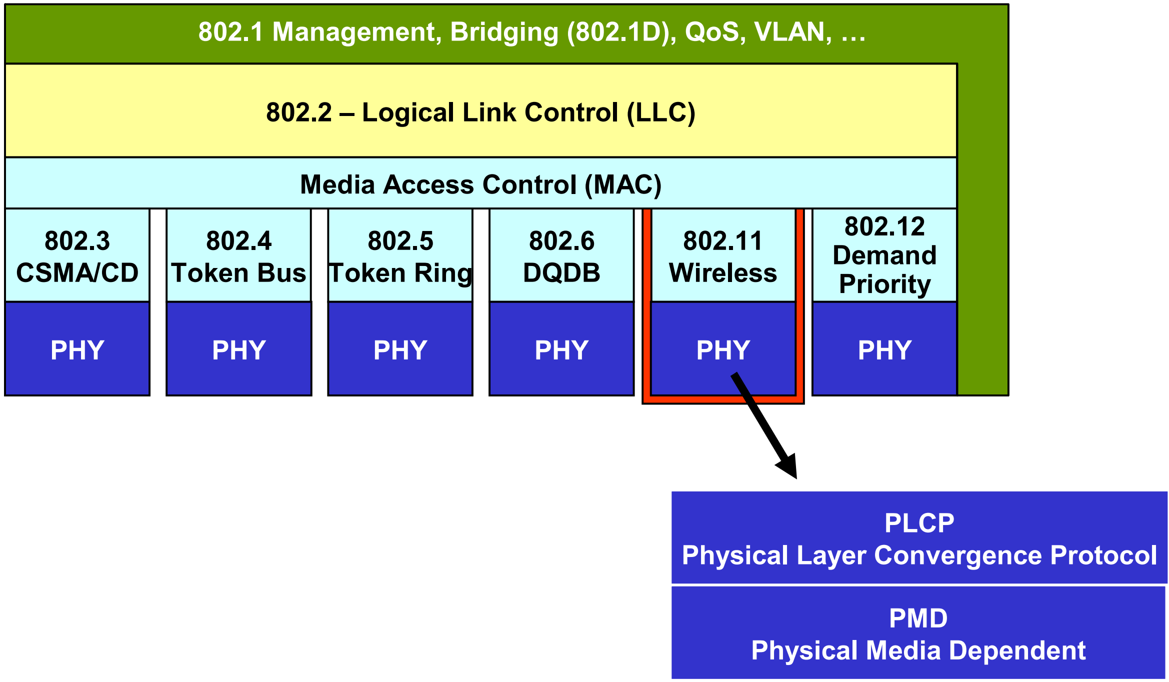
WLAN

Protocol

Protocol Layers

- MAC layer
  - Medium access control
  - Fragmentation
- PHY layer = PLCP + PMD
  - Established signal for controlling
  - Clear Channel Assessment (CCA)
  - Service access point
- Physical Layer Convergence Protocol (PLCP)
  - Synchronization and SFD
  - Header
- Physical Medium Dependent (PMD)
  - Modulation and coding



Clear Channel Assessment

- CCA is an algorithm to determine if the channel is clear
- But what is *"clear"* ?
  - Either measuring only WLAN carrier signal strengths
  - Or measuring the total power of both noise and carriers
- Minimum RX signal power levels should be configured at receivers (APs & clients)
  - CSMA would not allow to send any frames if the environmental noise level is too high
- Part of PHY, used for MAC

FHSS Frame Format

Bits: 80	16	12	4	16	variable
Synchronization	SFD	PLW	PSF	HEC	MAC + Data
PLCP Preamble		PLCP Header			

- PLCP header runs always with 1 Mbit/s
- User data up to 2 Mbit/s
- Synchronization with 80 bit string “01010101…”
- All MAC data is scrambled by a $s_{(z)}=z^7+z^4+1$ polynomial to block any DC component
- Start Frame Delimiter (SFD)
  - Start of the PLCP header
  - 0000110010111101 bit string
- PLCP Length Word (PLW)
  - Length of user data inclusive 32 bit CRC of the user data (value between 0 and 4095)
  - Protects user data
- PLCP Signaling Field (PSF)
  - Describe the data rate of the user data
- Header Error Check (HEC)
  - 16 bit CRC
  - Protect Header

DSSS Frame Format

128	16	8	8	16	16	variable
Synchronization	SFD	Signal	Service	Length	HEC	MAC + Data
PLCP Preamble		PLCP Header				

- PLCP header runs always with 1 Mbit/s (802.11 standard)
- User data up to 11 Mbit/s (802.11b standard)
- Synchronization (128 bit)
  - Also used for controlling the signal amplification
  - And compensation for frequency drifting
- Start Frame Delimiter (SFD)
  - 1111001110100000
- Signal (Rate)
  - 0x0A → 1 Mbit/s (DBPSK)
  - 0x14 → 2 Mbit/s (DQPSK)
  - Other values reserved for future use
    - 11 Mbit/s today with CCK
- Service
  - 0x00 → 802.11 frame
  - Other values reserved for future use
- Length
  - 16 bit instead of 12 bit in FHSS
- Header Error Check (HEC)
  - 16 bit CRC (ITU-T-CRC-16 Standardpolynom)

802.11g and 802.11a use similar frame format

MAC Principles

- Responsible for several tasks
  - Medium access
  - Roaming
  - Authentication
  - Data services
  - Energy saving
- Asynchronous data service
  - Ad-hoc and infrastructure networks
- Realtime service
  - Only infrastructure networks

