IEEE 802.11
Wireless Access Method and Physical Specification

Title: **The provisions required for handoff.**

Prepared by:

Wim Diepstraten
NCR WCND-Utrecht
NCR/AT&T MPD
Nieuwegein The Netherlands
Tel: (31)-3402-76482
Fax: (31)-3402-39125
Email: Wim.Diepstraten@utrecht.ncr.com

Abstract: This paper discusses the requirements for handoff, and suggests a procedure and relevant protocol elements. It further tries to identify the issue's involved.

Introduction

What are the IEEE 802.11 Requirements / goals for mobility.

The following is a summary of what I think should be the mobility goals for IEEE 802.11. The main requirement is:

> ***"To assure that a station can maintain full connectivity while moving around in an area covered by the ESA ".***

This involves (re-)association actions of the stations with the different AP's within the ESA, and interaction of the AP with the Distribution System (DS).
The protocol functions that need to be specified to accomplish this are:

- Protocol functions to perform the (re-)association functions
- Specify the functionality for communication across, and with the DS.
- Provide hooks for an arbitrary Distribution System (Different DS types possible)
  - How to solve router based DS problem
  - What hooks are needed.
- Data Loss requirements.

Part of the (re-)association function will require communication between the "new AP" and the "old AP" across the Distribution System, and between the AP and the DS.
This can be accomplished by specifying a so called ***Inter Access Point Protocol*** or **IAPP**.

In general the functionality that needs to be provided by an IAPP may depend on the specific type of DS, but the functions will have a high degree of commonality.
It is clear that interworking between AP's of different vendors will be an important aspect for a Wireless LAN and it is important that this becomes standardized.
To accomplish this, standards need to be developed for a number of IAPP's for certain common DS's. This standard will need to specify the functions and frame formats of the IAPP.
The issue is: ***What organization is responsible for this standardization?***

I think the objective of 802.11 should be as follows:

> ***As a minimum 802.11 should be responsible for a MAC level bridge based DS configuration IAPP standard.***

Further the requirements placed on the DS needs to be defined by 802.11. This will be needed in terms of:
- Functions.
- Delay requirements
- others?

MAC requirements for Handoff

General:
This document does not address security and authentication aspect which obviously do require initialization before the association, or before the actual traffic can be accepted. The authentication and security aspects are intimately related, so that authentication may be implicit when security is used. Authentication itself is definitely not a MAC function, and will therefor not be covered here.

Handoff model functionality.

A general handoff model is as follows:
Once a station finds it necessary to possibly associate with a (new) AP, the following actions need to be performed.

- Station to determine what AP to (re-)associate with (scan for best AP).
- Station to synchronize to the selected AP.
- Issue (Re-)Association Request
- New-AP to identify the change of a station presence to the DS, and communicate with the previous AP using the IAPP to establish a disassociation of the station with that AP.
- New-AP responds with Associate Response.
- Connectivity is now re-established and traffic can be accepted.

For an Initial Association the functions needed are very similar:
- Station to search and select can for best AP.

This involves the Probe function to solicit for a Beacon from the AP's within range.
- Station to synchronize to the AP of choice.
- Stations to Request an Association with the AP.
- AP to communicate the presence of the station with the DS.
- AP to acknowledge with an Association response.

During the process the station needs to obtain the information needed to initialize several parameters important for its operation. For instance this involves initialization of parameters like:
- NID (BSSID and ESSID)
- SID (Station ID needed for TIM interpretation)
- Encryption Key
- Beacon interval
- Power Management parameters.
- Hopping sequence details
- Services available.

When to start a Re-association:

Stations can start a Re-Association process based on several different events.
The idea is that only stations can initiate a Re-association process, not the AP. This is because there are numerous situations where connectivity can be lost completely, and only the station can recover from that by searching for an other AP.
However it is not practical for a station to continuously scan for "the best possible AP", and re-associate when for instance a better candidate is found. This is not practical to do from a Power Management point of view, but also from a performance point of view, because the scanning processes can be lengthy depending on the PHY used, during which the station is not available for normal data traffic.

The scanning process will therefore be initiated by the station based on "Link Quality" knowledge that it can obtain over time.
This "Link Quality" metric can be a collection of several communication aspects about the link with the AP it is currently associated with.
It can for instance be triggered by:
- A receive level measurement or any other signal quality metric of all frames coming from the AP that drops below a given threshold.
- A retransmission rate increase.
- Lack of Beacons over a given time interval.

The different events will occur depending on the environmental circumstance that a station can be in. For instance when a station is moving from one BSA to the other, then the Signal level will gradually decrease over time (from one frame to the other). When the signal level passes a given threshold, then a station can start the scanning process at some scan interval. Note however that level changes can also occur due to fading, which can cause the scanning process to start. Hysteresis will need to be used to prevent frequent unnecessary reassociations.

When however a station is suddenly going into an area with poor reception, for instance when the user enters an elevator, where there is poor or fast changing connectivity, then this can be detected by different events.

- It can still be a poor signal level of the traffic coming from the AP (when still within range)
- When connectivity is completely lost, then this will either be detected by a high retransmission rate increase during active communication, but more likely due to lack of a Beacon from the AP over a given time interval when the station is idle.

The algorithms used to start the scanning process do not need to be standardized and can be vendor specific. What needs to be specified are protocol mechanisms to allow the scanning process to occur, and the procedure needed to Re-associate with an other AP.

Seamless handoff requirement criteria.

