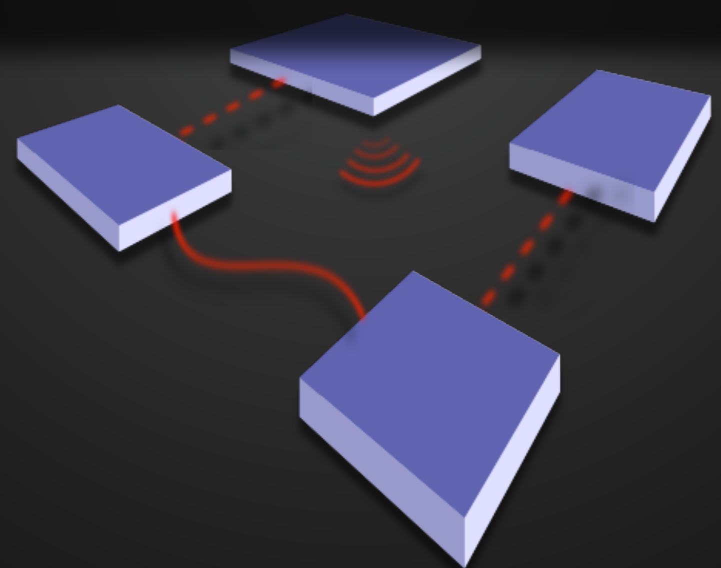
CS-435
spring semester 2025

Network Technology & Programming Laboratory

University of Crete
Computer Science Department

Stefanos Papadakis



CS-435

Lecture #13 preview

- 802.11e
- WEP, WPA
- 802.11i

802.11 access methods

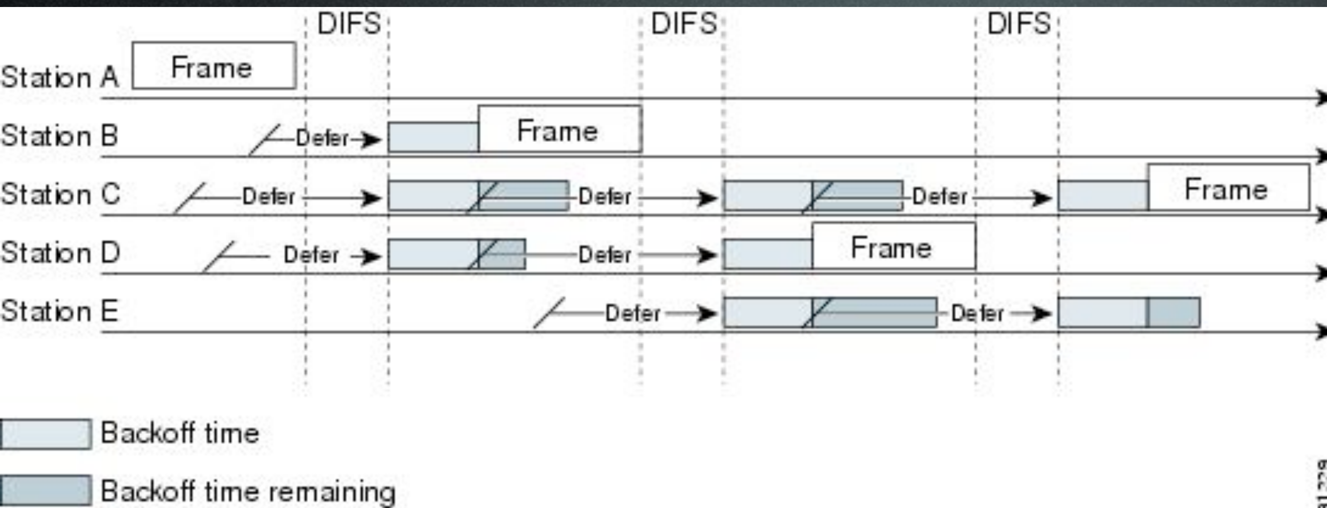
- **DCF** (Distributed Coordination Function)

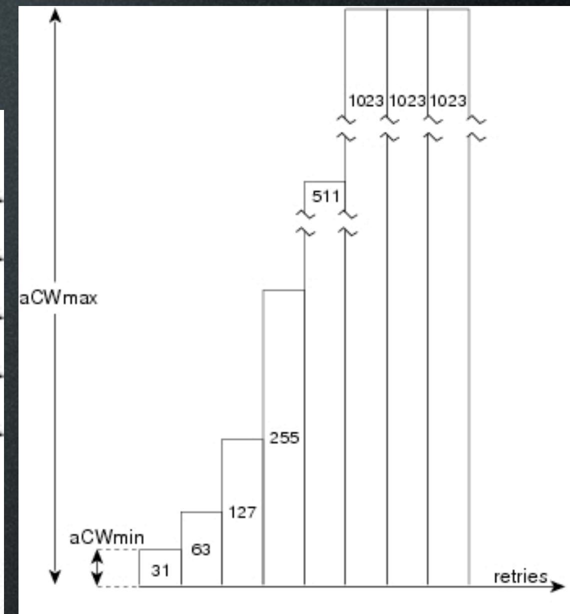
- **PCF** (Point Coordination Function)
  - Time divided into Contention Period (**CP**) and Contention Free period (**CFP**)
  - During **CP**, transfers use **DCF**, i.e., Data-ACK, or RTS-CTS-Data-ACK, with exponential back-off etc.
  - During **CFP**, the AP controls all transmissions: which STA transmits to the AP and which STA receives data from the AP.
  - All STAs may transmit/receive packets during the CFP. The ability to transmit during the CFP is optional.
  - No RTS/CTS in CFP

