# 802.11 Draft Standard Document P802.11-93/20B3 Comments

Frédéric J. Bauchot

CER IBM La Gaude
06610 La Gaude, France

Jim Panian

IBM Research Triangle Park
200 Silicon Drive, NC 27709 USA

## INTRODUCTION

This contribution gives a collection of comments on the draft standard document P802.11-93 20B3.

The comments have been classified in four different categories: **M** as major technical, **m** as minor technical, **Q** as question and **e** as editorial. The list is not intended to be complete. The editorial comments have been put at the end of the list.

Among the other comments (either technical or question), the top 5 ones in term of importance are the comments 1, 2, 7, 10 and 24 which respectively address mobility, compression, authentication, privacy and DTBS access method. Basically the four first ones state that any lack of standardization of the corresponding schemes will translate into interoperability problems among 802.11 compliant products. To ensure the success of 802.11, the standard must specify a minimal set of operational schemes allowing compliant products to interoperate with and without security support (authentication and privacy), with and without compression support, and with and without mobility support. The comment 24 recalls that we see Time Bounded Services as a major piece of the 802.11 standard and that the current level of definition is by far incomplete.

## COMMENTS LIST

- Comment 1.

  **Clause:** 1.1, page 1, line 16
  **Severity:** M
  **Comment:** It is said that 802.11 describes mobility. In the rest of the document it is by far not described. For instance the following aspects are missing:
  - pre-authentication scheme,
  - hand-off logic,
  - hand-off notification to upper layers,
  - hand-off impact on asynchronous & time bounded services,
  - hand-off impact on encryption key synchronization,
  - etc...

  **Recommended Change:** This required function needs to be architected and sufficiently described in the standard.

- Comment 2.

  **Clause:** Whole document
  **Severity:** q
  **Comment:** Why doesn't the draft specify a common compression scheme? Any non-standard compression implementation on top of 802.11 will raise interoperability problems.
  **Recommended Change:** Standardize on a common compression scheme, or set of schemes. It does not preclude the use of not standardized compression schemes, but it allows any 802.11 compliant products to find a common scheme that can ensure interoperability with compression enabled. Let assume that the 802.11 standard standardizes a compression scheme "A". Assume now that a first station X supports the schemes A, B and C and that a second station Y supports the schemes A and D. These stations will be able to use the common scheme A although they support other (proprietary) schemes. Another aspect that should be addressed by the standard is the protocol used by the stations to determine the set of commonly supported compression schemes.

- Comment 3.

  **Clause:** 2.2.2.1, pages 11, 13
  **Severity:** m
  **Comment:** Are associations needed between peer stations for the ad-hoc case? Section 2.2.1.1 implies this "To become a member of a BSS a station must become "Associated".
  **Recommended Change:** An association should only be required between a mobile station and an access point.

- Comment 4.

  **Clause:** 2.3, page 16, lines 12-18
  **Severity:** m
  **Comment:** Currently, the state machine diagrams show a "Mac Data Service" and a "Mac Management Service", and none of the services listed in 2.3.
  **Recommended Change:** The 802.11 architectural services need to be tied to the state machine diagrams.

- Comment 5.

  **Clause:** 2.3, page 16, line 18
  **Severity:** m
  **Comment:** Compression is not listed as an 802.11 architectural service.
  **Recommended Change:** Add compression to the list of 802.11 architectural services.

- Comment 6.

  **Clause:** 2.4, page 19, line 11
  **Severity:** q
  **Comment:** What path do control and contention free messages take (MAC data path or MAC management service path)?
  **Recommended Change:** Add text describing how control and contention free messages flow through the state machines.

- Comment 7.

  **Clause:** 2.4.3.1, page 22, lines 46-57
  **Severity:** q
  **Comment:** How can interoperability be ensured if no common authentication scheme is defined ?

