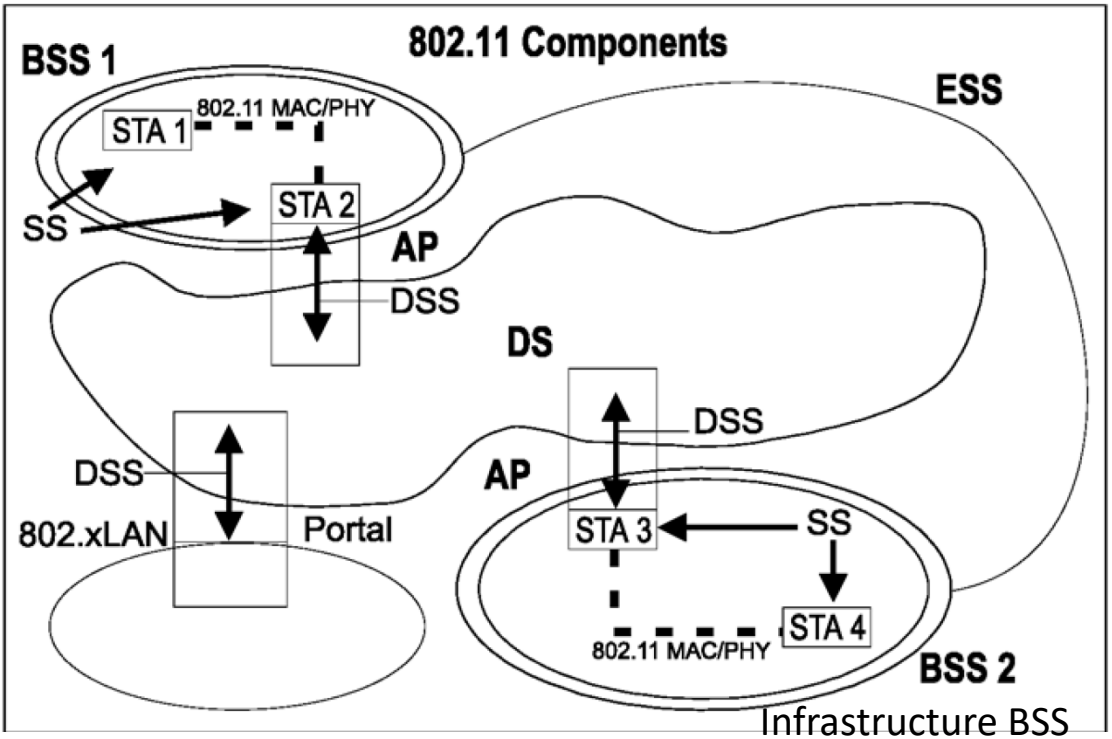
WLAN Technology. MAC Layer Functionality.

Wireless Local Area Networks Part 2

Based on:

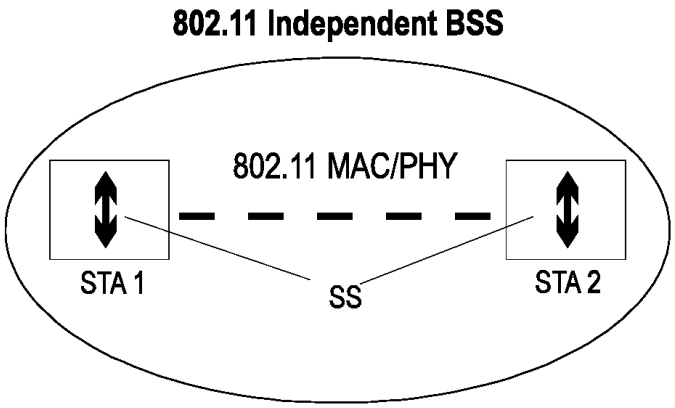
- Ivan Marsic: Computer Networks, Ch. 1.5.3 and 6.3.1 (Moodle)
- C. Beard & W. Stallings (2016), Wireless Communications Networks and Systems, Chapter 11:Wireless LAN Technology
- IEEE 802.11-2012 standard (Moodle)
- Wikipedia

Architectures of 802.11 networks



Infrastructure BSS

- STA - Station
- BSS - Basic Service Set
- ESS - Extended Service Set
- DS - Distribution System
- Portal
- In ESS stations are connected through the **Access Point** and the Distribution System

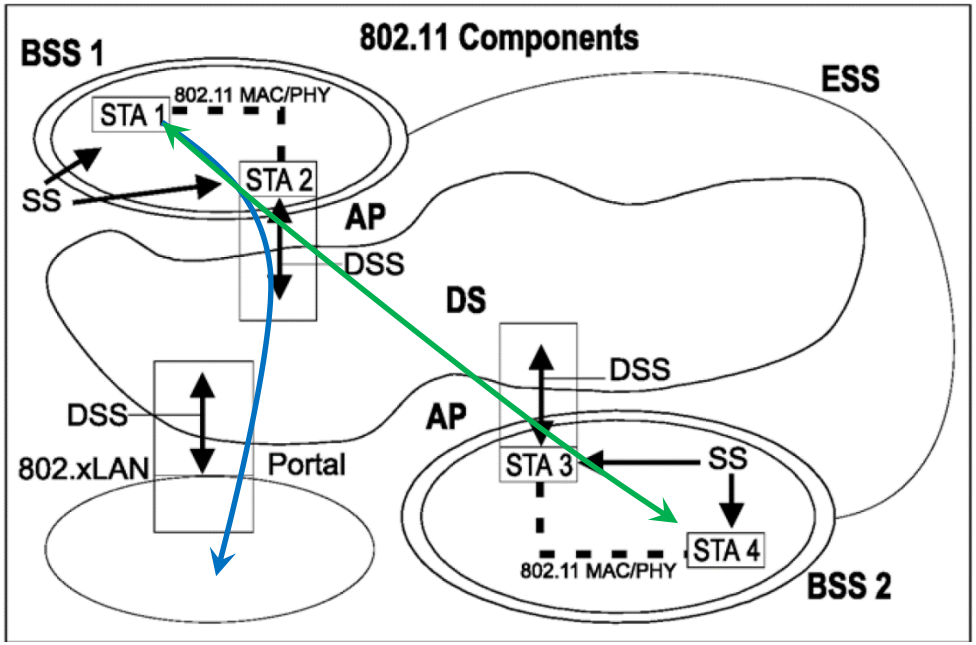


- In the Independent BSSs (IBSS), aka **ad-hoc,** networks stations are connected directly
- Independent BSSs can be extended into **mesh networks**

Logical services

SS – Station services:

- MSU delivery
- Authentication
- Data Confidentiality
- Radio measurements



DSS – Distribution System Services:

- Association
- Distribution
- Integration

The Reference model and General Frame structure

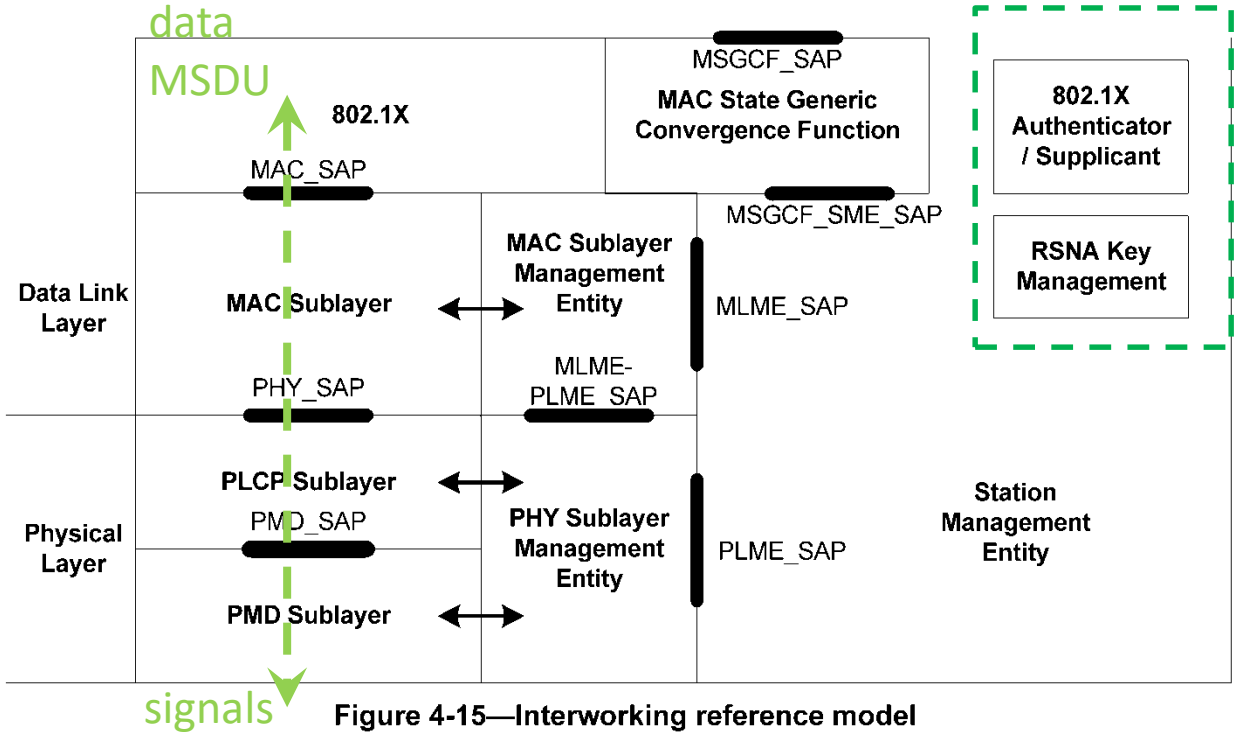
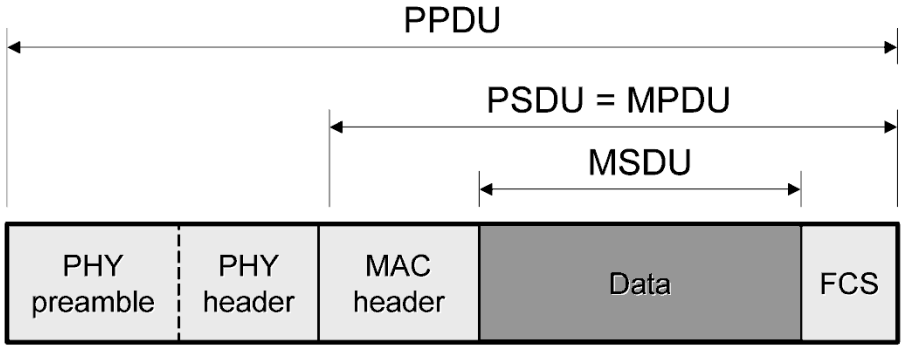


