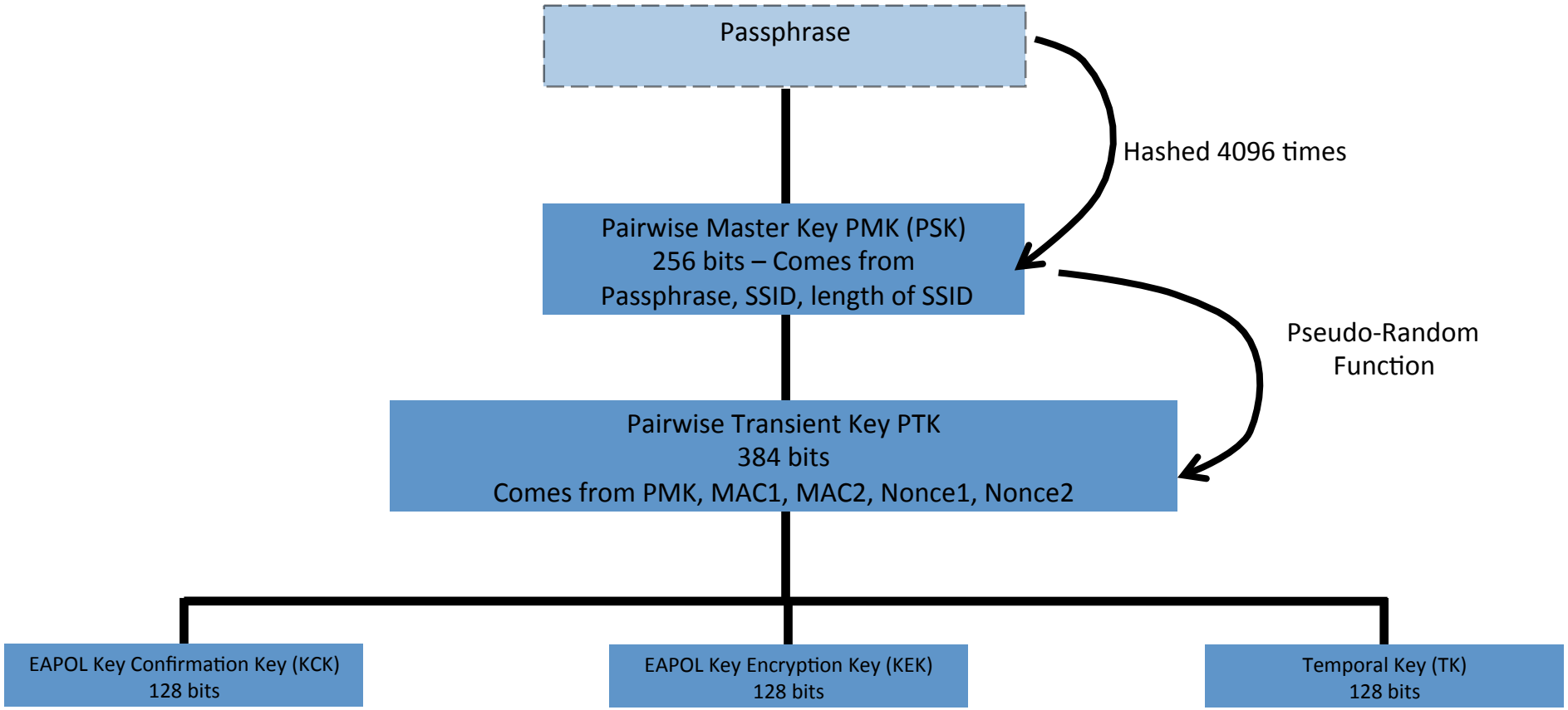
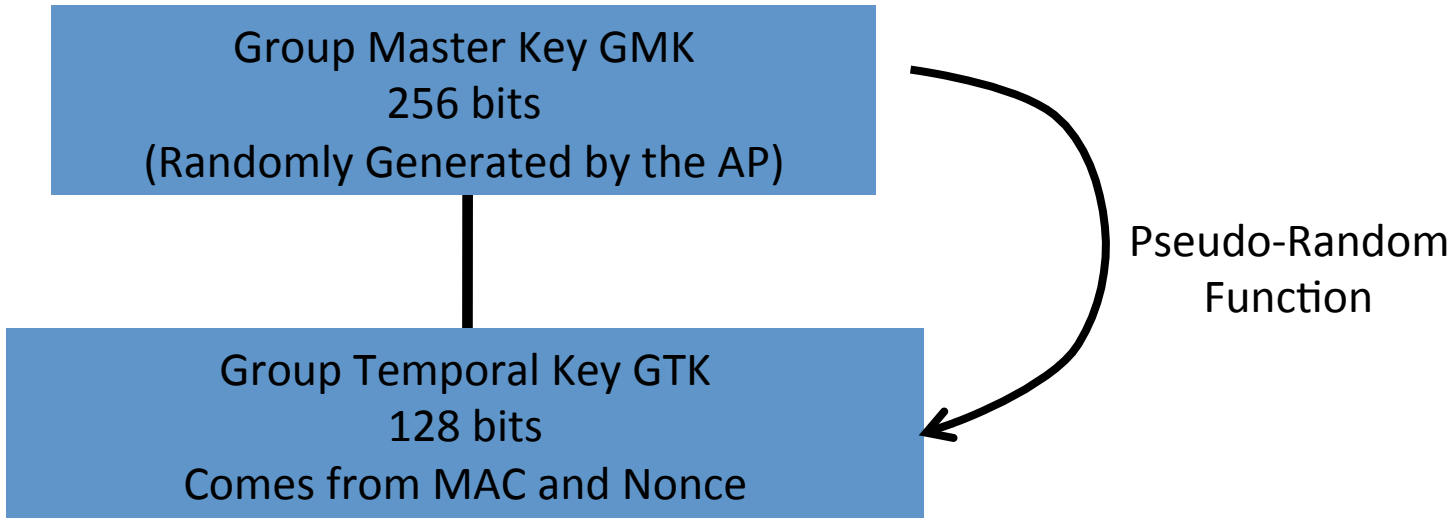
WPA2-PSK

