Extending B3 frame formats to include WDS support.

Revision 1.0

David Bagby
Bob O'Hara
Dave Roberts

Advanced Micro Devices
One AMD Place
Sunnyvale CA, 94088

Summary of proposed changes.

- Functionality:
  - Connectivity combinations
- Performance:
  - Header lengths
  - Duplicate detection / Miscorrelation
  - Frame filtering
- This presentation will comment on each of these subjects.

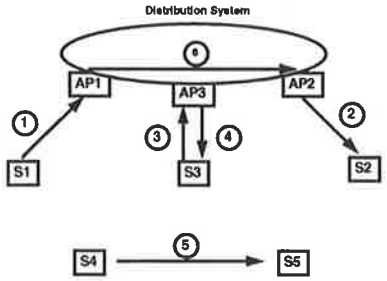
Guidance from August 94 meeting:

- Get functionality correct as highest priority.
- Efficiency improvements follow functionality in priority.
- Using this guideline, this paper analyzes functionality first, performance improvements second.

Connectivity cases:

- 10 connectivity cases:
  - 5 cases from 236
  - 5 additional cases

B3 Connectivity cases.



Additional cases

- Committee discussion has been using loose terminology, resulting in less than optimum analysis.
- Stricter terminology and attention to notational detail are required to correctly understand all the cases.
- Therefore, the first step in the analysis is to establish more precise terminology...

Terminology problems:

- STAn has been used to describe both a station and a station's address.
- APs, and their address are described as APn.
  - This obscures the fact that APs ARE Stations.
  - This obscures the fact that APs straddle two logically different address spaces.
    - » The two address spaces could physically be the same.

Terminology problems:

- The loose english concepts of "within a BSS", "within an ESS", "a member of a BSS", "associated" and "in the same physical volume" have been used interchangeably.
  - This has caused much confusion among members.
  - There are several of these cases depending on how the loose terms are interpreted.

Let's get more formal in terminology.

- Maddr(sta) == 802.11 MAC address of a STA.
  - This can only be a wireless medium address as that is the only address space used by 802.11.
  - This notation is for 802.11 stations.
  - This covers both STAs and APs, since APs are addressable STAs within the 802.11 MAC address space.
- DSaddr(sta) == the DS address of an AP.
  - This is the address used by the DS to address the DS side of an AP.
  - The details of the DS address space are dependent on the DS implementation and outside the scope of 802.11.
  - The single DS implementation that 802.11 impacts is when a DS is implemented using an 802.11 wireless medium.

B3 notation:

- B3 uses the following concepts:
- SA = source address
- DA = Destination address
- VIA = the address of the (single) AP which is a member of a specific BSS.
  - This name was changed to BSSID during the August meeting.
- "To bit": indicates if a frame was "to" an AP.
- "From bit": indicates if a frame was "from" an AP.

The connectivity categories:

- Infrastructure cases
- Independent BSS ("Ad-Hoc") cases
- Wireless DS cases
- Mixed terminology cases

Infrastructure cases:

- Case 1: STA to STA, via DS; first link
  - Example: Frame from S1 destined to S2, entering DS via AP1
- Case 2: STA to STA via DS; last link
  - Example: Frame from S1 destined to S2, exiting DS via AP2
- Case 3: STA to AP; frame destined for AP
  - Example: Frame from S3 destined to AP3
- Case 4: AP to STA; frame originated by AP
  - Example: Frame from AP3 destined to S3

Independent BSS ("Ad-Hoc") cases:

- Case 5: STA to STA direct.
  - Example: Frame originated by S4 destined for S5.

Wireless DS case:

- Case 6: AP to AP, distributing (a case 1 or 2 frame) via the same (i.e. in-band) wireless medium as that used for either the first OR last link.

Mixed terminology cases:

- "Overlapping", "within", "when a member of" etc.
- More later, after we have examined the concepts that are being intermixed...

Separate overloaded concepts

- Analysis of case 6 points out that we are still mixing concepts and overloading different concepts onto address fields.

Architectural "transit points":

- Originator of a frame.
- Terminator of a frame.
- Transmitter of a frame.
- Receiver of a frame.

