8. Positive ACK and Duplicate Detection

Broadcast and multicast frames are not acknowledged, and never retransmitted. With that exception ...

Like the WHAT protocol, the Spectrix is a positive ACK protocol, in both operating modes. When a DATA frame is sent the source station expects to receive an ACK immediately following transmission. If an ACK is not received after a known period of time the data is scheduled for retransmission. After N tries the data is discarded and a failure reported.

The goals of the retransmission mechanism are: (1) to minimize retransmission by not re-sending the data when only the ACK was lost; (2) filtering out as many duplicates as possible; and (3) guaranteeing that no data will be mistakenly discarded as duplicate. This mechanism does not guarantee that no duplicates will be passed on to the client protocol.

Retransmission and duplicate detection are accomplished using three single bit flags in the control field of frames. These flags are kept by each station for each station with which they have been in contact, i.e. they describe the point-to-point transfer between two stations:

- The retry bit is zero on initial transmission and one on retransmissions. Note that re-sending an RTS due to not receiving a CTS is not considered a retry - the DATA frame must have been sent for a retransmission to occur;
- The sequence bit is an alternation bit, which can be thought of as a single bit sequence number;
- The out-of-sequence bit invalidates the previous sequence bit. If this is the first data sent from station A to station B, the out-of-sequence bit is set. The out-of-sequence bit is also set after an expiration of the N retry count, because the sender no longer knows the last sequence bit received by the destination.

In the following diagrams, which illustrate the use of these three flags, each frame is followed by the state of the three flags. E.G. RTS(x,y,z) - in this notation x = retry flag; y = out-of-sequence flag; and z = sequence flag.

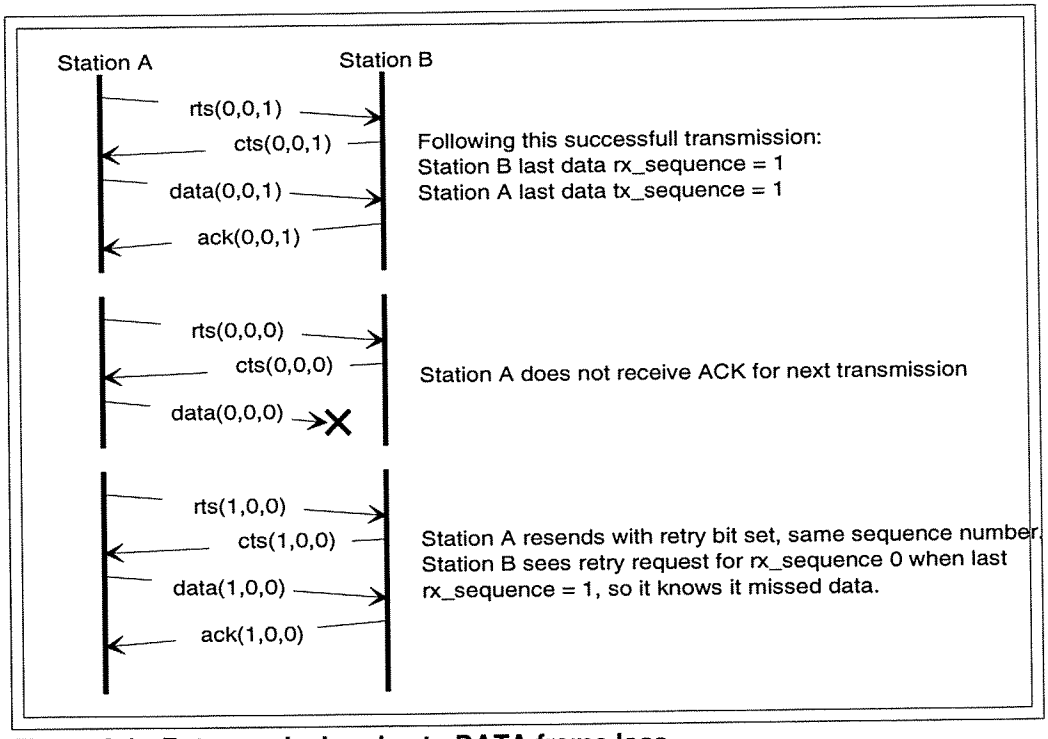


Figure 8.1 - Retransmission due to DATA frame loss

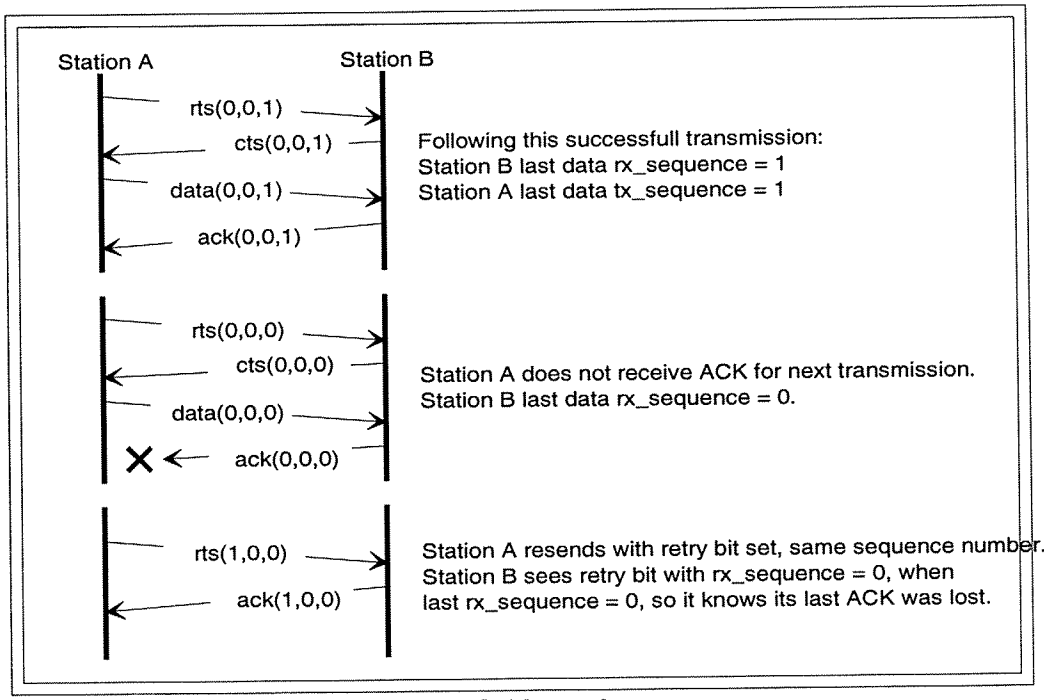


Figure 8.2 - Retransmission due to ACK frame loss

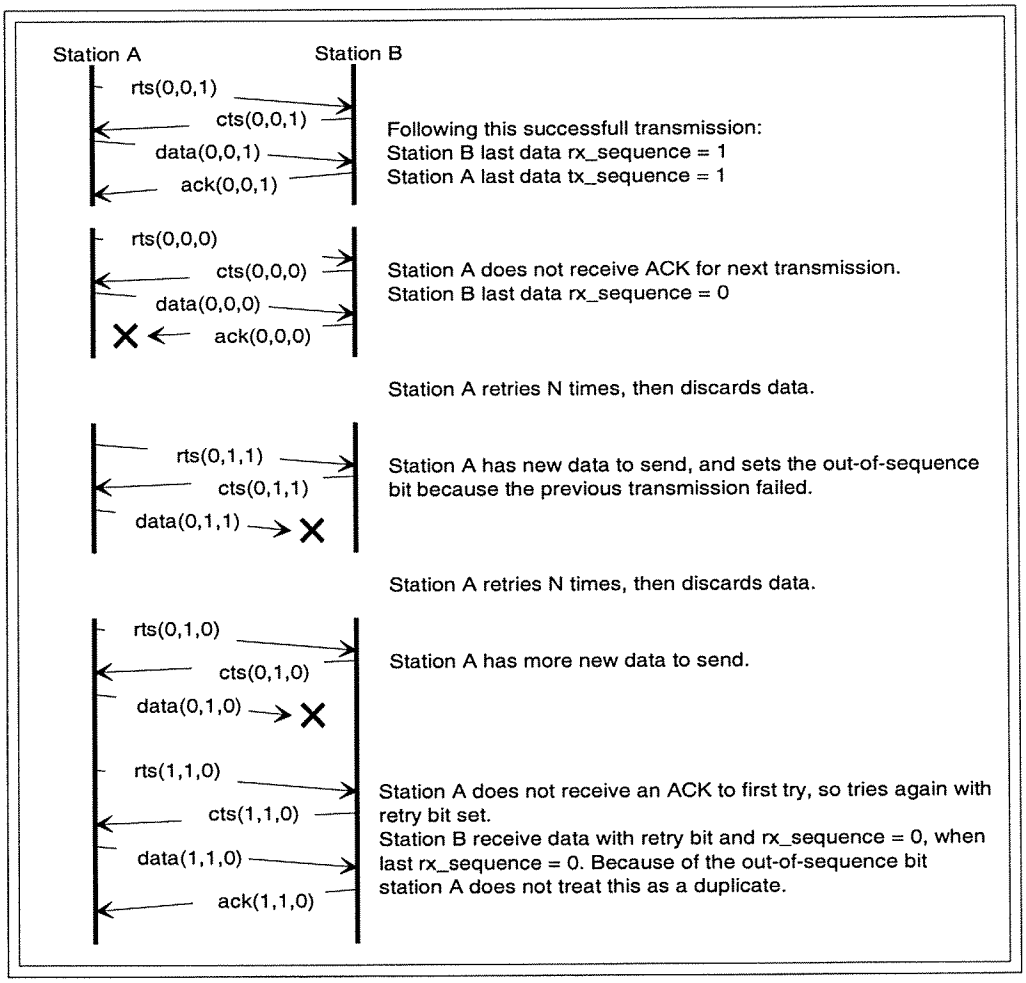


Figure 8.3 - Retransmission using the out-of-sequence bit.

