Tentative MAC Minutes
Monday AM, January 11, 1993

The meeting was called to order by chairman Dave Bagby at 10:30 AM. Carolyn Heide secretary.

Last meeting recap - DS discussion in general, and what services are provided. We talked about broad categories of services. We voted on a lot of issues, and can close them this time probably.

DS Services Transactions, IEEE P802.11-93/09, by David Bagby

This paper addresses what information flow is required to perform distribution system (DS) services. It presents the logical concept of a thing to used to transfer information.

Tom Siep: the legal concept of transaction is comprised of a two way exchange of information.
Dave B: transaction does not necessarily mean 2 way here.

Wim Diepstraten: what do you mean by link in slide 6?
Dave B: nothing in particular - just the two people exchanging information. Talking about authenticating a station (STA), not a user.
Wim: is this needed among all the end to end STAs or at the basic service (BS) level. What's the link - access point (AP) to STA?
Dave B: STA to AP, yes - a wireless segment.

We can't mandate any particular authentication scheme, need to support simple and highly secure systems - some scheme which selects among various levels is required. A challenge/response based transaction sequence can be used to handle this. The details of that will be presented in a later presentation this week. Slide 8 shows an overview of these steps. Slide 10 shows examples of various levels of complexity for use of those steps.

Leon Scaldeferri: 802.10 - above the MAC level there is a sublevel that provides these services.
Dave B: that is one of the systems you could agree to use.

The same approach is taken to the privacy issue. Bit encryption has a bunch of difficult issues, and may concern PHY implementation.

Tom Tsoulogiannis: privacy between STA and AP only?
Dave B: not really sure. It is needed STA to AP, because all existing wired networks have security - physical location. That wired level of security has been degraded by wireless. You may in addition need security end to end. That's a broader issuer, perhaps outside of our realm.
Phil Belanger: between the STA and AP is the only thing that's our concern - end to end is a higher level. We have to overcome our link weakness and no more.
Tom T: then you don't need to add anything additional to existing.
Dave B: you do because we have lost a physical level of security that use to be there. We need to replace that. If you go from an STA to an AP and through other AP and an STA and back - we are providing DS services, we must keep up the services AP to AP. It becomes another concept when you go out a portal into a wired system.
Wim: why would you think you need more than wired systems?
Dave B: for a very secure network, where all traffic is encrypted to the recipient, that request needs to be given to the other parties involved ...
Wim: that is end to end, a different level.
Ken Biba: that's an 802.10 problem, beyond our scope.
Dave B: a custom DS may have additional capabilities you want others to invoke. Would like to allow it , at least not preclude it.

Tom T: whether this is part of the MAC or just above the MAC, it is a node that is communicating - couldn't this be an option in the driver rather than in the MAC itself? Implementation-wise this is how would I do this. How would I make it unique?
Dave B: that's a key crypto system - same hardware but set differently for each equipment. The later presentation will cover that.
Leon: has been working on a secure architecture system for the government. This is a peer to peer MAC issue. You can carry that higher in the layers. The layered architecture (for a digital cellular to PSTN) provides a layering protocol to overlay security. At the application layer it overlays and this becomes transparent to lower layers.
Ken: we are restricted to a small part of the problem - one hop at the MAC to MAC layer. We can't rely on 802.10 or anything being there, so we need something.
Dave B: sounds like we're trying to invent a scheme. Would rather talk about this system of selecting a scheme rather than mandating one.
Ken: what do you mean by dynamic on slide 11 - what time bounds?
Dave B: STA and AP agree on it until they agree to change it. How often? It could be a bit in a header for every message, or it could take a sequence of messages to agree on it. Maybe some series of data may need a different level, but it would probably not change too frequently.
Ken: sometime during my STA to AP discussion I need some level of privacy - also of authentication?
Dave B: the difference I see is that "I" the MAC level probably didn't make this decision to change privacy level, some layer above me commanded me to try to change.
Tom T: we may not let them, so what then? Why have them tell the MAC to do it?
Dave B: I don't know.
Ken: we can't build the best privacy service here. We can: (1) do nothing; (2) do as much as a wire; or, (3) be flexible, selectable. An open ended system is needed that begins to look a lot like 802.10. Our goal might be to make it look as much like a wire in terms of security as possible. We don't want to get into the 'black hole' of mechanism definition.
Dave B: we are talking about authentication of the device, not the user - once it's established it doesn't change. The strength of that id is dependent on the authentication scheme.
Ken: the strength of the privacy system is directly coupled to the strength of the authentication system. If there are various levels of privacy then there must be various levels of authentication. That's what 802.10 does, in essence.
Tom T: but you can't get access to a wire.
Ken: you can listen to a wire if you want - they make great antenna. Do we have to do more - if we have some simple privacy method we will be much more secure than most wires.
Dave B: are you securing your payload or its destination, etc. - encrypting addresses and such? Personally feels only payload.
Phil: also once you scramble the header no negotiation is possible.
Tom S: if only payload, then it is a higher level.
Dave B: scrambling and spreading come to mind.
Wim: let's focus on what we are trying to accomplish and that is not end to end, but STA to AP - why would that need to be changed dynamically (Ken and Tom T. agree).

Question: is STA to AP the scope of privacy? 10 - yes, 0 - no.

Ken: sense is wireless service needs the level of security of a wire.
Tom T: should mandate at least one privacy scheme - provision for multiple, but one mandatory.
Dave B: we decided no options at the last meeting.
Tom T: this can't be left to the user - when you ask the question you must be able to understand the answer.
Leon: decisions made at the PHY level influence this - digital cellular TDMA and CDMA provide levels they consider equivalent to a wire. A field is provided in level to level headers that allow negotiation of security at higher levels. PHY can provide some level of physical

security, STA to STA base level. Don't want too many options there because there are many provided at the 802.10 level.
Dave B: seems to hear two levels favored - none and equivalent to a wire.

Back to the logical transaction level discussion at slide 13. Association and authentication are NOT the same things. An STA is associated with at most one AP, but could be authenticated to many APs. The DS has to know one AP to which to forward messages for an sta. An AP can be associated with many STAs at once, and authenticated with many STAs at once.

Wim: an AP must authenticate itself to an STA?
Dave B: authentication authenticates each end to the other. Not just one way.
Leon: an AP is an sta. One of its differences to an STA is it can associate with more that one other sta.
Dave B: what lives in the DS and what in the AP is a large issue. For functionality we must know the current association so things can be routed in the DS.

On slide 15 there are 4 states. The actual existence of state 3 is questionable.

Ken: state 3 should be illegal, and there is a null authentication scheme.
Dave B: agrees. Associations must be made because the DS needs to figure out what AP to give things to get them to an sta.
Sarosh Vesuna: need a state where you are associated and not authenticated because association is AP to sta. You can associate without any major transactions. The AP needs to know association only.
Dave B: if association without authentication, then a security hole exists - anyone can plug into your network.
Sarosh: talking to an AP does not mean talking to the network.

Slide 16, moving on to explanation by example.

Ken: association semantics imply that the forwarding mechanism for moving MSDUs in the DS is in place. The AP is an agent for the DS. Forwarding can take place within the DS once association is in place.
Tom T: if the DS doesn't need to know the association, then you have to authenticate before the AP will allow data to flow into the DS.
Dave B: you can't make a DS work without knowing associations. You can't deliver MSDUs within the DS without this knowledge.
Ken: access control is the purpose of authentication. Association facilitates routing within the DS.
Dave B: authentication is not the mechanism by which you become associated - it is enables association to take place.

This discussion seems to make state 3 on slide 15 an illegal state.

Wim: is authentication needed every time you want to use the network, or more off-line like registration?
Dave B: presuming that authentication is an expensive process, do you have to re-do it when changing APs? This is related to re-association. An STA can be authenticated with many APs. Do I have to re-authenticate with an AP every time I move - the overhead can be avoided, or a least the two steps can be de coupled in time.
Wim: when authenticated with one AP, also with entire ES?
Dave B: not necessarily. It may not be necessary to do that instantly, at the time of the first authentication.
Wim: once authenticated to the system, going form one AP to another requires re-association but not re-authentication?

Dave B: yes. The first authentication authenticates with all, or re-authentication could be required - both can be supported.
Phil: AP to AP conversation can accomplish dis-association. The STA uses the DS to tell the old AP that dis-association has occurred.
Wim: one assumption is that you can only be associated with one AP. Then re-association to another AP automatically removes the old association.

This is like file move, copy and delete. You really only have to have copy and delete to do move. how automatic this is to all pieces of the system is another story.

Slide 19. Have presumed so far that the STA has some mechanism to determine that an AP is there.

Phil: this can force a beacon driven protocol.
Tom T: what if you ask and you're not authorized to ask?
Ken: more information is required to become authenticated than to determine the presence of an AP. Eventually, when time based services are considered, beacons are going to be desirable.

Duplicates may be received at several APs when an STA sends a message. Dave assumes filtering at the receive point - only the associated AP pays attention to the messages from that STA, the others ignore them. Duplicates could be filtered at the destination AP, this would be transparent at the other end. If an AP is an interface to the DS, conceptually inside the DS you want to transfer one message, so keeping the filtering in the receiving (or DS entering) AP keeps it out of the DS.