Figure 4-15—Interworking reference model

- Medium Access Control (MAC) sublayer
- Physical (PHY) layer
  - PLCP (convergence procedure
  - PMD (Medium dependent)
- MAC and PHY management Entities
- SAPs service access points



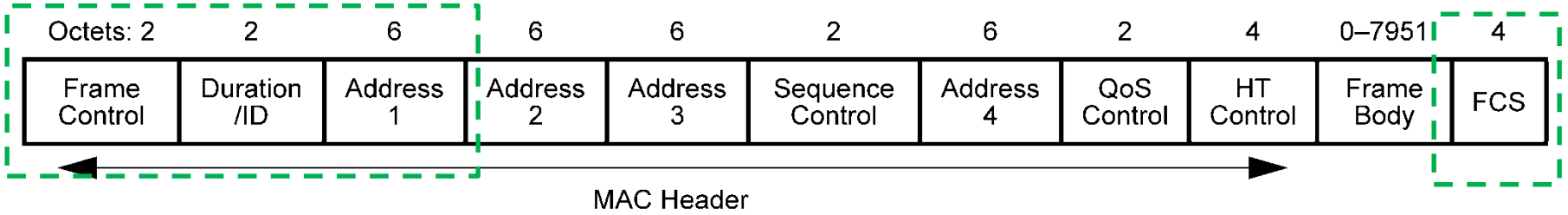
Key:
PPDU = PLCP protocol data unit
PSDU = PLCP service data unit
MPDU = MAC protocol data unit
MSDU = MAC service data unit

PLCP = physical (PHY) layer convergence procedure
MAC = medium access control

Aggregated frames A-MSDU possible

General MAC Frame format

Figure 8.1



- The first three fields (Frame Control, Duration/ID, and Address 1), 10 bytes, and the last field (FCS), 4 bytes, constitute the minimal frame format and are present in all frames.
- The fields Address 2, Address 3, Sequence Control, Address 4, QoS Control, HT Control, and Frame Body are present only in certain frame types and subtypes.
- There are three general types of frames related to three types of services and specified by 6 bits from the **Frame Control** field
  - Data Frames
  - Control Frames
  - Management Frames

Selected by bits B7-B2 in the Type-Subtype field of the Frame Control field

The Basic Medium Access Protocol – DCF

- The wireless medium is shared by all stations present in the coverage area, hence, frames from different stations can crash.
- The fundamental access method to the wireless medium (MAC) implemented in all IEEE 802.11 STAs is a
  - **Distributed Coordination Function** (DCF) also known as
  - **Carrier Sense Multiple Access** with **Collision Avoidance** (CSMA/CA).

The basic rules of the medium access are:

- For a STA to transmit, it must **sense the medium** to determine if another STA is transmitting.
- If the medium is not busy, the transmission may proceed.
- If the medium is busy, the collision avoidance procedure is followed.
- Time gaps between transmissions, known as **interframe spacing times**, allow a number of stations to share the medium.

MAC architecture – Access Methods

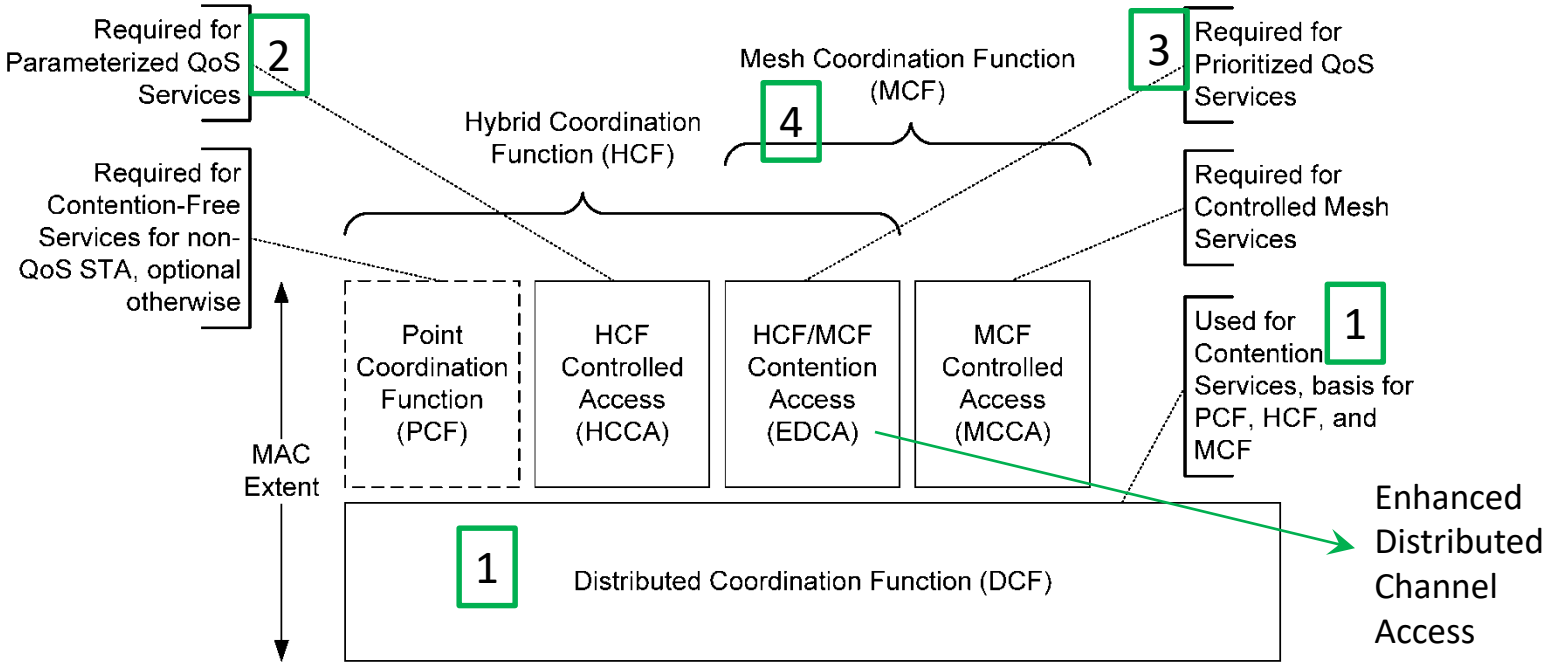


Figure 9-1—MAC architecture

- Two groups of methods: **Contention** access and **Controlled** access
- DCF aka CSMA/CA (contention access) is the basic access method on which all other methods are built.
- Hybrid Coordination Function (HCF) is used in the QoS and Mesh services
- Mesh Coordination Function (MCF) is used in Mesh Services

Interframe spacing (IFS) times

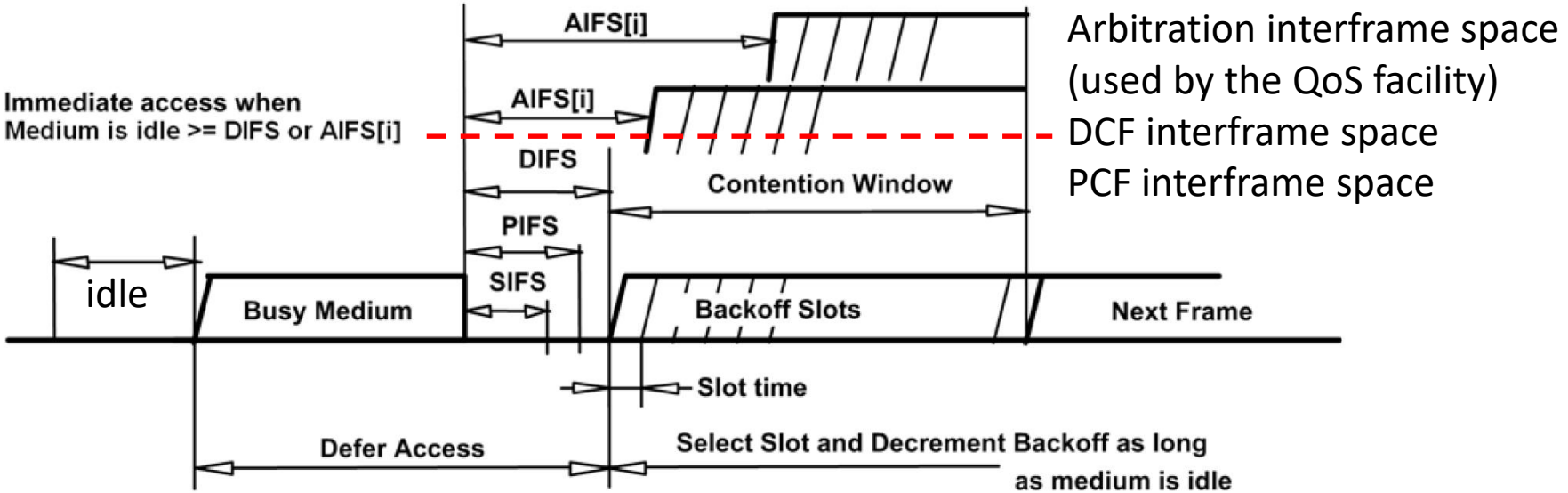
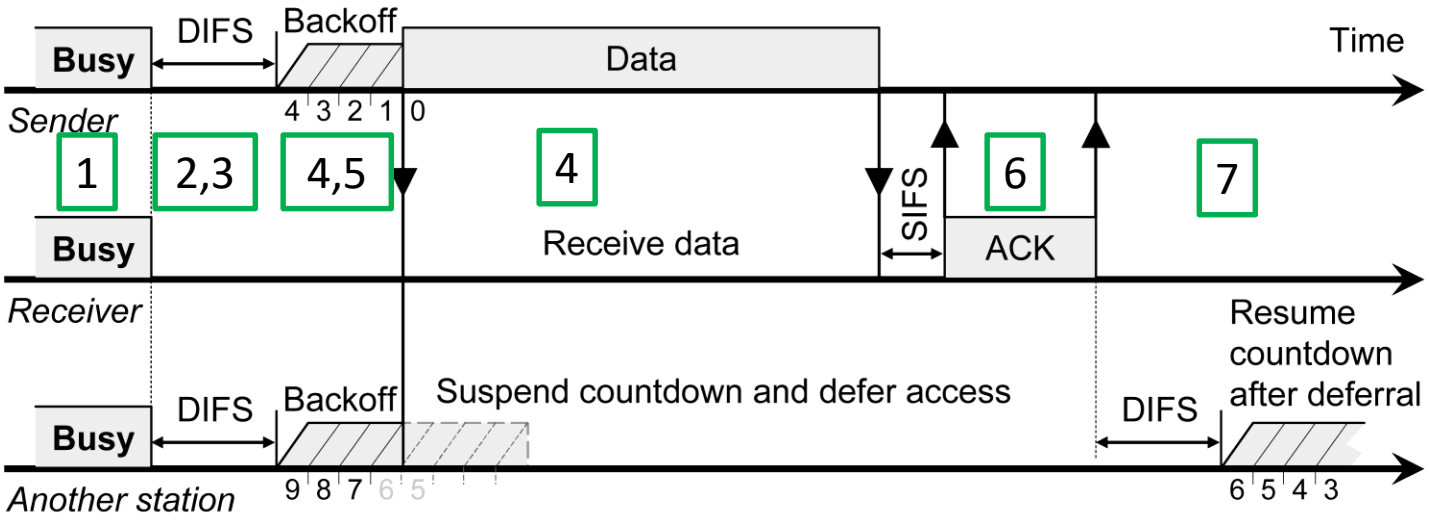