9. Overlapping Operating Modes

9.1. Distributed Mode Station Overlapping with Centralized Mode Station

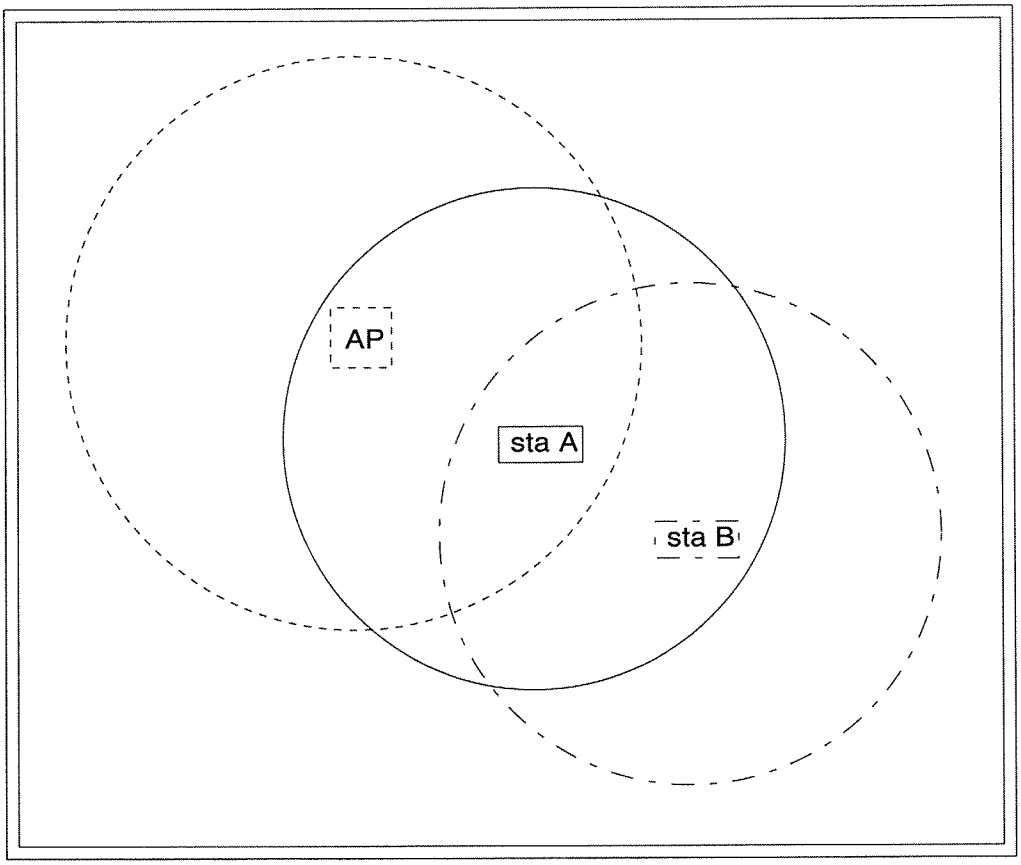


Figure 9.1

In the diagram above, assume that the AP is a controller station, so station A is operating in centralized mode. Station B is not within range of a controller, so it is operating in distributed mode.

Station B is operating in distributed mode, so it is listening to everything that comes from station A. It can tell from the destination ID of request frames from station A that station A is operating in centralized mode. What this means to station B is that when station A issues an RTS the associated CTS and DATA frames are not forthcoming immediately. It has no way to judge when they will come, so it has to consider the medium unavailable until they are seen.

Station B may see the medium as available during the request period, and if station A does not issue a request this is no problem. But if station A does issue a request it may collide with station B's frames, potentially interfering with station B's communication, but not affecting station A's request.

Station B may also see the medium as available during the AP's downward data period, and cause interference with the transfer of data from the AP to station A.

In summary, the performance of both the stations operating in distributed mode and the stations operating in centralized mode will be degraded by this type of overlap. However, although collisions may occur, all stations are still able to operate.

9.2. Overlapping Centralized Mode BSAs

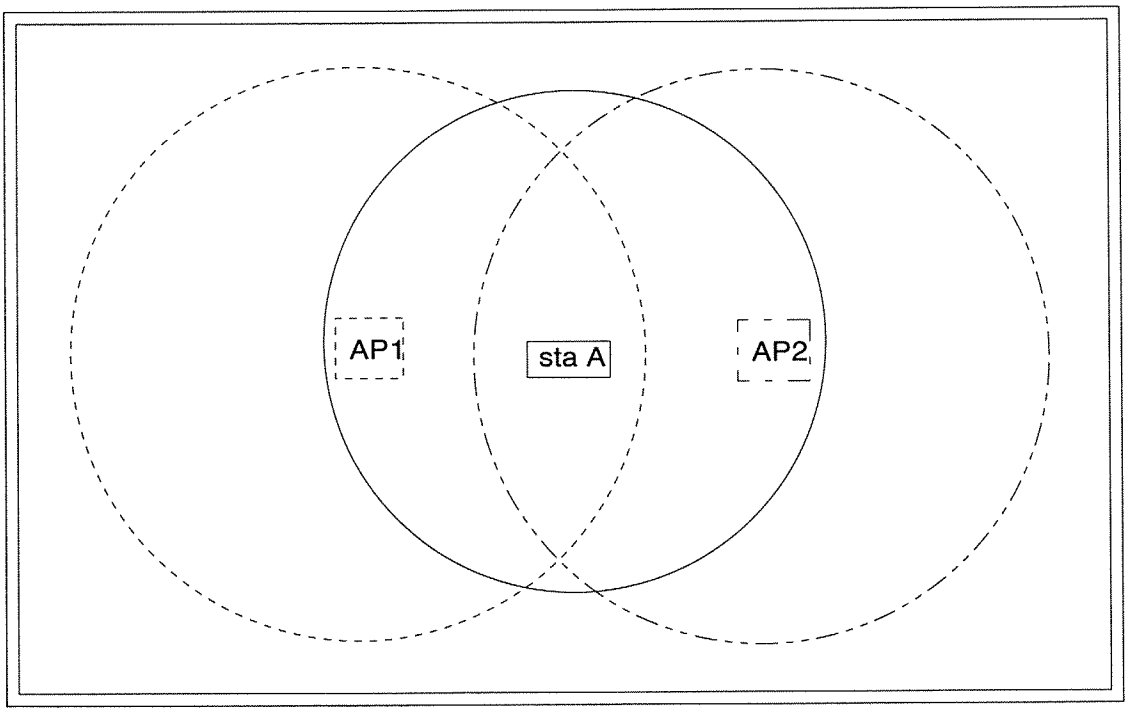


Figure 9.2

In the diagram above, assume that station A came alive, listened, and heard synchronization frames on the same channel from both AP1 which is operating as a centralized mode controller, and AP2 which is also operating as a centralized mode controller.

Station A cannot register with either AP without interfering with communication in the other AP's BSA. Station A could operate in distributed mode, but it will never find an opportunity to capture the media.

The proposed action in this case is for station A to register with one of the APs (causing repeated interference in the other until it successfully does so), with an indication in the registration request of the problem. Once one AP knows of the situation it can take some action. The station can also notify higher layers that it is not able to communicate.

Now assume that station A was already registered with AP1, and moved into range of AP2. This is even worse, because station A may never become aware of the situation. It has its receiver off during AP1's request period, and unless it has something to send, also off in the upward data period. In the downward data period it is most likely only listening to frames which are for it's own DID. So it may not see traffic from AP2's BSA. If it does, it can take the same action as described previously, alerting AP1 and its own higher layers of its inability to communicate. But until then, it is an interferer in AP2's BSA whenever it transmits in AP1's BSA.

10. Possible Enhancements

During the course of developing the centralized mode operation quite a number of suggestions/questions came up. Some yielded ideas which could be incorporated in the protocol, depending on how complicated one wants to make it.

1. "My number one concern is power consumption - I don't want to have to bring my receivers up to receive both the RSYNC and DSYNC, just for the downward data period."

   Fields could be added to the RSYNC to accommodate this, or there could be different frame type called an expanded RSYNC (ERSYNC). The ERSYNC could specify the total time of the request period and upward data period, and stations receiving an ERSYNC would know not to expect a DSYNC.

   The true length of the upward data period is not known at the time of ERSYNC transmission, but power consumption is considered so important that the implementer is willing to sacrifice bandwidth. The controller could always use a fixed length for the upward data period, or it could estimate the length based on previous traffic - this would be up to the implementation.

2. "My number one concern is power consumption - I don't want to bring my receivers up unless I know there is data for them."

   Fields could be added to the DSYNC for this or an EDSYNC frame could be created. The EDSYNC frame could contain a destination map indicating which stations must keep their receivers on during the downward data period. This means that data received from the distribution system to go to stations after the map has been sent must wait for the next superframe - power consumption must be more important than transmission latency (and overhead, because the map could be large!) to implementers using this approach.

3. "I have high population density and/or time-bounded requirement so I want to use centralized mode. But I don't care about power consumption, so I don't want to waste overhead."

   Use an ERSYNC, so you don't have to send the DSYNC. Specify in it that the length of the upward data period is zero, so all receivers will come on after the request period and stay on until the next RSYNC. Then you can mix your upward and downward data as you choose in the data period because all receivers are on.

