MAC Minutes
Tuesday, March 9, 1993

The meeting was called to order by chairman Dave Bagby at 8:45 AM. Carolyn Heide secretary.

First the agenda was sorted out as there were a lot of submissions, and there were people who needed to make presentations in both MAC and PHY groups.

Summary of last meeting: privacy and authentication discussed quite a bit. Some concerns about where that is implemented have been raised in 93/21 and there is a response to it in 93/22. We asked 802.10 to give us a tutorial about what we needed and where they should be. They responded with not having time to do anything, but sent us Leon with this presentation 93/28.

802.10 Standard for Interoperable LAN and MAN Security, IEEE P802.11-93/28,
by Leon Scaldeferri

There are very useful appendices and annexes in 802.10b SDE (which is being handed out at this meeting) which contain some justifications and explanations of what they have done. This SDE standard is the part of 802.10 which affects 802.11 most. So this presentation addresses that part - a layer 2 security protocol.

Page 6 lists the four security services provided, while page 7 describes the threats those services are intended to protect against.

The ISO model is concerned with security at the transport layer, while 802.10 addresses additional security services at the link layer.

Chandos Rypinski: connection type services are excluded? existing lans have branching point where one way is LAN and the other isochronous.
Leon: working with .6 and .9 on can this same protocol be applied to isochronous. right now the isochronous is excluded. It would be desirable if you could include it.

Using the primitives you can have a management function which can allow you the flexibility to have a secure or less secure system.

There is only a single type of PDU, described on page 13. Not the only non-optional thing in the PDU is the data.

Dave Bagby: does 802.10 identify choices for a algorithms or just say its out of our realm.
Leon: they give some examples and the describe a negotiation process for agreeing on the algorithm used.

Page 14 shows the layout of the SDU. There is no maximum size for the SDU, that is limited by the rest of the system. The algorithm for the ICV is not specified.

Dave B: because the pad length is after the pad, this must exclude variable length packets - you have to know the length to get to the pad length. So you can only use this on a system with variable length packets.
Leon: the data can be variable length, it is padded to a fixed size.

Construction of the SDE PDU, page 15 - A station that is not implementing the SDE will be see an LSAP which specifies this as an SDE packet. He just discards the packet because he doesn't know what to do with. The station that is SDE aware looks at the security association ID to see if he recognizes the sending party.

Page 16 describes negotiation of security attributes between stations.

Dave B: standardizing the id's of the security algorithms?
Leon: there are only 2 id's registered now (values for the SAID). You, the manufacturer, come in and ask for a number, or a block of numbers.
Bob Crowder: negotiation of algorithm used?
Leon: you send your list of things you'll do. I respond with what I'll do. You switch to mine, or that's it, we can't talk. It is a two step negotiation only.
Dave B: please ask 802.10 if there is an intent to standardize those ids.
Simon Black: it doesn't work if they don't.
Leon: the intent is that the SAID represents an algorithm, and that SAID always represents that algorithm because of the SAID is registered. The information exchanged in the MDF of the SMIB contains all information required to be shared to use that algorithm.
Bob C: as an individual I could buy a copy of a registered algorithm for less than $200? In this committee I am not interested in any algorithm that meets that criteria.
Leon: there are algorithms out there that meet that. But you can register company proprietary algorithms.
Bob C: that is totally against the 802 philosophy.
Dave B: we are looking at a mechanism that may be of use to us and trying to figure out how to use it. To us, whether it's a private or public algorithm doesn't matter.
Leon: this architecture allows custom algorithms to be used while still remaining compliant with 802.10. A private algorithm and a public algorithm could exist on the same wireless LAN.
Bob C: you describe coexistence not interoperability. 802.11 must pick algorithms that are public. Vender specific must not be allowed.
Leon: in the annex of 802.11 you can put the default algorithms that must be supported. If anyone wants to have private ones added they could be negotiated. The specification says all stations must support a and b, but if you want to implement others too that's ok.
Bob C: new issue: shall 802.11 include at least x number of default security algorithms which must be publicly published and are supported by all conformant implementations.

Page 17 and beyond addresses issues from the issue list specifically, with Leon's opinions their resolution.

Dave B: do have a feel for how ISO feels about adopting this work?
Leon: about the proposal to take 802.10 into ISO, people said that it's nice and they understand the reasoning for it. But you have to have 5 nations supporting changes to an international standard, and only the USA stood in support, the others don't seem to see the need.

Dave B: is the government likely to be amenable to a good algorithm that is secure but is public?
Leon: for authentication, yes. The real issue comes with what to do about confidentiality.
Dave B: if we specified an algorithm number that is equal to transparent, you wouldn't have to detect if SDE is implemented.
Leon: you must choose what to do if you don't have SDE - you don't pass SDE packets, or do you look at the some algorithm that tells you what to do with them. That is outside the 802.10 standard you can do what you want.
Bob C: a bit not normally used in a LSAP is set in the SDE LSAP identifying an SDE SDU immediately.
Tom Siep: about the diagram on page 9 and some minimal set of algorithms in 802.11 products. That diagram says you don't include the algorithms in 802.11.

Dave B: you include some set of names which all manufacturers understand. The implementation is not in the 802.11 layer, but in devices.
Bob C: another new issue: will one of the default security "algorithms" supported by all 802.11 nodes be no use of SDE?
Dave B: re-iterates Bob's new issues with different phrasing and Bob agrees to it.

Dave B: can I switch algorithms on the fly?
Leon: you may have an association (i.e. have gone through the security algorithm negotiation) with many different stations and they are all using different algorithms. You can also do that negotiation any time you want, not necessarily once only with each station.

Security Aspects of Wireless LAN Standards, IEEE P802.11-93/21, by Jan Kruys, presented by Wim Diepstraten

User needs

Cable equivalent; separation of wireless users into groups (e.g. staff and guests).

Higher levels of security should be left to other layers. It should have no impact on existing wired stations. Simple key distribution and management should be used for management of security.

Authentication

Required where device functionality is critical in assuring functional integrity.

User authentication may be required for a function like billing.

Device authentication is not needed in WLANs which are private systems. LAN operating systems provide device authentication, and the MAC should not duplicate this.