Architectural "transit points":

- The term "source" has been used to refer to both the *Originator* and the *Transmitter* of a frame.
- The term "destination" has been used to refer to both the *Destination* and the *Receiver* of a frame.
- Confusion occurs because we do not always mean the same thing by "source" and "destination" in all cases.
- This is probably because our brains have been constrained by thinking about networks with zero levels of indirection.
- The 802.11 architecture is a 1 indirection level system.

Architectural "transit points":

- In the Ad-hoc cases:
  - Originator = Transmitter = "source"
  - Terminator = Receiver = "destination"
- Infrastructure cases:
  - The VIA concept in B3, is a recognition that in transiting an ESS, "receiver" does NOT always equal "terminator".
  - Case 6, also points out that if you have a WDS, "originator" does not always equal "transmitter".
    - » This leads one to introduce the concept of "RA".

Let's name these different addresses.

- Let [variable] == the value of "variable";
- [SA] = Maddr (of the STA which originated the frame).
  - This is consistent with the term SA as used in other 802 standards.
- [DA] = Maddr (of the STA which is the final destination of the frame).
  - This is consistent with the term DA as used in other 802 standards.
- [RA] = Maddr (of the STA which is intended to receive the frame off the 802.11 wireless medium).
- [TA] = Maddr (of the STA which placed the frame onto the 802.11 wireless medium).

Frame direction wrt DS

- 802.11 has also found it necessary to specify the direction of a frame with respect to the DS.
- This is done by bits in the FC field of the frame header.
- "To bit" == Frame is entering the DS from the wireless medium via an AP.
- "From bit" == Frame is exiting the DS via an AP onto the wireless medium.

Frame direction wrt DS

- The truth table for these bits is:

TO	FROM	Meaning
False	False	"Direct, not via a DS"
False	True	"Frame outbound from DS"
True	False	"Frame inbound to DS"
True	True	"Frame wirelessly distributed"

- The concept is not to / from an AP.
- The concept is to / from the DS.
- We should correct the names of the bits:
  - "To AP" is changed to "To DS"
  - "From AP" is changed to "From DS"

Consider cases concepts separated out...

- Before optimizing the addressing needed for each case, we must clearly understand which address is needed for each case and why.
- Note: A claim that four addresses are needed in every message is *not* going to be made.

Independent BSS ("Ad-Hoc") cases:

- Case 5: STA to STA direct.
- Example: Frame originated by S4 destined for S5.
  - [SA] = Maddr(S4)
  - [DA] = Maddr(S5)
  - [TA] = Maddr(S4)
  - [RA] = Maddr(S5)
  - [To] = False
  - [From] = False

Infrastructure cases:

- Case 1: STA to STA, via DS; first link
- Example: Frame from S1 destined to S2, entering DS via AP1
  - [SA] = Maddr(S1)
  - [DA] = Maddr(S2)
  - [TA] = Maddr(S1)
  - [RA] = Maddr(AP1)
  - [To] = True
    - » Frame is inbound to DS
  - [From] = False

Infrastructure cases:

- Case 2: STA to STA via DS; last link
- Example: Frame from S1 destined to S2, exiting DS via AP2
  - [SA] = Maddr(S1)
  - [DA] = Maddr(S2)
  - [TA] = Maddr(AP2)
  - [RA] = Maddr(S2)
  - [To] = False
  - [From] = True
    - » Frame is outbound from DS

Infrastructure cases:

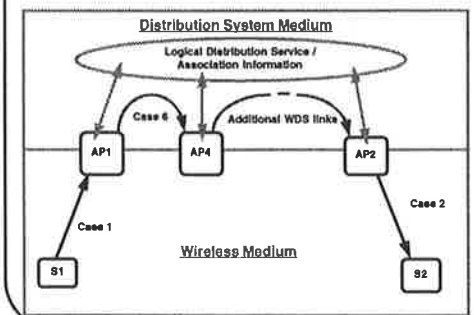
- Case 3: STA to AP; frame destined for AP
- Example: Frame from S3 destined to AP3
  - [SA] = Maddr(S3)
  - [DA] = Maddr(AP3)
  - [TA] = Maddr(S3)
  - [RA] = Maddr(AP3)
  - [To] = False
    - » frame is NOT inbound to DS, it is destined to the AP.
  - [From] = False
    - » frame is NOT outbound from DS

Infrastructure cases:

- Case 4: AP to STA; frame originated by AP
- Example: Frame from AP3 destined to S3
  - [SA] = Maddr(AP3)
  - [DA] = Maddr(S3)
  - [TA] = Maddr(AP3)
  - [RA] = Maddr(S3)
  - [To] = False
    - » frame is NOT inbound to DS
  - [From] = False
    - » frame is NOT outbound from DS, it originated at the AP.