   Send your DATA frames from the controller without the preceding RTS/CTS, if your desire for saving bandwidth outweighs the possibility of having overlapping distributed mode stations which may need that information to minimize interference.

4. "I want to have AP/controllers communicating over the distribution system so that I can overlap centralized mode BSAs using time isolation. But to save power I want to turn off the receivers in one BSA during the superframe of another."

   Add another type of synchronization frame, a pause sync (PSYNC) which specifies a time length for which receivers of stations registered with the controller sending it can turn off.

5. "It may take more than one IR transceiver (let's say 2) to cover a large room, but we want the room to be one centralized mode BSA. We can't run the two controller's transceivers simultaneously due to multipath interference."

Change the structure of the superframe a little. It is still composed of periods delimited by synchronization frames, but do two RSYNCs and two DSYNCs, each containing the same superframe number. Send an RSYNC from the first transceiver, get the request list from it. Send an RSYNC from the second transceiver, get the request list from it. Use the quality-of-signal information associated with each request to determine which transceiver is better for communicating with which station. Then do a DSYNC from one transceiver and service the stations that have better quality from it, then a DSYNC from the other and service the other stations.

This method has high overhead, because the request period was done twice. The total data period is only longer by one extra DSYNC.

This leads to the conclusion that the superframe can be composed of as many request periods and data periods as desired. The sync frames should contain a superframe number, so that stations know when to retransmit because they didn't get serviced in this superframe.

6. "I expect all my stations to register at the beginning of the day, and none, or very few after that."

When the controller has few stations registered, have a lot of registration slots available. When it has a lot of stations registered, have few or have only every third or fourth request period have any registration slots in it. Or when there are a lot of stations registered have complete overlap between owned and registration slots.

7. "I want the controller to able to know where all stations are at any given time, whether they have communicated lately or not."

Add a mandatory-response RSYNC frame (MRSYNC) and send it out periodically. When a controller issues a MRSYNC frame all registered stations must respond in their owned request slot. If they had not intended to generate a frame in their owned slot they must send a forfeit frame (FORF) there which has no effect other than to note their presence.

This method could also be used to age time slot ownership.

8. "All registered stations own a time slot in the request period, couldn't they send their ACK frame there in the first request period after they receive data from a controller?"

YES - the ACK could be sent at that time rather than immediately following data, and there could be a combined request/ack frame (or a control flag in the request frame). This would definitely save overhead.

BUT - without this enhancement the action of a station on receipt of a DATA frame is always the same (send an ACK frame immediately), regardless of centralized or distributed mode, and regardless of the DATA frame source.

11. Basic Frames

Request Sync

Preamble	
SD	
DID	⇐ Broadcast
Type	⇐ RSYNC
Control	⇐ Control flags: AP, sequence, out-of-sequence, retry, hierarchical
SID	⇐ Station Identifier, ID of originating controller station
TotalSlots	⇐ Total number of time slots in SyncPeriod (including RegSlots)
RegSlots	⇐ Total number of time slots which are for registration only
SuperFrame	⇐ Superframe number
FCS	
ED	

Data Sync

Preamble	
SD	
DID	⇐ Broadcast
Type	⇐ DSYNC
Control	⇐ Control flags: AP, sequence, out-of-sequence, retry, hierarchical
UpLength	⇐ length of Upward Data Period
SuperFrame	⇐ Superframe number
FCS	
ED	

Request To Send, Request To Send Indirect, Request To Send Time-bounded

Preamble	
SD	
DID	⇐ Destination Station ID
Type	⇐ RTS, RTSI, or RTST
Control	⇐ Control flags: AP, sequence, out-of-sequence, retry, hierarchical
SID	⇐ Source Station Identifier
DataLength	⇐ Length, in octets, of data the source wants to send
DA	⇐ Address station to which data is to be sent, 48-bit address
FCS	
ED	

Clear To Send

Preamble
SD

DID	⇐ Destination Station ID
Type	⇐ CTS
Control	⇐ Control flags: AP, sequence, out-of-sequence, retry, hierarchical
CTSSID	⇐ Clear to Send to Station Identifier
DataLength	⇐ Length, in octets, of the data the destination station is to send
FCS	
ED	

Registration Request
Registration (Time-bounded) Request

Preamble	
SD	
DID	⇐ Destination Station ID
Type	⇐ RREG or RTREG
Control	⇐ Control flags: AP, sequence, out-of-sequence, retry, hierarchical
SID	⇐ Source Station ID (registration time slot number)
SA	⇐ Address station registering, 48-bit address
FCS	
ED	

MPDU Data

Preamble	
SD	
DID	⇐ Destination Station ID
Type	⇐ DATA
Control	⇐ Control flags: AP, sequence, out-of-sequence, retry, hierarchical
SA	⇐ Address of data originator, 48-bit address
DataLength	⇐ Length, in octets, of data to be sent
Data	⇐ Data
FCS	
ED	

Acknowledge

Preamble	
SD	
DID	⇐ Destination Station ID
Type	⇐ ACK
Control	⇐ Control flags: AP, sequence, out-of-sequence, retry, hierarchical
SID	⇐ Source Station Identifier
FCS	
ED	

Mac Management Data

Preamble	
SD	
DID	⇐ Destination Station ID
Type	⇐ MDATA

Control	⇐ Control flags: AP, sequence, out-of-sequence, retry, hierarchical
SA	⇐ Address of data originator, 48-bit address
MType	⇐ Type of MAC management message
Data	⇐ according to MType
FCS	
ED	

MType	**Data**
Registration Accept	SID, SA
Registration Reject	none
Registration Cancel	SID, SA

12. Possible Enhancement Frames

Pause Sync

Preamble	
SD	
DID	⇐ Broadcast
Type	⇐ EDSYNC
Control	⇐ Control flags: AP, sequence, out-of-sequence, retry, hierarchical
SID	⇐ Station Identifier, ID of originating controller station
PauseLength	⇐ length of receiver off period
FCS	
ED	

Extended Data Sync

Preamble	
SD	
DID	⇐ Broadcast
Type	⇐ EDSYNC
Control	⇐ Control flags: AP, sequence, out-of-sequence, retry, hierarchical
SID	⇐ Station Identifier, ID of originating controller station
UpLength	⇐ length of Upward Data Period
DownMap	⇐ Map of stations to receive data in downward data period
SuperFrame	⇐ Superframe number
FCS	
ED	

Extended Request Sync

Preamble	
SD	
DID	⇐ Broadcast
Type	⇐ EDSYNC
Control	⇐ Control flags: AP, sequence, out-of-sequence, retry, hierarchical
SID	⇐ Station Identifier, ID of originating controller station
TotalSlots	⇐ Total number of time slots in SyncPeriod (including RegSlots)
RegSlots	⇐ Total number of time slots which are for registration only
UpLength	⇐ length of Upward Data Period
DownMap	⇐ Map of stations to receive data in downward data period
SuperFrame	⇐ Superframe number
FCS	
ED	

Mandatory-response Request Sync

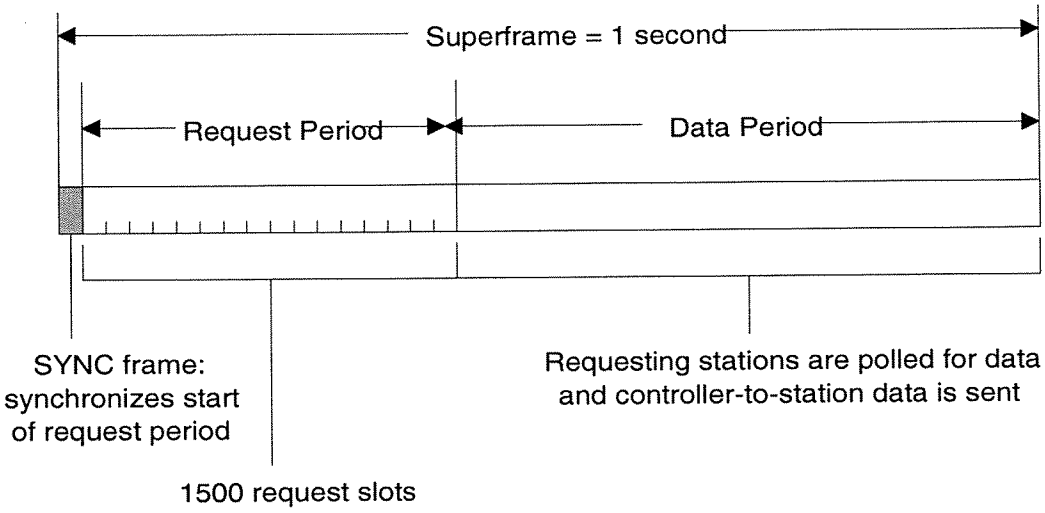
Preamble

SD	
DID	⇐ Broadcast
Type	⇐ MRSYNC
Control	⇐ Control flags: AP, sequence, out-of-sequence, retry, hierarchical
SID	⇐ Station Identifier, ID of originating controller station
TotalSlots	⇐ Total number of time slots in SyncPeriod (including RegSlots)
RegSlots	⇐ Total number of time slots which are for registration only
SuperFrame	⇐ Superframe number
FCS	
ED	