Leon Scaldeferri: there is a difference between wireless and wired device authentication needs. In wired scenarios you do a physical installation which is a level of security. In wireless anyone can walk in and access your WLAN. You need something that looks like you are going to let this guy hook up to the cable.
Wim: but do you need that or is it taken care of by the higher layers?
Tom Siep: you don't really have security with wire, it is just an illusion.
Dave Bagby: user id at a higher level is a different function than device identification at a lower layer. Similar, but for different purposes. To connect to a wire you need to get into the building. Impostors are easy to create on a wireless segment - you can compromise the entire LAN with just the wireless segment.
Francois Simon: you said the MAC should not deal with authentication?
Wim: device authentication.
Francois: what is the difference between user and device authentication as you see it?
Wim: user authentication is a login to the O/S, a password that identifies you as you and gets you services. Device authentication is more linked to whether the device is registered to operate in this building.
Francois: device authentication you see as a MAC function?
Wim: yes, if we need it. But do we need it. Jan says we don't need it in this paper.
Dave B: your statement about 'private systems' - there can be situations where this is true, but it is not necessarily true. Users understand logon, and presume that if you know the password you must be the person. The device and the user become merged after you logon. The device and the user must be conceptually separated.
Wim: but why do we need device authentication?

Leon: if the standard says you can bring company A's equipment into company B and can communicate, some method must exist for not allowing use of company B's equipment to access company A's LAN. Even today using a dial-in line you can tie up an input, although you can't get logged on. If your device has some way of denying you to getting as far as logon, you would free resources.
Wim: but it is still not clear to me why we need device authentication.

Meeting user needs

Confidentiality at MAC or PHY level. Encryption or stream cipher is sufficient and straightforward.

No impact on existing wired stations, means that 802.10 cannot be used because it is MAC to MAC service, but end to end.

Leon: the 802.10 architecture provides that. You can leave it on end to end or strip it off at the access point.

Key distribution and management are outside scope of a LAN standard but belong in total systems standard.

Keys change with time; the wireless LAN standard should provide for key synchronization.

Placement of the confidentiality service

PHY level confidentiality forces "single key approach" - no segmentation between user groups.

PHY confidentiality would also encrypt MAC header and deny clear text messages needed.

MAC level confidentiality is more flexible and need not be less than PHY confidentiality.

MAC protocol can provide hooks for key synchronization.

Wim: still, personally, has the basic question, do we need device authentication
Chandos Rypinski: is not the LAN address of a STA similar to device authentication. That address could be assigned. In cellular you have no user id; in password systems you have no device id; both systems have a lot of fraud. With both you just make it harder.
Wim: our focus is not to provide end to end security. We provide functions necessary to allow operation.
Bob Rosenbaum: without device authentication this standard will be difficult to market. Gaining access to a wireless LAN is too simple versus a wired LAN.
Ken Biba: agrees with Bob. Customers perceive that physical security for the wired LAN is in their control. User id at the next level is not our problem. There is a marketing perception that device authentication is necessary and sufficient.
Tom S: device authentication means a list of known devices where these devices and only these are allowed access?
Dave B: that would be one algorithm for doing that. We should provide enough hooks so that several different schemes could be used, which range from don't care to crypto systems.

A Clarification of the Concerns in 93/21, IEEE P802.11-93/23, by Dave Bagby

Read from 93/21 that it asserted that: (1) 802.11 features should be justified by market needs and that hadn't been; (2) a lot of features were going to have to go into 802.11 for security; and, (3) that 802.11 was going to have to compensate for the media.

Could see how you might get the wrong impression if you just read Dave's submission to the last meeting, which was just his slides. It was an education attempt, not a suggestion that all this stuff

had to be done in the MAC layer. It was to show that there were things that could be used to provide what we wanted as opposed to us having to put all this into the MAC.

93/21 says justification based on user needs is required. Dave feels that this has been considered, Leon Scaldeferri's discussion of needs is a good example.

93/21 suggest there is not a need for device authentication. Dave disagrees with this. In a wired LAN a physical connection is required to get access, and the security of the building can make it very difficult. It is also reasonably easy to detect something extra has been connected to your wire. In wireless there is no building security, and it is difficult to detect extra listeners. This compromises not just the wireless segment, but the wired LAN to which it is connected. Device authentication is the way to start providing security - without it WLANs must accept any and all devices. There are those that care and those that don't, and we must satisfy all of them. Impostors, are too easy to make - both impostors of the stations and of the wired LAN to which they communicate.

Agreed with most of 93/21 except on the subject of the need for device authentication.

Discussion:

Wim Diepstraten: Why do we need device authentication? The fact that I am using a certain key which is known to the system does authentication.

Dave B: you have assumed a keyed system, and you know the key. That is a privacy function - you have coupled privacy and authentication. Systems could use privacy and not authentication if they want.

Wim: authentication is needed only during the distribution of the key for the privacy function.

Bob Rosenbaum: key distribution system assumes a certain security is already in place. You assume our MAC has to have some sort of key distribution system.

Wim: key distribution is not part of the MAC.

Leon Scaldeferri: if you use 802.10 for the security services it is above the MAC and you can use it or not use it. Do you mandate in 802.11 where it resides is the question. We need to make sure the hooks are there to allow it, but do you allow anyone to produce a system without device authentication?

Dave B: what do you do if you don't want to worry about device authentication. The concept of authentication is always there and we can make it very easy to not use it. With the 3 step process outlined last meeting - assert identity, challenge that and then respond - if we make the asset the only mandatory part, then just believing that assertion could be compatible. If you want more authentication you can challenge. To make the degenerate case not doing anything at all makes the process harder. Why does Wim think we shouldn't have the concept if having it and not using if you don't want to - it doesn't cost you anything.

Wim: doesn't understand case where it is not implicitly provided by key management. Understands that it is easier to bring any device into the network for a WLAN, and you may need to go through some kind of registration - these are the devices known and they are the ones that can work. If that does not translate into the use of a key or something then that would have to be done for every packet.

Dave B: the authentication scheme can ensure that once it has been done no one can interlope, by exchanging some information at initial authentication. Use of the 3 step process, bi-directionally, allows support of as complicated or simple a scheme as desired.

Tom Siep: the reason the MAC is involved at all, is that it may need to route some messages in a different way because they are security messages.

Dave B: do you mix data and control in the same stream is the classic question.

At the last meeting we adopted device authentication as something we wanted to do, using the issue process. We can vote to re-open the issue. Wim feels that the whole subject of security still has a lot of work to be done, so the issue doesn't need to be re-opened now.

Tuesday PM, March 9, 1993

The meeting was called to order by chairman Dave Bagby at 1:30 PM. Simon Black taking the minutes [sec: thank you Simon].

