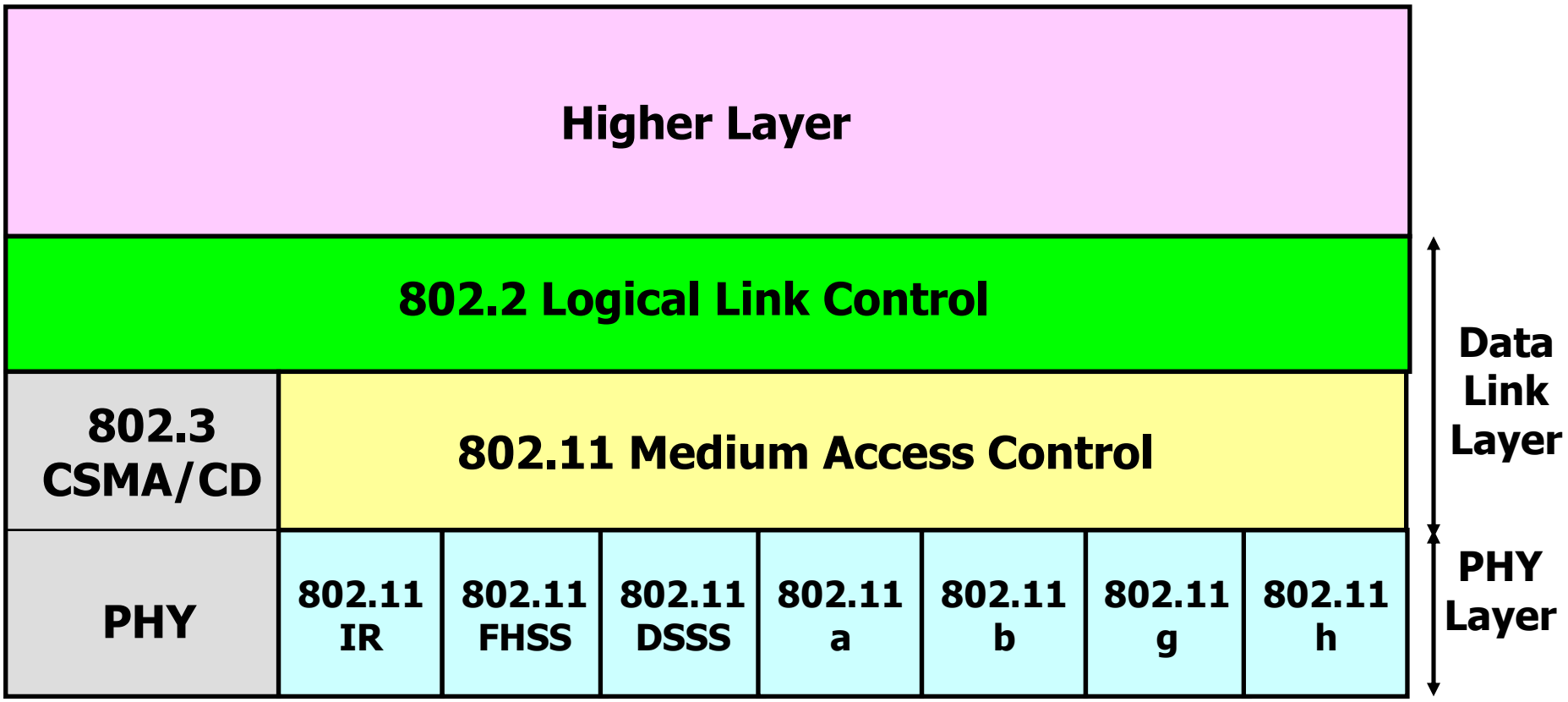
IEEE 802.11 frame format

Pietro Nicoletti
www.studioreti.it

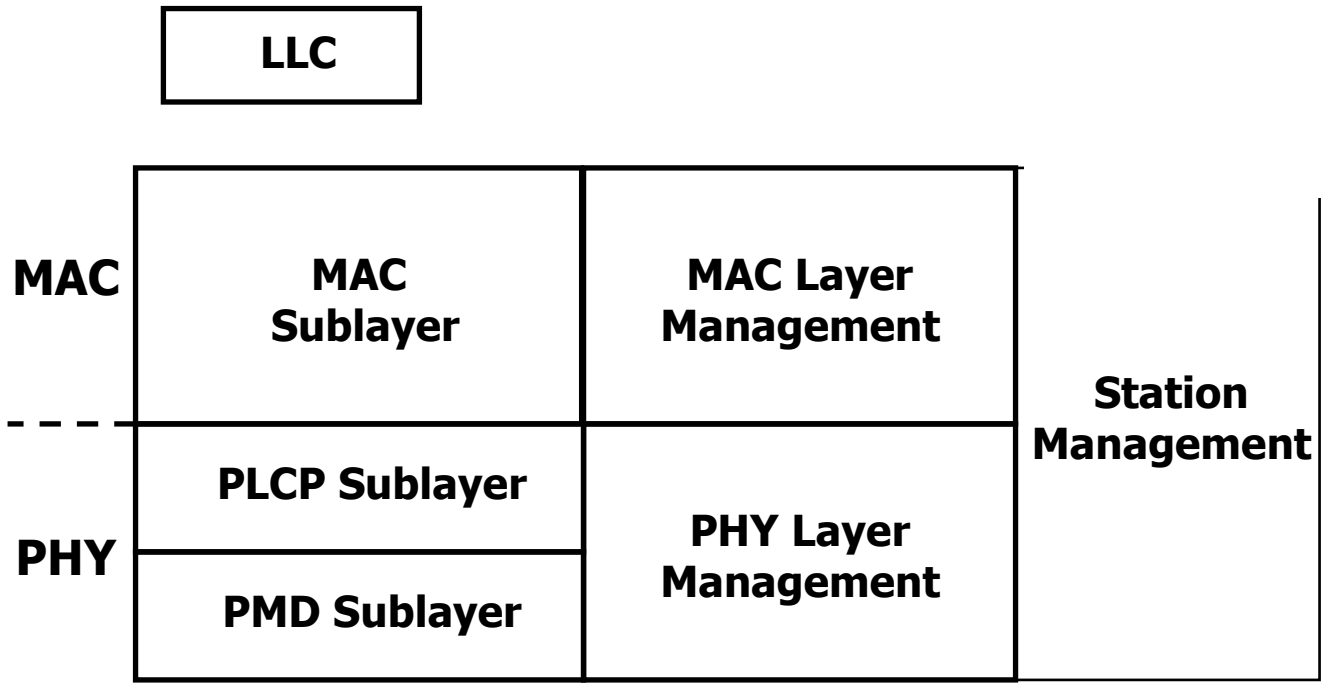
Copyright note

- These slides are protected by copyright and international treaties. The title and the copyrights concerning the slides (inclusive, but non only, every image, photograph, animation, video, audio, music and text) are the author's (see Page 1) property.
- The slides can be copied and used by research institutes, schools and universities affiliated to the Ministry of Public Instruction and the Ministry of University and Scientific Research and Technology, for institutional purpose, not for profit. In this case there is not requested any authorization.
- Any other complete or partial use or reproduction (inclusive, but not only, reproduction on discs, networks and printers) is forbidden without written authorization of the author in advance.
- The information contained in these slides are believed correct at the moment of publication. They are supplied only for didactic purpose and not to be used for installation-projects, products, networks etc. However, there might be changes without notice. The authors are not responsible for the content of the slides.
- In any case there can not be declared conformity with the information contained in these slides.
- In any case this note of copyright may never be removed and must be written also in case of partial use.