Derivation of Hierarchical Keys



Derivation of Group Hierarchical Keys



4-way handshake

Pairwise Transient Key PTK
Comes from PMK, MAC1, MAC2, Nonce1, Nonce2

Group Master Key GMK
(Randomly Generated by the AP)

Authenticator Nonce

Supplicant Nonce authenticated by the KCK

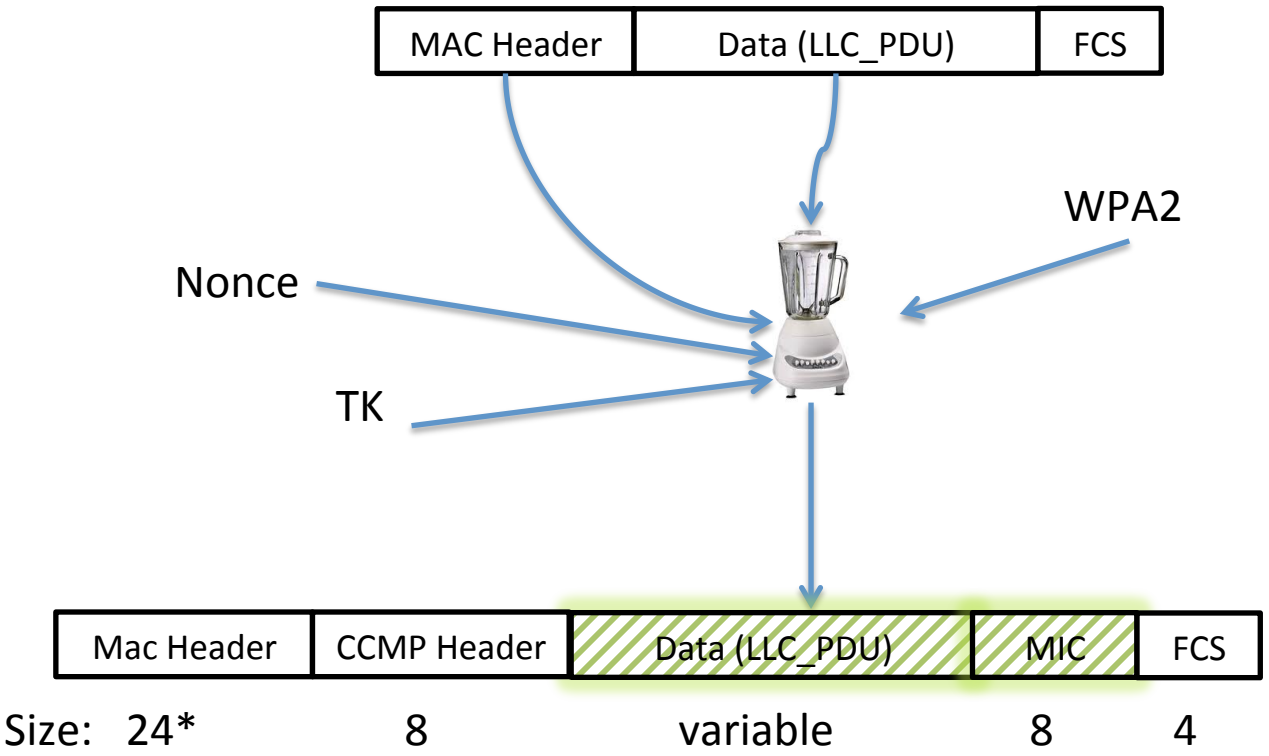
ACK contains GTK encrypted by KEK and authenticated by KCK

