Zerlegung des Dumps

Die Pakete sind in der Reihenfolge der Bits zumindest beim Mac Frame Format falsch herum. Wird alles Big Endian gemacht aber Small Endian dargestellt. Weiß auch nicht wieso die das machen.

4000 0000 FFFFFFFFFFFF 00F4B96A32ED FFFFFFFFFFFF 60AF 000A574C
414E37333630534C010402040B1632080C1218243048606C2D1A000119FF0000000000000000000000000000000000000000000003010ADD090010180200000400000DD1E00904C33000119FF00000000000000000010082006837FF3FD0070000B14B 15500C61

Frame Control: 4000 (in Bits: 00000100 00000000 00000000 00000000)

- Protocol Version (B0 B1: 00) -> Standard sollte immer 00 bei aktuellen Protokollen
- Type (B2 B3: 00) -> Management
- SubType (B4 - B7: 0100) -> nicht ganz klar wie rum das gelesen wird weil in der Tabell die Values umgedreht sind. Könnte entweder ein Reassociation Request oder ein Probe Request sein
- To DS und FROM DS sind null, siehe Tabelle

Address fields (siehe Management frame Format, Seite 418 des IEEE811) :

- Address 1, Destinantion Address: (FFFFFFFFFFFF)

- Address 2, Transmitting Address (also wer das gesendet hat): (00F4B96A32ED)
  Adresse vom iPhone

- Address 3, ist das BSSID, bzw hier eher ein Wildcard um zu sehen wer da ist…
  - 1) In management frames of subtype Probe Request, the Address 3 field is the BSSID. The BSSID is either a specific BSSID as described in item 4) below or the wildcard BSSID as defined in the procedures specified in 10.1.4.
  - 2) In management frames of subtype Action, Category Public, the Address 3 field is the BSSID. The BSSID value is set according to 10.19.
  - 3) If dot11OCBActivated is true, the Address 3 field is the wildcard BSSID.
  - 4) Otherwise:
    - i) If the STA is contained within an AP or is associated with an AP, the Address 3 field is the BSSID. The BSSID is the address currently in use by the STA contained in the AP.
    - ii) If the STA is contained within an AP or is transmitting the management frame to an AP, the Address 3 field is the BSSID. The BSSID is the address currently in use by the STA contained in the AP.
    - iii) If the STA is transmitting the management frame to one or more members of an IBSS, the Address 3 field is the BSSID of the IBSS. iv) If the STA is a mesh STA, the Address 3 field is the TA.

8000 0000 FFFFFFFFFFFF 001D1962967B 001D1962967B 901C 82C3E5F31500 0000 64003104
000C4172636F722D3632393633330108828 48B960C121824030109050400010000 2A010030140100000FAC040100000FAC040100000FAC020100320430486 06CDD180050F2020101030003A4010082006837FF3FD0070000A5A5 A5A5A5A5

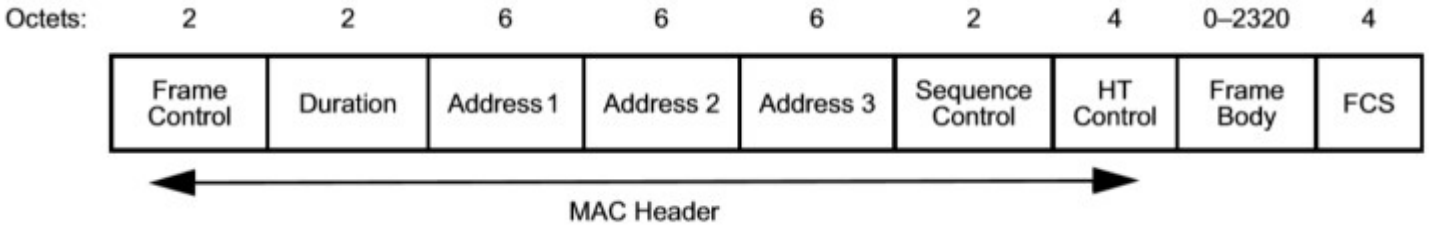
Frame Control: 8000

- Protocol Version wieder 00 wie verlangt
- Type ist 00, also Management
- Type ist Association Response oder Beacon

Address fields:

- Destination ist wieder Broadcast, die anderen Beiden sind wahrscheinlich die Station…

Wenn man das Paket analysieren würde, könnten wir herausfinden was diese Station so alles kann und so aber die Frage