**Recommended Change:** A standardized authentication scheme, or set of schemes, should be specified. It does not preclude the use of not standardized authentication schemes, but it allows any 802.11 compliant products to find a common scheme that can ensure interoperability. Let assume that the 802.11 standard standardizes an authentication scheme "A". Assume now that a first station X supports the schemes A, B and C and that a second station Y supports the schemes A and D. These stations will be able to use the common scheme A although they support other (proprietary) schemes. Another aspect that should be addressed by the standard is the protocol used by the stations to determine the set of commonly supported authentication schemes.

- Comment 8.

**Clause:** 2.4.2.3, page 21, line 9
**Severity:** m
**Comment:** How is a hand-off handled with Reassociation? When a mobile roams, does it perform the following order of events?
  - find a new AP
  - pre-Authenticate with new AP (optional)
  - privacy exchange with new AP
  - disassociate with old AP
  - reassociate providing MAC address of old AP + all information negotiated with old AP

**Recommended Change:** Specify the details behind the reassociation procedure.

- Comment 9.

**Clause:** 2.4.3.2, page 21, line 14 and 3.1.1.3, page 34, line 41-42.
**Severity:** m
**Comment:** There is no description of privacy flows for the ad-hoc case.
**Recommended Change:** Privacy needs to be described for the ad-hoc case where associations are not performed.

- Comment 10.

**Clause:** 2.4.3.2, page 23, lines 32-34
**Severity:** q
**Comment:** Why isn't a standard privacy algorithm specified? The lack of a standard specified privacy algorithm prevents seamless mobility. Clause 3.1.1.3, page 34 states that "All implementations of 802.11 shall provide for encipherment of data using the default algorithm(s). A default of "in the clear" is in conflict with clause 3.1.1.3.
**Recommended Change:** A common privacy algorithm, or set of algorithms, should be specified.

- Comment 11.

**Clause:** 2.5, page 24, figure 2-8
**Severity:** m
**Comment:** The figure does not take into consideration the ad-hoc case where associations are not performed.
**Recommended Change:** Enhance the figure to cover the ad-hoc case.

- Comment 12.

**Clause:** 2.4.3.2, page 23, line 24
**Severity:** q
**Comment:** To our knowledge, 802.10 SDE does not specify a privacy scheme; it only specifies how a privacy scheme can be agreed upon by a couple of stations.

**Recommended Change:** Investigate, and provide clarifying text.

- Comment 13.

  **Clause:** 2.7.1, page 27
  **Severity:** m
  **Comment:** There is no message type for time-bounded data.
  **Recommended Change:** Add a message type, and the necessary parameters for time bounded.

- Comment 14.

  **Clause:** 3.1.1.3, page 34, line 30
  **Severity:** q
  **Comment:** How is access control accomplished in conjunction with layer management?
  **Recommended Change:** Add explanatory text describing this function.

- Comment 15.

  **Clause:** 3.1.4, page 35, lines 18-20
  **Severity:** q
  **Comment:** "During the association exchange, parties A and B exchange attribute values of the security managed objects defined in IEEE 802.10 SDE. These values specify the security parameters (e.g. algortithm, key, etc,) that will be needed for the association." Is this text out of date?
  **Recommended Change:** Align this text with the Clause 2.4 , Overview of the Services (Association, Access and Confidentiality Control Services).

- Comment 16.

  **Clause:** 4.1.1, page 50, figure 4-1
  **Severity:** m
  **Comment:** The maximum frame body length of 2304 is not a "standard" mac frame size (see 802.3 or 802.5). Moreover this size could be increased to allow better compression ratio if compression is used. As fragmentation is used, larger maximum frame body length will not translate into an increase of transmission retries.
  **Recommended Change:** Change to a larger frame size. We believe that a size of 4 KBytes is a good figure.

- Comment 17.

  **Clause:** 4.2, page 50, figures 4-1 and 4-2
  **Severity:** m
  **Comment:** 2 bits for protocol version does not seem sufficient.
  **Recommended Change:** Add more bits for protocol version. The introduction of such bits will certainly ask for a new byte in the control field, but this control field needs also to be extended for other reasons (see next comment).