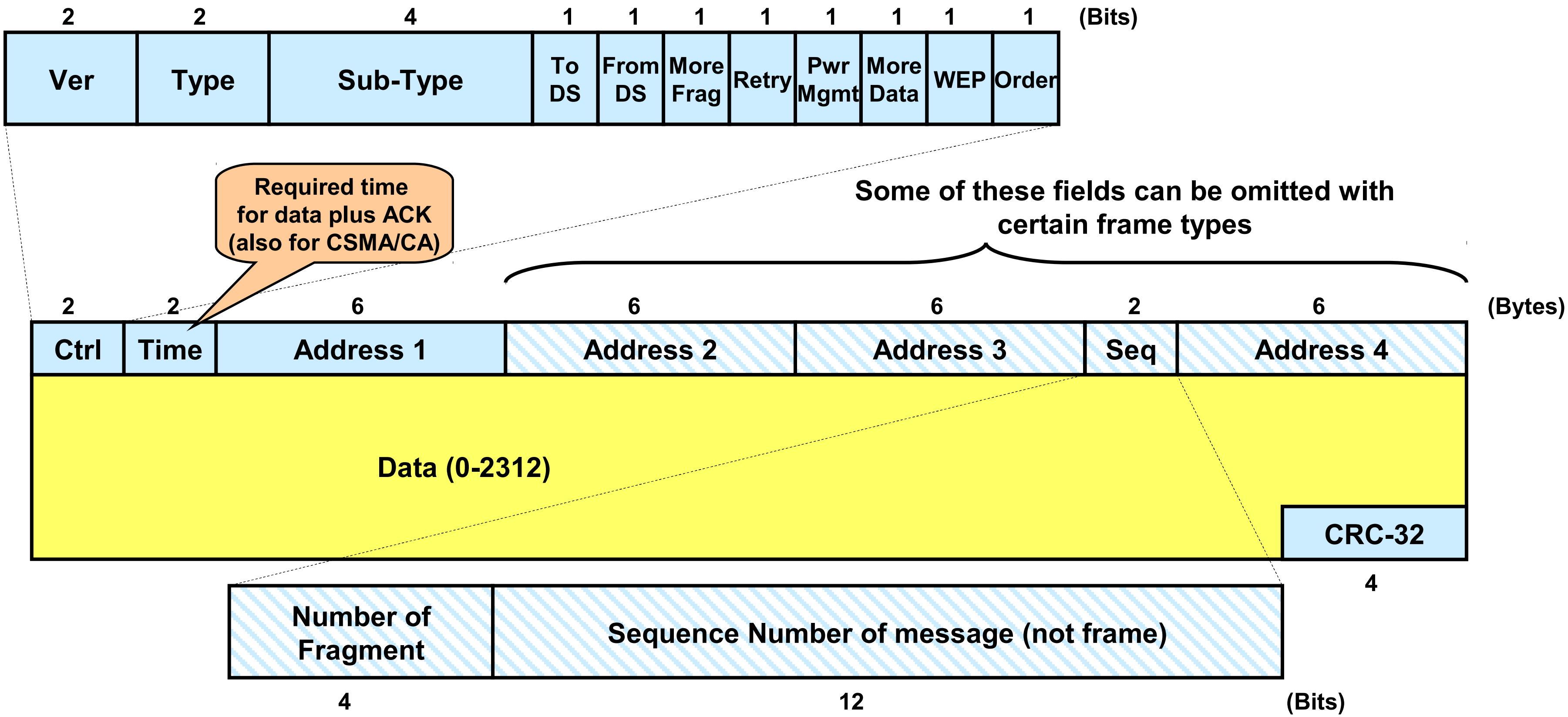
MAC Header – Overview

2	2	6	6	6	2	6	0-2312	4
FC	D-ID	Address 1	Address 2	Address 3	SC	Address 4	Data	CRC

MAC Header (FC through Address 4)

- **Frame Control (FC) includes**
  - Protocol version, frame type
  - Encryption information
  - 2 Distribution System Bits (DS)
- **Duration ID (D-ID) for virtual reservations**
  - Includes the RTS/CTS values
- **Addresses are interpreted according DS bits**
- **Sequence Control (SC) to avoid duplicates**

MAC Header – More Specific



- Header length: 10-30 Bytes
- Total maximum length: 2346 Bytes (without CRC)
- Time field also used for power saving

Header Details – Addresses

Ctrl: To DS	Ctrl: From DS	Address 1	Address 2	Address 3	Address 4	
0	0	Receiver	Sender	Cell	--	Used for all mgmt and ctrl frames. Used for data frames in Ad-hoc or broadcast situations.
0	1	Receiver	Cell	Sender	--	Communication inside BSS: Frame from AP to Receiver. Sender is originator. ACK must be sent to AP.
1	0	Cell	Sender	Receiver	--	Communication inside BSS: Frame from Sender to AP. Should be relayed to receiver.
1	1	Cell	Cell	Receiver	Sender	Communication between APs. Address1 is receiving AP, address2 is sending AP.

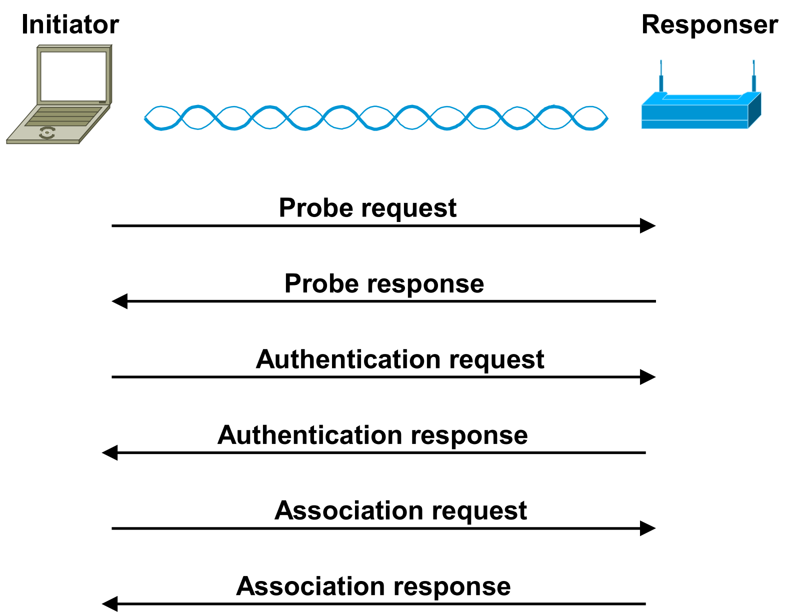
- **Infrastructure network:**
  Cell address = AP's MAC address

