Tentative MAC Minutes
Monday, May 10, 1993

The meeting was called to order by chairman Dave Bagby at 11 AM. Carolyn Heide secretary except when presenting, then Jim Schuessler took over.

Goal for this meeting was to do some protocol comparison and look at how the protocols satisfy the criteria in document 93/33. Dave had said last meeting that he would try to reformat that document but he apologizes that he didn't get to it. The second goal is to settle some security issues now that we have all had a chance to read the 802.10 standard - read that if you haven't.

The purpose of the protocol comparison is not to pick a protocol, but to get some real facts about the strengths and weaknesses of each protocol and evaluate them.

Network Layer Requirements, IEEE P802.11-93/64, by François Simon

There is an Internet Engineering Task Force (IETF), Mobile-IP Working Group that is looking at creating an implementation agreement concerning connectivity for mobile computers and would like to have an informal liaison with 802.11 to discuss mobility.

Discussion:
Dave Bagby: base station = AP in their terminology. Believes they have some implementation assumptions in their requirements. Their paper across the Internet read "tell me the address of the AP through which you are communicating and we can route to you". We have talked about a fuzzy DS and the concepts of association and re-association rather than an implementation. Greg Ennis: both of the requirements they have specified are what happens within the mobile station, they are not requiring the AP to provide any information there?
Dave: they are saying when you are inside the DS these are the things that you need to be able to ask and get answers to.
François Simon: how will our protocol provides passing that information upwards is the issue.
Dave: we have recognized this as events of association an re-association. They are asking to be notified of that. These services of the DS have been defined specifically for notifying them of this information they are asking for. The Mobile-IP group thinks very much of IP and can have a narrow view.
François: if you stick to the two requirements specified, they will be required of any network layer entity.
Chandos Rypinski: danger - the network layer must know how to address the mobile they want. Whether they need to know what AP to address is another story. One floor might have 16 APs, the fact that a station moved between these should not have to be known outside the room. We may have to define a distributed AP so that a mobile under any of them is accessible under one address. Otherwise the frequency with which a station must re-associate will be great. Somehow we have to say that the necessity of this function is not arguable, only the scale on which it should be applied. The domain of a common controller should be what the network layer is interested in rather than the individual AP.
Dave: summary - a higher stack group is interested in what we are doing. Starting a dialogue with them is a good idea. Anyone interested in that should talk to them.
Jim Schuessler: has been following this also. They go through the same vocabulary trials that we do - should we try to push them in our direction on terminology?
François: will give them our definitions.

The CODIAC Protocol, IEEE P802.11-93/54, by Carolyn Heide

The paper is in two part: The protocol description itself and a list of issues cross referenced with the original list of 21 Criteria (Doc. 91/138)

Goal is a combination of Co-ordination Functions (CFs) since she believes that one type will not meet the needs of all the users. Uses range from small autonomous groups to very high co-ordinated user populations. The proposed protocol operates efficiently in both by using a combination of Point CF (PCF) and Distributed CF (DCF).

Looked at two protocols. We all (should) be familiar with the WHAT protocol, but she prefers to call it the WHA protocol since the Time Bounded aspect is handled in the deterministic PCF side of CODIAC not in the TBS method specified by Xircom. The other is based on the Spectrix Reservation/Polling Protocol (RPP). It is highly controlled, slotted and controlled by a central node (PCF). It works well in a bounded universe, but as is, does not expand well or cover Ad-Hoc uses. Her goal was to combine the two and thus enhance both.

There are two modes, Centralized and Distributed, however ALL data transfer is done with the same four step RTS, CTS, Data, ACK process. A Mobile Station (STA) start-up procedure is simply to listen. If a controller (frame structure) is not detected, the STA has the option of WHAT or PCF protocol. Also makes the point that a PCF not necessarily be an AP, however not sure why anyone would want a PCF that was not also the AP.

The group applauds her brevity in explanation of Distributed protocol; one word: WHAT.

Centralized mode consists of a SuperFrame divided into two periods; Request and Data. Data is also divided in two: upward and downward. Phrases up and down come from reference point of controller (up from STA to Controller and vice versa). Protocol attempts to conserve power in mobile. If no data needs to be transferred, STA can power down during Request and Upward period.

Frédéric Bauchot: questions when STA can power down.
Ken Biba: Netware is 90% of market, so client is in control of environment and can power down for very long times as compared to superframe. Advantage to be able to do this.
Carolyn: This protocol can do this. You just can't receive data during the time you shut down. The non-office environment is not Netware.
Bob Beach: how long are these slots?
Carolyn: 250 microseconds in current implementation.
Chandos Rypinski: Is the superframe a variable length?
Carolyn: Yes, it can be on a frame by frame basis.
Ken: You must have an upper bound on length for initial acquisition.
Carolyn: Yes.

Forging onward ... Request Period has two purposes: to request bandwidth and to register with controller. Feels that STA should not experience any contention to request slots (requesting for bandwidth) and the dedicated slot handles this. There are some number of uncommitted slots after the owned slots for the use of unregistered STA.

Ken: Why do you separate registration and bandwidth request?
Carolyn: So there is no contention for bandwidth request.
KS Natarajan (Nat): so request period is limited only to registration and bandwidth request?
Carolyn: Yes, but could have the request sync specify zero registration slots and have this mean that all slots were available for both registration and bandwidth request, and thus force contention.
Ning Kong: You own slot after registration?
Carolyn: Yes, the controller gives you a slot number.
Nat: So if no data request, it is wasted data time?
Carolyn: Yes. However there could be a way to age out unused slots.
Ken: what is typical length of superframe if assuming 1 Mbit/s PHY?
Carolyn: I wouldn't try to imagine that. My implementations are fixed 1 second superframe at 1 Mbit/s (IR PHY) This is most not optimal.
Ken: If you have small cells with rapidly changing populations of STA seems to require small superframe size...
Carolyn: Operating in Distributed mode then would be more efficient.

Chan: Make clear that THIS system is better than current implementation, since it has dynamic length of superframe?
Carolyn: Yes, among other things.

Registration: Controller allocates slot to STA in request period. This becomes address of STA for further communications with the PCF. Understand that registration in this CF does not mean Association. Possible that completely isolated communications session could co-ordinate with this infrastructure to facilitate coexistence. Registration means you own a time slot only. This is the area to request bandwidth in a non-contentious manner. Question: Does this mean competitors companies must allow registration? Yes, you don't own the air. The request time slot number is used for addressing of all controller to STA communications. Broadcasts are done in downward data period so you can assure all are awake. There is a special FF address for this. Multicasts are done the same way with a multicast request and the multicast bit as defined by WHAT protocol. Questions: Concerns about address translation in controller. This is a valid concern, mapping the wireless address space to the DS address space may be complex, however 48-bit address is always known by both entities.

Data period, Upward: RTS is bandwidth request in bytes and CTS from controller may allocate less bytes or equal. Question: If CTS allocates less than RTS wants, will ACK take care of partial response? Not defined yet, but could choose not to transmit until you got full bandwidth request in one CTS. Upward data period, DATA only goes up, but frames go both directions, such as ACK.

Data period, Downward: Both Controller to STA and STA to STA data transfers possible. These exchanges take place using the four frame procedure (RTS, CTS, Data, ACK). Concern from customers that there is a waste of bandwidth here and perhaps we could remove some overhead. She would recommend that the protocol accept either immediate data or RTS/CTS exchange. STA to STA transfers are done in this period since you can be assured STA receiver is awake at this time. The controller issues CTS, but the Data goes to another STA which issues the ACK. Question: Are there two RTS messages - One for STA -> Cont. and STA -> STA? Could be, but as currently defined, no. Question: If you request and don't get serviced do you keep resending RTS for the same data? Must be some time-out since message may have gotten lost. When you retry should be implementation dependent.

Changing Modes: STA can change modes according with whether they hear a controller. There are nodes that are controllers all the time and nodes that can become controllers. One situation that might dictate this is observed traffic loads.

Ken: Centralized or Distributed mode has nothing to do with forwarding to a Distribution System? True?
Carolyn: Yes. Well put.

ACK and duplicate detection: Goal here was to filter "most" duplicates, with no guarantee and to minimize retransmission of data frames. The mechanism uses a Retry Bit, Sequence bit and Out of Sequence Bit. This not only handles retransmission of data but the loss of the ACK. She goes though several example foils -- see 93/54a. For STA to STA a particular RTS (RTSI) is defined to let the controller know it will not be generating the ACK for the resulting data portion. The controller could also repeat the data if the STA were not in range of each other. ACK is not related to mode (Distributed or Centralized), it is always there in either case. There is a time bound on wait for ACK. All retries are done is subsequent SuperFrames. The controller would not issue an RTS knowing that there is not enough time to finish the sequence with an ACK in the same SuperFrame. In other words, the four frame exchange is never split across SuperFrames.

In the case of STA to STA communication when they can't hear each other, one STA may in fact try to communicate directly at first, of course with no success, and then fall back to the repeat mode.

Chan: How would you feel about having the repeat mode as default?
Carolyn: Not a big issue. Should be provision for both.
Greg Ennis: Since the Controller generates the CTS in the Upward or Downward period depending on repeat or direct mode, it has to know the transfer mode beforehand.

How does this protocol work with fragmented packets? The number of re-assembly buffers equal to the number of possible stations that can transmit to you. Protocol has no way of distinguishing where fragments go ... Out of sequence fragments are not detected ... there are no sequence numbers - Therefore this is a single packet protocol.

Carolyn: yes, this may need to be added.
Chan: Fields could be added to accommodate this.
Carolyn: yes, could add complexity to accommodate anything, but worry about overly complex implementation.
Bob Crowder: An OSI node can only deal with 256 byte frames minimum. We must accommodate this as a minimum.
Dave B: OK, we need to think about packet length here a bit more.

Overlapping Modes, assuming a single channel case: Distributed/Distributed is a null case since it is the very definition of "distributed". Distributed/Centralized: Performance of both centralized and distributed STA in the overlap is degraded. Centralized/Centralized: STA in the overlap can't communicate without potential collisions. If there is a single channel system, APs or BSA's on different DS's better NEVER overlap. This is a characteristic of all single channel PCF systems, not just this protocol. We could try to warn the other AP to do something.

Chan: Actually overlapping BSA in single channel systems could be a reliability asset - if one AP could co-ordinate with another AP.
Bob C: Could stagger or Time Divide the channel. Doesn't think centralized systems have any disadvantage here.
Greg: Can't assume AP's can communicate over DS. They may be quite separate.
Dave: Don't confuse AP with CF.
Bob C: Thought we were talking about AP interfering with another AP. This is solvable.
Wim Diepstraten: Suggest use of Distributed CF! Solves problem.

Possible Enhancements: Page 21 of 93/54.

Did not address Frame Format details on purpose. Only important to Carolyn as an implementer, but largely could be defined by the group later. Of course there are some important aspects, such as Dest. ID (DID) at the front of the header.