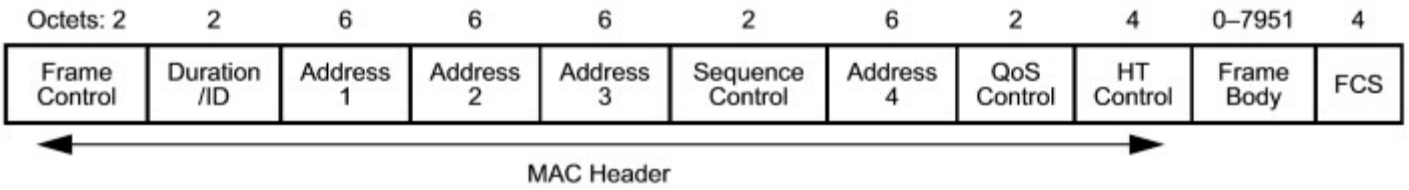


Figure 8-1—MAC frame format

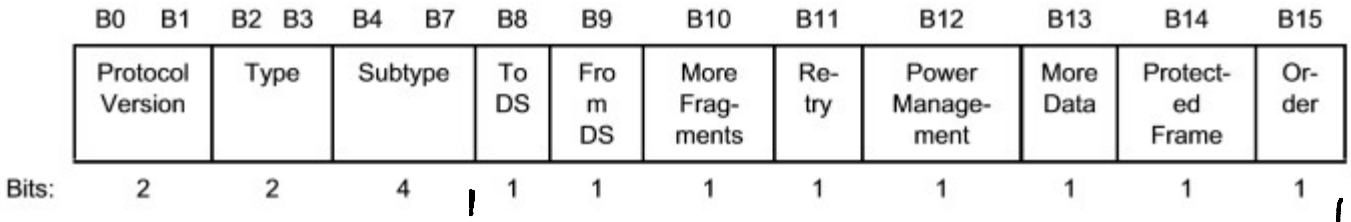


Figure 8-2—Frame Control field

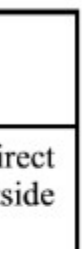
Table 8-1—Valid type and subtype combinations

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110	Timing Advertisement

Table 8-2—To/From DS combinations in data frames

To DS and From DS values	Meaning
To DS = 0 From DS = 0	A data frame direct from one STA to another STA within the same IBSS, a data frame di from one non-AP STA to another non-AP STA within the same BSS, or a data frame out the context of a BSS, as well as all management and control frames.

ue	Type description	Subtype value b7 b6 b5 b4	Subtype description
	Management	0111	Reserved
	Management	1000	Beacon
	Management	1001	ATIM
	Management	1010	Disassociation
	Management	1011	Authentication
	Management	1100	Deauthentication
	Management	1101	Action
	Management	1110	Action No Ack
	Management	1111	Reserved
	Control	0000–0110	Reserved
	Control	0111	Control Wrapper
	Control	1000	Block Ack Request (BlockAckReq)
	Control	1001	Block Ack (BlockAck)
	Control	1010	PS-Poll
	Control	1011	RTS
	Control	1100	CTS
	Control	1101	ACK
	Control	1110	CF-End
	Control	1111	CF-End + CF-Ack
	Data	0000	Data
	Data	0001	Data + CF-Ack
	Data	0010	Data + CF-Poll
	Data	0011	Data + CF-Ack + CF-Poll
	Data	0100	Null (no data)
	Data	0101	CF-Ack (no data)
	Data	0110	CF-Poll (no data)
	Data	0111	CF-Ack + CF-Poll (no data)
	Data	1000	QoS Data
	Data	1001	QoS Data + CF-Ack
	Data	1010	QoS Data + CF-Poll
	Data	1011	QoS Data + CF-Ack + CF-Poll
	Data	1100	QoS Null (no data)
	Data	1101	Reserved
	Data	1110	QoS CF-Poll (no data)
	Data	1111	QoS CF-Ack + CF-Poll (no data)
	Reserved	0000–1111	Reserved



- Destination ist wieder Broadcast, die anderen Beiden sind wahrscheinlich die Station…

Wenn man das Paket analysieren würde, könnten wir herausfinden was diese Station so alles kann und so aber die Frage ist ob das wirklich notwendig ist…

Summary:
Ich glaube wenn wir den Typ ordentlich auslesen können, dann ist es zumindest bei den Management Frames sicher, die zweite Adresse als Destination zu nehmen. Wenn wir dann noch die Beacons ignorieren würden wir auch weniger Daten haben aber wüssten dann natürlich nicht was für Stationen wir haben. Wäre zum Beispiel interessant auf welchen Kanaälen die Funken und diese Kanäle dann stärker überwachen oder so…

To DS = 0 From DS = 0	A data frame direct from one STA to another STA within the same IBSS, a data frame di from one non-AP STA to another non-AP STA within the same BSS, or a data frame out the context of a BSS, as well as all management and control frames.
To DS = 1 From DS = 0	A data frame destined for the DS or being sent by a STA associated with an AP to the Port Access Entity in that AP.
To DS = 0 From DS = 1	A data frame exiting the DS or being sent by the Port Access Entity in an AP, or a group addressed Mesh Data frame with Mesh Control field present using the three-address MAC header format.
To DS = 1 From DS = 1	A data frame using the four-address MAC header format. This standard defines procedures using this combination of field values only in a mesh BSS.

irect side
t
C
for