CS5070/IITHYD

IEEE 802.11 MAC

Bheemarjuna Reddy Tamma

Adapted from Schiller's textbook on Mobile Communications and other sources

802.11 - MAC layer principles (1/2)

Traffic services

- Asynchronous Data Service (mandatory)
  - exchange of data packets based on “best-effort”
  - support of broadcast and multicast
- Time-Bounded Service (optional)
  - implemented using PCF (Point Coordination Function)

Access methods (called DFWMAC: Distributed Foundation Wireless MAC)

- DCF CSMA/CA (mandatory)
  - collision avoidance via randomized „back-off“ mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- DCF with RTS/CTS (optional)
  - avoids hidden terminal problem
- PCF (optional)
  - access point polls terminals according to a list

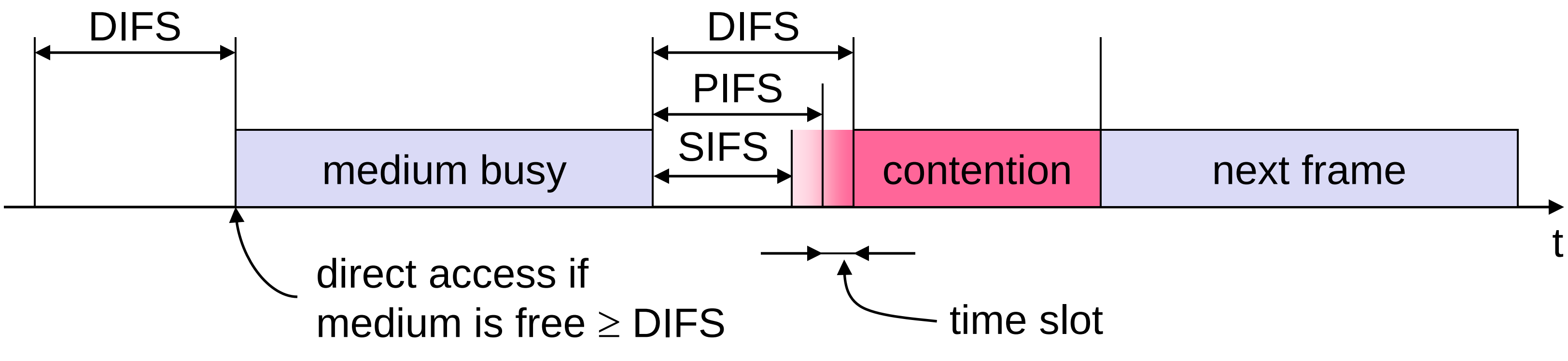
DCF: Distributed Coordination Function

PCF: Point Coordination Function

802.11 - MAC layer principles (2/2)

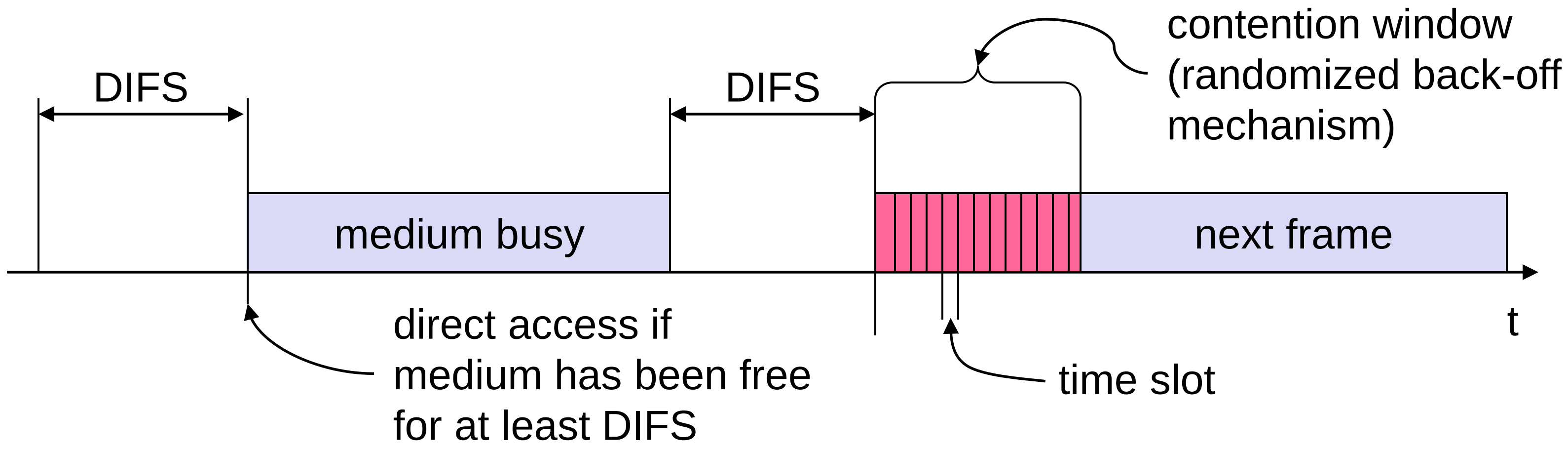
Priorities

- defined through different inter frame spaces
- no guaranteed, hard priorities
- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
  - lowest priority, for asynchronous data service



Note : IFS durations are specific to each PHY

802.11 - CSMA/CA principles



- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS (DIFS), then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (to increase fairness)