Further Exploration of Transactions and Name Spaces 93/22, IEEE P802.11-93/22,
by Dave Bagby

Corrections to and extensions of the things discussed at the last meeting. About half in the room were at the last meeting, so presentation this time will include some background (but not all the detail).

Corrected these ideas to take into account comments last time. Added name spaces and attempted to define some of the transactions - in a sort of pseudo code.

Slide 1 - Simplified Architecture

Three different name (address) spaces and media - wireless, distribution and integrated.

Many make assumptions about physical implementations of distribution systems and address spaces. However, want to resist certain assumptions (page 6).

> Simon: do we need to define an integration medium and address space - is this is not a separate sub network outside the scope of 802.11?
> Dave B: as you will see the concepts of integration medium/space are advantageous when considering communication with stations on the integrated network.

How does a portal differ from an access point ? May have to provide some additional integration services.

What do we mean by address space? Use tuple in these concepts - value of the address, type of space address belongs to

Are addresses globally unique? No assumptions taken - have not considered mapping to physical addresses (e.g. 48 bit IEEE)

APs and Portals live in two spaces - APs in WAS, DAS, portals in DAS, IAS

In the DAS - DAS address = physical location. This is certainly NOT true in the WAS, i.e. in WAS, and address does NOT correspond to a physical location.

We are not going to deal with mobile access points - this is a level of complexity we choose to avoid !

IAS - portals are addressable entities within the IAS

> Francois: Do you make the assumption that at any point in time an wireless station address will be associated with a particular access point ?
> Dave B: Yes, at the moment.

Last time we talked about possible four states.

Page 15 is not intended to be a formal state diagram.

Need to become authenticated before becoming associated. Could be authenticated with many APs while being associated with only one - relaxes requirement for real time authentication (hence pre-authentication).

Wim: missed the point of pre-authentication.
Dave B: When sitting in authenticated, associated state may wish to authenticate to more than one AP (may later become associated with one of these APs)

Which transactions involve more than one name space? Distribution, association, disassociation, reassociation.

(1) Distribution Transaction

- Intended recipient of message and address of message are distinct.
- For distribution - we need to know *origin* (e.g. for response), *destination* - intended recipient, and *next* indicating where message is to be sent next.
- Assumption is that there is only one WAS.
- Who maintains message *next* information ? STA only has to know which access point it is associated with.
- Location of list of associations may be handled in more than one way - essentially stored within a DS (could be within an AP, might not be).
- For BSS communication - destination and next are the same.
- For ESS communication - the message is sent to the AP, if AP is final destination its for the AP, else pass to the DS. AP is not usually the destination, exception might be management information.
- At AP is there a routing table ? Could be, but there are other implementations I am not trying to handle the details of the internals of the DS (only the services). We decided that this was the approach we wanted to take. A message enters distribution system. You know the output through the associations. I do not intend to specify how it gets from input to output.

Ken: Seems that this presupposes a solution because you are proposing a routing solution. Essentially this looks like an IP routing solution where you have to know the next hop
Dave B: I don't think this is so
Ken: but the address does contain routing information as part of its address (the next part). This is source routing
Dave B: I'm just passing the message to the AP that the STA is associated with
Ken: if you make a system where at any given time there is a 1:1 association between STA and AP then putting this information in the message is adding redundancy. In fact it may be restrictive. Ideally you want put as little information as possible in at the end station. All you really need to know is the source and destination addresses and the fact that the STA has an association (but not necessarily the addresses associated with that association)

- DS uses association service to determine output from DS (DS delivers message between input and output).
- At output AP need to check that intended STA is associated with that AP. If yes, then we can send the message to the destination. If not (and this is possible if associations have changed since message entered the DS) then this is an error condition. Some DSs may give up at this point, some may try a bit harder to deliver the message.

Ken B: What you have suggested is very close to classical routing systems
Dave B: I'm not specifying routing within the DS - only the input and output
Ken: There are essentially three hops: Wireless ->DS, DS->DS, DS->Wireless

(2) Association

- To set up an association - already have to be authenticated
- Knowledge of associations - DS needs to know. Not saying how and where associations are stored.

(3) Disassociation

- Simply canceling an association

(4) Reassociation

- Reassociation may be just disassociation/association. However a reassociation function is useful in certain implementations (it makes things easier) - therefore it is retained

Wim: did you work through how this might work if the DS consists on wired LANs with routers ?
Dave B: I have illustrated two examples of distribution systems. I will come to this. This is not a great deal of functionality for a distribution system. I think we are very close here.
Ken: But it doesn't tell you about performance constraints, e.g. delay. Therefore this only solves part of the problem
Dave B: We set out to specify how to make the thing work. Given that we can move on to specify how well it works. Different customers may purchase different DSs depending on the performance they need
Simon: or on what systems they already have installed

Several requests for real examples to illustrate the architecture. Two examples considered - centralized, distributed

Access point may contain other things beyond a MAC and PHY (which it has to have from its definition). A range of AP implementations are possible from thin (dumb) to thick (intelligent).

If we are going to allow access points to be a dumb interface - we will mandate that DS supports certain functions - such as association.

In centralized example. Two BSSs may have different PHYs - one IR one RF (although two RF are shown)

DSs are functionally interchangeable (i.e. to the stations two different DSs are indistinguishable) - though the performance might vary between two different implementations.

Since the integrated network is outside 802.11 may be a set of integration services to be able to sent and receive messages to stations on the integrated network.

We should not constrain ourselves to a particular DS implementation

Wim: what about putting bridges or routers in the DS
Dave B: I don't care about what the DS is made of, only the logical functionality
Bob: Do I assume that each of the APs needs to be aware of the DS algorithm, whether its distributed or centralized
Dave B: There are a key set of questions to ask on the way in to the DS and on the way out. I don't care how this is done - but it has to be done somewhere
Bob: Is it the business of 802.11 to define the distribution algorithm
Dave B: No. We have decided only to specify the services the DS provides (its a black box)
Greg: Market will want standard DS components. So somebody has to do some sort of standardization - maybe based on existing 802 LANs for example.

Dave B: personal opinion. I don't believe what you're describing is essential for the success of the standard. Problem is that to make a DS work it takes you out of the realm of 802.
Greg: That may not necessarily be so, e.g. bridges.
Chan: if we can achieve the air interface and functions of DS, then downstream we may take on a standard DS protocol
Dave B: Moving on - did not talk about integration transactions, net management transactions
unidentified: Argument that we define a real distribution system (rather than a logical one).
Dave B: there is no such thing as a real distribution system today.
Phil: Suppose I make a DS out of an IP network
Dave B: If you are talking about wanting to access a resource on an IP network then you can use an IP address on an IP integrated network. If you want to extend this such that the DS and STAs are based on IP addresses then you are collapsing the model (all address spaces the same). You have to accept the limitations that this may bring.