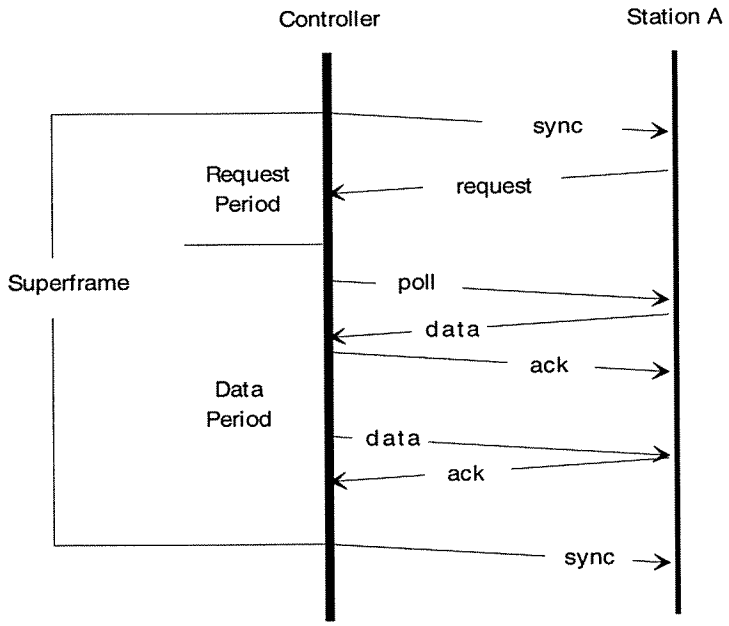
Forfeit

Preamble	
SD	
DID	⇐ Destination Station ID
Type	⇐ FORF
Control	⇐ Control flags: AP, sequence, out-of-sequence, retry, hierarchical
SID	⇐ Source Station Identifier
FCS	
ED	

Appendix A - An Implementation of Spectrix' Reservation/Polling Protocol



Stations have fixed addresses, 0 to 1499. A station's address is the number of its owned time slot. When a station has data to send it issues a request in its owned time slot. In the data period the controller polls all stations which have issued requests, and sends data to stations.



- Direct station-to-station communications not supported.
- Controllers are Access Points connected to existing wired LANs.
- Infrared PHY, single channel. Network isolation by space - BSAs do not overlap.

Appendix B - 802.11 Issues (21 criteria item # in parenthesis)

3.1 What is the impact of the MAC implementation complexity in regard to time-to-market? (15)

The CODIAC protocol can be implemented in many levels of complexity. Where time-to-market is of primary concern a simple implementation could be chosen to accomplish this.

4.5 Can a station be a member of an ad-hoc and non-ad-hoc network at the same time?

Yes. Station A can be registered with a controller/AP, and associated with that AP - a member of an infrastructure network. Station B may be registered with that controller/AP, but not associated with the AP, it is registered only for the purpose of conversing with other wireless stations - it is not a member of the infrastructure network. These two stations can converse without station A having to dis-associate from the AP, so it retains its membership in the infrastructure network while forming an ad-hoc network with station B.

5.3B What logical functions are needed to support the defined infrastructure services?

These services are defined in closed Issue 5.3A as: association, re-association, disassociation, authentication, privacy, integration, and network management.

For any of these services which require exchange of information over the wireless medium, the CODIAC protocol proposes using MDATA frames. Because delivery of these frames is critical, they are transferred in the four-step transaction in the same manner as client data. These frame formats are yet to be fully defined.

Association, re-association, disassociation, and integration all require an AP. These services are supported by the AP bit which is set in frames sent by the AP, which also serves to notify stations of its presence.

5.9 How to determine that Access Points (APs) are present?

All frames are marked with an AP bit which indicates that they originate with an AP. If a station listens and does not hear frames from an AP, it can send a broadcast RTS with the Hierarchical bit set, which indicates that the RTS is intended for an AP only - this will cause any AP present to identify itself.

6.3 Unauthorized access impact MAC throughput. (1)

The philosophy of the CODIAC protocol centralized mode is that registration with a controller is completely separate from association and authentication with an AP. The purpose of registration is to facilitate coordinated sharing of the bandwidth - stations cannot be precluded from this on the basis of authorization. The example of the centralized network that covers the park across the street from the building in which it is implemented is such a case. Stations in that park must register with the controller to share the bandwidth - they must not be excluded from using that bandwidth.

In distributed mode the bandwidth is available to all stations, the registration process does not exist.

In either mode stations get associated with and authorized to use the infrastructure through an AP by an association/authentication process. Unauthorized stations can repeatedly attempt to get authorization and be rejected, and this will impact throughput by adding a repeated transaction.

9.2 What are the area coverage implications of MAC timing constraints? (10)

On the assumption that this issue arose from the Ethernet maximum cable length specification which is driven by the timing constraints of CSMA/CD: No timing constraints are imposed by this protocol that would limit coverage area of LAN dimensions.

9.3 Must the same MAC work in a minimum system and maximum system (network size independence)? (16)

Yes. Not just to work in both, but to work efficiently in both is the goal of the CODIAC protocol.

10.1 What Coordination Function (CF) will be specified in the standard?
10.2-B Do multiple CFs need to be specified?

Both Distributed Coordination Function (DCF) and Point Coordination Function (PCF) are required to support efficient operation with network size independence for asynchronous service. PCF is required for TBS, but this should not be forced on small population and ad-hoc networks.

10.2-A What are the events that cause switching between multiple CFs?

1. Switch from DCF to PCF: Request for Time-bounded service from a station to a controller which supports TBS.

2. Possible implementation, switch from DCF to PCF - detection of high traffic causing high rate of collisions.

10.3 What are the issues surrounding the Point Coordination Functions (PCF) and Distributed Coordination Function (DCF) arguments?

1. PCF is required for TBS support.

2. DCF facilitates ad-hoc networks better because it does not require a controller.

3. PCF is better than DCF for minimizing power consumption of portable stations.

4. PCF is better for high population networks, deterministic media access to avoid collisions.

5. DCF is lower overhead and possibly lower access delay (in small population BSAs).

11.3 Is there a need for multiple APs per Basic Service Set (BSS)?

Although no need is envisioned, no reason for preclusion is seen. With the CODIAC protocol only one controller per centralized mode BSA is required, but any number of stations could be APs.

13.3 What support will the standard provide for power management:
13.3A DC power (power consumption)?
13.3B RF power (signal strength)?
13.6 How will the MAC standard address Power Consumption? (9)

13.6 & 13.3A Power Consumption

Some implementations are more concerned with power consumption than others. The CODIAC protocol allows implementations to trade off power consumption requirements with overhead and access delay. These features are described in the main text of this document.

13.7 & 13.3B Signal Strength

Section 10, point 5 addresses one way in which the centralized mode may be used to aid in signal strength management. No investigation has been done in this area, research and development may uncover more.

14.4 Ability to establish peer-to-peer connectivity without prior connection (e.g. without "knowledge of the presence of your peers"). (2)

Interpretation - can a station initiate communications with another station without knowing that it is present, and what its wireless address is?

Yes. In the RTS frame contains the 48-bit address of the intended destination station. In distributed mode this frame is broadcast, so the destination station can respond if it is there. In centralized mode the RTS is sent to the controller, and it can use its knowledge of registered stations to determine the wireless address of the destination.

Also, use of the AP bit and the Hierarchical bit allow stations to identify APs without any prior knowledge.

15.6 What is the algorithm for managing partitioning of capacity between Time-bounded and Asynchronous services?

That should be left to the discretion of the implementation. The CODIAC protocol allows different implementations to tailor servicing of stations to their needs while still remaining compatible.

15.8 Do all stations and all infrastructures support the Time-bounded service?

a) Stations

The CODIAC protocol requires that all non-controller stations be well behaved in both operating modes. This means a station must be: (1) capable of communicating in both modes; or (2) capable of communicating by the distributed mode rules only, but it must be quiet in the presence of a controller; or (3) capable of communicating by the centralized mode rules only, but it knows it must be quiet when it does not hear a controller.

This means that for non-controller stations "supporting" (where "supporting" means not precluding other stations from using TBS) TBS with the CODIAC protocol is a given, because TBS is provided by centralized mode operation .

For controller stations, whether they can operate in both modes should be an implementation decision. However if a station requests TBS, there should be a specific negative response to that request if the service cannot be provided (not yet defined).

b) Infrastructures

Yes, where the definition of support is to handle in a well behaved manner - i.e. where a station requests TBS there should be a negative response to that request if the service is not provided.

If support = provide, then No.

Summary - in agreement with Pro arguments 3.1 and 3.5

15.9 How will the standard address the MAC ability to service various traffic: data, voice, and video. (6)

The CODIAC protocol supports asynchronous and time-bounded services. The centralized mode can be implemented to support the requirements of various TBS time constraints.

17.2 What level of reliability for Broadcast (Multicast) Addressing is required? (20)

Multicast and broadcast reliability is directly tied to the MSDU error rate, as they cannot be acknowledged. This is the case for all LANs, wired and wireless. These are not inherently reliable delivery mechanisms.

17.3 What is the extent of Multicast? (BSS or ESS)

Both ESS and BSS multicast should be supported, a station should be able to explicitly control the scope of multicast (this supports the position of document 93/40 on the WHAT protocol). The hierarchical bit provides this capability.

17.5 What is meant by address: size? is IEEE 802 addressing OK?

IEEE 802 addressing is required (supports the position of document 93/40 on the WHAT protocol). Wireless stations should be identified by 48 bit unique IDs that are compatible with other IEEE 802 standards. The 48 bit addresses of source and destination stations are contained in the four step transaction of the CODIAC protocol.

18.3 Will the standard support PHY with variable rates?

Yes. RSYNC frames could be issued at different rates within a superframe, or different superframes could be issued. PSYNC could be issued at one rate while communication was going on at another.

Little consideration has been given to this issue at this time. However, this is a very important issue. First generation wireless LANs will be released at lower speeds than forthcoming generations, but they must coexist - it is not desirable tell customers they must upgrade their equipment because the company across the hall installed a newer, higher speed LAN.