802.11 - CSMA/CA principles

Backoff Time = random(0, CW) * *slottime*

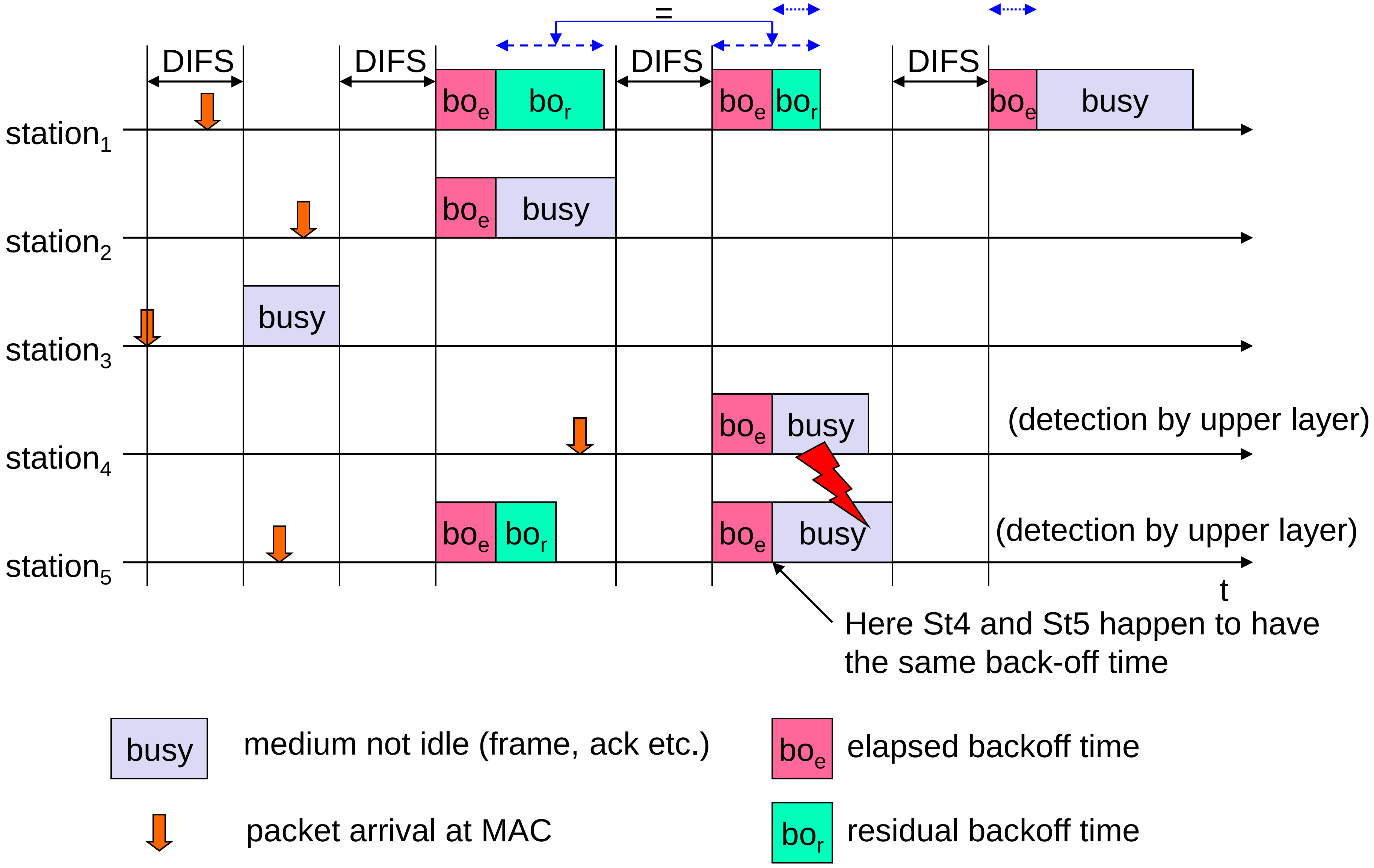
CW_{min} <= CW <= CW_{max}

slottime = Time needed for detecting a frame + Propagation delay + Time needed to switch from the Rx state to Tx state + Time to signal to the MAC layer the state of the channel

IEEE 802.11 parameters

Parameter	802.11 (FHSS)	802.11 (DSSS)	802.11b (HR/DSSS)	802.11a (OFDM)
$slotime$	50 μsec	20 μsec	20 μsec	9 μsec
SIFS	28 μsec	10 μsec	10 μsec	16 μsec
PIFS	SIFS $+t_{slot}$			
DIFS	SIFS$+(2 \times t_{slot})$			
Operating Frequency	2.4 GHz	2.4 GHz	2.4 GHz	5 GHz
Maximum Data Rate	2 Mbps	2 Mbps	11 Mbps	54 Mbps
CW_{min}	15	31	31	15
CW_{max}	1,023	1,023	1,023	1,023

802.11 – CSMA/CA broadcast



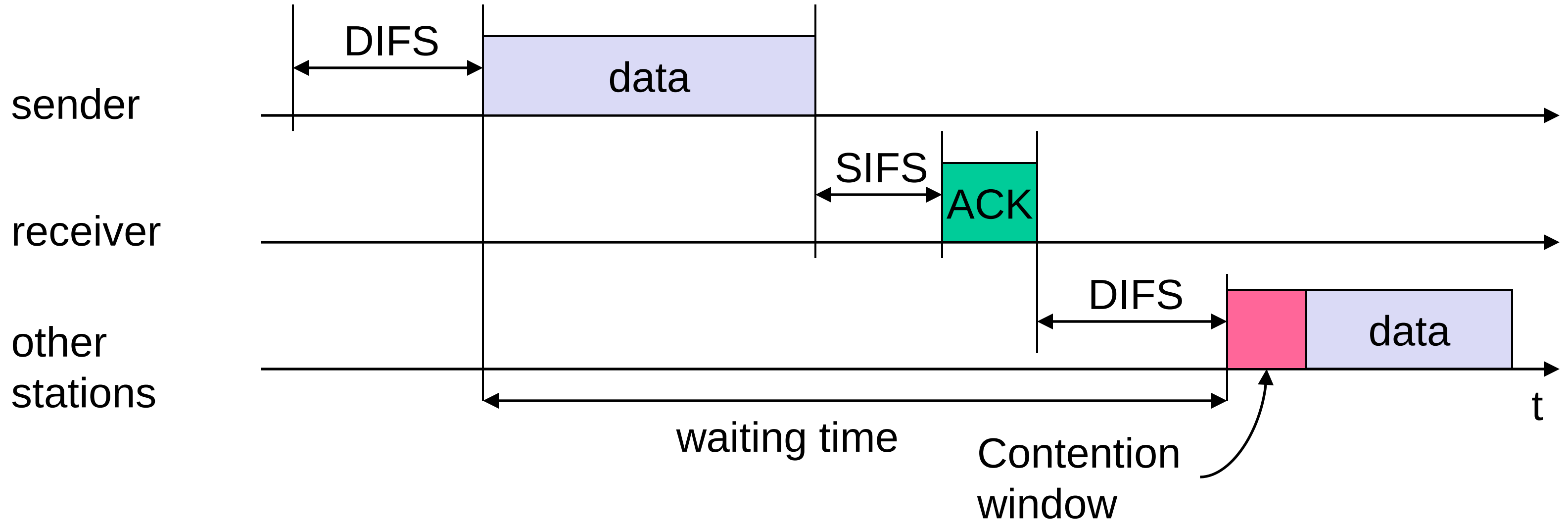
The size of the contention window can be adapted (if more collisions, then increase the size)

Note: broadcast is not acknowledged

802.11 - CSMA/CA unicast

Sending unicast packets

- station has to wait for DIFS before sending data
- receiver acknowledges at once (after waiting for SIFS) if the packet was received correctly (CRC)
- automatic retransmission of data packets in case of transmission errors