Wireless DS cases

Wireless DS general case



Wireless DS case

- Case 6: AP to AP, distributing a frame via the wireless medium.
- Example: Frame from S1 destined to S2, transiting a wireless DS between AP1 and AP4
  - [SA] = Maddr (S1)
  - [DA] = Maddr (S2)
  - [TA] = Maddr (AP1)
  - [RA] = Maddr (AP4)
  - [To] = True
    - » frame IS inbound to DS from the wireless medium
  - [From] = True
    - » frame IS outbound from DS onto the wireless medium

Wireless DS case

- Note: with all four addresses, it is possible to handle an arbitrary number of WDS hops.
- This provides a general solution for wireless distribution.

Mixed terminology cases

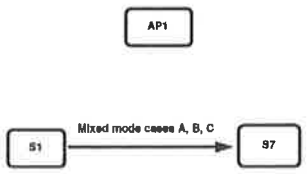
- Many loose terms causing confusion:
  - "Overlapping"
  - "within"
  - "when a member of"
  - "in the same volume as"
  - "Associated with"
  - etc...
- The key concept is Overlapping coverage volumes.

Mixed mode case analysis

- The cases under discussion are those where a STA desires to both make use of the services of an ESS, and also be able to communicate directly with another STA.
- There are 3 combinations which cover the permutations.
- The key is to understand that the state of a STA (with respect to membership in an ESS) is orthogonal to the communication method used for any particular frame.

Let's Consider the mixed mode cases wrt SA, DA, RA, TA, To, & From...

Mixed mode case diagram



Mixed mode case A

- S1 is a member of a BSS which contains AP1 and is Associated with AP1,

AND

- S7 is not a member of the same BSS.
  - [SA] = Maddr (S1)
  - [DA] = Maddr (S7)
  - [TA] = Maddr (S1)
  - [RA] = Maddr (S7)
  - [To] = False
    - » frame is NOT inbound to DS from the wireless medium
  - [From] = False
    - » frame is NOT outbound from DS onto the wireless medium

Mixed mode case B

- S7 is a member of a BSS which contains AP1 and is Associated with AP1,

AND

- S1 is not a member of the same BSS.
  - [SA] = Maddr (S1)
  - [DA] = Maddr (S7)
  - [TA] = Maddr (S1)
  - [RA] = Maddr (S7)
  - [To] = False
    - » frame is NOT inbound to DS from the wireless medium
  - [From] = False
    - » frame is NOT outbound from DS onto the wireless medium

Mixed mode case C

- S1 is a member of a BSS which contains AP1 and S1 is Associated with AP1,

AND

- S7 is also a member of the BSS which contains AP1 and S7 is Associated with AP1.
  - [SA] = Maddr (S1)
  - [DA] = Maddr (S7)
  - [TA] = Maddr (S1)
  - [RA] = Maddr (S7)
  - [To] = False
    - » frame is NOT inbound to DS from the wireless medium
  - [From] = False
    - » frame is NOT outbound from DS onto the wireless medium

All three of the mixed mode cases are the same.

- Wrt SA, DA, RA, TA, To & From, all three mixed mode cases are identical.
- All three mixed mode cases are also identical to case 5 (direct communication).
- B3 contains confusion when it talks about the address of the BSS, within a ESS of which S1 is a member, and overload this concept with BSSID.
- So let's examine the concept of BSSID...

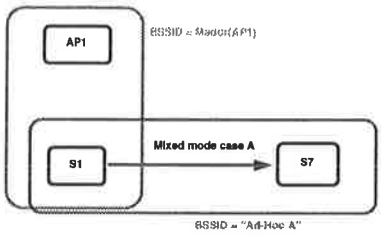
BSSID vs mixed modes

- It is desirable to have a BSSID so that receiving STAs can filter incoming msgs based on BSSID.
  - In particular, there is interest in filtering Broadcast and Multicast msgs.
- BSSID is substituting in our shared media environment for the concept of a "logically separate media".

BSSID vs mixed modes

- The key question: What is the BSSID that should be used for mixed mode cases A, B and C?
- Answer: The BSS that contains both S1 and S7.
- This may or may not be the same BSS which contains AP1.
- Lets look at each case closer...