Figure 9-3—Some IFS relationships

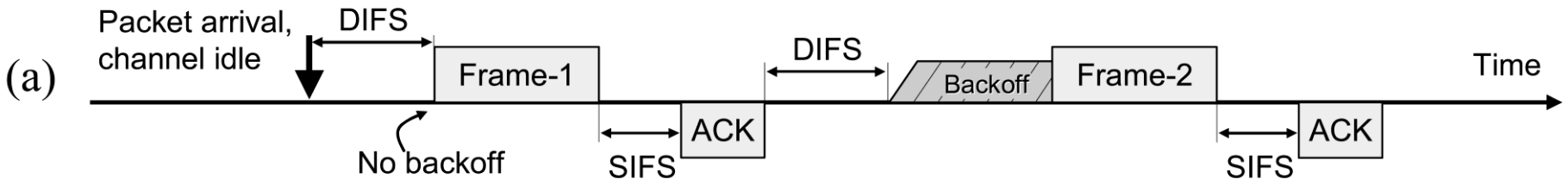
- Medium Access methods are specified in terms of IFS time intervals.
- The slot time ($t_s \approx$ 10µs) is the shortest time.
- The short interframe spacing (SIFS) is determined by the physical properties of the medium and can be ≈ 10µs
- PIFS = SIFS + t_s , DIFS = SIFS + $2t_s$
- Note: the **idle** time, the **defer access** time and the **backoff** time

DCF Transmission example



1. The **Sender**, **Receiver** and **Another Station** observe the medium (Carrier Sense)
2. At some point the Sender and Another Station observe that the medium is available.
3. They wait for the DIFS time and generate a random number of time slots (**backoff counter**). In the example: 4 for the sender and 9 for the other station.
4. The backoff counter is being decremented every slot time and when it reaches zero, the **Sender transmits** the data.
5. The other station suspends the count down
6. After the receiver receives the correct data (as confirmed by the FCS), it waits for the SIFS time and generate the Acknowledgment (ACK) frame destined to the sender.
7. The other station see the ACK frame and when the transmission is completed, it waits for the DIFS time and resumes the count down of its backoff counter.

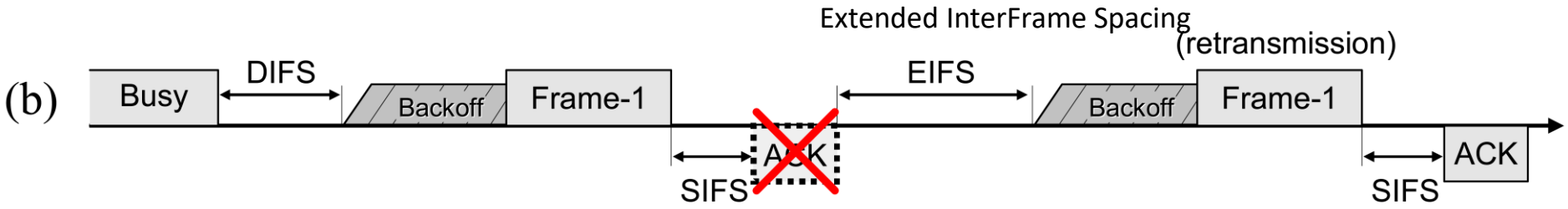
Timing of successful frame transmissions under the DCF:



The sender's actions are shown above the time axis
The receiver's actions are shown below the time axis.

- Assume that a single station has two frames ready for transmission on an **idle** channel.
- If the channel is idle upon the packet arrival, the station transmits immediately, without backoff.
- However, it has to backoff for its own second transmission.
- This gives other station a chance to access the medium.

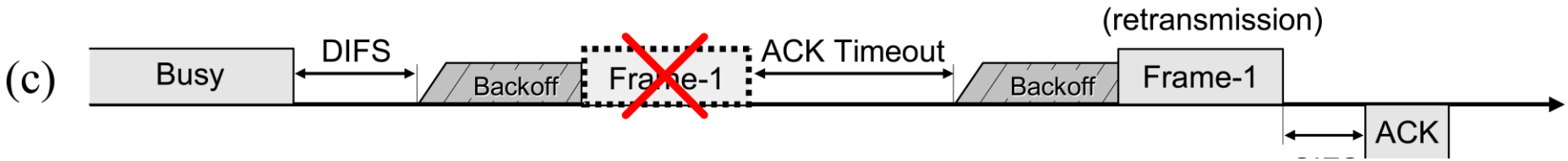
Corrupted acknowledgment:



- Assume that a single station has one frame ready for transmission on a **busy** channel: → DIFS → Backoff → Send
- The acknowledgement for the frame is corrupted during the first transmission.
- The transmitter waits for an EIFS interval and re-contends for the medium to retransmit the frame.
- The EIFS is derived from the SIFS and the DIFS and the length of time it takes to transmit an ACK frame at the lowest PHY mandatory rate:

$$EIFS = SIFS + DIFS + ACKTxTime$$

Corrupted data frame:

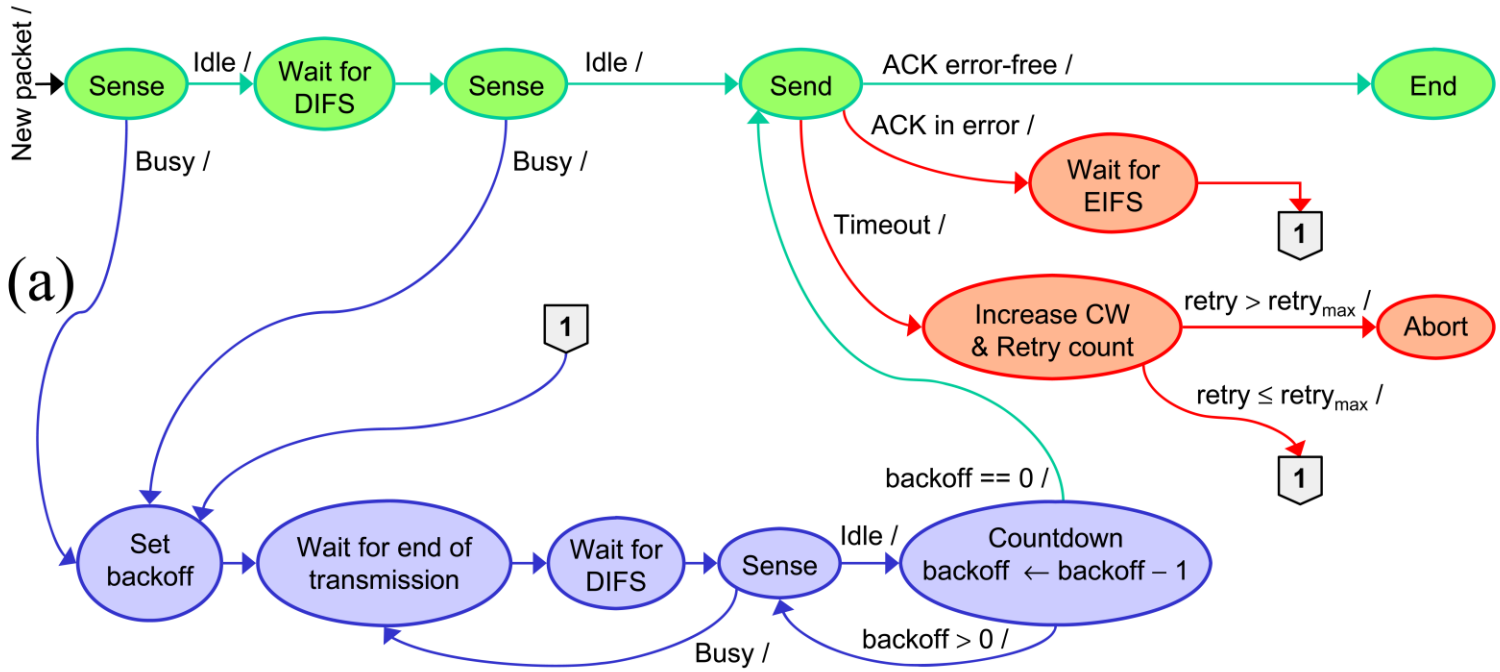


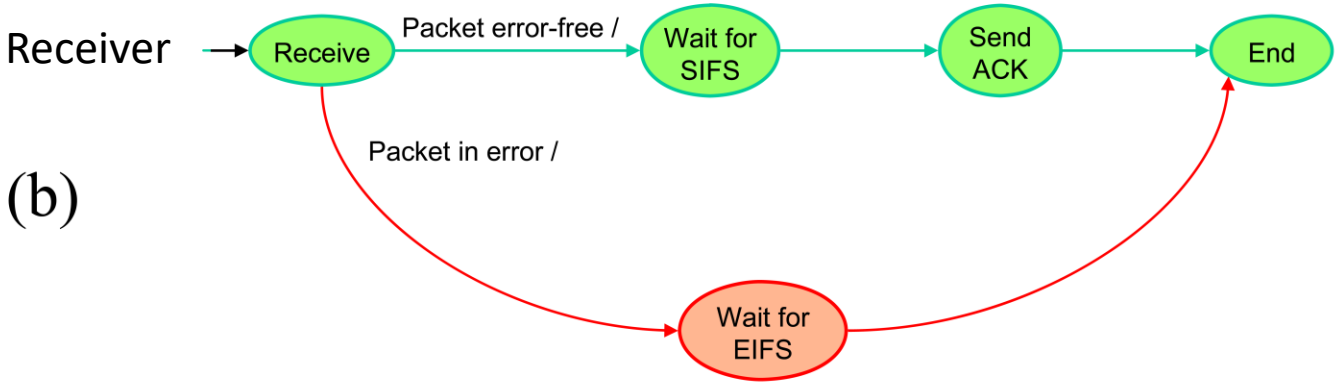
- Assume that a single station has one frame ready for transmission on a busy channel.
- The data frame is corrupted during the first transmission – no ACK frame is received within a **timeout interval**.
- The transmitter contends again for the medium to retransmit the frame after an ACK timeout.
- Notice that the ACK timeout is much shorter than the EIFS interval:

$$ACK_{timeout} = t_{SIFS} + t_{ACK} + t_{slot}$$

Basic MAC state diagrams (from Ivan Marsic)

Transmitter/Sender

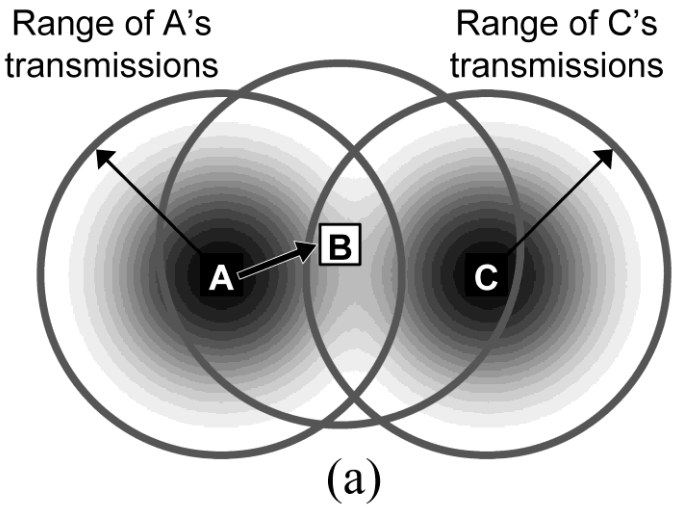




Identify the flow of activities with relation to four previously described cases.

Hidden station problem

(From Ivan Marsic)



C is a "hidden station" to A

- The coverage area for the station A **does not** include the station C
- The station *C* cannot hear station *A*'s transmissions and may mistakenly conclude that the medium is available.

- At the same time there can be transmission pending between the station A and B
- If *C* does start transmitting, it will interfere at *B*, wiping out the frame from *A*.

- A station that can sense the transmission from both the source and receiver nodes is called **covered station**.
- If there is a transmission established between A and C,

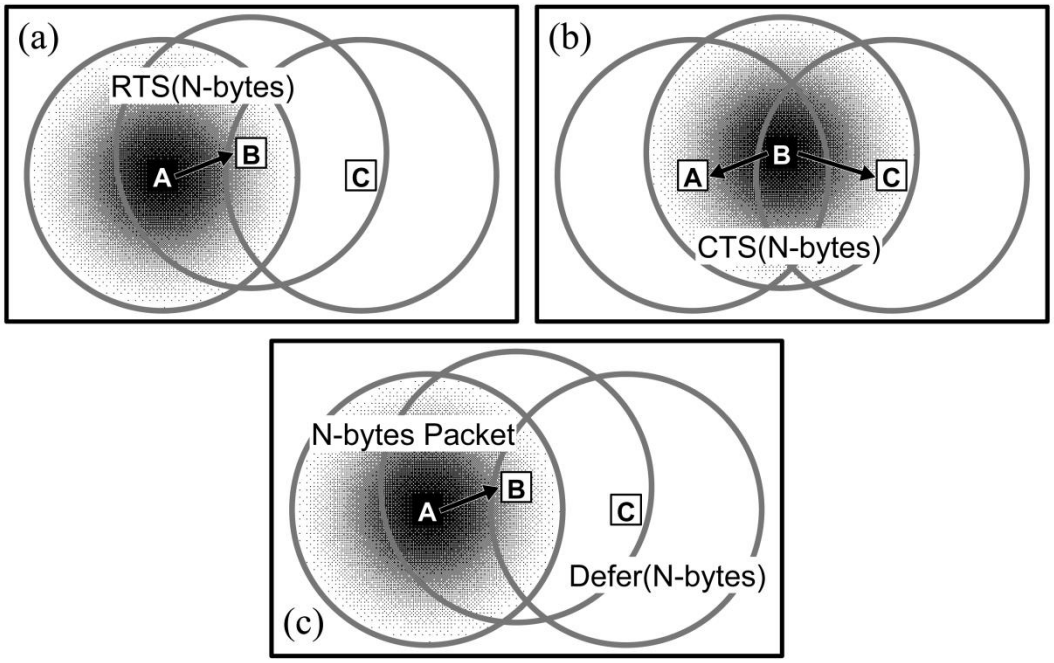
STA **B would be a covered station**.

Solution to the hidden station problem

- A common solution to the hidden/exposed station problem is
- to induce the **receiver** to transmit a short "warning signal" so that other potential **transmitters** in its neighbourhood are forced to defer their transmissions
- IEEE Std 802.11 extends the basic access method (DCF – CSMA/CA) with two more frames:
  - *request-to-send* (RTS)
  - *clear-to-send* (CTS) frames
- RTS/CTS are short frames exchanged before the data and ACK frames.

RTS/CTS frames

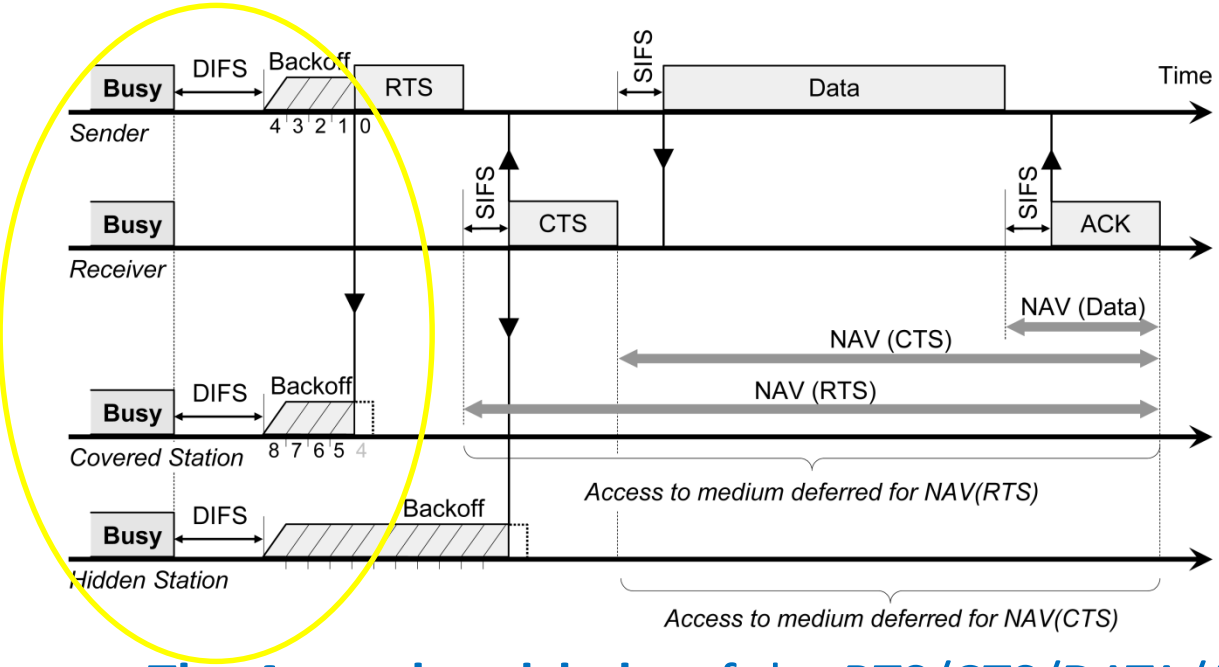
The sender A first sends the **RTS frame** to the receiver B



If the transmission succeeds, the receiver B responds by outputting the short CTS frame.