Ken: if the entering AP does not do the filtering, then you don't need association.
Dave B: you need association to decide what is the destination AP to get to an sta.
Ken: could send it to all of them.
Dave B: that develops a broadcast system and Dave believes we previously decided not to do that.

The entering AP needs to find out what AP to send the message to, to get the message to the destination sta. Unless you go to the system where everybody always gets everything. Now you can get that message delivered to the output point of the DS without association. If the routing is no good anymore - you get the message to its destination AP and the STA is no longer associated with that AP - this must be handled.

Ken: don't force an informal requirement to limit quality of service in this delivery scheme. Why not just drop it on the ground if the guy isn't there anymore? Bump it up to a higher level to handle.
Dave B: if designing a DS to handle these things, the DS must know associations to do routing.
Ken: getting involved with delivering no duplicates, and the reliability of delivery are assigning implicit constraints on the service to be provided.
Dave B: the destination AP could receive multiple copies of the message and send all of them to the sta. However, we have discussed that the DS is likely to be built out of what the user already has - some wired network. Most of these don't like multiple copies, so filtering first is why this way was chosen. How to decide what AP is the destination is why we need association.
Ken: quality of service between source STA and destination STA - you are talking about re-transmission by the entering AP.
Dave B: is not trying to imply guaranteed delivery, but trying to avoid just falling back on higher layers because it may happen a lot.
Ken: have we defined lost packet quality and service level? (no) suggests that quality of service and best effort delivery definitions are essential.
Wim: the reliability requirement is implied by the LLC services delivery definition within 802.
Ken: there is no upper bound there.

Wim: we know we have to do something extra to maintain up to wired reliability - going beyond that point is not interesting. Higher levels will be using these MAC services the way they are used to using them.
Ken: explicitly stating those is a useful exercise.
Wim: at the implementation level - is some ack required for success of STA to AP - a segment ack? Or do we have an end to end ack, STA to STA?
Dave B: if you just give up, and the destination STA is not at the destination AP anymore, that's OK. Some DSs could give up and others not - the upper levels can recover from it one way or another. But it would be nice if the DS could be somewhat robust in that area. It increases the probability of success. The higher level could take you through the same procedure if you leave the responsibility to it, so this could just make it more efficient.
Tom T: if you try too hard the higher level cause you to have you having duplicates running around trying to get delivered.
Dave B: you have to give the DS enough information to figure out how to deliver something.
Ken: the probability of undelivered messages requirement determines how to do this.
François Simon: AP to AP communication implies that you have some kind of routing protocol between APs. That protocol is at the MAC layer?
Dave B: assuming that from the intended recipient the DS has to derive what output AP to use. The DS involves some routing. 802.11 shouldn't say anything about routing or not. If I just give all messages to all APs, it would still work.
François: DS implies routing protocol, I agree, but the movement of STAs makes it different from currently existing DSs. Routing protocol will have to account for the fact that this is wireless - existing routing protocols on the DS can't be applied directly to wireless LAN output. There is implication that 802.11 will have to deal with higher layers than MAC because of the DSS.
Dave B: not relevant to 802.11. If the DS is existing Ethernet routing protocols and I choose to use them, they may or may not be sufficient. How you route from input to output is interesting, but not 802.11 . we just require it be there.
Chandos Rypinski: it will turn out that multiple copies must exist because overlap will be required to get coverage. We don't have to put that in the standard, but not preclude it also. Each AP shall have the responsibility to decide upon the deliver ability of the message received.
Ken: we are defining a set of interface functions of the DS. Formal part of the standard or not, one part of the standard must show how you get there with existing systems. Some routing functions will have to be invented. The DS destination database will define how fast you can roam, the range of cells, etc. - we have to show that embedded within our MAC we can build such systems.
Dave B: predicated that the DS will be built out of existing well known network. If the DS performs badly, then roaming speed is effected. Time-bounded-services (TDS) will be affected by existing networks also. If you know the functions that the DS must provide you, you can evaluate if a DS is the right one to use for the system you want to build, even though all of them meet the standard.
Ken: performance levels are part of the functionality.
Dave B: if you can't do it, it doesn't matter how fast you can't do it.
Jim: the DS destination is now a routing function, but you said we aren't dealing with routing?
Dave B: it tells me where I'm delivering something, not how.
Jim: OK, but that's above the MAC. We have to provide hooks for that, but trying to define the DS would be biting of more than we can chew.
Dave B: this need to know the destination within the DS only is a justification of why we need association. Not trying do define it.
Ning Kong: the DS is a higher layer of infrastructure. We need something to support the routing function. Id, station number, is needed to support routing, or infrastructure. In the MAC we need a DS that supports the function, but we don't need to do it.

Dave B: remember the DS may be custom and the wireless may be IR - we are trying to stay out of the details and in concept.
Tom T: what is the MAC supposed to do as far as association is concerned and how does that information get transferred to the DS?
Dave B: when the association is created the DS gets a piece of information it needs.
Tom T: how do we put that into the standard - how does that affect the standard?
Dave B: don't know.
Tom T: isn't there a bias to a particular implementation here? Why not just tell us what you want and let us evaluate it.
Dave B: am trying to talk about what you need to consider in the abstraction - the core building blocks. Thinks that you have to have association as a concept to be able to get things from the input to the output of the DS.
Rifaat Dayem: simplistic approach - AP is a MAC level bridge according to 802.1 and does source routing and MAC level bridging. Now, wireless needs to do some special things on top of that. Take the 802.1 body of knowledge and see what we need to modify. At least we would start with a body of knowledge.
Dave B: wants to allow that, but not restrict us to that only. Believes we discussed and decided that previously.
Tom S: DS destination gets worked out for every transaction or there a virtual connection?
Dave B: probably answered every time the DS is invoked, but not for every transaction and not a virtual circuit.
Leon: an STA is associated with only one AP at an instant, and there is a way to dis-associate and re-associate. The DS is made aware of the association of STA and AP - there are many ways that could be done. Broadcast or specific or a central switch - doesn't matter which is used to pass data. the concept of associating an AP and an STA allows the DS to be almost anything. From a reliability stand point when STAs move there must a mechanism that does that efficiently and reliably, but that is different from just the concept of association and DS being aware of that and using that. There is no restriction on those things from this concept, and does not design the DS.
Wim: why association is needed is no issue at all. We are struggling with - we need a better model of the AP. Where functions exist and where the interfaces are is confusing. We need to develop an AP model and check it against the concepts so far.
Dave B: could take examples of DS (say central switch, existing LAN and single wire), and show that this model supports all.

Re-association and re-authentication: if ap1 trusts ap2 then the STA that used to be authenticated with ap2 is authenticated with ap1 when it gets there.

Wim: for authentication of STA to infrastructure this might be true, but what about the other way around? How does an STA know what APs are authenticated for that network?
Dave B: doesn't see the need for an STA to know all APs which it can talk to.
Tom S: security hole created if they don't?
Dave B: depends on the authentication scheme used. Open system doesn't care. In a public key crypto system it's not an issue. If all links of the chain are secure, then the whole chain is.

Slides 29, 30. STA uses DS to get authentication with all APs it can hear, if it wants. Given that authentication might be expensive, you can move it out of time critical positions.

Ning: telephone network - you go to another area you need authorization. How can we re-associate without re-authentication by a third party. Local conditions at AP must be considered. Re-association and re-authentication is not really "re" - you associated once, you moved, you associate again.

Dave B: instead of doing it again, if you hear the second AP you tell your first AP, "associate me with him too so that I don't have the authenticate with him should I ever go there". Not required, but could possibly be useful.
Jim: why have authentication limited to APs you can hear - why not authenticate with entire infrastructure, entire DS?
Dave B: no problem, the set you want to authenticate with is OK, but it can get expensive - this may be seen in the forth coming presentation on public key systems.
Phil: if the DS is one big trusted system then it is many to one not many to many.
Dave B: you may not be authorized to talk to all APs and STAs, but the AP may be able to route for you.
Phil: DS is the set of APs and portals, or the thing that connects them. Does the STA ask the AP or the DS to do authentication with other APs?
Dave B: the APs are a good place to do some of this functionality.
Phil: the set of APs is the DS and it doesn't matter how they are connected only that they can be. That set of APs can then be considered one trusted entity and you only have the authenticate once.
Dave B: don't know if it's desirable, is there any down side?
Tom T: an AP could be reserved for certain high priority users due to limited bandwidth scenario. An STA may not be wanted in all AP coverage zones.
Unidentified: STA hearing other APs - you are assuming a lot of cell overlap. This usually is just on the boundary.
Dave B: prevailing feeling is there will be a lot of overlap, but if you didn't hear another one then you wouldn't request authentication on another one. There is no conflict.

Slide 31, then 33 and 34 discuss re-association.