802.11 architecture and OSI model



802.11 architecture and OSI model

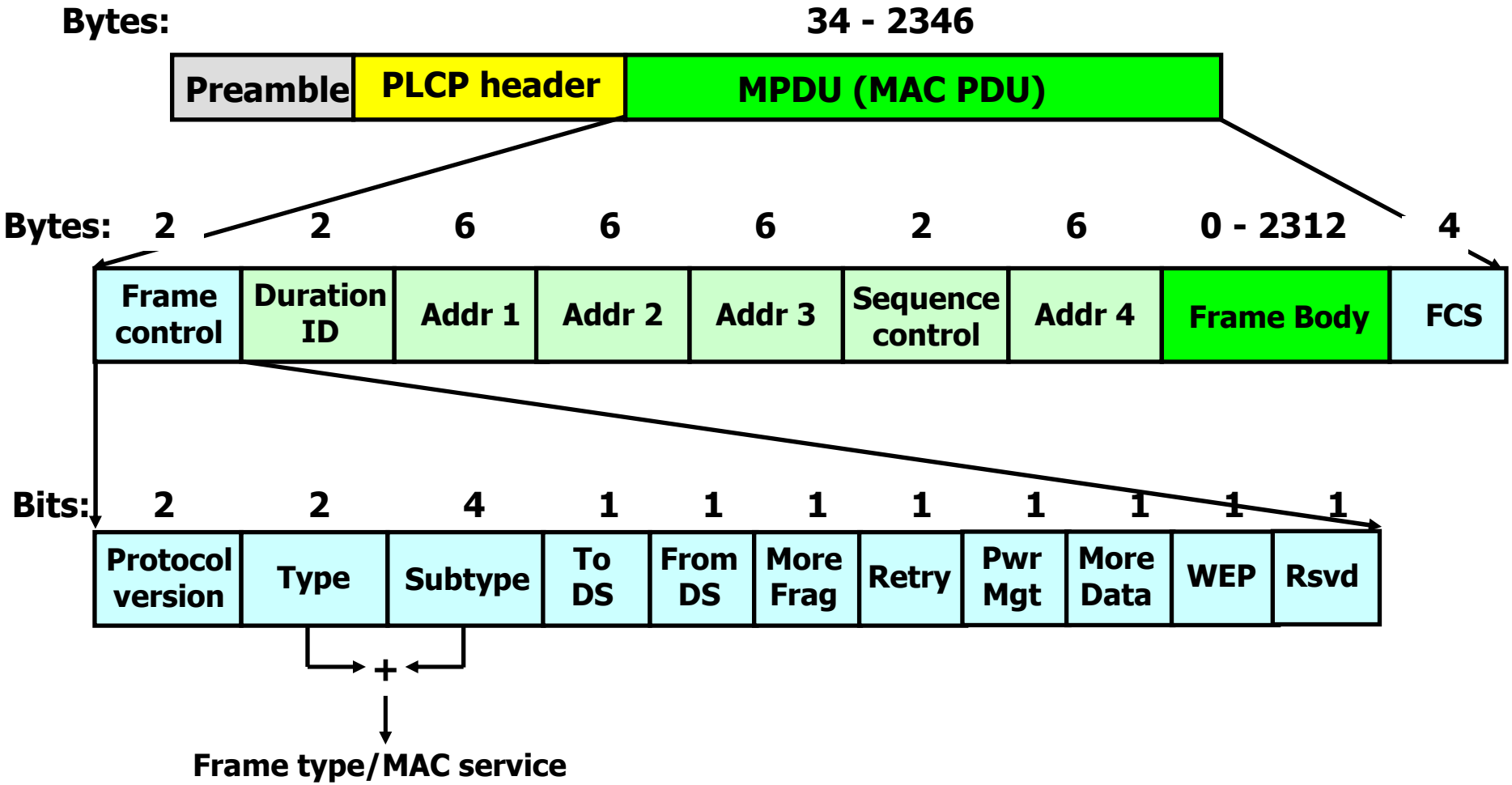


PLCP = Physical layer convergence procedure
PMD = Physical medium dipendent

PLCP: Physical layer convergence procedure

- Adaptation layer between Physical and MAC layers dependent by speed ad techique transmission
  - PLCP specific for FHSS
  - PLCP specific for DSSS in 802.11 (1 & 2 Mb/s)
  - PLCP specific for DSSS in 802.11a (from 6 to 54 Mb/s)
  - PLCP specific for DSSS in 802.11b (from 1 to 11 Mb/s)
  - PLCP specific for DSSS in 802.11g (from 1 to 54 Mb/s)
- Defin:
  - Operational speed
  - Modulation and coding

802.11 frame format



Frame Control field

- Protocol Version:
  - zero for 802.11 standard
- Type= frame type:
  - data, management, control
- Subtype = frame sub-type:
- ToDS:
  - When bit is set indicate that destination frame is for DS
- FromDS:
  - When bit is set indicate frame coming from DS