Some clarification on authentication discussed last time - how do you get authentication in three exchanges.

Three explicit exchanges of information are the middle three in slide 43:
Challenge of AP assertion and assertion of station ID
AP response to STA challenge and challenge of STA assertion
STA response to challenge of assertion

One implicit exchange - the first:
Assertion of identity of AP
Happens implicitly as part of STA finding the existence of the AP

There may also be a final acknowledgment.

Meeting adjourned: 5 PM.

Wednesday PM, March 10, 1993

Meeting called to order at 1:45 PM, by chairman Dave Babgy. Carolyn Heide back at the keyboard.

The Wireless Hybrid Asynchronous Time-bounded (WHAT) MAC Protocol,
IEEE P802.11-93/40, by Phil Belanger,

The document is a complete protocol description, while this presentation is aimed at the support of time bounded services. First reviewed the protocol in general.

Slide 8

Wim Diepstraten: why do the RTS on multicast?
Phil: have optimized use of bandwidth by putting not all information in all frames, so this avoids a custom data frame for multicast.

Slide 9

Wim: RTS frame - is there carrier sense before transmitting it?
Phil: yes for sending the RTS, but there is more to the total carrier sense than that. The decision to tx is based on that plus the RTS/CTS exchange.

Slide 11

Frederic Bauchot: what happens if multiple APs are in range of a frame with the hierarchical bit set?
Phil: uses the net id. If this is its net id and the hierarchical bit is set then it needs to assist in the transmission of this MPDU.
Frederic: you need to know the net id, so you might just as well know the address of the AP.
Phil: but this means that the STA does not need to take different actions if it doesn't want to. You can set the bit all the time if you are registered with an AP. But if you want to pay attention and see that the AP is forwarding to a STA in your own BSS you can send without the bit.
Frederic: two independent nets that overlap - can they have the same net id?
Phil: the net id is managed by an administration function. Part of it is an organization id. Within net id there is a BSS and a domain id, if you want to think of it that way. Maybe 16 bits won't be big enough.

Announce frames are either sent by an AP or some node that takes the responsibility. Regularity of announce frames may depend on the PHY. Maybe something like 10 times per hop on an FH PHY.

Wim: scope of multicast?
Phil: the hierarchical bit allows the station to control the scope of their multicast. Set this bit to 1 to send this to an AP and use it investigate the world.

Slide 12

Real-time voice as the primary application of time-bounded services (tbs). Rates from 1 to 20 Mb, current implementation at low end. Designed to support a link between a STA and an AP or CF (99% of the time this is the same thing). Not an adhoc service.

Frederic: address scheme - so these MPDUs are not standard?
Phil: tbs has an explicit call service which defines the quality of service for that service. After that you can assign a local id for it and use that. There is a field which identifies what type of frame it is.
Greg Ennis: are calls always between a pair or can they be conference?
Phil: point to point only so far.
Ken Biba: how to build the infrastructure to do full isochronous service is still unknown, so we have chosen to solve the last 50 meters of the problem between the AP and the STA.

Slide 12

KS Natarajan: AP always initiating the exchange - how does it know?
Phil: because of the call setup that was done, by the MAC management thing.

Slides 16, 17

Asynchronous traffic occurs in the gaps between the tbs. The time bounded traffic 'reserves' bandwidth by use of the gap time and the more field. This makes the tbs traffic higher priority because the async traffic can only reserve for the immediate data. You request a call from the AP and from then on the AP sets the timing for the connection.

Simon Black: when there are multiple stations with tbs within a BSS, other stations that want the async service have a large overhead of keeping track of the future.
Phil: not a lot of overhead. Just an extension of what they had to do for the async service.
Greg: scaling for 64k voice?

Phil: an ATM cell is being used as the payload model. If you had good compression you would increase the gaps.

You can adapt your system to maximize throughput or minimize delay.

If you were asleep, or you're new, you have wait for the first MPDU. There are collisions possible, that may have to be enhanced.

Frederic: you may have interference on the isochronous users by the async traffic. If you have to listen for a long time there before coming alive there is a long dead time.
Phil: without isochronous stations listening for 1 MPDU is fine. If you have isochronous users the AP can give you information on association.
KS: call setup - you ask for n number of frames and the AP grants you that. You go through this sequence at regular intervals?
Phil: you are not asking for a specific number of transmit opportunities, you are asking for a quality of service, which means, for a fixed length frame, you need to transmit that often. Either side can abort the connection.
Wim: reason for having the RTS/CTS on the isochronous packets?
Phil: because you want to convey the information from both ends of the connection each time you transmit. You reserve n times ahead and you need to do that from both sides.

Slide 18

Node b connects to AP2 then starts to move closer to AP1, he moves into conflict with another tbs connection as he goes. He would have to abort the connection. That might tell him that it's time to do a BSS transition.

Ken: the tbs challenge is when overlapping APs without a god-head figure. In offering these ideas we recognize there are still holes related to coordination between APs, especially of differing administrations.

Slides 19, 20

Wim: does tbs degrade gracefully too?
Phil: from async point of view the tbs is one of the harsh conditions under which it degrades gracefully. Don't know how the tbs degrades. Async service simulations have been done, but not tbs.
KS: 'small adhoc groups', what about many nodes?
Phil: we have done work on 5 - 10 nodes systems.
KS: if one station does not receive the traffic it will not have an accurate vector.
Phil: to cause a problem you need to want to transmit when your vector is incorrect. You play the odds of the likelihood of the happening.
Ken: this system propagates information through the system.
KS: 20 or 30 users with an equal probability of discussion - you have to listen to everything although you only have to transmit sometimes.
Phil: not likely that many in the same room.
Ken: controller has nothing to do anyways.
KS: battery consumption?
Phil: protocol allows for sleep.
Francois Simon: 93/40 page 5 specifies DA - all addresses are 802.3 48 bit. Implies that the ds will always be a LAN?
Phil: thought we were developing a LAN and so it should be a LAN thing and didn't want to invent a new one. Do think it should be 48 bits. If you had something like a frame relay distribution system (DS), then the DS is used as a DS. For addressing something inside the AP