Ken: says that any association kills any old association.
Phil: APs may wish to re-associate STAs - having an AP initiate a dis-association accomplishes this. Then the STA is forced to re-associate. The AP can only know that dis-association is required, not which AP the STA should re-associate with. The STA then associates, not re-associates.
Wim: agrees, only the STA knows.
Chan: disagrees. The STA is desired to be simple. The STA cannot judge the quality of signals - it receives. To trigger an event by inadequacy is too late. The DS at all times should know the relative quality of the signal from an STA, and should know which AP an STA should use. The STA should never have the intelligence to do this sort of thing - it will simply use the AP it is directed to use.
Jim: re-association transaction is to complex, association and dis-association can used (ala Phil and Wim). Re-association is efficiency at the cost of complexity, not simple and elegant.
Dave B: push vs pull model of re-association initiation. You could say that only the STA knows the signal quality at the sta. Either way Doesn't break anything - so why not bi-directional? There is information both ends have exclusively.
Tom T: re-association could just be a modified association with more information for the AP to do the dis-association at the old AP. Bi-direction just means that you're just not saying anything - you can't have it both ways. Tom thinks the STA should initiate re-association.
Tom S: system is broken if you get into an endless argument between AP and STA over this. Someone must be in control.

Vote on choices on line 1 of slide 34: from STA to AP = 9; from AP to STA = 3; bi-directional = 5.

Carolyn Heide: must be bi-directional because it can be needed from both ways. there are times when the AP needs to tell the STA to get lost and go associate with another AP.

Phil: dis-association initiated by AP is OK, but not re-association - AP should not order STA to associate with another AP. Can accomplish that with dis-association from the AP, then letting the STA associate with some new AP.
Chan: the DS can have the information to make the re-association assignment. Only the DS has knowledge of what is going on in the entire system.
Tom T: it is the MAC doing the association and authentication, the STA and AP MAC are different.
Leon: we are talking about who can initiate a request for re-association. Both should be able to initiate the change, it has to be negotiated between the two.
Dave B: was thinking in terms of who can initiate it. If you make such a request can it be refused?
Ken: assumed that dis-association from AP is OK, that forces re-association. Assumed 3 transactions: association, dis-association, re-association. Under that assumption an AP can cause re-association by dis-associating all it's sta.
Phil: under that definition agrees.
Dave B: association is a request which may or may be successful. Re-association is either a request or a command, and that maybe depends on the direction.
Ken: a re-association command emitted from an AP that says "STA go re-associate with another AP" can be simulated by AP dis-associating, then all the STAs associate again.
Dave B: if you do that, you now cannot get data to those STAs, so they will establish an association somewhere and once done that's OK. But in between you can't do anything, but if you had a re-associate command you can know where they're going and fix things up nicely.
Phil: if allowed it would be possible for the new APs to reject and failure occur, and the meaning is lost. Forcing a dis-association could break the thing it has control over.
Ken: re-association command has STA, old AP and new AP information is implied. In the time of this re-association maybe the information has changed.
Tom S: how is bi-directional defined now?
Ken: what we thought of as uni-directional can be used to achieve bi-directional.
Bill Stevens: does bi-directional mean that you cannot build a system that supports only one way? What are the options?
Dave B: last meeting we decided to avoid options, but that is another discussion.
Tom T: is the question who initiates, or who decides the destination of the re-association.
Ning: association and dis-association - if we can do without re-association then bi-direction is not an issue.

Same vote as before (9,2,4)

Who believes there should only be dis-association, association =12; those plus re-association = 4. Dave thinks that people like the simplicity of only the first.

Wim: is it sufficient? In the DS you must update all the routing tables and functions. Re-association action becomes different from association.
Dave B: information is lost by having just 2 commands. Can accomplish the function with the two, but there is less information in the pair than in doing this as one operation. The intent is to move rather than make go away. The overhead and updating may be different.
Phil: the association primitive can have the 3 parameters in it then there are only 2 commands needed. associate(new AP, old AP, STA). If the 'new AP' is null, then it is just an association, if both are there it is a re-association.
Dave B: the information I was afraid of loosing can be inferred from the parameters?
Ken: the association command should only have one parameter. If the new AP is not equal to current then this is obviously a re-association. Any AP can determine what the current AP is for any sta. If you associate, your new AP can dis-associate for you.
Dave B: since you have to have the information in the AP, why have it in the STA too.

Tom T: there are situations when the AP doesn't know the old AP, so it should be in the command.
Ken: the AP cannot do its function if it doesn't know that.
Tom T: the more general case is to leave it in. All implementations are covered by this.
Ken: leaving the parameter in doesn't affect anything.

Dave suggests people should think about this so we can come back to it later.

Ken: we need to see a description of the set of primitives between the AP and DS.

These things stay as firmly undecided. On to slide 35.

Wim: what does "integration service" transactions mean?
Dave B: data going from an AP to a portal.

Last but not least, the summary slide.

Jim: how can a MAC protocol be evaluated based on this? Aren't all presentations equal on these services?
Dave B: we got too detailed in our evaluation of protocols previously, these are more general criteria.
Jim: this is not THE way to evaluate, but it would help.
Dave B: if we have a better defined set of functions that must be done, it might be easier for protocol proposers to aim their presentation.

General Discussion

Wim: a better model is required for the AP. Where is the DS boundary and how is an AP different from an STA? That is not clear based on last meetings' discussion and today's too. This AM the filtering function implementation, for instance - source or destination AP doing that function makes a big difference. What functions reside where? A layered architecture model for an AP, where functions reside, is required.
Dave B: not something that can be done on the fly in this group now. This is an area to say we should have it on the agenda for the next meeting. To see if an AP model can be made that meets the implementations people have in mind. APs physically probably contain a little piece of hardware, but logically they are the edge of the DS - what pieces of information go across that line? To answer that you need to know where information lives. It could be centralized or distributed. The only common thing is to identify the questions to be answered.
Tom T: are these functions inside of the MAC or higher - relate the functions to a software architecture picture. The key to whether we should discuss anything is 'is it the responsibility of the MAC'.
Dave B: we know that in the ad-hoc case there is a PHY to PHY STA communication. In non ad-hoc the STA PHYs don't communicate to each other. Where functions reside that facilitate that is undefined - a cloud with DS in it?
Leon: the middle of that - do I go back up to the LLC level, or to layer 3 and cross connect there? Depending on where the DS is and how it interfaces that middle could have more layers than the two STAs.
Ken: if we are trying to accomplish STA talks to STA in ignorance of what's between them, we have a layering violation because our MAC has to have someone else's MAC in it. It would be easier to assume AP is a bridge, but 802.1 is in charge of that. And what's a bridge? And can a network be comprised of bridges alone?
Dave B: tunnelling gets involved. You seem to skip layers. It's confusing and hard to draw.
Tom S: why is drawing intermediate stacks in the middle not desirable.

Dave B: it implies that an AP is very smart. Chan would like to have a simple AP and have the intelligence in one box. That's why we said an AP is in interface into a DS, as opposed to a packaged box.
Tom T: but a MAC at the AP is essential.
Tom s: but we're going from MAC to MAC - 2 stacks.
François: AP could be viewed as a relay function.
Alan: STA has one interface to an AP; the AP interfaces to an STA and the DS; and, the DS interfaces to the AP. Why do you need to know more than that? The AP must have those two interfaces.
Chan: urges that the primary property of an AP is an air interface, and all geographic location of all the other things is not yet defined. The layers have to be provided but not in geographic proximity to the antenna.
Dave B: how the intelligence is distributed - why pick only one way? Look to decide what needs to go between functions.
Tom T: but DS destination is not a MAC function?
Dave B: I could do it that way. We said we would have a DS and the interface to it would be exposed. Doesn't know if they live in the MAC.
Wim: we could look at the standard model and see what we need to add.
Dave B: would anyone like to prepare that - no one volunteers, maybe that tells us something.

Meeting adjourned: 5 PM.

Tuesday AM, January 12 1993

Meeting called to order at 10:30 AM, by chairman Dave Bagby. Carolyn Heide secretary.

What are Ad-hoc Wireless LANs, IEEE P802.11-93/03, by K'S Natarajan,
introduced by François Simon

This submission addresses the question which was asked at the last meeting - what is ad-hoc - in Nat's view. It lists important properties of an ad-hoc network, to facilitate communication without relying on infrastructure. Issue 4.1 .François would like Nat to present the paper at the next meeting to address the details. No solution is presented here just a view of ad-hoc.

Wim Diepstraten: doesn't say much about environments. For instance what if there is an infrastructure available? What does that mean for the infrastructure?
François: probably a year ago we discussed this - if an AP is available, should we use it? This goes back to if we are authorized to use the AP. If you're not, you may need to form an ad-hoc in the presence of an infrastructure.
Jim Schuessler: some benign co-existence is required - use different channels, or share bandwidth politely.
Dave B: I think we said if some infrastructure is present, the AP can have some control over when you talk, but you don't use it to communicate.
Carolyn Heide: in our terminology, the ad-hoc network shares the co-ordination function (CF) the AP is using.

