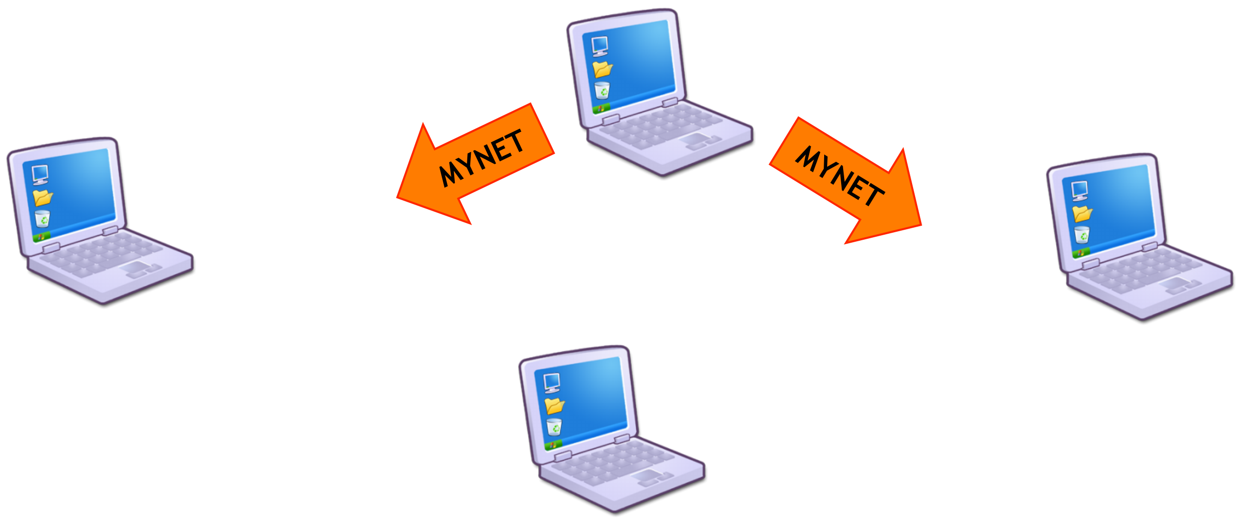
802.11 Wireless-Lan: Infrastructure Mode Basic

- A station that wants to connect does the following:
  - Scan: check all the available networks for one known
    - Passively, by receiving “Beacons”, or Actively, by sending “Probes”
  - Authenticate: proves to the AP she knows something
    - Easiest case: simply send her identity, wait for an ack
  - Associate: station and AP shares mutual capabilities
- Eventually:
  - Station sends/receives traffic



802.11 Wireless-Lan: Ad-Hoc Mode Basic

- Stations create an Ad-Hoc network with a specific “NAME”
  - No AP needed: Independent BSS (IBSS)
  - The first station active starts sending beacons (e.g., leader)
  - Other stations can join the Ad-Hoc network
    - If they do not receive the beacon from the leader, they transmit one!



A very incomplete standard synopsis

Document	year	modulation add-on	band (GHz)	width (MHz)	spatial stream	Rates addon
802.11	97	DSSS	2.4	20	/	1, 2
802.11b	99	CCK	2.4	20	/	5.5, 11
802.11a	01	OFDM	5	20	/	6 … 54 (8 rates)
802.11g	03	/	2.4	20	/	all the above
802.11n	09	MIMO & OFDM+	2.4 & 5	20, 40	up to 4	HT-PHY MCS [max 600Mb/s]
802.11ac	13	MU-MIMO & OFDM++	2.4 & 5	20,40, 80,160	up to 8	VHT-PHY MCS [max 6.7Gb/s]

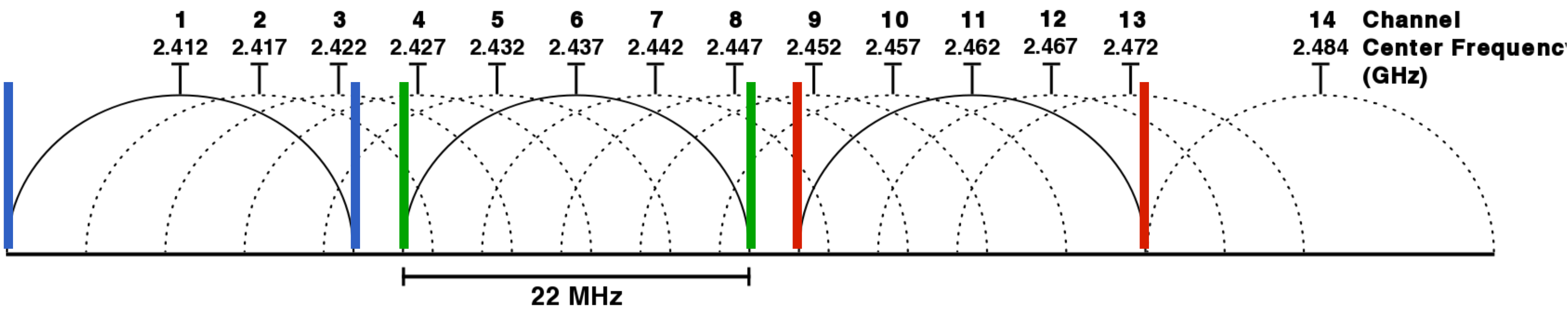
A very incomplete standard synopsis

- In this course we will use 802.11bg only devices
  - Yeah, pretty old hardware but…
  - … we have access to the NIC internals, we can play with the standard
  - All the standards share the same basic algorithms for channel access

Document	modulations	band (GHz)	width (MHz)	Rates
802.11b/g	DSSS/CCK OFDM	2.4	20	1, 2 / 5.5, 11 6, 9, 12, 18, 24, 36, 48 ,54

IEEE 802.11: insight of the 2.4GHz band

- ISM 2.4GHz band spans range [2400-2483.5]MHz worldwide
  - Availability subject to country regulations
    - E.g., USA [1-11], Italy [1-13], Japan [1-14] (but 14 only 11b!)
- Standard: 13 channels (5 MHz spacing) + channel 14
  - ch_N @ [2407 + 5 * N]MHz, $1 \leq N \leq 13$; very busy ☹
  - ch_{14} @ 2484MHz; not used outside Japan ☺
- How many orthogonal channels? Remember 20MHz width

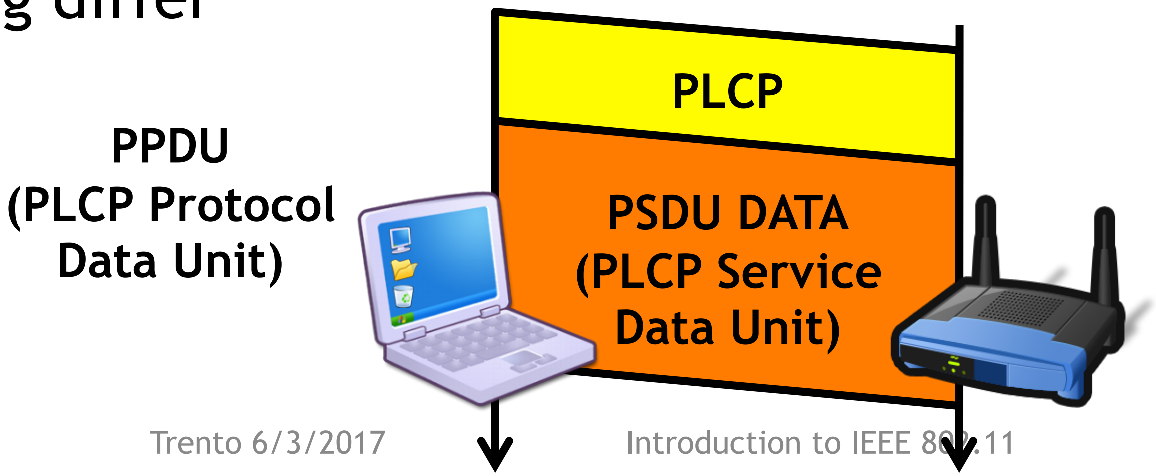


Wireless LAN Standard

802.11bg Physical Layer analysis

IEEE 802.11bg: a frame unit (no MAC yet)

- Each frame preceded by PLCP preamble
  - Physical Layer Convergence Procedure
- PLCP helps the receiver
  - Understanding a transmission is beginning (energy raise)
  - Knowing which data-rate encoding is used for data and its length
  - Synchronizing the decoding subsystem
- PLCPs of 11b and 11g differ
  - Let’s check!