19.1 Shall the 802.11 standard depend on the layers above the MAC for recovery from failed transmits? If so to what extent?

Partially. A retry mechanism should be implemented in the MAC as required to bring the MSDU loss rate up to the equivalent of wired LANs. (See Issue 19.5)

19.2A Will the IEEE 802.11 MAC look like all other 802 MACs regarding delivery reliability?
19.2B How does Multicast affect this decision?

19.2A - Yes - see 19.5

19.2B - Broadcast and Multicast will not be as reliable - see Issue 17.2

19.5 What kind of error recovery mechanisms are to be incorporated into the MAC?

Supports the position of document 93/40 on the WHAT protocol - the 802.11 MAC should include a positive acknowledgment protocol with low level retries. This mechanism helps the MAC present approximately the same level of MSDU delivery reliability as other IEEE 802 protocols.

19.6 What is the strategy for capacity control?

The CODIAC protocol is in itself a strategy for capacity control. The purpose of the two operating modes is allow efficient media use under different capacities, and in centralized mode each implementation's strategy for management of request periods and data periods in centralized mode is its strategy for capacity control.

19.7 Is the maximum number of stations to be specified? If so how many? (5)

No. That should be up to the implementation.

In distributed mode the protocol will begin to break down at a certain number of stations, and the implementer should decide what action to take about that - whether to switch operating modes, or to make the degradation limit a parameter of the network.

In centralized mode it is a function of the intended application. An application with huge numbers of stations with small payload and/or tolerance for large transfer delays can be supported, as can an application with smaller population with need of shorter transfer delays. The CODIAC protocol can be set up to accommodate either, without loosing compatibility.

19.8 How will the standard address the MAC robustness in the presence of co-site dissimilar networks? (8)

On the assumption that "dissimilar" means not so different that they don't see each other (e.g. IR and SS), and not so similar as to be able to recognize each other's MSDUs - Co-site dissimilar networks interfere with each other. There is nothing the MAC can do about this that is different from handling interference of any other kind.

19.10 How will stability under heavy load be addressed?

The centralized mode of the CODIAC protocol remains stable under heavy load by increasing transfer delay. This is further explored in document "Performance of the CODIAC protocol".

19.11 How will transmission lost be addressed?

Issues 19.1 and 19.5 cover this issue.

The CODIAC protocol proposes positive ACK and retransmission to bring the transmission loss rate to approximately the same level of MSDU delivery reliability as other IEEE 802 protocols.

20.2 Can MAC handle different preamble lengths from different PHYs?

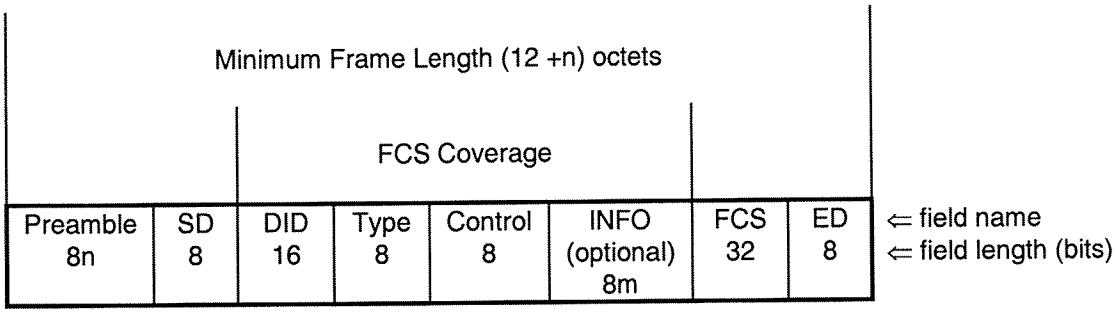
No. If different PHYs must generate different preamble lengths then preamble should be handled by the Medium Independent Layer, which is on the PHY side of the MAC/PHY interface. The preamble would be stripped off by the time the frame is seen by the MAC.

To facilitate MAC independence from preamble length, perhaps the preamble should not be considered part of the MAC frame.

20.3 What is the MAC frame structure?

The frame structure is designed with the following goals: (1) to minimize the frame size while keeping a consistent frame structure; (2) to have a minimum size destination identifier at the start of the frame to

allow destination determination of frames as quickly as possible; (3) to provide a level of error detection suitable to the high bit error rate of the wireless media.



Preamble = Preamble (n to be determined)
SD = Start Delimiter
DID = Destination Identifier
Type = Frame Type
Control = Control Flags: AP, sequence, out-of-sequence, retry, hierarchical
INFO = Information (0 <= m <= to be determined)
FCS = Frame Check Sequence, CRC-32
ED = End Delimiter

20.4 How is the MAC time preservation ordering of SDU to end systems (LLC requirement) addressed by the standard? (21)

The CODIAC protocol is a stop-and-wait ARQ, it does not change the order of MSDUs.

21.2 How will the MAC robustness in the presence of non-reciprocal wireless medium be addressed in the standard? (14)

If this means stations may have different receive and transmit coverage area:
In CODIAC protocol centralized mode, if the relationship between the controller and a station is asymmetric the station will not be able to register. Minimal bandwidth will be lost as it repeatedly tries to do so. In distributed mode the RTS/CTS exchange will fail, avoiding the wasted bandwidth of attempting to send the data itself.

If this means non-reciprocal traffic load:
The CODIAC protocol is flexible in the assignment and duration of the data periods in centralized mode, both at run-time and per implementation, creating no problems handling non-reciprocal traffic loads. This is a moot point for distributed mode as it has no directionality.

25.1 Will the standard provide a procedure to reserve medium channel capacity?

Not a lot of work has been done so far in this area, however this facility can easily be incorporated into the CODIAC protocol by adding information to the request frame specifying a reservation of a particular length, or even making a "connection request" for a certain amount of bandwidth which could stand as a reservation of channel capacity until the connection is torn down, rather than having to issue a request every superframe.

25.2A Must the MAC work on a single channel PHY?
25.2B Will the standard support multiple channel PHYs?

Yes and yes.

25.5 What is the definition of MAC fairness of access? (11)

The definition of fairness of access is all stations having an equal opportunity to access the media. Things about a MAC that can make access opportunity unfair are:

(1) sensitivity to the near/far bias (capture effects);
(2) allowing one station to hold the medium once it has it;
(3) bias to a particular data path - AP to station; AP from station; or station to station;
(4) bias to a traffic type, TBS or asynchronous.

The CODIAC protocol addresses these items:

(1) see Issue 25.6.
(2) Maximum frame length controls this to in both modes. In distributed mode once a station has made a transaction, of up to maximum length, it must re-contend for the medium like all the other stations. In centralized mode the controller implementation controls this fairness. At the end of the request period it has the information required to divide up the data period bandwidth as it sees fit.
(3) In distributed mode there is no distinction between these data paths. In centralized mode the controller implementation controls this.
(4) In both modes the AP implementation controls this. An AP could deny a TBS request if it feels that the asynchronous traffic is being unfairly denied access by the amount of TBS traffic.

25.6 How will the standard address the MAC facilitation of 'access fairness' (insensitivity to near/far bias)? (12)

In the CODIAC protocol centralized mode sensitivity to the near/far bias will only come into play in the registration slots. If two stations attempt to register in the same slot and one of them has signal strength enough to obliterate the other, the winner will get registered and the loser will have to try again next superframe.

Summary - (1) the near/far bias can cause a minor delay in registration, but the protocol is insensitive to it for data transfer in centralized mode; (2) Distributed mode is sensitive to the near/far bias during the RTS/CTS exchange.

26.1A Does the concept of priority need to be addressed in the MAC?
26.1B Different traffic priorities?
26.1C What is priority? (13)

26.1C - Priority is a station having better access to the medium, in terms of access delay and/or time length of access, than other stations.

26.1A - If the concept of priority is addressed in the MAC: The CODIAC protocol lends itself very well to the implementation of priority in centralized mode. If priority is added to the RTS frame then the controller can service requests in prioritized sequence in the data period. The controller can also assign quantity of bandwidth to requesting stations in a prioritized fashion. Priority is not a concept which can be applied to the CODIAC protocol distributed mode.

26.1B - With respect to traffic types, in distributed mode TBS traffic is not supported so it is not relevant. In centralized mode the protocol does not give priority to either traffic type, but an implementation could do so, as TBS requests are marked.

Exhibit 11

IEEE 802.11
Wireless Access Method and Physical Layer Specifications

Title: A Wireless MAC Protocol comparison.

Presented by:
Wim Diepstraten
NCR SE-Utrecht
NCR/AT&T Network Product Group
Nieuwegein
The Netherlands
31-3402-76482 (V)
31-3402-39125 (Fax)
Wim.Diepstraten@Utrecht.ncr.com (Email)

Abstract: In this paper a several protocol comparison aspects are addressed. An analyses is provided that shows the obvious advantage of a distributed access protocol. The WAVELAN CSMA/CA protocol is explained and its performance is compared against the 4-WAY LBT protocol as proposed by Ken Biba, and against an extension of the current Wavelan protocol with a MAC level recovery. Several performance analyses methodologies are proposed to build a common ground for protocol comparison. The presented results are preliminary and are based on the simulation approach described in IEEE P802.11-92/26.