General Discussion:

Jim: issue 4.1 is so easy to close maybe we should close it right now with "yes". But open new issues like does the ad-hoc network use an existing CF if one is present.
Dave B: [reads issue 4.1, 92/64 page 4-2]. Is there anyone who would like to say no?
Wim: is there a formal definition of ad-hoc.
François: ad-hoc is not in the definitions document.

Wim: we should know what we are voting about. What are the boundaries of ad-hoc?
Dave B: we could open another issue that is "what is the definition of ad-hoc".
Tom Baumgartner: has a basic concern about the complexity ad-hoc support adds to the MAC.
Chandos Rypinski: is opposed to ad-hoc as the normal operating mode of an STA, but has concluded that ad-hoc support is a marketing necessity. If you start in the other mode then this can become a subset with less stringent requirements. So there may not be cost significance. For the reverse situation where ad-hoc is the only mode, the burden is a little tougher to assess.
François: ad-hoc is a subset as Chan said. There is no additional burden on the implementation.
Dave B:. There has been some consensus that the scenario for ad-hoc is two people walk into the room and want to talk. They are in physical range and it is the same as the basic service area. The complexity added is little or zero, the primary difference is at higher levels. This is why peer to peer is so different - ad-hoc is a transitory basic service set.
Leon Scaldeferri: yesterday we talked about determining AP presence by listening or asking. This falls in there. If you listen and then ask, if you hear nothing then try to start to talk. It could still be done fairly simply.
Dave B: related to determining what APs are around. The who's around query can be used to start the ad-hoc network. If some others are around and they see an AP too it becomes more complex.
Carolyn: doesn't feel that it's necessarily simple. If we choose a deterministic, beacon driven protocol, then every AP has to have (a) the ability to become the beacon generator, or maser, (b) the ability to share or pass around the mastership with other unit; or, (c) fall back to a completely different protocol in the absence of the beacon generator. This can be a substantial amount of complexity added to every sta.
Dave B: aren't an AP and a STA the same functions with respect to air interface.
Carolyn: an AP is an STA, but may be more than that also.
Chan: every STA may have to become a master in an ad-hoc situation, but it may need to be a different kind of master than an AP. Any problem is easy solved if you lower your standard of performance enough.
Ken: in an ad-hoc case you need to be only master of your own fate - what you need to do is co-operate. That is a different case.
Carolyn: yes, but it means you are operating in a different mode than when you are in the non-ad-hoc network. It means all STAs must support two operating mode.
Tom Siep: this has an implication on the deterministic system - interlopers use some of the bandwidth, and the system becomes no linger deterministic.
Ken Biba: the complexity added is not a question of ad-hoc vs infrastructure. Deterministic performance is what introduces complexity into the system. The requirement for time-bounded services forces the deterministic requirement and that is what introduces complexity. It also introduces a wide range of performance constraints. If we build a time-bounded support deterministic system there won't be any existing infrastructure for us to connect too anyway.

Vote on issue 4.1, "will the standard support ad-hoc networks": (21, 0, 0). So detailed protocols proposal must consider this.

Jim: doesn't see a need to open a new issue on this. We have a good definition of ad-hoc, the first three bullet points of document 93/3.
Wim: it doesn't mention that every STA should see each other.
Dave B: could those 3 bullets provide the definition we need?
Greg: questions the use of the term mobile - we don't want to preclude stationary stations.
Dave B: second bullet says peer-to-peer appearance and that is not necessarily true.
Jim: we can improve the words here if our aim of provide a perfect definition of ad-hoc - we can spend a lot of time on that without much value. It is acceptable to me to leave this as somewhat ill-defined.
Wim: in the issue document it says that ad-hoc is not equivalent to peer-to-peer. Within an ad-hoc network would all communication be peer to peer or not or is that irrelevant?

Dave B: the issues document refers to a paper which expresses opinions about that. Peer to peer implies some status between the 2 STA - it could be master-slave and still be ad-hoc. Peer to peer and ad-hoc are different concepts.
Jim: there are some interesting issues to open with respect to ad-hoc network - in an ad-hoc is all communication peer to peer or is it controlled by a CF? That may be an issue.
Dave B: invites papers about ad-hoc issues.
Ken: suggest that peer to peer is a loaded term as it is used in network OS to defined a class of service. In terms of the LLC all networks are peer to peer networks. For topology - how I get messages around, number of hops, etc., this is the wrong terminology.
François: we have an issue open on what is the definition of ad-hoc. Are the 3 bullets of 93/3 paragraph 2 an argument there. [some people say yes]

Dave B: does a line from one PHY directly to another cover ad-hoc?
Ken: a case can be made that ad-hoc will allow some kind of intermediate sta.
Dave B: an ad-hoc BSS network is covered by that line, and an ad-hoc ESS is formed by going more than one PHY hop.
Ken: ad-hoc is a whole lot like a BSA. how are they different?
Phil: then if you have an ESS, you have infrastructure?
Dave B: use of a DS creates an ESS. A wireless repeater could be that ESS - is that still an ad-hoc then? If so, then the repeater came into existence when needed it and isn't that more complex than we need?
Jim: not worthwhile to have ad-hoc ESS. One BSA formation requirement has been a point cf. With that one way to do STA to STA is through the point cf. That is physically 2 hops.
Dave B: a CF says when you should talk, so saying given x CF you have y hops is invalid. Point CF says only the CF lives in one place.
Ken: there are a lot of choices here. I think of ad-hoc as BSA with some kind of single hop. Never find APs in a BSA - they are for building ESAs.
Jim: are you putting together an AP and a CF as one entity?
Ken: it relates to what is an AP. An AP is a widget, distributed or CF, that builds ESAs.
Wim: what about standalone wireless BSA with one connection into the wired network?
Ken: the AP is a bridge (portal to means bridge or router).
Phil Belanger: single BSS one AP, those STA communicate by using that AP. The AP extends the BSS.
Dave B: that's an ESS because your range was extended. [There is general disagreement in the room because you can't have an ESS without another BSS] A long time ago we wanted ad-hoc so that if two of us want to talk we don't want to have to go get a third chunk of anything to be able to talk.
Dave draws the following charts and fills in the following vote counts:

	BSS	ESS
ad-hoc	supported: yes-16, no-1	supported: yes-0, no-10
infrastructure	understand & want to define-4, don't understand & want to define-12, don't understand & don't care-5	supported:yes-16, no-0

Dave B: vote on the bottom left box - there is still a lot of confusion here. If people really care they will make submissions about it. If we get no input we can do no more work.
Phil: I want to know what that bottom left box means.
Ken: it's valuable to discuss if it exists, or is not useful. 2 cases (i.e. top left and bottom right) would be more useful that four.

Chan: in an ESS when one STA needs a repeater to get to another STA, it will be repeated without use of the DS. An AP which receives a message and repeats it need not use the DS. The repeater existence is just semantics, it is inherently a subset of a DSS AP. An autonomous system will work better with a repeater, but I would never make it a requirement.
Bill Stevens: shall we support ad-hoc was how we started this discussion. Then we got into what is an ad-hoc, and from there into the functions of BSS and ESS. Ad-hoc is a mode of behavior exhibited and observed by the users of equipment that is how they desire to use that equipment. On a minute by minute basis ad-hocs are different from others as it needs to be convenient to set up and tear down on a human time scale. It takes s functional description of how we use it to understand if we will need it.
Ken: the notion of how people use the system is a very important aspect. If we brought in infrastructure and tore it down next week this could be called ad-hoc too. It is an issue of ease of use and management. On the opposite poll to that a highly managed and controlled network would be distinguishing.
Mike Bergman: ad-hoc has to do with a priori information about the node in the BSS. If you have that information then it is not ad-hoc. If you don't then it is ad-hoc. In an ad-hoc there is no existing table of nodes that are in there, if you want to add by simply entering range that is ad-hoc.
Dave B: as a user, whether I had to know ahead of time I wanted to set up a network or it was spontaneous is the difference to me. The a priori knowledge doesn't seem as important to me.
Ken: what is the opposite of an ad-hoc network? I have a LAN manager who minimizes down time, and maximizes bandwidth - his criteria is not building network quickly but having best resources and use of them. Different selections are made on the way access control is used, performance and efficiency are judged, amount of network management required - those things may define the polls. In both cases I might want infrastructure - in an ad-hoc, or not.
Phil: a BSS with an AP, but no other BSS on the DS. Is this an ESS?
Wim: an ESS is the connection of BSSs, if the number of BSSs can be one, then its a null issue.
Sarosh Vesuna: in this mornings definition of ad-hoc, it says that the co-ordinating STA may or may not be involved of data transfer, that STA could be your AP. The single AP and STAs, is that an ad-hoc network - by this definition, yes.
Dave B: maybe ad-hoc and infrastructure are not ends of the same scale.

The conclusion is that a lot more exploration of ad-hoc is needed. Everybody think about it and somewhere about mid-morning tomorrow when this meetings submission have been done discussion time will be available to return to these sort of open topics.