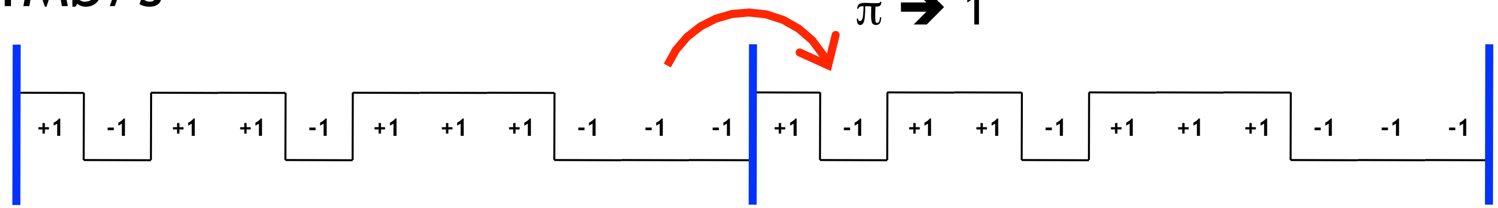


IEEE 802.11b: PPDU format/1

- Direct Sequence Spread Spectrum modulations
  - Each bit is “spread” to a sequence of 11 chips (Barker train)
  - A sequence of 11 “chips” transmitted repeatedly by shifting phase
  - Phase shift of consecutive chip trains encode the PPDU

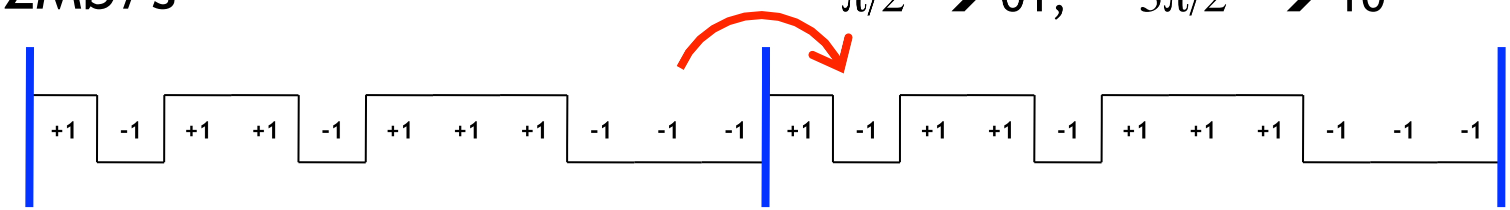
1Mb/s

Phase shift $0 \rightarrow 0$, $\pi \rightarrow 1$



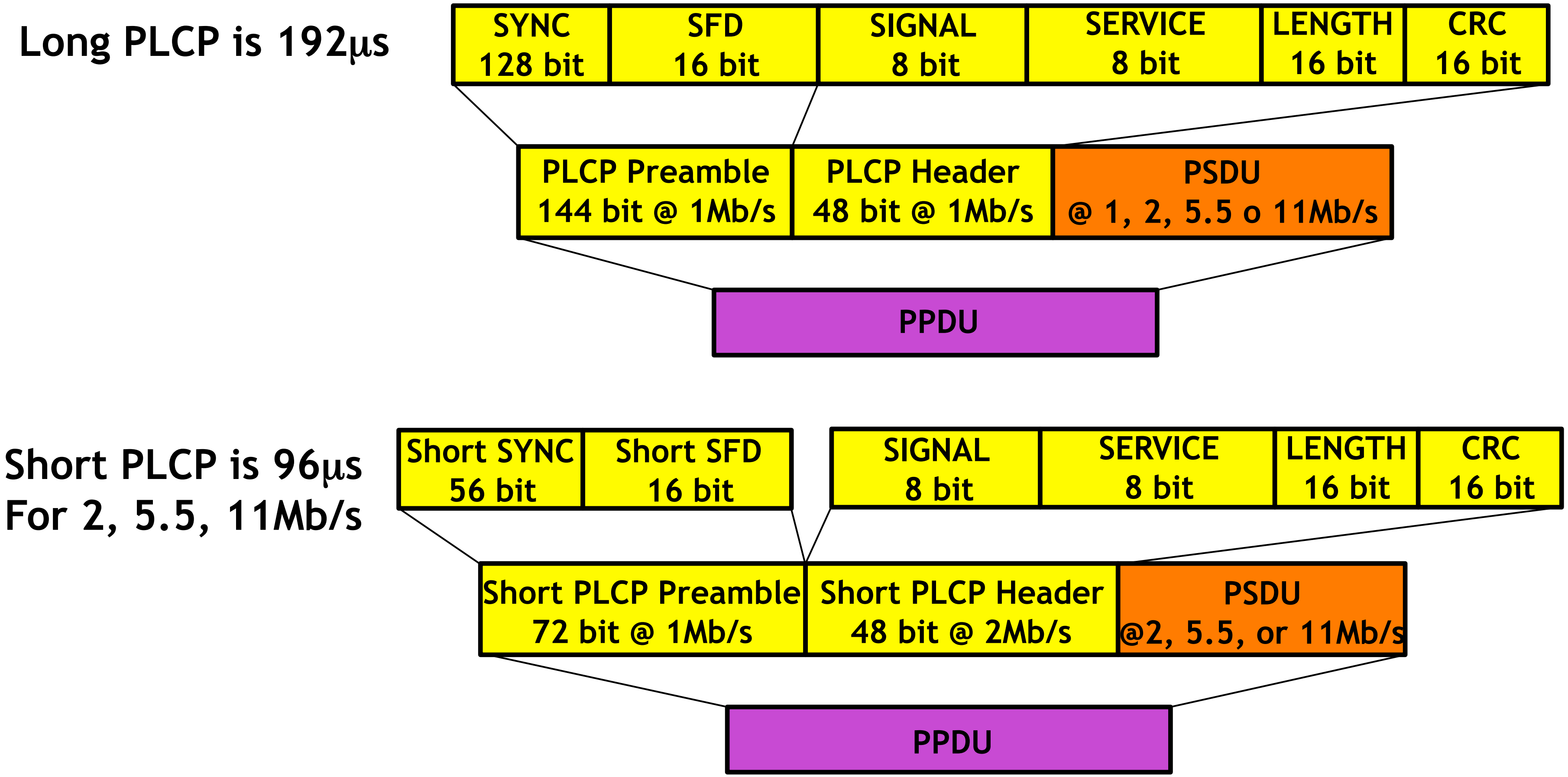
2Mb/s

Phase shift $0 \rightarrow 00$, $\pi/2 \rightarrow 01$, $\pi \rightarrow 11$, $3\pi/2 \rightarrow 10$



IEEE 802.11b: PPDU format/2

- Two possible PLCP format:



IEEE 802.11b: PPDU format/3

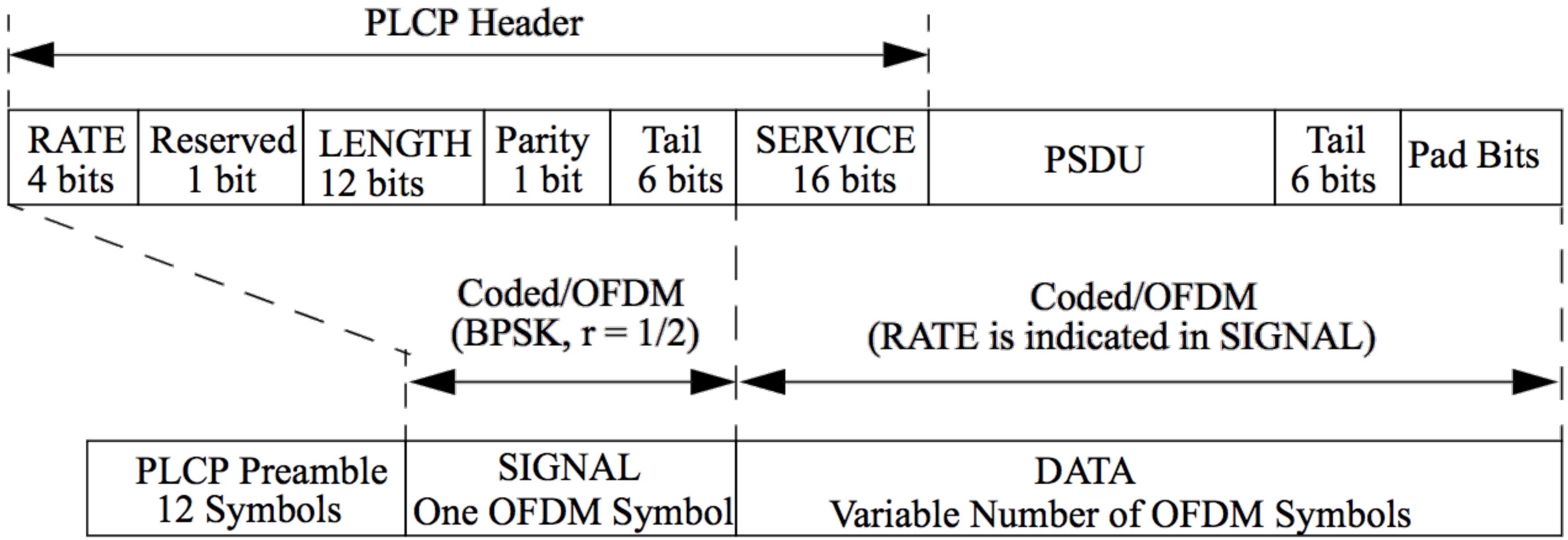
- PPDU format is very inefficient!

- E.g.: Acknowledgement (shortest frame), 14byte = 112bit
  - Preamble PSDU
  - @1Mb/s, $192\mu s$ $112\mu s$
  - @2Mb/s, $192\mu s$ (or 96) $56\mu s$
  - @5.5Mb/s, $192\mu s$ (or 96) $21\mu s$
  - @11Mb/s, $192\mu s$ (or 96) $11\mu s$

PLCP much longer than actual data!

IEEE 802.11g: PPDU format/1

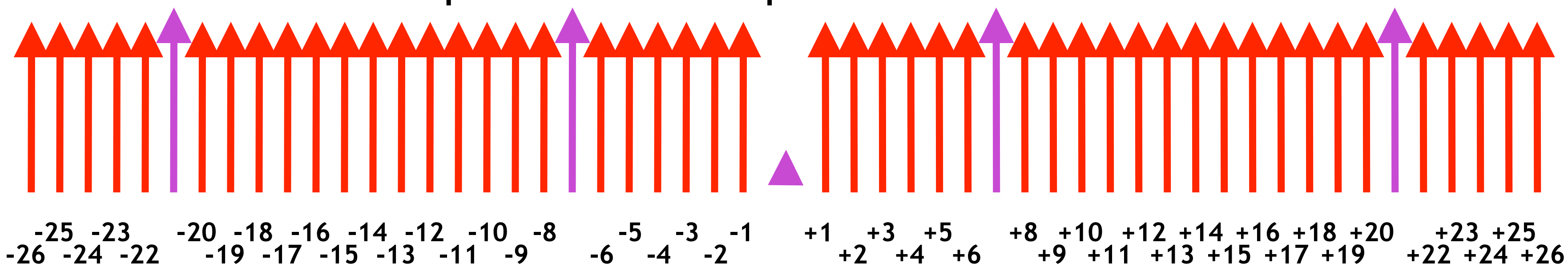
- 802.11g: new PLCP, very short



PLCP is 20μs

IEEE 802.11g: PPDU format/2

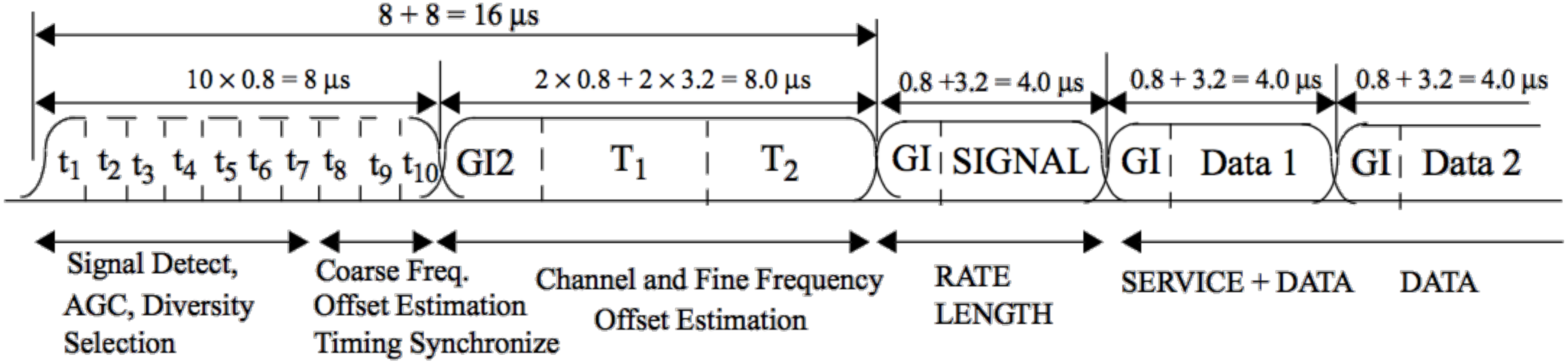
- Orthogonal Frequency Division Multiplexing (6Mb/s)
  - PPDU is divided in groups of 24 bits (three bytes)
  - Each group of 24 is expanded to 48 bit (FEC)
  - Each bit of these 48 weights a specific carrier (with -1 for 0, +1 for 1)
  - Five additional pilot carriers - pink - inserted



  - Time signal computed by running ifft of the carrier weights
  - Each group takes 4μs, call this “OFDM symbol”
- Higher data rates map more bits to each carrier/symbol

IEEE 802.11g: PPDU format/2

- 802.11g: frame includes
  - PLCP Preamble made of 10 short symbols ($8\mu s$) + 2 long ones ($8\mu s$)
  - PLCP Header made of
    - SIGNAL field in its own symbol ($4\mu s$, PSDU length+rate)
    - SERVICE field, first 16 bits of first data symbol
  - PSDU made of symbols, each one carrying N bits, N depends on Rate
  - PSDU terminate with CRC32 and at least 6 padding bits



IEEE 802.11g: PPDU format/2

- 802.11g: data payload
  - Bit expanded by convolutional encoder for FEC, $R = [1/2, 2/3, 3/4]$
  - Groups of N_{CBPS} (Coded Bit Per Symbol) or N_{DBPS} (Data Bit Per Symbol)
  - Each subcarrier transport N_{BPSC} bit (Bit Per SubCarrier)