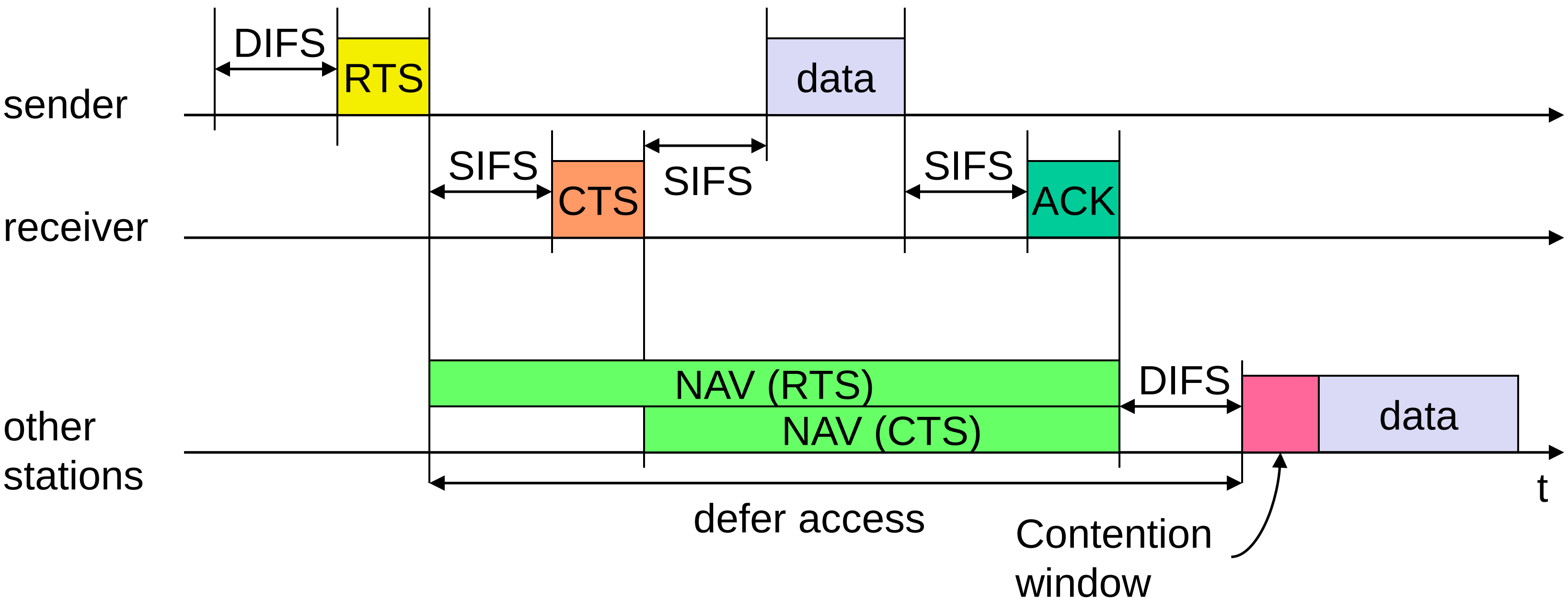


The ACK is sent right at the end of SIFS (no contention)

802.11 – DCF with RTS/CTS

Sending unicast packets

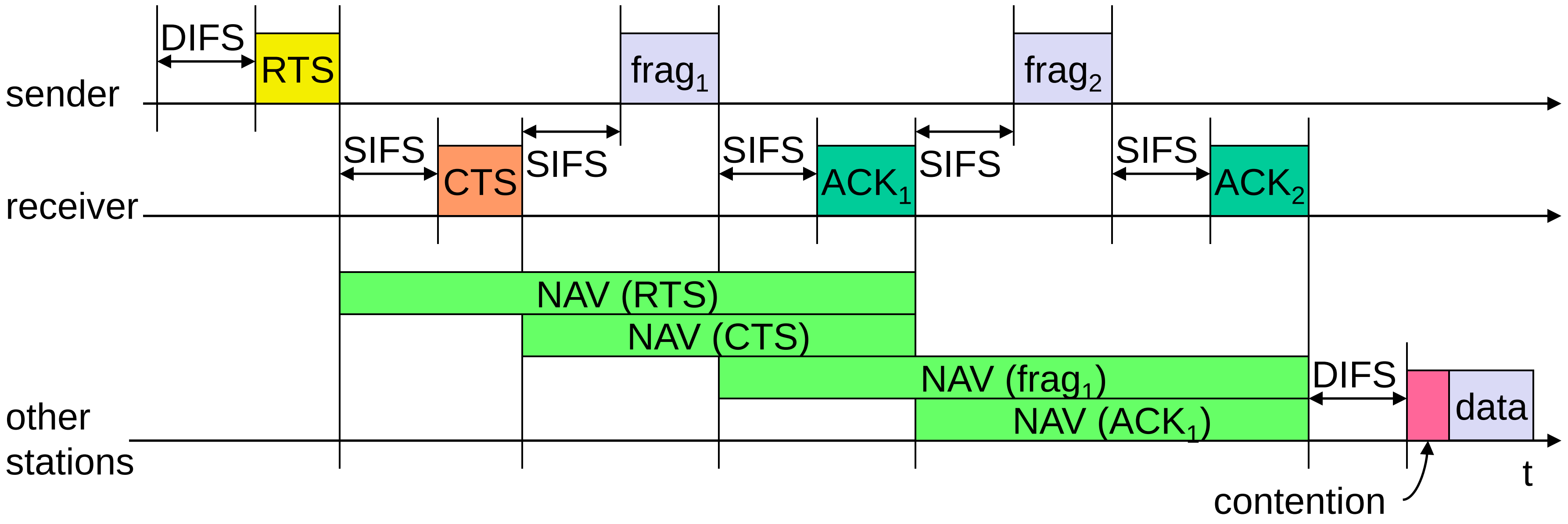
- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium reservations distributed via RTS and CTS