- **The CTS** frame is intended not only for the sender, but also for all other stations in the receiver's range
- All stations that receive a CTS frame know that this frame signals a **transmission in progress** and must avoid transmitting for the duration of the upcoming (large) data frame.
- Through this indirection, the sender performs "floor acquisition" so it can send frames unobstructed because all other stations will remain silent for the duration of transmission

The RTS/CTS/DATA/ACK exchange of DCF protocol

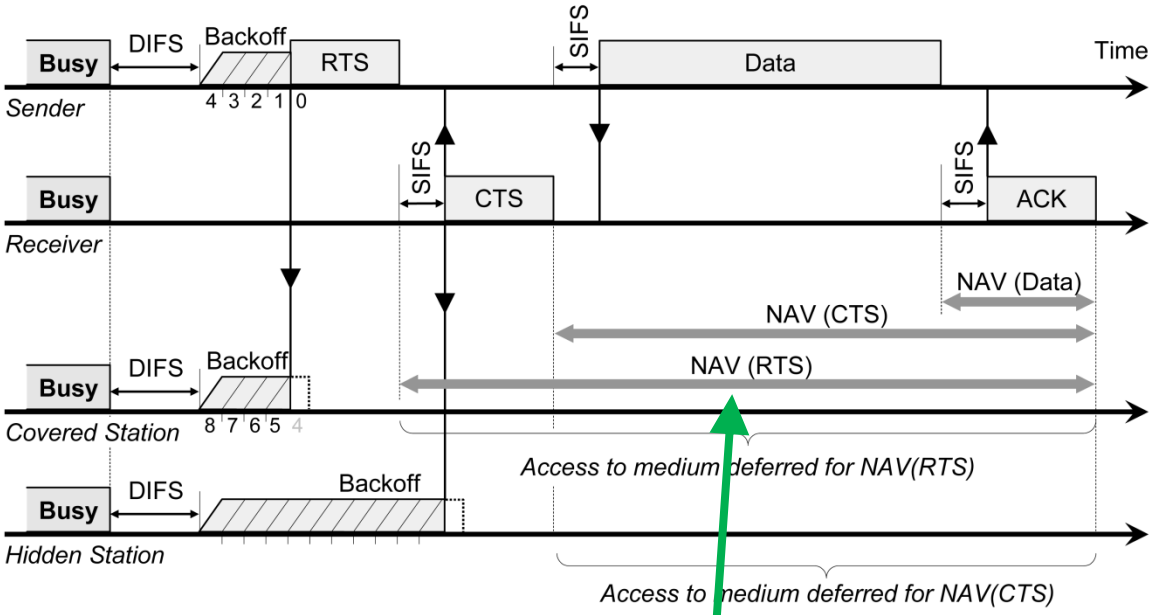


Note

- the sender
- the receiver
- the covered station
- the hidden station

- **The 4-way handshake** of the RTS/CTS/DATA/ACK exchange of the DCF protocol requires that the roles of sender and receiver be interchanged several times between pairs of communicating nodes.
- As before, all four stations sense until the medium has become idle, wait for the DIFS time and generate random backoff values.
- The sender wins the competition and generate the RTS frame intended to all stations that can receive it (the receiver and the covered station)

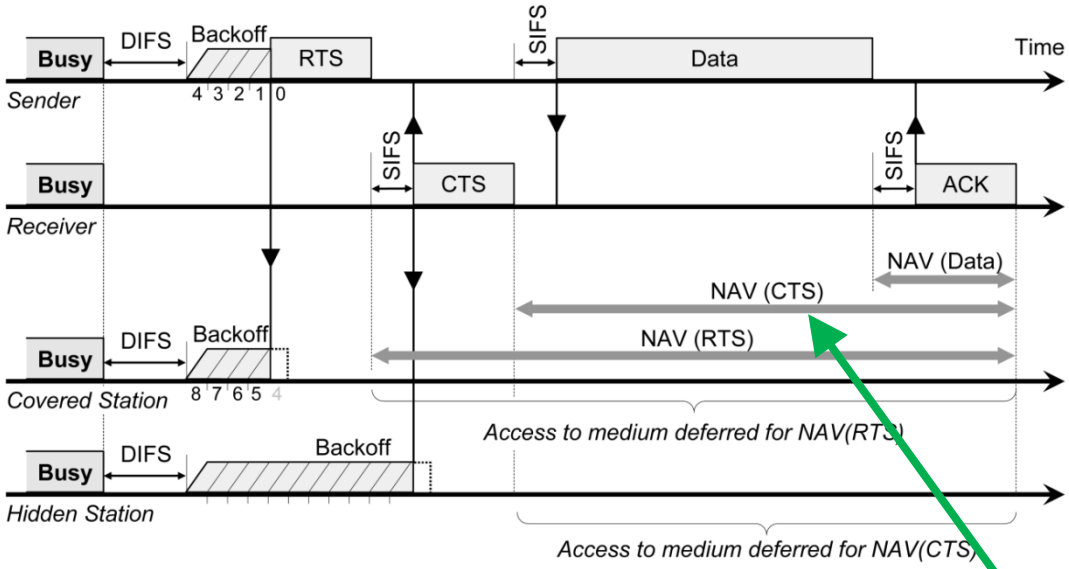
The RTS frame – NAV



The **RTS frame**

- suspends the backoff countdown in the **covered** station
- sends the ***network allocation vector*** (NAV) values in the Duration/ID field of its frame
- This defers the access to the medium in the neighbouring stations, the **covered** station in the example

The CTS/DATA and ACK frames

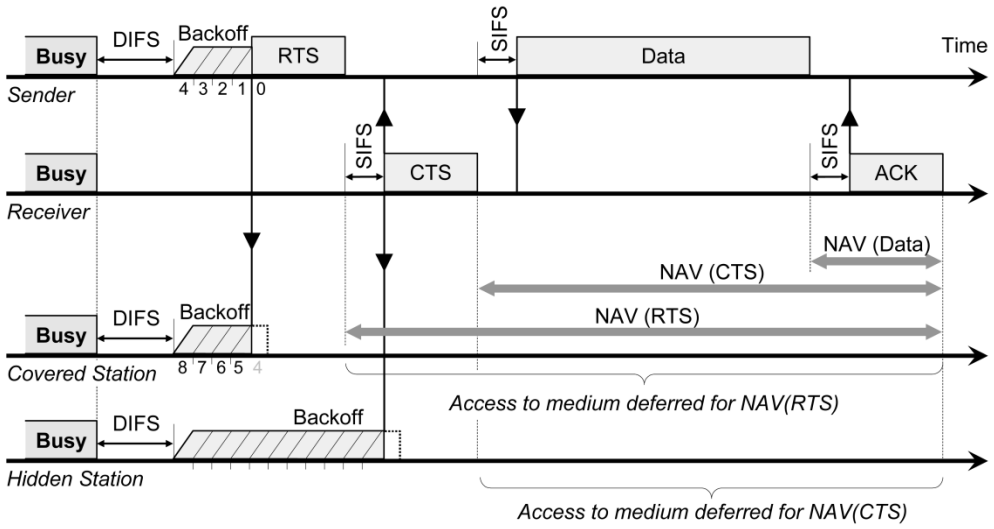


- After receiving the RTS frame and waiting for the SIFS time, the receiver generates the **CTS** (Clear to Send) frame
- The hidden station receives the CTS frame, and suspends the backoff countdown.
- The CTS frame has a new value of the Network Allocation Vector (**NAV**) long enough to cover the transmission of the data frame.
- The sender after receiving the CTS frame and waiting for the SIFS time sends the data frame, with another **NAV** to cover the time for the ACK frame.
- If the data frame is received correctly, the receiver sends the ACK frame.

The Virtual Carrier Sense Mechanism

- The RTS/CTS frames and the Network Allocation Vector create the virtual carrier sense mechanism.
- The NAV time duration is carried in the frame headers Duration/ID field) on the RTS, CTS, data and ACK frames.
- The nodes neighbouring the receiver and the sender set their network allocation vector (NAV) values from the Duration/ID field specified in either the RTS or CTS frames they overhear.
- Notice that the NAV vector is set only in the RTS/CTS access mode and *not* in the basic DCF access mode

Is the Hidden Station Problem Solved?



- The additional RTS/CTS exchange shortens the vulnerable period from the entire data frame in the basic DCF method down to the duration of the RTS/CTS exchange in the RTS/CTS method.

The hidden station problem
is solved only partially, because:

- if a hidden station starts with transmission *simultaneously* with the CTS frame,
- the hidden station will not hear the CTS frame,
- the sender will receive the CTS frame correctly and start with the data frame transmission,
- this will result in a collision at the receiver.

IEEE 802.11n (Clause 20)

- **IEEE 802.11n** builds on previous 802.11a, b and g standards by adding mechanisms to improve network throughput:
  - multi-input multi-output (MIMO) radio transmission
  - 40 MHz channels to the physical layer (PHY)
  - frame aggregation to the MAC layer
- operates in the 2.4 and 5 GHz frequency bands
- achieves a significant increase in the maximum **raw data rate:** from 54 Mbps to 600 Mbps,
- improves reliability
- increases transmission distance. At 100 m:
  - 802.11g performance drops to 1 Mbps
  - 802.11n networks operate at up to 70Mbps, which is 70 times faster than 802.11g.

IEEE802.11n High Throughput devices

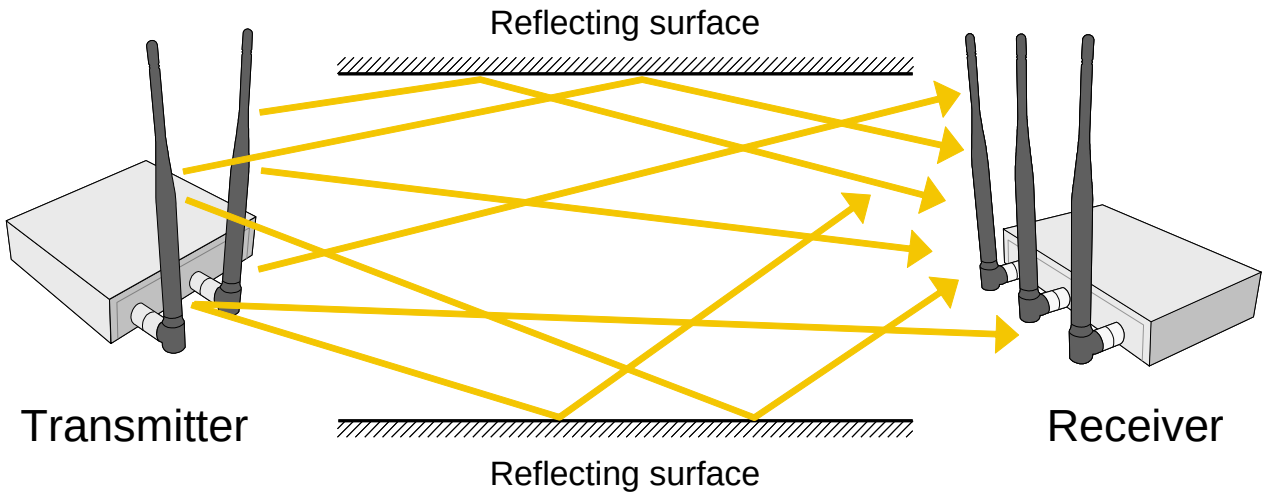
- IEEE 802.11n-capable devices are also referred to as *High Throughput (HT*) devices.
- An HT device declares that it is an HT device by transmitting the *HT Capabilities element.*
- The device also uses the HT Capabilities element to advertise which **optional capabilities** of the 802.11n standard it implements.
- The HT Capabilities element is carried as part control frames that wireless devices exchange during the **connection setup** or in periodical announcements.
- It is present in the following frames:
  - Beacon
  - Probe Request and Response
  - Association and Re-association Request and Response

More on HT devices

- IEEE 802.11n standard distinguishes the frame formats used by 802.11n devices from those of "legacy" 802.11 devices.
- 802.11n devices can operate in pure high-throughput mode, this is known as the "**greenfield mode**," because it lacks any constraints imposed by prior technologies.
- This mode achieves the highest effective throughput offered by the 802.11n standard.
- The standard describes mechanisms for backward compatibility with existing 802.11a/b/g devices

Multiple Antennas (MIMO)

- 802.11n speed increase is due to the use of **Multiple-Input Multiple-Output (MIMO)** technology
- 802.11n access points and stations can have up to four antennas.
- Each antenna can establish a separate (but simultaneous) connection with the corresponding antenna on the other device.