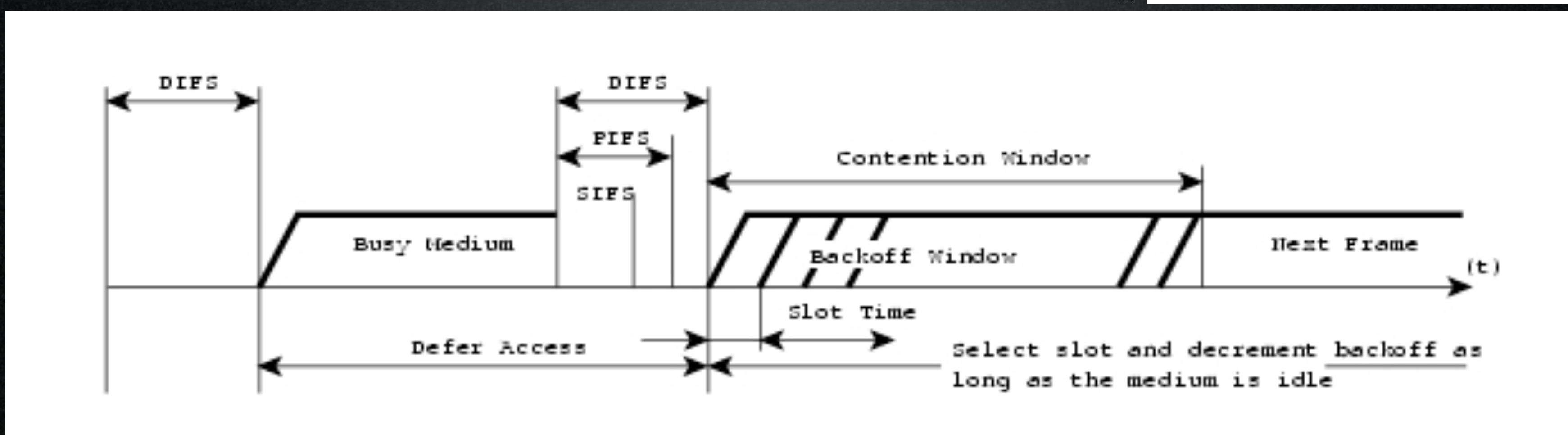
802.11 access methods

- **DCF** (Distributed Coordination Function)
  - DIFS: DCF Interframe space
  - SIFS: Shortest Interframe space
  - DIFS = SIFS + 2 * SlotTime
- **PCF** (Point Coordination Function)
  - PIFS: PCF Interframe Space

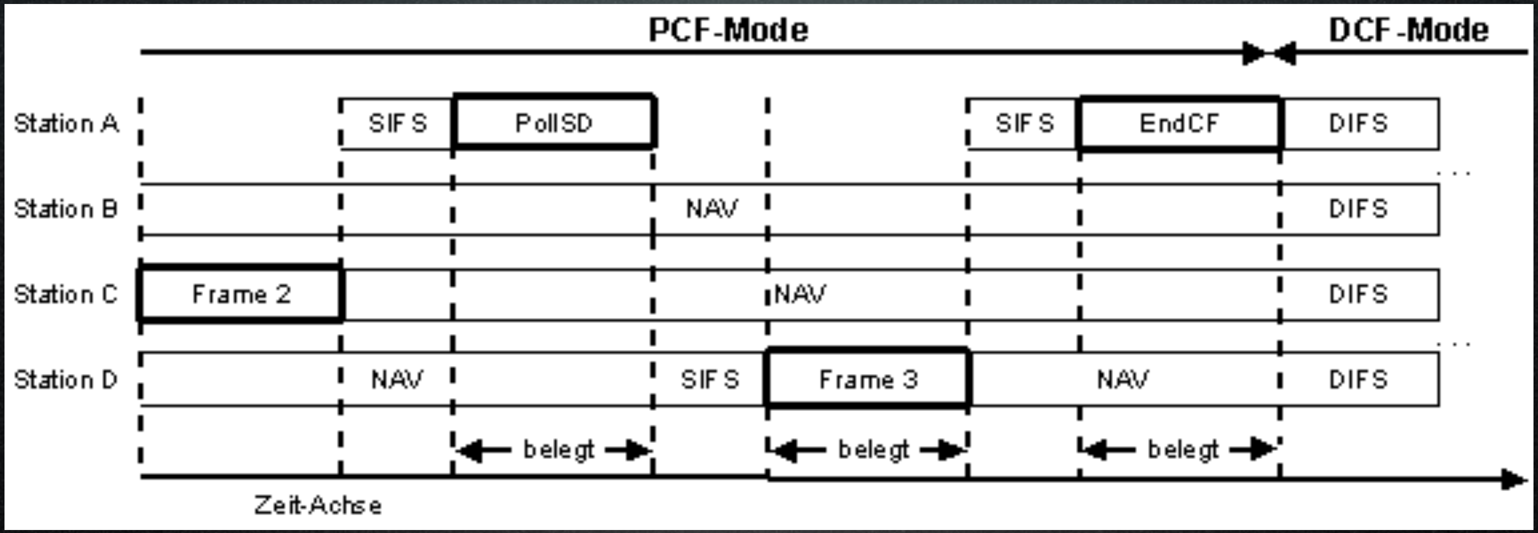
DCF


DIFS
DIFS
DIFS
Station A
Frame
Station B
Defer
Frame
Station C
Defer
Defer
Defer
Frame
Station D
Defer
Defer
Frame
Station E
Defer
Defer
Backoff time
Backoff time remaining
91229


aCWmax
aCWmin
31
63
127
255
511
1023
1023
1023
retries


DIFS
DIFS
PIFS
SIFS
Contention Window
Busy Medium
Backoff Window
Next Frame
(t)
Slot Time
Defer Access
Select slot and decrement backoff as long as the medium is idle

PCF



PCF-Mode
DCF-Mode
Station A
SIFS
PollSD
SIFS
EndCF
DIFS
Station B
NAV
DIFS
Station C
Frame 2
NAV
DIFS
Station D
NAV
SIFS
Frame 3
NAV
DIFS
belegt
belegt
belegt
Zeit-Achse

Polling during CFP

- STAs can only transmit data one SIFS after being polled & only one frame
- If the pollable STA transmits a frame in response to a CF-poll but does not receive an ACK, then it cannot retransmit until it is polled again or until the CP.
- A STA can set the MoreData bit is set
    - The more data bit is in the MAC header. The STA can only set it when responding to a CF-poll request.
- A STA should respond to a poll within SIFS. If not, the AP will regain control PIFS after the CF-poll was sent.
- If a STA has no data to respond with but the CF-poll had data (Data+CF-poll or Data+CF-ACK+CF-poll), then the STA responds with CF-ACK, with no data
- If the STA is polled without data (i.e., CF-poll or CF-ACK + CF-poll), then it should sent a null frame (no data). This ensures that the AP does not think that that STA missed the due to radio transmission error.