Note

- **If an AP is used, ANY traffic runs over the AP**
  - **Because stations do not know whether receiver is associated to this AP or another AP**
- **Cell address = AP‘s MAC address**
  - **Always specified in header**
  - **Not *needed* in Ad-hoc network**

Service Set Management Frames

- **Beacon frame**
  - Sent periodically by AP to announce its presence and relay information, such as timestamp, SSID, and other parameters
  - Radio NICs continually scan all 802.11 radio channels and listen to beacons as the basis for choosing which access point is best to associate with
- **Probe request frame**
  - Once a client becomes active, it searches for APs in range using probe request frames
  - Sent on every channel in an attempt to find all APs in range that match the SSID and client-requested data rates
- **Probe response frame**
  - Typically sent by APs
  - Contains synchronization and AP load information (also other capabilities)
  - Can be sent by any station (ad hoc)



Authentication and Association

- Authentication frame
  - AP either accepts or rejects the identity of a radio NIC
- Deauthentication frame
  - Send by any station that wishes to terminate the secure communication
- Association request frame
  - Used by client to specify: cell, supported data rates, and whether CFP is desired (then client is entered in a polling list)
- Association response frame
  - Send by AP, contains an acceptance or rejection notice to the radio NIC requesting association
- Reassociation request frame
  - To support reassociation to a new AP
  - The new AP then coordinates the forwarding of data frames that may still be in the buffer of the previous AP waiting for transmission to the radio NIC
- Reassociation response frame
  - Send by AP, contains an acceptance or rejection notice to the radio NIC requesting reassociation
  - Includes information regarding the association, such as association ID and supported data rates
- Disassociation frame
  - Sent by any station to terminate the association
  - E. g. a radio NIC that is shut down gracefully can send a disassociation frame to alert the AP that the NIC is powering off

Beacon Details

- Clients verify their current cell by examine the beacon
- Beacon is typically sent 10 times per second
- Information carried by beacon:
  - Timestamp (8 Bytes)
  - Beacon Interval (2 Bytes, time between two beacons)
  - Cell address (6 Bytes)
  - All supported data rates (3-8 Bytes)
  - Optional: FH parameter (7 Bytes, hopping sequenz, dwell time)
  - Optional: DS parameter (3 Bytes, channel number)
  - ATIM (4 Bytes, power saving in ad-hoc nets) or TIM (infrastructure nets)
  - Optional but very common: vendor-specific INFORMATION ELEMENTS (IEs)
- Problem: Beacons reveals features and existence of cell

SSID

- 32 bytes, case sensitive
  - Spaces can be used, but be careful with *trailing* spaces
- Multiple SSIDs can be active at the same time; assign the following to each SSID:
  - VLAN number
  - Client authentication method
  - Maximum number of client associations using the SSID
  - Proxy mobile IP
  - RADIUS accounting for traffic using the SSID
  - Guest mode
  - Repeater mode, including authentication username and password
- Only "Enterprise" APs support multiple SSIDs
  - Cisco: 16
  - One broadcast-SSID, others kept secret
  - Repeater-mode SSID

```
AP# configure terminal
AP(config)# configure interface dot11radio 0
AP(config-if)# ssid batman
AP(config-ssid)# accounting accounting-method-list
AP(config-ssid)# max-associations 15
AP(config-ssid)# vlan 3762
AP(config-ssid)# end
```

The IEEE 802.11 Protocol

CSMA/CA

Access Methods - CSMA/CA

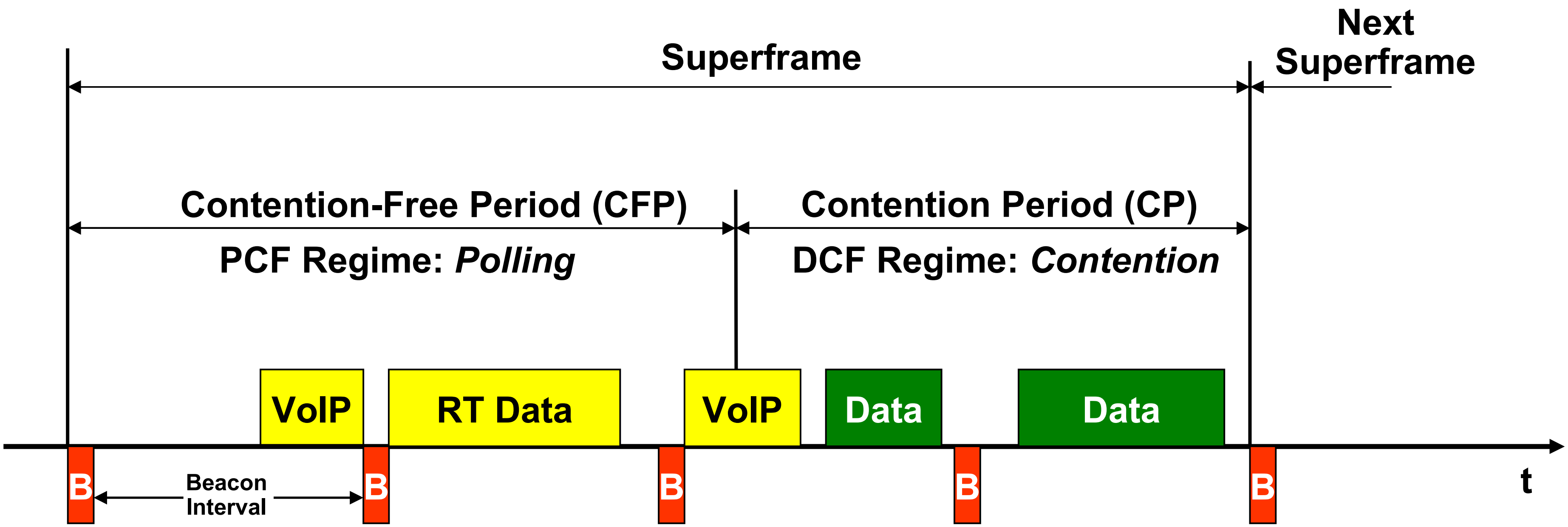
"Distributed Foundation Wireless Medium Access Control" (DFWMAC)