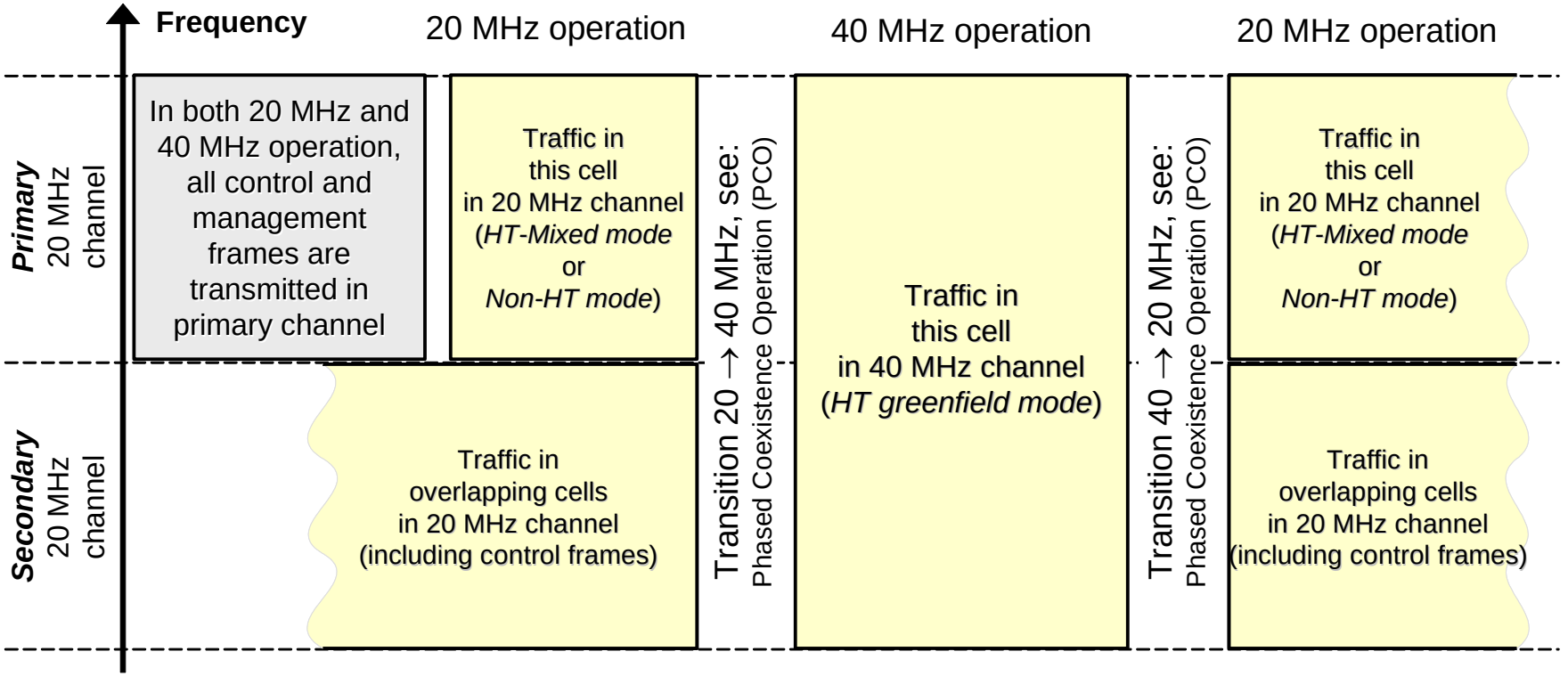
MIMO receiver

- Each receiver receives a separate data stream from the transmitter and recombines the data into the original data stream.
- This technique is called Spatial Division Multiplexing (SDM).
- MIMO SDM can significantly increase data throughput as the number of resolved spatial data streams is increased.
- Spatial multiplexing combines multiple beams of data at the receiving end, theoretically multiplying throughput—but also multiplying the chances of interference.
- The transmitter and the receiver must cooperate to mitigate interference by sending radio energy only in the intended direction.
- The transmitter needs feedback information from the receiver about the received signal so that the transmitter can tune each signal it sends.
- This feedback is available only from 802.11n devices

20MHz and 40MHz Channels

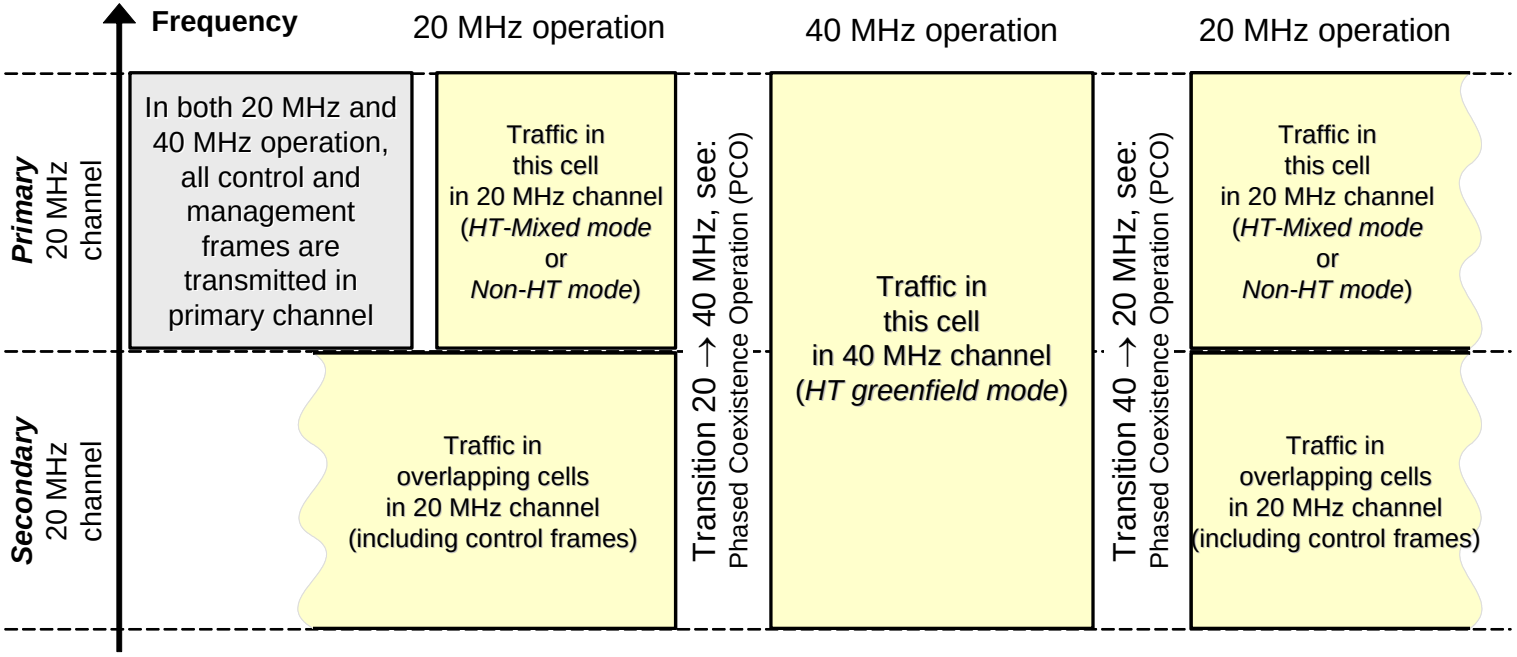
- The physical layer of 802.11n can use double-wide channels that occupy 40MHz of bandwidth.
- Legacy devices use 20MHz-wide channels to transmit data.
- 802.11n can bond two 20MHz channels that are adjacent in the frequency domain into one that is 40MHz wide.
- Doubling of bandwidth results in a theoretical **doubling of data transmission rate**.
- Up to four data streams can be sent simultaneously using 20MHz or 40MHz channels.
- A theoretical maximum data rate of 600 Mbps can be achieved using four double-width channels (40MHz).
- In the 2.4 GHz band only two non-overlapping 40MHz channels are possible.

