Wireless LAN 802.11

Tomasz Kurzawa

Wiereless LAN 802.11

- Introduction
- The 802.11 Architecture
- Channels and Associations
- The 802.11 MAC Protocol
- The 802.11 Frame

Introduction

- Wireless LANs are most important access networks technologies in the Internet
- Most popular is the IEEE 802.11 wireless LAN, known also as Wi-Fi
- There are several standards for wireless LAN technology

IEEE 802.11 Standards

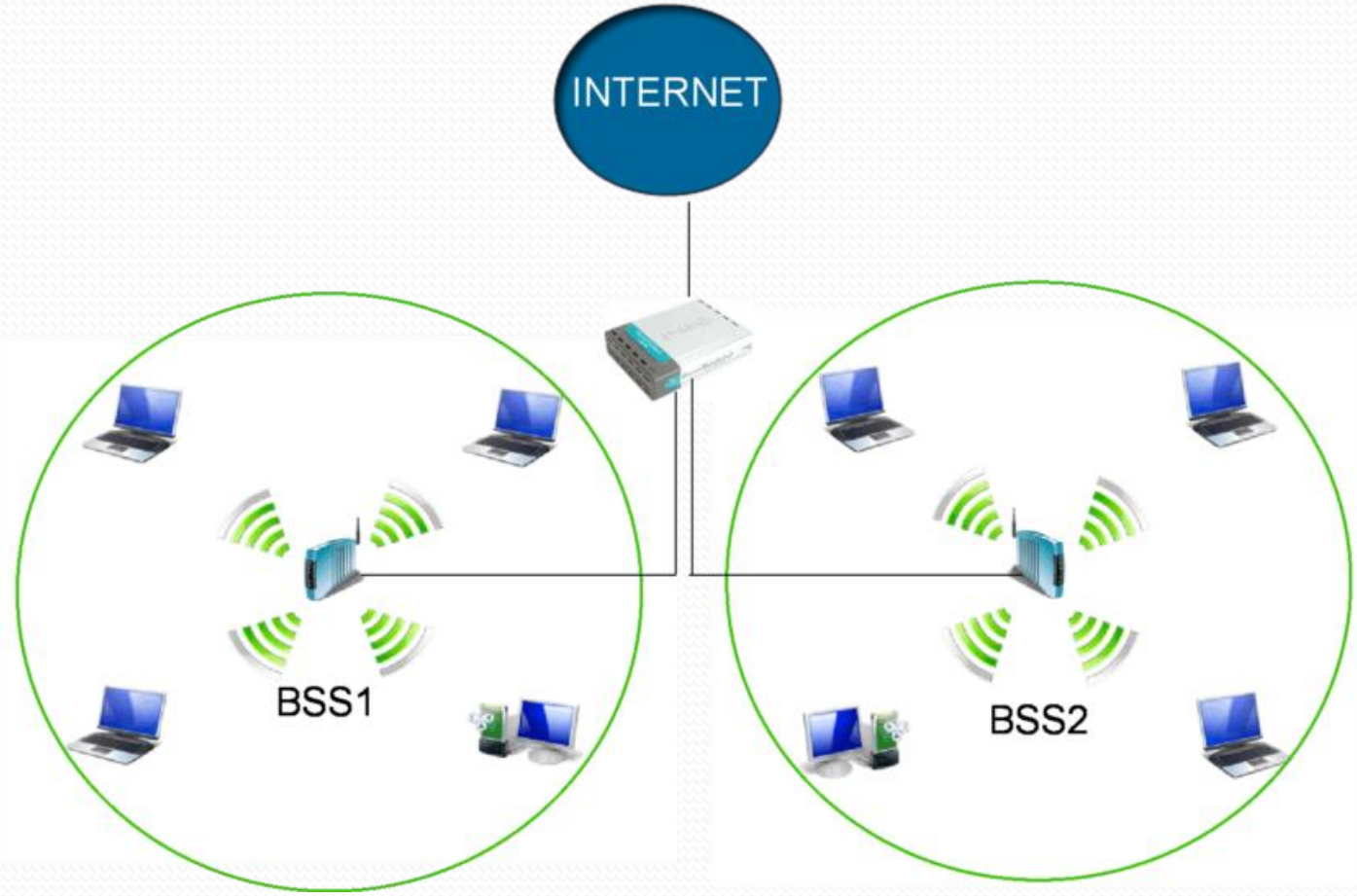
Protocol	Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)	Range (Outdoor)
Legacy	1997	2.4-2.5 GHz	1 Mb/s	2 Mb/s	?	?
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	25 Mb/s	54 Mb/s	~25 meters	~75 meters
802.11b	1999	2.4-2.5 GHz	5.5 Mb/s	11 Mb/s	~35 meters	~100 meters
802.11g	2003	2.4-2.5 GHz	25 Mb/s	54 Mb/s	~25 meters	~75 meters
802.11n	2007 (unapproved draft)	2.4 GHz or 5 GHz bands	200 Mb/s	540 Mb/s	~50 meters	~126 meters

The IEEE 802.11 Architecture

- **Basic Service Set** (**BSS**) is the fundamental building block of the architecture. It can contain one or more wireless stations and one central base station, also known as **Access Point** (**AP**).