Dave: Let's take the next 15 minutes for questions before the break. The section of the paper that addresses the issues log will be transferred without comment.

Nat: Registration is something that maybe happens once at the beginning of the day. How about handoff?
Carolyn: Based on one central controller that does not overlap with another.
Ning: Protocol is based on a centralized mode protocol existing network and is proven, and second part, distributed mode has been simulated by Xircom, but newly centralized mode changes are not proven yet. True?
Carolyn: Yes.
Ken: Yes, but remember distributed mode is only part of the WHAT protocol, not the "T" part.
Bob C: Carolyn has done a service by merging the protocols. Seems like a good place to begin work from.
Carolyn: My goal is to convince the committee that we need two CFs that work together. It's important to my users to have no contention in high population environments and I need support for single channel. I would like to see the starting point of further MAC work as this proposal, where distributed mode is the WHA protocol and centralized mode is this protocol enhanced with features from the other PCF protocols proposed so far.
Dave B: Assumption that PCF always present for Isochronous Services - true?
Carolyn: yes. Controller could decide that length of SuperFrame should become much more stable to support isochronous.
Greg: Why is it that the "T" in WHAT is not as viable for TBS?

Carolyn: TBS support is not the point of this PCF, but rather large populations.
Greg: Why eliminated the "T"?
Carolyn: It is really redundant with the Centralized CF mode.
Ken: Yes, the "T" is a Point CF in itself.
Dave B: You have traded off latency (access delay) with bandwidth efficiency with Reservation slots. We need to examine this. How does this compare with the latency with the contention CF?
Bob Beach: for a 1000 stations, you are burning 7/8ths of your bandwidth in the Request time to allocate 1/8th.(12%) of bandwidth. Most LANs work pretty well at this loading. Are you willing to do this? Why not just run a contention protocol?
Bob C: Those numbers are not accurate.
Carolyn: you can set these ratios up as you wish. Your calculations are along the right lines, but 65% is closer for 1000 or more stations. There are a number of trade-offs you can make here.

Discussion between Bob Crowder, Bob Beach and Dave Bagby at high speed.

Evaluation of the CODIAC Protocol, IEEE P802.11-93/, by Carolyn Heide

Next paper is Carolyn's document (93/59) on answering the questions raised in Wim's document from last meeting (doc. 93/33) There were several areas that needed more clarity before a clear answer could be made. In particular the "reliability requirements" don't seem to exist. They are addressed in a number of issues in section 19 of the issues log on reliability. See paper.

Discussion of how to implement time-bounded support. There need to be limits on length of SuperFrame or at least on number of service opportunities within one SuperFrame. Could have multiple DSYNC's within one SuperFrame.

What does different service levels mean? Means different periods for time bounded service or different priorities for traffic. Quality of Service (QOS) could be included in service level, but there is a lot dissent on that. Delay or functionality (broadcast for instance) or bandwidth are all QOS issues. Bob Crowder thinks of functionality as conformance, not QOS.

How do you initialize a network that has multiple access points Dave B. mentions but doesn't want to discuss it now.

Straw poll: Who thinks we need time bounded service with a distributed CF? After much discussion (i.e. words..) no one believes this is necessary; most believe it's not possible.

2.1.2 What is STA to STA between BSA's? Rather, do we handle single BSA and multiple BSA? In a single channel environment, we must have isolation between cells. According to KS Natarajan the answer is always no, since question doesn't make sense.

2.2 Important to separate bandwidth allocation function from Association with a particular network. Two people could have an Ad-Hoc network using a Point CF (Centralized system) by registering with PCF, but not attempting Association to become a member of the network DS that PCF may be connected to. We need to look at Distributed mode overlapping with the Centralized case and look at the implications.

2.3 Might want to create an AP to AP protocol to handle mobility. (Will MAC carry 48 bit addresses <DID, SID> in each packet transmitted?) What are the implications of having another way to spell the name space? (aliases for IEEE addresses.) Long discussion on addressing. There is a range of addresses for controllers (which may be APs) and a range for mobile nodes (STA). You don't address the CF, but rather the station containing the CF.

Question to think about: Can we say that in the case of the presence of STA containing an AP, it always contains the PCF if operating in Centralized mode for that BSS? General agreement here.

Wim Diepstraten: Doesn't cover the definition of PCF well. At any given time it is only located at one point If a token ring or bus ... no, everyone says this is distributed CF.
KS Natarajan (Nat): What about the PCF shifting from one STA to another?

Dave Bagby: We allowed for this to make power consumption more fair to battery powered users.
Greg Ennis: If all sta within BSS are always co-ordinated with the same PCF?
Much disjointed discussion surrounding location of PCF in presence of AP and/or Ad-Hoc networks.

Summary: Everybody think over the issues here.

2.4 Operation with multiple BSAs with single channel. 2.4.1 Yes, but without co-ordination, there is degradation. If a protocol over the DS between AP could be invented, these problems could be mitigated. No solution for BSSs in multiple ESS. 2.4.2. May infer use of power control to optimize spatial reuse. This is a MAC Management issue really. 2.4.3 Must watch the definition of overhead verses payload according to Chan. 2.4.6 There are data and management data frames that are kept separate with a control bit. Perhaps we could combine Registration with Association. Response time linked to SuperFrame length for Re-association. You must wait for next SuperFrame to issue next Re-association request. (this is true for all access when moving boundaries of BSA) Wim states question is "what is involved in Re-association"? This protocol does not define this process. This is not related to general response time of the protocol.

This is a good between categories break point, we will start again tomorrow after the joint MAC/PHY meeting.

Meeting adjourned: 5:05 PM.

Tuesday, May 11, 1993

The meeting was called to order by chairman Dave Bagby at 10:10 AM. Carolyn Heide secretary except when presenting, then Jim Schuessler took over.

Evaluation of the CODIAC Protocol, IEEE P802.11-93/, by Carolyn Heide (con't)

3. Support for Ad-Hoc Networks. Note again that registration to AP does not mean association, thus Centralized mode allows Ad-Hoc simultaneously with Infrastructure based. 3.3 - No-one in the room disagrees that separation of Ad-Hoc and Infrastructure versus centralized and distributed modes. 3.4 - A controller box could be built to support Ad-Hoc networks in a centralized fashion if that was desired.

4. MAC Must support low power operations. 4.1 versus 4.2 is a "micro" verses "macro" view of time. There are elements of the CODIAC protocol that minimize power consumption on each SuperFrame (a micro sense) as well as allowing power down for hours or days. Wim's view is that all packets must be accepted, i.e. that sessions not be broken.

Dave Bagby: interpretation is that if there are particular features that support low power, what are they, what are the trade-offs?
Leon Scaldeferri: Interpretation of question: Are there things needed when the station is powered off that it needs to power back on? What "state" information needs to be stored?
Carolyn: yes, that is a good question and we need to put time bounds on this as well.

5. MAC need to support multiple PHY. Greg Ennis thinks it might be interesting to address relationship between timings for SuperFrame and timings of a FHSS PHY. Carolyn says SuperFrames could be made to work with FHSS very well.

6. MAC Access Function Requirements

6.1 - Carolyn suggests that, if you wanted to, you could implement stations which only operate in Distributed mode and then "shut up" in Centralized mode, i.e. not work, but not interfere. Dave Bagby says that would have to be an option, there may be a problem with standardizing this type of operation.

6.3 fairness - Greg wonders, looking at the controller as a station: is it getting any preferential access? Carolyn says yes it does have a small advantage in that it doesn't have to make a register to get request slot to be able to send data.

6.6 - Leon think this question means look at ISM interference as some non-WLAN interference such as microwave ovens. The co-channel is like-system interference. Carolyn agrees, but we have addressed this issue in numerous other places, this question is redundant.

6.8 Overhead - Part of the overhead is the request and registration slots, and these can be allocated on a user definable basis.

Pablo Brenner: Understand that there is a switching time Rx/Tx that could be hundreds of microseconds. Should we include this in overhead number?
Carolyn: doesn't agree there are many turnarounds compared to other protocols. Also feels we should not include PHY dependent timings.
Chandos Rypinski: My belief is that a radio that does not turnaround in a few microseconds is not suitable for 802.11 use.
Ken Biba: possible to build radios that switch much faster at reasonable cost.
Kerry Lynn: we should be aware of PHY issues that might impact us.

Wireless LAN Medium Access Control Protocol: 2nd Update, IEEE P802.11-93/62,
by Frédéric Bauchot

Second update of the protocol introduced in 1991.

New: (1) introduction of LBT when required by the PHY layer, to comply with UPCS (User-PCS) band of single channel PHY requirement. C-period may be optionally LBT if required by the PHY layer. It is a hybrid between LBT and reservation-based.

Operation on different PHYs: ISM band - relies on cell isolation provided by PHY layer. No LBT required. IR - if channelized LBT not used. Otherwise use LBT in the contention based interval.

Greg Ennis: ISM band, cell isolation for DS requires use of different spreading sequences (Frédéric agrees). Spreading code length doesn't offer much isolation.
Frédéric: longer code, better isolation, but we may have to face that the number of overlapping cells is not large, so limited may suit all practical applications.
Phil Belanger: FH offers cell isolation, but that isolation is not perfect. There is the problem of frequency overlap. How does the protocol operate that case?
Frédéric: same as any interference - low level packet ack and retransmit.
Phil: agrees. But for the protocol described there is also a superframe imposed in the channel. What if part of that is damaged, the headers?
Frédéric: if one STA doesn't hear a header and it was addressed it losses a slot assigned to it and the AP has to reassign. You miss a superframe. Headers are broad so it is the same as if they were lost to bit error.

The purpose of these modifications is to optimize performance in the UPCS band.

Dave Bagby: overview of UPCS - in WinForum some etiquette work divided frequency into 2 bands, one for voice, isochronous functions and the other was left open for more LBT, contention based traffic. This proposes splitting this protocol to accomplish this goal.
Jim Schuessler: parallelism - listening with some other radio portion during the c-period as well as sending the header. What is going on in the isochronous channel when you are doing that?
Frédéric: nothing, but the idle time is short.
Jim: why cross that boundary and leave the bandwidth idle when you could be leaving the bandwidth for the asynchronous STAs. Difficult to use that isochronous bandwidth for data, so difficult that it is prohibitive?
Bob C: if that is truly a requirement of that etiquette you should tell them that sucks.
Wim: you are using 2 channels: for data transfer the isochronous part; for the c-part the requirement is that it be done in that data channel?

Frédéric: there is data in the other part too. Bursty traffic may go in the c-interval. But if you have voice or multi-media you may choose to use the a and b intervals.

The information in first two periods is considered a burst in UPCS concept etiquette, so each of the a and b headers has LBT first, then each transfer in the C period is LBT.