Channel bonding



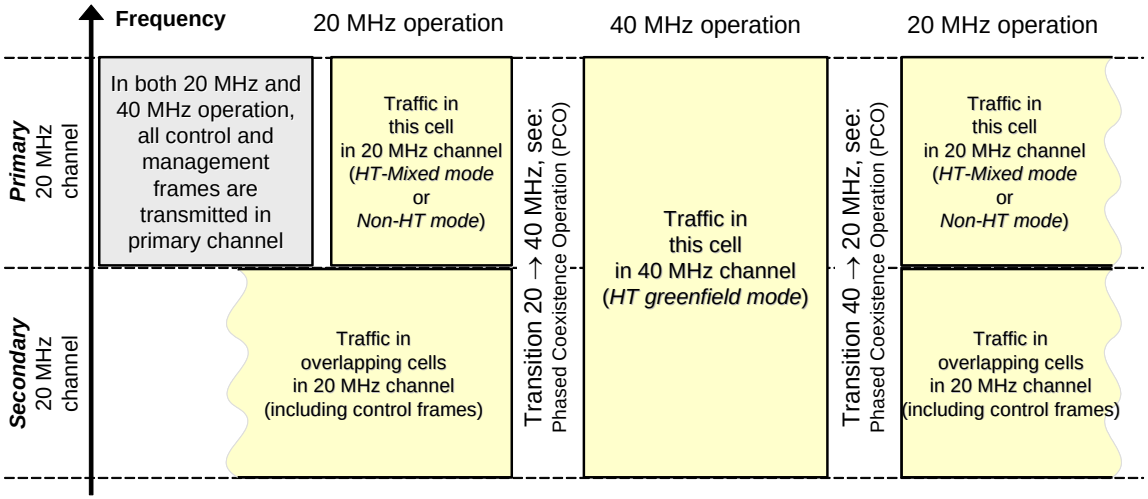
- **Primary channel** is the common channel of operation for all stations (including HT and non-HT) that are members of the BSS (Basic Service Set).
- To preserve interoperability with legacy clients, 802.11n access point transmits all **control and management frames in the primary channel**.
- All 20-MHz clients (whether HT or legacy non-HT) only associate to the primary channel, because the beacon frame is only transmitted on the primary channel.

Phased Coexistence Operation



- **Phased Coexistence Operation** (PCO) is an option in which an 802.11n access point alternates between using 20-MHz and 40-MHz channels.
- Before operating in the 40-MHz mode, the access point explicitly reserves both adjacent 20-MHz channels.

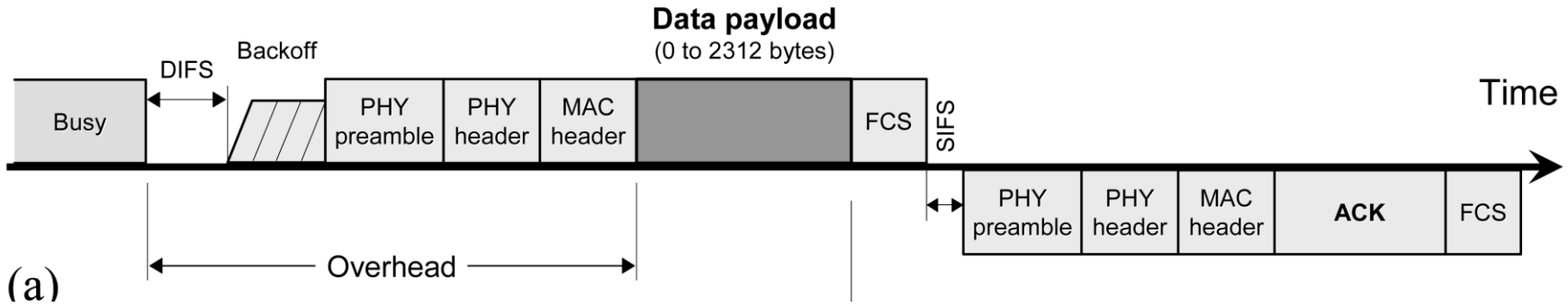
The Secondary Channel



Secondary channel is a 20MHz channel associated with a primary channel.

- May be located in the frequency spectrum below or above the primary channel.
- It is used only by HT stations for creating a 40MHz channel.
- A station is not required to react to control frames received on its secondary channel, even if it is capable of decoding those frames.
- The secondary channel of one BSS may be used by an overlapping BSS as its primary channel.
- If an access point detects an overlapping BSS whose primary channel is the access point's secondary channel, it switches to 20MHz operation.

Aggregating Frames: MAC layer overhead



- Every frame transmitted by an 802.11 device has a significant amount of fixed **overhead**: PHY header, MAC header, interframe spaces, and ACK of transmitted frames.
- At the highest of data rates, this overhead alone can be longer than the entire data frame.
- **Contention** for the channel and collisions also reduce the maximum effective throughput of 802.11.
- 802.11n addresses these issues by employing the frame aggregation mechanisms.

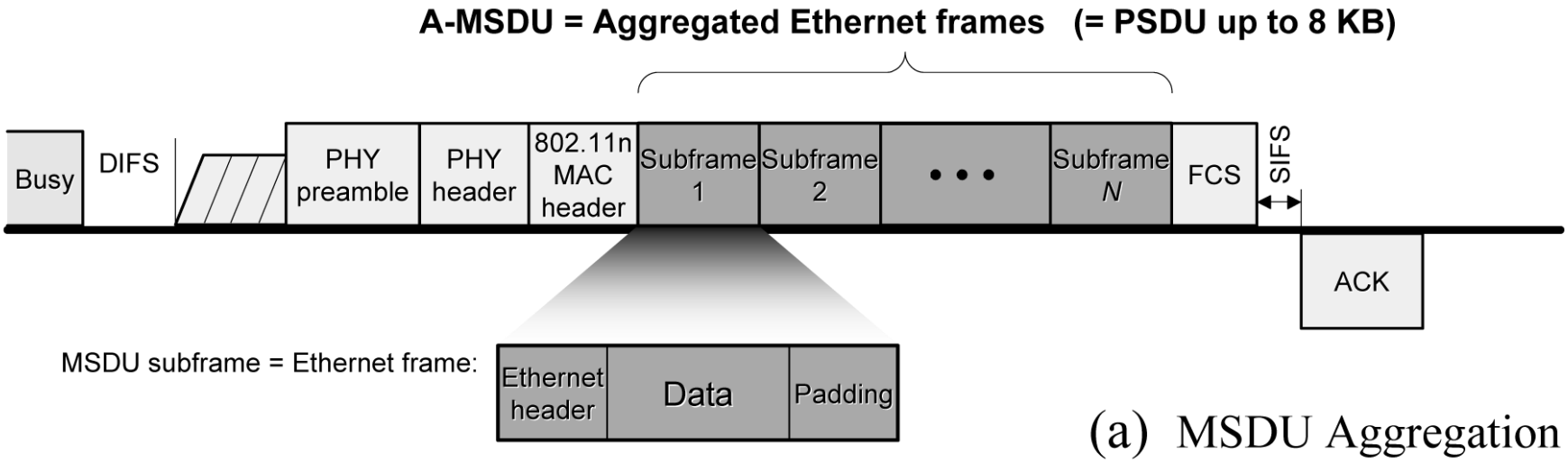
Two Types of Frame Aggregation

- The frame aggregation can be performed within different sublayers of the link layer.
- The 802.11n standard defines two types of frame aggregation:
  - *MAC Service Data Unit (MSDU)* aggregation
  - *MAC Protocol Data Unit (MPDU)* aggregation.
- Both aggregation methods group several data frames into one large frame and reduce the overhead to only a single radio preamble for each frame transmission

MSDU Aggregation

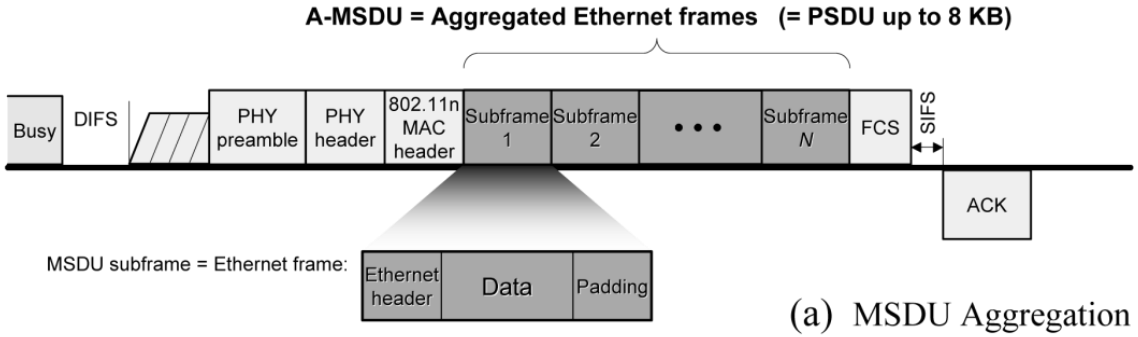
- MSDU aggregation exploits the fact that most mobile access points and most mobile client protocol stacks use Ethernet as their “native” frame format.
- It collects Ethernet frames to be transmitted to a single destination and wraps them in a single 802.11n frame.
- This is efficient because Ethernet headers are much shorter than 802.11 headers.
- For this reason, **MSDU aggregation** is more efficient than **MPDU aggregation**.
- MSDU aggregation allows several MAC-level service data units (MSDUs) to be concatenated into a single Aggregated MSDU (A-MSDU).