- Typical architecture consist of few BSSs connected to some interconnection device like hub or switch which lead to the Internet

The IEEE 802.11 LAN Architecture



The IEEE 802.11 LAN Architecture

- **Infrastructure wireless LAN** is a term often referred to wireless LANs that deploy AP, with the infrastructure being the APs along with wired Ethernet infrastructure that connects APs and router, hub or switch

- IEEE 802.11 stations can also group together and form **ad hoc** type network with no connection to internet

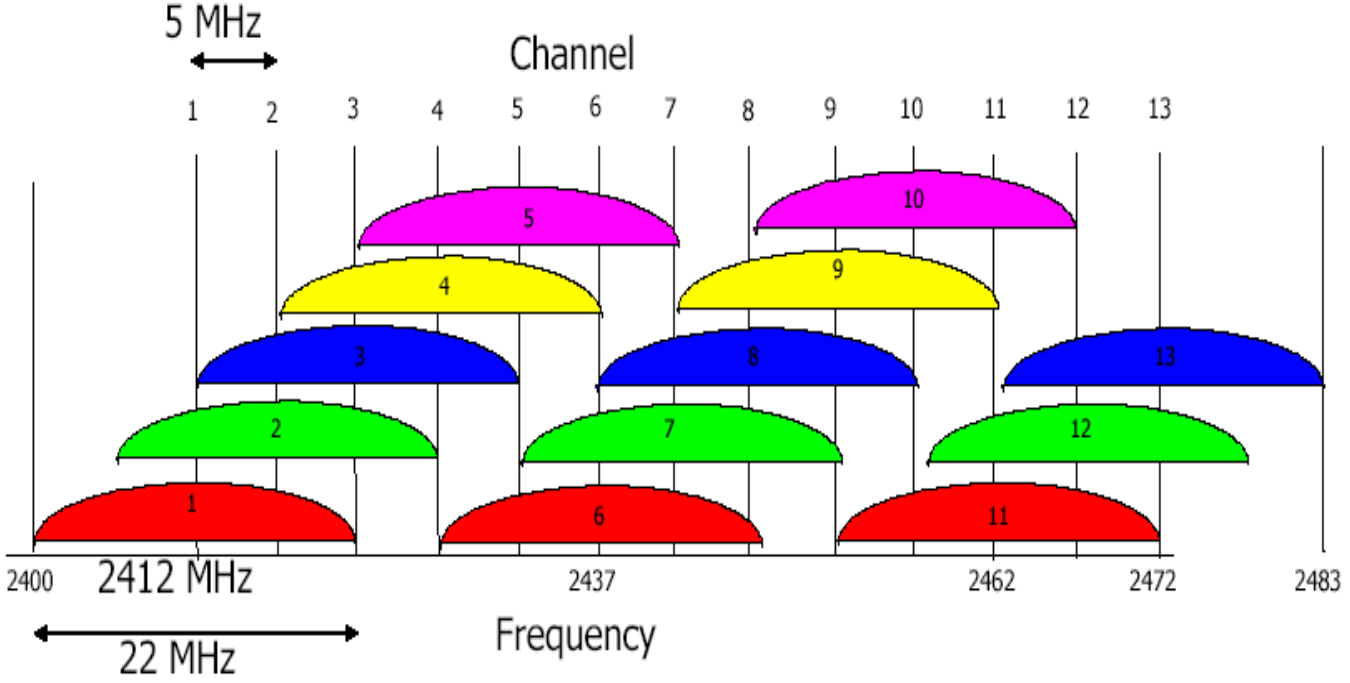
The IEEE 802.11 ad hoc Architecture

Channels and associations

- Each station in BSS needs to associate wit an AP before it can send or receive 802.11 frames.
- Each Access Point (AP) has assigned Service Set Identifier (SSID) and channel number by administrator
  - E.g. 802.11b operates in range between 2.4 and 2.485 GHz and has 11 overlaping channels
- two channels are not overlapping if and only if they are separated by at least 4 channels
  - E.g. 802.11b has 3 non overlaping channels: 1, 6, 11

Channels and associations

- Non overlaping channels are very important in situation of Wi-Fi jungle, that is when wireless station receives a strong signal from two or more Aps.To use internet station needs to be associated with only one AP.