Modulation	R	N_{BPSC}	N_{CBPS}	N_{DBPS}	Data rate
BPSK	1/2	1	48	24	6
BPSK	3/4	1	48	36	9
QPSK	1/2	2	96	48	12
QPSK	3/4	2	96	72	18
16-QAM	1/2	4	192	96	24
16-QAM	3/4	4	192	144	36
64-QAM	2/3	6	288	192	48
64-QAM	3/4	6	288	216	54

IEEE 802.11g: frame format/6

- E.g.: Acknowledgement, 14byte = 112bit
- PLCP: $20\mu s$
- $DATA_{PSDU}$: 16b(SERVICE)+112b(PSDU)+6b($tail_{min}$)=134b

Data rate	PLCP	N_{DBPS}	bit	symbol	ΔT	Extension	Total
6	$20\mu s$	24	134	6	$24\mu s$	$6\mu s$	$50\mu s$
9	$20\mu s$	36	134	4	$16\mu s$	$6\mu s$	$42\mu s$
12	$20\mu s$	48	134	3	$12\mu s$	$6\mu s$	$38\mu s$
18	$20\mu s$	72	134	2	$8\mu s$	$6\mu s$	$34\mu s$
24	$20\mu s$	96	134	2	$8\mu s$	$6\mu s$	$34\mu s$
36	$20\mu s$	144	134	1	$4\mu s$	$6\mu s$	$30\mu s$
48	$20\mu s$	192	134	1	$4\mu s$	$6\mu s$	$30\mu s$
54	$20\mu s$	216	134	1	$4\mu s$	$6\mu s$	$30\mu s$

Wireless LAN Standard

802.11bg Frame format analysis (@ layer 2)

IEEE 802.11: Frame types

- Three types of Mac Protocol Data Unit (MPDU):
  - Management, e.g. Association Request/Response, Beacon, (De)Auth
    - Network/BSS Advertisement, BSS Join, Authentication etc
  - Control, e.g. ACK, RTS, CTS, Poll, etc
    - For channel access (RTS, CTS), positive frame acknowledgment
  - Data: Plain data + QoS Data, etc
    - Frames with user data
  - MPDU fields: depend on frame type!

2	2	6	6	6	2	6	2	0-2312	4
Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	Frame Body	FCS

IEEE 802.11: PSDU fields/1

- Frame Control:
  - Protocol version, only 0 today
  - Type and Subtype encode frame type + subtype
  - ToDS: frame is for Distribution System; FromDS frame is from DS
    - If both set to 1, frame is transported by a Wireless DS
  - More: announce other fragments are coming (PSDU is fragmented)
  - Retry: help rx’er understanding this is a retransmission
  - {Pwr Mgt, More Data} deal with power management, save
  - Protected: announce Frame Body is encrypted

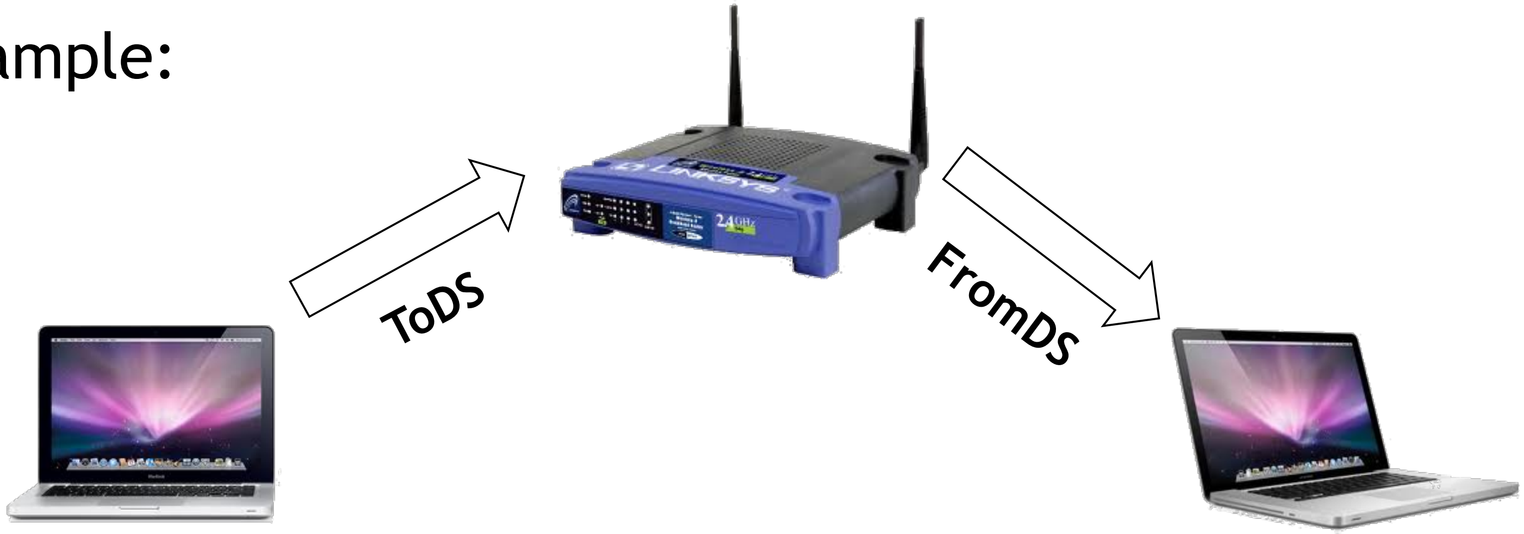
b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}
Protocol Version		Frame Type		Frame Subtype				To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	Crypt	Order

IEEE 802.11: PSDU fields/2

- Duration/ID
  - Meaning depends on MPDU type
  - Data: number of μs after frame end during which medium is reserved
    - Used by Virtual Carrier Sense, set the Network Allocation Vector (NAV)
- Address fields: they depends on ToDS/FromDS fields:
  - BSSID: Basic Service Set IDentification
    - Address of the AP
  - DA: Destination Address, “final destination”
  - RA: Receiver Address, immediate frame destination
  - SA: Source Address, who has generated this frame
  - TA: Transmitter Address, who has forwarded this frame

IEEE 802.11: PSDU fields/3

- Example:



To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA = DA	TA = SA	BSSID	N/A
0	1	RA = DA	TA = BSSID	SA	N/A
1	0	RA = BSSID	TA = SA	DA	N/A
1	1	RA	TA	DA	SA

IEEE 802.11: PSDU fields/4

- Sequence Control:
  - Fragment number, 4 bits
    - For fragmented PSDU, it's the number of this fragment
  - Sequence Number, 12 bits, unique for PSDU
    - Identify the PSDU (used by rx'er to avoid accepting same frame > once)

b_0 … b_3	b_4 … b_{15}
Fragment number	**Sequence number**

- QoS Control: identify Traffic Category (optional field)
- FCS: CRC/32 Frame Check Sequence protecting the PSDU

IEEE 802.11: PSDU example - Data Frame

- IP packet, no QoS, from STA to AP (ToDS): Data frame
  - Logical Link Control (LLC) encapsulation is used
    - 8 bytes before IP: 0xAA, 0xAA, 0x03, 0x00, 0x00, 0x00, 0x08, 0x00 (ethertype: 0x08, 0x00)
  - Type: Data frame
    SubType: 0 ⇒ Byte#0 := 0x08
  - ToDS ⇒ Byte#1 := 0x01
  - Duration: time to tx an ACK + SIFS
  - Address: it's a ToDS frame, fill the three address fields
  - SeqCTRL: seq. no:=33 ⇒ SeqCTRL:=0x0210