Wim: means that in the b period where you have STA to AP or STA to STA they do not use LBT?
Frédéric: that whole period is considered a burst, do you LBT before the whole thing.
Phil: works for any STAs conforming to this protocol. What about others?
Frédéric: you may ask STAs to understand the a-header. With that alone an STA knows how long to postpone access.
Phil: for the a-period but not for the b-period. During the b-period there will be idle slots? Are there gaps - no energy detected by a protocol that doesn't understand this protocol?
KS Natarajan (Nat): a gap for less than the time you listen is not a gap.
Jim: using LBT before the a-header. This will cause your superframe to become non-deterministic, so TBS will not work.
Frédéric: for a single channel PHY channel, you may face a problem.
Dave: protocol is much happier with multi-channel PHY than single channel, it wants PHY layer isolation. How much does it require, or how sensitive is it to non-isolation - can this be quantified? How does the protocol react, is there some kind of linear reaction to changing levels of isolation?
Frédéric: it is better for perfect cell isolation provided by PHY. Otherwise it has to cope with interference. The addition of the LBT has enhanced this protocol's ability to deal with these.
Bob C: paper says this is like a 2 FH PHY - This places a large implication on DSSS implementation.
Frédéric: this is proposal maps the protocol into the UPCS band.
Bob C: number of frequencies in the FH increases the isolation provided. It should be possible to actually chart the reaction as the number of channels changes.
Wim: lower level of performance under no isolation.
Frédéric: don't believe that is the only criteria providing performance. The amount of bandwidth is more important.
Chandos Rypinski: a system characterization of isolation is using reuse number as an index. A lot of cells, and 100% coverage requirement, some number of frequencies required to get independent operation. Cellular design based on 7 frequencies to get 100% area coverage with independent use. Depends on AP, robust modulation, etc. The net affect is a smaller reuse number. MAC group has no way to deal with a PHY medium proposal other than by postulating a reuse num. We would have a hard time agreeing on one. MAC could say there is a possibility of simulating use of certain combinations of STAs being blocked.
Frédéric: if PHY provides some cell isolation, this can be used as a means of increasing the throughput of the system. E.G. FH may be used to increase the capacity of the ISM band as opposed to using a simple contention based access and using a lot of overhead to avoid collision. If PHY can be used to avoid this overhead, let's use it.
Bob C: in the a- and b-periods - is there an essential difference between this and CODIAC?
Frédéric: the fact that CODIAC has no contention after registration. IBM proposes a combination, and results in contention in the c-period.
Carolyn Heide: CODIAC uses reservations for everyone, while IBM allows STA which don't need fixed interval service to contend for service.
Phil: also IBM has backed the polls into the header. When requesting multiple slots, are the slots contiguous?
Nat: they are how the scheduler allocates them, but continuous would be the easiest. It is implementation dependent.
Phil: it terms of TBS; e.g. real-time voice, you may not want them contiguous.
Frédéric: in the reservation request you can specify the amount of information you asked for. Could be expanded to specify this information - whether you want contiguous slots or not.
Wim: isochronous and asynchronous reservations are different. Isochronous is for a lot time. What about async?
Frédéric: request for a given amount of data to be transferred. Assume large frame segmented - I have 10 pieces, so I ask for 10 slots. I contend for this reservation request, but once I get it it's mine.

Jim: squashing CTS info into one header frame.
Carolyn: CODIAC keeps RTS and CTS individual frames to maintain compatibility of our step process in both centralized and distributed mode. This allows for low implementation complexity of STAs, despite the bi-modal CFs.

Question about ack. There is no broadcast ack of course. Otherwise acks directly follow each data frame. If you miss the ack you move to the next superframe to retry. If one STA has two slots, to preserve sequence you keep trying to get each one out before you move to the next. Send first frame, first slot. If it doesn't get acked, send it again in the second slot. Might take you to the next superframe to get it all across.

Bob C: loss of ack can cause duplicates.
Wim: an STA requests bandwidth, gets allocated - how does the controller know that the data arrived at the STA?
Frédéric: if the AP is the destination of that data, no problem, it can allocate slots for retransmission. If the destination is another STA, then the STA must repeat the reservation. AP is not aware that the transmission didn't work (we can't rely on his seeing this failure). The STA must re-request. If the AP saw it can initiate re-assignment of slots.

Criteria for MAC Protocol for Wireless LANs, IEEE P802.11-93/63, by KS Natarajan

Purpose of submission is to provide short assessment of the most recent version of the IBM protocol. Primarily follows Wim Diepstraten's items in document 93/33.

2. Are infrastructure-based multi-cell networks supported?

Wim: ad-hoc overlap - would they be supported by the infrastructure network?
Nat: each is an independent network. Single channel they will impact each other dependent on the overlap and what the STAs in the overlap are doing.
Wim: what do you consider an overlap - same channel? What is the impact?
Nat: if you have an infrastructure, that can help, but no co-operation between the two APs is assumed. To give an answer you have to make assumptions about the overlap extent and amount of traffic. If there is only one STA in the overlap and it is asleep, there is no overlap.
Bob Crowder: overlapping BSA in the same ESA - how is this handled? If SuperFrames are not co-ordinated don't STAs in the overlap interfere (single channel)?
Nat: STA is associated with one AP, even if it hears two. The extent of interference depends on traffic and number of units.
Leon Scaldeferri: contention overlap would get some traffic through, reservation periods would suffer most.
Carolyn Heide: you might be able to synchronize BSAs in same ESA to maximize contention period overlap.
Wim: no specific communication procedures across the infrastructure have been specified?
Nat: there are schemes that can be used, but they have not been proposed here.

Single channel operation.

Dave Bagby: AP knows STA has left because they get notified by another AP?
Nat: yes.

Multi-channel operation.

Wim: when do you analyze topology of network?
Nat: at installation time. Or you can try to learn as the network operates.
Dave: how do you find an AP in a multi-channel environment? When do you look for a new one? How do I know what channels to listen on - is there any help provided by the protocol to do these things?
Nat: for the initial association you listen, find APs and register with one. As you loose an AP by moving you have to initiate a procedure to find the next one.

Frédéric Bauchot: for instance, any AP may be aware of other APs and could share this information with others. The APs can use the help of the DS. Not just a MAC point but a PHY point too - if the PHY is agile, any STA will have to do channel scanning to find APs.
Dave: since your MAC is better for multi-channels, I thought there might have been more consideration for this kind of thing.
Wim: getting in synchronization again with an FH AP is a problem.
Frédéric: no clean boundary can be made between MAC and PHY in these areas.
Ning Kong: this is a MAC protocol presentation. This problem fits into some kind of MAC to PHY frequency management issue. The protocol itself is transparent to DSSS, FH or IR.
Phil: thinks it's a MAC issue. It should be acceptable for Nat to say we haven't disclosed that yet and move on. How an STA moves around, how it re-associates and how do you find APs quickly are generic MAC issues. The last is the only with one any PHY aspect.
unidentified: a common channel could be used as a reference point for scanning information.
Nat: you could assure that each superframe will pass through a particular channel and only have to listen for a superframe time to guarantee hearing it.

3. Are ad-hoc networks supported?

Carolyn: setting up an ad-hoc?
Nat: manual intervention to turn an STA into the PCF, quick and easy. A rotating PCF procedure could be developed, not as not been yet.
Bob C: so a new station listens ...
Nat: and joins a network if it hears one, may choose to create one if it doesn't.
Bob C: many little networks created like that.
Nat: expects networks to be formed in a more organized fashion.
Dave: but there could be an extreme case where each two of the STAs could form there own network and have a great number of overlap networks. Supposes we probably wouldn't let this happen, we would all agree and network together with human intervention.
Nat: assumption about ad-hoc is that it is an extreme case where there is nothing but the portables available and there is no help from the infrastructure.
Dave: separating registration from association gives some flexibility here. I have to be authorized to associate with the infrastructure but anyone can register with the PCF.
Frédéric: it has to be an end user decision to set up an ad-hoc. The decision to have an ad-hoc network belongs to an end user first. Everybody entering the room may ask (i.e. the human beings, not the STAs) if they want to join.
Carolyn: this imposes a requirement on the upper layers. The users select somehow from their application that they want to join the network and that information must get conveyed down to the MAC layer.

There is a discussion of registration with the controller and association with an AP, and overlap in the two protocols (IBM and CODIAC), which is too disorganized to capture.

Bob C: we will need to decide, do we have a super co-ordination function that everyone in range must join, or do we elect to not have that.
Phil: everybody within range - from who's point of view?
Bob C: the PCF. When you are out of range you degrade to other, DCF MACs.
Jim: also we are needing to bring in a single channel versus multiple channel situation. Increasing the aggregate bandwidth by changing channels is a desirable thing.
Bob C: not all methods of channelizing may allow that bandwidth advantage.
Bob R: negative impact to protocol if implemented registration with a control point if you hear one.
Nat: the possibility of registering without joining the infrastructure could be added.
François Simon: AP will always be a PCF - is that a valid assumption?
Nat: the word AP is not required by ad-hoc.

Greg Ennis: does the PAR mention support of ad-hoc and support of TBS simultaneously? If no TBS is required in ad-hoc, why not have two different CFs, one which is just the enhanced LBT that you do in the c-period.
Dave: ad-hoc you have referred to as extreme - do you mean uncommon? Thinks ad-hoc may the first implementation we see.
Nat: no, extreme but not uncommon.

4. Will MAC support low power operation? Yes.

Bob C: for single channel system the power impact of re-association is marginal. If you have to scan channels it is different. Worst case you might have to listen through n channels if there are n channels.
Nat: you can do better than that.
Dave: impact of multiple channels can be the length of time it takes you figure out what's going on when you wake up.

Number of STAs

Carolyn: c-period is slotted ALOHA, so isn't there a point where according to number of STAs and traffic load where that breaks down?
Nat: refers to referenced performance documents.
Dave: contention characteristics change depending on the PHY being used, that is an interesting characteristic that may not apply to some of the other protocols.

Robustness

Wim: doesn't remember ack being part of the original papers.
Nat: every slot is data followed by ack - up, down and c-period.
Phil: how big is the ack?
Nat: 80 bits.
Wim: granularity of bandwidth for isochronous slots?
Nat: some integral number of the number of slots, implementation dependent, multiple slots per frame can be assigned. Changing the scheduling algorithm is all that is required to accommodate the varying requirements of isochronous.

Nat will try to get a copy of reference LAM93 *[see note - which he did later in the week.]*

Wim: for TBS, typically one slot or a few concatenated slots reserved per superframe?
Nat: one or some fixed number of slots per superframe it depends on the bandwidth you request. You may need a bi-directional slot reservation. The more variety you have the more sophisticated the scheduler becomes.
Wim: recovery - you described recovery in the next SuperFrame. Voice might not handle that.
Frédéric: in some cases recovery will be very straightforward. If 2 slots per frame, and in a given superframe you use only one. If that one has an error then you can use the second to retry. If you can't afford to wait until the next superframe when you have only one slot, you may choose not to try to recover that time.
Nat: if you think the channel is bad you may ask for a extra slot.
Dave: why LBT for single channel only?
Frédéric: don't burden a multiple channel system with the overhead. Single MAC for all PHYs does constrain all solutions with the tightest criteria. The LBT can be large or small, but even saving small is worth while.
Bob C: specifying retires desired or not has a lot of considerations, but it shouldn't be an implementers decision. It is a QOS decision.

