IEEE 802.11
Wireless Access Method and Physical Layer Specifications

Title: **Monday Afternoon MAC group Meeting**

Chair: David Bagby
11 May 1995

(Let it be noted that Johnny Zweig has volunteered to record the minutes without much of an exact idea of what that entails but I tend to take relatively complete notes anyway, so what the heck.)

Approval of March MAC meeting minutes.

No objections raised. Approved unanimously by those present.

New Submissions

Any papers to be submitted that were not identified this morning? None.

Goals:

Incorporate April LB changes to create D1.1 draft.
Finish processing D1 letter ballot comments (resulting in proposed changes for incorporation into D1.2)

Papers without agenda request before meeting:

[14] -- proposed new MAC state machine
[16] -- MAC/PHY interface functions (Mike Fischer says this is not high priority)
[80] -- Proposed value for contention window (best done in full MAC group)

(Ed Geiger borrowed the projection screen so his group will buy a round of drinks this evening ;-)

Scheduling

The MAC group will have flexible scheduling for the rest of the week.

Contention Window

Wim Diepstraten is presenting his paper [95/80] on contention window for consideration by the whole MAC group. (Unannotated statements are from Wim.)

CW is important for proper collision avoidance, so it needs to start with an offset, to avoid collisions where they are most likely to occur.

All STA should use the same CW or the access mechanism will be unfair, so it needs to be fixed in the std. It can impact total achievable throuput. PHY-indpendent.

Simulations determine the optimum CW window. Double CW value for retransmission. Simulator described in 11-92/26. Included fading/capture/distance. No hidden STA, 2 Mbps, with MAC and PHY overhead as per draft standard. Stations transmit to random other STA.

Three different traffic patterns: 100% long (1088Bytes); 100% short (64Bytes); 60% short + 40% long. Overall load controlled by a simulation parameter. STA do not generate next frame until after successfully transmitting current frame. (Load versus # of contenders graph for 10 active stations). Want to analyze: Collision Probability vs load factor, xfer delay vs load factor, throughput vs load factor, impact of CW on single station maximum throughput. Done with 0, 9, 29 other active stations. Tried 8/16/32/64 slots for CW. Only tried RTS/CTS for the 10 STA case.

Graphs of collision probability vs load for each traffic mix for each CW value. CW value of 8 leads to high collision probability.

Q(Chris Zegelin): What do you mean by Long versus Short contention windows? Wim: the paper means "CW for long frames" and "CW for short frames" etc.

Graphs of average delay.

Graphs of throughput. Largest CW has highest throughput.

Q(Simon Black): Is this CWmin or CWmax? CWmin. Wim doesn't know about CWmax.

Q(Simon): What about 2 stations contending? The 1 station plot shows how much the large CW is hurting performance. (No response from Wim)

Q:(Michael Fischer) Aggregate throuput? Yes.

Q (Chris): Network performance is delay/thruput, and in your graphs they are on top of each other; only the collision probability differs between CW sizes -- so why not use the smallest CW since it maximizes single station throughput (Large CW penalizes small number of STA situations)? Note that this is for ACKed frames. For broadcasts, the collision probability matters much more since there is no ACK. (Chris: broadcasts are not handled well with the current 802.11 mechanism anyway, so let's not use CW to address what is a more fundamental breakage in the standard) Wim: 32 seems the best tradeoff.

Q: (Simon) less is better since we don't always need it... (No response)

Q: (Mike F) There exist algorithms for estimating the average load on the network, maybe we could use one of them for 802.11, and we could adjust CW dynamically? Item for future consideration. An AP could actually tell its STA how busy the BSS is.

Dave: since this value is currently missing, maybe we should use this value for now and see how the committee members vote.

Simon: I want to see lower values.

Wim moves that we adopt the value 32 slots for the minimum CW size (CWmin). Seconded by Mike Fischer.

Discussion:

Chris: I am pleased that this work has done, but this will be completely dysfunctional for FH systems, since FH has such big slots.