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7
Protocol Version		Frame Type		Frame Subtype			

b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}
To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	Crypt	Order

b_0 – b_3	b_4 – b_{15}
Fragment number	Sequence number

2	2	6	6	6	2	8	N	4
08 01	3A 01	BSSID	SA	DA	10 02	AA AA 03 00 00 00 08 00	IP	FCS

IEEE 802.11: PSDU example - Data Frame

- ❑ Example with WireShark
  - Open a trace file
  - Show Beacons
  - Show Data, retry etc

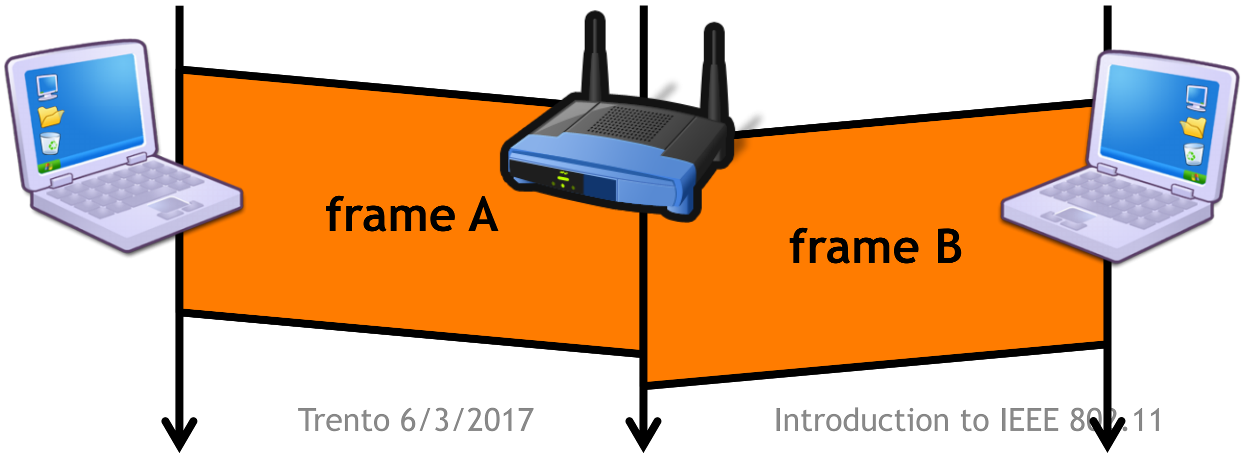
Wireless LAN Standard

The Basic Access Scheme

Distributed Coordination Function (DCF)

Transmissions in a Broadcast Medium

- If two stations transmit at the same time
  - Receiver(s) cannot decode packets (collision)
  - Transmitters do not know whether data was received
- 802.11 standard introduces
  - Slotted medium
  - Positive Acknowledgment with Retransmission
  - Carrier Sense Multiple Access/Collision Avoidance



Time Slot

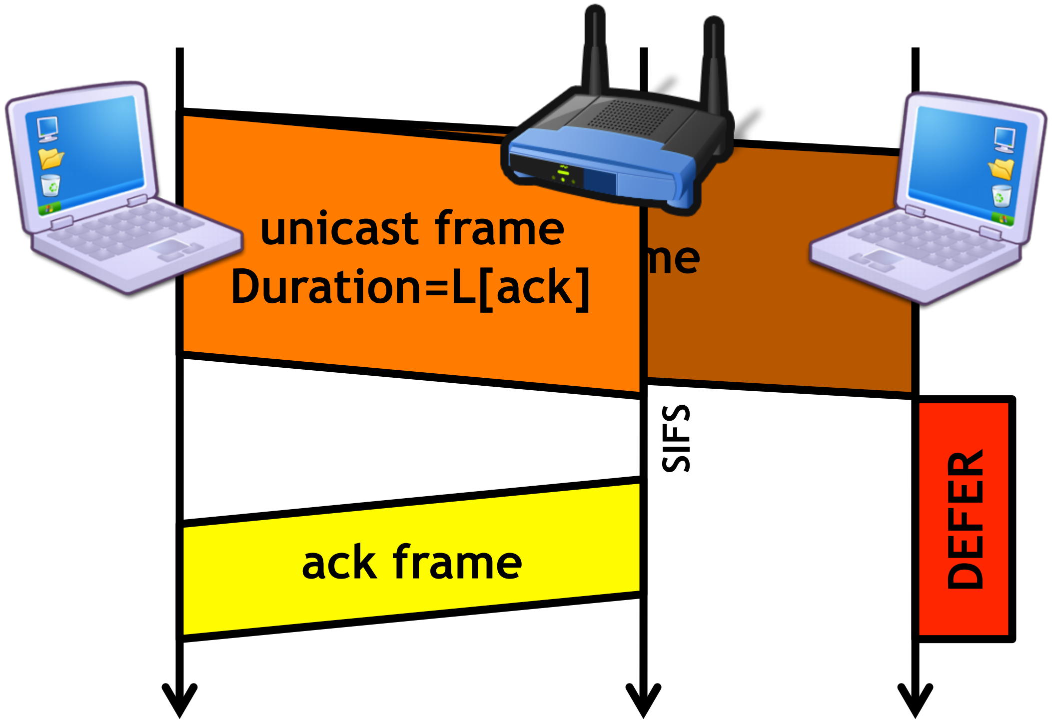
- Time is divided into intervals, called **slots**
  - Working with slot (tx may start with slot) reduces uncertainty
- A Slot is the system unit time
  - 802.11b Slot Time is 20μs, 11g is 9μs
- Time synchronized by Beacons transmitted by the BSS AP
  - Each Beacon carries a 64bit time value (1μs granularity)
  - Stations in the BSS copy beacon time to their clock registers
  - Skews due to poor clock design periodically corrected
- A BSS is a synchronous system!!

InterFrame Space (IFS)

- ❑ Time interval between consecutive transmissions
- ❑ Different IFSs allow different access priorities
  - Short IFS: separate transmissions belonging to the same “dialogue”
    - SIFS in 11bg it’s 10μs
  - Point Coordination IFS: used by the Point Coordinator
    - PIFS is SIFS + Slot Time
  - Distributed IFS: waited by stations when contending for a free channel
    - DIFS is SIFS + 2 * Slot Time
  - Extended IFS: waited by stations when receiving a bad frame
    - EIFS is SIFS + TxTime[AckFrame] + DIFS

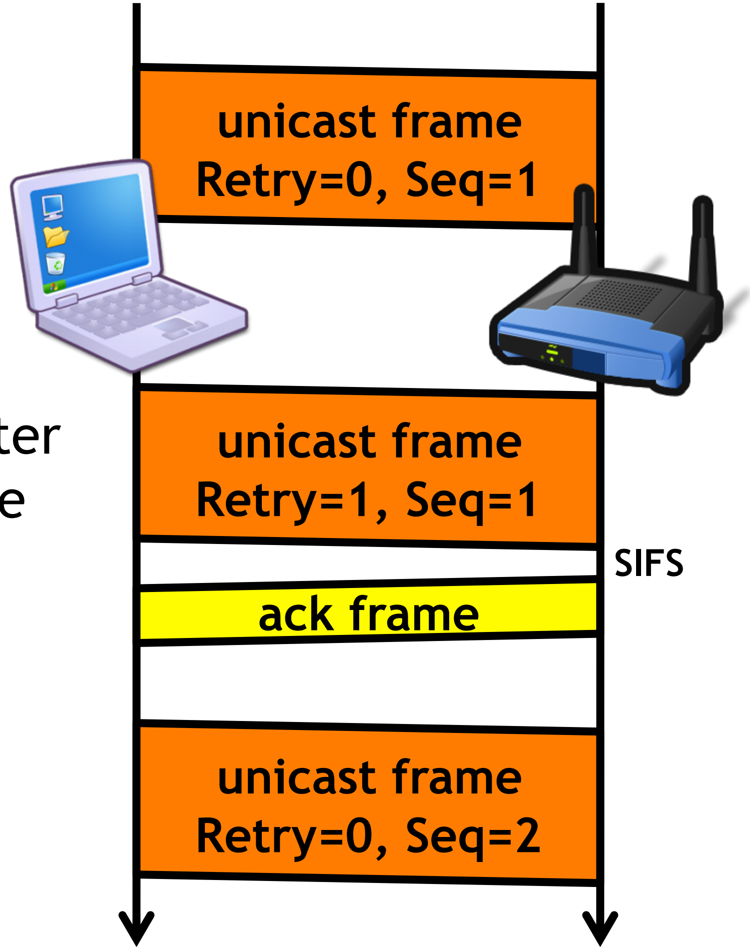
Positive Acknowledgment & Retransmissions