NAV: Net Allocation Vector

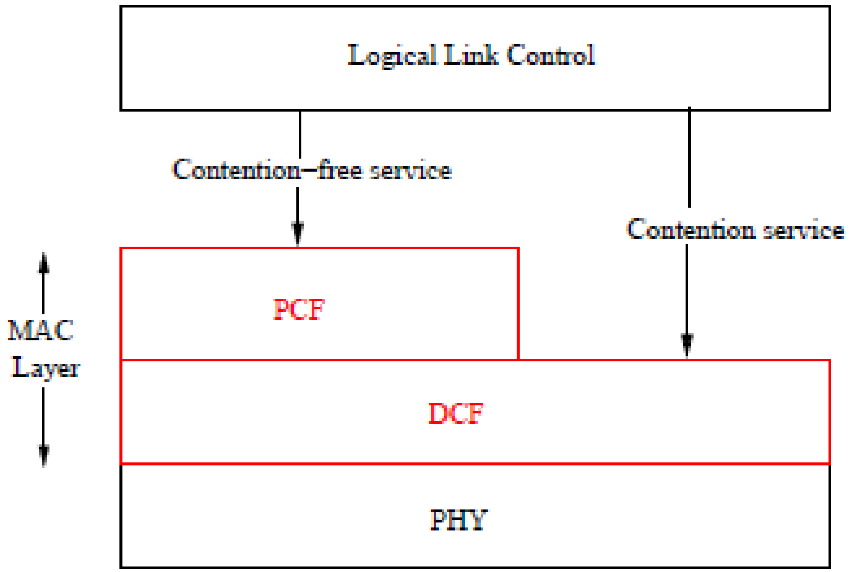
RTS/CTS can be present for some packets and not for other

Fragmentation mode



- Fragmentation is used in case the size of the packets sent has to be reduced (e.g., to diminish the probability of erroneous frames)
- Each $frag_i$ (except the last one) also contains a duration (as RTS does), which determines the duration of the NAV
- By this mechanism, fragments are sent in a row
- In this example, there are only 2 fragments

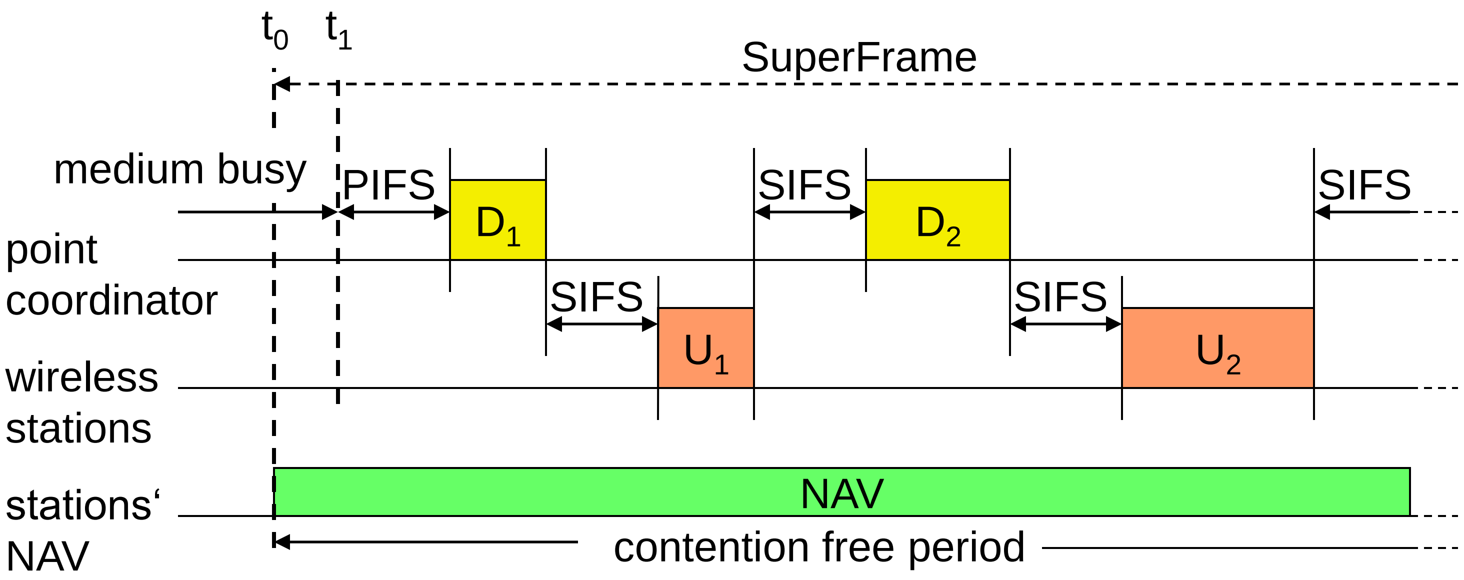
802.11 – Point Coordination Function (1/3)



IEEE 802.11 Protocol Architecture.

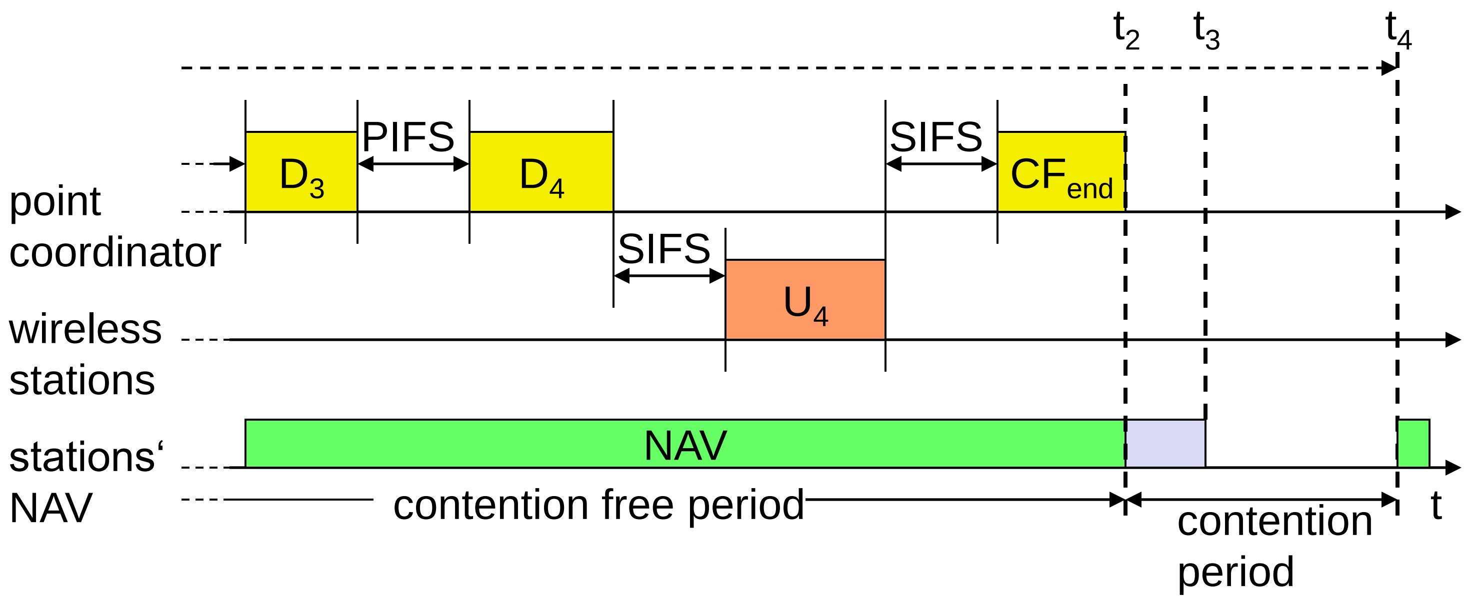
- PCF Provides a time-bounded service in WLANs
- But optional access method implemented on top of the DCF
- It requires a centralized controller (i.e., Point Coordinator) to coordinate the activity of stations
- Not usable for ad hoc networks