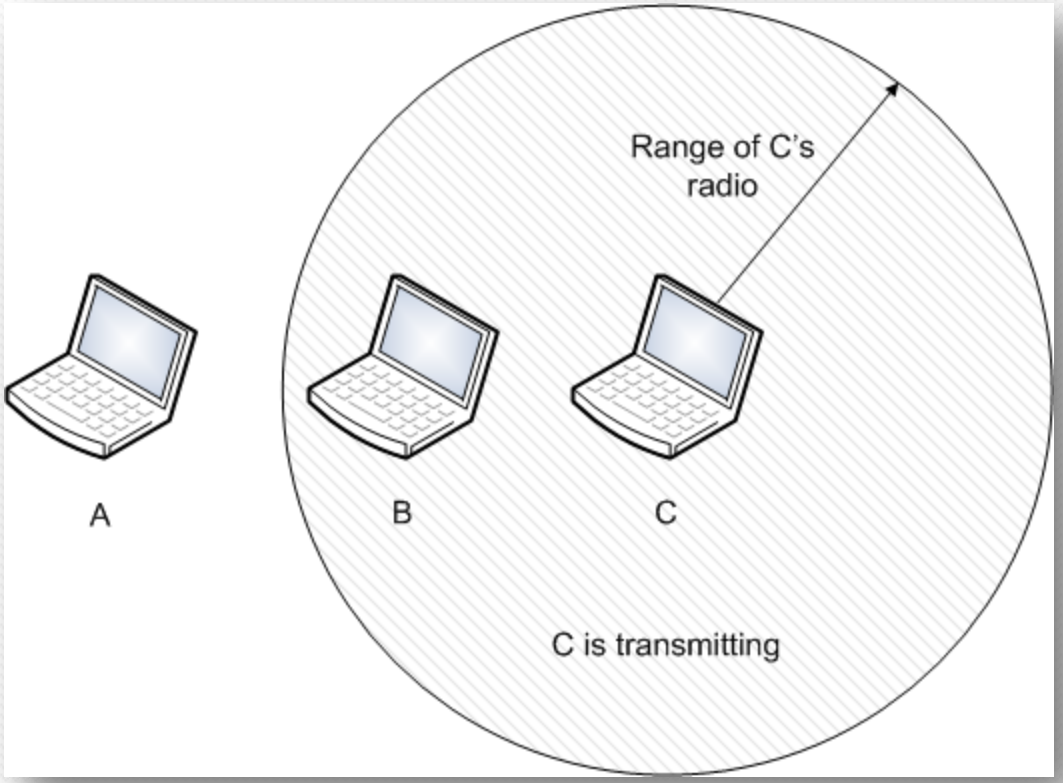
Association process

- Associating process starts at AP which periodically send beacon frames, each of which consist of the AP's SSID and MAC address
- Wireless station scans 11 available channels and tries to catch the bacon frames send from different APs.
- After learning which APs are available in current location system or user chooses one of the APs for association (process can be made automatically by the system)

Association process

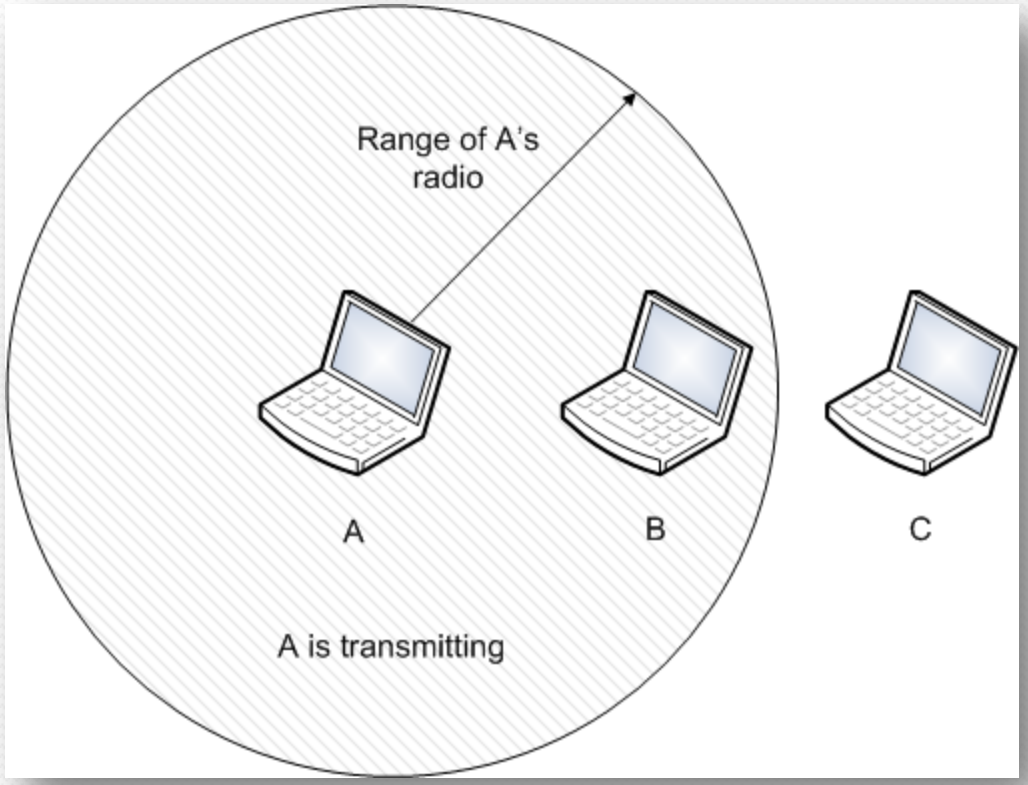
- During the association station is joining the subnet to which selected AP belongs.
- After finishing association, station will send a DHCP message in order to obtain an IP address in subnet.