→ DCF (CSMA/CA)

→ PCF

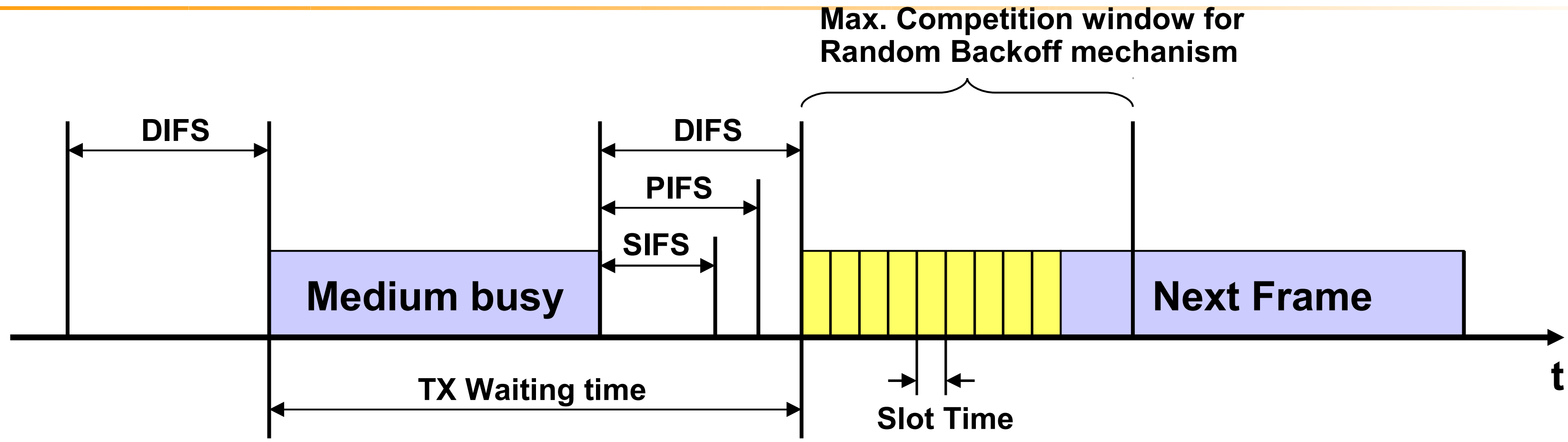
- **Distributed Coordination Function (DCF)**
  - Asynchronous data service
  - Optionally with RTS/CTS
- **Point Coordination Function (PCF)**
  - Intended for realtime service (e. g. VoIP)
  - Polling method
  - Optional

Superframe



- Beacon is sent by "Point Coordinator" (PC=AP)
- Minimum CP period guaranteed
  - To avoid starvation of non-realtime data
  - At least one frame can be sent
- Note: Poll-Frames and ACKs omitted in this picture!

CSMA Access Method



Basic Ideas

- **No standing waves in free space => no Ethernet-like collision detection possible**
- **Collision is detected by missing ACKs!**
- **Truncated Random Exponential Backoff like in Ethernet and 802.3**
- **Simple fragmentation mechanism**
  - **Ethernet compatibility**
  - **Performance (interferences)**
- **CCA to determine medium state**
- **CSMA: "Listen before talk"**
- **A safety Inter-frame Space (DIFS | PIFS | SIFS, plus Backoff) must be awaited before TX**