A Distributed Access Protocol proposal supporting Time Bounded Service, IEEE P802.11-93/70, by Wim Diepstraten

Based on a distributed access method that has been discussed but not presented. Based on CSMA/CA that is working well in existing products today. This is a first level of introduction, further details will come out in

subsequent submissions. Tried to show how this type of MAC can support time bounded services. Described in 92/51.

Dimensioning for voice allows support of a host of industrial implementations that are usually based on TBS.

There is no issue of any STA taking on a PCF to support ad-hoc, support is seamless.

Carrier sense function provided by PHY. Procedure - MAC senses carrier; when it is free for asynchronous inter frame spacing (AIFS) access is immediate.

Immediately following the deferral is where you need to avoid collisions. The slot time is picked randomly (could be by whatever Ethernet uses). Following a defer is when you use the backoff. When traffic is low you don't defer, you so don't wind up doing backoff.

ACKIFS (ack inter frame spacing) is a set time which may be PHY dependent. Transmitter turn on time, media propagation delay plus carrier sense detect time are the total detection time = slot time. The difference between ACKIFS and IIFS (isochronous inter frame spacing) and AIFS can be multiples of slot time. As an example, document 92/37 shows a system with slot time of 23 microseconds.

Retransmission algorithms may differ per PHY. In an FH you may have an algorithm which prefers to wait for the next hop.

Performance evaluation in 92/51, which also deals with simulations of overlapping BSAs.

Jim Schuessler: where would 802.3 show in these graphs?
Wim: around the same curve, in the same range. In CSMA/CD the slot time is longer. This has longer IFS, but shorter slot time.
Bryan Hartlen: what about hidden nodes?
Wim: assumes all STAs can see all others.
Dave Bagby: overlapping BSAs is just the same as increasing the number of STAs as this is entirely distributed.
Wim: simulations take into account attenuation, which allows for packets seen by some and not others. Document 92/26 describes the simulation environment.
KS Natarajan (Nat): do you have a comparison chart with same offered load but increasing number of STAs?
Wim: refers to page 21, shorter packets, Novell size, with twice as many STAs.
Nat: to see the affect of increasing STAs with the same offered load would be useful.
Ning Kong: increasing STAs would eventually cause performance to degrade after it levels off. Packet size is important too. What does buffered load mean in these charts?
Wim: refer to 92/51 for the description of that.
Bryan: MAC overhead included in throughput - figure 1 and 1a. If the 87% includes overhead then where is the remaining 13% ?
Wim: collisions and the gaps (IFS). Collisions which are not collisions can go on - simultaneous transmissions, but the interference ratio is such that the packet is accepted. Those medium affects are taken into account.
Bryan: how much is the MAC overhead included?
Wim: 20 bytes per frame plus the PHY overhead, the training time of the PHY in use - 150 microseconds per frame. The frame bytes are counted as payload in these STAs. In 92/51 are charts showing pure LLC payload.
Chandos Rypinski: caution - a Novell time-out may make some portion of blocked stations disappear.
Wim: that is taken into account in the simulations.

The carrier sense is more sensitive than the data coverage. Fast receive-to-transmit turn around is essential for carrier sense accuracy.

Phil Belanger: how would this MAC perform on different PHYs? How many of the PHYs we are working on could provide the point? The ones I work on don't provide that - a 10 dB sensitivity is unusual.

Wim: 23 microseconds is not that aggressive according to our experts. A wider bandwidth than a DSSS PHY, but in symbol rate it would be the same bandwidth as a FH. The wider bandwidth gives us more noise, so the ratio would be the same as for a FH - it has less bandwidth but also less noise.

TBS characteristics described.

Nat: congestion control?
Wim: coding schemes in voice which are built such that you could drop half of your packet and still the first half contains sufficient information for the quality desired. That allows you to drop half and still maintain your connection.
Jim: can't start dropping half your isochronous frame without knowing your CODEC scheme. The MAC would need to know what type of compression you are using to do that. You can't apply that universally.
Wim: this is outside the MAC, facility can be used by higher layers to take advantage of this.
Frédéric: if you are not at all aware of the CODEC at all, do you get any benefit?
Wim: different service levels could be taken advantage of to accomplish this. Different applications follow different strategies for what to do when your transmission is failing.
Frank Koperda: 802 is considering allocating a bit for priority indication, that could be an indication for it.
Frédéric: what are typical examples of congestion situations?
Wim: focusing on voice applications right now. Dimension connections to take advantage of talk spurt characteristics.
Frédéric: thanks to the characteristics of the talk spurts you can overcome what would have been limitations?
Wim: suppose the maximum isochronous capacity available is for 10 connections, that would be 10 100% load. Look at what capacity would be available for any talk spurt, you may be able to handle 20 or more than that. If you said I have room for 10 channels of 100%, you may say I can go to 15 to be safe because of the talk spurt nature.
Frédéric: congestion is a characteristic of the class of service.
Frank: when you try over committing, you get into trouble. When you need 100 percent you've got it, but the asynchronous can go on in the gaps opened up by the bursty nature.
Wim: limiting the capacity of the isochronous capacity so that the asynchronous bandwidth is our priority. Won't over commit.

For TBS a regular beacon is issued by AP, AP contains PCF for TBS. Overlap situation the same as every other PCF. Beacon goes out regularly, but not every "superframe" (which is not really an appropriate word for this protocol).

Ning: how do you distinguish TBS and asynchronous traffic?
Wim: the services are using the access method with different priority levels. Difference of priorities is the difference in the IFS. Because the IIFS is shorter the isochronous traffic has priority.
Ning: with no deferral, how is priority assigned?
Wim: an asynchronous access method is used to set up the connection. Set-up is not shown here, only use.
Nat: connection id comes back from set-up ...
Wim: connection id is address. AP randomizes the isochronous STAs per "superframe". Length of superframe is such that it can still contain a maximum size asynchronous frame.
Phil: balance STA polling order with minimized delay variance?
Wim: burst may last entire superframe time. AP has built data to go at beginning of SuperFrame. Data arriving in a superframe waits for next superframe, so that is the total delay.
Phil: reserving ahead - is there a method and if so is it necessary?
Wim: assumes something setting up the connection before this game starts to role.
Phil: that means only managing the limits, making sure the isochronous doesn't get bigger than you want.
Wim: don't want the overhead of putting everyone in the polling list when they don't have an active connection. So only when there is an active connection will they be polled.
Bob Beach: Why always allocate enough space for maximum size asynchronous frame in TBS?
Wim: to prevent a large asynchronous frame in progress at start of superframe using up the whole TBS time. Connections would loose data. If desired, isochronous connections have recovery procedure using

asynchronous methods, those need to be done before the start of the next superframe. Isochronous STA must make sure it is awake in time for the next poll. Asynchronous portion of superframe could be used to scan for better APs.
Jim: is it possible that a large asynchronous frame followed by an AIFS, then a full length asynchronous frame starts - it will take up a lot of the SuperFrame, but not all of it.
Wim: you might loose some asynchronous time, but there is still time for isochronous.
Jim: do beacons bring you back from the creeping off base that you might do?
Wim: there is no creeping. SuperFrames are at fixed length.
Jim: STAs all keep timing information?
Wim: yes. The beacon contains information for time synchronization purposes. The transmit blackout period around the superframe boundary avoids the collisions that could arise when no deferral.
Jim: why isochronous ack?
Wim: to give a chance for recovery in the same SuperFrame if you want it.
Jim: comment - 20 millisecond SuperFrame, within that the delay variance is large. 10 milliseconds may be about the maximum you want on one side of the MAC to human interface boundary. In a previous submission Jim concluded about 30, but during the presentation comments reduced it.
Wim: high speed PHYs can be used to accomplish that. To allow mixed voice and data on lower speed PHYs around 20 is the limit. Shorter increases overhead. Dimensioned with a maximum packet size of 1500 bytes. Fragmenting to lower packet limit could be used to lower that SuperFrame size.
Bryan: what is the relation to patents on this process? How could we adopt it? You should share that information with us out front.
Wim: CSMA/CA implementations are patented, but CSMA/CA is public.
Dave: 802 rules don't prevent you from adopting anything not public.
Vic: has the guidelines of the IEEE patent policy.
Wim: it just so happens that Vic is also NCR's intellectual property guy. Perhaps he has a nice phrase for us to cover this.
Dave: requests NCR to please identify what portions are covered by intellectual property rules you own so that we can make decisions about what we can use and how to proceed. Standing request to anybody presenting to identify such things. Don't want a sales job then discovery that something has been withheld.
Frédéric: what if the PHY is UPCS band. How does this work?
Wim: I'm not up to date on WINTech matters right now, so defers the question.
Bryan: does the beacon use CSMA? If so what are the timer accuracy ramifications?
Wim: yes, but could give it a high priority. Beacon comes from same source as isochronous, so there will be no problem there.
Tom Baumgartner: what about power management support?
Wim: isochronous can turn off from poll to end of superframe. Asynchronous power management will be dealt with in other submissions.

Presents performance example (analysis not simulation).

Jim: assumption in talk spurts - are you dropping half the samples?
Wim: activity factor of 40%.
Jim: how many ISDN b-channels could be supported?
Wim: 4 for the 1500 byte packet scenario. Fragmenting the packets smaller would increase the maximum isochronous capacity. Have been assuming the 20 milliseconds also, increasing the framing period increases the capacity. There is useful capacity left over with PHY speeds such as we are aiming for.
Chan: this result is for one isochronous cluster. You did overlapping and moved the clusters farther apart, doubling the capacity. 5 diameters apart gave you 10% improvement. So a continuous carpet gives a 25% reuse factor.
Wim: without considering boundaries - no isolation factors. Also a constant attenuation coefficient independent of the distance between the networks. In reality the farther away you get the more that increases.
Chan: the 25 number is improbable, but whatever the isolation cluster is has to be divided by the reuse number.
Wim: depends on the PHY and the channels.

Chan: improving the reuse number is needed for getting improvement in a continuous system
Wim: other things like power control can be used to improve the system too.

Not all copies of 70a contain slide 13.

Meeting adjourned: 5 PM.

Wednesday, May 12, 1993

Meeting called to order at 8:45 AM, by chairman Dave Bagby. Carolyn Heide secretary.

WHAT Protocol Evaluation, IEEE P802.11-93/85, by Phil Belanger

Purpose of submission is to provide an assessment WHAT protocol following Wim Diepstraten's items in document 93/33.

Page 6 discussion

Jim Schuessler: maybe this is just semantics, but doesn't an AP have to be connected to a wired LAN to be an AP?
Phil: repeating between stations is an AP function.
Dave Bagby: it's an AP with a null distribution system, but let's not get into that.