The 802.11 MAC protocol
The hidden station problem



A wants to send to B but cannot hear that B is busy

The 802.11 MAC protocol
The exposed station problem



B wants to send to C but mistakenly thinks the transmission will fail

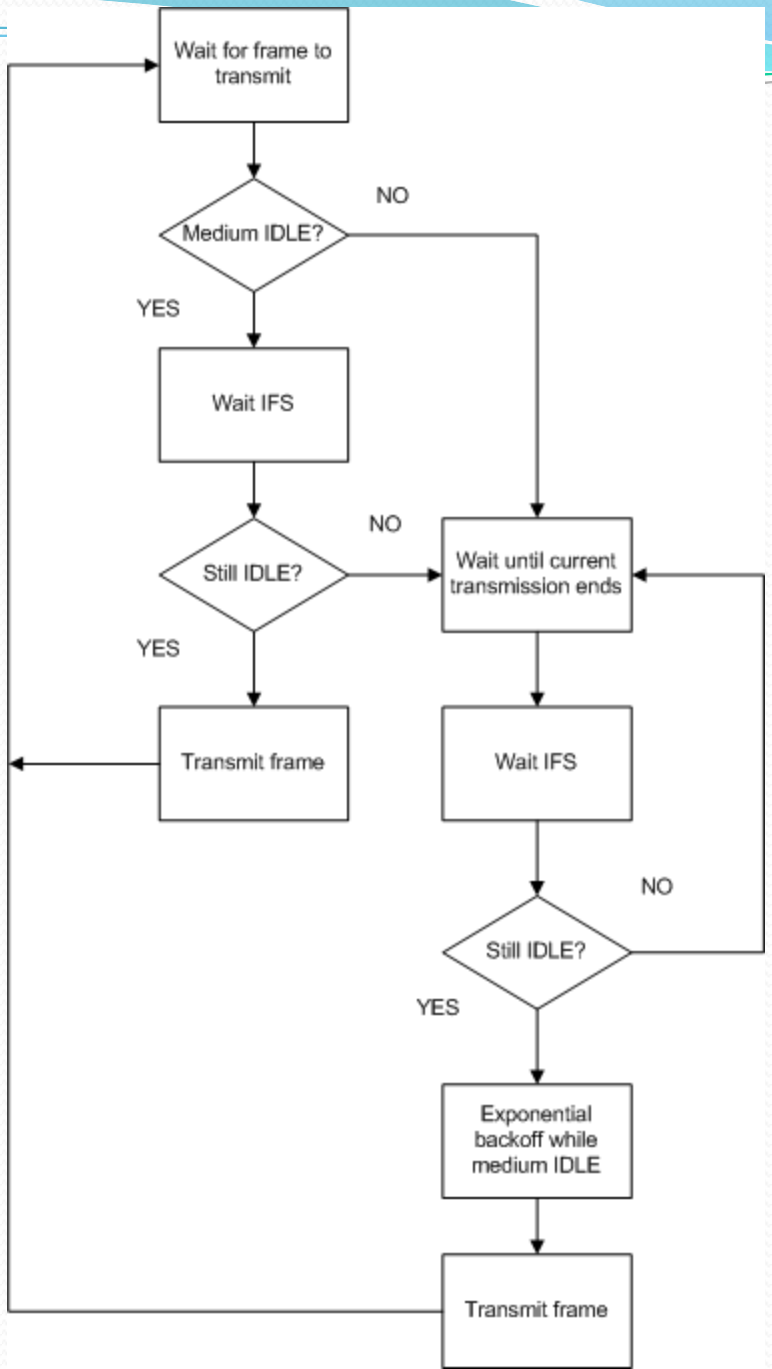
The 802.11 MAC protocol

- To deal with problems of hidden station and exposed station problems 802.11 supports two modes of operation
- **DCF** (**Distributed Coordination Function**) , does not use any kind of central control
- **PCF** (**Point Coordination Function**) , uses the base station to control all activity in its cell
- All implementations must support DCF but PCF is optional