- ❑ Received unicast frame must be acknowledged
  - – Other nodes defer transmissions by using the received "Duration"



Positive Acknowledgment & Retransmissions/2

- If no acknowledgment coming from receiver
  - Retransmit the frame with Retry bit set and same sequence counter
- When acknowledgment received
  - Increase the sequence counter and switch to the next frame

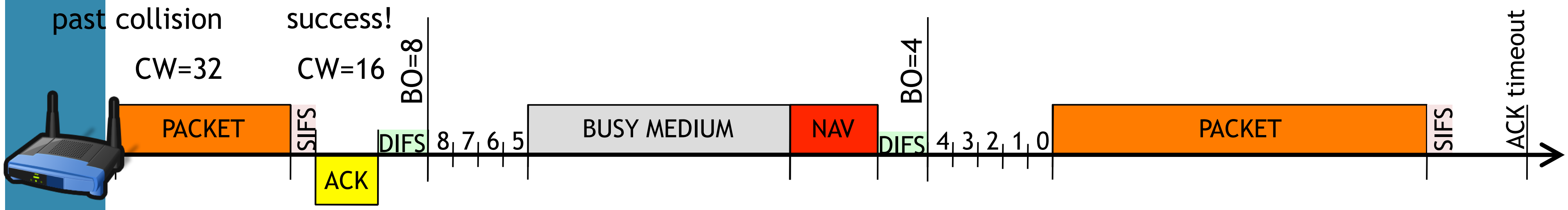


Carrier Sense Multiple Access/ Collision Avoidance

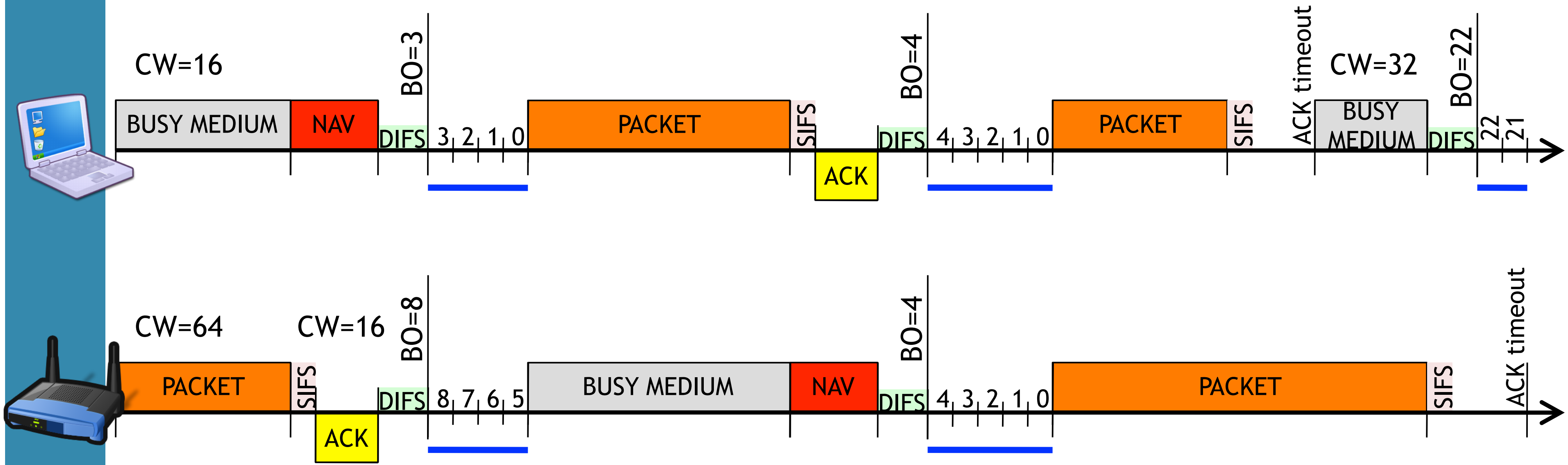
- ❑ Apart from slot synchronization
  - No other explicit coordination among stations
- ❑ To **avoid** repeated collisions
  - Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)
  - Given free-space attenuation, /Collision Detection is not feasible!
- ❑ CSMA/CA Basic
  - Stations willing to transmit have to contend for channel access
  - A station repeats the contention procedure for every (re)transmission

CSMA/CA and channel contention

- Each station keeps a Contention Window (CW) parameter
  1. At the end of the previous transmission attempt
     - If collision (no ack), double CW, otherwise **reset** to CW_{min}
     - Extract Backoff value (BO) ∈ U[0, CW - 1]
  2. “Monitor channel free for t > DIFS”
  3. Backoff stage: decrement BO to zero
     - Backoff: if medium free, decrement BO at every SLOT
     - When medium busy ⇒ Suspend: BO freezed & goto 2
     - If BCKOFF == 0 ⇒ Transmit!