Page 8 discussion

Carolyn: ad-hoc with TBS overlapping two PCFs?
Phil: to be tweaked to allow this.
Ken Biba: information is propagated so STA in the overlap do know there is a conflict.

Page 9 discussion

Wim Diepstraten: what kind of PHY co-ordination do you mean?
Phil: for instance FH sequence at start-up time.

Page 11 discussion

Phil: doesn't think ad-hoc and infrastructure connection simultaneously should be a requirement although you can do it. Thinks the application for that is limited - is the complexity worth it?
Frédéric Bauchot: thinks simulation with both should be a requirement.
Jim: what application for this?
Wim: visitors come in for a meeting and I want to set up an ad-hoc meeting with them rather than connecting them all to the infrastructure. But I want to participate in the meeting as well as stay on my own infrastructure.
Phil: if you have already been associated with an AP, you just go away for a while and come back without loosing that association.

Default ad-hoc has no security, anyone participates, generated automatically. Also have named ad-hoc networks where the participants need to know the name in order to participate, and along with the name you get a level of scrambling.

Dave: whether you can access or not depends whether you know the name - authentication is based on knowing the name?
Phil: no authentication - if you know the name you can play in the BSS.
Wim: scrambling is tied to the name somehow?

Phil: it is a parameter used when the network is set-up. Requires a little administration to get a little security. If you don't care you operate in the default.

Page 12 discussion

Dave: you have provided a mechanism for some other layer to recognize the state (sleep-wise) you are in. When I'm asleep I have a way to tell the AP that the STA is asleep. It can then do something because it knows you are asleep.
Jim: requires timer on STA asleep so that it knows when to wakeup and check for something for it.
Ken: export information to take advantage to the behavior of the stack above you.
Jim: elements of the protocol intrinsically support that. You are described things that are above the protocol.
Phil: there are things that allow you to notify the AP that you are off-line. Allows you to go off-line for hours/days. Tie it into a notebooks regular sleep function, and wakeup and be in the same state you were in when you went to sleep.
Dave: necessary but maybe not sufficient. If there is no traffic coming to you, OK ... but what other facilities could you get to work in conjunction with this - buffering is finite.
Phil: look at applications - real transfers in a client/server model is initiated by the client. Gratuitous server messages are a different story. There is a cost of re-acquiring the network, when you wake you have to figure out what's going on. On the asynchronous service, 1 Mb 5 ms-10 ms is about the time (TBS is TBD). Use this mechanism to do a low duty cycle using timers in the STA, based on the cost of re-acquiring the network.
Dave: AP has PCF in it. Is there an interaction between sleep and the isochronous service? If you tell the PCF you're asleep does it free up the bandwidth reserved?
Phil: that would be an error case - if you have an active connection you don't go to sleep.

Page 13 - concept of appending the PHY specific information immediately after the preamble to 'parameterize' the service.

Page 17 - in an infrastructure network a key is handed out on association with the infrastructure and data is scrambled according to that. Only the payload is scrambled. This is done transparently to the STA user.

Jim: different keys for each 'link' in and infrastructure?
Phil: have chosen to keep them the same in the same infrastructure domain. But you could do that if you wanted.
Frank Koperda: some governments don't allow encryption, or specify that it must be breakable.
Ken: consider this as an option you can turn off at manufacture time. Just trying to make this as secure as wire, not solve the end to end high level.
Bryan Hartlen: key from AP or control point?
Phil: not part of the CF. It is a management function that resides in the AP because that's the gate you must pass to get the infrastructure.
unidentified: you are passing the key - so anyone can listen to it.
Phil: the key is more encrypted than the data after you know the key. Each STA has its own private key and the management service has a public key that corresponds to that. The AP and STA authenticate each other prior to giving out the key.
Kerry: is key fixed for duration of the association? Each AP has a database and I am known by the all APs so that I can associate with any of them?
Phil: key can be changed as often as you like. What you do with that database is up to you. You must be known by all APs you must go through. You can choose not to do this.
Dave: these are above the MAC, what's important is that you have hooks to them.
Wim: as secure as wired?
Phil: believes that the wireless piece is now more secure than the wired LAN. Scrambling sequence is 16 bits, the key is 16 bits.

A Compromise MAC Protocol Concept, IEEE P802.11-93/75, by Jim Schuessler

Talked about point 3 from the abstract in the joint meeting yesterday.

Carolyn Heide already presented the CODIAC protocol which is a hybrid of WHAT and a Reservation/Polling protocol. Independent of this there were thoughts roaming around the world about how to combine WHAT and IBM - there are various ways of doing that and this proposes one of them.

Motivation - how to get a compromise and how to make progress in this committee. One way to do this is to hurt both parties equally. A compromise isn't a compromise unless both sides make changes.

In a non-infrastructure based system the WHAT doesn't change in implementation, but the frame structure changes to HDLC frame structure. HDLC frame structure has been tested and it works, and there are some advantages in terms of the overhead. To prove that takes a computer and a simulator and a lot more time than I have.

Wim Diepstraten: why change frame structure?
Jim: to change WHAT protocol. In a compromise both sides must change.
Ken: thinks the combination of CFs is a good goal. The WHAT protocol already has a reservation based system in the 'T' part of the protocol. Trying to use an alternate 'T' system - the Spectrix proposal or this proposal is intriguing. But framing is a different issue entirely. Why do we need 16-bit CRC, bit stuffing, and frame delimiters?
Jim: I did this independent of what Carolyn did, and it's gratifying to see thoughts are converging.

What is an option, is an issue that arises here. Can we have STAs that only do one CF or the other, not both. Phil Belanger and Ken Biba think that you should operate DCF, or in the presence of a PCF join it.

unidentified: maybe two co-ordination systems is a good political solution, but technical compromises are always bad. Twice the implementation complexity and everyone chooses one.
Ken: no. The frames don't change, this does not have to be a doubling of the protocol, it may be in the order of a 10% increase in the protocol. What's the benefit? Traffic models and efficiency we can do to show this, but nobody really knows and no simulation will be truly accurate. The distributed CF is good for low delay and low traffic, the other better for high population and less data.
Dave: whether compromise results in a bad things is a philosophical aside. There is a very promising thing happening here. There is a wide recognition that anyone who says "this is what I propose and I'm not changing anything and you should adopt it" is not going to get anywhere. Encouraging to see people thinking about compromise. In strict technological terms there might be some cost, but without it there wouldn't be standards.
Jim: but, as chairman, how do we move forward?
Dave: thinks we will deal with that later this week. Amazing things have occurred - proposals in front of us with contention used to get started, PCF used for isochronous. Very different implementation but same philosophy. How to move that forward is a different story.
Kerry Lynn: first time I have been here - there appears to be a consensus between the 2.4 GHz FH from bottom up. If we can build consensus from top down we may come together.
Dave: Jim asked how can I merge IBM and Xircom. We don't have that much consensus yet. But using that as an example, what do those groups think? If anyone is here with orders not to compromise, admit it now please.
Tom Baumgartner: has a sword to bear - if it appeared we were going to agree on a CSMA/CA only Spectrix would certainly leave.
Dave: has a strong suspicion that CSMA/CA would not satisfy your needs. What is that need that is not met - the group can decide that the need is met or that it is not relevant.
Tom: need is expressed in the need to handle very large populations.
Ken: having looked at the problem of managing the slot exchange I could argue the problem can be handled by CSMA/CA.

Chan: supports Tom, if CSMA/CA decision believes that would be unworkable in large systems. The radio channel is never silent. Simply listening for carrier, that is not a compromise-able point to me. The system would be unworkable.
Ken: agrees, you have to do more than that. Examining compromise is a very useful direction. We are convinced that some mixture of a CSMA/CA and a PCF is a useful direction to research. Market is a different story. Bi-modal CF advocate.
Tom B: yes, he is too.
Dave: Nat or Frédéric, what do you think?
Frédéric: thinks this may be a starting point for investigating future avenues. Cannot say more than that.
Carolyn: just a note, reason Spectrix advocates bi-mode operation is for high population support, not TBS support.
Kerry: next meeting can we talk about framing issues separately? The compromise sounds like a good one. Are we in agreement that this is a fruitful direction?
Bob C: likes the Spectrix detente (has no relationship to Spectrix). Is neutral, and thinks it is the better protocol. Solves the problem of the single channel PHY because all STA required to register with the PCF if it is there. It may cause degradation, but doesn't degrade below any others proposed. Services TBS better than any of the CSMA/CA solutions. Puts complexity in the headend and takes it out of the STA. The STAs only deal with the same set of frames. Low cost DCF system can be made.
Frédéric Bauchot: IBM protocol shares some of the same characteristics.
Bob C: can't let the fact that we have big companies here run over the best solution.
Ken: looking for direction as opposed to support of particular protocols. Some straw vote representing that direction may be a good. Love to hear IBM's answer too.
Nat: haven't had an opportunity to evaluate the Spectrix protocol in depth yet.
Carolyn: thinks that the PCF's are very similar.
Tom B: made an attempt to incorporate a lot of the WHAT protocol into our system, with Xircom's permission, so we can't take all the credit for all of any praise we might receive (thank you Bob C.).
Bob Beach: doesn't like the Spectrix protocol at all. Large overhead, needed only for vastly complicated systems. CSMA/CA gets through approval committees fast and is easy to implement. If we want a protocol this decade don't aim for complexity - no bi-modal operation. Let's not argue the value of CSMA/CA - we have used it for years. Reservation protocols need too powerful a system to implement. These are speculative ideas of what we might be able to get working sometime.
Jim: asks Bob C - you compared CODIAC to WHAT, but not CODIAC to IBM.
Bob C: CODIAC has: requirement that DCF collapse into the PCF when it is there. It maybe could be added to IBM, but is not. That is essential. Registration separate from association. Being registered and requesting in slots for the data will be more efficient than a CSMA. Has no problem with the IBM a- and b-periods, just the c-period. Doesn't like contention for every data transfer.
Jim: IBM could be adapted to suit, but they haven't yet.
Kerry: likes idea that STAs could operate DCF and then revert to a PCF. Product could be built expeditiously that only used DCF and had option for PCF support when it came along later. Straw poll might be looking for agreement that DCF and PCF switching is something we want.
Nat: paper says proposing use of LBT and it will be further specified later.
Bob C: in the WHAT protocol, doesn't like the understanding he has of the error recovery scheme when duplicates detected by storing frames from every other STA (Phil says that that is not how the protocol operates, Bob must be mistaken). Also TBS in WHAT, thinks non-synced users in the same BSA could clobber TBS (Phil disagrees, thinks that interference sources are the same for all other protocols too). Feels that if STAs in the area must play by the PCF, the number of interferers is minimized.

On return from morning break, Dave Bagby: progress has been made here along the lines of wanting to merge stuff. Don't imply the protocols being discussed this AM are the only protocols. This is our first look at some of these, and we need to go off and think and learn more. Would like to stop this discussion and move on to other topics (there is no objection in the room.)