802.11 – Point Coordination Function (2/3)



- D_i represents the polling of station i
- U_i represents transmission of data from station i

802.11 – Point Coordination Function (3/3)



- In this example, station 3 has no data to send

802.11 - MAC Data frame format

Types

- control frames, management frames, data frames

Sequence numbers

- important against duplicated frames due to lost ACKs

Addresses

- receiver, transmitter (physical), BSS identifier, sender (logical)

Miscellaneous

- sending time, checksum, frame control, data

bytes	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	Data	CRC

Frame Control: version, type, fragmentation, security, ...

Sequence Control: detection of duplication

802.11 Frame Format

Frame Control

Frame Ctrl	Duration ID	Address 1	Address 2	Address 3	Seq	Address 4	Frame Body	FCS

Protocol	Type	Subtype	To DS	From DS	MF	Retry	Pwr Mgt	MD	Prot Frame	Order

Duration/ID Field

Depending on bits 14-15 (most significant) this field is defined one of three ways:

bit 0 … bit 15

															0

Network Allocation Vector (Duration)

0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Connection Free Period (CFP) Frames

AID (Range: 1–2007)	1	1

Power Save-Poll Frames

Address 1 Field

Used by the receiver.

Address 2 Field

Used by the transmitter.

Address 3 Field

Used by the receiver for filtering.

Sequence Number (Seq No) Field

Fragment Number	Sequence Number

Address 4 Field

Additional addressing used to traverse the Distribution System.

Frame Body Field

This is also known as the data body or packet payload. Higher level protocols and/or user application data reside in this field (length can be 0–2312 bytes).

Frame Check Sequence (FCS) Field

The FCS is often referred to as the cyclic redundancy check (CRC). It allows stations and APs to check the integrity of received frames.

QoS: Quality of Service
IBSS: Independent Basic Service Set
802.11h: Defines dynamic frequency selection (DFS) for spectrum management and transmit power control (TPC) for power management in the 5GHz band.

Protocol Field = 00

Type & Subtype Field

00 = Management
- 0000–Association Request
- 0001–Association Response
- 0010–Reassociation Request
- 0011–Reassociation Response
- 0100–Probe Request
- 0101–Probe Response
- 1000–Beacon
- 1001–Announcement Traffic Indication Message (ATIM)
- 1010–Disassociation
- 1011–Authentication
- 1100–Deauthentication
- 1101–Action (used for 802.11h & QoS)

01 = Control
- 1000–Block Acknowledgement Request (used for QoS)
- 1001–Block Acknowledgement (used for QoS)
- 1010–Power Save (PS) Poll
- 1011–Request to Send (RTS)
- 1100–Clear to Send (CTS)
- 1101–Acknowledgment (ACK)
- 1110–Contention Free (CF) End
- 1111–CF-end + CF-ACK

10 = Data
- 0000–Data
- 0001–Data + CF-ACK
- 0010–Data + CF-Poll
- 0011–Data + CF-ACK + CF-Poll
- 0100–Null Data
- 0101–CF-ACK
- 0110–CF-Poll*
- 0111–CF-ACK + CF-Poll*
- 1000–QoS Data
- 1001–QoS Data + CF-ACK
- 1010–QoS Data + CF-Poll
- 1011–QoS Data + CF-ACK + CF-Poll
- 1100–QoS Null*
- 1110–QoS CF-Poll*
- 1111–QoS CF-ACK + CF-Poll*

11 = Reserved

* *No data transmitted.*

To DS & From DS Fields

	To DS = 0	To DS = 1
From DS = 0	All Management and Control frames. Data frames within IBSS (never infrastructure data frames).	Data frames transmitted from a wireless station in an infrastructure network to the DS.
From DS = 1	Data frames received from the DS for a wireless station in an infrastructure network.	Frames within a distribution system.

All Other Frame Control Fields

More Fragments (MF)
1 = additional fragments to follow
0 = last frame

Retry
1 = this packet is a retransmission
0 = this packet is not a retransmission

Protected Frame (Prot Frame)
1 = the frame is protected with link layer security such as WEP or WPA/2
0 = the frame is transmitted as clear text

More Data (MD)
1 = indicates to the stations the AP has at least one frame buffered for the station
0 = no buffered packets in the AP for the station

Order
1 = strict ordering supported
0 = strict ordering not supported

Power Management (Pwr Mgt)
1 = station is in power save mode
0 = station is active (out of power save mode)

Source: Xirrus Inc. Tutorial: **802.11a/b/g Demystified**

MAC address format

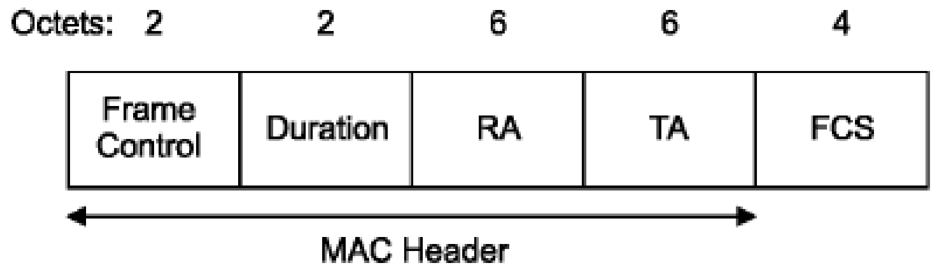
scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution System
Address1: Physical recipient of frame
Address2: Physical transmitter of frame
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
- infrastructure BSS : MAC address of the Access Point
- ad hoc BSS (IBSS): random number