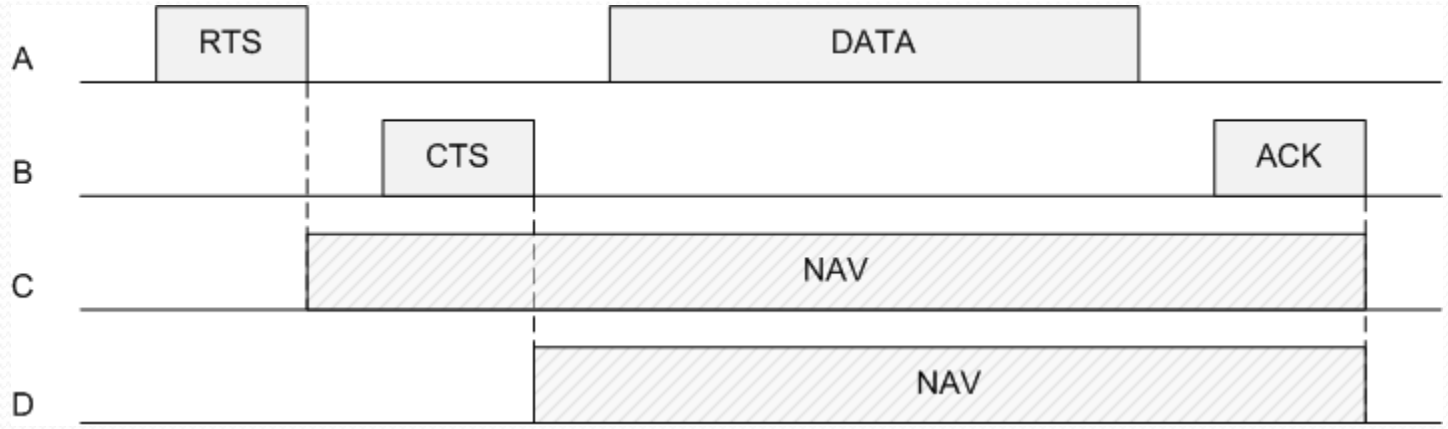
CSMA/CA protocol

- Station ready to transmit
- If channel is idle start transmitting (emits entire frame do not sense channel while sending)
- If channel is busy, defer until channel is idle and than transmit
- If collision occurred, wait random time (binary exponential backoff algorithm) and try again

Medium Access Control Logic



CSMA/CA with RTS/CTS



A transmits data to B

NAV (**Network Allocation Vector**) – signal is not transmitted ; its internal reminder to keep quite for a certain period of time.

PCF (Point Coordination Function)

- The base station polls the other stations, asking them if they have any frame to send
- Transition order is controlled by the base station , no collision ever occurs
- Base station broadcast a beacon frame periodically (10 to 100 times per second).

Interframe time intervals

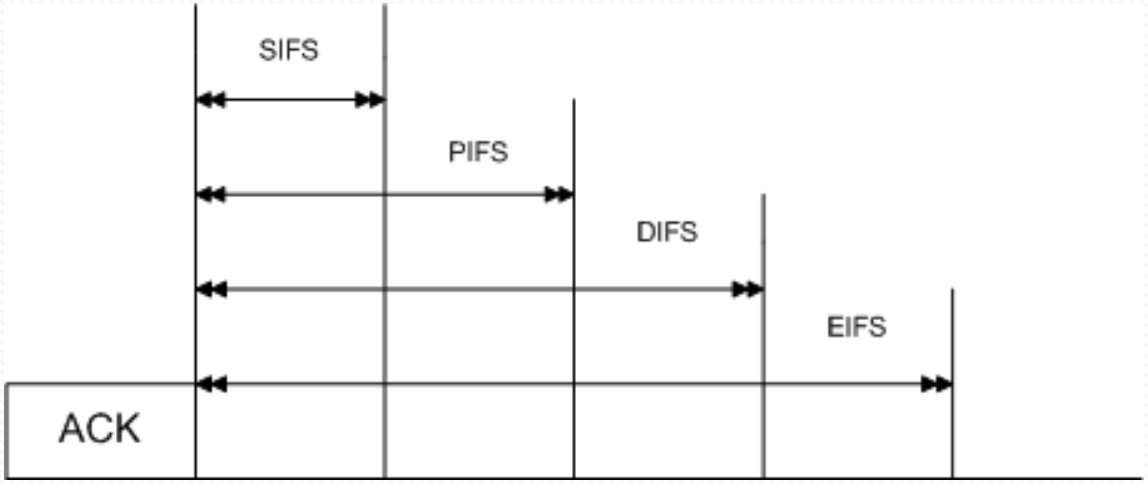
- **SIFS** (Short InterFrame Spacing) – used to allow the parties in a single dialog the chance to go first.
  - Let receiver send CTS in respond to an RTS
  - Let receiver send an ACK for a fragment or full data frame
  - Let sender of a fragment burst transmit the next fragment without having to send an RTS again