Frame Control field

- Retry:
  - Set in case of retransmission frame
- More fragments:
  - Set when frame is followed by other fragment
- Power Management
  - bit set when station go Power Save mode (PS)
- More Data:
  - When set means that AP have more buffered data for a station in Power Save mode

Frame Control field

- WEP:
  - When set indicate that in the Frame Body field there are datas need to processed by WEP algorithm.
- Order:
  - When set indicate restrictions for transmission

Frame type and MAC service

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110–0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101–1111	Reserved

Frame type and MAC service

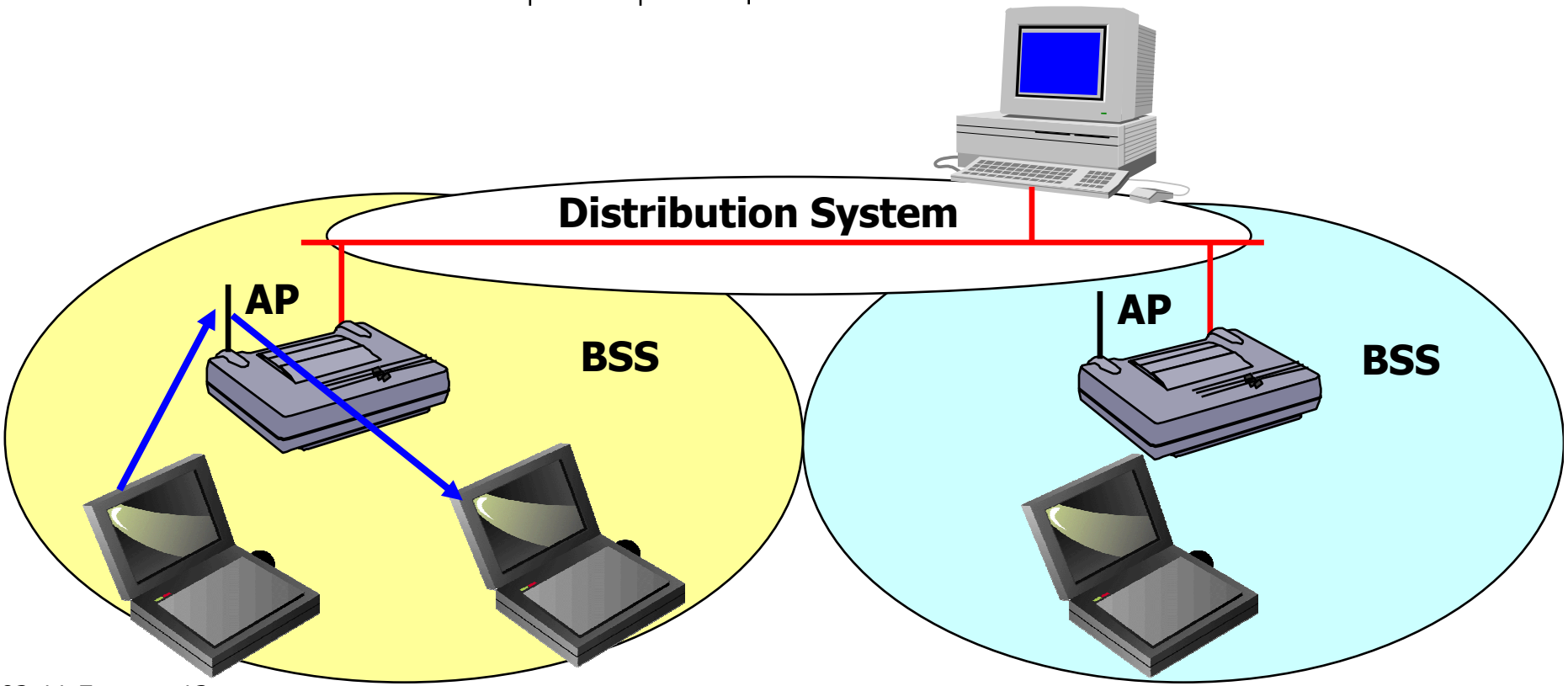
Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
01	Control	0000–1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Acknowledgment (ACK)
01	Control	1110	Contention-Free (CF)-End
01	Control	1111	CF-End + CF-Ack