QoS Limitations of 802.11

- DCF
  - Only supports best-effort services
  - No guarantee in bandwidth, packet delay and jitter
- PCF
  - Unpredictable beacon frame delay due to incompatible cooperation between CP and CFP modes
  - Transmission time of the polled stations is unknown
  - The Point Coordinator (PC) does not know the QoS requirement of traffic

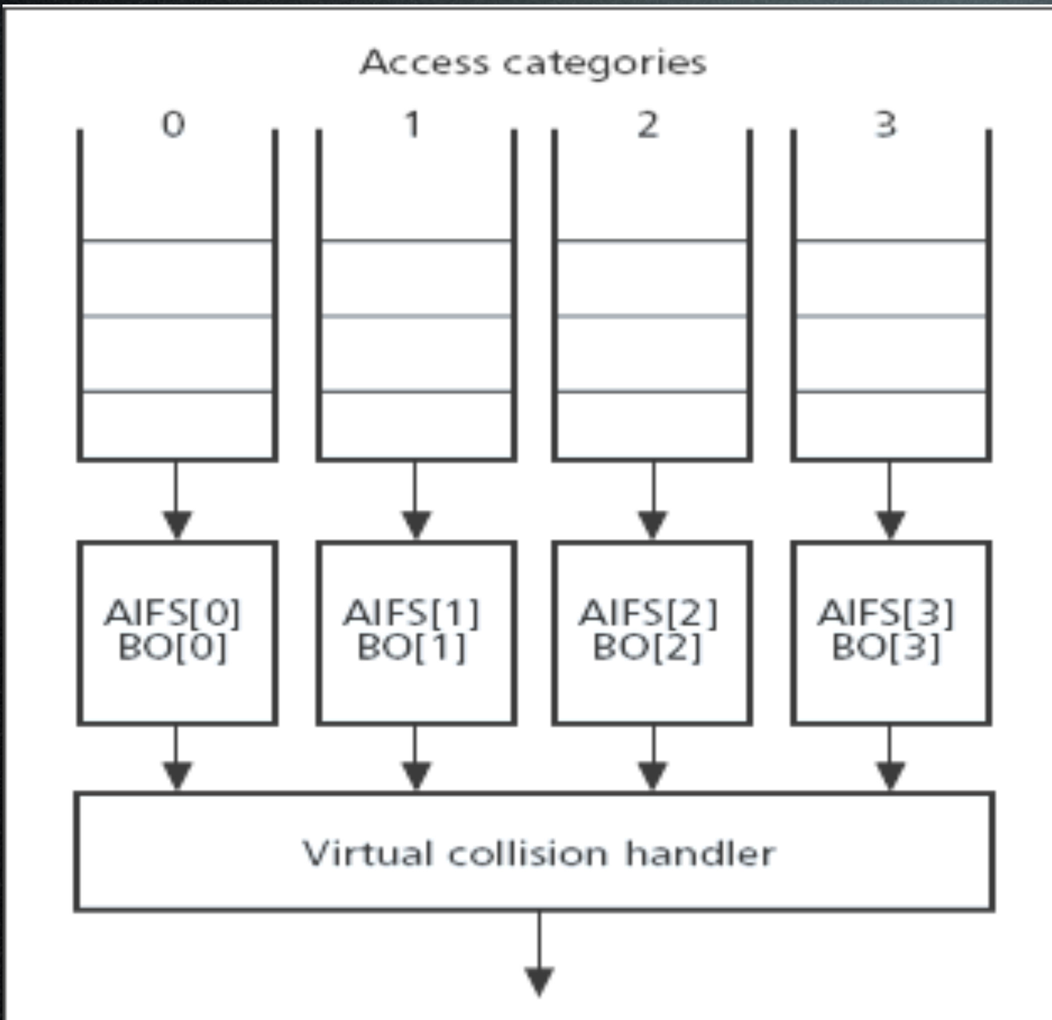
Overview of 802.11e

- Support QoS in WLAN
- Backwardly compatible with the DCF and PCF
- Hybrid Coordination Function (HCF) access method is added, including
  - Contention-Based channel access
    - Enhanced Distributed Channel Access (EDCA)
  - Controlled channel access
    - HCF Controlled Channel Access (HCCA)

Major Enhancements in 802.11e

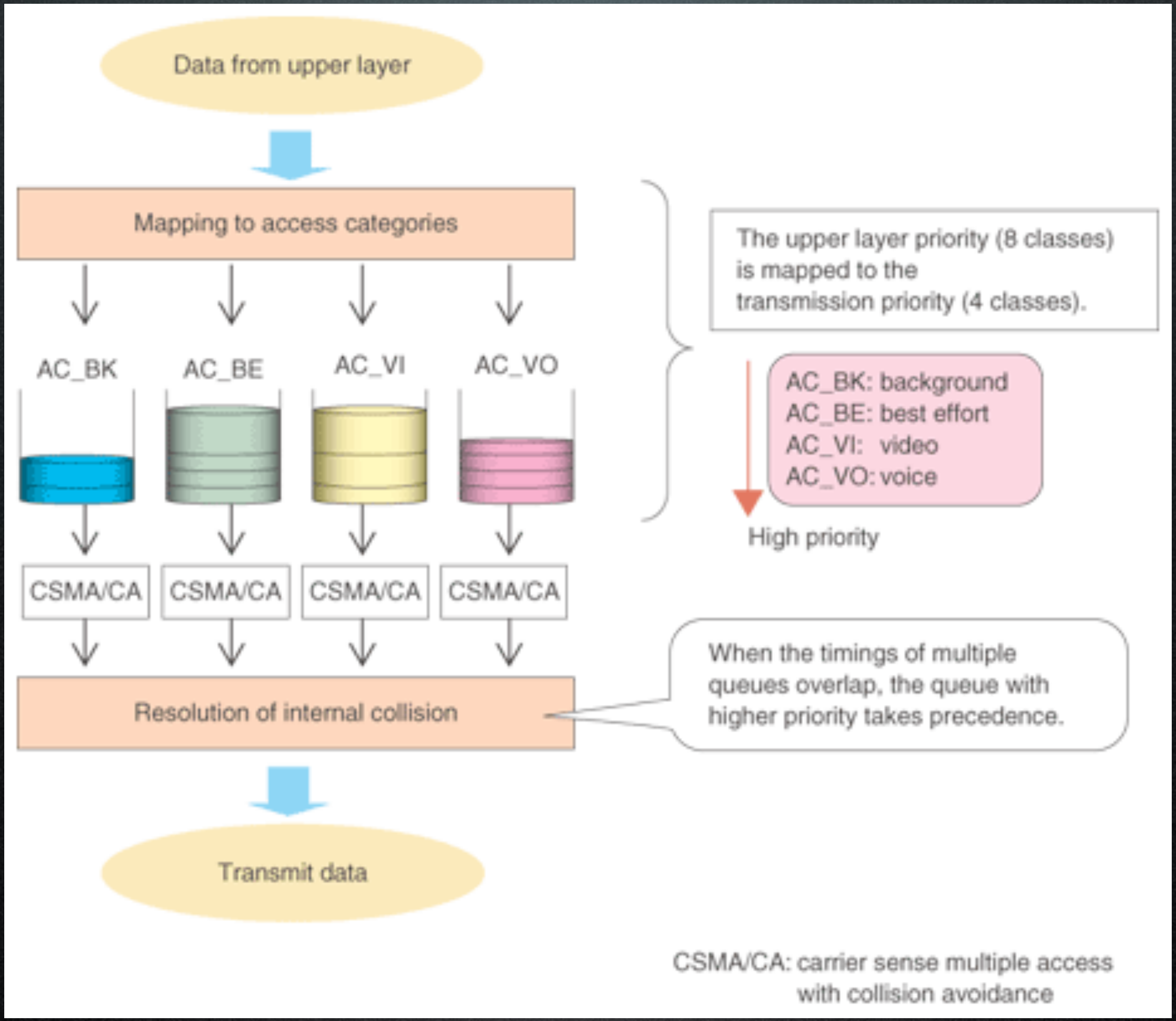
- Basic elements for QoS
    - Traffic Differentiation
    - Concept of Transmission Opportunity (TXOP)
- New Contention-based channel access
    - Enhanced Distributed Channel Access (EDCA)
- New Contention-free channel access
    - HCF Controlled Channel Access (HCCA)
- Other new mechanisms for higher throughput
    - Block Acknowledgement (Block Ack)
    - Direct Link Protocol (DLP)