Dave's introduction to the following submission: there is a fairly simple sequence of events that if we provide hooks for will make security straight forward. This is a ground floor of what you can do with key encrypto systems. The intent is not to imply that we should embed any of this functionality, what we do need to do is leave the hooks for them. We need to have a common understanding of the concepts for that reason.

Wireless Network Security, IEEE P802.11-93/08, by Whitfield Diffie

This presentation tries to describe some very basic requirements of security implementation and what you have to do to accomplish those requirement.

Discussion:
Jim: if you updated keys and the recipient of old message didn't keep a copy of your old key you couldn't communicate.
Whit: There is no objection to archiving public keys.
Vic: why would you change public keys?
Whit: the key might become compromised. Imagine a copy has been made of the private key - someone can now use that key pretending to be you. You manufacture a new key and use it to

sign a message and send it to the CA. The person who stole my key can't stop me from doing that. The intruder doesn't want to do that himself because then I will notice the intrusion.

There is a trade off in the longer that you keep a key the more risk of comprise you take, but the more often you change it the more expensive overhead you incur.

Cryptography frees you from the length and the direction of the path for security.

Discussion

Jim: does there exist an exportable encryption algorithm the gives a sufficient security level?
Whit: non are published, so how am I supposed to know?

Dave B: the 3-step transaction referenced in my presentation yesterday, slide 14 - If what we do for authentication is provide a way for these 3 steps, then by adjusting the contents of theses steps we can implement any system
Jim: at what layer?
Whit: layer 2.
Wim: does what we have seen specifically address our problem of achieving a certain security level in the wireless segment, or is it end to end?
Whit:same technique for end to end, but a wireless segment is what has been worked on so far. The idea is to do the minimum work necessary to add this feature to the wireless segment.
Colin: if you do security at layers 3 and 4 then it's not necessary at the lower layers.
Whit: many purposes are well achieved with end to end at layer 4. If done end to end, then the equipment cost is proportional to the number of hosts. Everything is fine, but we don't want to disturb the network to add a wireless segment, by having to add functions to all the existing members. Adding the segment added a vulnerability the affected the whole network, but solving this can be isolated to the wireless segment.
Wim: once public key transported for authentication purposes, you could update it whenever you want a new key. But you have to maintain a history?
Whit: if you want to verify old signatures only. You never care about verifying at the time of engaging a conversation - you don't want to verify yesterday's conversation. Only for document validity for a period of time is that relevant. In communications it's not a consideration.
Colin: the certification authority (ca) is present on the wireless segment?
Whit: the ca must be an off-line activity. You can get at it any way, but the response must not be needed in real time.
Colin: this is not present on the wired network?
Whit: it could be, but must not be real time. It is off-line and references the certification directory. Being denied the services of the ca is not critical - registering new users would be the only interrupted service.
Colin: this entity outside of the wireless network that does this service, so it is outside of the scope of what we're doing here.
Dave B: if we have the 3-step transaction, if you want the contents of the steps to use this facility that's fine. In the scope of 802.11 we don't say you have to do this, only that if the steps exist you can use them for this.
François: is this method standardized anywhere?
Dave B: the list of choices must be for the steps to work - if you tell me what services you have I must understand your answer.
François: is this method to be defined by 802.11?
Dave B: I don't know. Maybe this should be done by 802.10, or they already do have them. Only the open system needs to be completely standardized.
Wim: what about a mixed approach - some STA with security and others not?
Dave B: maybe not all APs are the same, so some support an elaborate system and others support only a completely open system. So an STA might only speak to some APs.

Wim: what is the acceptable level of security to obtain the goal - being as secure as a wired network?
Dave B: yesterday there seemed to be sentiment for at least two levels - none, or as good as an existing wired LAN. What the latter is is the remaining question.
Wim: authentication being bi-directional - isn't that implicit when you do this? Do you need these 3 steps, or do you need to do the whole thing the other way to making a total of 6 steps?
Whit: you can put the challenge and response in both directions in theses 3 steps.
Phil: the session key - is that used for the encryption for that session?
Whit: yes.
Dave B: all I want to see from 802.11 is that these 3 steps are included so that we can cover everything from open systems to very secure systems. For authentication, not privacy.

Registration Scenarios for WLAN MAC Protocol, IEEE P802.11-93/02, by François Maut

This presentation provides a certain amount of answer to the security request issued in the NSA presentation this morning. The idea is to provide (1) not having to change the existing LAN to cover security in addition of a wireless LAN; while (2) providing maximum flexibility for users who want various amounts of security.

Discussions:
Wim: how do achieve the network access control to which your refer?
François M: one way is a simple network id.

Wim: authentication masking could be different from station to station? But when you go wireless you create a security problem in your wired network, so you would not want to have it disabled on any stations.
François M: it puts some additional burden on the station so you want to avoid it if you don't need it at the application level. It gives you high flexibility.
Dave B: there must be some minimum level of security - François is saying it is none, Wim is saying it must be some.
François M: but it could be by AP. The AP can allow the stations to run with no security if it knows that is OK. But if it feels that mobiles threaten the network, then it enables security. It allows networks to be configured with maximum suitability for the user.

Dave B: where do you assume encryption is occurring? If it's above the MAC layer, then we don't care. If in the MAC, then I assume it applies only to the payload.
François M: yes, the MAC encrypts and decrypts dynamically, and it can be turned on and off for each mobile to station link.
Dave B: If so, we have to specify encryption and decryption, and we have to pass around the keys. This is difficult and expense.
Colin: isn't that what you implied in the previous presentation?
Dave B: was proposing that a higher layer does it, and we select turning it on and off.

François M: when you change APs you either have transfer the key or compute a new one.
Wim: what do you mean by "key generation and sharing"?
François M: this is a shared key crypto system, both STAs have a copy of the same key. You could have a key per station if you want.
Dave B: anyone who intercepts the key can intercept the traffic too in shared key crypto systems. Dave holds that shared key is sufficient for some situations, but not good enough for us to provide this as our only method. A public key system is better.
Wim: a key per station is too much - it is more than equivalent to a wired LAN.
Dave B: why have you chosen to do registration and then authentication (page 4)?
François M: this is "basic" registration - it really means just being able to communicate. At a PHY level, you have verified that you can move control data between the two parties.

Bill: (1) basic reg is for instance sync'ing with the CF, so you can req authentication. (2) in the absence of data masking how do you protect against someone impersonating an existing authentication STA?
Dave B: that's life. Only signing each individual payload can protect against that.
Wim: when an access control procedure is based on network id that comes first.
François M: that is a different level of access control - there is network id, and you can add more complex procedures such as password if you want.
Bill: all you need to do is listen to a station register, authenticate and get the key, and you can now pretend to be him.
Colin: that's another argument for doing it above the MAC - users will desire varying amounts of security by application.

Dave B: do you perceive shared key crypto as being sufficient?
François M: with this system you have security and flexibility given you are doing this at the MAC/PHY boundary.

Wim: what is the value of authentication if it is done in the clear? After you authenticate anyone can pretend to be you, so why did you bother - providing you don't use data masking.
François M: generally after authentication you would go to encryption.
Leon: after authentication this threat exists. This is, however, a very sophisticated attacker. But the higher levels are going to pick it up because he cannot do it unless you there too.
Dave B: but you can disrupt the network.
Bill: no, it looks as if you, the one station, has opened multiple connections.
Colin: thinks the AP could be designed to realize that this is happening. Besides, if you really want to penetrate a network you can do spend enough money to do that, even wired.

Meeting adjourned: 4:30 PM.

Wednesday AM, January 13 1993

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

Office of Information Security Research, IEEE P802.11-93/10, by Leon Scaldeferri

Discussion:
Wim: you refer to block cipher as DES, but is there not a stream cipher mode also?
Leon: yes, DES has various modes. DES modes also have implications on error handling. In block mode an individual block can be identified as in error rather than the stream mode having the entire stream corrupted.
Chan: what is an order of magnitude for a block length in practice?
Leon: 64 bits in DES, in public key is your choice. NIST standard public key system has 320 bits overhead - 160 bits signature and 160 bits header added to you data. Regardless of the size of your data this gets added.
Wim: a stream of packets that are continuously encrypted - multiple packets in a row? Couldn't you encrypt per packet?
Leon: data may be a stream cipher and for transmission you have broken them up. Yes, you could encrypt on a packet basis. Some of these processes are applied typically at a higher layer. So if you don't exchange your frame boundary information between layers you loose information.
Wim: so you are assuming encryption done at a higher layer?
Leon: yes, but if you are doing it at the layer you are blocking data you could encrypt per block. This information could be used advantageously.

Wim: which system multiplies error less or not at all?
Leon: stream does not multiply errors because cypher is added one bit at a time (Whit called it conventional crypto). You don't use any knowledge of the previous bits to do the encryption. In chained DES you pass the data through the algorithm and take the result and pass it through the algorithm, so once you make an error you are out of sync. There is a DES version where the key generates an encrypted random number and then uses it - given the receiver maintains sync on that.
Wim: public key comes in stream and block mode also?
Leon: message oriented only. Whit touched yesterday on this - exchanging two random numbers in the challenge/response sequence. The AP encrypts a random number and that's the challenge. The STA decrypts, uses it to encrypt and sends it back with his key - if you get your number back you're authenticated. When you have authenticated each other you have been able to exchange 2 random numbers. Then these numbers can be used as the key to the sync process.