Conclusion:

It was concluded that the interference robustness and medium sharing behavior are the most important characteristics of a wireless protocol. Based on this a global analyses shows that a distributed "coordination function" is best suited to achieve automatic sharing of the available medium bandwidth, without additional coordination overhead. To improve the robustness of the protocol a MAC level recovery mechanism is very effective.
In addition it is shown that CSMA/CA as used by WAVELAN does have a very high throughput efficiency paired with a low transfer delay, which is similar than the performance of 802.3 CSMA/CD networks.
Wavelan CSMA/CA, CSMA/CA + Ack and the modified Ken Biba 4-way LBT protocol are compared on several aspects. A Peer-To-Peer Buffered Load test methodology is proposed and allows protocols to be compared to several relevant characteristics. The relevant comparison methodologies are explained and illustrated with several simulation output charts. A Client-Server test

configuration is suggested to evaluate the net performance for an application.
Further work will be needed to compare the different protocols, and this will be subject for future contributions.

Introduction:

When analyzing MAC protocols, the question is what kind of characteristics should be looked at and, what would be the suitable method to do it. Clearly one important aspect will be the throughput and response times for the individual stations, and the capacity of the whole system. In a wireless environment in particular, the robustness for interference, and the ability to share the medium are very important characteristics which need to be analyzed when comparing different MAC protocols. This document addresses the important characteristics, and proposes a methodology to analyze them. Only the asynchronous services are evaluated.
As an example three possible protocol implementations are compared against each other. The following protocols are used as an example:

- CSMA/CA protocol as used by WAVELAN.
- CSMA/CA + Ack protocol extension.
- 4-WAY LBT protocol (a modified Ken Biba proposal)

The intention of this paper is not to arrive at a conclusion about the preferred access method, because to date not enough simulations are done to fully compare all characteristics of the protocols.

Protocol Characteristics:

The main characteristics of a protocol will depend on the type of services that the MAC layer needs to supply to a particular application. We can distinct a few different categories of applications that use two different types of services as follows:

- Connectionless service.
  This is the type of service which most of today's wired LAN's provide, and on which the majority of Network Operating Systems and applications are based on. It is ideal for "Bursty" traffic. It is characterized by a very low response time, and is generally very tolerable for large deviations in transfer delay.
- Connection oriented service.
  This is a type of service that can guarantee a fixed bandwidth to an application, and is characterized by a relative long setup time for the connection, after which the data transfers are usually providing a more or less constant bit stream with relative low deviation in transfer delay. This type of services are used for applications which need

real time data like voice or video, and for time bounded transfers of data in for instance an industrial environment.

This document will primarily deal with the connectionless type of service, most commonly utilized by the majority of today's Network Operating Systems.
The following is a list of characteristics that need attention:

- Throughput:

  . Total system throughput
  . Individual station throughput as function of Network load.
  . How is throughput shared with other Networks using the same channel.
  . Effect of interference: From other Networks.
    From other sources.

- Transfer Delay at various load conditions.
- Max number of stations.
- Fairness.
- Behavior/Stability under heavy load conditions.
- Behavior/Stability under varying fade conditions.
- Effect of "Hidden" terminals.
- Effect on higher layer protocols.

As concluded in IEEE P802.11-92/26 simulations will become very important to analyze the performance aspects in a complex environment like Radio Lan's. The relevant Radio medium characteristics need to be modeled such that their major impact on the performance and operational robustness are factored in. This is done in the described simulation approach.

The results of the simulations need to be analyzed in such a way that the major protocol characteristics as listed above are covered.

Protocols considered:

In general two access protocol implementation categories can be distinguished, by the type of "Coordination Function" which is applied.
The two "Coordination Function" types are:

- Centralized
- Distributed

When the "coordination function" is centralized in nature then there is some mechanism that assures, at least in one network segment, that only one station is allowed to access the medium at any one time. The "coordination function" can itself be located in a fixed station, like in a polling environment, or it can be traveling through all stations within a network segment (BSA) like in a token passing system.

When the "coordination function" is distributed in nature then there is a procedure defined by which individual stations are trying to access the medium resolve the contention on the medium. This applies to the CSMA type of random access protocols.

A wireless medium is very different from a wired medium, and most obvious is the channel separation difference and availability of bandwidth. In a wired environment the separation between different physical networks is infinite, because they run on separate cables. Increasing the system capacity can simply be achieved by increasing the system bandwidth by running extra cables.
In a wireless environment however spectrum resources are scarce. The consequence is that at worst multiple networks will need to share the same band. The isolation between the different network segments (BSA's) will be dependent on the number of channels available.

- In a multi frequency channel system the isolation can be relatively high and will depend on the spatial re-use distance that can be achieved with the given number of channels available. When multiple overlapping channels are used then the channel separation will depend on the transmitter and receiver design (PHY). The spurious emissions of the transmitter in a neighbor channel, and the non linear distortion generated in the receiver by a strong nearby transmitter are causing this interference.
- When only one frequency band is available then an other method for channelization can still be applied by using different (orthogonal) codes in a direct sequence spread spectrum system. The achievable isolation will depend on the code length used, and will be the trade-off between raw bitrate and isolation. In practice for bitrates higher than 1 Mbit the achievable isolation will be very poor compared to the dynamic range of the radio signal, and accurate power

control mechanisms are needed to make it useful. In addition not many orthogonal codes will be available.

Bottom line, the co-channel interference in these systems can still be significant, and needs careful consideration for the protocol design.

- The lowest isolation will be the system which has only one channel available without any further separation provisions. Here the same medium must be shared by multiple networks unless sufficient spatial isolation can be achieved.

In all three cases the protocol has to deal with a certain co-channel interference level. Since the protocol must be able to run on different PHY's, the worst case situation needs to be considered, being the single channel environment. Please note that one of the requirements listed in the Draft 802.11 requirement document was the ability to support a single channel environment.
Therefore the coverage area of a wireless LAN segment (BSA) will be interference limited rather than noise limited.

The interference tolerance of a protocol specifically the tolerance for co-channel interference will be a very important factor in the MAC protocol design.
This will translate into two different aspects:

- The access mechanism:
  The "coordination function" should be robust for interference.
- The transfer success:
  The interference situation at the intended receiver station will determine the success of the data transfer. Since it will be very hard to predict this from the transmit station or any other "coordination function" location, especially in the case of other (non co-channel) interference sources, the success of a transfer can not be guaranteed. Hence the protocol should be tolerant for lost packets.

The latter can best be achieved by a recovery mechanism on the MAC, to become independent from the recovery mechanisms used at higher protocol levels. This is because those recovery procedures are not designed for an environment where interference is dominating the packet error probability, so they are less efficient. A positive acknowledge mechanism, which will indicate to the transmitting station that the packet has been successfully received, can be used to detect that packets are lost.
For the access mechanism the basic choice will be between the centralized and distributed "coordination function".
In my mind the determining factor affecting this choice is primarily the ability and efficiency to share the same medium with other networks. For "bursty" traffic a centralized "coordination function" will not be able to efficiently coordinate the medium access between multiple BSA's, especially

when those BSA's are not part of the same ESA. It would involve coordination via the distribution system if any exist more or less on a per packet basis. This type of coordination could perhaps be dealt with for connection oriented traffic, but still a big problem remain between multiple ESA's. In any event this type of "coordination function" will be pretty complex and relatively inefficient (for bursty traffic).
This is where a distributed "coordination function" can be very efficient because it provides for automatic sharing of the medium without any added complexity (for the coordination).
A further advantage is that at a low average network load which is typical for most LANs today, the transfer delay is very low and provides for a "snappy" response.
An other factor which needs to be considered is the amount of bandwidth needed for the "coordination function" on the Wireless medium and on the distribution system (backbone network). To give an example: a token passing scheme would continuously use scarce bandwidth even when no load is applied to the system. This will seriously effect the sharing of the channel with neighbor BSA's.

Coordination Function type Conclusion:

The main characteristic for a Wireless MAC protocol is its robustness for interference, and related to that the ability to share a single medium with other networks efficiently. A global analyses shows that for "Bursty" data traffic typical for the connectionless services used by most Network Operating systems today, a distributed "coordination function" promises low response times and more or less automatic sharing of the medium between overlapping networks. This allows for a graceful degradation in throughput per individual network. Apart from this access mechanism it will always be necessary to have a method of dealing with lost packets, and a MAC level recovery mechanism will therefore be essential to achieve adequate robustness. To allow the implementation of a MAC level recovery mechanism a lost packet detection mechanism is needed, which can be done with a relative simple positive Acknowledge facility.

Possible "distributed" access methods.

In wired LAN environments CSMA/CD is accepted to be a very effective medium access method. In a radio environment it is however not practical to implement the CD function because of the extreme high dynamic range required. The WAVELAN product on the market today uses CSMA/CA, which is CSMA combined with a collision avoidance strategy. This provides for a medium use efficiency near the CSMA/CD efficiency. The 4-WAY LBT protocol proposed by Ken Biba is also a distributed type of access protocol.

CSMA/CA explained:

The main access mechanism is 1-persistent CSMA. First of all the medium is sensed for valid Spread Spectrum carrier, and when silence is sensed during the duration of a slot, the medium will be accessed. When the medium is sensed busy, then the transmitter will defer until the end of the packet. Normally in CSMA a deferring station would access the medium immediately after the IFS (inter frame space) period. At medium to high network load, there is however a high probability that more stations were deferring on the same packet, and when they both access the medium after the IFS period this will result in a collision, assuming that at the intended receivers both signals will interfere with each other. This is the situation which CSMA/CA is trying to avoid. A deferring station will at the end of the packet start a random backoff sequence which is designed to significantly reduce the probability that the multiple deferring stations will collide. So when a station senses a busy network it will use p-persistent CSMA right after the IFS.