Frame type and MAC service

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000–1111	Reserved
11	Reserved	0000–1111	Reserved

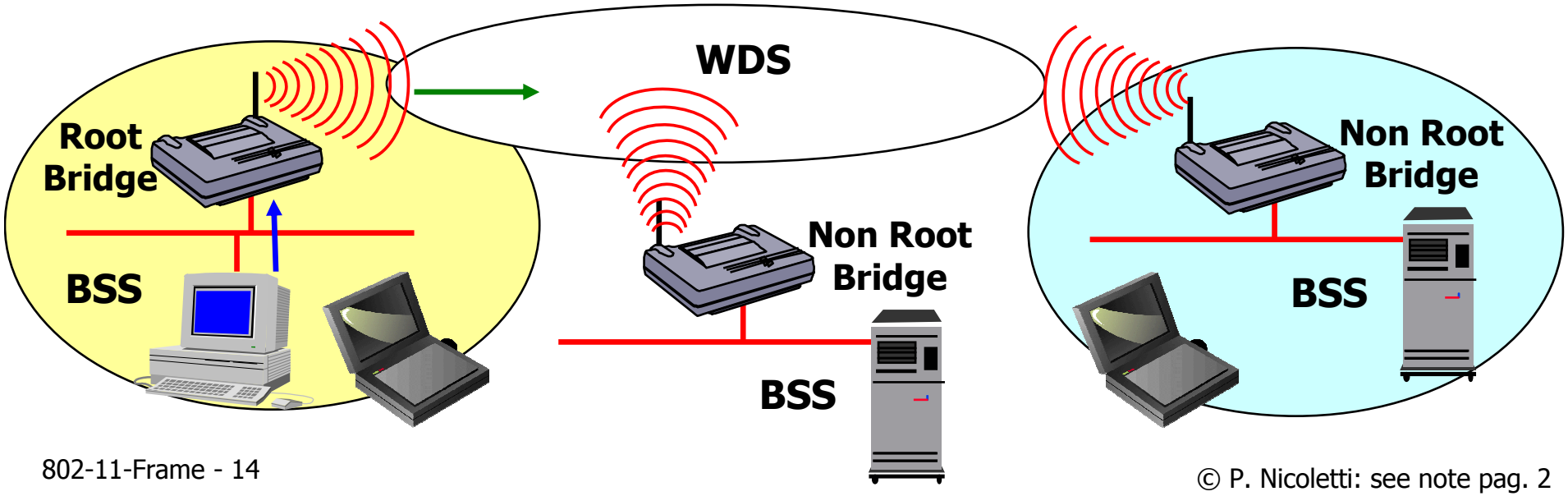
Transmission between station's in the same BSS