ACK authenticated by KCK

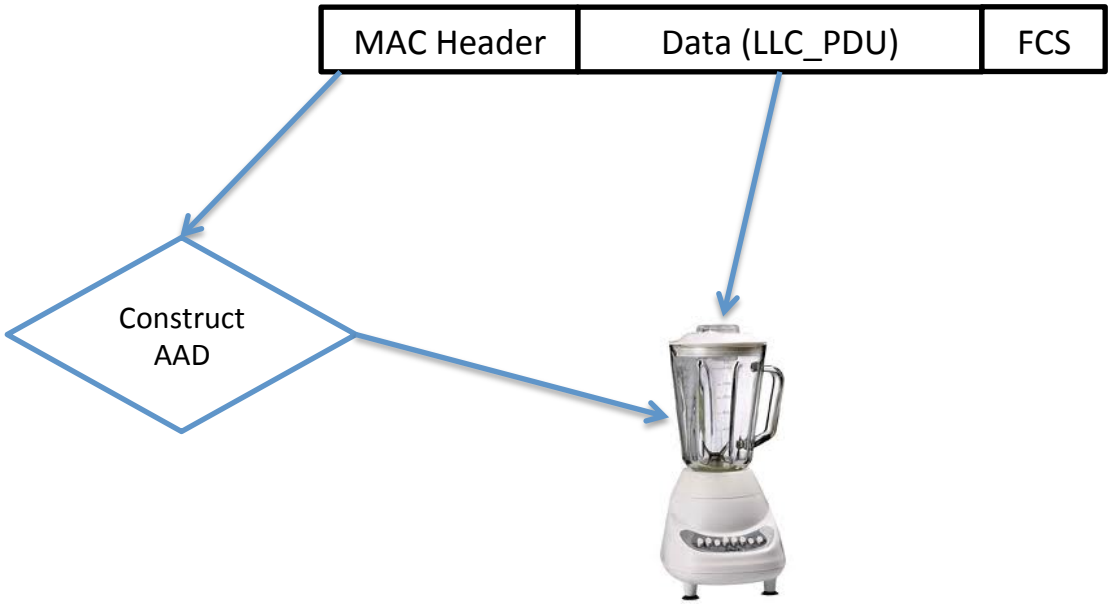
WPA2

- Security enhancements proposed by the Wi-Fi Alliance as the successor to WEP not using RC4
- Based on the CCMP (Counter Mode with CBC-MAC) Protocol
- Uses CTR (Counter mode) for confidentiality
- Uses CBC-MAC (Cipher Block Chaining Message Authentication Code) for integrity and authentication
- Uses the AES (Advanced Encryption Standard) algorithm