CSMA/CA Performance:

Figures 1 compares the WAVELAN CSMA/CA performance with ALOHA and slotted CSMA which is run on the same WAVELAN PHY. As shown, the efficiency of the protocol is very good, and reaches approximately 87% of the 2 Mbps raw bitrate for long packets. This is similar to the efficiency of CSMA/CD parameterised according to the 802.3 standard. It should be noted that part of the overhead is due to the training time required by the PHY to select the best antenna (for antenna diversity), and achieve proper synchronization. The slotting time relates to the time required for proper Spread Spectrum signal detection on a particular antenna. Given the low medium propagation delay, the slotting time can be much lower than used in the 802.3 CSMA/CD networks today. For Wavelan the slottime is in the order of 10% of the 802.3 standard.
This clearly shows that a distributed access method can achieve high efficiency, paired with low transfer delay, and is stable even under high load conditions.

Comparing MAC protocols.

The WAVELAN CSMA/CA access method is used further to compare it against possible alternatives.

One clear alternative is to extend the CSMA/CA access method with a MAC level recovery mechanism based on a packet loss detection by means of an Acknowledgement of successful reception of the MSDU by the intended receiver.
The other distributed control protocol under analyses is the 4-WAY LBT protocol as proposed by Ken Biba in Doc IEEE P802.11-91/92. The described protocol has been adapted in certain area's, and is run on the Wavelan PHY, so that a direct comparison between the MAC protocols is possible.
The intention of this paper is not to arrive at a conclusion about the preferred access method, because to date not enough simulations are done to fully compare all characteristics of the protocols. The rest of the paper is intended to describe the possible methodology for comparing the protocols on several aspects.

4-WAY LBT Protocol modifications:

The 4-WAY LBT protocol proposal of Ken Biba in Doc IEEE P802.11/91-92 is changed in some area's as explained below:

- The RTS, CTS, DATA and Ack frame structures are changed a bit in size to reflect the following:
  - The preamble is effectively longer to reflect the training length requirements of the WAVELAN PHY.
  - The CTS and ACK packets contain the source address of the original transmitter that is captured by the intended receiver.

- The document was unclear about the behavior of the receiver when it receives a RTS packet. The document suggest that when a station is receiving a valid RTS addressed to that station, then it will send back the CTS packet. This is changed, so that the CTS packet is only returned when the station is enabled to transmit by the "Net allocation vector", to prevent it from interfering with on-going transfers in a nearby network.

Simulation environment:

The simulation program as described in doc IEEE P802.11-92/26 was extended to include the modified 4-WAY LBT protocol from Ken Biba. All the different protocol derivates shown here are controlled by setting different parameters in the simulation program. In addition some changes were made to the reporting facilities, and the results are imported into SigmaPlot version 4.1 and processed to provide the graphical output as shown in the appendix. This allows for postprocessing of the large amount of simulation results, and makes it possible to correlate all kind of situations with the different parameter sets used.

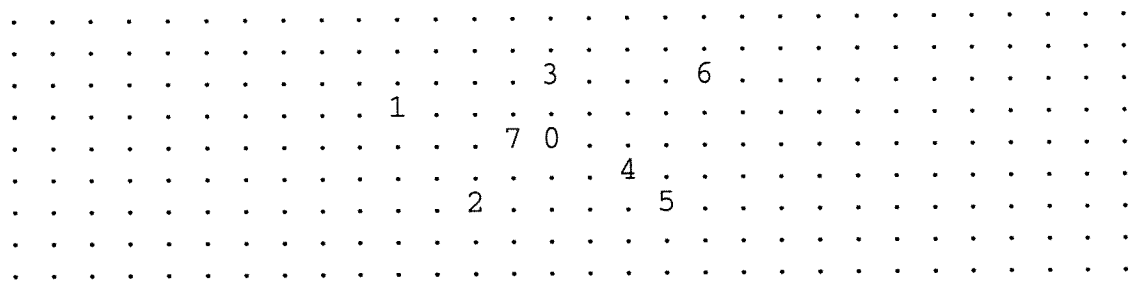
Simulations performed:

The three protocols CSMA/CA, CSMA/CA + Ack, and 4-WAY LBT are being compared against each other with various type of simulations:

- Throughput and Transfer delay versus Buffered Load.
  - . with 100% Long packets (Novell length).
  - . with a 60% Short packet + 40% Long Packet mix (Novell lengths).
- Throughput and transfer delay versus the number of stations.
- Max throughput as function of the PHY preamble length.
- Medium sharing behavior (at high load).
  - . Throughput and Transfer delay versus distance between two networks.
  - . Throughput and Transfer delay versus distance between two networks in a multi floor environment.
  - . Individual station behavior in various multi network environments.
  - . "Hidden Station" behavior.
- Throughput in a high load Novell environment (Client Server).

All simulations are based on the WAVELAN PHY which provides a 2 Mbps raw bitrate data channel.

All simulations were done with a network of 7 stations scattered across an environment as follows:



Scale = 10 meters per dot.

In the above configuration station 0 is a Server station, which is used only during the Client-Server tests.
The attenuation coefficient is set to 3.5 which is typical for most semi open office environments.
During this test all communication is Peer-to-Peer with random destinations per packet.
The throughput measured during the Peer-to-Peer test includes only the successful received packets and includes the standard MAC overhead of source, destination, length and CRC. It does not count the overhead of the Ack packet in CSMA/CA and the RTS, CTS and Ack packet in the 4-way LBT protocol.

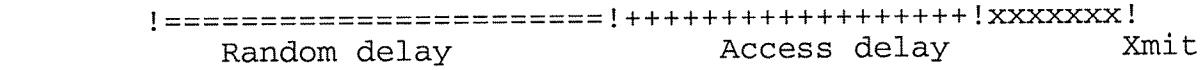
Test Configurations used:

The basic test configuration used is the Peer-to-Peer test, in which the stations generate traffic with random destinations. As described in doc IEEE P802.11-92/26 this results in different path attenuation for every individual link, and effects of capturing and co-channel interference are included in the model.
To investigate the influence of the MAC characteristics on higher protocol layers, a CLient-Server test will be performed. In particular the handshaking as used within a Novell network operating system environment is used during these tests.
For that reason the used Short and Long MSDU lengths are based on the packet sizes used in a Novell environment. To allow comparison between the different test environments, these packet lengths are also used in the Peer-to-Peer test environment.

Buffered Load:

In a simulation environment it is not practical to apply a Poisson distribution function to generate traffic for the medium. Also in a real "Bursty" traffic environment this approach is not realistic. In the simulation we have to deal with a (fixed) number of stations that want to get a certain amount of data through the medium. In real applications the actual traffic source is a transaction or a large file which take a number of packets to complete a communication session. In reality a new packet will not be generated until the previous packet has been transferred. The MAC protocol needs to resolve the contention between all the stations who have packets to transmit. This is the load offered to the "coordination function", and is what I called the "Buffered Load". The buffered load is generated and calculated as follows:

Traffic generation model:



==	Random delay	Used to control the "buffered load" during the test, it is generated randomly with a fixed minimum time of in this case 1 msec. This represents the minimum processing time that is needed to generate a new packet by a station.
++	Access delay	This will be the time required for the MAC to gain access to the medium.
xx	Xmit delay	This is the time required to transmit the total packet, at a given raw bitrate.

The buffered load per station is = 1/(Average Random + Xmit) * Average Packet length

For the total system the buffered load will be the buffered load per station times the number of active stations.
In words the buffered load represents the average amount of data waiting to be transmitted across the medium. It would be the maximum achievable throughput when the access delay is zero. It should be noted however that for the protocols which have a MAC level recovery function, the access time includes the extra time needed for this recovery.
The advantage of this approach is that the transfer delay in an overload situation does still have a meaning and shows the actual average response times achieved at this network load level.
It also gives a good overview of the stability of the protocol under high load conditions.

I would like to propose that this "Buffered Load" definition is used to produce the Throughput and Transfer Delay versus Buffered Load curve.

Throughput and Transfer delay versus Buffered Load curves:

Figure 1 compares the performance of CSMA/CA with slotted 1-persistent CSMA and ALOHA for a 1K data + Novell + MAC overhead packet size of 1088 Bytes to set a reference.
Figure 1a is the same with somewhat adapted load axis to show the stability at high overload conditions.
Figure 2 and 2a compares the performance of CSMA/CA with CSMA/CA + Ack and the modified 4-WAY LBT protocol of Ken Biba.
Figure 3 compares the 3 protocols in a more realistic network environment which is typical for Novell traffic. The load consist of 60% Short Novell(+MAC overhead) packets of 64 Bytes, and 40% of Long Novell Packets based on a data contents of .5 KByte, resulting in 576 Bytes.

CSMA/CA shows a higher throughput than both other protocols, but it should be noted that the lost packets are not recovered by the MAC itself so this must be resolved at higher protocol levels. This will effectively result in a lower performance when this is taken into account compared to the CSMA/CA + Ack protocol. The results show that the 4-WAY LBT has a lower performance which is due to the higher MSDU overhead, and the effect of the PHY training overhead which will be shown later.

Throughput and transfer delay versus the number of stations.

An other relevant parameter in the behavior of an access protocol is the total number of stations for which the contention needs to be resolved. This is especially relevant when those stations apply a high load burst to the network. The probability of successful access resolution in a distributed access protocol will decrease when the number of stations accessing the medium at the same time increases.
Typically a network is dimensioned such that the average load is relative low, so that on average a very good response time is achieved. The probability that at a certain point in time n stations are accessing the medium simultaneously will depend on the application, and will be very low for high values of n. In other words: the probability that the protocol needs to resolve access contention between 10 stations in a network with 100 stations will generally be very low.
However in a single channel wireless environment where all BSA's need to share the same band, the total population of stations which "hear" each other is larger then the number of stations belonging to the same BSA. This will depend on the propagation characteristics of the environment, and the total station density.