Bits:	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
				0	0						



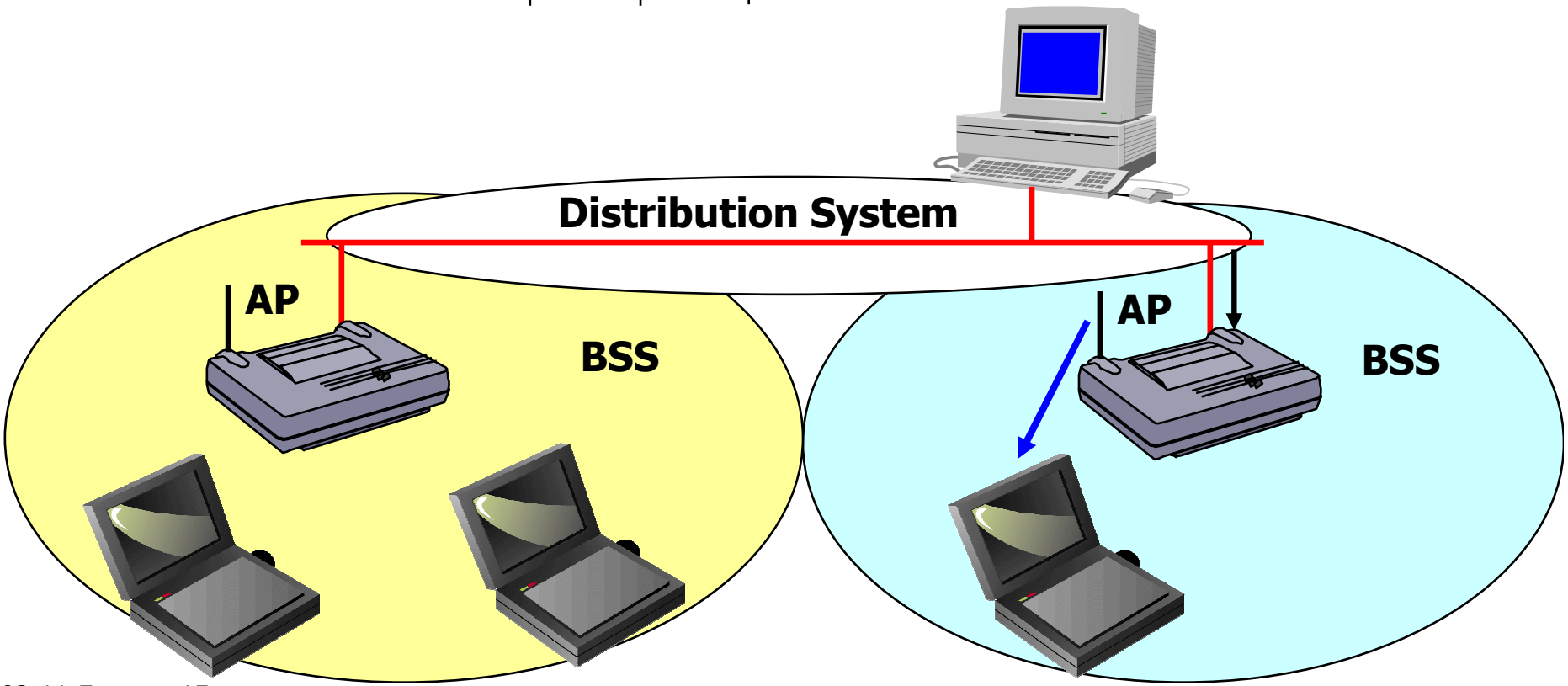
Frame transmission designated for Distribution System

Bits:	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
				1	0						



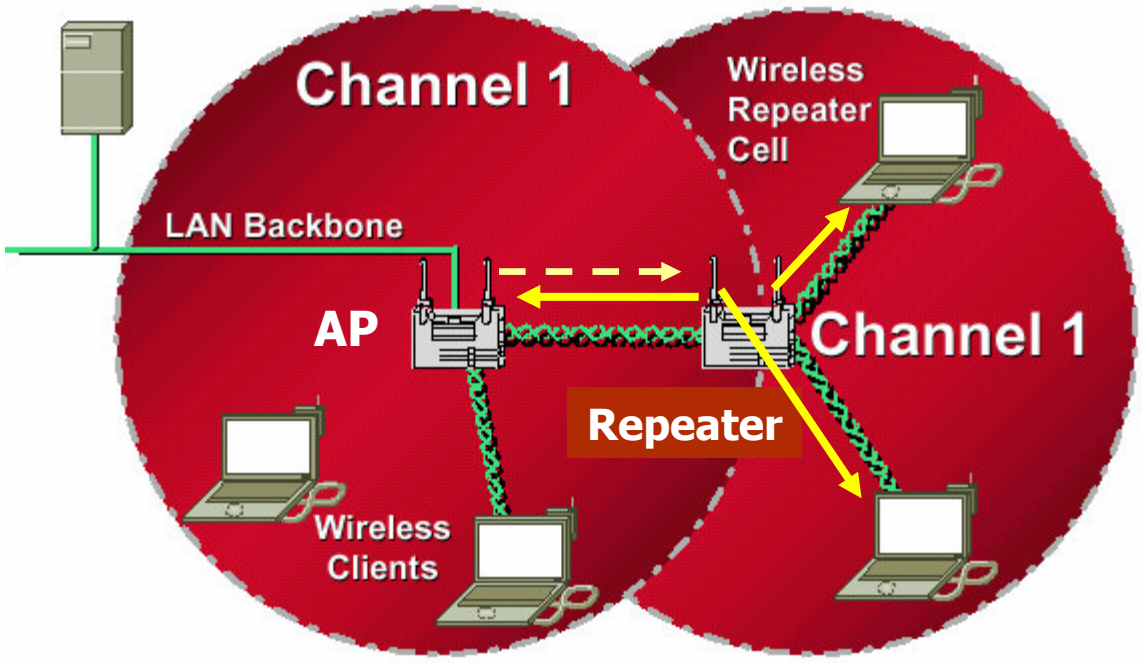
Frame transmission coming from Distribution System