Johnny: Won't exponentiation backoff work? Mike: with CSMA/CA it is much more expensive to collide, so working up to larger CW is costly. We need to decide if this is targetted at large or small PHY number of users.

Greg Ennis: There is a PHY dependency (# of stations in a BSS and range and slot size), so we may need different values for different PHYs.

Wim: For broadcast frames, reducing the contention window will have a high collision probability at high loads, and they will get lost.

Greg: On that point, this is not an infrastructure system, and those systems have different charactertstics with respect to broadcast frames. This anaysis was thus not complete, and I'd like to see if they are different.

Johnny: infrastructure is also asymmetric (broadcasts going from an MU to the wire are ACKed by AP, but the other direction they are not)

Wim: ACKs are applied to the most interesting case to the AP, not from the AP. This mechanism is independent of hidden STA. It gets worse when you introduce hidden STA.

Chris: The most interesting graph is the RTS/CTS case shows the lines on top of each other; this most closely matches the infrastructure case. So again I think it suggests that CW down at 8 makes alot of sense.

Dave: is further discussion useful? We seem to have two opposed groups just trying to convince each other.

Mike: In the infrastructure case, since the AP is not special, outgoing broadcasts get reamed.

Phil: I like having the CW be PHY specific, since slot size matters alot, and might eliminate the controversy. (Not a formal motion).

Dave: call for vote.

In favor: 3 Opposed: 11 Abstain: 5. Motion rejected.

Dave: Straw poll for what size people prefer: <8 slots (5 votes); 8 slots (5); 16 slots (8); 32 slots (3); 64 slots (0); >64 slots (0)

Dave: another straw poll: Should CW be PHY dependent? (9 votes) Not ?(1) Abstain (11)

Dave: yet another straw poll: (Tom T suggests using a dynamic approach to vary CW, with algorithm TBD) 0 in favor, 7 opposed, 12 abstain

Organization of Subgroups

Now let's move into smaller groups to discuss sections of the draft. Since some work needs to touch sections 1, 2, 3, 4, 5.4 (security cleanup), maybe that should be a separate group, or we could do that afterwards. Dealing with them as a lump seems wise -- we might even move section 5.4 text into section 3.

Groups:

Security: 1, 2, 3, (some of) 4, 5.4 (lead by Dave B)
4 (lead by Simon -- Need input from section 7 folks)
5 (lead by Mike F, though he also wants to participate in security group)
7 (lead by Bob Ohara)

Suggest we meet in 3 groups (security, 5 and 7) for today and tomorrow, then get to section 4 on Wednesday morning so it can use input from the other 3 groups. Wednesday morning we'll figure out how to communicate everything to group 4 and continue with the other groups.

Adjourn to individual subgroups.

==========

Tuesday Morning MAC subgroup meeting

9 May 1995 08:30
The MAC group needs to try to get our text together as we go so that we can present it to the rest of the group Thursday. Want to avoid sending stuff out for a letter ballot without having had a chance to discuss it in the meeting.

Adjourn back to individual working groups from yesterday. Lunch at noon, joint MAC/PHY meeting in this room at 13:00.
Section 4 in room 171. Sections 5 and 7 here. We can use the outdoor poolside tables after 14:00.

Goal: Finish 7.2 and get into 7.3 this morning.

==========

Wednesday Morning MAC group

Chair: David Bagby

10 May 95 08:39 (starting a teensy bit late)

Updates from smaller groups (summary of progress so far):

Sec 1/2/3/4/5.4 (Security):
If [95/95] and [95/96] adopted, then all comments will have been addresssed from D1 ballot. Comment table is updated. Will create delta table doc.

Sec 3:
Only issues outstanding are detailed service specification has lots of missing text in 3.2.2. Propose to add text there before second meeting out of ISO 8202 document. All D1 LB comments dealt with. Tom Siep will prepare text and submit for LB before July meeting. (Discussion about updating comment tables with resolutions to comments that have been dealt with here this week.) D1 LB tables are updated, so no new doc dist needed before D1.1.