- Comment 18.

  **Clause:** 4.1.2.1, page 50, figure 4-2
  **Severity:** m
  **Comment:** There is no flag specifying if the frame is compressed and/or encrypted. Such bits would ease protocol implementation, either in software or in hardware.
  **Recommended Change:** Add bits to the frame format to flag a compressed/encrypted frame body.

- Comment 19.

  **Clause:** 4.1.2.5, page 53

**Severity:** m
**Comment:** The 16-bit Duration field must be tied to time units to make it a useful field.
**Recommended Change:** Specify the time base for bits in the Duration field. Also, specify a value that means "ignore the Duration field" for frames such as Probe-request. An interesting proposal has been documented by P.Brenner on the reflector; it could be used as a starting point.

- Comment 20.

**Clause:** 4.2.1.4, page 56
**Severity:** m
**Comment:** What purpose does the stationID (SID) field serve in the Poll frame?
**Recommended Change:** Describe the use of the field, or remove it from the Poll frame.

- Comment 21.

**Clause:** 4.2.3, page 57
**Severity:** m
**Comment:** It does not seem like one common management frame format applies to all of the management frame types. Why does a beacon and ATIM need the Duration field? Why does the Probe request need the Sequence Number, Fragment Number, and Duration fields? What value should go into the BSS-ID field for a Probe request? Clause 7.1.3.2 indicates that a Probe request should contain the ESS-ID and not a BSS-ID specifically.
**Recommended Change:** Place fields into the frame formats that carry necessary information. Otherwise specify null values for fields that appear in frames where their appearance is to only reduce the number of unique frame formats.

- Comment 22.

**Clause:** 4.2.3.1, page 57
**Severity:** m
**Comment:** The Beacon needs to contain the BSS-ID. BSS-ID is required for a station to initiate an Association request to an access point. Also, Beacons need to indicate whether the network is ad-hoc or infrastructure. Otherwise, the station will not know whether to associate with an access point or not.
**Recommended Change:** Add BSS-ID and a field that indicates ad-hoc or infrastructure network to the Beacon.

- Comment 23.

**Clause:** 4.3, page 59
**Severity:** m
**Comment:** The "DATA-DATA (fragmented broadcast MSDU)" is missing.
**Recommended Change:** Add this item to the list.

- Comment 24.

**Clause:** 5.2.13.3 , page 82, line 11
**Severity:** M
**Comment:** The DTBS channel access mechanism is missing.
**Recommended Change:** This required function needs to be architected and sufficiently described in the standard.

- Comment 25.

**Clause:** 5.2.6.6, page 77, line 23
**Severity:** m

**Comment:** The draft states that "the source station will transmit all fragments of the MSDU without releasing the channel as long as there is enough time left in the dwell time". Does this mean that there is no SIFS between fragments?

**Recommended Change:** Specify that each fragment is transmitted after waiting SIFS.

- Comment 26.

**Clause:** 5.2.11, page 79, lines 24, 36, 41
**Severity:** m
**Comment:** The standard does not specify when the timers T1 & T3 are started.
**Recommended Change:** Specify with T1 and T3 are started relative to the start/end of RTS, CTS.

- Comment 27.

**Clause:** 5.2.6.6, page 77, lines 37-38
**Severity:** m
**Comment:** The text is ambiguous regarding the applicability of the duration field for fragments and ACKs.
**Recommended Change:** Change the sentence that starts on line 37 to read "Each fragment and ACK acts as a virtual RTS and CTS for the next fragment to come."

- Comment 28.

**Clause:** 5.2.6.6, page 78, figure 5-xx: RTS/CTS with Transmitter Priority w/ missed ACK
**Severity:** m
**Comment:** The figure is incorrect in showing the NAV being set by ACK 1 when ACK 1 is never sent.
**Recommended Change:** Remove the NAV (ACK 1) from "Other" from the figure.