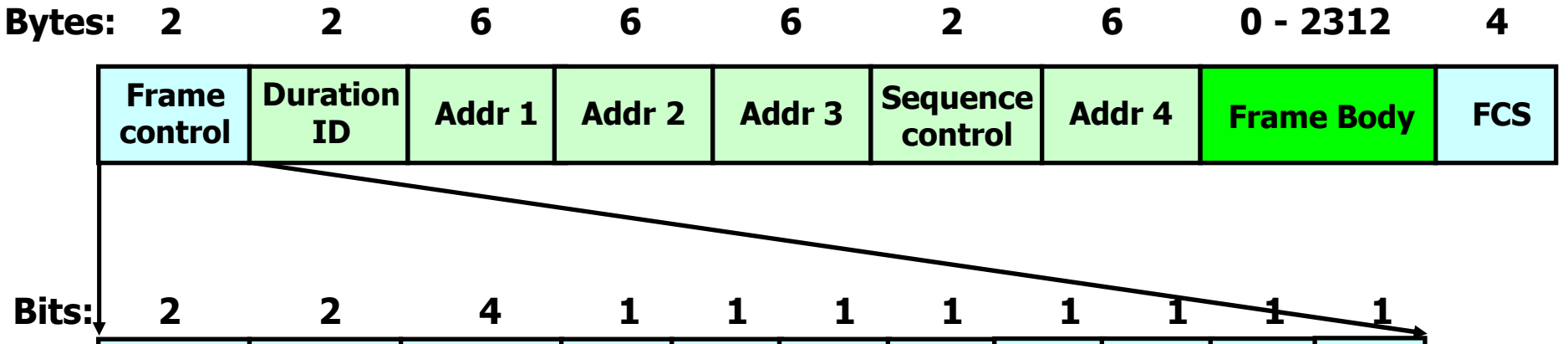
Bits:	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
				0	1						



Transmission designated to STA in other BSS, transmitted between AP trough Wireless Distribution System

Bits:	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
				1	1						





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

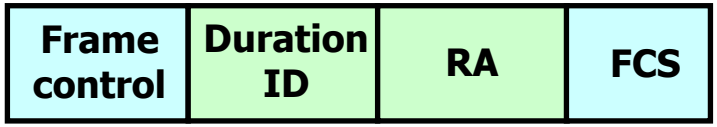
MAC address in 802.11

- DA = Destination MAC Address
- SA = Source MAC Address
- RA = Receiver Address indicate MAC Address of station in WM that have to receive frame
- TA = Transmitter Address indicate station wich have transmitted frame in WM
- BSSID

RTS & CTS

- RTS frame
  - Duration field contain value in μs of time need to transmit data or management + CTS + ACK + SIFS interval

- CTS Frame
  - Duration field contain value in μs obtained by previous RTS minus time need to transmit CTS and it SIFS interval



ACK & PS-Poll

- ACK frame:
  - Duration field contain value in μs obtained by previous data or management frame received miuns time need to transmit ACK and it SIFS interval