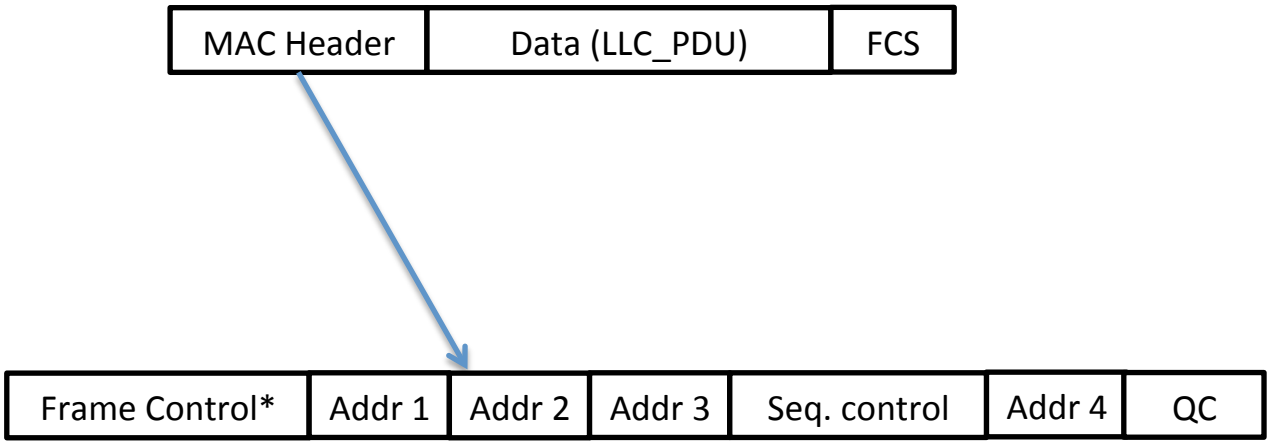
General View



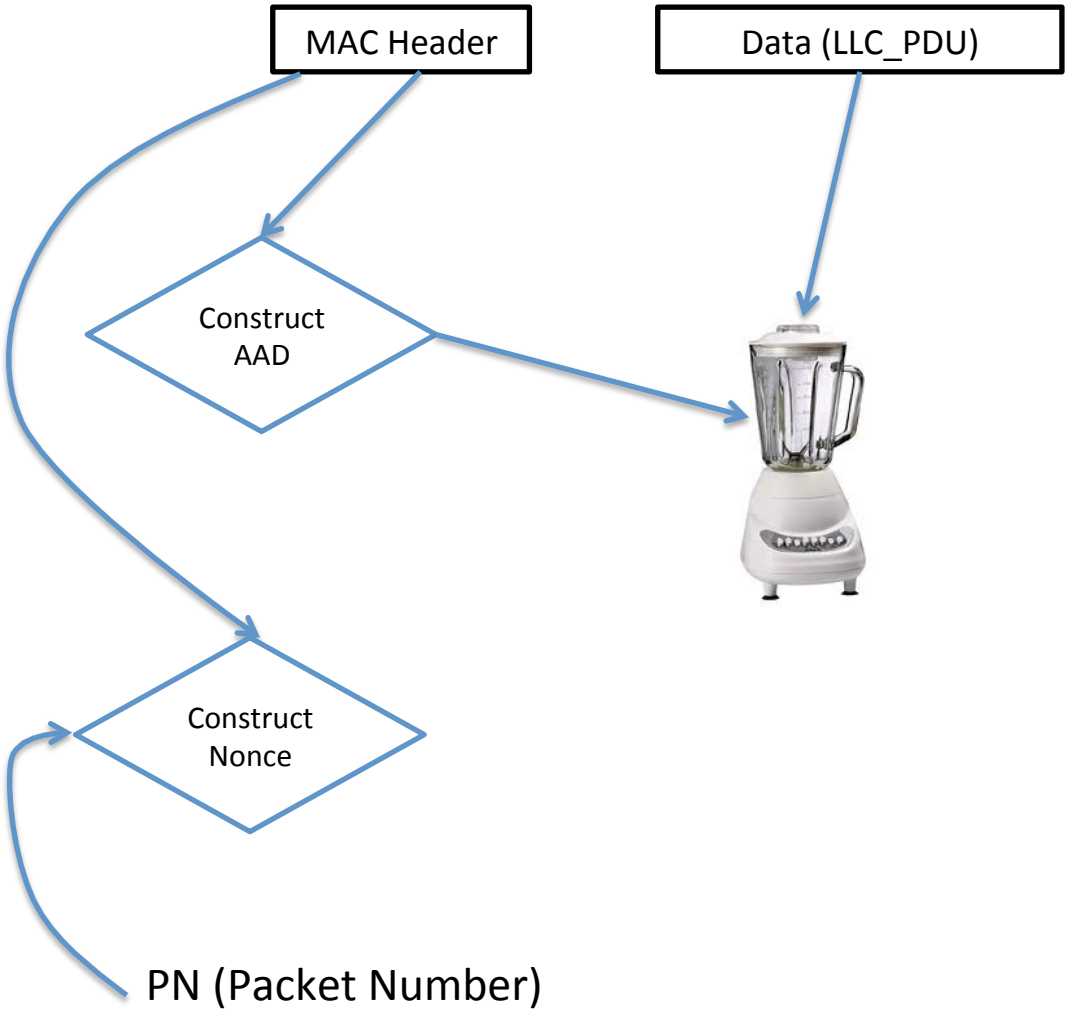
*depends on the type of frame


MAC Header