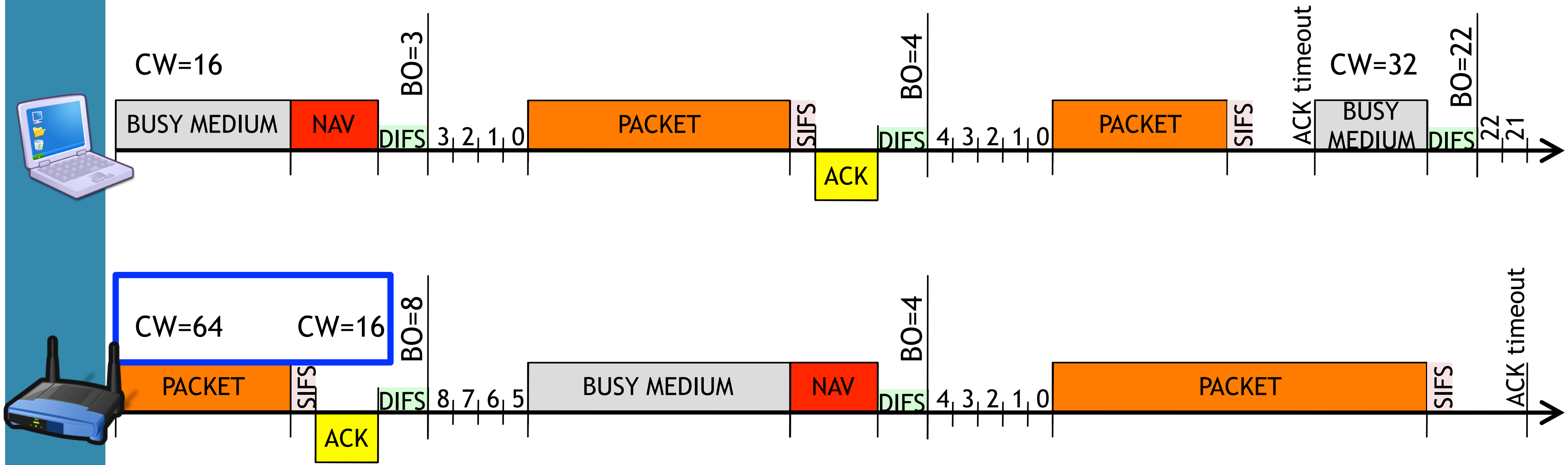


CSMA/CA and channel contention/2



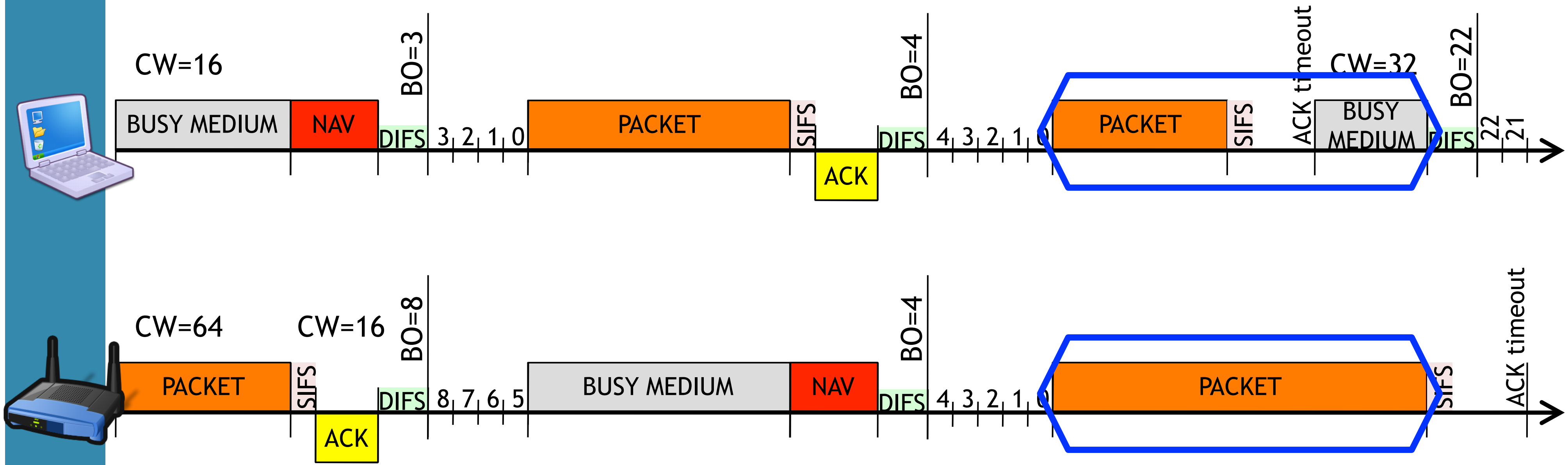
Backoff count-down, channel idle

CSMA/CA and channel contention/3



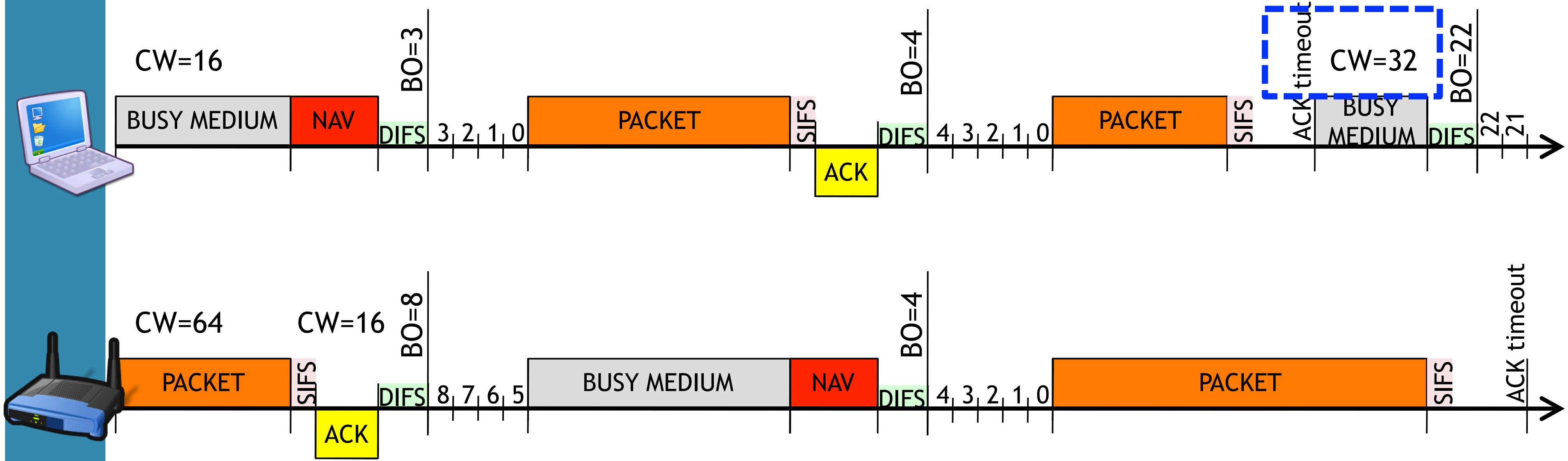
CW reset after success

CSMA/CA and channel contention/4



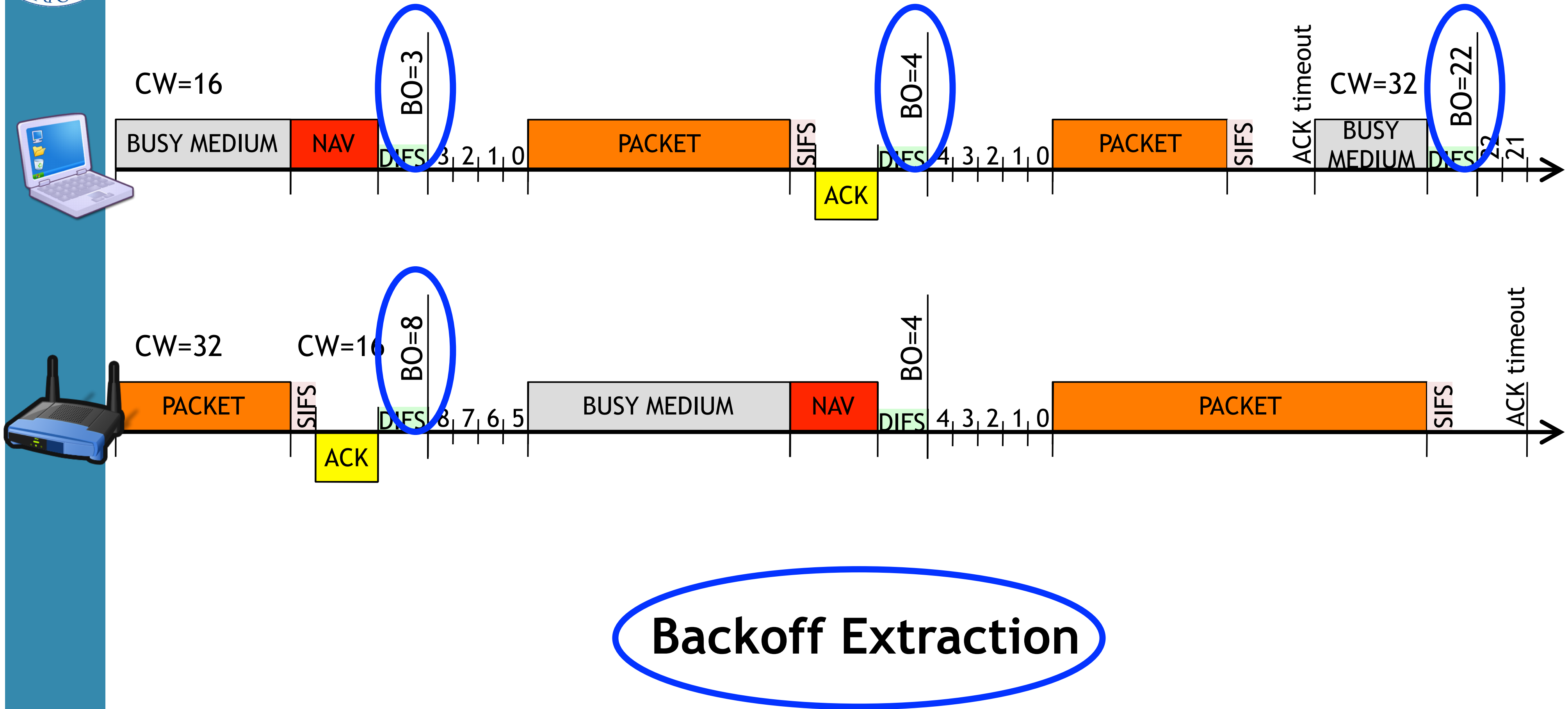
Collision!