Frame control	Duration ID	RA	FCS

- PS-Poll frame:
  - AID field contain association ID

Frame control	AID	BSSID	TA	FCS

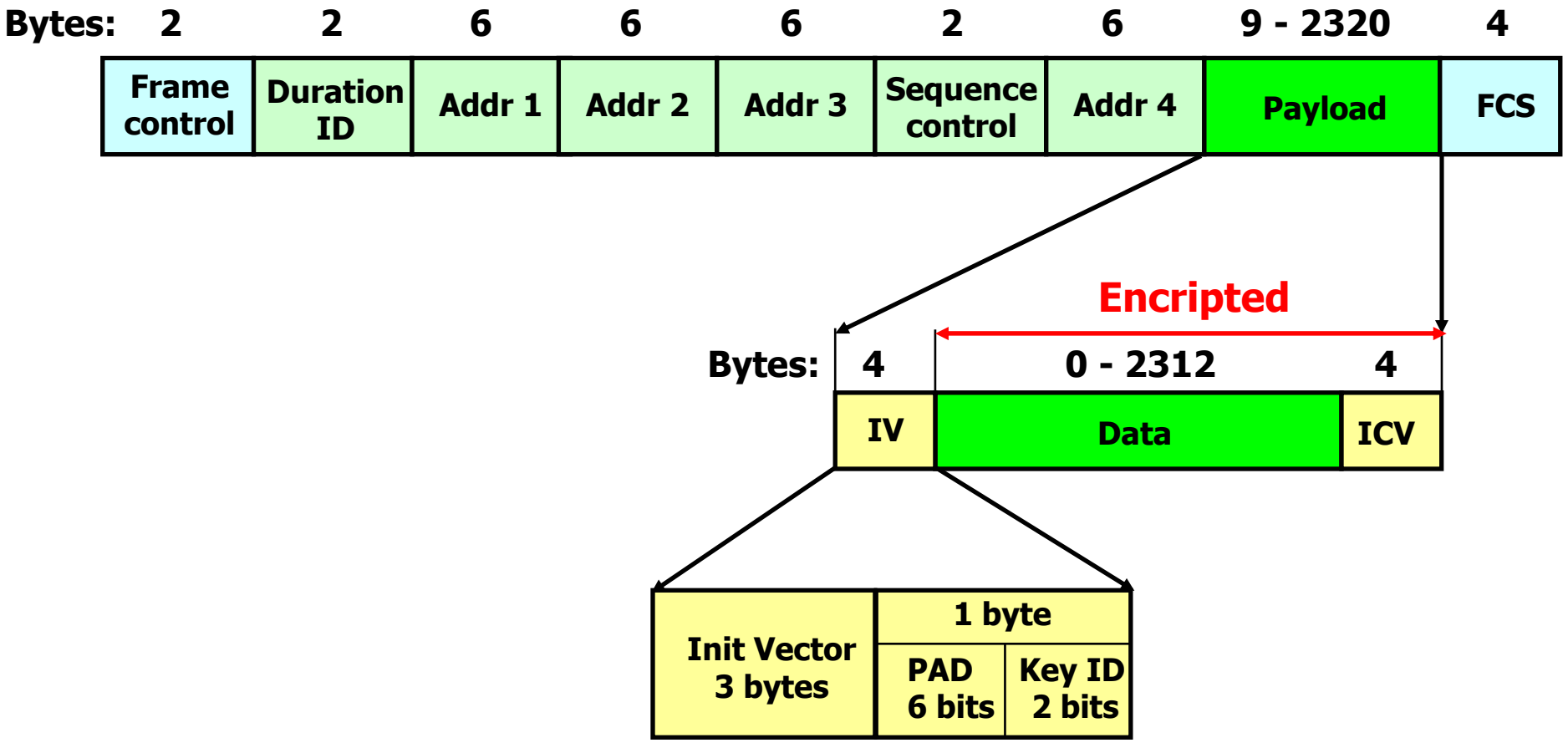
Beacon frame

Frame control	Duration ID	Addr 1	Addr 2	Addr 3	Sequence control	Addr 4	Frame Body	FCS

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set information element is present within Beacon frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	The DS Parameter Set information element is present within Beacon frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	The CF Parameter Set information element is only present within Beacon frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set information element is only present within Beacon frames generated by STAs in an IBSS.
10	TIM	The TIM information element is only present within Beacon frames generated by APs.

MSDU with WEP

- Extend Payload of 8 bytes



PLCP Header

- Contain information for adaptation between PMD e MAC layers
- Header change depending on specific PLCP for:
  - FHSS
  - PLCP specific for DSSS in 802.11 (1 & 2 Mb/s)
  - PLCP specific for DSSS in 802.11a (from 6 to 54 Mb/s)
  - PLCP specific for DSSS in 802.11b (from 1 to 11 Mb/s)
  - PLCP specific for DSSS in 802.11g (from 1 to 54 Mb/s)