

---

# Indoor WLAN Design

*Part III: Understanding the 802.11 MAC*

**Kjell Jørgen Hole**

UiB

Last updated 17.01.07

Mail: [Kjell.Hole@ii.uib.no](mailto:Kjell.Hole@ii.uib.no)

URL: [www.kjhole.com](http://www.kjhole.com)

- What is Medium Access Control (**MAC**)?
- Why you need a good understanding of the 802.11 MAC
- Challenges for the MAC
- MAC details
  - access technique
  - timing
  - frame format
- Bridging

## Definition of MAC

---

KJhole.com

**MAC** Medium Access Control. The function in a wireless network that arbitrates use of the network capacity and determines which MSs are allowed to use the medium for transmission

# Why You Need to Understand the MAC

- A few years back most 802.11a,b,g networks had a relatively small number of users and were rarely subjected to severe stresses. This picture has changed. There now exist large networks with many BSs and MSs
- Tuning a wireless network is tied to parameters in the MAC specification. Knowledge of what those parameters do is needed to understand the behavior of a network and the effects of tuning
  - RTS threshold
  - Fragmentation threshold

## ... Understand the MAC

---

KJhole.com

- Device drivers may expose low-level parameters. A good understanding of the MAC is needed to optimize these parameters
- Troubleshooting a wireless network may be difficult. A *packet sniffer* can be an invaluable aid. To take full advantage of the sniffer, you need to understand what the packets mean to interpret the network's behavior

# Challenge for MAC: RF Link Quality

---

**RF link quality** Radio links in the Industrial Scientific and Medical (ISM) band are subject to:

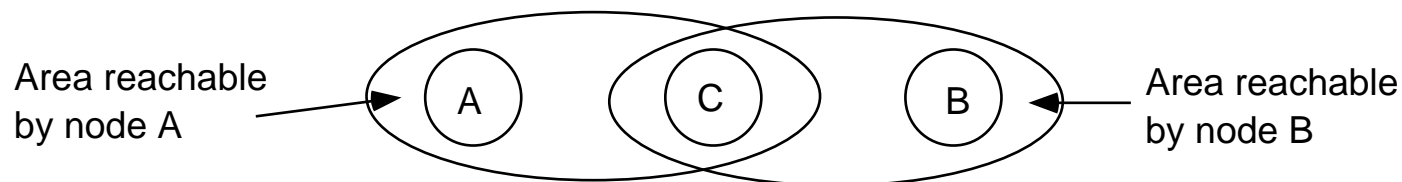
- interference
- noise
- multipath fading

! To alleviate these problems, all transmitted frames must be acknowledged

– a packet is considered lost if no ack is received

# Challenge for MAC: Hidden Node Problem

- Nodes A and B both want to communicate with node C
- Radio waves cannot reach full distance between A and B
- From the perspective of node A, node B is a **hidden node** since A cannot hear B
- Simultaneous transmissions from A and B will collide at C



## ...Hidden Node Problem

---

KJhole.com

- BSs and MSs are generally *half-duplex* transceivers, i.e., they don't transmit and receive at the same time
  - difficult to detect collisions caused by hidden nodes
- ! As we shall see, the MAC utilizes *Request to Send* (**RTS**) and *Clear to send* (**CTS**) signals to prevent frames from colliding

# 802.11 MAC Overview

---

- All 802.11 (a,b,g) networks use the same MAC
- The MAC layer sits on top of the physical layer
- The MAC adapts Ethernet-style networking to radio links
- The MAC uses *Carrier Sense Multiple Access with Collision Avoidance* (**CSMA/CA**) to control access to the transmission medium

# Distributed Coordination Function (DCF)

- Ethernet-like CSMA/CA access is provided by the *Distributed Coordination Function* (**DCF**)
- DCF first checks to see that the radio link is clear before transmitting. To avoid collisions, MSs use a **random backoff** after each frame, with the first transmitter seizing the channel
- In some cases DCF uses RTS and CTS signals to further reduce the possibility of collisions caused by hidden nodes
- **Remark:** enhanced distribution functions (802.11e) add quality of service functionality and introduce traffic classes

# RTS/CTS (1)

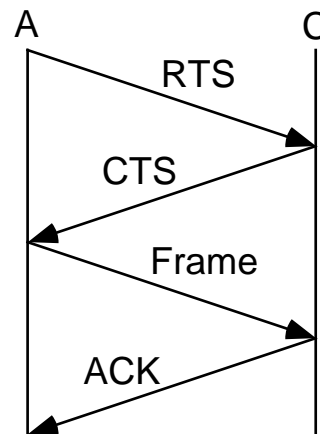
---

- Assume that node A wants to send a frame to node C. Node A initiates the process by sending an RTS frame. The RTS frame has the following purposes:
  - it reserves the radio link
  - it silences any MS that hears it
- If node C receives the RTS, it responds with a CTS. The CTS also silences nodes in the vicinity