Traffic Differentiation



Priority	AC	Designation
1	0	Best effort
2	0	Best effort
0	0	Best effort
3	1	Video probe
4	2	Video
5	2	Video
6	3	Voice
7	3	Voice

Traffic Differentiation



EDCA

Difference from original DCF

- Contention between ACs (Not STAs)
- New Inter-frame Space (IFS) for each AC: Arbitration Inter frame Space (AIFS)
- Transmission Opportunity (TXOP)

Access Category (AC)

- In EDCA, media access is based on the AC of MSDU
- 4 AC’s defined:
  - AC_BK (background)
  - AC_BE (best-effort)
  - AC_VI (video)
  - AC_VO (voice)
- In EDCA, the size of Contention-Window (CW) and Inter-frame space (IFS) is AC dependent

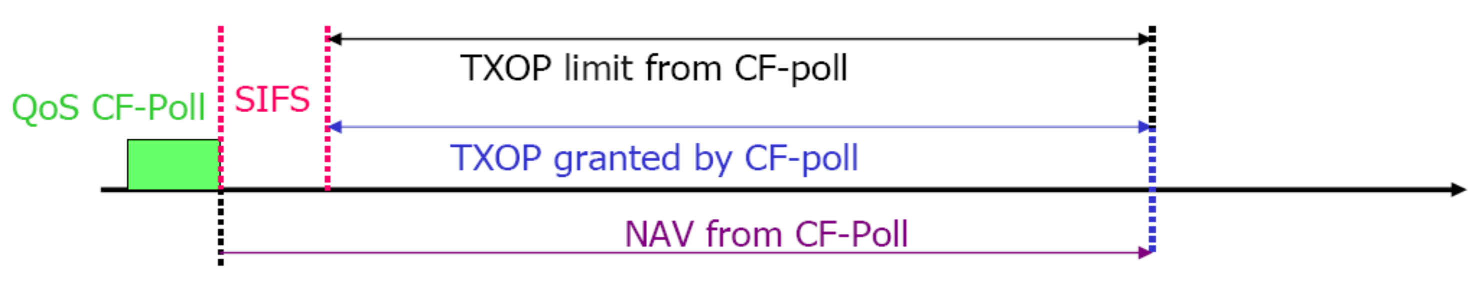
Arbitration Inter-frame Space (AIFS)

- QSTAs use AIFS to defer the contention window or transmission for each AC
- AIF[AC] = AIFSN[AC] x aSlotTime + aSIFSTime
  - AIFSN for each AC is broadcast via beacon frame containing “EDCA Parameter Set” element
- DIFS = 2 x aSlotTime+ aSIFSTime

AC	CWmin	CWmax
AC_BK	aCWmin	aCWmax
AC_BE	aCWmin	aCWmax
AC_VI	(aCWmin+1)/2-1	aCWmin
AC_VO	(aCWmin+1)/4-1	(aCWmin+1)/2-1

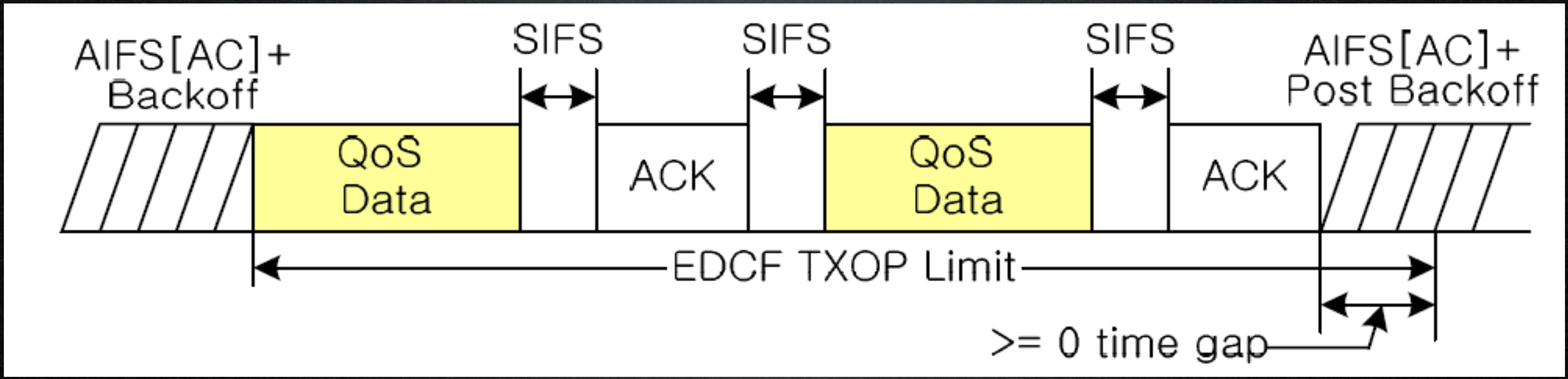
Transmission Opportunity (TXOP)