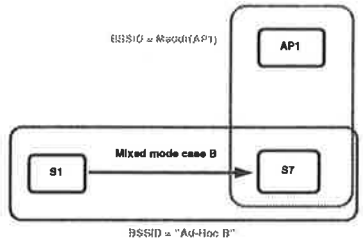
Mixed mode case A



Mixed mode Case A BSSID

- For the frame going from S1 to S7:
- BSSID must = "Ad-Hoc A"
- This is the only piece of info common to both S1 and S7.

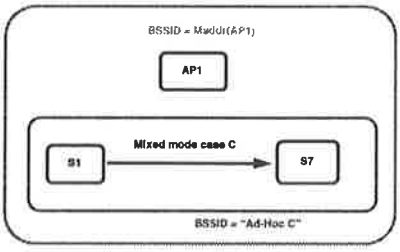
Mixed mode case B



Mixed mode Case B BSSID

- For the frame going from S1 to S7:
- BSSID must = "Ad-Hoc B"
- This is the only BSSID known to S1.
- This is the only piece of info common to both S1 and S7.

Mixed mode case C



Mixed mode Case C BSSID

- For the frame going from S1 to S7:
- There are two choices for BSSID:
  - "Ad-Hoc C"
  - Maddr(AP1)
- Either will get the msg from the source to the destination without causing any problems at an AP.
  - [To] = [From] = False, so APs will not attempt to process the frame.

Direct communication BSSID conclusion

- The BSSID must be that of a BSS of which both the Source and Destination stations are members.
  - This allows both choices for Case C.
- Such a BSS always exists for direct communication cases.
- The choice of BSSID to use for mixed mode case C can be unspecified by 802.11 - either works from the MAC viewpoint.
  - The choice of which to use and/or try first is not of significance to 802.11 MAC operation.

Infrastructure BSSID values

- For BSSs which are part of an ESS:
  BSSID = Maddr(AP).

Using ESSID to find BSSID

- In an ESS, a STA learns about local APs.
- What it learns is { ESSID, Maddr(AP) } pairs
  - Contained in beacons etc
- STAs wishing to join a particular administrative group, pick an AP by using the Maddr(AP) of an AP which belongs to the desired administrative group.

Using Ad-Hoc admin group to find BSSID.

- The BSSID of an IBSS = Maddr(the STA which initiated establishment of the BSS)
- The same mechanism used by a STA to find BSSID from ESSID is sufficient.
- A STA wishing to join an IBSS simply selects a Maddr which corresponds with the desired administrative grouping.

Independent BSSID values

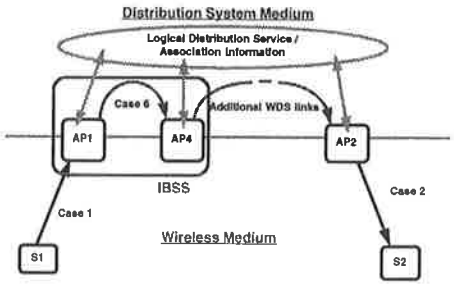
- Conclusion: For Independent BSSs, BSSID = Maddr(the STA which initiated establishment of the BSS).
- This supports as much differentiation between different IBSSs as desired.
- Thus broadcast, multicast filtering by BSSID is provided.

Mixed mode interaction conclusions:

- At any given instant:
  A STA may be a member of zero or 1 ESSs.
  AND
  A STA may be a member of as many IBSSs as it desires.
- Since APs are STAs, this also applies to APs.

WDS components

Logically, IBSSs are used to build WDSs.



Logically, IBSSs are used to build WDSs.

- Two APs must be in direct communication or they can not be used to wirelessly distribute a frame.
- Interestingly, the BSSID of the *logical* IBSS is not required within the case 6 frame.
  - See case 6 frame examples later in paper.
- Only a DS need know how APs are related.
  - (In order to figure out which APs to use to wirelessly distribute a frame).
  - If were needed, the logically correct BSSID for a case 6 frame is the ID of the BSS which contains both AP1 AND AP4.
  - Whether a DS actually does, or does not, set up the logical IBSSs is irrelevant to the 802.11 MAC.
  - Mobile STAs neither need to know, nor care, about these logical BSSs.