Data (LLC_PDU)
FCS
Construct
AAD

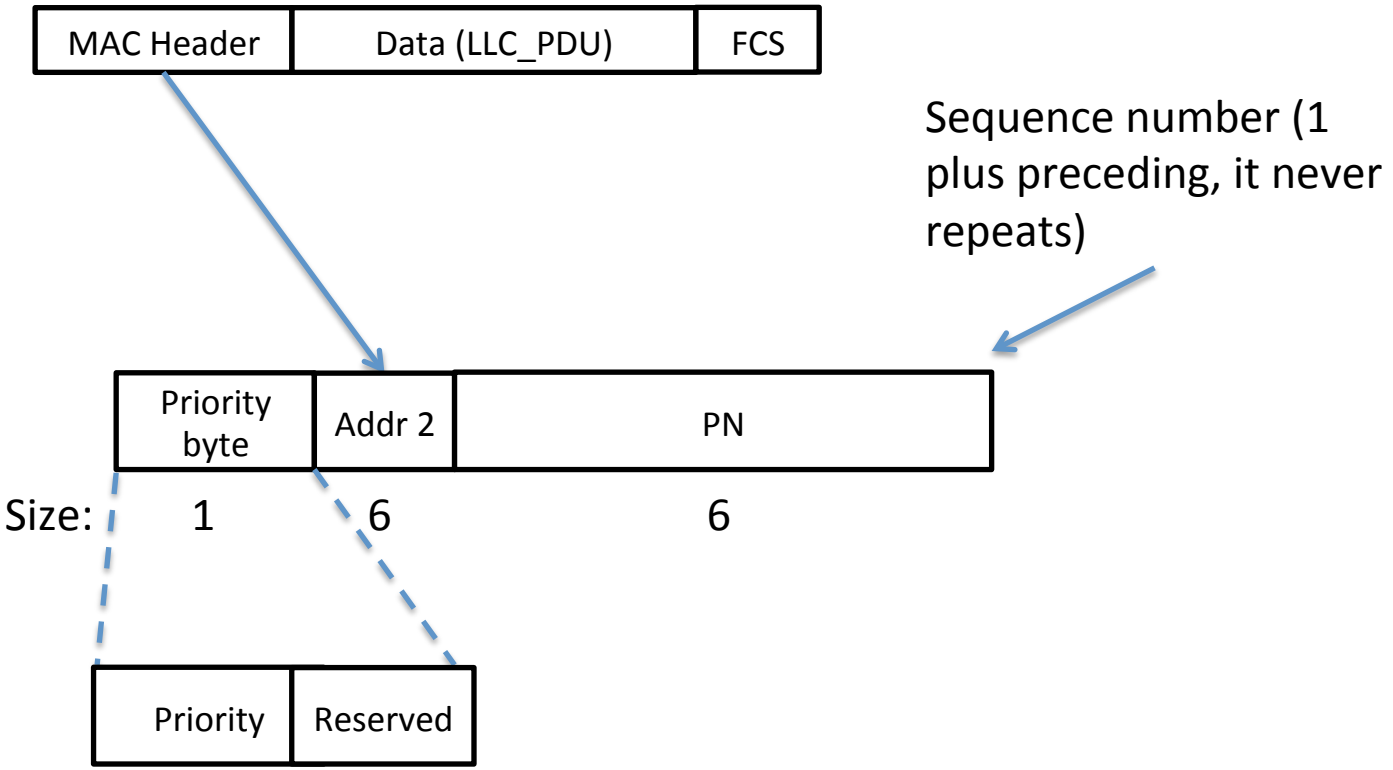
AAD (Additional Authentication Data) based on the MAC Header