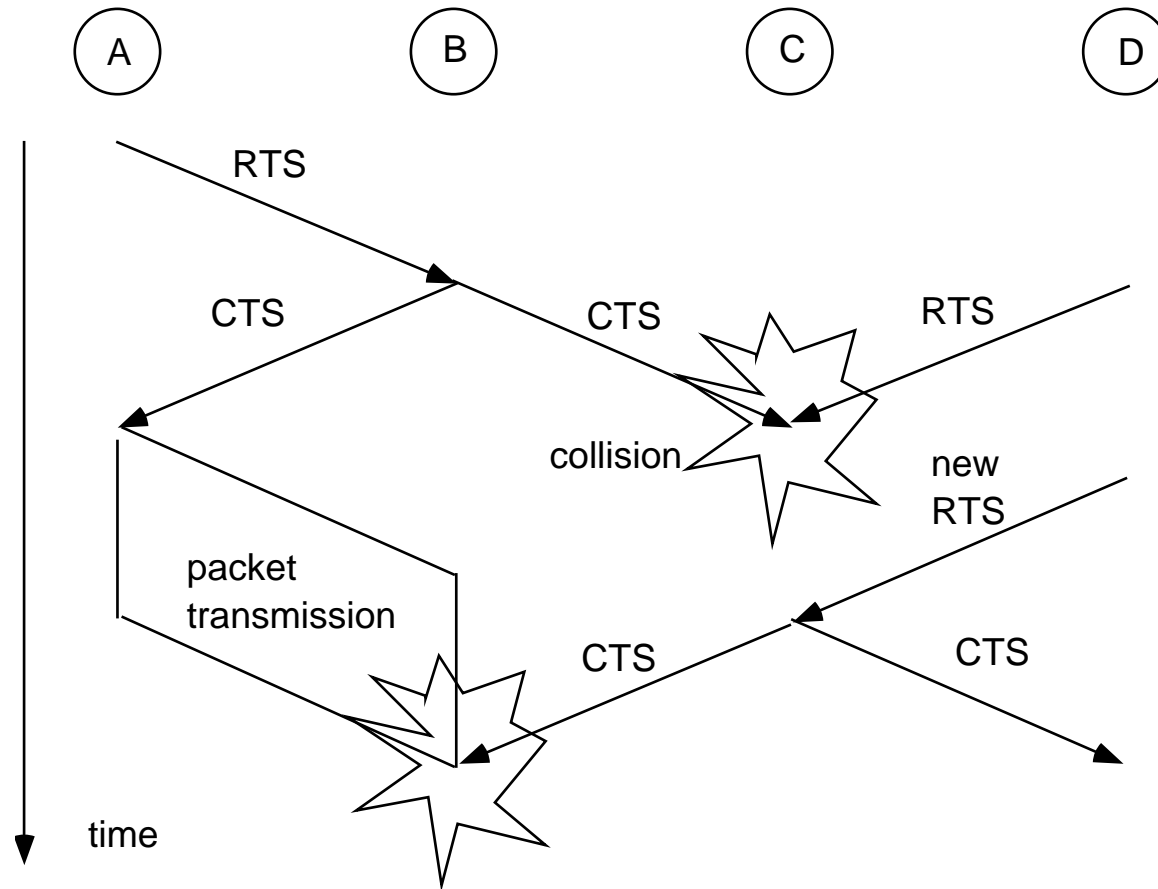
## RTS/CTS (2)