- After SIFS interval always exactly one station is entitled to respond.

- If station fails to make use of it chance and a time **PIFS** (**PCF InterFrame Spacing**) elapses, the base station may send a beacon frame or poll frame. It allows sending station to finish sending frame without anyone getting in the way, but gives base station chance to grab the channel.

Interframe time intervals

- If base station has nothing to say and a time **DIFS** (**DCF InterFrame Spacing**) elapses, any station may attempt to acquire the channel to send a new frame.
- **EIFS** (**Extended InterFrame Spacing**) – is used only by station that has just received a bad or unknown frame to report the bad frame.



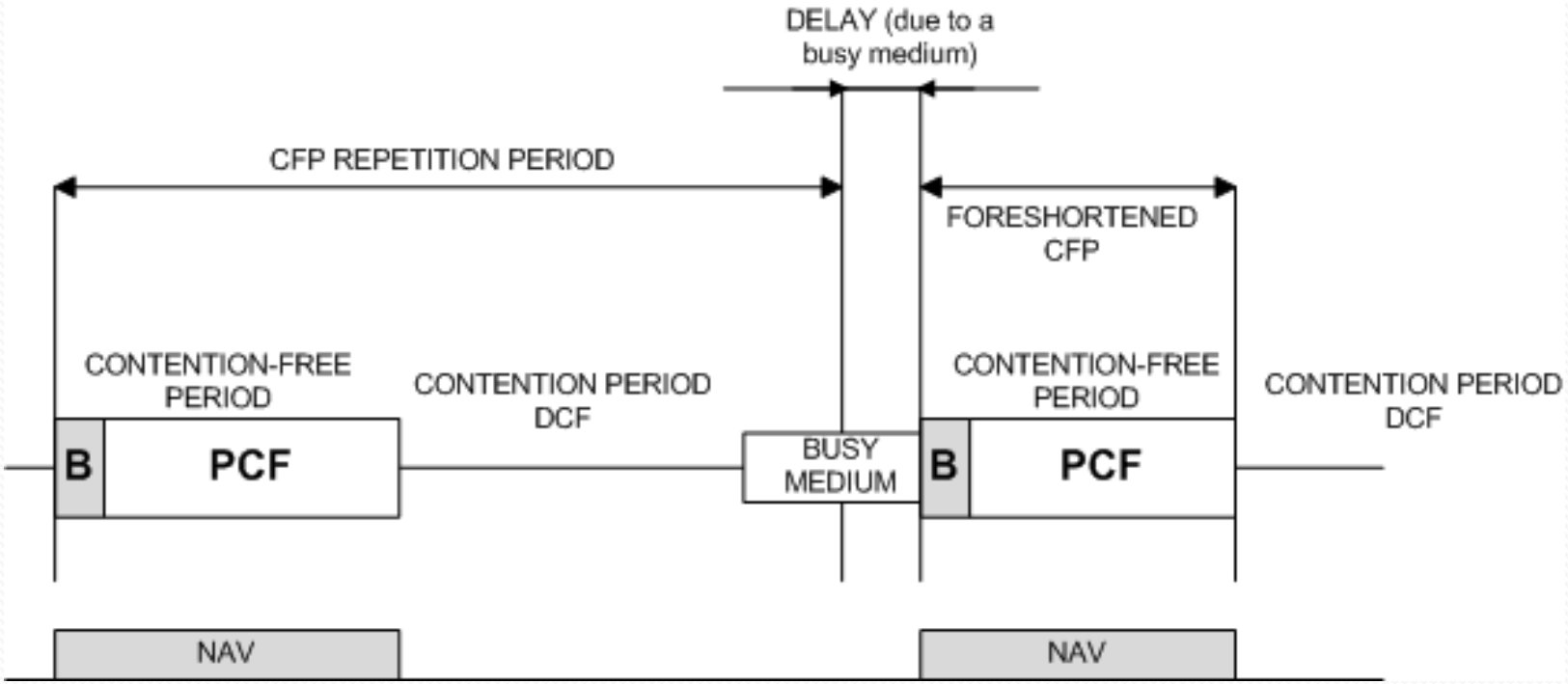
Coexistence of PCF and DCF

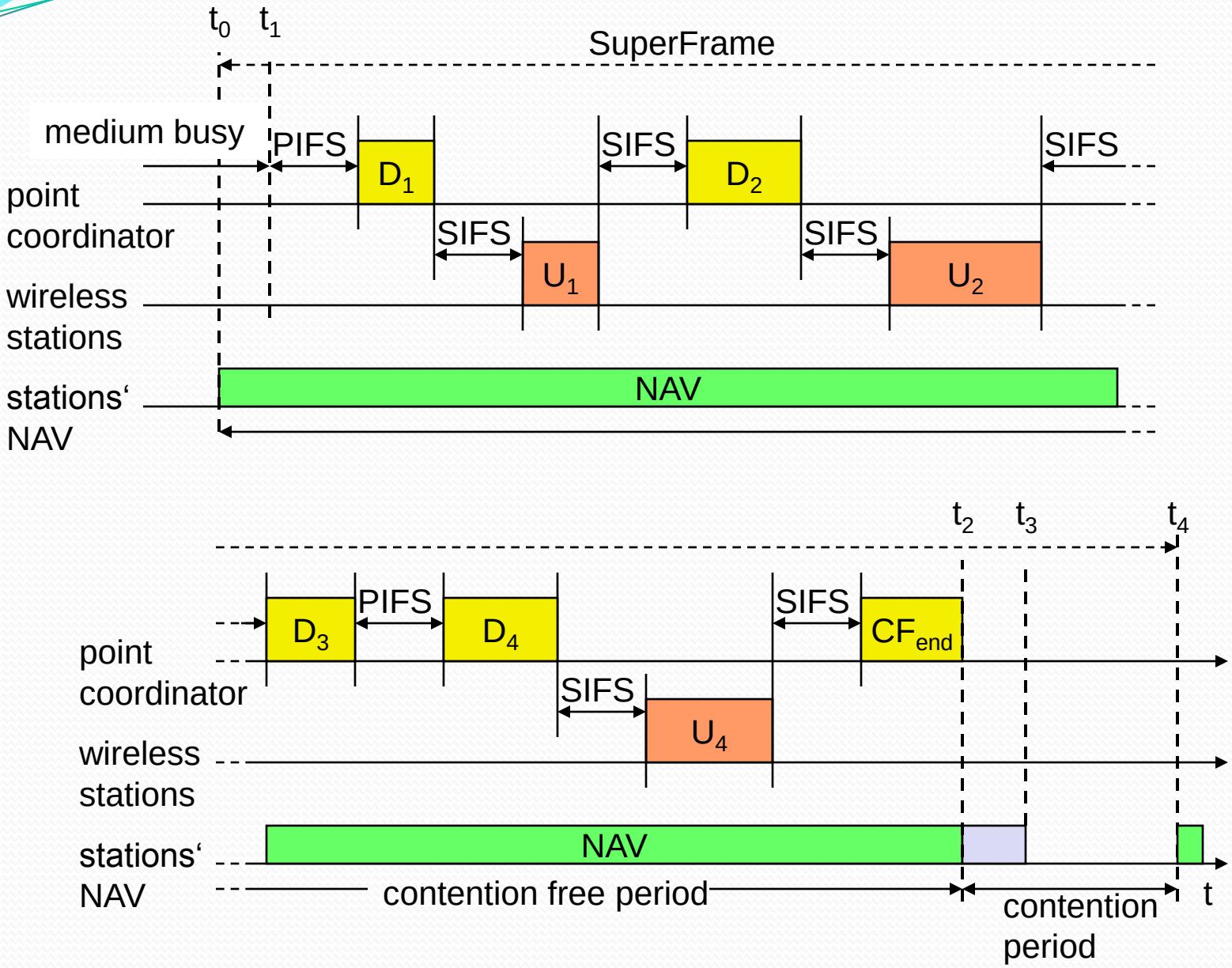
- A **Point Coordinator** (**PC**) resides in the Access Point and controls frame transfers during a **Contention Free Period** (**CFP**)
- Beacon frame send from PC starts the CFP period.
- A **CF-Poll** frame is used by the PC to invite a station to send data. Stations are polled from a list maintained by the PC
- A **CF-End** frame is sent to end the CFP period.
- In between, data transfer takes place to and from PC also to and from one or more STA.

