802.11 Frame Body Contents

David Bagby
Bob O'Hara
Dave Roberts
AMD
One AMD Place
Sunnyvale, CA 94088-3453

Rick White
Mark Demange
Motorola
50 East Commerce Dr.

Jon Rosdahl
Novell
122 East 1700 south
m/s C-22-1
Provo, UT 84606-6194

802.11 frame information contents

• Specifies information required for each frame
  – field name
  – data type
    » fixed length
    » variable length
  – length of info if fixed length

• Does not specify how the information items are encoded with in the frame.
  – separate proposals will cover encoding issues.
Frame types

- Data
- Control
- Management

Frame Subtypes

- Data
  - Asynchronous Data
  - CF Up
  - CF Down
- Control
  - RTS
  - CTS
  - ACK
  - CF-ACK

Presentation
Frame Subtypes

- Management
  - POLL
  - Beacon
  - ATIM
  - Probe
  - Association
  - Reassociation
  - Disassociation
  - Authentication
  - Privacy

Frame information contents.
Data contents

- Asynchronous Data
  - MSDU
- CF Up
  - MSDU
- CF Down
  - MSDU

RTS contents

- Null
  - header contains all needed information
CTS contents

- Null
  - header contains all needed information

ACK contents

- Null
  - header contains all needed information
CF-ACK contents

- Null
  - header contains all needed information

POLL contents

- PSP and POLL are both used as names for the same frame in B2; editors please clean up.
- SID
Beacon contents

- Time stamp
  - B2 4.3.1
    » fixed length, 4 octets
- Weight
  - B2 4.3.9
    » fixed length, 2 octets
- Beacon interval
  - B2 4.3.2
    » fixed length, 1 octet
- DTIM period
  - B2 4.3.5
    » fixed length, 1 octet
- continued...

Beacon contents

- DTIM count
  - B2 4.3.4
    » fixed length, one octet
- Channel sync info
  - Referenced in B2, but not fully defined.
    » Hop sequence, where in sequence etc.
    » variable length structure
- ESS ID
  - string
    » variable length
    » max size of 128 octets
- continued...
Beacon contents

- TIM
  - B2 4.3.3
    » variable length
- Broadcast indicator
  - B2 4.3.6
    » fixed length, Boolean

ATIM contents

- Null
  - header contains all needed information
Probe contents

• Request / Response indicator
  – Fixed length, Boolean
• Request:
  – null

Probe contents

• Response:
  » Same as beacon w/o TIM and Broadcast indicator
  – Time stamp
    » B2 4.3.1
      • fixed length, 4 octets
  – Weight
    » B2 4.3.9
      • fixed length, 2 octets
  – Beacon interval
    » B2 4.3.2
      • fixed length, 1 octet
  – DTIM period
    » B2 4.3.5
      • fixed length, 1 octet
  – continued...
Probe contents (response)

- DTIM count
  » B2 4.3.4
   • fixed length, one octet
- Channel sync info
  » Referenced in B2, but not fully defined.
   • Hop sequence, where in sequence etc.
  » Variable length structure
- ESS ID
  » string
   • variable length
   • max size of 128 octets

Association contents

- Request / Response indicator
  - Fixed length, Boolean
- Request:
  - Privacy Algorithm number
    » fixed length, 2 octets
    • length determined by 802.10
    • value = current privacy algorithm in use
### Association contents

- **Response:**
  - Status value
    - Boolean values:
      - Successful
      - Not successful
  - Not Successful, followed by
    - Error indication
      - fixed length, one octet
      - specific error codes TBD
  - Successful, followed by
    - SID
      - B2 4.3.7
      - fixed length, 2 octets
      - item not included in msg in B2, required after Association as the SID is the index into a TIM

### Reassociation contents

- **Request / Response indicator**
  - Fixed length, Boolean

- **Request:**
  - Current AP address
    - fixed length, 6 octets
  - Privacy Algorithm number
    - fixed length, 2 octets
      - Length determined by 802.10
      - value = current privacy algorithm in use
Reassociation contents

- **Response:**
  - Status value
    - Boolean values:
      - Successful
      - Not successful
  - Not Successful, followed by
    - Error indication
      - fixed length, one octet
      - specific error codes TBD
  - Successful, followed by
    - SID
      - B2 4.3.7
        - fixed length, 2 octets
      - item not included in msg in B2, required after Association as the SID is the index into a TIM

Disassociation contents

- null
  - all needed information in header
  - msg from STA to AP
    - “I’m disassociating”
    - SA = STA disassociating
    - DA = old AP
  - msg from AP to STA
    - “you’re being disassociated”
    - SA = old AP
    - DA = STA being disassociated
Privacy contents

• Transaction sequence number
  - Fixed length, 1 octet
  - values: 1, 2

Privacy contents

• Transaction sequence = 1:
  - Supported algorithm list
    » variable length structure
    » structure fields
    • Number of alg supported
      - fixed length, one octet
    • Privacy Algorithm number
      - fixed length, 2 octets
      - one field for each alg supported
Privacy contents

- Transaction sequence = 2:
  - Status value
    » Boolean
    » values:
      • Successful
      • Not successful
  - Not Successful, followed by
    » Error indication
      • fixed length, one octet
      • specific error codes TBD
  - Successful, followed by
    » Privacy Algorithm number
      • fixed length, 2 octets
      • Privacy algorithm selected

Authentication contents

- Transaction sequence number
  - Fixed length, 1 octet
  - values: 1, 2, 3, 4, 5, 6
- Transaction is started by S1, to S2
  - general for STA to STA
  - For infrastructure S1 = STA, S2 = AP
- Challenge response information notation
  - 3 structures
    » authentication alg dependent contents
    » variable length
    » contained in authentication transaction msgs
Authentication notation

- Challenge (by, of)
  » by challenging STA, of STA being challenged.
  » variable Length structure
    • Len fixed, 2 octets
    • rest = alg dependent challenge contents
- Challenge_Response (by, to)
  » by STA that was challenged, to STA issued challenged
  » variable length structure
    • Len fixed, 2 octets
    • rest = alg dependent response contents
- Challenge_Result (from, to)
  » from STA challenging STA, to responding STA
  » variable length structure
    • Len fixed, 2 octets
    • rest = alg dependent result contents

Authentication contents

- Transaction sequence = 1:
  - Supported algorithm list
    » variable length structure
    » structure fields
      • Number of algs supported
        - fixed length, one octet
      • Authentication Algorithm number
        - fixed length, 2 octets
        - one field for each alg supported
Authentication contents

- Transaction sequence = 2:
  - Status value
    » Boolean
    » values:
      • Successful
      • Not successful
  - Not Successful, followed by
    » Error indication
      • fixed length, one octet
      • specific error codes TBD

- (Transaction 2 continued)
- Successful, followed by
  » Identity assertion by S2
    • not in frame body
    • contained implicitly in msg header
      - SA = S2
  » Authentication Algorithm number
    • fixed length, 2 octets
    • Authentication algorithm selected
    • determines how contents of subsequent frames parsed for rest of this authentication transaction sequence.
Authentication contents

• Transaction sequence = 3:
  - Challenge (by S1, of S2)
  - Identify assertion by S1
    » implicitly in msg header
    • SA = S1

• Transaction sequence = 4:
  - Challenge_Response (from S2, to S1)
  - Challenge (by S2, of S1)

• Transaction sequence = 5:
  - Challenge_Result (from S1, to S2)
  - Challenge_Response (from S1, to S2)

• Transaction sequence = 6:
  - Challenge_Result (from S2, to S1)
Motion:

- That the information contents of frames as described in 94/214a be adopted and that the draft be updated to reflect this.