or the portal there is something that does not that needs to be specified. Assuming all those addresses are the same is a danger.
Francois: registering those ids to Ethernet is not favorable.
Phil: just because we use that address type doesn't mean they are registered Ethernet ids. Proposes using 48 bits and not inventing a new encoding of ids, and that doesn't tie us to a particular DS. A flat address space with unique unchanging addresses is potentially valuable.
Frederic: page 9 of 93/40 - no negative ack. That means you cannot discriminate between not received and received under some invalid conditions. You are losing some information.
Phil: you are bundling more than one function into that function. It is only to overcome the bit error rate, it does not convey anything about the state of the receiver. Not used for flow control or anything else.
Frederic: there is some potential loss of bandwidth while stations look to form their vectors. Do you intend to do any fragmentation to overcome this.
Phil: has that in mind, and we might want to consider that.
Wim: ack for tbs needed? Mobility may cause you to step on someone else's isochronous packet and there may be no mechanism to detect that.
Phil: no attempt to retransmit in that case to preserve the real-time nature of the voice. As the result of movement your connection may be damaged or you may damage another one. You may not detect the loss of a particular MPDU.
Greg: FH - are you synchronizing the regulation of the bandwidth with the hopping sequence?
Phil: absolutely. Because during the new frequency the time period in which you are dead needs to occur during one of those gaps.
Wim: PHY dependent issues - isochronous service on an FH PHY. Is the performance sufficient for a voice connection, because no deferral method built in for isochronous?
Phil: at 1 Mb a small number of connections in a BSS could be supported. AP has some policy it uses to allocate and grant connection requests, those issues are hidden in that policy. One metric it could use would be are there enough gaps still left for async traffic.
KS: tbs assumptions - some are restricted by voice always going through the AP.
Phil: viewed a voice system wanting to plug into a wired DS. Enhancements might needed to be added to do things like tbs in an adhoc system, but we need to realistic about what services we need to provide.
John Eng: what about data collection?
Ken: much of the performance limits in data collection are not strict. Using the async service is good enough for them in many cases. It is important to offer a reliable isochronous service for voice, which is the primary aim of this service.

Data Compression, IEEE P802.11-93/29, by Frederic Bauchot

Suggests optional compression as part of the MAC protocol, this is meant to open discussion more than to actually specify a solution. Suggest we should leave the hooks in for compression.

Wim Diepstraten: the payload of the upper layers could be compressed. Isn't that independent of the MAC?
Frederic: the wireless segment may be slower than the wired segment, we could use data compression to hide this.
Ken Biba: agrees with compression as part of the MAC. The challenge at upper layers is that the entities at the two ends are not the same. For the wireless segment we may have a lower speed segment so this is a good place to handle this. Supports more than just the hook, specify it.
Dave Bagby: the use and need for fragmentation has been discussed too. You never know how much you can compress the data so this implies the use of fragmentation too. Why propose as an option - if its good why not do it all the time?

Frederic: end user's choice - he may have compression at a higher level already. If you compress compressed data it expands, so the user may need to turn it off.
unidentified: why MAC and not MAC management if it is an option?
Frederic: the MAC must be the guy who does it. It may be set by the management.
Greg Ennis: side benefit of reducing the size of the packets is good too, due to the expected error rates.
Wim: example suggests collecting 3 packets and sending them in one frame. Is that the goal, or should you send an MPDU and compress it and send a smaller packet?
Frederic: if the layer above the MAC is delivering to you at a rate that allows you to package them together is just less work for you to do.
Wim: factor of 3 - is that really possible?
Frederic: picked 3 just as an illustration. It is difficult to estimate - it depends on the data and on the algorithm.
Ken: considering small sizes plus LAN data does not compress well, the improvement may only be 10 to 30 % - this is still a pretty interesting improvement.
Tom Siep: have to specify algorithm to ensure interoperability too.
Frederic: some kind of id specifying what algorithm you are using. Further work must be done there.
Dave B: might want to it turn off as you said earlier - that doesn't make it an option. All implementations have the ability to use it, but you need the ability to turn it off. Open an issue of do we do data compression at the MAC, and do we have to specify the algorithm. If you specify the algorithm then you know the best you can get.
Phil Belanger: in general this could improve performance and allow effectively higher bandwidth, but what about transfer delay?
Frederic: don't know. Believes the compression you will get will compensate, but has no facts.
Leon Scaldeferri: comment - if you have privacy, you have to cipher after you compress. So if 802.10 is above, you have considerations.
Wim: transfer delay in certain protocols could translate to some slower stations than others. Short control packets could wind up with a negative compression, so you would want to turn compression on/off on a per packet basis.
Simon Black: that is a good reason for doing it apart from the MAC - maybe above security layer perhaps. That would skip the MAC control packets.
Frederic: a good compression for large packets is desirable. If compression on a packet basis puts a lot of burden perhaps you need a limit on the size of packet you will compress.
Dave B: the intent is to compress only the payload.
Ken: algorithms almost never do negative compression - there are algorithms that are responsive to that. There is a lot of work being done in this area particularly in the disk saving basis.
Greg: watch out for patented compression algorithms.
unidentified: has found in research that below 108 bytes you gain nothing when you account for the average processing delay.

ATM Cell Base Access Method for Wired and Wireless Local Distribution,
IEEE P802.11-93/24, by Chandos Rypinski

Discussion:
Wim Diepstraten: in the ATM networks you know there is no clock issue?
Chan: there is usually a bearer.
Ken Biba: if each station has an individual point to point connection to a switch, there is no miultidrop. So there is another difference.
Chan: two ended link = absence of multidrop. Yes.
John Eng: small packets can be sent efficiently?

Chan: there are a lot of ways to do it. You have to assume how long it takes to acquire clock. Assumes something less than an octet.

Phil Belanger: scope of a request is for a call, or connection - what size transfer?
Chan: for stations originating packet or connection the contents of the packet differ. You are requesting to use the media and there may be contention on the request - a low probability but not an impossible event.

Wim: MAC payload is 48 bit cell?
Chan: for externally destined cells.
Phil: for external you transmit only the ATM payload, not the ATM control information.
Chan: not using the isochronous ACF field which is one octet, but everything else.