The relation between throughput, delay and number of stations doing simultaneous access needs to be analyzed.
This is done in figure 4 with the diagram showing the total throughput and the delay as function of the number of stations. In addition to that, Figure 4a shows the percentage lost packets encountered. In CSMA/CA those packets are not recovered, so this needs to be resolved on higher protocol layers, resulting in a lower average response time as shown in the diagram. This is also the reason why CSMA/CA and one of the reasons why the 4-WAY LBT protocol show a lower throughput performance and a higher transfer delay.

Delay distribution:

Currently the simulation program does not have sufficient provisions to evaluate the delay distribution. It does average the delay on a per station basis, and this is again averaged on a per network basis as shown in the various figures. This is however one of the characteristics that need to be analyzed when comparing protocols. Further simulation program development and simulation effort is needed in this area.

Dependency on PHY

The main parameter which will have influence on the MAC protocol performance is the preamble length needed to allow the PHY to achieve sufficient quality of service. This is in effect the training time needed in the PHY to obtain sufficient synchronization for a good quality demodulation. This will particular have a large influence on High speed systems. When for instance an equalizer needs to be trained to allow the high modulation rates, then this will need extra preamble time in the MAC. Even when the absolute time to achieve synchronization stays the same when increasing the data rate of a system, will increase the overhead percentage, because the overhead expressed in bittimes will increase with the same ratio.
To analyze the dependency on this a simulation is needed that shows the throughput as function of the PHY related preamble time. This simulation is done at high load situations, because there the effect is dominant. This is shown in figure 5.
As is obvious from the diagram the 4-WAY LBT protocol is highly effected by the preamble length, because one MSDU transfer translates into 4 packets on the medium, which each need to train the PHY.

Medium Sharing Behavior

In wireless the multi network behavior is essential especially when only one frequency band is available. It is important to share the (single) medium as efficient as possible, also when multiple ESA's overlap. Related to that is also the fairness of access that individual stations experience.

This should be evaluated for both the fully and partly overlapping case. For this purpose a simulation is set up for two networks, in which the distance between both networks can be varied. Because the simulation program takes into account every individual attenuation path between all the stations of the two networks, the co-channel interference effects are automatically included.
The simulation configuration uses 2 networks of seven stations each, with variable distance between the networks. In addition an extra attenuation can be specified between the networks to simulate that both networks are on a different floor, or in different area's separated by a thick wall.
For each of the three protocols 2 sets of simulations are run.

- With a additional separation of 0 and 20 dB.
- With varying the distance between the networks from 5 to 605 meters in steps of 50 meters.
- A 60% Short and 40% Long MSDU mix is used throughout the tests.
- Test duration is 5 seconds per point.

This way all possible situations can be evaluated. It does contain both fully and partly overlapping situations, and contains "Hidden Station" situations.
For instance the test configuration with 20 dB network separation offset in particular does contain a lot of "Hidden Station" situations.

The results need to be looked at in several ways to evaluated the different aspects:

- Throughput and delay versus network separation distance. Figures 6
  This gives a global overview of the total capacity and how effectively it is shared. Also shown on the same page is the number of "Data" packets lost per individual station over the total test period of 5 seconds.
  However if part of the stations have a lousy performance because the access scheme is unfair, this would hardly show up on the total throughput performance, because then the bandwidth would be used up by other stations.
- Individual station performance.
  The total network throughput performance does not sufficiently show all the effects of the network overlap, and the fairness between the stations. For this purpose the number of successfully transferred packets per individual

station is given in Figure 7. They show how fair the bandwidth is divided over the different stations in the fully overlapping case. In the partially overlapping case there will be a large deviation between stations, because some of the stations need to share with stations of both networks while other stations do not see the other network or see only part of the stations of the other network.

- For the CSMA/CA protocols the cause of the errors can be analyzed, by looking at the number of collisions and number of overjammed packets per station.
- For the 4-WAY LBT Protocol two other values are of interest which give equivalent information. These are the number of lost RTS packets, which is equivalent to the collision count, and the number of times no CTS packets could be returned because the destination station was not enabled to transmit. This is shown in Figure 8 and 8a.

The detailed information is needed to get a good feeling for the most dominant factors influencing the individual performance. They can also be used to optimize the different parameters of a given protocol.

Result evaluation:
As is shown in the total network throughput graphs, there is no significant difference in the sharing behavior between the 3 evaluated protocols. A difference would be expected however for the 4-WAY LBT protocol, because this protocol effectively prevents any parallel transmissions in an area around both the transmitter and the receiver, while the CSMA/CA protocols do this only around the transmitter. The difference can possibly be explained by the setting of the CRS level and minimum reliable receive level.
When looking at the individual station throughput in figure 7, then it shows that there is less variation between the stations in the 4-WAY LBT protocol than the CSMA/CA protocols.
Further analyses of the results are still needed for a good comparison.
A preliminary conclusion is that the extra overhead involved in the 4-WAY LBT protocol to prevent the loss of a "Data" packet is less efficient then CSMA/CA + Ack. So accepting loss of bandwidth of a long "Data" packet is and retransmit the packet is more bandwidth efficient than the continuous overhead for every packet.

Throughput in a Novell environment:

A separate class of simulations will be needed to evaluate the effect of the MAC protocol on higher level protocol layers, and to investigate the performance under several traffic load conditions. One of such traffic models is included in the simulation model and represents the Novell Perform3 test. This test puts a high load on the network, and models the Netware transport protocol NCP (Network Core Protocol).
This test is very representative for a Client-Server environment in which all traffic is between a station and a server station, with Request/Response handshaking per packet.

The total throughput performance is shown in figures 9 and 9a, which in this case show the net application data, so without the Novell handshaking overhead and MAC overhead.
In such a configuration the effect is that all the traffic in a network runs via the Server, which means that the server typically generates 50% of all the packets. The consequence is that the throughput relations and the error probability can be much different from the figures resulting from the Peer-to-Peer test configuration. This is because the buffered load and the average number of stations who are simultaneously accessing the medium is less than 50% than in the Peer-to-Peer configuration. This is because on average more than half the stations are waiting for a response of the Server station before they can generate the next MSDU. This difference is also demonstrated in doc IEEE P802.11-91/125, which shows the throughput and lost package probability as function of the number of stations for both a Peer-to-Peer and Client-Server configuration.
A comparison of the individual station performance is shown in figures 10 and 10a, which shows only the number of packets received from the server.
An other aspect that is the effect of a lost packet on the higher layer protocol. This is however only relevant when this higher layer protocol needs to recover from this. In the case where the lost package detection and recovery is done in the MAC, like in the CSMA/CA+Ack and 4-WAY LBT protocol, this would be much less of an issue, and the result would only be a longer response time for that station, so a bit lower throughput. The effect of this is very visible in the individual performance of the CSMA/CA protocol, which need recovery from the higher protocol layers. The effect is a pretty large deviation in individual performance, because of the long time-out period used in the higher layers to detect the occurrence of a lost packet.

The protocols with MAC recovery do however increase the "Buffered Load" on the medium when many lost packets need to be recovered. This is an effect which is not visible in a Peer-to-Peer test configuration, but becomes more visible in a Client-Server test.

An other aspect that will impact the result is the physical location of the Server, especially in a multi network test. It

will make a difference when the Server is located in the middle or near the edge of a network.
Bottom line is that we have to look at the individual station performance rather than the total network throughput performance. This is because a poor performing station will have a low impact on the total throughput, because other stations will use the bandwidth that becomes available when a poor performing station is waiting for a time-out.

Other simulations needed:

In addition to the test configurations discussed, simulations would be needed to test the effect of other interfering sources like microwave ovens etc. As already indicated previously also the transfer delay distribution, or at least the maximum delay a station encounters should be looked at. This will help also in optimizing the backoff algorithms for CSMA/CA and the lost packet recovery retry procedure.

Conclusion:

It was concluded that the interference robustness and medium sharing behavior are the most important characteristics of a wireless protocol. Based on this a global analyses shows that a distributed "coordination function" is best suited to achieve automatic sharing of the available medium bandwidth, without additional coordination overhead. To improve the robustness of the protocol a MAC level recovery mechanism is very effective.
In addition it is shown that CSMA/CA as used by WAVELAN does have a very high throughput efficiency paired with a low transfer delay, which is similar than the performance of 802.3 CSMA/CD networks.
Wavelan CSMA/CA, CSMA/CA + Ack and the modified Ken Biba 4-way LBT protocol are compared on several aspects. A Peer-To-Peer Buffered Load test methodology is proposed and allows protocols to be compared to several relevant characteristics. The relevant comparison methodologies are explained and illustrated with several simulation output charts. A Client-Server test configuration is suggested to evaluate the net performance for an application.
Further work will be needed to compare the different protocols, and this will be subject for future contributions.

WIRELESS MAC PROTOCOL COMPARISON

* What are the most important characteristics of a Wireless MAC Protocol

* Global selection of the type of protocol most suitable to meet the most important characteristics.

* Comparing Distributed Access Protocols

* Define the type of simulations needed

* Explain the test configurations

* Describe the comparison methodology

* Discuss the performance results

What are the most important characteristics of a Wireless MAC Protocol

* Protocol characteristics needed for data
  - Bursty traffic requires low response times
  - Need high average throughput
  - Can tolerate large transfer delay variations

* Services used for data
  - Connectionless service most commonly used by todays Network Operating Systems.
  - Isochronous not considered during comparison