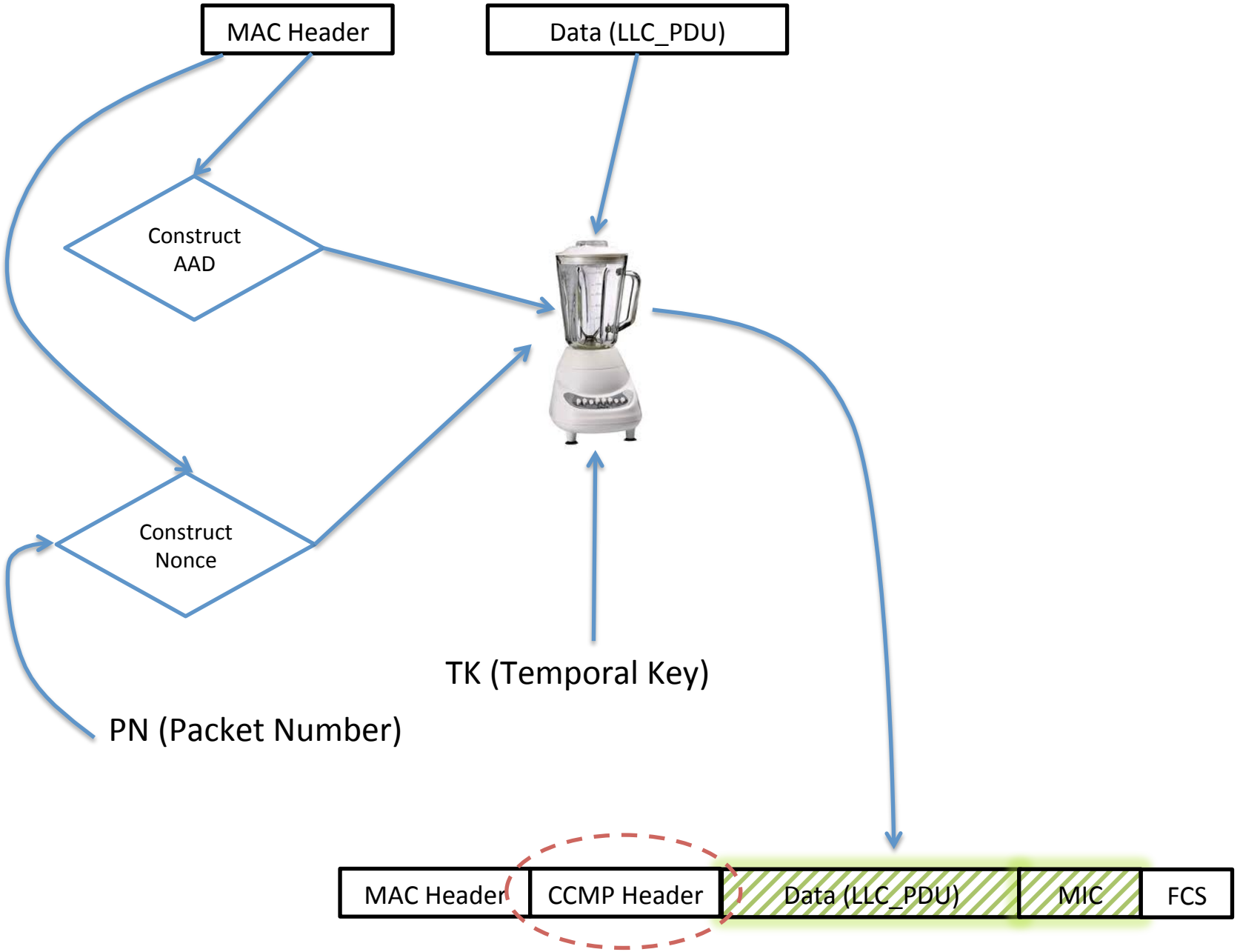
*The fields that would change in case of a retransmission are se to 0