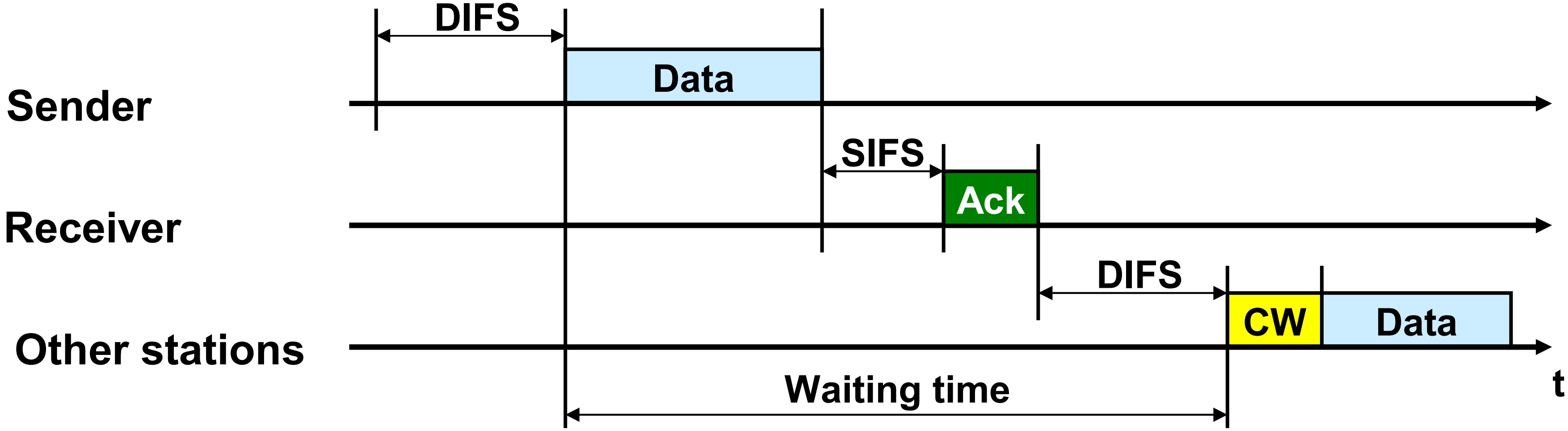
Details

- CW is multiple of Ethernet slot time
  - If medium is busy: Backoff
  - Slot time: 47 µs (9 µs)
- DCF Inter-Frame Space (DIFS)
  - Longest waiting time, 128 µs (34 µs)
  - Used for asynchronous data services
- PCF Inter-Frame Space (PIFS)
  - Used for APs to stop user communication, 78 µs (25 µs)
- Short Inter-Frame Space (SIFS)
  - Shortest waiting time, highest priority, 28 µs (16 µs)
  - Used for ACKs

Backoff Policies

- Random backoff reduces collisions
- Competition window (CW)
  - Start value of 7 slot times
  - After every collision → CW doubled
  - To a max of 255
- Post-backoff
  - After successful transmission
  - To avoid "channel-capture"
- Exception: Long silent durations
  - Station may send immediately after DIFS

CSMA/CA in Action

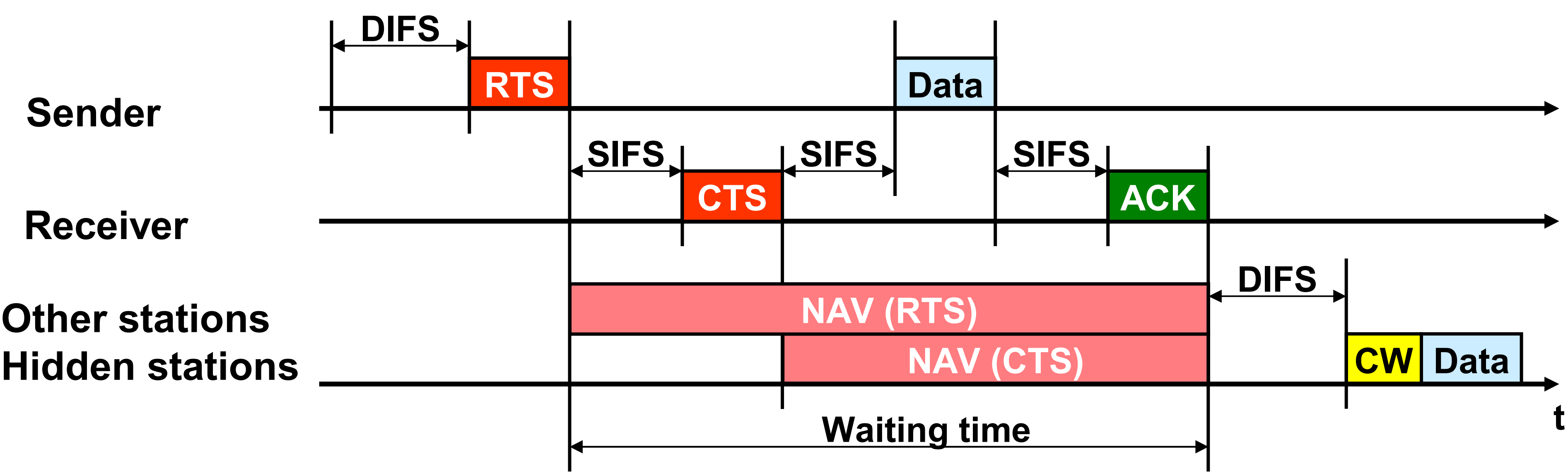


- **Point-to-point communication**
- **Acknowledgment is send after SIFS**
  - **Before all other communications**
  - **Guaranteed collision free**
- **Re-transmitted frames have no higher priority over other frames**

CSMA/CA with RTS/CTS

- Avoid the problem of invisible devices or "Hidden Stations"
  - Station receives data from two other devices
  - The two other devices didn‘t see each other
  - Each device thinks medium is free → Collision
- 2 special packets → RTS and CTS
  - Every station must listen to this packets