John: would this *not* work for 1 mb, since you said 16 required?
Chan: yes. The access delay is a function of medium rate. As bandwidth of the channel gets close to the bandwidth of the circuit you are trying to provide you have no way of gauge access delay. The aggregate demand for circuit capacity must be a minor fraction of access delay to the medium. For multi-media support you must have up to primary rate (2 Mb). You must sustain multiple connections, and packets at the same time and organize all that.
John: even for just voice traffic?
Chan: delay is critical for some, less so for others. There is no such thing as too much transfer rate.
Wim: you are saying that we should have a MAC which would be ATM based as a primary approach. This eliminates a lot of PHYs which can't provide the required 16 Mb.
Chan: FH would have a lot of problems with my assumptions. High capacity is restrictive and limiting.
Dave B: raising the floor on the capacity - saying 1 to 16 is not acceptable - is a problem.
Chan: anything with a rate of under 16 Mb is unacceptable in my view. If this group wants to make a 1 Mb PHY, they should loose any illusion that that meets the general need for multimedia - 4 Mb is not even in the ballpark.
Dave B: we are trying to create a MAC that works with several kinds of PHYs. If the PHY group came back and said we can provide a reasonable PHY that meets this requirement, choosing a MAC that says this would be acceptable.
Chan: the access method will work at any speed. But the access delay for connections makes it un-marketable.
John: so if specification says certain access delay results in certain throughput, that should be acceptable.
Chan: yes.

Francois: with respect to the diagram on page 3, where is your ATM layer?
Chan: not shown in this diagram. MAC deals with the VCIs, it is not constrained to be ATM within, only at the edges.
Francois: above ATM there is the adaptation layer which provides multiplexing functions as well as assembly and re-assembly.
Chan: we can transport ATM cells and control the access to the medium in an appropriate and convenient way.

Note that nothing about this precludes direct peer to peer. In a good system what AP was used to communicate is not important.

There was a discussion of how many ATM venders there are now, and a conclusion that the important thing is how many will there be when we're finished. There is a lot of interest in ATM in the market today.

Chan has quit e a few reference papers, including ATM published descriptions and Chan's older papers. See him if you're interested.

Comparison of Regular & Asynchronous Time Division Multiplexing of Wireless PHY, IEEE P802.11-93/26, by Chandos Rypinski

Why it was written - time slotted media have been proposed. A whole asynchronous medium is Chan's preference.

The right time to begin a new message is when the last is finished. The length of a message should be the length it requires.

Access status is perishable and should be used as soon as possible after its created. Time slotted mediums are not acceptable.

Fair Control in Contention-Based MAC for Wireless LANs, IEEE P802.11-93/35, by Yoshihiro Takiyasu

Addresses how to solve the unfairness due to the near-far problem of stations using the BLMA protocol. To overcome this problem employ request cycle method. First base station declares request cycle by transmitting request cycle id in the frame control slot at the top of the frame. Station which has data to transmit reserves some bandwidth from the base station. The station can reserve bandwidth up to the window size - the total number of fragment blocks one station can reserve in one request cycle. The base station judges, uses carrier sense in the request indication slot. The station with data to send requests by sending any pattern in the request indicator slot.

Greg: request slot period is slotted ALOHA - what happens if no requests get through due to collisions.
YOSHIHIRO: carrier sense is available so base station knows active stations exist, so the base station compensates next time.

More time will be allocated for this paper at the next meeting if people have questions after they have had a chance to read it.

On the GRAP - A Proposed MAC Protocol, IEEE P802.11-93/39, by KC Chen

This paper is a summary of how the GRAP protocol meets the 21 (20) criteria.

Some highlights:

- The purpose is to divide the stations into groups, so the number of stations competing for the channel is reduced. Time-bonded services (tbs) can go into each group. How to divide into groups - based on a random number.
- If a stronger transmitter exists, he will shift from group to group based on the random number, so he will not dominate the same group of stations everytime.
- Overlapping BSS's - no handoff is needed, it is inherent (unless you're doing tbs).
- Transparency to different PHYs - random address on different PHY transmissions.

More time will be allocated for this paper at the next meeting if people have questions after they have had a chance to read it.

Meeting adjourned: 5:45 PM.

Thursday AM, March 11, 1993

Meeting called to order at 8:40 AM, by chairman Dave Babgy. Carolyn Heide secretary.

Intro to 93/33. we need evaluations of mac proposals about how the mac does the things we need to do, and what are the short coming, the areas that might have problems. we need a rational evaluation technique.

also need to be issues evaluation at the end of this AM.

802.1 MAC Requirements & Comparison Criteria, IEEE P802.11-93/33, by Wim Diepstraten

Required MAC services

Simon Black: what do you mean by voice?
Wim: compressed voice.

Tom Baumgartner: would have thought that support of isochronous and asynchronous traffic on the same channel would be mandatory?
Wim: this is a checklist to verify that.
Tom B: is there is difference between "mixed" and "co-exist" in your use?
Wim: coexist is units that only support asynchronous service coexisting with those that support isochronous.

Support infrastructure based multiple cell networks

Dave Bagby: peer to peer?
Wim: distinguishes peer to peer and direct peer to peer. Peer to peer can be through an AP, direct peer to peer cannot.
Dave B: "station to station" would be more clear ("peer to peer" being a loaded phrase).
Phil Belanger: not sure 3rd point is a MAC requirement. That may be an implementation requirement of a product built using the MAC.
Dave B: we would be interested if a MAC precluded this.
Leon Scaldeferri: all the answers on a checklist do not have to be "yes".
Carolyn Heide: the word "requirements" in the opening paragraph should be changed.

Tom B: this document will replace the famous 21 criteria?
Wim: looked at those 21 criteria in making this list, didn't call them out specifically.

Infrastructure considerations

Dave B: the case opposite to 1st point - which would be "can any non-802 LAN be used as a Distribution system" - may be relevant also.
Phil: this brings up the address space question.
Francois Simon: if it is a requirement to have infrastructure support, we have worked hard to specify the things required from the infrastructure too.

Dave B: it may be easier to say 'have any assumptions about the DS been made' and 'are there any requirements from the DS that are made that we have not made already' when evaluating a MAC. What assumptions are used is the real question.
Simon: that is general though. Somehow a wireless station needs to learn about what DSS are provided.

Dave B: point 5 - those objects reside within the DS, you may not have any way of knowing what, or whether, those things are.
Wim: the question is not what is there, but are you providing information that may be needed.
Phil: what you mean is 'does the mac restrict the way you can do implementations in a complicated world across routers and bridges'.