- Comment 29.

**Clause:** 5.2.7, page 67, line 11
**Severity:** m
**Comment:** The text states that for data after an RTS/CTS exchange "The asynchronous payload frame (e.g. DATA) shall be transmitted after the end of the CTS frame and an SIFS gap period. No regard shall be given to the busy or free status of the medium." If the clear channel assessment determines that the medium is occupied already (possibly by a station in an overlapping BSS), why then should the DATA frame go out? If the medium is busy, it is unlikely that the DATA frame will be successfully transmitted anyway.

Relying on the NAV information only would work fine if all the wireless stations within range would follow the "802.11 discipline", but if CCA reflects a busy medium, it clearly indicates that this condition is not true and thus that the transmission will almost certainly fail.

**Recommended Change:** Strike the sentence that reads "No regard shall be given to the busy or free status of the medium."

- Comment 30.

**Clause:** 5.2.10, page 79, line 20
**Severity:** m
**Comment:** The text states that for an ACK "The transmission of the ACK frame shall commence after a SIFS period without regard to the busy/free state of the medium." If the ACK is transmitted with a busy medium, there is a good likelihood that the ACK will collide with a message from another BSS, causing both signals to be corrupted. Since there is an

ACK_timeout MIB value available, it can be set to a value that n*SIFS allowing for several SIFS to take place before a free medium is detected before a valid ACK is sent out.

**Recommended Change:** Strike the last sentence of the first paragraph of clause 5.2.10. Strike the second paragraph of 5.2.10.

- Comment 31.

  **Clause:** 5.3, page 83, lines 6-7
  **Severity:** m
  **Comment:** The last sentence of the introduction reads that "Nor, must all STA's be capable of participating in PCF data transfers." This implies that for power management, DTIMs cannot be scheduled during the contention-free period. Also, Beacons and ATIMs cannot be put out during the contention-free period.
  **Recommended Change:** Require all stations to be capable of participating in PCF data transfers during the contention-free period.

- Comment 32.

  **Clause:** 5.3.5.2, page 86, lines 28-29
  **Severity:** m
  **Comment:** The asynchronous contention free procedure indicates that stations can get contention free service by "simply sending frames in the Contention period. This may be detected by the PCF, which may put the STA on the polling list". This is not a desirable mechanism. It is non-deterministic. When the CF-down flows, the station may not have a need to send data to the network via the access point, and the access point may not have data buffered for the the station.
  **Recommended Change:** Limit the case where a PCF places a station on the polling list without a poll request to DTIMs, and Beacons.

- Comment 33.

  **Clause:** 5.3.3, page 85, line 2
  **Severity:** m
  **Comment:** The text refers to the APF bit. The APF bit has been replaced by type b'11' and subtype b'0001'.
  **Recommended Change:** Correct the text to reflect the removal of the APF bit.

- Comment 34.

  **Clause:** 5.4, page 88
  **Severity:** m
  **Comment:** An important section (DCF PCF coexistance) is missing.
  **Recommended Change:** This required function needs to be architected and sufficiently described in the standard.

- Comment 35.

  **Clause:** 5.6, page 91, line 26.
  **Severity:** m
  **Comment:** The text does not describe if an ACK is returned for a duplicate fragment.
  **Recommended Change:** Specify that the duplicate fragment is acknowledged even if the fragment is discarded.

- Comment 36.

  **Clause:** 5.7.2, page 92

**Severity:** m
**Comment:** The MAC layer state machine should be driven by MAC and PHY service primitives.
**Recommended Change:** Explicitly show MAC and PHY service primitives driving the flows in the MAC layer state machines.

- Comment 37.

**Clause:** 7.1.2.3, page 109
**Severity:** q
**Comment:** How is the beacon interval set and used by stations? What if the value changes and a sleeping station does not catch the change? How does it become re-sycnhronized?
**Recommended Change:** Investigate the power management effects on synchronization.

- Comment 38.