Four-way handshake:
1. RTS
2. CTS
3. Data
4. ACK

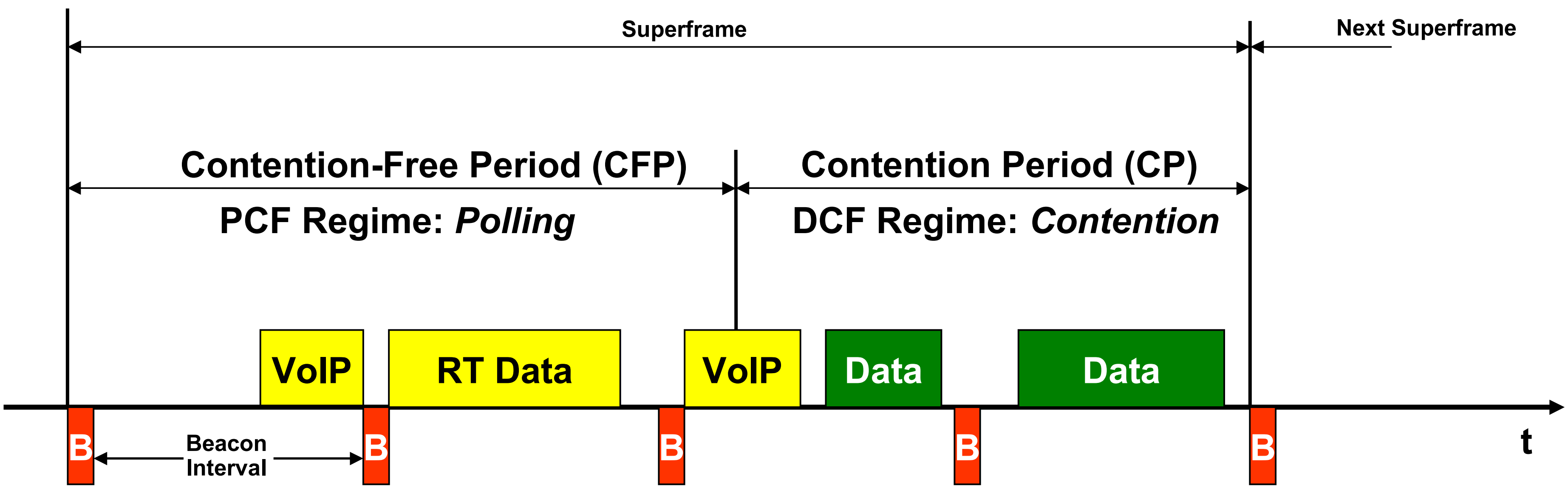


RTS/CTS => "Virtual Reservation"

- Collision can only occur at the begin or after a transmission
- Much more overhead
  - RTS/CTS packets increase the total access-delay
- Usage guidelines
  - Only when longer frames are sent on average (> 500 Bytes)
  - When hidden stations are expected

PCF – Polling Principle

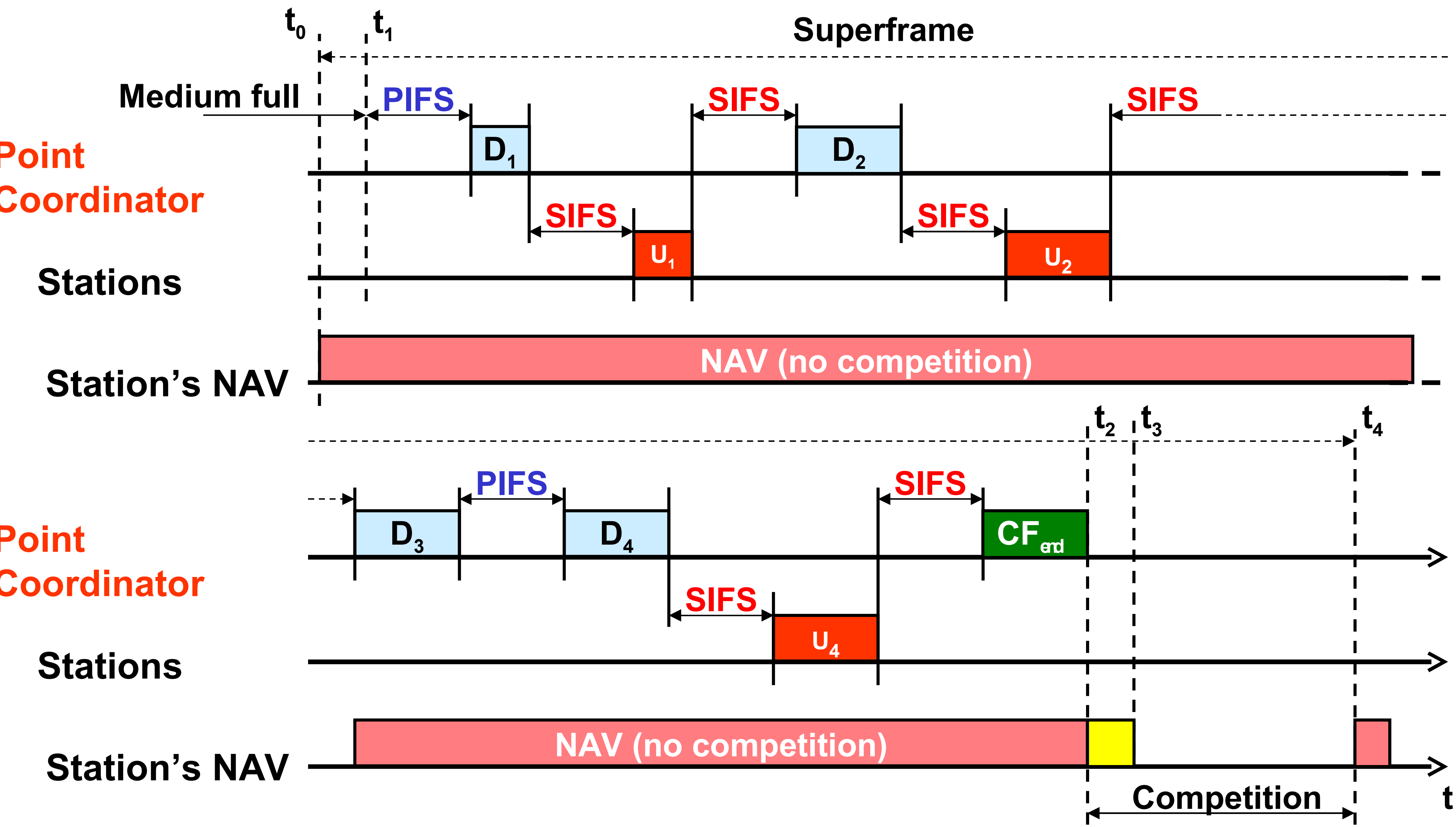
- Guaranteed transmission parameters
  - Minimum data rate
  - Maximum access-delay
- AP necessary (!)
  - For medium access control
  - Polling and time-keeping
  - Acts as "point coordinator“
- Point Coordinator (PC) splits access time into a Superframe
  - Contention-free period (PCF method)
  - Contention period (DCF method)
- Target Beacon Transmission Time (TBTT) is announced in each beacon