- TXOP: the duration a QSTA is enabled to transmit frame(s)
- When will a QSTA get a TXOP ?
  - Win a contention in EDCA during CP
  - Receive a CF-poll (“polled TXOP”) from HC

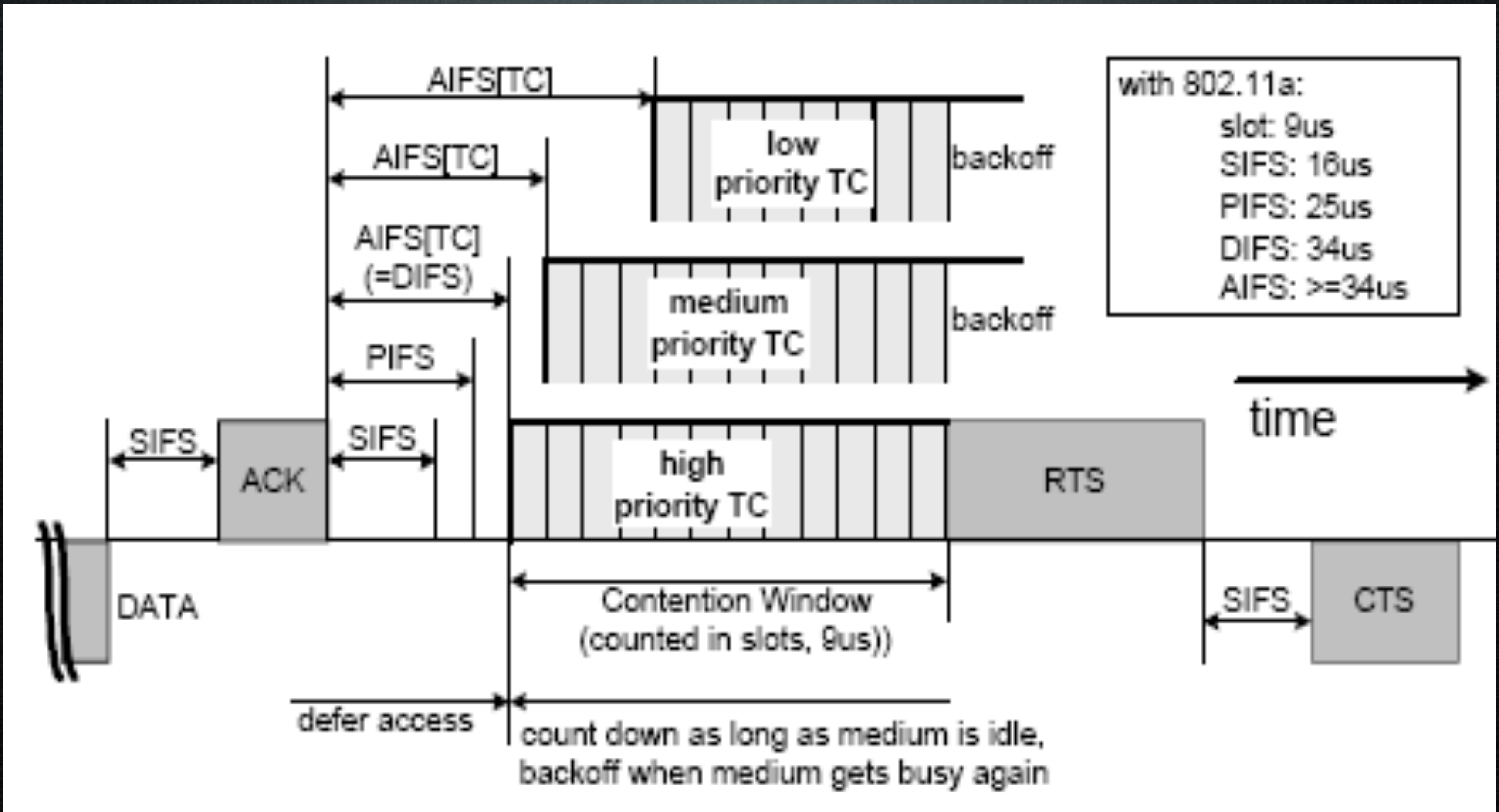


Transmission Opportunity (TXOP)