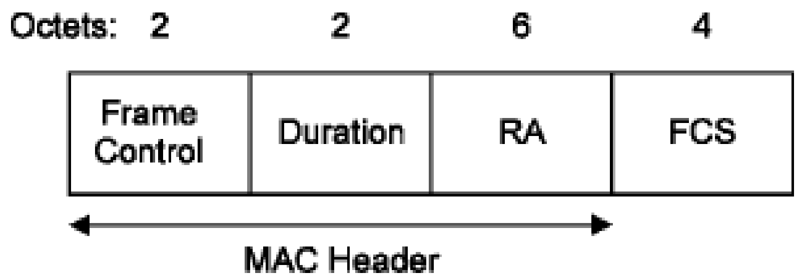
RA: Receiver Address
TA: Transmitter Address

Control Frame Formats

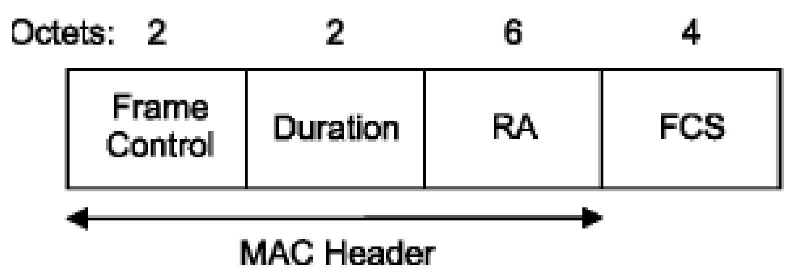
- RTS



- CTS



- ACK



802.11 - MAC management

- Synchronization
  - Purpose
    - for the physical layer (e.g., maintaining in sync the frequency hop sequence in the case of FHSS)
    - for power management
  - Principle: beacons with time stamps
- Power management
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements
- Association/Reassociation
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
  - scanning, i.e. active search for a network
- MIB - Management Information Base
  - managing, read, write

Beacon Frame Format

Octets: 2	2	6	6	6	2	0 - 2312	4
Frame Control	Duration	Address 1 (DA)	SA	BSSID	Sequence Control	Frame Body	FCS

MAC Header

Frame Body contains:

Timestamp

Beacon Interval

Cabability

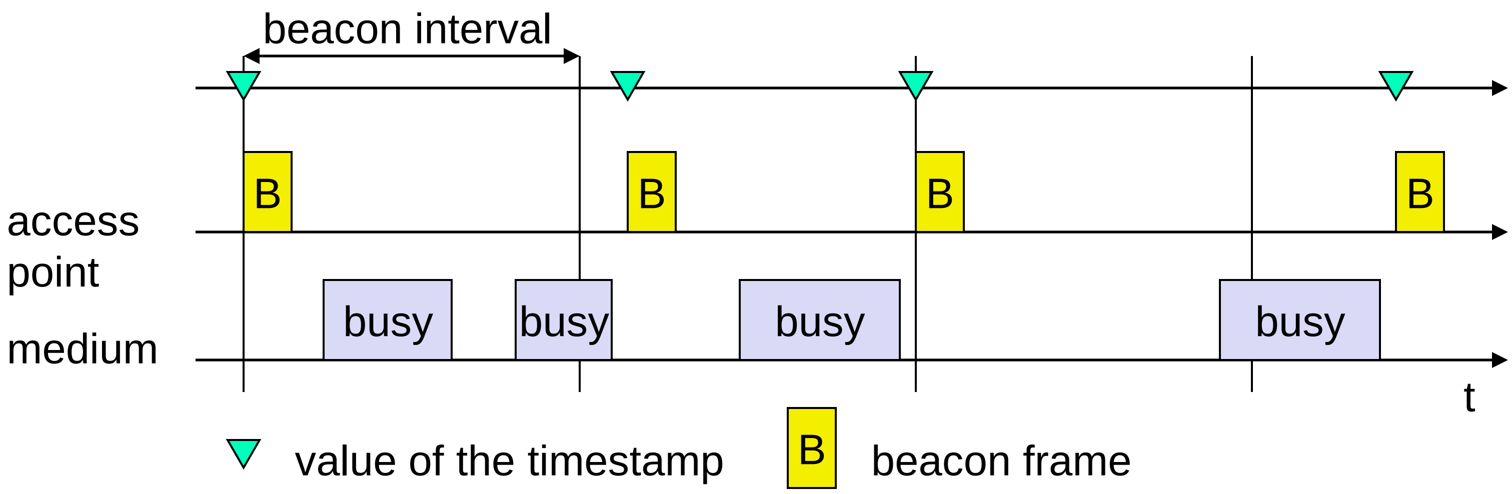
SSID

Supported PHY Data Rates

FH/DS/CF/IBSS Parameter Set

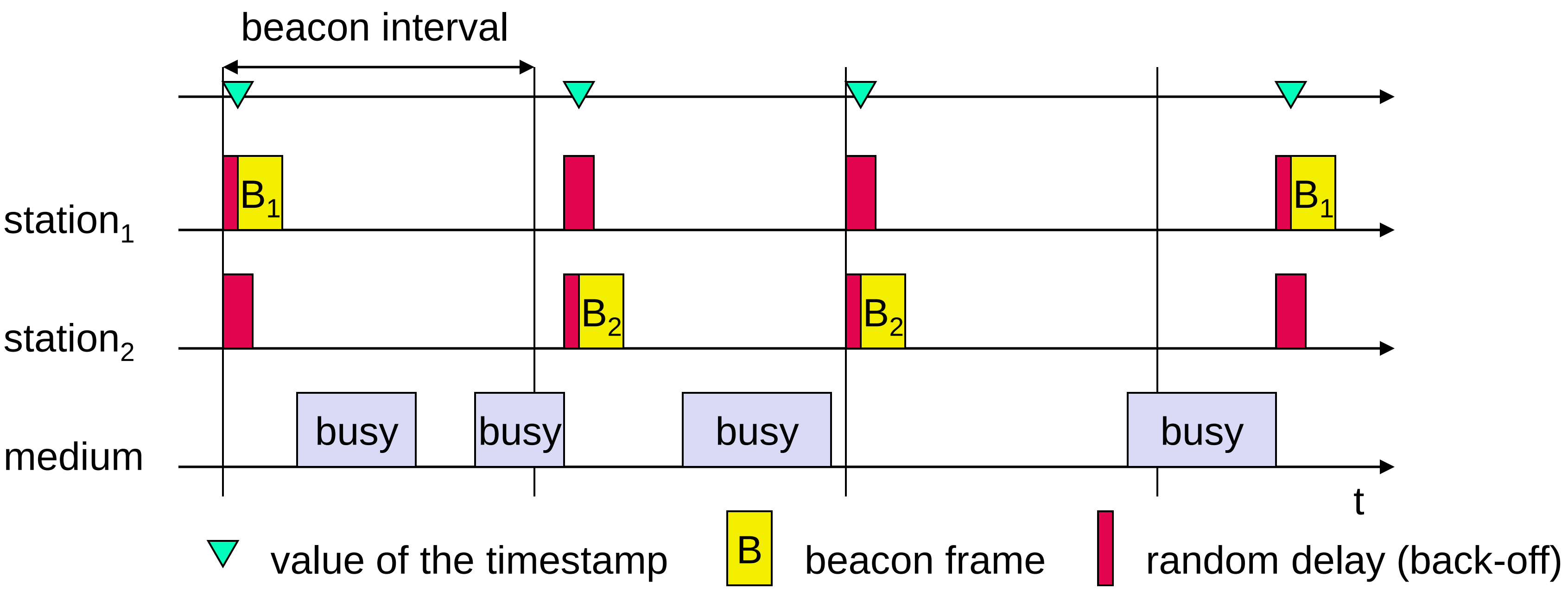
TIM, Country, BSS Load, QoS Capability, Vendor specific, etc