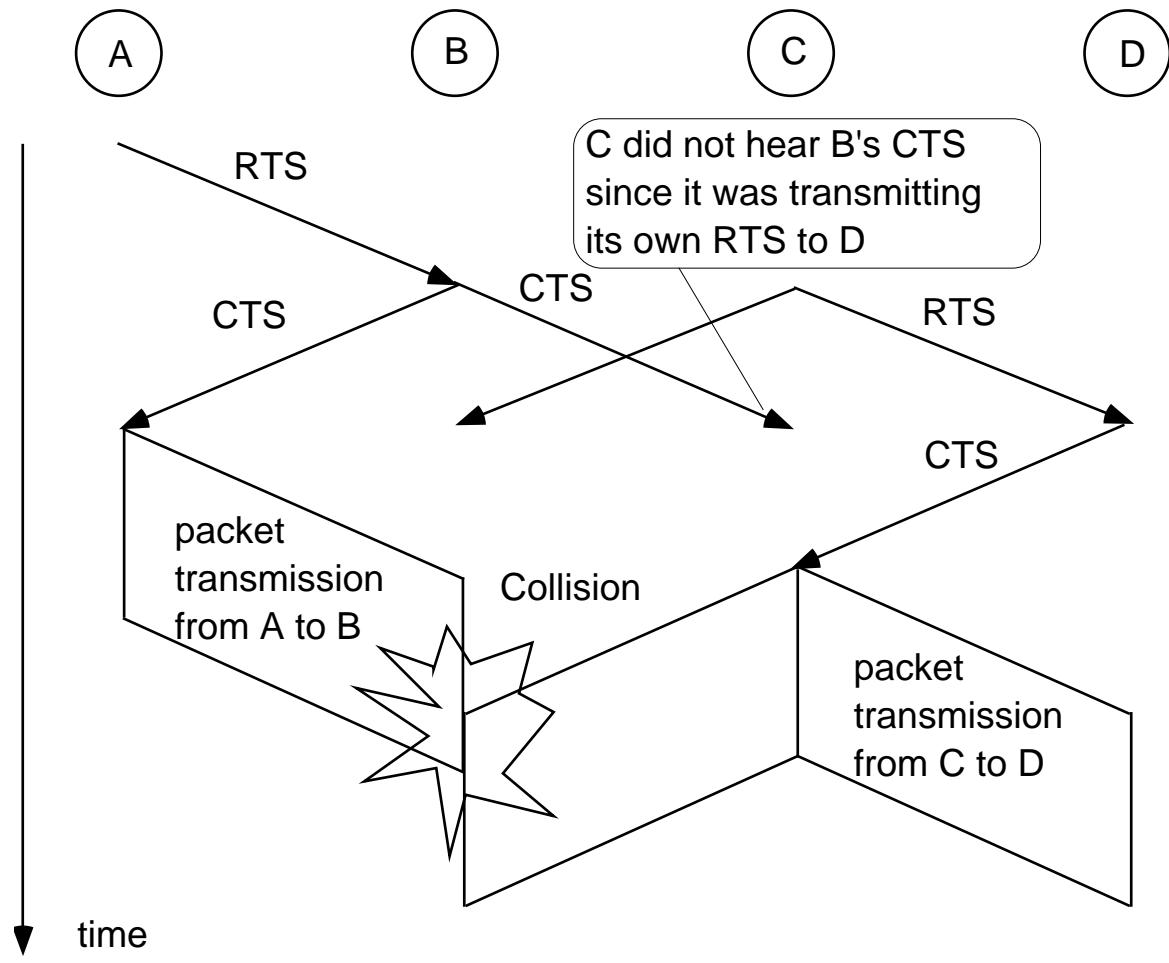
---

- When the RTS/CTS exchange is complete, node A transmits a frame (containing user data) to node C
- Node C must acknowledge the frame using a separate ACK frame



# Shortcoming of RTS-CTS Solution



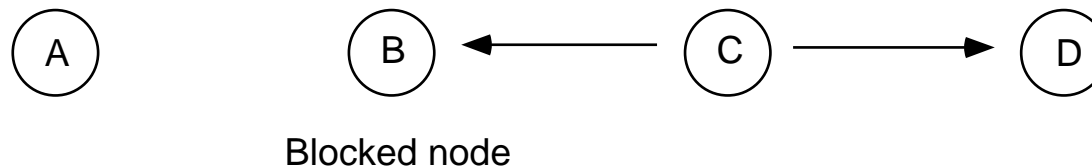


Another illustration of the RTS-CTS problem

# Shortcoming: Exposed Node Problem

---

- Node C is transmitting to D
- B overhears this, and is blocked
- B wants to transmit to A, but is blocked by C



# Exposed Node Problem

---

KJhole.com

- To alleviate the exposed node problem, a node must wait a random backoff time between two consecutive new packet transmissions time

# RTS/CTS Overhead

---

KJhole.com

- Since the multiframe RTS/CTS transmission procedure consumes capacity, it is only used for frames larger than the **RTS threshold**
- Some device drivers allow you to control the RTS/CTS procedure by setting the RTS threshold