- In TXOP, frames exchange sequences are separated by SIFS



Multiple backoff of MSDU streams with different priorities



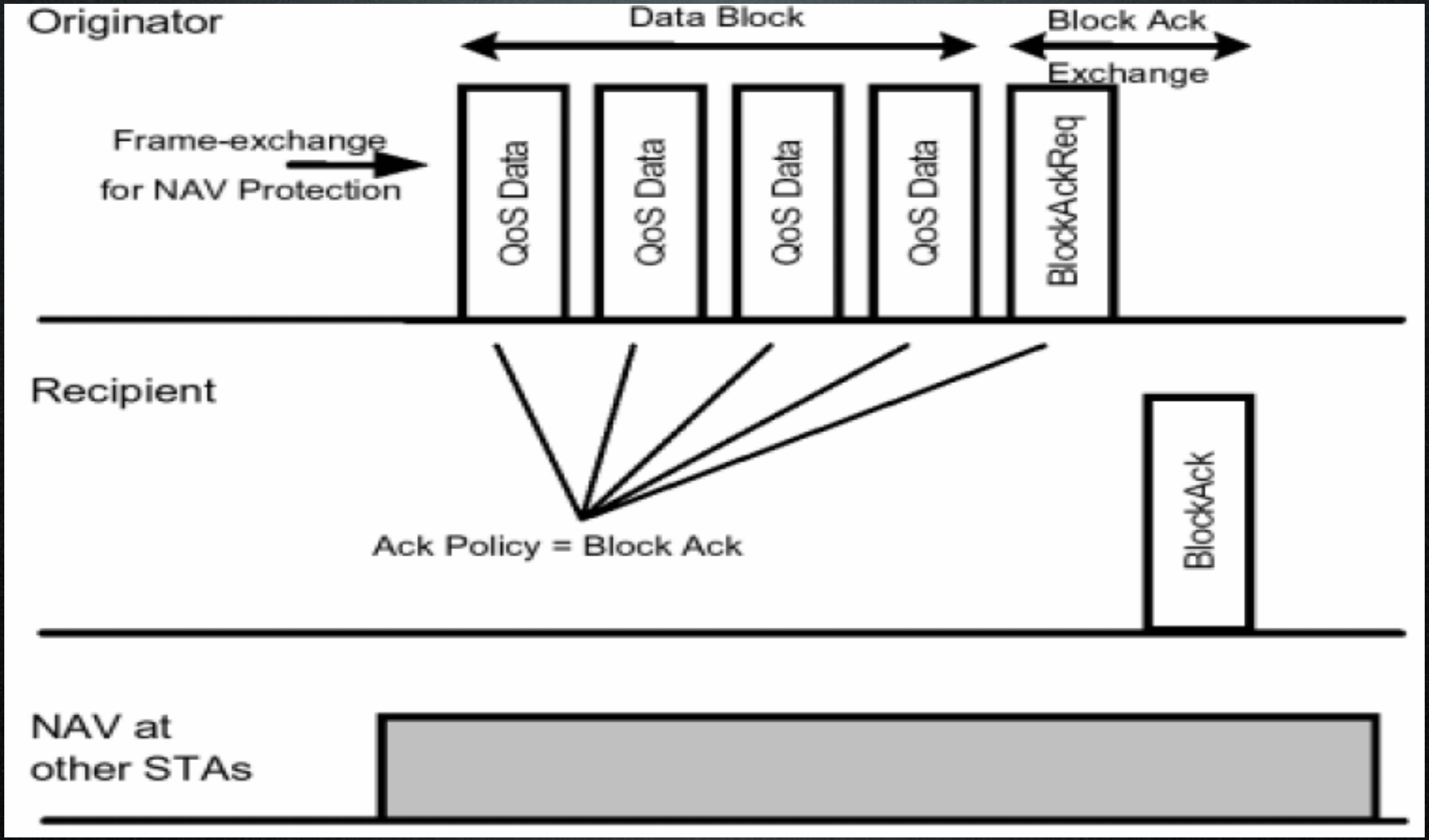
HCF Controlled Channel Access (HCCA)

- The procedure is similar to PCF
- Hybrid Coordinator (HC)
  - Operate at QAP
  - Control the iteration of CFP and CP
    - By using beacon and CF-End frame and NAV Mechanism (Same as PCF)
  - Use polling Scheme to assign TXOP to QSTA
    - Issue CF-poll frame to poll QSTA
    - Polling can be issued in both CFP & CP

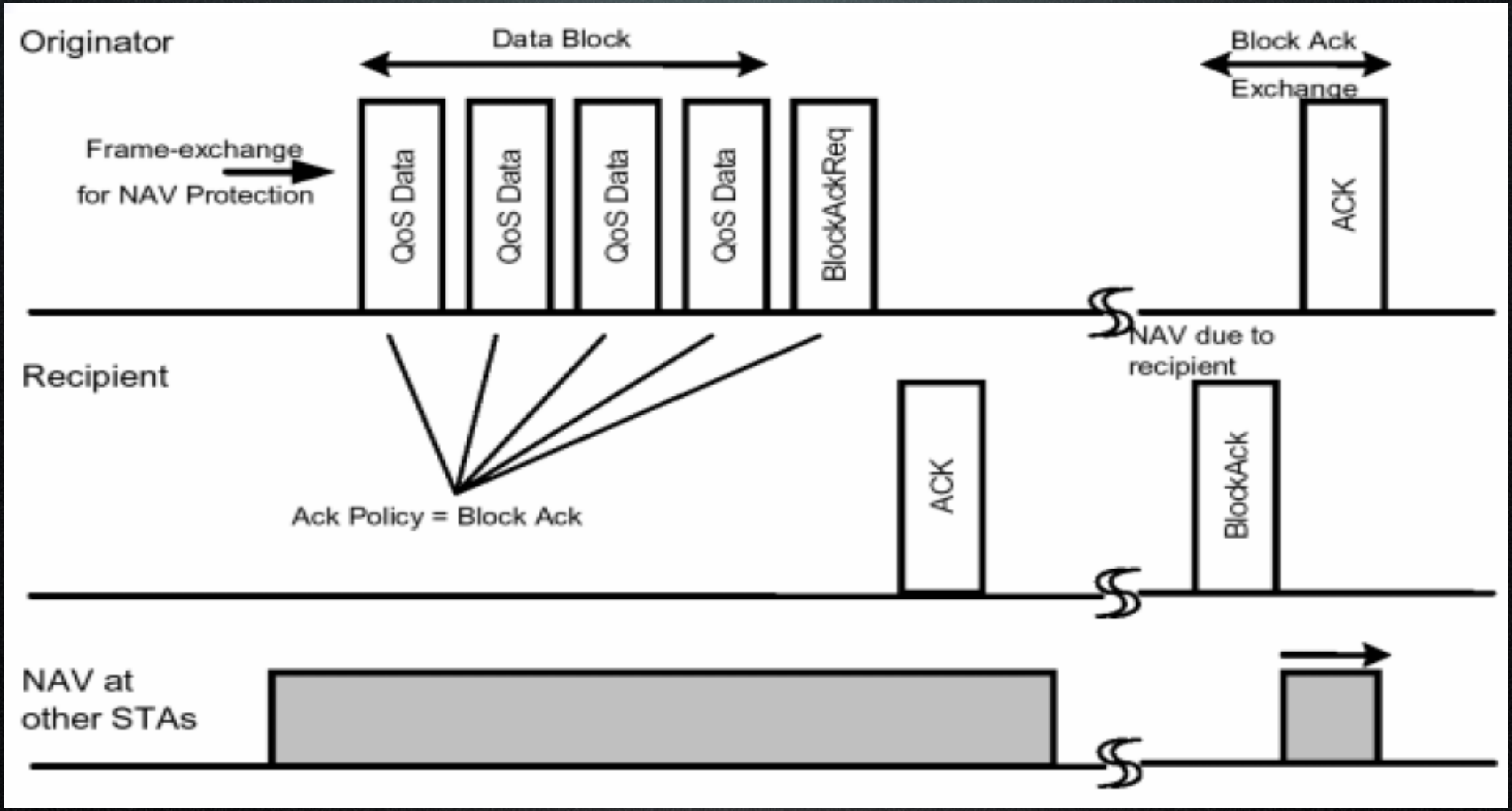
Brief of Block Ack

- Optional function
- Improve channel efficiency
  - By aggregating several acks into one frame
- Two types
  - Immediate Block Ack
    - Suitable for High-bandwidth, low latency traffic
  - Delayed Block Ack
    - Suitable for applications tolerating moderate latency