Observations about WDS case:

- Case 6 is only required for wirelessly distributed DATA type frames.
- Control frames never transit a DS.
  - RTS, CTS, ACK, POLL
- Management frames never transit a DS.
  - They are always between directly communicating STAs
  - STA to STA in a BBS
  - STA to AP in an ESS
- Only Data frames are ever Distributed and hence transit a DS.

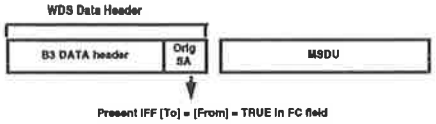
Observations about WDS case:

- Case 6 (WDS) is the only case where all four logical addresses can actually have 4 distinct values.
- In all case 6 "hops", the logical Distribution Service, is invoked.
  - Required in order to access the Association information to determine how to distribute the original frame from S1 to S2.
  - Whether this functionality is implemented within a physical AP is not relevant.

WDS Data frame support.

- We should enable support of WDS.
- Wirelessly distributed msgs are identified by [To] = [From] = true.
- WDS link msgs use a WDS Data header.
  - Provides support for WDS links.
  - Only a small amount of additional information is needed (above a normal Data header) for specific msgs.
    - One address
  - Overhead cost is only paid for msgs that are actually wirelessly distributed.
  - No other msgs have increased overhead.

WDS Data header



Impacts on frame headers:

- Now that we have explored the previously overloaded concepts, lets look at what this means for frame headers...

Header Address field contents for each msg type:

- RTS
  - all examples
    - » [SA field] = TA = Maddr(transmitting STA)
    - » [DA field] = RA = Maddr(receiving STA)
    - » [To DS] = False
    - » [From DS] = False
- CTS
  - all examples
    - » [DA field] = RA = Maddr(receiving STA)
    - » [To DS] = False
    - » [From DS] = False

Header Address field contents for each msg type:

- ACK
  - all examples
    - » [DA field] = RA = Maddr(receiving STA)
    - » [To DS] = False
    - » [From DS] = False
- POLL
  - all examples
    - » [SA field] = TA = Maddr(transmitting STA)
    - » [To DS] = False
    - » [From DS] = False

Header Address field contents for each msg type:

- DATA & Mgt
  - Case 1
    - » [BSSID field] = Maddr (AP1)
    - » [SA field] = Maddr (S1)
    - » [DA field] = Maddr (S2)
    - » [To DS] = True
    - » [From DS] = False

Header Address field contents for each msg type:

- DATA & Mgt
  - Case 2
    - » [BSSID field] = Maddr (AP2)
    - » [SA field] = Maddr (S1)
    - » [DA field] = Maddr (S2)
    - » [To DS] = False
    - » [From DS] = True

Header Address field contents for each msg type:

- DATA & Mgt
  - Case 3
    - » [BSSID field] = Maddr (AP3)
    - » [SA field] = Maddr (S3)
    - » [DA field] = Maddr (AP3)
    - » [To DS] = False
    - » [From DS] = False

Header Address field contents for each msg type:

- DATA & Mgt
  - Case 4
    - » [BSSID field] = Maddr (AP3)
    - » [SA field] = Maddr (AP3)
    - » [DA field] = Maddr (S3)
    - » [To DS] = False
    - » [From DS] = False

Header Address field contents for each msg type:

- DATA & Mgt
  - Cases 5, A & B:
    - (case 5 example shown)
    - » [BSSID field] = Maddr (ad-hoc initiating STA)
    - » [SA field] = Maddr (S4)
    - » [DA field] = Maddr (S5)
    - » [To DS] = False
    - » [From DS] = False

Header Address field contents for each msg type:

- DATA & Mgt
  - Case C
    - » [BSSID field] = Maddr (AP1) or Maddr (ad-hoc initiating STA)
    - » [SA field] = Maddr (S1)
    - » [DA field] = Maddr (S7)
    - » [To DS] = False
    - » [From DS] = False

Header Address field contents for each msg type:

- DATA (WDS DATA support frame)
  - Case 6

    (using 236/B3 field names)
    - » [BSSID field] = Maddr (AP4)
      - is actually RA field
    - » [SA field] = Maddr (AP1)
      - is actually TA field
    - » [DA field] = Maddr (S2)
      - is actually DA field
    - » [Orig SA] = Maddr (S1)
      - is actually SA field
    - » [To DS] = True
    - » [From DS] = True