LAN & MAN Security Revisited, IEEE P802.11-93/66, by Leon Scaldeferri

That SDE layer sort of floats, and could have been sucked into the MAC or LLC, but wound up at the bottom of the LLC (as opposed to the top of the MAC).

Page 4 - header means security header, not addresses.

Page 9 discussion

Wim Diepstraten: specific association between two STAs?
Leon: could be a group association. In this table when I see the SA and DA show up I know how to associate them. The first question you ask is "do I have an association between these two, if not, I'm not going to do anything". This is after you have registered.
Wim: question would be asked by the AP?
Leon: For instance, when in the CODIAC protocol you require a STA to register with the PCF to do ad-hoc, if one of those STAs asked to send something into the DS, you would look and see no association so you wouldn't do it.

On non-implementation of features the appropriate blocks in the flow diagram become a null action.

Wim: function of the SDE designator?
Leon: the SAID allows more granularity of groups - group ids and individual ids. It is an option provided, don't ask me why it was provided. Why both these paths should be provided, ask 802.10 !
Bob Crowder: the right hand path has pre-established associations. The left path is more applicable to wireless - you conduct a negotiation prior to establishing the association.
Leon: because the SDE is only between MAC entities, it may well be that it is to facilitate an end to end association. A MAC to MAC association may only travel the right path, no clear header because it is a local event.
Wim: the left is more end to end, the right is MAC to MAC?
Bob C: more pre-established versus negotiation. This may make wireless more on the left path because they may not be shipped with a pre-existing associations.
Wim: SDE designator is optional, so the clear header is optional - how do I recognize whether it is there?
Leon: the SDE designator is a reserved LSAP, so a normal LLC PDU would have a LSAP there. You can't have a protected header without a clear header, so if the clear header is not there, the first field is the regular LSAP.
Dave Bagby: 802.10 provides a rich variety of things you can do. We don't specify which ones will be used in 802.11, they are available to implementers.

General discussion

Wim: your assessment - the standard is such that we can use it as we want it. But what we need is clearly MAC to MAC only.
Leon: ISO model says encryption is an authentication method - if you can't decrypt him he doesn't belong. The NCR paper seems to imply the headers are not desired. It doesn't answer the question of how you establish the initial set-up. How you are going to exchange the keys.
Kerry: those issues are de coupled.
Leon: yes. Key management issues are de coupled from this process which is what you do when you've chosen the key.
Kerry: chicken & egg problem. I want to join a WLAN and I don't know the key. I want to associate with an agent who can authenticate me and give me the key. I have to do this in the clear - is that a trap door?
Dave: please refer to the paper from Whit Diffie - we have discussed these things previously, and there well known are ways around it.
Kerry: if the MAC can accept clear traffic for exchanging keys then are we trapped into accepting clear data?
Leon: the 802.10 procedures allow you to pass through to talk to the registrar, wherever that may be.
Phil Belanger: you still have to demux 2 streams of traffic, encrypted and de-decrypted. Until you get the key your conversation is in the clear, so the registrar must be able to understand 2 types of traffic.

Dave: this is outside the scope of 802.11.

Security in Wireless LANs, IEEE P802.11-93/69, by Jan Kruys, presented by Wim

This paper addresses (1) how applicable is 802.10, and (2) device authentication.

Jan's assertion is that 802.10 is an end to end security service, and we a need MAC to MAC confidentiality service. But Wim thinks maybe Leon's presentation just said that 802.10 does provide this MAC to MAC service. Leon says yes, he believes it can be used as a MAC to MAC confidentiality service.

Kerry Lynn: if SDE does support the bottom picture on page 2, would you have any objections to it?
Wim: I don't object to 802.10. It has a lot of flexibility. I contend that we can pull a subset of 802.10 into the MAC and give it the functionality. The lower picture on page 2 is what we need. We don't want the upper, because it would force changes in all stations on the wired LAN.
Tom B: if we can be convinced that 802.10 performs the function in the lower picture would you accept 802.10 as the security that we need?
Wim: yes, we could adopt 802.10 as the prime source of the functionality into the MAC and use a subset which will meet our needs. No, I don't want the full 802.10 capability overhead.
Tom B: your answer is no?
Wim: yes my answer is no.
Dave: 802.10 sits between LLC and MAC. If it provides what we want how do we implement it - do we want to require that every 802.11 widget has it all in it? We could say if you build a widget that needs security here are the hooks that allow you do use whatever 802.10 hooks you want. It doesn't matter whether it's in every widget or not. You just couldn't have a secure conversation with anyone who chooses to do none of it.
Wim: trying to get a whole picture of this myself. In my mind I see that function more integrated into our MAC and we adopt a subset of the functions specified by 802.10. It's not that the security level we think we need can at will be implemented on a user basis by having that user implement an SDE between the LLC and the MAC on the STA. My feeling is that it should be more integrated with whatever we do in the AP.
Dave: I think you get what you want by using 802.10.
François: to Leon - is there a conformance test suite for 802.10 (Leon doesn't know). If there is we have to pay attention to that.
Leon: believes they have identified the objects you will be able to flow through their diagrams without getting stuck anywhere. Assumes that a kind of PICS proforma is where they're headed.
Dave: there is no combination of entries in that table that is illegal, so it's a bit different.
François: worried about choosing a subset that does not match that PICS entry.
Dave: we should not redo their work and run the risk of breaking something.
François: take 802.10 as is and let the user choose their own PICS.
Leon: you could go down the list of questions - false to clear head, true to confidentiality, etc. If that's our set and it remains fixed, then now we have a set that remains compliant.
Dave: don't believe the set will be static.

Jan's assertion is that we use it as an example, but it is end to end so we can't just use it.

Dave: believe that the way 802.10 works satisfies what you say there. Is an algorithm defined for these things, if not you have to define it.
Wim: not referring to any particular algorithm.

Ron Bjorklund: today in the wired LAN that is handled at higher layers. Why would you need security levels at the MAC?
Wim: prevent eavesdropping by externals.
Dave: if you assume a shared key crypto system then you are concerned that people shouldn't read each other's stuff. The only thing to do is encrypt different messages with different keys. But you could use a different system to get around this without this at the MAC layer.
Ron: this kind of security need not be provided at the MAC layer.

Dave: 2 aspects - just on the wireless link itself. You try to avoid compromising the wired LAN. The end to end security is not our concern.
Ron: is a subnet wireless network level of security really a valid concern.
Dave: thinks that you could do that at 802.10 layer.
Bob C: you have to put those mechanism in since 802.10 is at the layer boundary.
Ron: if you want security then use the level provided by the entire LAN. If you do that then is there a necessity to have another level?
Dave: do mean encryption of encryption, or do you mean degree of encryption?
Ron: different security between STA and AP for each AP in system.
Dave: 802.10 provides you with that.
Bob C: can't see a lot of algorithms in these STA, it is either going to be negotiated or fixed.
Leon: we are trying to get as secure as the cable.
Dave: 802.10 provides: choose the algorithm none, there or not there is irrelevant and we want that for sure; if you choose algorithm number that provides just enough to get as secure as a wire; (possibly those two are the minimum we require) or you could choose the latest couldn't break it anywhere - the same mechanism gives you all three. Just a matter of where we set the minimum.
Bob C: may wind up with the AP having to support the highest level all the time.
Leon: would have to have a flag that told the AP to remove it or not as appropriate.
Dave: what does the AP do? It knows what's being used and could choose to remove it or not and it all still works fine. It all depends on your DS. From the .11 point of view you set it up between the STA and the AP and the rest is transparent.
Leon: whether you remove it or leave it at the AP is just a Boolean in the association process. It is set up in the negotiation of the association.
Dave: let the DS take care of it, the decision gets made at the AP.
Bob C: you may be putting a big burden on the AP.
Leon: it depends on the DS.
Bob C: if we had one algorithm on the LAN then the AP would know remove this on entry to the DS or not.
Wim: undo it at the AP all the time, even if it has already been done at the ends. We are trying to help the wireless segment security, not predict end to end.
Dave: but what if I want something stronger?
Bob C: so have the AP not strip that. We don't want every node and AP to be burdened.
Leon: for an association between 2 STAs they negotiate their key, then only those 2 STAs can talk to each other no one else can eavesdrop. If an AP has more than one association he has to store a key for every STA associated with.
Dave: 802.10 can do that. The AP has to store the keys, but that's the price you pay. I would not want to make that a minimal requirement for all 802.11 implementations.
Wim: foresees this as an important functionality. Do we need additional protocol functions to do this.?
Dave: this is above the MAC. You are building logical networks. Believes you could do this without any additions to the MAC protocol only to the DS. Minimal set ought to be either clear or just enough to be equivalent to the wire. Not all .11 adapters should have to have this.
Wim: but the architecture should allow you to do this.
Bob C: solution should not depend on public key algorithms because it could become a business problem - implementing the complexity of the AP.

Discussion on key synchronization.

Dave: do you believe key sync is a MAC problem? Dave believe it is a network problem.
Bob C: key management happens at layer 7.
Wim: in addition to that we need to handle a synchronization issue between the management part and the data part. You need to know if data is encrypted by old key versus encrypted by the new key.
Bob C: that's what SAID are for.
Dave: the granularity to me here is when an STA associates to an AP you choose some security system and that is constant until the association is broken. If you need a new key, break the association and do it again. That is how you change the key. It's not the MAC level that determines when the key is changed.

Carolyn: hears Wim saying write a piece of 802.10 over again in the 802.11 specification.
Bob C: thinks Wim is saying refer to 802.10 specifications with the list of security association parameters as minimum requirement for 802.11.
Wim: technically in the writing of the specification, yes. What I picture is that whatever we pull into 802.11 would be compliant with some parameter set of 802.10 .
Bob C: your group security would require you to more do than the minimum 802.10 functions.
Wim: still wonder whether we need protocol elements to do this?
Bob C: we don't have the complete set of association primitives and parameters. These things are parameters of association and re-association and such.

Device Authentication

Chairman: we discussed device level authentication, we settled the issue and closed it in January. We re-examined it again in March. If you want to re-open we need a % vote to re-open. The fair thing to do is take the vote, if there aren't enough people we shouldn't discuss it anymore.

Issue 6.5 - vote to reopen: yes: 2, no: 8, abstain 6. The issue is not re-opened for discussion.

Issues we decided to close in March to the determination that 802.10 was suitable.

Issue 6.4 - How will authentication and registration be specified in the 802.11 standard?