Dave B: point 6 - what you really want to know is have they made any assumptions about what the DS has to be.
Bryan Hartlen: do you have any questions/requirements about throughput expectations within a single BSA? Some kind of efficiency level expected?
Wim: we did have some about MAC to MAC.
Dave B: looking for people to provide us information, rather than setting a target.
Simon: to be able to compare MAC to MAC you need standard channel models set up.
Dave B: things like what kind of performance do you expect and under what circumstances.
Simon: standard assumptions about a PHY and a traffic load are needed to evaluate these. We will get MACs we can't compare, because they have different weak and strong points.
Tom B: one that we could put in now is some overhead versus payload criteria.
Dave B: too early for such detail.

MAC should be able to operate in a multichannel environment

Phil: are you implying that there might be a different algorithms in multi than single?
Wim: there could be.

Support of adhoc networks

Dave B: the definition of adhoc does not mean infrastructure or not, but how easy it is for them to come into existence.
Wim: what we have said previously was you shouldn't have to bring in extra equipment to make it happen - stations themselves are enough.

Leon: in point 43 - by connected you mean associated?
KS Natarajan: the first question is whether you can be, the second is whether you want to be.
Dave B: think of this as a list of things we would like to know, as opposed to a list of requirements which the MAC must perform.

KS: is the point about power savings unique to adhoc?
Dave B: same with the next point, security.
Phil: some of those features may require infrastructure, so how do you provide those in the adhoc mode too is relevant.
Dave B: sees it the other way round, this is a general requirement, but are there cases where you don't support it, such as in the adhoc case.

MAC must support low power operations

Dave B: might want to check phrasing - perhaps use 'what is the provision for ...' rather than 'must'.

MAC need to support multiple PHYs

Wim: may have to do some active things to support some PHYs, so the list is here as food for thought.
KS: we can't evaluate against things that don't exist yet.

MAC Access Function Requirements (i.e. Characteristics)

Dave B: also, is there any policy assumed by the MAC about what balance it makes between asynchronous and isochronous traffic. Or is it independent of the MAC and set separately. Some MACs have implicit that one kind of traffic can starve out another, others say you can go to either end of the scale as you choose.

Access Method Independent Features

Phil: in point 4, did you have in mind anything other than security functions?
Wim: yes, for instance bridge functionality.

Conclusion

KS: priority of these items as far as MAC meeting them?
Wim: this just a checklist.
Dave B: this is a way to ferret out information about a MAC. Even if we call it a checklist it is not a case of grading the amount of checks. We invite and encourage MAC proposers to bring input on what is great about their MAC, what isn't, etc. If not, we may break into groups and decide these things about individual MACs ourselves, with the help of the authors if they're present.
Francois: what are you looking for from the MAC proposers?
Dave B: for instance on an issue like 'how fair is the access method', maybe be paragraph that says 'I believe it is very fair because it works in the following way and under these conditions everyone is happy'. Phil's statement, in his presentation, about assumptions made (e.g. voice, not video) and the statement if you want to go beyond that you might need to do more, was a very good example of the information we need.
Tom B: since this document is to be edited anyway, it should be checked against the 21 criteria.
Phil: what about the harder step of turning some of these items into functional requirements - when will we update the functional requirements document.
Dave B: as we take a position on issues, some of those issues are about functional requirements. Closing issues adopts requirements.
Phil: there is a level of frustration trying to show requirements conformance, because the requirements don't give much meat to write about. Taking the next step would be nice. There's a subset of things Wim discussed which could be made to be reasonable requirements.
Dave B: someone could bring a list of things that they think are hard requirements which should be adopted.

General Business

(1) Issue processing and closing

[sec note: you may say as you read this, this would be a lot easier to read if the secretary put the issue text in here as well as the number. You're right, it would be. However, I purposely didn't do that because you should get out your issue log while reading this section and have the issue's history in front of you to help you understand the decisions reached here.]

Issue 5.3b

Document 93/22R1 will be circulated it is 93/22 with changes as agreed upon Tuesday PM.

Motion #1: **To split issue 5.3b into sub issues:**

5.3B: Distribution, Association, Disassociation, Reassociation. Closed per 92/22R1.

5.3C: Authentication, Privacy, Integration, Network Management. Still Open.

Moved by: Dave Bagby
Seconded by: Simon Black

Motion Discussion:

Phil Belanger: reassociation - is that what we talked about at last meeting?
Dave B: a description of the functions you need, does not say implicit or explicit.
Paul Eastman: very broad state diagram?
Dave B: conceptual description, from the stations point of view. Very informal, not non-deterministic.
Tom Siep: adoption of this means that we have to support pre-authentication in re-association?
Dave B: no, the intent is not that you *have* to.
Tom S: someone is going to take that diagram and not look at the supporting text which says that.
Dave B: text must go to the editor for the draft standard when issues are closed. I will do this for this issue.
Bryan: acceptance of this means accepting all addressing done in a tuple format?
Dave B: yes. Architecturally you could make short cuts, but that function is what is intended.
Bryan: does this exclude acceptance of non-tuple implementations?
Dave B: I believe this is the most general architectural solution. An implementation that only understood 48 bit Ethernet addresses would still fit this criteria, but be very limited. Depends on placement of bits in the MAC.
Phil: big fear of the tuple is are you creating a new MAC header field by agreeing to this motion.
Dave B: confident the answer can be no because data moved by the MAC is all within one color of the diagram. On the input side of the AP came from the WAS space. How the integration services get worked out I'm not quite sure.

Approved: 12 Opposed: 0 Abstain: 3 *Motion #1 passes*

Issue 6.2

Motion #2: **accept recommended answer of no (ref 93/28).**

Moved by: Leon Scaldeferri
Seconded by: Tom Baumgartner

Motion Discussion:

Frederic Bauchot: what does "support" mean?

Leon Scaldeferri: 'perform' means it does it. 'support' means a piece of data is passed to the PHY, or something needs to come back from it, for the service to be performed. The MAC is able to do whatever we need to do and the PHY knows nothing of it.
Dave B: last time we talked about the possibility of the PHY doing the encryption. The intent here was that the PHY doesn't have to take any specific action to facilitate.
Leon: on the issue sheet we can explain what we meant by support.

Approved: 16 Opposed: 0 Abstain: 1 *Motion #2 passes*

Issue 6.3

Motion #3: **To clarify and move the issue to the performance section.**

Moved by: Leon Scaldeferri
Seconded by: Dave Bagby

Motion Discussion:
Wim Diepstraten: what is unauthorized - unauthenticated?
Leon Scaldeferri: authorization is the result of authentication.
Dave B: where would we put the issue?
Carolyn Heide: Is a person constantly asking to authenticated a source of interference?
Francois Simon: suggests that constant repetition of authentication requests affect performance, so that section 9 is the right place for this.