Aggregated MAC Service Data Units (A-MSDUs)



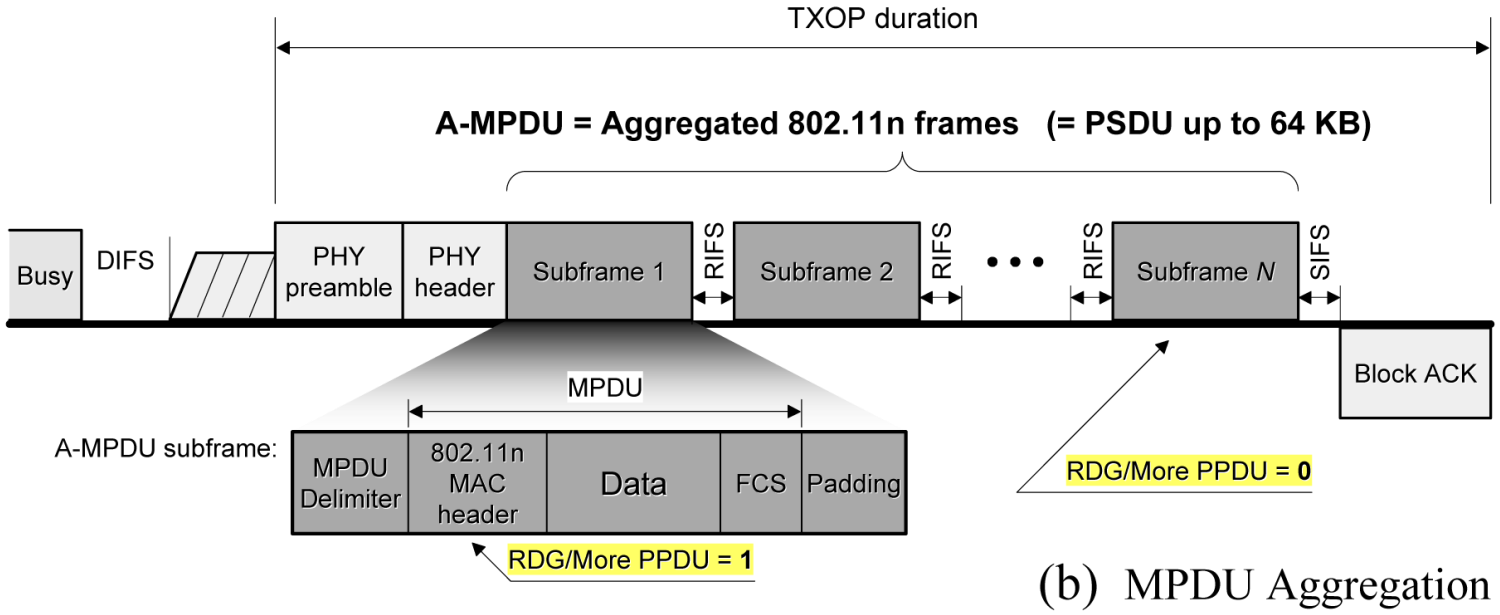
- The frame format for A-MSDU: **one**
  - PHY header
  - MAC header
  - FCS
- for a number of data frames.
- The resulting 802.11n frames can be up to 8 Kbytes in size.

A-MSDU



- When the **source is a mobile device**, the aggregated frame is sent to the access point, where the constituent Ethernet frames are forwarded to their ultimate destinations.
- When the **source is an access point**, all of the constituent frames in the aggregated frame must be destined to a single mobile client, because there is only a single destination in each mobile client.
- With MSDU aggregation, the entire, aggregated frame is encrypted once using the security association of the destination of the outer 802.11n frame wrapper.
- If no acknowledgement is received, the whole 802.11n frame must be retransmitted.
- An A-MSDU aggregate fails as a whole even if just one of the enclosed MSDUs contains bit errors.

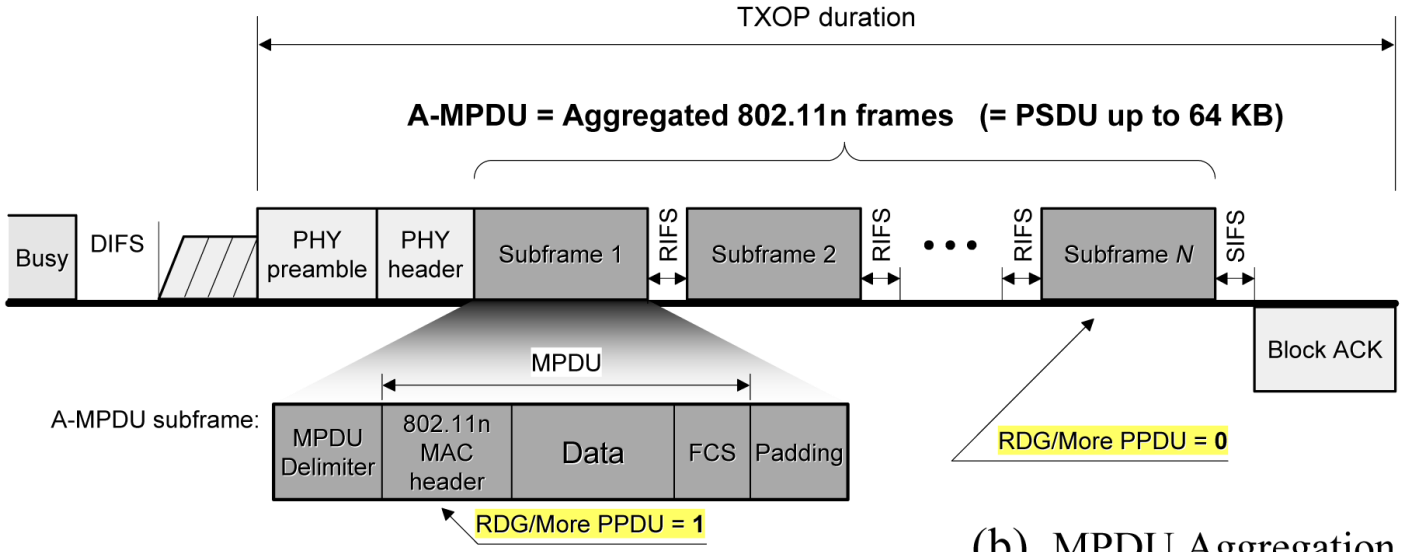
MAC Protocol Data Units (MPDUs) Aggregation



(b) MPDU Aggregation

- MPDU aggregation also collects Ethernet frames to be transmitted to a single receiver, but it converts them into 802.11n frames.
- It may be more efficient than MSDU aggregation in environments with high error rates, due to the **block acknowledgement** mechanism.
- This mechanism allows each of the aggregated data frames to be individually acknowledged or retransmitted if affected by an error.
- MPDU aggregation scheme enables aggregation of several MAC-level protocol data units (MPDUs) into a single PHY-layer protocol data unit (PPDU).

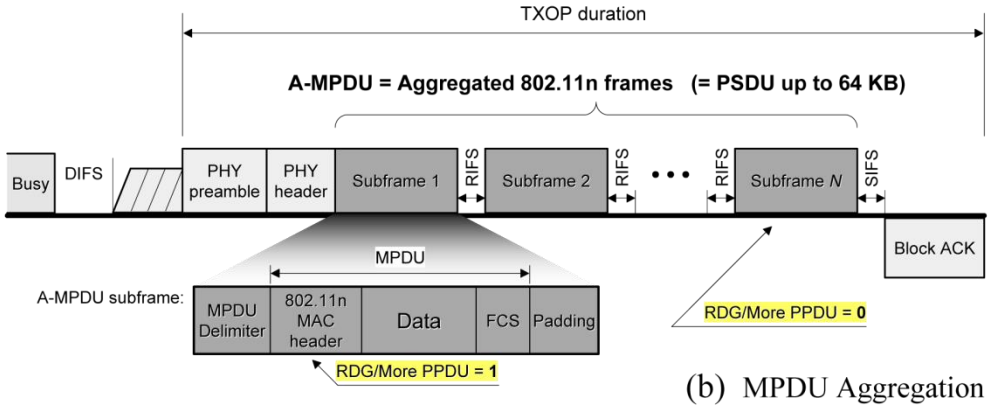
MPDU Aggregation



(b) MPDU Aggregation

- A-MPDU consists of a number of MPDU delimiters each followed by an MPDU.
- Except when it is the last A-MPDU subframe in an A-MPDU, padding bytes are appended to make each A-MPDU subframe a multiple of 4 bytes in length, which can facilitate subframe delineation at the receiver.
- A-MPDU allows bursting 802.11n frames up to 64 KB.
- The purpose of the *MPDU delimiter* (4 bytes long) is to locate the MPDU subframes within the A-MPDU such that the structure of the A-MPDU can usually be recovered when one or more MPDU delimiters are received with errors.
- Subframes are sent as a burst (not a single unbroken transmission).

MPDU Aggregation cont.



(b) MPDU Aggregation

The subframes are separated by the *Reduced Inter-Frame Space* (RIFS) interval of 2 µs duration (compared to 16 µs SIFS interval).

- Note that the sender uses the "RDG/More PPDU" bit of the HT Control field in the MAC frame to inform the receiver whether there are more subframes in the current burst.
- If the "RDG/More PPDU" field is set to "1," there will be one or more subframes to follow the current subframe; otherwise, the bit value "0" indicates that this is the last subframe of the burst.
- Subframes of an A-MPDUs burst can be **acknowledged individually** with a single Block-Acknowledgement.
- The A-MPDU structure can be recovered even if one or more MPDU delimiters are received with errors.
- Unlike A-MSDU where the whole aggregate needs to be retransmitted, only unacknowledged MPDU subframes need to be retransmitted.

Channel Coherence Time

There are several limitations of frame aggregation.

1. All the aggregated frames must be sent to the same destination, STA or AP
2. All the frames to be aggregated have to be ready for transmission at the same time.
3. The maximum frame size that can be successfully sent is affected by a factor called ***channel coherence time***.
   - Channel coherence time depends on **how quickly** the transmitter, receiver, and other objects in the environment **are moving**.
   - The time for frame transmission must be shorter than the channel coherence time.
   - When the things are moving faster, the channel data rate is reduced, and therefore the allowed maximum frame size becomes smaller.

Throughput vs Latency

- Frame aggregation can increase the throughput at the MAC layer under ideal channel conditions.
- A larger aggregated frame will cause each station to wait longer before its next chance for channel access.
- There is a tradeoff between **throughput and delay** (or, latency) for frame aggregation at the MAC layer (as **throughput increases, latency increases** as well).
- Under error-prone channels, corrupting a large aggregated frame may waste a long period of channel time and lead to a lower MAC efficiency.

Transmit Opportunity

- The frame aggregation mechanism reduces the contention and backoff overhead and thus enhances the efficiency of channel utilization.
- Duration of channel occupation for aggregated transmission is specified by the **transmit opportunity (TXOP)** parameter
- During **TXOP** period of time, the station that won channel access can transmit multiple consecutive data frames without re-contending for the channel.
- The TXOP holder can perform **truncation** of TXOP by transmitting a **CF-End** (Contention-Free-End) frame, if the remaining TXOP duration is long enough to transmit this frame.

Summary of LT04 & LT05

Reflections on:

- Explain the roles of layers in the IEEE802.11 architecture.
- Describe the services provided by IEEE 802.11
- Explain the use backoff, interframe spacing, point coordination, and distributed coordination for MAC layer operation of IEEE 802.11.
- Describe the main methods used to improve throughput in IEEE 802.11n, IEEE 802.11ac, and IEEE802.11ad.
- Explain the IEEE802.11i WLAN security procedures.