CSMA/CA and channel contention/5

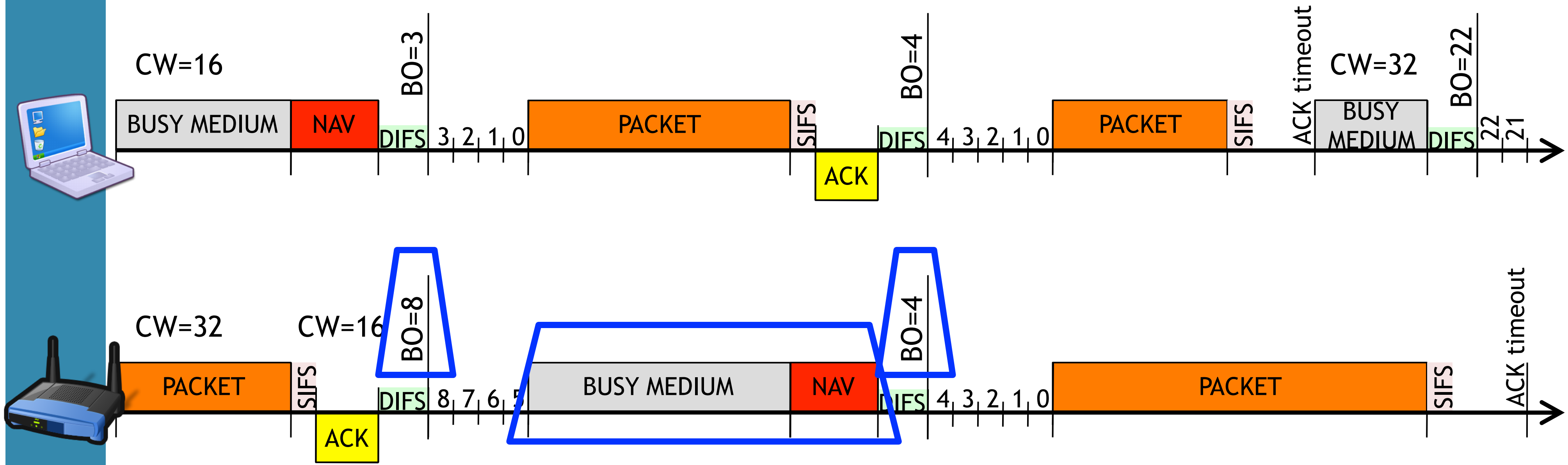


CW doubling after failure

CSMA/CA and channel contention/6



CSMA/CA and channel contention/7



Backoff Freeze, channel busy

CSMA/CA, Exponential Backoff rule

- BCKOFF value is computed after every tx attempt
  - BCKOFF taken from [0, 1, …, CW-1] with uniform distribution
- Contention Window (CW) refreshed
  - CW = 2 * CW if after tx attempt there is a collision
    - Up to CW_{max}, then stay with CW_{max}
  - CW = CW_{min} if after tx attempt, tx was acked by acknowledgment
- Standard values:
  - CW_{min} = 16/32, CW_{max} = 1024
- For tx a packet that requires ACK
  - Repeat access procedure up to MAX_{times} (e.g., 7), then discard packet
- This procedure guarantees network works correctly!!

CSMA/CA, pseudo-code

- Neglecting initializations:

procedura di trasmissione

```
while true do
        wait for packet
        wait for channel_idle_for_DIFS
        while channel_is_idle do
                BCKOFF--
                if BCKOFF == 0 then
                        send packet
                        wait for acknowledgement or timeout
                        if ack received then
                                reset CW
                                remove packet
                        else
                                grow CW
                        end if
                        BCKOFF = extract CW
                        leave do
                end fi
        end do
end do
```

Wireless LAN Standard

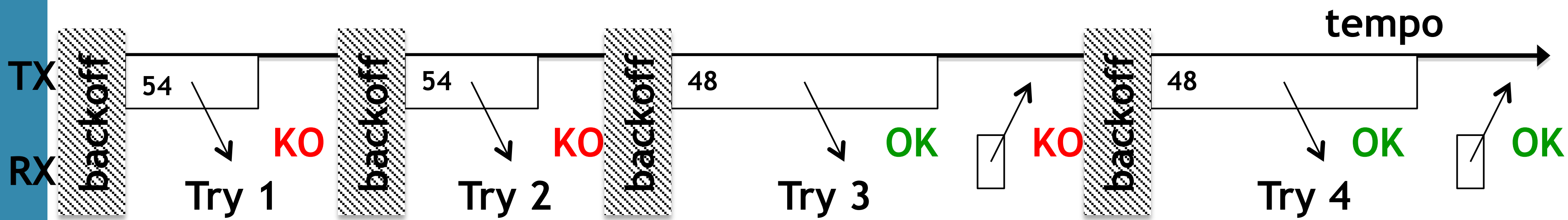
Rate control algorithm (super-quick)

IEEE 802.11bg: rate choice

- How to choose the rate is not specified by the standard
  - Rate Controller algorithm: RC
- RCs use feedback based techniques
- E.g. Minstrel algorithm, the default today in Linux kernel
  - Count total frames transmitted PER every rate, assess success probability
  - Rate that has best success delivery ratio is the winner
  - Periodically (every N frames) send a frame at a “look-around” rate
    - Constantly scan the entire rate set
  - Rely on frames that require ACK, by counting:
    - Number of attempts per packet
    - Failed rate, success rate

IEEE 802.11: rate choice/2

- Example: UDP packet
  - RC set up these rates: [54Mb/s{1,2},48Mb/s{3,4},12Mb/s{5},1Mb/s{6,7}]



  - At the end of this packet, RC refreshes its table…

Rate	Success	Failure
54	2812/3004 (93%)	192/3004 (7%)
48	408/507 (80%)	99/507 (20%)
36	102/402 (25%)	300/402 (75%)

Rate	Success	Failure
54	2812/3006 (93%)	194/3006 (7%)
48	409/509 (80%)	100/509 (20%)
36	102/402 (25%)	300/402 (75%)

- Don't change decision (not now ☺)

Bibliography

- [1] IEEE 802.11-2007, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 2007.
- [2] Tutorial on 802.11n from Cisco: http://www.wireshark.ch/download/Cisco_PSE_Day_2009.pdf
- [3] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function". IEEE Journal on Selected Areas in Communications, 18(3), pp. 535-547, 2000.