# Carrier-Sensing Functions

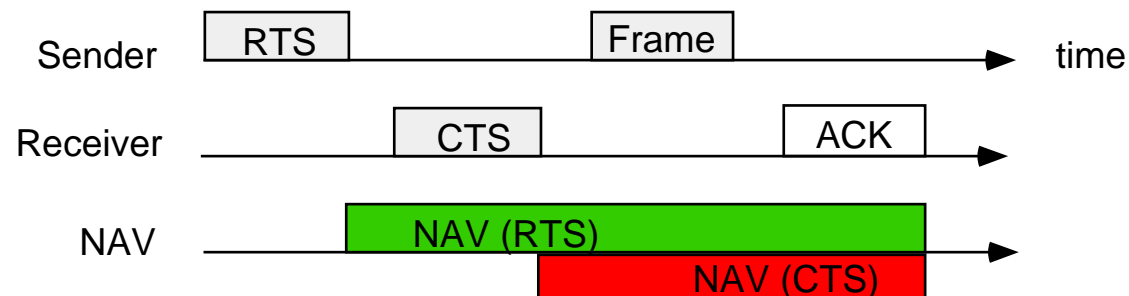
---

Carrier sensing is used to determine if the medium is available. Two types of carrier-sensing functions exist:

**Physical carrier-sensing** Provided by the physical layer. Cannot provide all necessary information due to hidden nodes

**Virtual carrier-sensing** Provided by the *Network Allocation Vector (NAV)*. NAV is a timer used to indicate how long the medium will be reserved. The NAV is sent from a transmitting station to a receiving station. Other MSs count down from the NAV to zero. When the NAV is nonzero, no frame is sent. A station also updates its own NAV when it transmits a frame

- Since an RTS frame is not necessarily heard by all MSs in the vicinity, the receiving station sends a CTS frame with another NAV
- By using NAV, MSs can ensure that **atomic operations**, such as an RTS/CTS sequence, are not interrupted



# Interframe Spacing

---

KJhole.com

- Three different interframe spaces are used to coordinate access to the transmission medium
  - similar to Ethernet
  - create different priority levels for different types of frames
  - independent of transmission speed

# Different Interframe Spaces

---

KJhole.com

**Short interframe space (SIFS)** Used for the highest-priority transmissions, such as RTS/CTS frames and positive ack. High-priority transmissions can begin once the SIFS has elapsed

**DCF interframe space (DIFS)** Minimum medium idle time for contention-based services. MSs may have immediate access to the medium if it has been free for a period longer than the DIFS

**Extended interframe space (EIFS)** Used only when there is an error in frame transmission

# Contention-Based Access Using the DCF

Two basic rules apply to all transmissions using DCF:

- I.** A station with a frame to transmit senses the medium. Carrier sensing is performed using both a physical medium-dependent method and the virtual (NAV) method. If the medium is idle, it waits to see if the medium remains idle for a time equal to DIFS. If so, the station may transmit immediately.
  
- II.** If the medium is busy, the station waits for the channel to become idle for the DIFS and prepares for an *exponential backoff procedure* (to be explained)

# Additional Rules (1)

---

1. If the previous frame contained errors, the medium must be free for the amount of the EIFS
2. Error recovery is the responsibility of the MS sending a frame. Senders expect acknowledgments for each transmitted frame and are responsible for retrying the transmission until it is successful
  - (a) positive acknowledgements are the only indication of success
  - (b) atomic exchanges must complete in their entirety to be successful
  - (c) all unicast data must be acknowledged (not broadcast data)

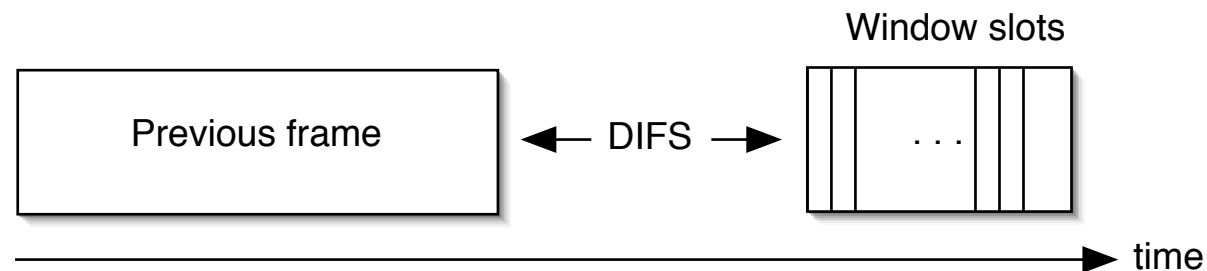
## Additional Rules (2)