Header Address field contents for each msg type:

- It is proposed that for the WDS Data header, the fields be renamed to accurately reflect their function.
- The case 6 example would become:

  DATA (WDS DATA support frame)
  - Case 6
    - » [RA] = Maddr (AP4)
    - » [TA] = Maddr (AP1)
    - » [DA] = Maddr (S2)
    - » [SA] = Maddr (S1)
    - » [To DS] = True
    - » [From DS] = True

Header Address field contents for each msg type:

- WDS DATA header field names:

FC	RA	DA	TA	Seq #	Frag #	Dur	SA

Extended B3 Headers

- RTS

FC	DA	SA	Dur

- CTS

FC	DA	Dur

- ACK

FC	DA	Dur

- POLL

FC	BSSID	SA

- DATA / MGT

FC	BSSID	DA	SA	Seq #	Frag #	Dur

- WDS DATA

FC	RA	DA	TA	Seq #	Frag #	Dur	SA

Mixed mode case corrections to B3 section 2 text.

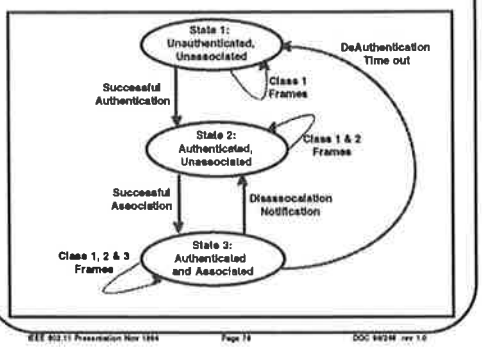
B3 Section 2 State Diagram Corrections

- Now that we understand the mixed mode cases it becomes clear that the transmitting station state diagram in sec 2.5 is incorrect and needs to be corrected.
- The existing states described in B3 section 2 are still correct, but the division of services is not.
- The correct dependency on STA state is sets of allowable transmit frames, not services.
- Any frame can be received at any time, but if not in a correct state at the receiver (e.g authenticated), an error occurs.

Station States

- State 1:
  - Initial start state, Unauthenticated, Unassociated.
- State 2:
  - Authenticated, not Associated
- State 3:
  - Authenticated and Associated.

STA State vs frame types



STA State vs frame types

- Class 1 frames (anytime)
  - Legal from within States 1, 2 and 3
  - Control Frames
    - » RTS
    - » CTS
    - » ACK
    - » Poll
  - Mgt Frames
    - » Probe R/R
    - » Beacon
    - » Authentication
      - Success enables Class 2 frames.
      - Failure leaves STA in State 1.

STA State vs frame types

- State 1 -> 2 transition
  - Successful Authentication frames sequence transitions to state 2.

STA State vs frame types

- Class 2 frames (IFF Authenticated)
  - Legal from within States 1, 2 and 3
  - Data frames
    - » Async data
      - Direct only NOT to/from DS
  - Mgt frames
    - » ATIM
    - » Association R/R
      - Success enables Class 3 frames.
      - Failure leaves STA in state 2.

STA State vs frame types

- State 2 -> 3 transition frames
  - Successful Association frames sequence transitions to state 3.

STA State vs frame types

- Class 3 frames (IFF Associated)
  - Legal from within States 1, 2 and 3
  - Data frames
    - » Async Data
      - Direct and indirect allowed
  - Mgt frames
    - » Privacy R/R
    - » Reassociation R/R
    - » Dissasociation
  - continued...

STA State vs frame types

- Class 3 frames (IFF Associated)
  - CF Frames
    - » CF Data frames
      - CF DATA
      - CF DATA + ACK
    - » CF Control frames
      - CF END

STA State vs frame types

- State 3 -> 2 transition frames
  - Dissasociation: STA now Unassociated, so back to state 2 and Class 2 frames.

STA State vs frame types

- State 2 or 3 -> 1 transition events
  - Current draft assumes Authentication is aged during inactive periods.
  - This can result in "disauthentication" as an error response.
  - Disauthenticaion => Disassocaition, so is back to State 1 and Class 1 frames.
    - (As shown in B3 state diagram.)

Conclusions:

- Motion: That in order to provide WDS support, the extensions and corrections to B3 contained in 94/248 and 94/248A be adopted and that the changes be incoroprated into draft B4.