Synchronization (infrastructure case)



- The access point transmits the (quasi) periodic beacon signal
- The beacon contains a timestamp and other management information used for power management and roaming
- All other wireless nodes adjust their local timers to the timestamp

Synchronization (ad-hoc case)

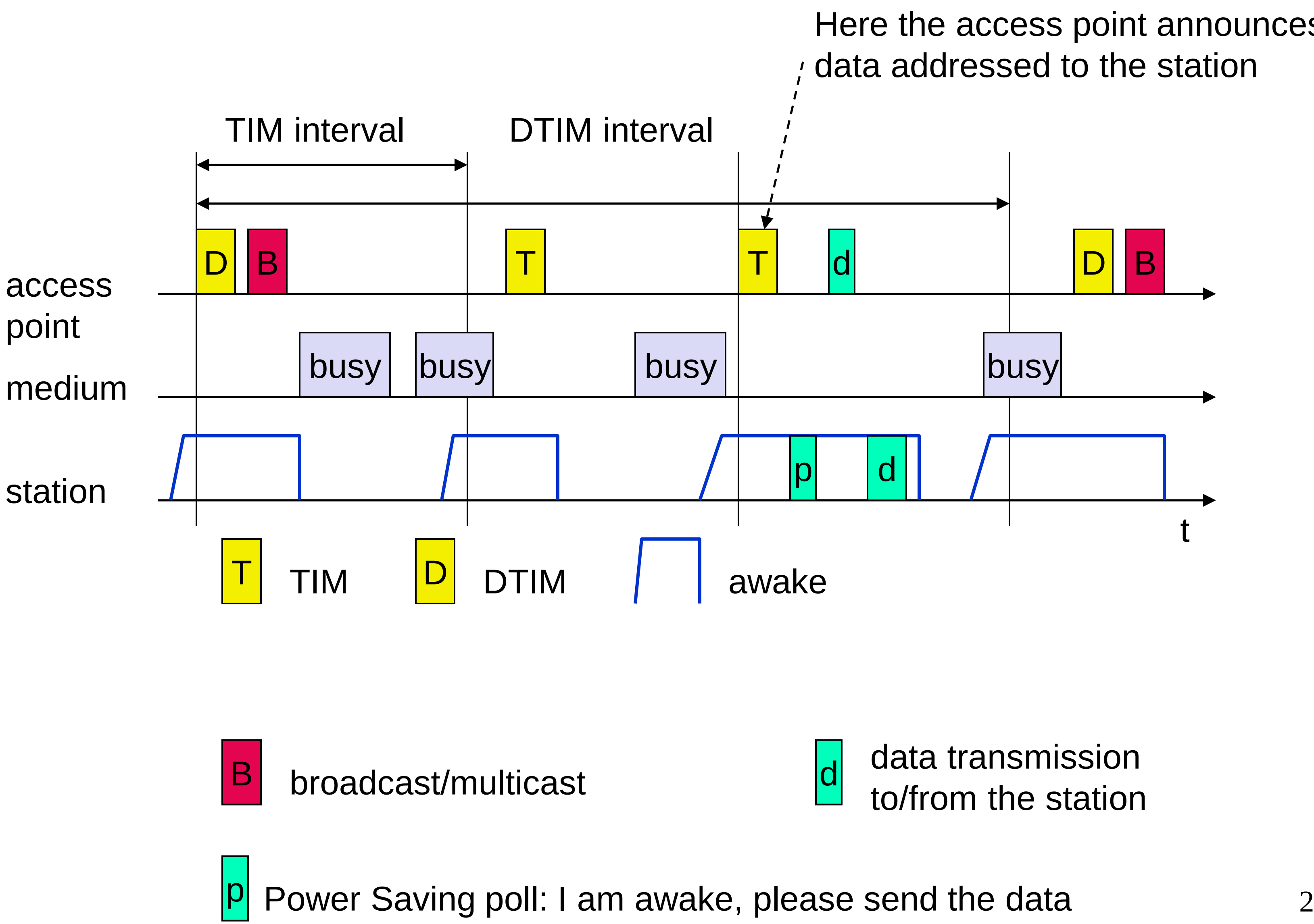


- Each node maintains its own synchronization timer and starts the transmission of a beacon frame after the beacon interval
- Contention ➔ back-off mechanism ➔ only 1 beacon wins
- All other stations adjust their internal clock according to the received beacon and suppress their beacon for the current cycle