In some of the schemes bit or block errors don't cause loss of crypto-sync. Small errors in voice can cause of bit of noise, but are acceptable.

Discussion:
Jim: in digital data where one bit error stops interpolation - are people using block data for that?
Leon: if it's important that you don't go through an ARQ process - you can always do that or provide block error correction to the encipher data if the environment isn't too bad.
Dave B: we want to set up some method for privacy, but there is a level of complexity here that maybe I want to use a different kind of encryption for the time-bounded path.
Leon: if you did encrypt in MAC or PHY then it probably doesn't matter whether it's time-bounded data or not. How much delay does the process put in is what would be important. For a block mode cipher you have to collect the entire block, so you introduce a delay. The public key systems work on the fly, the message digest and signature are built while the data is being transmitted and then are transmitted after it.

Even giving levels above the MAC a block of data that is wrong is better than just skipping it. The higher level may be able to keep crypto-sync using that. You must not delete pieces of data or add data unknown to the upper layer, it will loose crypto-sync.

Wim: you see that as a MAC function?
Leon: if you are transferring data from an application that previously ran on some other media that did not give duplicates, you want to replicate that service.
Wim: a sync MAC can generate dummies, but in for an async isn't that a function of the LLC? The MAC has no knowledge of what data was expected.
Leon: agreed. The use of a super-frame MAC scheme may facilitate some small frame count mechanism. For overlap and handoff it may turn out to be necessary anyway.
Ken: how expensive is re-sync on frame loss?
Leon: depends on the application, but it could take seconds. You want to assess the probability of it happening, and if it is likely then you want to take steps to avoid it. That would be a parameter of quality of service (QOS).
Ken: also what threats we are guarding against needs to be considered when choosing the method. In a system like Ethernet where the MAC has no responsibility of integrity, about the only thing you could implement is a block cipher.
Leon: some advantage would be gained by having no dependency on previous data. Any frame can be decrypted because it is bounded by the frame. You could use stream or block within the frame. Part of the QOS required by the application would specify the probability of loosing bit count integrity to be x.
Wim: our security concern is bounded to the wireless segment only, not end to end, so it would be interesting to evaluate if this function is above or in the MAC.

Leon: if the application said 'I need sync service' it has the required QOS parameter with a number specified for loss of bit count integrity. You need to evaluate what that means and see if you can provide that given the media you are looked at.
Ken: how often you re-sync has some couple to the strength of the system. There is nothing to prevent the system doing encryption at multiple levels. We might choose to do frame at a time to make it as good as the wire - remove the casual ease dropper. Then for applications that need intensive algorithms they can rely on transport level facilities to provide guarantee of data integrity.
Leon: there are applications that are going to request sync service and a certain QOS.

802.10 may provide a set of algorithms from which you can choose, stream and block types included. If privacy is provided by saying 802.10 is required, you might also want to choose a frame oriented algorithm from the types they provide for you to accomplish this. If this is not sufficient, what does the higher level provide - bit count integrity is a required of some applications that got sufficient QOS from a wired network.

Greg: if the application requirement is something that can sit on top of an existing transport level then that's no problem for use. The difference for us is if the thing sitting on the MAC expects bit integrity from the MAC - that is where we may need to do something.
Leon: at layer 4 and above digit cellular handles this and it's transparent to the user. It's not a reasonable expectation of a MAC - so far it is expected from layer 3 and 4. We may say if you want that bit count service you have to use the appropriate layers 3 and 4. As long as no one above MAC is expecting you to provide this and you don't.
Greg: we need to understand exactly what services from the MAC that time-bounded services expect or require. Do they require bit count integrity or can we assume there are higher layer services providing those? We need that service definition.
Chan: comment - we already have an obligation to render isochronous service that neither adds nor subtracts bits. If we make an effort to achieve that it would inherently satisfy these requirements. We have to convert continuous streams into bursts, and we have to do whatever we have to do to ensure that what came in is what comes out. Listening to you has upgraded the importance of start and end delimiters and block counts in my mind.

The examples on page 6 represent delays incurred by packetizing stream data. Low bit rate and large packet sizes incur delays in accumulating the packet. In GSM frames are presented frequently the delay is as low as 5 ms, while the others range as high as 40 ms.

Page 7 - we must think in terms of what delay we are adding in the wired segment - how do we change the end to end delay. If you want the piece you add to be completely transparent, you better add a delay of no more than 5 ms in a telecommunications system.

General Business

Summary of the week:

We didn't identify any new DS services.

No discussion of network management was held.

A lot of authentication and privacy presentation and discussion. Dave suggests that a presentation from 802.10 would be in order next meeting. Chan notes that it may be time to inform 802.10 that we are considering needs to be added to our own.

DSS services discussed, but not used to evaluate MACs. It seems to be too soon for that.

A small core of people are bringing presentation, while most are listening and learning and not contributing to the goal. It is time for more people to stop being leeches.

Parametric MAC/PHY interface approach was on the agenda and not discussed because there were no submissions. The PHY needs input from us and they're not getting it. After the afternoon break we will meet with the PHY group jointly. We need to give them input or they are just going to present us with a PHY.

Issue processing and closing

Issue 4.1

Vote 21,0,0 to support ad-hoc.

This created a new issue of what is the definition ad-hoc. There is the definition found in the 3 bullets if the second paragraph of 93/03, and a definition presented by Bill Stevens, which after some manipulating says "a network created for a specific purpose, typically in a spontaneous manner. The principal characteristic of an ad hoc net is that the act of creating and dissolving the net is sufficiently straightforward and convenient so as to be achievable by non-technical users of the network facilities (I.e. no specialized "technical skills" are required) with little or no investment of time and no additional resources required beyond the stations which are to participate in the (ad hoc) network.

Discussion:
Mike: likes the definition concerning how the user perceives it. One kind is non-infrastructure. Is another hooking into an existing infrastructure? Keep in mind what the user thinks ad-hoc means.
Ken: ad-hoc-ness is - can a set of ordinary users come into a room, form a network, and the network no longer exists when they walk out. No needing to call the network manager to set anything up first. [generally people say yes] The network is only in place as long as the end users are there. Doesn't think presence of infrastructure should preclude this - if the end users bring it into the room with them. Ad-hoc-ness = end users can set up without a network administrator.
Wim: Ken says if you bring something that supports the creation of an ad-hoc network, that could be called an ad-hoc network. But an ad-hoc network should not require someone to bring a device, just normal STA hardware.
Bill: agrees with Wim, ad-hoc should not require anything more than 802.11 STAs. If some centralized CF can be implemented in all STAs, that's an OK way to implement it. Adding something to improve performance and capacity of the ad-hoc should not be precluded.
Dave B: ad-hoc is independent of infrastructure-ness. Agrees.
Greg: does the existence of an AP preclude the existence of an ad-hoc?
Jim: that is another issue - will an STA that wants to form an ad-hoc network conform to an existing infrastructure. That needs more discussion.
Bill: an ad-hoc should co-ordinate if it is the presence of a CF with which it can co-ordinate. The STAs in an ad-hoc must be able to inter-co-ordinate within their group.
Dave B: thinks that there is feeling that they must coexist.
Ken: ad-hoc or not, inter-penetrating networks of different management will exist, and there will be those that don't want to inter-operate. They may share air space, hopefully fairly, but they will never share packets. If we call that sharing the same CF that's fine.
Greg: so can an STA be in an ad-hoc and an infrastructure network at the same time?
Ken: I might want to do that.
Mike: if there is an existing CF, then during ad-hoc creation it should use that. If there is no CF existing then it has to create its own or work without it.

straw poll on the two definitions we have: 93/3 def. = 2; of Bill's def. = 13; abstain = 1.

New issues arising from this discussion - can a STA be member of an ad-hoc and a non-ad-hoc in the same time period? Do we support coexisting multiple 802.11 networks in the same geographical space?

Issue 4.2

Discussion:
Ken: this is not orthogonal to the ad-hoc question. Is an ESS a system with infrastructure? Without infrastructure is a BSS, with is an ESS.
François: read issue 4.2 pro 1.2 .
Dave B: ad-hoc and infrastructure were thought to be opposites. We seem to not think that way anymore. If infrastructure translated to ESS, then the PAR forces this support. Seems that this is either no question or the answer is forced due to the PAR.
Ken: is DS = infrastructure, and if not how and why is it different - so far we have been using them interchangeably. Is an AP part of the DS? Both of these could be issues.
unidentified: does infrastructure = existing infrastructure? An infrastructure can be divided into DS which is 802.11 unique, and another part which is existing 802.3, etc. Together they make in infrastructure.
Ken: would prefer to have one term that means this is the way you get from a BSA to an ESA.
Dave B: doesn't think it matters to solving this issue.
Bill: can answer yes here but feels there is some exposure here in that.
Wim: vote and further clarify the definition by adding new issues. Calls the question, Ken seconds (11, 2, 4)

Vote on 4.2: yes (11, 0, 5).