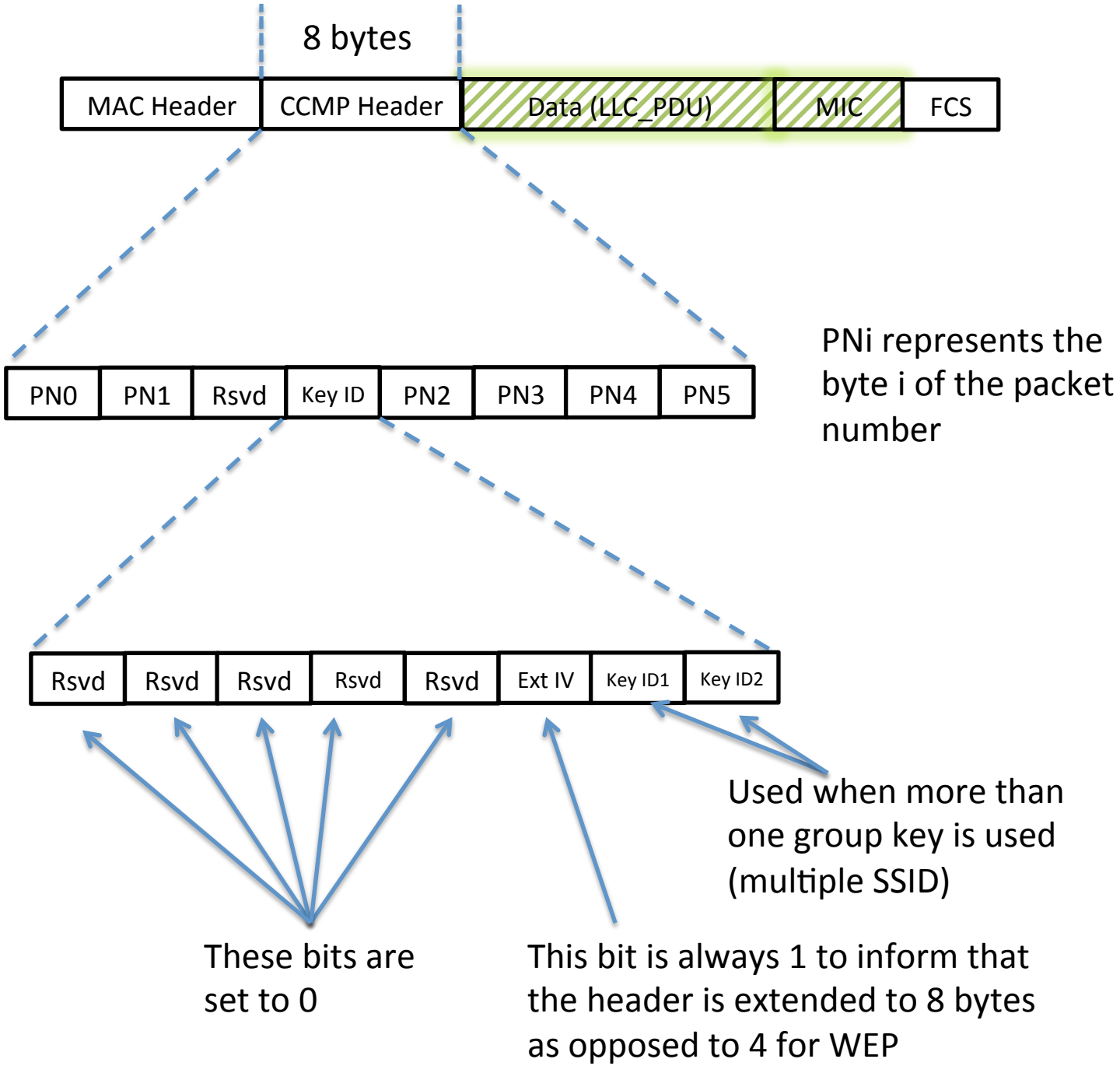

MAC Header
Data (LLC_PDU)
Construct AAD
Construct Nonce
PN (Packet Number)

Nonce : based on the source address and the packet number



- Addr 2 is the source address
- If there's no QoS, the priority byte is set to 0