Wim: in light of discussion we had, shouldn't we try to identify what subset is applicable to what we want to achieve?
Dave: issue 6.9 addresses this.
Wim: no, 6.9 talks about the algorithm not the subset we are going to support.
Dave: if you choose 802.10 as the mechanism it provides a coverage wide enough to supply what we need. You pass algorithm numbers and there is an authority that maps numbers to algorithms. The assumption in 802.10 is that once an algorithm has a number it never changes. You can pick the number you want for the level of security you want. The question do we want to pick an algorithm to give us a common algorithm, is viewed as independent from do we want to use 802.10 as the mechanism to get that algorithm.
Wim: there is no relation to what algorithm we chose, OK. You want to say use 802.10 mechanism to refer to that algorithm. Wim thinks we need to specify the minimum subset of 802.10 . We don't require an 802.10 implementation that needs to understand all the options provided by 802.10 .
Dave: you want to specify a combination of parameters necessary to identify the minimum amount of functionality to incorporate into 802.11 widgets. The only way to answer that is to decide what is the minimum level of security required. A coming question is about getting to the equivalent level of wires. You want further refinement.
Leon: just saying use 802.10, means using that security/association object list they have, then figuring out what is true and false for 802.11's default case.
Phil: what does registration mean in this issue? I'm happy to apply 802.10 concepts, but if we're talking about registration with a CF, or as previously applied to association with an AP, neither of these has to do with 802.10. Association has more in it than just authentication, we can't look to 802.10 to define all of it.
Francois: if one is to use 802.10 and select to have the null set, can one provide his own mechanism on top of 802.10.
Dave: my opinion - if you pick the null algorithm then you are using the algorithm null. But if pick the algorithm which is your own number, then no you can't have both. But does it allow you to do your own algorithm - yes.

Leon draws two overlays on top of page 7 of document 93/66, which lists the station and security objects for 802.10:

The first column shows how some of those objects would be set to get the clear setting, and second to get a minimal set that gets you what might be the equivalent security to a wire:

Station_Clear_Hdr:	FALSE	FALSE
Station_MDF:	FALSE	FALSE
Local_SAID:	N/A	N/A
Remote_SAID:	N/A	N/A
Assoc_MDF:	N/A	N/A
Confid:	FALSE	TRUE
Confid_Alg_ID:	N/A	xx
Integ:	FALSE	FALSE
Integ_Algo_ID:	N/A	N/A
Padding_pres:	FALSE	
ID_pres:	FALSE	
Remote_SDE:	FALSE	

Wim: this is in the association transaction, not part of each a frame structure?
Dave: watch the 802.10 meaning of association.
Leon: a STA might say I support xx and yy, and you tell me which one you want to use today. When two STAs become associated they find a mutually agreeable set. This is exchanged at association time.
Wim: is there any frame overhead when you choose the null case?
Leon: no overhead.
Frédéric: last meeting we addressed problems if compression is not done before encryption. Encrypted data is not compressible. We can compress in the MAC if we use compression. Issue 9.5 is related to this.
Leon: 802.10 is a logical layer. If you combine the compression algorithm with the encryption algorithm you can still use this table of parameters.
Frédéric: but it resides in the LLC. A bridge has no LLC.
Leon: we can put in the MAC, and say we have incorporated an 802.10 implementation with the following parameters. The table that shows the layer is logical only - you can implement it anywhere you want.
Dave: we have an open issue, shall we do compression. Suppose we choose no security - 802.10 can still turn up at any time or place and you are going to have the problem of compression.
Frédéric: is just warning that privacy decision reflects on the compression decision.
Phil: so it is a layering question. The 802.10 functions would be fine if we could put them at any place in our world ,and I think Leon says we are free to do that.
Leon: this a transparent layer, its location is not important at implementation time. Ask for an xx algorithm that does compression and encryption.
Jim: that's interesting - maybe we identify a control structure for compression. It makes compression negotiation very easy.
Phil: we might wind up with 3 algorithm numbers: encryption, compression, and both.
Jim: those fields are all optional in 802.10 . There's a lot of decision as to which fields we chose.
Dave: uncomfortable with the thought that we need to understand .10 in detail before we can decide what to do.
Kerry: I can think of an algorithm that might require a clear header. There is some relation to issue 6.9 .
Ning: don't have a clear picture of why we want to use 802.10 . The reason is authentication, registration is a 802.11 MAC problem. Registration is a MAC function. Authentication we can manually insert a table of addresses into APs, for security we only need a secure way to send that. We can use 802.10 to help us in authentication and registration, but not just take it to do these functions.
Leon: 802.10 is a layer 2 entity designed to provide confidentiality and association control at layer 2. We are in layer 2, and this is a layer 2 entity. It provides a framework to identify the functions you need to do and gives you the flexibility to do the implementation you want.

Dave: there is an 802 standard that does what we need for security, as a member of 802 we might not be allowed to do anything else.
Jim: agrees we should use 802.10. But 802.10 has options - it's not as simple as saying we just use 802.10.
Dave: we have to decide to use it before we choose the options.
Wim: is this a layer onto of our MAC, or is it part of the MAC?
Leon: believes that you could define a standard that says you do these 802.11 things and these 802.10 things.
Bob C: we can't declare a requirement for a higher layer. It is a sub layer above the MAC. This is a conformance question.
Dave: we have the right functions either way, and we will find out a way to fix the wording.

Then ensued discussion between Bob C. and Leon about whether you can stack 802.10 implementations (i.e. can data that has already 802.10'ed be 802.10'ed again). Leon thinks you can and Bob thinks you can't (thinks that at least it has not been analyzed for that).

Close the issue with the following wording: Use 802.10 mechanisms and we will have to decide what is needed to define the (eventually) agreed minimal functionality from 802.10" and we will need to identify the 802.10 parameters. **Vote: 19,0,0.**

Issue 6.6 - Is there any additional work on security that needs to be done in 802.11 in addition to the work done by 802.10?

Dave: the intent of this issues was do we need to invent anything.
Bob C: but we have to define an algorithm.

Vote to close the issue with the answer yes: 20,0,1

Issue 6.7 - How does re-association interact with authentication?

Dave : believes we didn't close this issue because we wanted to decide on 802.10 .
Wim: didn't realize that we were talking about 802.10 in general, but specifying it as the confidentiality solution.
Dave: association we have talk about - to become associated you must have successful authentication to a confidentiality level. This refers to what you need to do to become associated.
Wim: we have voted to adopt the 802.10 mechanism for doing confidentiality specifically.
Bob C: are we saying that every time you change APs, you break your association, and re-associate so any security association must go on again.
Dave: that is your fall back position. So we invented pre-association so that could be done out of the critical path. The AP pre-authenticates you to other APs (if you ask it to), so when you move you just re-associate and you're authenticated already. It's really just a case of *when* did you invoke the 802.10 .
Frédéric: pre-authentication is to remove the burden of authentication or to minimize it?
Dave: to minimize.
Rifaat Dayem: this requires APs to communicate - this gets out of the MAC level.
Dave: this a is facility you can make use of but if you don't or cant, then you don't get the benefit.
Bob C: we must know what are confidentiality issues and what are conformance issues. Pre-authentication is a conformance issue. Does 802.10 define an authentication mechanism?
Leon: if you decrypt right you are authenticated is one way to do it.
Dave: we have talked about the 3 step process and the example transactions. Some of those transaction invoke 802.10 functions.
Bob C: pre-established or negotiated SAIDs is what SDE does for you.
Dave: how re-association interacts with authentication is sometimes it causes you to invoke 802.10 functions.
Kerry: authentication implies a database, and I prove I am OK to the owner of that database (or message signature), and he hands me a key. Will an authentication method be part of 802.11?
Dave: believes we have convinced ourselves that we have the appropriate hooks to support these mechanisms.

Bob C: the association is done by 802.11 or some undefined key management - it is not done by 802.10 for you. 802.11 will define an authentication protocol and 802.10 will provide the mechanism for finding or negotiating pre-established security associations.

Close the issue with the following text: 802.11 will define authentication transactions and 802.10 provides the mechanism for negotiation or finding pre-established security associations. Pre-Authentication transactions mitigate possible performance impacts. **Vote: 12, 0, 1**

Issue 6.8 - How does re-association interact with privacy?

Close with the following text: The only interaction is if the new AP can not support the current privacy algorithm, then it impacts the re-association (which could fail). **Vote: 15, 0, 2**

Issue 6.9 - Shall the 802.11 standard specify one or more publicly available privacy algorithms which all stations shall be required to support (one privacy option shall be "none")?

Bob C: this means your AP must talk with the none option, you can't refuse to associate with someone.
Jim: have to negotiate down to the minimum. This means you have to
Bob C: this is an end to end protocol, the node can reject you but the AP can't.
Kerry: you're talking about information security as opposed to communication security. A customer in your lobby cannot join your network without permission.
Bob R: once you come onto the AP, if I am the mobile node it is my concern whether the stuff I am sending is safe. If I decide to operate in the clear or not that's my choice. Trying to get to anyone's end node is a different story. Does just access to the network constitute a potential breach - it's like hanging Ethernet drops out in the parking lot.
Dave: privacy = at what level can we talk. Authentication = I know who you are. Association is after both of those, will I talk to you now. If you can only talk in the clear I can say no, I won't talk to you that way.
Alexander Belfer: in ad hoc is there no security because we're using 802.10? Mechanisms discussed earlier force authentication process to be in an AP.
Leon: 2 STAs in an ad hoc may authenticate each other.
Dave: steps between an AP and a STA, are just the same as STA to STA. There is an open issue about who initiates the transactions, undecided yet.
Bob C: so ad hoc is harder to set up than infrastructure.
Jim: we need to go through the procedure maybe.
Kerry: there is also implicit authentication - you and I agree beforehand what our password/key is, and so when we meet we can ad hoc.
Bob C: so the guy who entered the password has become the authenticator.
Dave: this does not restrict you to AP either.
Jim: from a user point of view this is OK. But I can't map this into the procedures we have heard.
Leon: remember group identifiers in 802.10 - we will all have the same key settings because we are all in the same group.
Bob C: we are mixing authentication and key setting. We use the three step process to accomplish this.
Dave: let's get back to the issue.
Wim: minimum is clear means yes, 802.11 will select other algorithms but they don't need to be all implemented.
Dave: proposes that the minimal is in the clear and a set that is equivalent to a wired LAN be defined. Believes we will need wired equivalent as a minimum to success in the market.
Carolyn: if I want to be able to be unsuccessful in my market I should have the right to do so. (Jim Schuessler agrees) Believe that the minimum should be clear. Some PHYs can give a physical level of security closer to a wire.
Rifaat: if I am building a network and I want to run in the clear can I do it? (people say yes) Can I have a more secure implementation (again, yes).
Dave: you can't be guaranteed of any level but clear.
Carolyn: doesn't think the last bullet of the text belongs there. It effectively closes one issue and opens another.

Close with following bullet text:

- yes (one is "none, see below for other(s))
- The minimal required is "in the clear".
- Additionally, 802.11 will request the list of standardized algorithms from 802.10 and examine them to see if there is one 802.11 also wishes to include in the minimal supported set (or offer one of our own to 802.10 for "numbering" should we decide to do so).
- After reviewing the 802.10 algorithm information, we must answer the issue: Shall we expand the minimal security algorithm set to include a privacy "equivalent" to wired LANs?