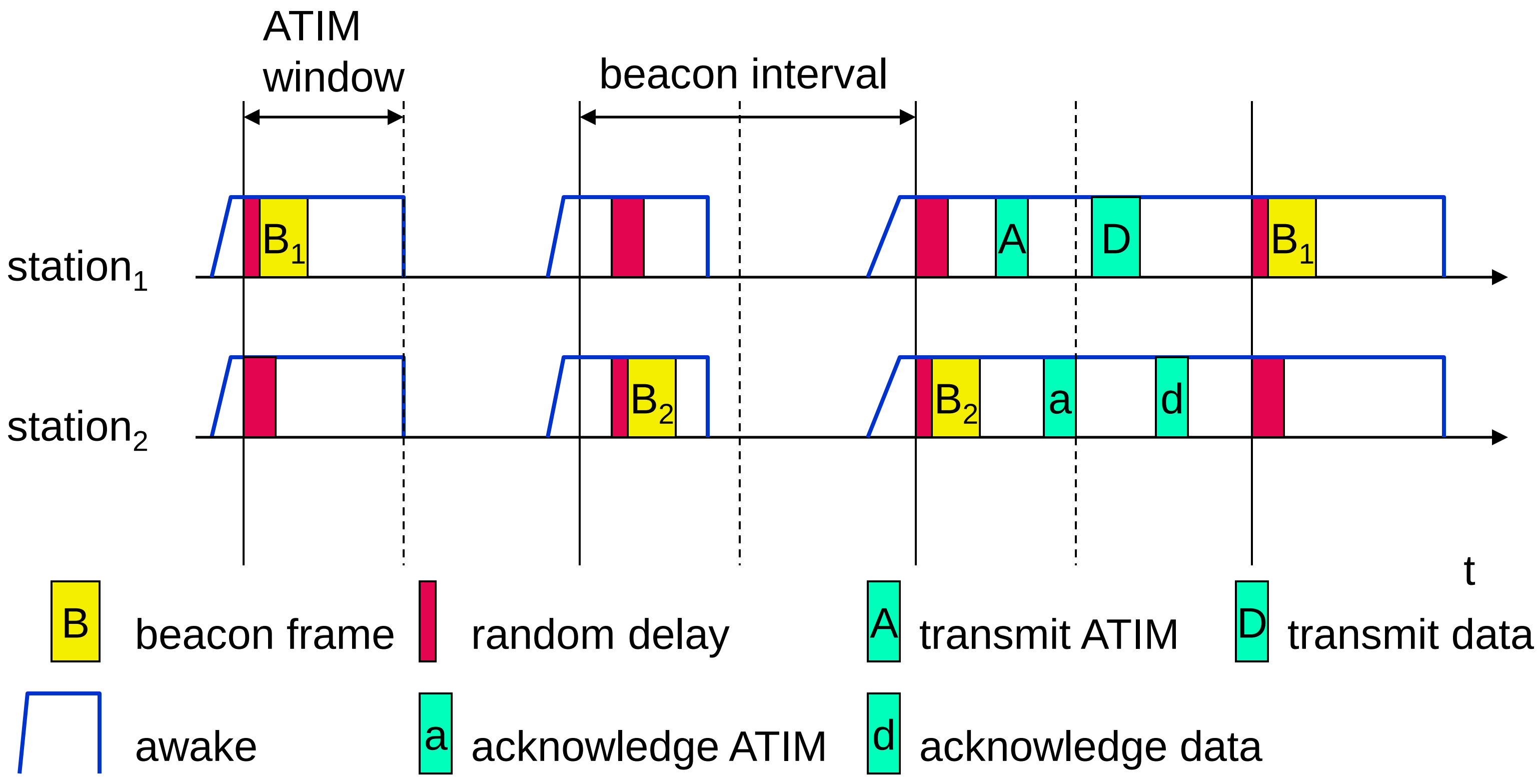
Power management

- Idea: switch the transceiver off if not needed
- States of a station: sleep and awake
- Timing Synchronization Function (TSF)
  - stations wake up at the same time
- Infrastructure case
  - Traffic Indication Map (TIM)
    - list of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)
    - list of broadcast/multicast receivers transmitted by AP
- Ad-hoc case
  - Ad-hoc Traffic Indication Map (ATIM)
    - announcement of receivers by stations buffering frames
    - more complicated - no central AP
    - collision of ATIMs possible (scalability?)

Power saving (infrastructure case)



Power saving (ad-hoc case)



- ATIM: Ad hoc Traffic Indication Map (a station announces the list of buffered frames)
- Potential problem: scalability (high number of collisions)

802.11 - Roaming

No or bad connection? Then perform:

Scanning

- scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer

Reassociation Request

- station sends a request to one or several AP(s)

Reassociation Response

- success: AP has answered, station can now participate
- failure: continue scanning

AP accepts Reassociation Request

- signal the new station to the distribution system
- the distribution system updates its data base (i.e., location information)
- typically, the distribution system now informs the old AP so it can release resources

Inter-Access Point Protocol (802.11f)

- Compatible solution for Roaming between different vendors' APs
- Load-balancing between APs

How does a STA join an existing BSS?

- STA needs to get synchronization info from the AP of BSS
  - Active scanning (Probe-REQ/Probe-Response)
  - Passive scanning (listen for beacons)
- Association with AP
  - Association REQ/Association Response
  - STA capabilities, PCF requirements, Power-saving mode, etc
- Authentication with AP
  - Authentication REQ/Authentication Response

IEEE 802.11 – Standardization efforts

IEEE 802.11b

- 2.4 GHz band
- DSSS (Direct-sequence spread spectrum)
- Bitrates 1 – 11 Mbit/s

IEEE 802.11a

- 5 GHz band
- Based on OFDM (orthogonal frequency-division multiplexing)
- transmission rates up to 54 Mbit/s
- Coverage is not as good as in 802.11b

IEEE 802.11g

- 2.4 GHz band (same as 802.11b)
- Based on OFDM
- Bitrates up to 54Mb/s

IEEE 802.11n

- MIMO (multiple-input multiple-output)
- 40MHz channel (instead of 20MHz)
- Can operate in the 5GHz or 2.4Ghz (risk of interference with other systems, however)
- Bitrates up to 600Mb/s

IEEE 802.11i

- Security, makes use of IEEE 802.1x

IEEE 802.11p

- For vehicular communications

IEEE 802.11s

- For mesh networks

IEEE 802.11 Channel Allocation

Channel Allocation

2.4GHz Channel Allocation

Channel	Frequency f_c (MHz)	U.S.	EU	Japan
1	2412	X	X	X
2	2417	X	X	X
3	2422	X	X	X
4	2427	X	X	X
5	2432	X	X	X
6	2437	X	X	X
7	2442	X	X	X
8	2447	X	X	X
9	2452	X	X	X
10	2457	X	X	X
11	2462	X	X	X
12	2467		X	X
13	2472		X	X
14	2484			X

5GHz Channel Allocation

Channel	Frequency f_c (MHz)	U.S.	EU	Japan
184	4920			X
188	4940			X
192	4960			X
196	4980			X
208	5040			X
212	5060			X
216	5080			X
36	5180	X	X	X
40	5200	X	X	X
44	5220	X	X	X

Channel	Frequency f_c (MHz)	U.S.	EU	Japan
48	5240	X	X	X
52	5260	X	X	X
56	5280	X	X	X
60	5300	X	X	X
64	5320	X	X	X
100	5500	X	X	
104	5520	X	X	
108	5540	X	X	
112	5560	X	X	
116	5580	X	X	

Channel	Frequency f_c (MHz)	U.S.	EU	Japan
120	5600	X	X	
124	5620	X	X	
128	5640	X	X	
132	5660	X	X	
136	5680	X	X	
140	5700	X	X	
149	5745	X		
153	5765	X		
157	5785	X		
161	5805	X		

Source: Xirrus Inc. Tutorial: **802.11a/b/g Demystified**