Coexistence of PCF and DCF

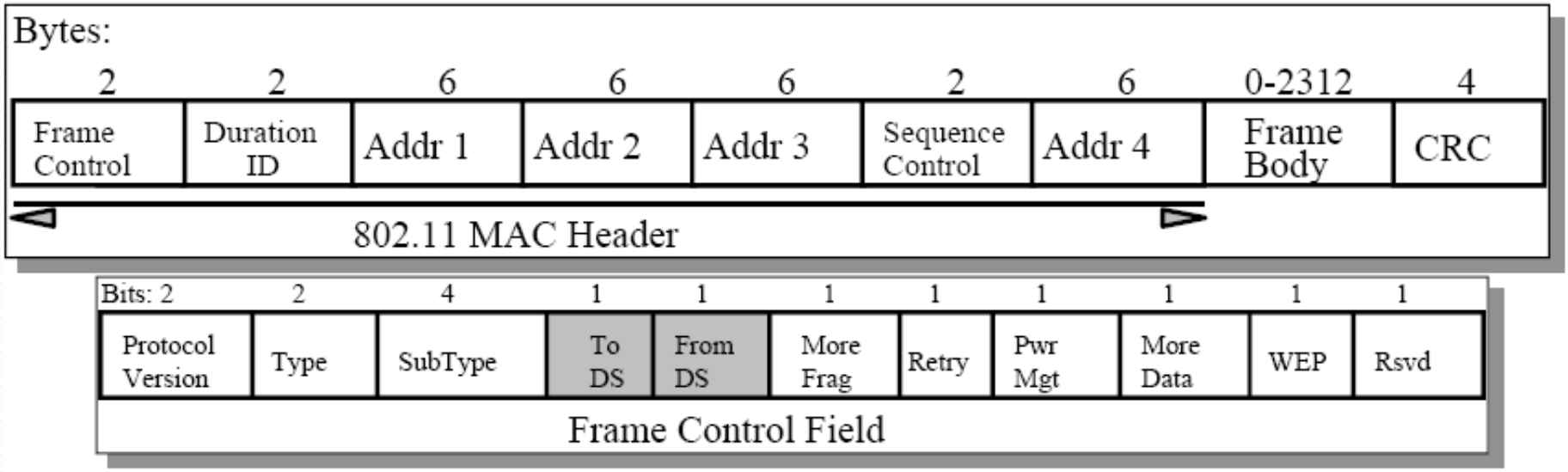
- The CFP alternates with a **Contention Period** (**CP**) in which data transfers happen as per the rules of DCF
- This CP must be large enough to send at least one maximum-sized packet including RTS/CTS/ACK
- CFPs are generated at the CFP repetition rate
- The PC sends Beacons at regular intervals and at the start of each CFP
- The CF-End frame signals the end of the CFP

CFP structure and Timing




t0
t1
SuperFrame
medium busy
PIFS
D1
SIFS
D2
SIFS
point coordinator
SIFS
U1
SIFS
U2
wireless stations
NAV
stations' NAV
t2
t3
t4
D3
PIFS
D4
SIFS
CFend
point coordinator
SIFS
U4
wireless stations
NAV
stations' NAV
contention free period
contention period
t

The 802.11 frame



Notice : The 802.11 frame has four address fields able to hold 6 byte MAC addresses.

The 802.11 frame

- For 802.11 network it is necessary to use three address fields for moving datagram from a wireless station through the Access Point to a router. The forth address is used in ad hoc networks.

- Address 1 field holds the MAC address of the station that is suppose to receive the frame.

- Address 2 field holds the MAC address of station that sends data.

- Address field 3 contains the MAC address of the router to which AP is connected.

The 802.11 frame

- Sequence number helps to distinguishing between a newly transmitted frame and the retransmission of a previous frame.
- The duration value field is used when transmitting station reserves the channel for the time to transmit data frame and ACK.
- Frame control fields type and subtype are used to distinguish the association , RTS, CTS, ACK, and data frames.
- The to and from fields are used to define the meaning of the address fields which meanings change depending whether it is an ad hoc or infrastructure network.
- The WEP field specifies if encryption is being used or not.

The 802.11 frame

- More Frag field specifies that more fragments will come
- Retry bit indicates retransmission of a frame sent earlier
- Pwr Mgt field is used by the base station to put the reciever into sleep state or take it out of sleep
- More Data indicates that sender has more frames for the reciever
- Rsvd bit tell the reciever that a sequence of frames with this bit must be processed strictly in order