Sec 4:
Only met for half a day on their own. Been working on getting management frames defined. Waiting for input from Sec 7 and Security groups. Have done beacons, probes, probe responses. Have a proposal for elements vs fixed frame discussion. Have been updating comment tables; hope to be completed this week. Will create a document that goes into next mailing. Notice that in beacon, putting TIM and DTIM stuff at the end makes a probe response look exactly like a beacon that has those elements truncated.
Will disribute diagrams, even if they don't get a chance to write supporting text, since most people only need to see diagrams in order to know what they mean.

Sec 5:
Dealt with sec 5.3, which is the first major section of comments not addressed in March. Should be back from repro tomorrow. All 5.3 LB comments addressed, covered by [95/100] and [95/101]. 5.0-5.2 still have issues that need to be discussed in the larger group, as major issues need to be resolved. Some LB comments not processed, since small group could not address them. 5.7 says "multirate should be removed" which is a contentious debate topic. 5.4 is in the security group. 5.5 and 5.6 will be in D1.1; all LB comments processed. 5.8 is so out of date that there will be a proposed replacement for the entire section mailed out for LB before July. Vote to put forward carries (15 in favor/0 opposed/1 abstain).
5.3 summary: "superframe" concept is being globally replaced with CF period, and is being linked to beacon interval (beacon begins each CF period). Thus beacons must be generated by point coordinator. Text has been clarified. Note that CFP not confined to a single dwell in FH PHY. This helps deal with some CF-over-FH comments. This also means that more than one beacon can be included within a CFP, with the

semantics of CFP-time-remaining in this CFP. There are some rules for polling list maintenance (minimal) to ensure interoperability (so comments that that is not the MAC's job were rejected).

Sec 7:
Have been attacking power management, have made some progress and addressed many comments, but need to examine implications of PS interactions with CF and TB users, so have gotten slowed down. Propose we split into power-mgmt/association separate sub-sub-subgroups. No MIB work done yet. Will have text to go with comment document.

Editor's Announcement:

Bob Ohara has D1.1 electronic copy available for distribution.

Proposed Changes to Security Sections for D1.2 (resulting from D1 LB comments)

David Bagby, Leon Scaldeferri, Tom Siep.
WEP Usage: WEP becomes the only privacy algorithm in 802.11 -- if you want more, use 802.10 above 802.11. Only needs a bit in the header. WEP remains an option (export concerns). WEP header bit only allowed to be set for Data and Authentication Mgmt frames. No other frames are ever encryted. Added MIB variables to control turning WEP on/off, so privacy mgmt message no longer needed. WEP usage is all based on receive and transmit STA addresses, not end-to-end addresses.
Authentication: Simplified the mechanism, so there are two types -- none and ESS-wide key. There is still a hook to expand later if necessary. Shared-key authentication requires implementation of WEP option, so must either implement both or neither (no need for WEP but no authentication). First msg of exchange always in the clear.
Note that shared-key authentication only guarantees that the STA knows the key, not that he is who he says he is. Need public key cryptography for that.
Hooks exist to add public-key challenge/response later as that technology matures, and as support grows to the point where 802.11 knows which one to add to the standard.
Editorial Reorganization: Security stuff taken from 2, 3, 5.4 and collected into a single new section that the editor will decide where to place. Changes to D1.1 Sec 2.3, D1.1 Sec 2.4.3, D1.0 Sec 4, D1.1 Sec 5.4 (deleted from section 5, moved to new section).
This addresses all LB comments on security.
Moved by Mike Fischer seconded by Chris Zegelin that:
802.11 adopt the changes as detailed in document [95/95]. Called unanimously to question.
Vote by MAC group -- In favor: 13; Opposed: 1; Abstain: 3. Motion adopted.
The one thing that hasn't been addressed is which pseudorandom number generator to use. RC4 is the only solution that has been prosposed, and has been shown to be relatively strong, and has special status as far as exportability goes, giving it good legal status. It has reasonable implementation costs. There are emotional issues associated with the fact that it is proprietary and owned by RSA, Inc. and many people don't want to adopt that into a standard. How much will it cost? Cannot discuss that in an IEEE meeting. RSA has been approached about using RC4 in 802.11. RSA has agreed to satisfy 802 requirements for reasonability, and will give **identical** licenses to anyone who wants to use RC4 in their 802.11 implementation. RSA has said they will offer terms with a choice of small-up-front-fee+royaties or lump-sum one-time payment, possibly with other choices.
Moved by Mike F, seconded by Chris Z that:
802.11 conditionally adopt RC4 as the WEP PRNG algorithm, provided that the following conditions are satisfied:

1) **RSA to send a letter to IEEE satisfying the requirements for "fair and equitable " availability of RC4 before the July 1995 IEEE 802 meeting.**
2) **RSA to further state in a letter to IEEE that it will make RC4 available under terms that are identical for anyone who wishes to use RC4 for an 802.11 WEP implementation**
3) **RSA specifies licensing terms for 802.11 WEP implementations which include at least the following scenarios:**
   - **litte or no fee up-front, with a per-unit royalty**
   - **a one time, per-company fee, with no per-unit royalty**

Discussion: Johnny Z asks whether text is available on paper. No, but it is online. Mike F points out that the restriction that we only reference RSA's document, not reproduce it, is reasonable since RSA is not allowed to disclose their algorithm publicly. Question about whether companies can use existing licenses with RSA for 802.11 implementations. Answer is that it depends on the specifics of those licenses. Ask RSA about that.
Vote by MAC subgroup: In favor: 18; Opposed: 2; Abstain: 1. Motion adopted.

Adjourn to sub-subgroups (10:40)

==========

Thursday Morning MAC group

Chair: David Bagby

11 May 95 08:30

Documents to be submitted:

Security

[95]
[96]
[??] Revised D1 LB comments

Section 3

[??] Revised Section 3 text

Section 4

[??] D1 Revised Comment Tables
[??] Revised Section 4 text

Section 5

[101] Revised Section 5 text
[100] Comment Resolutions
[14] Replacement State Machines

Section 7

Power Mgmt and Association have been addressed
Need a document number for reassociation text
[106] Proposed Changes to Section 7 text
[107] Comment Table

Status Reports from Working Groups

There seems to be a fairly high degree of consensus among those present concerning the state of the MAC report.

Paper Subject Ordering

Incomplete Subjects from March meeting
There are some topics still left unaddressed. For example, multirate.

Open subjects from D1 letter ballot:
Section 1 processed
Section 2 processed
Section 3 processed, except one section of text still being written
Section 4 processed, except mgmt frame formats for connection services, and needs elements for connection frames
Section 5 processed, except for multirate in 5.1, RTS/CTS usage, fragmentation (deferred from March)
Section 6 still empty; group agrees that the section cannot be deleted; Greg Ennis, Tom Tsoulogiannis, Bob O'hara and Mike Fischer volunteer to work on this section; need a document number; proposed text to be FTP-available by the end of June so people can download it before the July meeting
Section 7 processed, except 7.1 comments that were left over from March, and the MIB (needs many changes incorporated from May meeting changes, to be reviewed in July); 7.2 and 7.3 have been processed

Goals for July 1995

Send D1.3 MAC chapters for 802.11 letter ballot approval to forward to Sponsor Ballot.

Operating rule: "No putting decisions off." There will be a decision for all issues via process of elimination if no better rationale can pursuade the group to reach technical consensus.

After second letter ballot, there will be some TBDs that may or may not be addressed by LB comments, and we need to be prepared to deal with them expeditiously in the July meeting.

Adjourn back to small working groups to finish up

Goals for the rest of this morning:

1) capture the work we've done this week
2) try to address remaining open issues listed above if possible