---

3. When a station receives a medium reservation that is longer than the current NAV, it updates the NAV. Setting the NAV is done on a frame-by-frame basis
4. Packets larger than the *RTS threshold* must have RTS/CTS exchange and packets larger than the *fragmentation threshold* must be fragmented
5. The following types of frames can be transmitted after the SIFS and thus receive maximum priority: acknowledgments, CTS, and fragments in fragmented sequences

# Backoff with the DCF (1)

- After frame transmission has completed, and the DIFS has elapsed, MSs may attempt to transmit congestion-based data. A period called the **contention window** or **backoff window** follows the DIFS



- The backoff window is divided into slots. Slot length is medium-dependent; higher-speed physical layers use shorter slot times

## Backoff With the DCF (2)

---

- Stations pick a random slot and wait for that slot before attempting to access the medium; all slots are equally likely selections. The station that picks the first slot wins
- Contention window sizes are always 1 less than a power of 2 (e.g. 31, 63, 127, 255)
- Each time the retry counter increases, the contention window moves to the next power of two

## Backoff With the DCF (3)

---

KJhole.com

- The size of the contention window is limited by the physical layer
- When the contention window reaches its maximum size, it remains there until it can be reset
- The window size is reset to its minimum size after a successful frame transmission

# Fragmentation and Reassembly

---

- Higher-level packets and some large management frames must be broken up into smaller pieces to fit through the wireless channel
- Fragmentation improves reliability in the presence of interference
- A packet (or frame) is fragmented when the length exceeds the **fragmentation threshold**
- NAV is used to ensure that other MSs do not use the channel during a fragmentation burst

# Format of Generic MAC Frame

---

- There exist three major types of MAC frames. We only consider the basic frame structure in this lecture
- The frame contains no less than four address fields. Not all frames use all the addresses

Frame control	Duration/ ID	Address 1	Address 2	Address 3	Seq- ctl	Address 4	Frame body	FCS
---------------	-----------------	-----------	-----------	-----------	-------------	-----------	------------	-----

**Frame control** two-byte field with 11 subfields:

- *Protocol version* consists of two bits that indicate which version of the 802.11 MAC is used. At present, only one version is defined
- *Type and subtype fields* identify the type of frame used. Examples are Beacon, RTS, and CTS frames
- *ToDS and FromDS bits* indicate whether a frame is destined for the Distribution System (DS), i.e., the wired backbone network and the bridging functions in the BSs

## More Frame Control Subfields

---

KJhole.com

- *More fragment bit* is set to 1 in all fragments, except the last, when a higher-level packet is fragmented by the MAC
- *Retry bit* is set to 1 when a frame is retransmitted
- *Power management bit* indicates whether the sender will be in power-saving mode after a frame is transmitted. A BS can never be in power-saving mode

## Even More Frame Control Subfields

---

- *More data bit* is set by a BS to indicate to an MS in power-saving mode that at least one frame addressed to the MS is buffered at the BS
- *WEP bit* is set when data is encrypted with WEP
- *Order bit* indicates whether fragments are transmitted in “strict ordering”

## **Duration/ID Field**

---

KJhole.com

**Duration/ID field** can be used to\*

- set the NAV in microseconds, or
- used by slumbering MSs to retrieve frames buffered at the BS

\*Assuming that DCF is utilized

## Address Fields\*

---

KJhole.com

**Destination address** is a 48-bit IEEE MAC identifier corresponding to the final recipient of the frame

**Source address** is a 48-bit IEEE MAC identifier that identifies the source of the transmission

\*There exist two more address fields not discussed here

## Three Last Fields

---

KJhole.com

**Sequence control field** is used for both defragmentation and discarding duplicate frames

**Frame body** contains the higher-layer payload

**Frame check sequence** is a Cyclic Redundancy Check (CRC)

# Bridging (1)

---

- A BS can be viewed as a bridge that translates frames between a wired network and a wireless network
  - 802.11-to-Ethernet bridge
- When a BS receives a frame on the *wireless interface*, it checks for basic integrity, removes a duplicate frame, decrypts content, re-assembles fragments, and translates MAC header into a Ethernet MAC header
  - the new frame is transmitted on the Ethernet interface

## Bridging (2)

---

KJhole.com

- Bridging frames from the wired network to the wireless network is quite similar to the reverse of the process just described

- The 802.11 MAC is designed to provide Ethernet-style networking to radio links
- The DCF (Distributed Coordination Function) allows multiple independent MSs to interact without central control, and thus may be used in an *ad hoc* network mode
- It is likely that network administrators must have a good understanding of the MAC to troubleshoot heavy loaded networks