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

Issues 6.4, 6.6, 6.7 & 6.8

Wim: compression also impacts security considerations - there is interaction between compression and security, and where both are done.

Anyone interested in these issues should do their homework and read the 802.10b SDE standard.

Issue 4.4

Motion #4: **take the position yes.**

Moved by: Phil Belanger
Seconded by: Leon Scaldeferri

Motion Discussion:
Wim Diepstraten: does this imply independence of any PHY - overlapping networks on the same channel.
Dave B: can't answer that question from this issue. It may be an absolute requirement that an adhoc must exist with an infrastructure.
Chandos Rypinski: function of necessity, method is not implied.
Tom Baumgartner: word 'support' - does it means certain cases but not every conceivable case.

Bryan Hartlen: must understand if this means on the same channel or not. Support of multiple BSA a on the same channel is an important requirement.
Tom Siep: assumed coexist meant same channel or there is some impact on the infrastructure. Should add that the infrastructure may have the ability to preclude that - it should be able to prevent extra unregulated traffic.
Dave B: if we're talking about channels which have no interaction there is no issue here. We are constrained to work with a single channel PHY.
Tom S: if the infrastructure is the owner of the space it should be able to preclude the adhoc network. Maybe that's a different issue.
Leon Scaldeferri: the argument of owned space - if this is unlicensed no one owns it. There may be an issue of coming into a used area and being polite.
Tom B: this is not another issue, the whole point is the adhoc and the infrastructure coexisting. If it is another issue we must vote no on this one
Carolyn Heide: Tom Siep is talking about a possible implementation of one solution to this issue (adhoc and infrastructure coexisting by way of one shutting down the other).
Dave B: people do not own spectrum, just because they the space inside their building. You could be in the park across the road with an adhoc network and have a non-RF secure building trying to shut it down.
Phil Belanger: this is a broad issue. Adhoc and infrastructure is not the only case here, there cab be multiple adhocs and multiple infrastructures too. All of those must be supported or considered by the standard. Tom Siep brought up an interesting mechanism and it should be considered. But we must answer yes to this issue.
Tom S: retracts his previous suggestion, everything we do is etiquette, there is no enforcement.
Chan: there are several aspects to the solution. Quite a bit can be done by the physical medium. The most important thing is if the aggregate requirement by the users is a small fraction of the channel capacity they can coexist. If they only interfere 10% of the time the recovery mechanism will take of it. We need to pick protocol that can live with lost transfers.
Tom B: 'support' should not be constrained to mean guarantee. The list of coexisting things that Phil made also includes different PHYs (i.e. DS and IR) - this is another dimension.
Wim: supports phil - this should be yes without restrictions to support adhoc in the presence of an infrastructure.

Motion #5: **To table this motion.**

Moved by: Tom Siep
Seconded by: Tom Baumgartner

Motion Discussion: none

Approved: 6 Opposed: 7 Abstain: 2 ***Motion #5 fails***

Paul Eastman: the motion (#4) itself doesn't say very much. It just says we have to consider it. That's not very contravertial. Calls the quest, secondec by Carolyn Heide (10,0, 2)

Approved: 16 Opposed: 0 Abstain: 0 ***Motion #4 passes***

Issue 4.5

Motion #6: **to take the position no.**

Moved by: Phil Belanger
Seconded by: Tom Baumgartner

Motion Discussion:
Wim Diepstraten: can see that you might want to do this - communicate with guests and get at my files on the wired LAN at the same time.
Phil Belanger: this is a good example, but it not necessarily mean being a part of both at the same time. Your MPDU belongs to one network or the other - when communicating with the wired LAN you're a member of one network, when with your guest, another. You are never both at the same time.
Wim: maybe the question is 'should a station be able to be associate with both an infrastructure and an adhoc at the same time'. More specific than the destination of individual MPDUs.
Phil: at the MAC layer there is not the need to be associated with both networks at the same time.
Tom Siep: what is the actual affect of this? What your destination is determines this, if you're a good citizen you could do both. Can't think of any extra burden on the MAC to do both.
Leon Scaldeferri: setting up two associations is the question here. There are some security threats that exist with a dual association.
Dave B: is concerned about having multiple associations. Might be able to make it work in this particular case (adhoc and infrastructure at the same time), but is concerned about multiple infrastructures overlapping. Can traffic flows be made right with overlapping CFs.?
Carolyn Heide: it is premature to say no - if someone can come up with a MAC that does both elegantly why would we preclude it. Is opposed to the motion.
Wim: agrees - are there currently reasons to apply this restriction. It is an un-necessary restriction.
Tom Siep: retracts earlier statement. Opposed to the motion.

Approved: 9 Opposed: 8 Abstain: 0 *Motion #6 fails*

Issue 5.4

Motion #7: **to take the position "MAC".**

Moved by: Dave Bagby
Seconded by: Tom Baumgartner

Motion Discussion: none

Approved: 13 Opposed: 0 Abstain: 0 *Motion #7 passes*

Issue 5.6 - this is still controversial, no discussion at this time.

Issue 5.9 - straw poll indicates this is still controversial, no discussion at this time.

Issue 17.3 - straw poll indicates this is still controversial, no discussion at this time.

Issue 19.2

Dave Bagby: agrees with intent but is upset about the wording. Intent is to provide a delivery service reliability which will not upset levels above us, but we have an expectation about bit error rate in the PAR.
Tom Baumgartner: interprets delivery reliability to be something not in the MAC's purview anyway. Reliability didn't mean bit error rate in the first place.
Paul Eastman: whether this means reliability in a given period of time, as opposed to the reliability of the data that you get through, the undetected bit error rate still has to remain extremely low. Does this issue mean the reliability of being able to send a message or the reliability of the message itself?
Phil Belanger: understanding what we mean should mean getting the wording right - that is what we have to do in the future.
Bob Crowder: the wording in the PAR is sufficient for this issue.

(2) Overview of report to be made to the Full Working Group

Dave gave it.

(3) Objectives for next meeting

- new MACs still welcome.
- primary focus on evaluation of MACs.
- small groups to focus on sections of issues returning to full MAC group with recommendations for closing or re-wording.

Carolyn Heide suggested that although it is difficult to impossible to get documents to Vic in time for the pre-meeting mailings, it would be nice if people could try hard to do so. Documents can be reviewed faster and better if they have been read beforehand.

Meeting adjourned: 12 noon.