**Clause:** 7.2.1.7, page 115
**Severity:** q
**Comment:** For an access point-based network, can TIMs, DTIMs and frames destined to stations in TAM, PSNP, and PSP modes be sent during both the contention-free and contention portions of the superframe? Since the definition of CAM states that a "station can receive frames at any time", does this imply that all CAM stations must be able to support receiving data from the point coordination function?
**Recommended Change:** Please provide clarifying text.

- Comment 39.

**Clause:** 7.2.2, page 116
**Severity:** q
**Comment:** Is the PSP power savings mode supported in the ad-hoc case?
**Recommended Change:** Please provide clarifying text.

- Comment 40.

**Clause:** 7.2.2.3, page 117
**Severity:** m
**Comment:** The text states for ad-hoc power management that "Each station shall monitor the power-management status of the other stations with which it needs to exchange frames. This is determined by examining the power-management bits within the frames generated by other stations." What if a station A changes its power management state and indicates it during a frame to station B while station C is sleeping. How is the sleeping station C supposed to know that station A changed state?
**Recommended Change:** A source station that determines that a destination station is in CAM mode transmits the frame using the normal CSMA/CA transmit rules. If no ACK is returned, the source station retries the transmission assuming that the destination station is not operating in the CAM or TAM mode.

- Comment 41.

**Clause:** 7.3, pages 118-151
**Severity:** m
**Comment:** It was premature to assign object identifiers to the management definitions. Object identifiers should have been assigned right before the draft is released as an official standard. Object identifiers indicate that a management definition is fixed in time, and will never be changed. That is not the case with the MIB as it stands today. Since the draft is still open to comments, the MIB definitions with object identifiers already assigned will be changing.

**Recommended Change:** Remove the object identifiers from the management definitions. When it is certain that the management definitions will not be changing, then assign a new group of object identifiers to the management definitions.

- Comment 42.

  **Clause:** 2.7.5, page 29
  **Severity:** e
  **Comment:** The direction of message is swapped for Privacy Response.
  **Recommended Change:** Change to "From STA 2 to STA 1"

- Comment 43.

  **Clause:** 4.1.4, page 50, figure and 4.1.2.1, page 50, figure
  **Severity:** e
  **Comment:** Units are missing from the figures.
  **Recommended Change:** Specify the units (octets for figure 4-1, and bits for figure 4-2).

- Comment 44.

  **Clause:** 5.1, page 64, line 23
  **Severity:** e
  **Comment:** MAC is written as "Mac".
  **Recommended Change:** Put "Mac" in all capital letters

- Comment 45.

  **Clause:** 5.1, page 64, line 24
  **Severity:** e
  **Comment:** In referring to the MAC state machine the sentence reads "It may also provide the sequencing required to provide the point coordination function and the associated time-bounded and contention-free communications services."
  **Recommended Change:** Change "may" to "must".

- Comment 46.

  **Clause:** 5.1.5, page 69, lines 5, 18,24
  **Severity:** e
  **Comment:** The primitive is MA-UNIT-DATA, not MA_DATA.
  **Recommended Change:** Correct primitive name.

- Comment 47.

  **Clause:** 5.2.6.6, page 77, fig. 5-xx: RTS/CTS with Fragmented MSDU and 5.2.6.6, page 78, fig. 5-xx, RTS/CTS with Transmitter Priority
  **Severity:** e
  **Comment:** RTS is not within a "box".
  **Recommended Change:** Correct the figure.

- Comment 48.

  **Clause:** 5.3.2, page 84, lines 29-33
  **Severity:** e
  **Comment:** The text is confusing PC and PCF, in this section and later sections.
  **Recommended Change:** Limit the use of the PC to the first sentence of clause 5.3.2.

- Comment 49.

  **Clause:** 5.3.3, page 85, figures on the page

**Severity:** e

**Comment:** The figure caption is missing from the first figure. The figure number is out of range for the second figure.

**Recommended Change:** Add and update the figure captions.