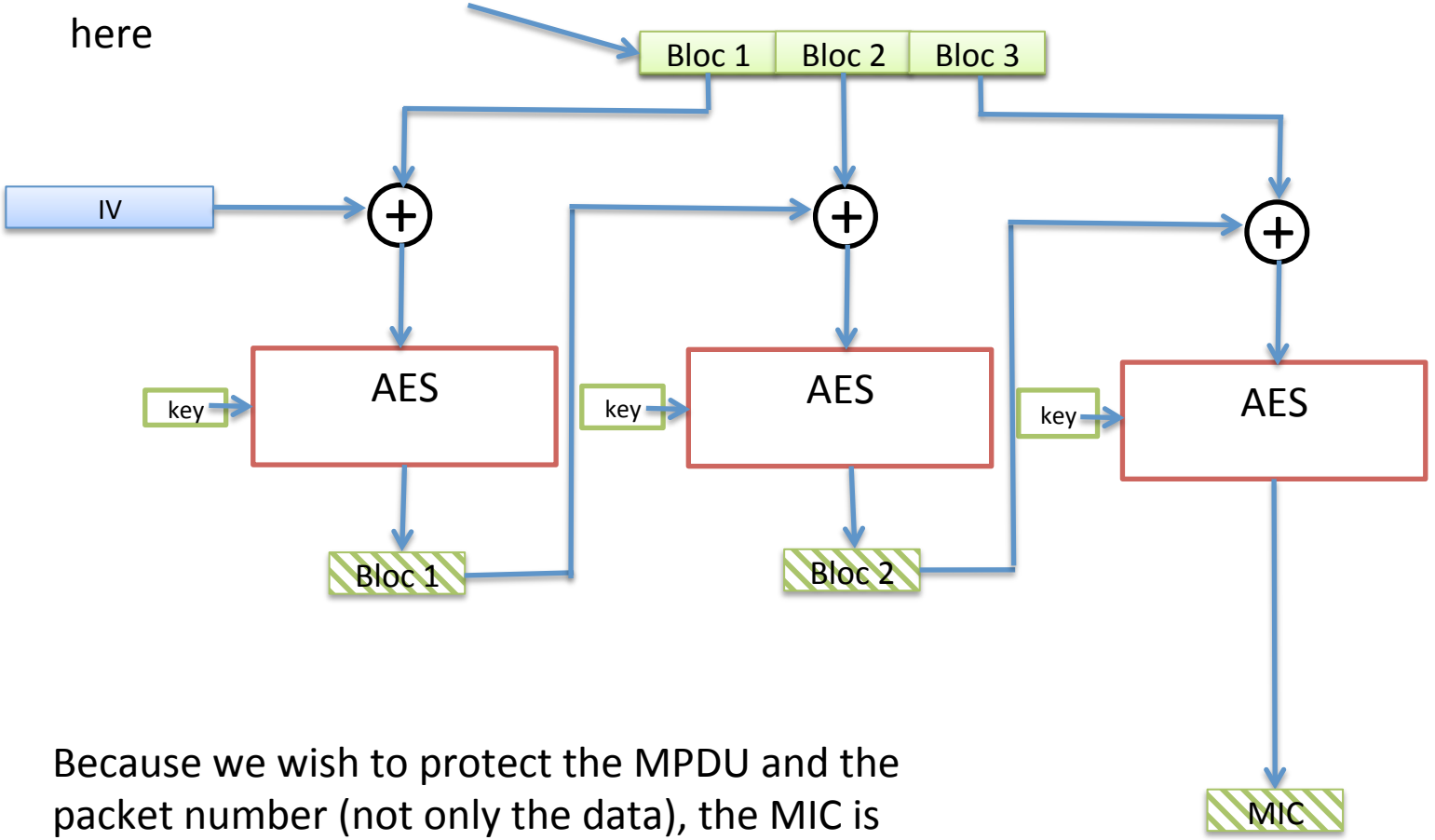

MAC Header
Data (LLC_PDU)
Construct AAD
Construct Nonce
TK (Temporal Key)
PN (Packet Number)
MAC Header
CCMP Header
Data (LLC_PDU)
MIC
FCS


8 bytes
MAC Header
CCMP Header
Data (LLC_PDU)
MIC
FCS
PN0
PN1
Rsvd
Key ID
PN2
PN3
PN4
PN5
PNi represents the byte i of the packet number
Rsvd
Rsvd
Rsvd
Rsvd
Rsvd
Ext IV
Key ID1
Key ID2
Used when more than one group key is used (multiple SSID)
These bits are set to 0
This bit is always 1 to inform that the header is extended to 8 bytes as opposed to 4 for WEP

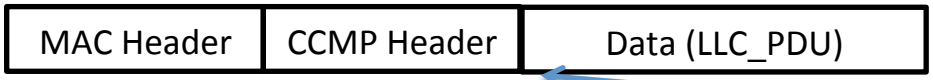
Based on CCMP (Counter Mode with CBC-MAC) Protocol

Cipher Block Chaining (CBC-MAC)

AAD and Nonce are here



Because we wish to protect the MPDU and the packet number (not only the data), the MIC is calculated over:



AAD and Nonce are here

Basé sur CCMP (Counter Mode with CBC-MAC) Protocol

Counter Mode Encryption