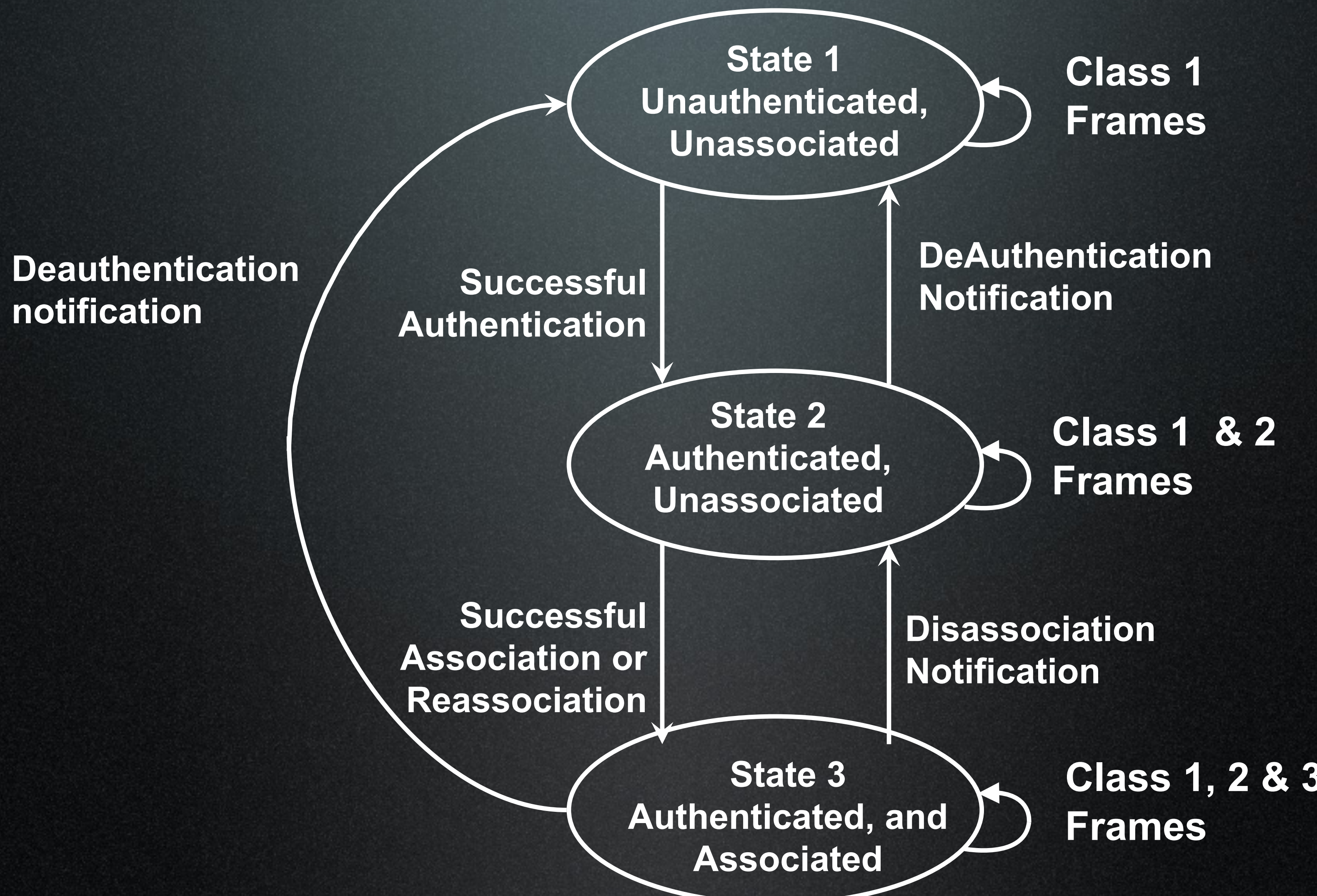
Immediate Block Ack



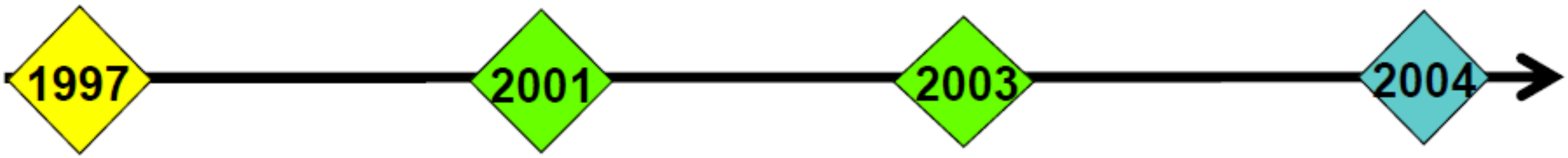
Delayed Block Ack



802.11 & security…



Chronology of Events



Original 802.11 Security:
- **Native 802.11 authentication**
- **WEP encryption**

WEP issues documented October 2000-August 2001
802.1X with WEP
- **802.1X authentication**
- **802.1X key rotation**
- **WEP data protection**

WPA = pre-standard subset of 802.11i
- **802.1X authentication**
- **802.1X key management**
- **TKIP data protection**

802.11i
- **802.1x authentication**
- **enhanced 802.1X key management**
- **AES-based data protection**
- **enhanced support infrastructure**
- **Ratified June 23**

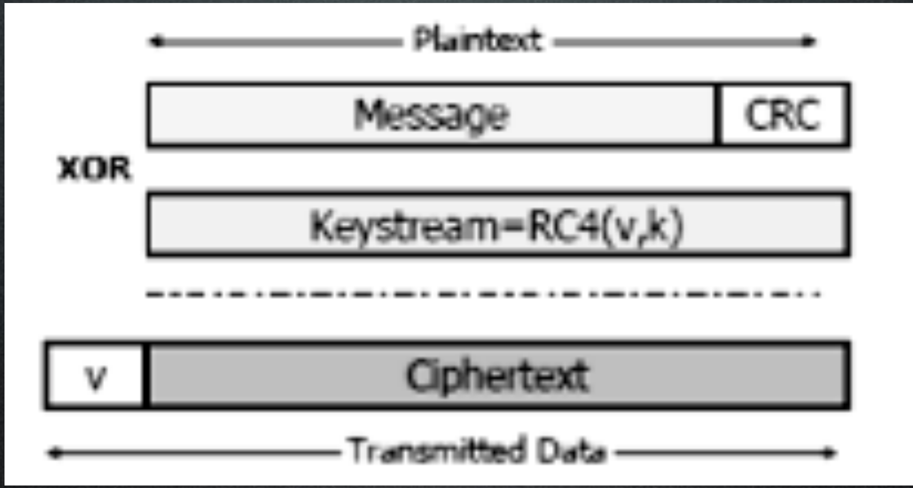
WEP?