Steve Chen: for ad-hoc, we closed the 'are we going to support' issue and opened a define it issue. We should do the same here.

New issues from this discussion: what is the definition of infrastructure?

Issue 6.5

Tom S: seemed that there was a strong sentiment that that wasn't our domain, except from the point of view that we need to be as secure as a wire.
Dave B: thinks he heard a strong sentiment in favor of authentication and privacy provision. Heard that people feel it's mostly someone else's realm but we needs hooks left to support it.
Tom S: intent is to have the MAC have the ability to close the door if you don't qualify.
Leon: these functions need to be performed somewhere in a wireless LAN. Maybe just the hooks to get into what 802.10 provides. A particular implementation may not invoke those services at all. We don't have to DO security, we have to be able to get those services from 802.10

Vote: yes=13; no=0; abstain=1

Issue 12.2b

unidentified: can't we just connect to the LLC like all the other 802 standards? We are 802 and we have a well defined LLC interface, the DS interface is above that.
Dave B: DS may not be accessed by going up through the LLC, there are other ways too. We have chosen in the past not to be constrained by that path only. If exposed and you use it you must use the defined interface. Should they be exposed is the question?
Marvin: is the exposed MAC to LLC sufficient to support all the services we need.
Ken: existing 802 documents specify a bridge has a special exposed interface. So there is already a position saying that there is a second interface.
Bill: if 802.2 was the interface that provided DS functions - it does not provides time-bounded services, so we would still need something else.
Greg: what are the 2 entities on either side of the interface - the DS and what?
Ken: is the interface to the DS the same as the interface to the infrastructure. Two STAs with PHY, MAC and LLC in each. We know that LLC in not complete because of time-bounded services, so we already have 2 interfaces - one to LLC and one to something else. If these 2

STAs share the same CF then they are in the same BSS. (If they don't share the same CF then they are in something else?) The interface we have to define is the interface between the MAC/PHY in one STA and the MAC/PHY in the other. Is arguing that the thing being defined in addition to an STA is an infrastructure which has 2 interfaces - one is an AP (interface to the air), the other is to the DS. This goes back to does ds=infrastructure. The service specification at MAC/LLC boundary is not changed by the presence of infrastructure. DSS are a description of the interactions between a STA and the infrastructure.
Greg: we would define a MAC entity with a collection of interfaces into it one of which is an AP another is a DS.
Ken: repeaters are a test of this - that is a PHY extender. Is that part of the infrastructure? Based on BSS is something that shares CF, the repeater is a BSS extender It does not create an ESS, and is therefore not part of an infrastructure.
Greg: what are the 2 entities on the opposite sides of the DS interface?
Dave B: two 802.11 MACs.
François: the question seems to be is the AP interface exposed. The DSS interface is between the AP and the DS.
Ken: we are trying to define the infrastructure which contains the AP(s) and DS. There are interfaces between AP and STA, and AP and DSS. The infrastructure has the responsibility of connecting these.
Leon: if I built a physical device to do this, all as one package all the way up to the LLC, there is nothing exposed.
Dave B: if you don't expose an interface you can do whatever you want.
Leon: if I decide not to expose anything until I get to the LLC, am I compliant with the standard? So I have to adhere to an interface definition where I don't want one?
Tom S: the MAC in the STA is the same as the MAC in an AP?
Dave B: the STA MAC is in the AP, plus more.
Ken: the difference between the 2 MACs may be in the infrastructure, not the actual MAC.
Greg: there may be MACs in the system which have the AP function and those that don't.

No one objects to modification of the issue with the clarification discussed.

Greg: there's still the question of whether the AP is a thick interface or a thin entity.
Dave B: if AP to STA and AP to DS interface are the same, then AP is very thin. But we don't know yet.
Chan: doesn't object, but wishes an AP were a point and no more. Behind it are a PHY and a MAC which are necessary. An AP has a topological connotation rather than a physical one. When the AP reaches back into the machine and has roots Chan is not comfortable with it.
Ken: we are trying to unload the AP by suggesting how it might get implemented.
Wim: what is the thickness of the AP given that you have 2 interfaces specified?
Ken: all this says is that thickness is defined by later work. This definition allows thickness or nothing if the two interfaces are the same.

Dave calls the question, Chan seconds (16,0,1)

Shall we expose the interfaces AP to STA and AP to DS? (13,1,3).

Issue 5.3a

Chan: can think of some other functions which can probably fit under those categories. For instance the directory of information about which AP is usable from which STA, this may fit under association (Dave says authentication). Another is isochronous services - I thought integration meant IVD and 802.9, so these words don't mean the same thing to everyone. Maybe there should be separate categories for the management and the separation of isochronous and packet services. Should there be a new category for things relating to voice data or the fact that there are two kinds of services.

Dave B: these are categories needed, not necessarily a complete list. Can we use these as a place to start is the question?
Mike: can you add another category that is "others" so that the list is complete? (Dave does that.)
Ken: these are functional categories on what entity? They should probably be called infrastructure services now. (Dave changes the issue to be about infrastructure services.)
Greg: on distribution - this is moving data from one AP to another through the DS. If a portal is attached, does that distribution item cover this?
Dave B: yes. Integration is an open hole in case we need to add anything in that area.
Ken: an infrastructure is now APs, DS, and portals - so isn't there a portal interface that we didn't include in the last issue?

Vote - list of things to adopt for infrastructure services. (16,0,1)

Return to issue 12.2b

Suggest ion to add "infrastructure = DS + AP(s) + portals(0-n)"

Motion #1: **to make the change above to issue 12.2b.**

Moved by: Ken Biba
Seconded by: Greg Ennis

Motion Discussion:

Approved: 16 Opposed: 0 Abstain: 1 ***Motion #1 passes***

Issue 15.4

The core here is stating that we have to provide enough security to protect the wired LAN to which we may be attached.

François: agrees with this as long as its not mandatory. There is the real world requirement that says if you are going to export your product in some countries it is required that you have no security.
Tom Baumgartner: must not be mandatory because of the cost factor and processing burden at higher speeds than those being talked about now.
Dave B: if we assume that we are providing wire equivalent security the cost could be very high or very low. What that costs is important, but are we willing to take the risk of providing even one link that could compromise the security of a wired LAN?
Ken: the level of algorithm required to meet the objective is no penalty - we are talking simple algorithms to accomplish this. A couple of shift registers with mutually primed registers - a public key, very little hardware.

Straw poll - would like this (equivalent to wired network security) as a minimum requirement = 5; how many would like optional minimal requirement = 12; how many don't want this = 1.

Tom S: voted "not at all" because there isn't really a level of security provided by wires, it is an illusion.
Dave B: it is clear that people would like to have the ability to have the security there, but not mandatory.
Jim: would like to not have an option, but is worried about international ramifications.
Tom B: would like to not have key management procedures.
Jim: can make it mandatory defaulting to a key displayed in the standard, so that is not hidden.
Tom B: that would change my vote. Don't think any key management should be imposed on the user.
Mike: public key does not have to impact the user.
Dave B: no security is closer to wire level than any kind of crypto system is.

Ken: one of the features that will be built in every adapter is the ability to make a sniffer. We have to have this ability and we have to come up with a way to get around it.
Dave B: is hearing that we need to ask the PHY group if they have or are considering anything.
Tom B: it needs to be optional because those that want it aren't going to be satisfied with something simple. So putting in something by passable is not sufficient.
Mike: has NCR sold any DES options? Most MIS managers want to know if it's secure without any idea of level of security. All varieties of need will be encountered.
Dave B: uncomfortable with option because we said we would do that only when absolutely necessary, and we seem to be saying that we want to avoid doing this, which is not good justification. We will return to this at some later date.

Issue 15.8

Anyone want to speak that all STAs and all infrastructures must support time-bounded services (TBS)?

Chan: looked into STAs supporting both, concluded that some part needs to be put into all STAs that wouldn't be there is it weren't convertible to tbs.
Wim: would call that a TBS coexistence function which must be implemented in every sta. So that you don't disrupt the STAs that are using tbs.
Jim: page 15-13 has a lot of discussion on this issue. We concluded that support doesn't mean implementation. Agrees with Wim. Likewise an AP non-support shouldn't stop a TBS support STA from communicating with that AP in a packet manner. Symmetry between APs and STAs is required.
Dave B: but if I have to get something through the DS? If the two APs have the support and the DS in the middle doesn't, that's not very useful.
Jim: the function of the DS is not part of out domain. We may need to find out if the DS can handle tbs.
Dave B: might be able to talk to another STA, then he moves to be on a DS that doesn't support that and I cant talk to him when I did before. Reality may be we can't just say yes everything must support this.
Jim: support to me means can't be precluded, not has to work. This is an evolutionary process - there will be some STAs that are packet only, some TBS only, and some mixed. If support means its got to work, then I say no, but I don't interpret it that way.
Greg: agrees, but also thinks STA and infra structure are two different questions.
Mike Bergman: shall a STA respond to a request for tbs. Shall a STA that does not support TBS be required not to muck up a STA that does support TBS? These are the questions here.
Tom S: to answer yes are we requiring use of an infrastructure which doesn't exist today?