CFP Policy

- Beacon starts CFP by announcing maximum duration of CFP
  - Can be multiple of Beacon intervals
  - Intermediate Beacons indicate the remaining CFP duration
- Between two successive CFPs there must be space to send at least on frame in the CP mode!
- The AP may finish the CFP earlier!
  - Sending the CF-End Control Frame
- CFP is *optional*
  - CSMA/CA-only clients must not interfere
  - CFP also relies on CSMA/CA

PCF Medium Access



PCF Algorithm

- At t_0 starts the competition free zone
- Medium gets free at t_1
- After PIFS the PC can access the medium
  - No other station can access because PIFS is smaller than DIFS
- Now PC polls first station (D1)
- Stations may answer with user data after SIFS
- Stations must Ack within PIFS
  - PIFS is shortest idle period within CFP
- All frames are sent through AP !!!
- AP maintains list of all stations that should be polled
  - Announced by association process
  - PC continuously polls listed stations
- PC can send data together with beacon (piggy-back)
- By sending a CF_{end} frame the PC starts the CP

802.11g/b Compatibility

- "b" expects CCK preamble and cannot detect OFDM signals
  - Therefore collisions with legacy "b"
- Compatibility mode
  - g-devices only use RTS/CTS
    - Always 1 Mbit/s and BPSK
    - Newer "g" sends a CCK-based CTS before each OFDM-based data frame
  - "g" suffers from reduced throughput
    - 8-14 Mbit/s instead of 22 Mbit/s
- "g" reaches longer distances (=>OFDM)
  - Cell design must consider b-only clients
  - Only when same power level used !

Realtime Problems with 802.11

- Available BW is shared among clients
- No traffic priorities
- Once a station gains access it may keep the medium for as long at it choses
  - Low bitrate stations (e. g. 1 Mbit/s) will significantly delay all other stations
- No service guarantees
- PCF does not support traffic classes
  - However, the PCF is typically not implemented in APs and client adapters

Specific PCF Problems

- Irregular Beacon delays
  - Stations may finish each transmission even if TBTT already expired
  - Up to 2304 bytes (2312 bytes if encrypted, new: even 2342 bytes allowed)
  - Station may even send all fragments of a L2-fragmented packet
- Hidden station and interferences
- No traffic classes means: All applications have equal TX opportunity

802.11e – EDCF and HCF

- New coordinate functions relying on Traffic Classes (TCs)
- Enhanced DCF (EDCF)
  - Better CHANCES for high-priority classes
  - But NO GUARANTEES ("best effort QoS")
  - Performed within CP
- Hybrid Coordination Function (HCF)
  - Is an enhanced PCF
  - Allows precise QoS configurations on the HC:
    - BW control
    - Guaranteed throughput
    - Fairness between stations
    - Classes of traffic
    - Jitter limits
  - Performed within CFP

802.11e – HCF Details

- Stations announce their TC queue lengths
- The Hybrid Coordinator (HC=AP) does not need to follow round robin but any coordination scheme
- Stations are given a Transmit Opportunity (TXOP)
  - They may send multiple packets in a row, for a given time period
- During the CP, the HC can resume control of the access to the medium by sending CF-Poll packets to stations
- Also allows to send multiple data frames followed by single ACK

802.11e – Facts

- Concept Summary
  - CP allows to prioritize certain TCs instead stations
    - More important traffic classes will be preferred—statistically
  - CFP allows bandwidth reservation by stations and non-round-robin polling
    - Not yet implemented (Fall 2004)
- Hybrid Controller (HC) required
  - Controls all other "enhanced stations"
  - Typically implemented within AP (not necessarily)
  - "QBSS" instead of BSS
- Main driver for QoS is "Voice over Wireless IP" (VoWIP)