- **WEP** relies on a secret key which is shared between the sender and the receiver.
- **SENDER**: Mobile station
- **RECEIVER**: Access Point
- **Secret Key** is used to encrypt packets before they are transmitted
- **Integrity Check** is used to ensure packets are not modified in transit.
- The standard does not discuss how shared key is established
- In practice, most installations use a **single key** which is shared between all mobile stations and access points

WEP?

- To send a **message M**:
- Compute a **checksum c(M)** (is not depend on secret key k)
- Pick an **IV v** and generate a **keystream RC4(v,k)**
- **XOR <M,c(M)>** with the keystream to get the **ciphertext**
- Transmit **v** and **ciphertext** over a radio link
- When received a message **M**
- Use **transmitted v** and the **shared key k** to generate the **Keystream RC4(v,k)**
- **XOR** the **ciphertext** with **RC4(v,k)** to get **<M’,c’>**
- Check is **c’=c(M’)**
- If it is, accept **M’** as the message transmitted

WEP?


Plaintext
Message
CRC
XOR
Keystream=RC4(v,k)
v
Ciphertext
Transmitted Data

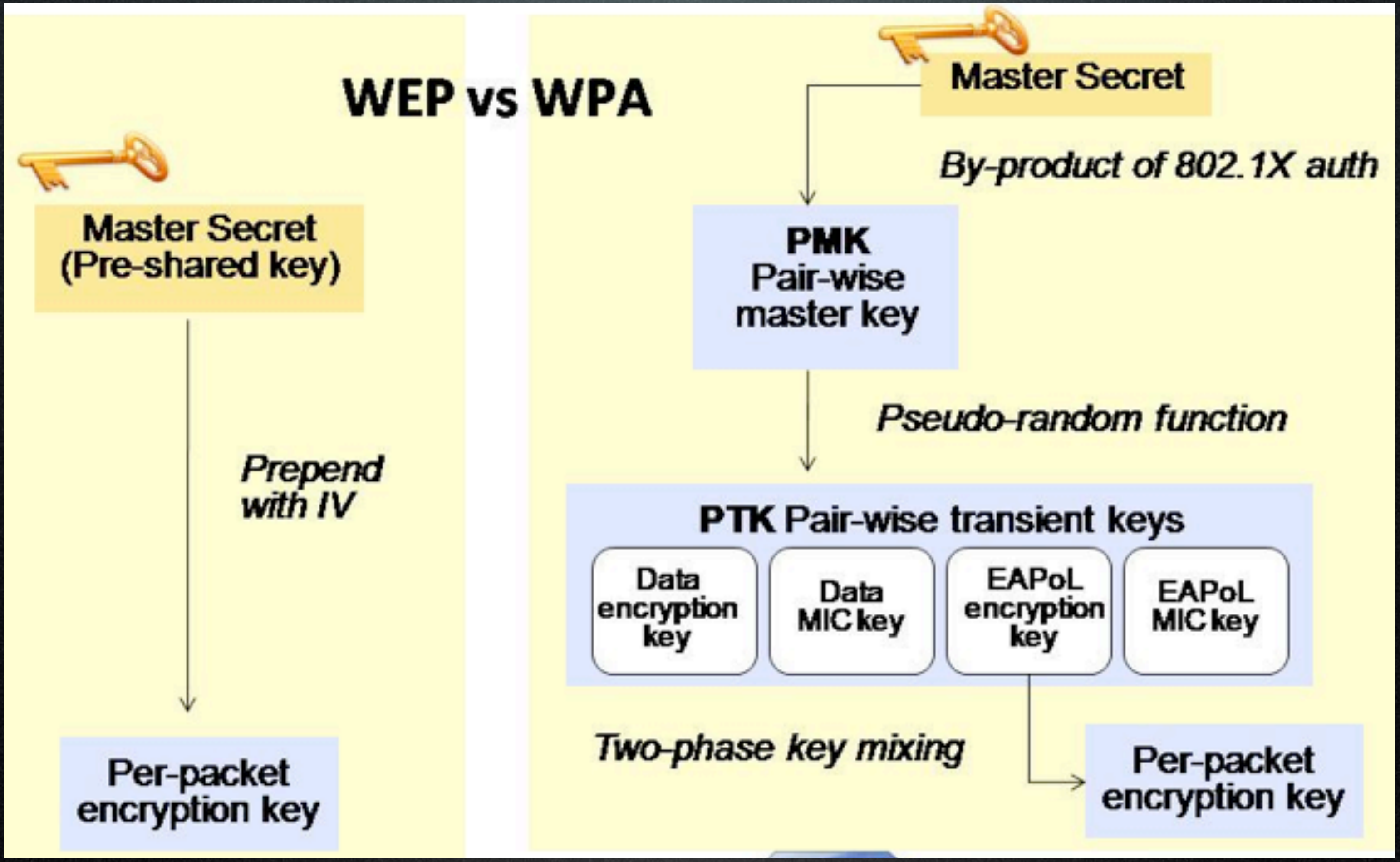
RC4

- WEP uses the RC4 encryption algorithm known as “stream cipher” to protect the confidentiality of its data.
- Stream cipher operates by expanding a short key into an infinite pseudo-random key stream.
- Sender XORs the key stream with plaintext to produce the ciphertext.
- Receiver has the copy of the same key, and uses it to generate an identical key stream.
- XORing the key stream with the ciphertext yields the original message.

Two simple flaws…

- If an attacker flips a bit in ciphertext, then after decryption, that bit in the plaintext will be flipped.
- If an eavesdropper intercepts two ciphertexts encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts.

WEP vs. WPA



WEP vs WPA
Master Secret
(Pre-shared key)
Prepend
with IV
Per-packet
encryption key
Master Secret
By-product of 802.1X auth
PMK
Pair-wise
master key
Pseudo-random function
PTK Pair-wise transient keys
Data
encryption
key
Data
MIC key
EAPoL
encryption
key
EAPoL
MIC key
Two-phase key mixing
Per-packet
encryption key