Meeting adjourned: 3:10 PM.

Thursday AM, January 14 1993

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

General Business

Issue 16.8

Security and authentication discussions this week seem to make the issue of crossing a service area boundary are not terribly relevant. What you need is to be able to become associated or re-associated and authenticated or re-authenticated. Who "owns" the AP is irrelevant, as long as you are authorized on the infrastructure (infra) the authentication will be successful.

Phil: passing you 'context' from one infra to another will not happen. A message waiting for you in your old infra won't get to you. This may be a difference between roaming/handoff and just associating in a new BSA.
Dave B: sure, but does that have anything to do with us? It involves things outside our scope to try to get continuity there.
Leon: if you moved to different companies' BSAs, you are going to have to re-authenticate and make a new 'connection'. Within the same infra if you change BSAs you have continuous connection. These are concepts which could make roaming and handoff different terms - the first is within the same ESS.
Dave B: it depends if you stay in the same ESS. If you leave it, these things are beyond our scope.
Wim: 92/126 said roaming and handoff are intermixed in the way they are used but are very different concepts. The ability to move around and get associated with new APs in an ESA is completely different from roaming. Roaming is the ability to be registered in somone else's domain. This has nothing to do with the ability to staying connected to your network when moving within your ESA.
Dave B: isn't the ability to stay connected in your ESA simply a matter of re-authenticating?
Wim: with roaming you become a member of a network and authentication is verifying you are a member. Handoff is the dynamics of moving from BSA to BSA associating to a new AP.
Dave B: within an ESS - moving around (a) within a BSS nothing happens, (b) changing BSSs within the same ESS, that is re-association. Part of that may include re-authentication or a third party authentication that has you authenticated already when you get to the new BSA. When you authenticate you assert your identity both ways, and then the AP decides "i know who you are, are you allowed to be here". Authentication determines if membership is allowed. At the 802.11 level all we need is the authentication hooks, whether the network allows use is a higher decision.
François: the definition in issue 16.2a and 16.2b we may need to look at here. Those issues have definitions of roaming and handoff.
Dave B: definition of roaming here assumes some sort of temporary usage, that is assigned according to information we provide to higher levels, that we have obtained by authentication.
Tom S: the word 'connection' automatically takes you beyond the realm of the MAC every time you use it.
Wim: doesn't object that roaming is above our scope and authentication is the heart of the matter. But you have said that there is no distinction between roaming and handoff, and I don't agree with that.
Dave B: I only meant from the point of view of 802.11, we don't need to be involved in those processes whatever they are.
Wim: handoff is the process of changing APs within an ESS, and as such has nothing to do with roaming.
Leon: at 802.11 once authentication has occurred how much further it goes is the responsibility of some the above intelligence.

Issue 16.2a and b

Dave B: thinks that roaming as described in 16.2b is the same as re-association. 16.2a describes a concept which is relevant for layers above 802.11 .
Wim: the issue is simply what is it, not whether we have to handle it or not. 92/126 does not define roaming as an STA crossing between ESSs. It describes an off-line process to register with an MIS manager that gives you all the information needed to become someone who is allowed to use that network. Has to do with billing process perhaps.
Dave B: these terms were pulled from the cellular phone world. Handoff is where you move around transparently. Roaming is where you go to some other city. What happens is if you use your phone now its signal is picked up by the local administration, and it picks up the id of the phone. The cellar phone system believes the id, then completes the call because by knowing the

id it knows how to do the billing, or doesn't complete the call because it can't find that id. Relevant to us, is the in the authentication we may do more verification of the id. To support this functionality all we have to do is support the authentication procedure and provide this information to someone else. Two APs in un-connected ESSs, if you move between them it is just as if the unit turned off in one and then on in another. If you want seamless roaming between ESSs, it is too much for us to provide.
Phil: doesn't find this definition of roaming very useful to us. Moving even from one BSS to another the STA has to actively do something to make that happen. Let's use the word roaming "the act of an STA crossing BSA boundaries" as it means something relevant to us.
François: if 802.11 thinks that roaming is outside our scope, don't use the term - don't redefine it.
Leon: if there is a digital cellular definition of roaming, don't use it here to mean something else. Implies transferring control to a different administration. Handoff means staying within the same administration.

Quantum concepts: (1) just not moving; (2) moving, but not moving out of the range of an AP; (3) moved from one BSS to another, but not leaving the ESS; and (4) moved from one ESS to another.

Tom B: combine 1 and 2 as there is no difference.
Wim: roaming is not involved with moving, but with a registration action. There are terms for the transitions as well as for the states.
Steve Chen: if we are not using exactly the same definition as other parts of the industry we should use a different word.
Leon: in the NPRM the FCC uses roaming as meaning one service provider to another. An ESS by our definition is a single service provider. We can't guarantee transparent service continuity across ESS boundaries.
François: in roaming we can't guarantee continuity, in fact we can probably guarantee that you will not have continuity. If you have continuity, then you are not roaming, you are in the same ESS.
Tom S: reason to have a term is usefulness. Agrees with Tom T from the network point of view 1=2
Dave B: proposes terms: 1=2=no transition; 3=bss transition; 4=ess transition. These are the terms we will use when we are talking.

No one objects to presenting to the WG that these are the terms we will use.

Motion #2: **To use the word re-association instead of handoff to describe the transition between BSSs.**

Moved by: Tom Siep
Seconded by: Tom Baumgartner

Motion Discussion: none

Approved: 11 Opposed: 1 Abstain: 2 ***Motion #2 passes***

Issues 162a

Wim: reads the definition of roaming from 92/126.
Phil: problem is roaming talks about temporary-ness of the registration which has no meaning to us.

Motion #3: **close issue 16.2a as MOOT as the term refers to concepts outside the scope of 802.11 that we can neither support or effect - see paper 92/126.**

Moved by: Wim Diepstraten
Seconded by: Leon Scaldeferri

Motion Discussion:
Phil: someone might think we don't support the concepts because we closed the issue as moot.
Leon: we have covered the problem by describing the functionality in the new terms we added for transitions.
Tom B: someone said within an ESS there is only one service provider - that is not true. But it does not matter to us.
Dave B: aggress.

Approved: 10 Opposed: 0 Abstain: 0 ***Motion #3 passes***

Issue 13.1

François: at the last meeting a management model in 92/98 was presented. We said we recognize that we need a management entity and we looked at functions that could be added to that function. See the discussion in the issue list. Proposes that we close the issue in accepting this as a starting list.
Steve Chen: We need a starting point to get work done in this area, which is why I presented this paper.
Dave B: there is no controversy about the need. We have only had one model proposed, so the choice is pick it or don't start.

Motion #4: **to adopt the model in 92/98 and 92/124 as the starting point for our network management functionality.**

Moved by: Steve Chen
Seconded by: Jim Schuessler

Motion Discussion: none

Approved: 10 Opposed: 0 Abstain: 0 ***Motion #4 passes***

new issues to report to plenary

(1) what is the direction of the association service transaction?

(2) how to determine what APs are present?

(3) how does re-association interact with authentication?

(4) how does re-association interact with privacy?

(5) do we need an explicit re-association transaction?

(6) what is the direction of the re-association transaction?

(7) given an FH phy who is responsible for the real-time aspects of the phy?

(8) do we support geographic coexistence of multiple overlapping 802.11 networks?

(9) can an STA be a member of an ad-hoc network and a non-ad-hoc at the same time?

Motion #5: **that we open the above issues**

Moved by: Phil Belanger
Seconded by: Steve Chen

Motion Discussion: none

Approved: 10 Opposed: 0 Abstain: 0 ***Motion #5 passes***

For next meeting

Goal: determine functional specification of transaction needed to support adopted infrastructure services.

Goal: define first cut of required management functions.

Goal: initial specification of functions of the PHY dependent portion of MAC given an SFH PHY.

Further issue processing.

Goal: determine what requirement we need from other 802 groups

Initial exploration of impact of provision for power management abilities.

By May we would like to be able to make comparisons of MAC proposals vs infrastructure services, functional services and other adopted requirements. This can be construed as a requirement for submissions for MAC proposers to say how they are going to operate with and support the infrastructure requirement proposed.

Goal: provide sufficient information to MAC proposers to enable them to bring contributions for the May meeting related to the above paragraph.

Discussion of changes in the draft standard 92/140

François: is planning to maintain a list of changes as you see on page 4 of that document, that reflects the changes for the last 2 meetings, from plenary to plenary.
Dave B: would like to see some kind of revision number or something on the draft. Same thing with the issues list, some revision indicator on the page would be nice. That way each changed page gets a new number.

Motion #6: **to adjourn MAC group.**

Moved by: Carolyn Heide
Seconded by: Leon Scaldeferri

Motion Discussion: none

Approved: 8 Opposed: 0 Abstain: 0 ***Motion #6 passes***

Meeting adjourned: 11:55 AM.