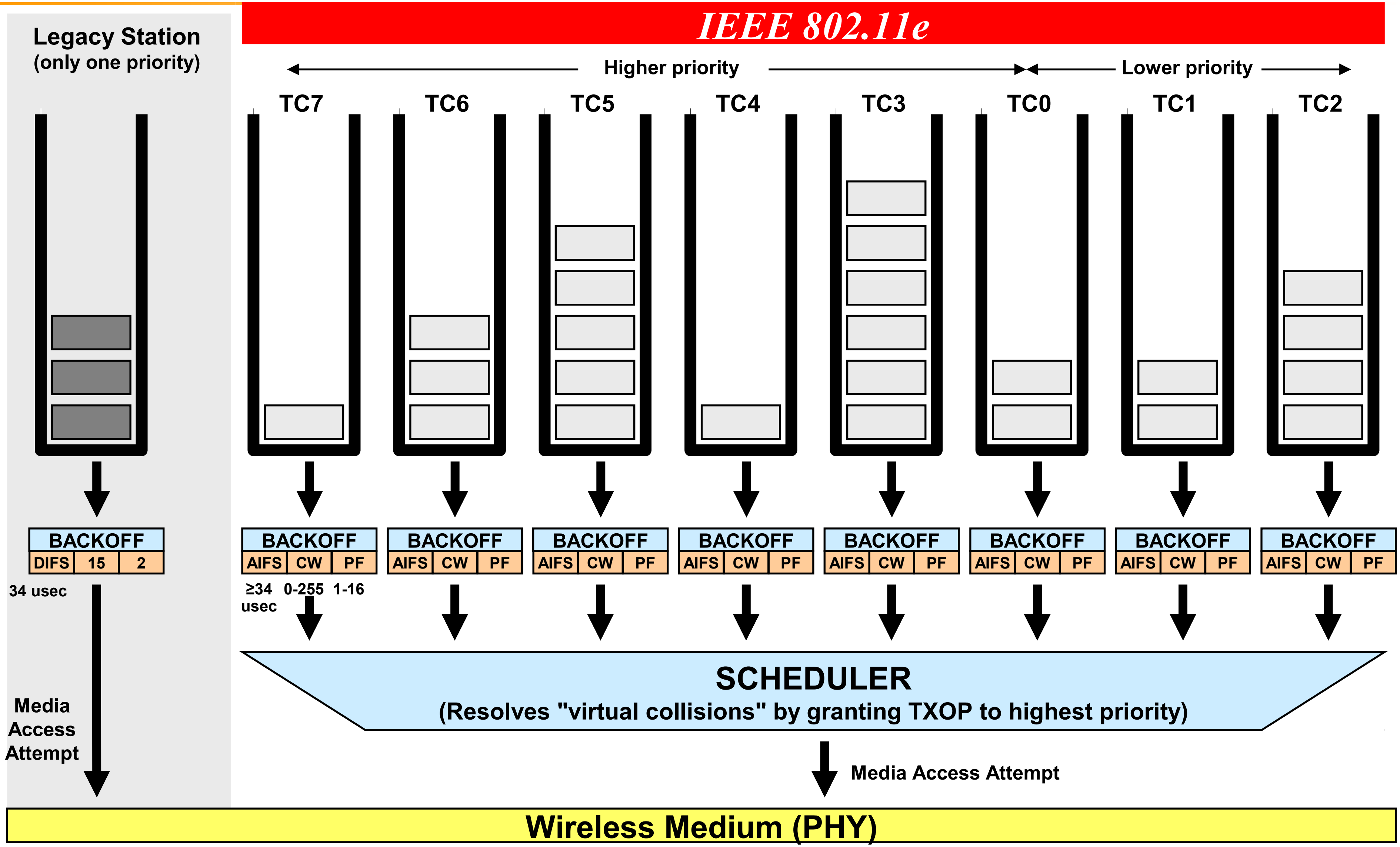
802.11e – Algorithm (1)

- All traffic is separated into TCs
  - Enhanced stations must maintain a separate back-off timer for each TC
- Up to 8 priority queues for each TC
  - "Virtual Stations" inside enhanced stations
- Each TC has different priority value
  - To avoid collisions if the counters of two TCs expire
- TCs compete within Arbitration Interframe Space (AIFS)
  - Different AIFS for each TC possible
  - At least one DIFS long
- Persistence factor (PF) solves collision
  - Used to calculate new back-off values
  - PF=1..16
- Legacy stations must have a CWmin=15 and PF=2

802.11e – Algorithm (2)

- Transmission Opportunity (TXOP)
  - Time slot during a station may send
- EDCF-TXOP
  - Issued by EDCF algorithm
  - Limited by system-wide TXOP-limit announced in beacon frames
- Polled-TXOP
  - Issued by HCF
  - Limited by parameter announced in poll-frame
- HCF can redefine TXOP at each time
  - And finish the CP earlier
- HC also supports controlled contention
  - Polling frames announce sending desire of other stations
  - Legacy stations must wait until end of controlled contention period

802.11e – Queuing Concept



WiFi Multimedia – WMM

- WMM implements a subset of 802.11e to satisfy urgent QoS needs
  - Certification start: 09/2004
- Only supports prioritized media access:
  - 4 access categories per device: voice, video, best effort, and background
  - Does not support guaranteed throughput

Legacy QoS

- ***Most legacy (no 802.11e) APs only support downstream QoS***
  - On the AP, create QoS policies and apply them to VLANs
  - If you do not use VLANs on your network, you can apply your QoS policies to the access point's Ethernet and radio ports
- ***Note: APs do not classify packets!***
  - Only already classified packets are prioritized (DSCP, client type, 802.1p)
  - EDCF-like queuing is performed on the Radio port; only FIFO on Ethernet egress port
  - Only 802.1Q tagging supported – no ISL !!!

802.1x and WAN Congestion

- Congestion on WAN links: prioritize 802.1x packets
- Classify and mark RADIUS packets using the Cisco Modular QoS Command Line (MQC)
  - Method to determine the appropriate queue size for the 802.1x/RADIUS packets
  - And to determine how to enable queuing on router interfaces

```
ip access-list extended LEAPACL                           !!! Create ACL for interesting traffic
 permit udp any host 172.24.100.156 eq 1645

class-map match-any LEAPCLASS                             !!! Classify
 match access-group name LEAPACL

policy-map MARKLEAP                                       !!! This is a policy group
  class LEAPCLASS
   set ip dscp 26                                         !!! Corresponds to AF31 (Class=3, 1=low drop)

interface FastEthernet0/0.100                             !!! Attach marker on interface
 encapsulation dot1Q 100
 service-policy input MARKLEAP                            !!! Mark inbound (input) packets only

policy-map LEAPQUEUE
  class LEAPCLASS
   bandwidth 8                                            !!! 8kb/s if needed (dynamical management)

interface Serial3/0:0                                     !!! Attach policy-map on WAN interface
 ip address 172.24.100.66 255.255.255.252
 load-interval 30
 service-policy output LEAPQUEUE
```