Vote: 12, 0, 3

Meeting adjourned: 5:25 PM.

Thursday, May 13, 1993

Meeting called to order at 8:35 AM, by chairman Dave Bagby. Carolyn Heide secretary.

General Business

(1) New issue -

Can we say that in the case of the presence of an STA acting as an AP, it always contains the Point CF if a Point CF is present?

Chandos Rypinski: if "one or more" AP - PCF should be available from all of them.
A discussion ensued about whether more than one of the APs should have the PCF, and whether there should be more than one AP allowed in a PCF..
François Simon: this is about the relationship between a CF and AP - why is there any association between them?
Dave: Monday the discussion was "yes, you can separate them but why would you want to".
Chan: motivated originally by the desire to incorporate a PCF in one of an autonomous group of portables. Number and position of APs must be to provide service.
Bob Rosenbaum: during Carolyn's presentation on Monday logical separation of PCF and AP was brought up. Don't see any reason to force combining them.
Jim Schuessler: previously we had thought that putting the PCF in the AP was a simplification without precluding anything. Perhaps we should not force anyone to do this.
Dave: hearing sentiment that a strong statement on this is not desired.

Chairman Dave wants to discuss the plan for the rest of the morning. The PHY group will probably be finished in an hour or so, so full working group could be started any time (after Dave has had time to prepare for it). A general survey says that most people will be out of here about 3 or 4 PM to catch planes. So the full working group should be at 1 PM, so Dave wants to stop this meeting at 11 AM so that he gets time to prepare and eat lunch too for a change.

Dave notes that one paper submitted has still not been presented. That is 93/58 Alternatives & Arguments on Some Issues by Carolyn Heide. She says this paper was motivated by going through the issues log looking for issues addressed by the CODIAC protocol proposal, and when she saw other issues about which she had something to say she jotted it down knowing that issues discussion was on the objectives for this meeting. Since we didn't get to that the paper does not necessarily need presenting.

François: if people want an issue argument to be recorded in the log refer to the issue by number or point it out as a new issue.

Jim: was hoping for some kind of a straw poll on combining DCF and PCF. Dave, will/may we get to that?
Wim Diepstraten: why not go through our issues process as we traditionally do for opening and closing issues at the end of the meeting?
Dave: wanted to spend a lot more time doing that this meeting, is concerned that we do not spend enough time doing that. Had wanted to split into groups and talk about issues but we wound up with too many submissions.
Wim: a lot of new things came up this week, but traditionally Thursday morning is issue processing. phy finished early doesn't mean we have to be.

(2) Intellectual property disclosure

Whether to take to the full working group the motion: That 802.11 formally adopt the policy that any current and/or future submissions which contain techniques covered by intellectual property law, be so identified in good faith to 802.11 (current submissions to be identified before the end of the July 1993 meeting).

Kerry Lynn: in favor, but is it in line with IEEE policy?
Dave: we just need to know if there is no problem adopting it.
Bob R: the last statement about taking any action if non-disclosure is problematic - if they don't disclose it how do we know it. Circular problem.
Dave: problem of how much will people tell versus how devious do they want to be. Don't believe in contracts that have no enforcement clause (personal opinion).
Bryan Hartlen: something else needs to go in there - before I vote on something not only do I need to know if its patented/copyrighted I want to how much it is going to cost me.
Dave: what you need is the disclosure. Don't want to tell submitters that they have to bring a contract with them. ANSI uses the term 'fair and equitable', which does not necessarily mean free. Disclosure will bring that information out - if people are asking it will get worked out.
KS Natarajan: will you clarify the IEEE policy?
Dave: I don't know that information, if we bring this to the working group we can ask then
Bob R: in the past ideas have been presented without intellectual property coverage and other companies have wound up using them.
Rick White: concerned about case where people disclose the information and there may not be a patent issue but they might have applied. Once disclosed it is no longer patent-able in some countries. In USA you have one year. Why couldn't the committee have a copy of that filing or patent to determine what is or is not covered?
Frank Koperda: but there is a 2 year moratorium on the information. Even if you filed the patent office doesn't allow it to go into the search record or to competitors. That's why it's a good faith effort to make people aware of what you're doing.
Dave: the submitter has a business decision to make, certainly.
Chan: thinks this should be requirement for anything that might be adopted, but there are things I would be reluctant to disclose if there was no potential of adoption.
Dave: yes Chan, but that is a business decision you must make. Doing the disclosure after the decision has been made to adopt something is not acceptable because that decision to adopt is affected by that information.
Frank: since it's in good faith and we just talked about circumstances when you can't, the last part taking action needs to be removed.
Greg Ennis: why does this committee need something different from 802?
Nat: we need to understand the 802 standards first.
Frank: IEEE and ANSI are the same - generic - if there is something, try to disclose it. If you agree to license on a fair and equitable basis. That's why I have a problem with the last sentence. (sec note: which was "and that failure to disclose intellectual property rights will results in submissions being removed from considered by 802.11")
Greg: whatever 802 rules exist that's something that has been developed legally. We won't come up with wording that is as legally clear (which is an oxymoron!).

Dave: doesn't believe we are constrained to do exactly the 802 rules, but rather not do anything in conflict with them.
Phil Belanger: why do we need more than the 802 rules? The ground rules for 802 participation are well known and that is enough.
Dave: reflecting a strong sentiment in the group.
Leon Scaldeferri: I don't know what 802 says, and for all I know this is the 802 position. Bringing this statement forward serves to have someone tell us.
Chan: we are governed by the 802 policy and it isn't possible to take any other course. What is now on the table is getting to know what we are eventually entitled to know a bit earlier. Are we politely requesting sooner release of information? That's all we can do.
Kerry: what if we require people to say things are not protected. The second bullet must be removed.
Dave removes it.
Jim: agrees with Leon, it should be brought forward. It will cause debate in the working group meeting this afternoon - bring it up there and let's move on.

Vote for MAC group to bring this up in plenary: 19,1,0

(3) Enough MAC Proposals?

Propose: That the MAC group stop accepting *new* MAC protocol submissions at the end of the July 1993 meeting, after that time it will take a simple majority vote of the MAC group (voting members) to consider a new protocol approach.

There has been discussion, informal, about when do we expect to stop accepting new MAC proposals. The response so far has been no concept yet. When we said May was going to be comparison month some people got motivated to crawl out of the woodwork. How long do we want to allow this to go on? At some point we have to draw this to a close and accept modification, improvements but not complete extreme new proposals.

We are getting to a common theme with very different details. There has been discussion about combining features of protocols and companies getting together.

Kerry: relax the time frame a bit because of companies not here today that don't get this information for a while. Or companies that have intellectual property things that can't be worked out by July. Suggests September instead.
Bob R: we went through this a year ago. July of last year was supposed to be the cut off. What happened to that (everyone says the motion for that failed). The group hasn't been inhibited to date by newer proposals. Assimilation of what goes on here may have brought out some of the new proposals, is that something we wish to stop?
Ken: may have a biased point of view. Believes we are beginning to see the common trends. Something amazingly new may not happen any more, but a deadline brings out clever ideas often so let's set a deadline.
Chan: first, I made that motion last year, so I still support it. But what's workable? All we can do is - if someone comes in later the hurdle is higher. It should keep getting higher, but we can't just say no. Next - we have enough pieces on the table that what we end up with is negotiable (i.e. compromise). We should view this as marking the time when we stop defended protocols and start making modifications.
Frédéric: 1 if we go with a deadline are we breaking any 802 rules? (Dave thinks this is not a problem) 2. can we clearly identify what is a new proposal or what is in fact a combination of existing ideas - or a basically existing MAC with new parts.
Dave: what I would like to accomplish with this - I know a couple of companies that have said they would like to come forward but they're not ready. Creating a deadline should motivate people to get going. Making our schedule to meet contributors is not acceptable. We have been doing this for years now. The deadline is not short with respect to that, and we have to get on with our work. We get about a 6 hours day work done at meetings, and a very large % of a meeting goes to a new protocol presentation, cutting into our time. We can't afford the time much longer. The point of people not here - it will be in the minutes which go out quickly after each meeting, and if they're not paying attention or attending meetings, too bad.

Ning: has seen enough protocols but not enough simulations, particularly by third parties. Different proposals allow compromise. A really new idea we don't want to miss. Based on current proposals we can come to a compromise solution.
Jim: like to speak in agreement with this. It encourages compromise, submissions will be forced to look like compromises on old ones. It also sends out a message.
Leon: supports this idea. But supports September - people won't get the minutes for at least a month. It's not irrevocable. We can just as easily change our minds. Stop the perception of open forever. We would like to publish a standard some time.
Tom B: we (Spectrix) only got ours done for this meeting because we perceived this as the last chance. So a deadline does create action.
Kerry: restates argument for September. Even if I started the process now I would not be ready for July (Apple).
Nat: could we get an idea of who might be bringing new proposals - we see 2, and Dave knows a 3rd, and Bob C makes it 4.
Dave: why did attendance at the PHY group pick up this month? Because last time they said this was the end of submissions for DSSS and FH proposals. Sees Kerry's, but that's not my problem. Setting the deadline for a company's legal problems is not my problem. Apple has been pushed many times before this meeting, at least 2 to 3 months ago. (Just using Apple as an example, not a personal admonishment). Tactical games are being played, using other protocols to help identify flaws before submission.
Ken: 1. supports Chan. 2. proposes accept all at July, after that require a positive vote to consider new proposals. On the subject of short notice - you have had 2.5 years notice. If they're not here at this minute to hear this warning - tough. If they are not active participant I have no sympathy for them.
Phil: supports July with the Chan/Ken caveat. There is always the ability for someone to come and convince us to listen to their major new work.

Straw poll: no limit - 0, escape clause - a lot, July - 12, Sept 7.

Marvin Sojka: could make free in July, 25% vote in Sept, 50% after that.
Dave: might have write another standard just for the algorithm.

There was discussion of the percentage required. There was discussion of whether majority means voting members or people in the room at the time of the vote. Consensus was at the time of the vote, and in the back of the room there was creation of a company called "votes-r-us".

Greg: how do you get people to do this vote?
Dave: mail out your submission, or give a brief introduction - we are trying to save our time at the meeting.

Formal vote on July versus Sept. Sept - 6, July - 13.

Vote that the paragraph should be taken to the plenary for ratification: 19, 2, 2

Several people have asked for straw polls about compromise, etc. But asks for patience from the group because company representatives here may not be able to commit off the cuff, so let's not put them on the spot.

(4) Review report to be made to the Full Working Group

We did.

Straightening out, clarifying criteria: Carolyn Heide, Dr. Natarajan and Phil Belanger would help Dave Bagby do this on an ad hoc basis. Nat suggests priorities, weighting would be useful on the criteria, Dave counters that his priorities might be different than others.

Meeting adjourned: 11 AM.