The above also demonstrates that there will be situations where the handoff can not be seamless such that no traffic will be lost.
When connectivity disruption during active communication is shorter then a retransmission timeout at higher layers, then MAC level recovery of the data that was still pending at the Previous-AP is possible. When a higher layer timeout occurs, then that will rendor the buffered traffic useless, so that data recovery will only increase the problem.When the total duration of the handoff process can be limited to sufficiently less then the higher layer retransmission timeout, then traffic recovery may make sense.

> This timeout is approximately 400 msec in the case of for instance LLC-2. When TCP/IP is used, which utilizes a form of dynamic timeout mechanism based on measured delay and delay variance statistics, then this retransmission timeout can be significantly shorter.

However there will be situations where the disruption is longer, causing a higher layer recovery, which makes MAC level recovery very undesirable, because it may only make things worse.This means that at least a temporary performance reduction will occur during the handoff.In practise most handoffs will occur when communication is idle, so then there is no noticeable impact at all.
What is however the main requirement from a user point of view.

> *For a user, seamless communication means that temporary traffic disruptions are tolerable, but the communication sessions/connections should be maintained, so that no user intervention is needed to restore communication.*

The feasibility of meeting this will depend on the recovery mechanisms implemented at higher layers. The sensitivity of the Network Operating Systems (NOS) in use today for temporary traffic disruption will depend on the higher layer protocols and the

parameterization they use. NOS vendors who want to take mobility requirements into account will need to parameterize their system to allow a relative high communication disruption tolerance.
Question is still whether we need to specify some sort of performance limit related to handoff.

What is needed to find a better AP.

The DFWMAC document specifies procedures needed to scan (search) for an AP, and subsequently synchronize the station Sync timer to the new AP. Two scanning methods are described that can be specified:

- A passive scanning method that can be applicable for networks with only a few channels, and short Beacon_intervals.
- An active scanning method that is applicable for multichannel networks. It makes use of Probe and Probe Response frames to exchange the necessary information.

A PHY independent methodology is been defined, reference the DFWMAC document.

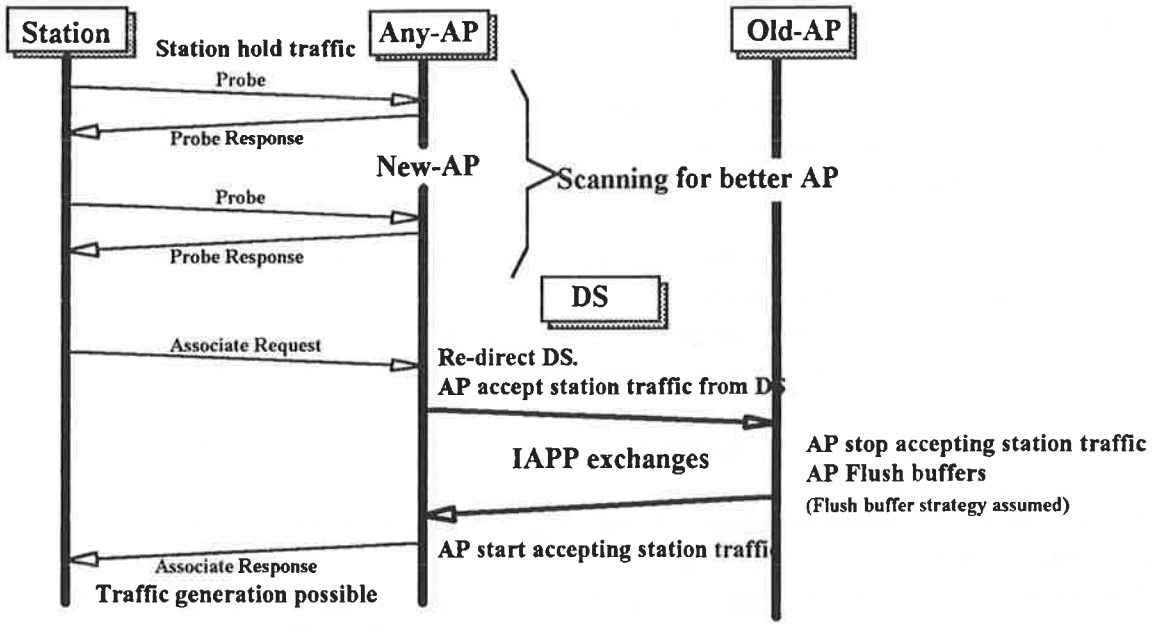
A question remains however, about whether requirements need to be specified for the performance of the scanning process.
The duration of the scanning process may depend a lot on the PHY used, in particular the number of frequency channels used by the PHY within the ESA can effect scanning performance. There are numerous ways to limit this delay, so it will depend a lot on the specific algorithm the vendor is using.

Handover Model details:

In more detail, a station will generally go to the following procedure to Re-Associate.

- Based on a vendor specific algorithm, a station will start a scan for a better AP process.
- To prevent "loss of traffic" directed to that station during the scan process, the station can choose to go into one of the Power Management modes, so that the AP will buffer all traffic for it.
- A station can stop the scan process as soon as it has found a better candidate AP, or it could do an exhaustive search to find the best AP.
- Station to synchronize to the AP of choice.
- Stations to Request a Re-Association with the AP, providing the new AP with the IEEE address of the AP it was associated with (previous AP).
- The AP needs to communicate with the DS, where the station will be located from now on. This is part of the IAPP.

- The AP then needs to exchange information via the IAPP to tell the previous AP via the Distribution system, that the previous AP should clear the association with the identified station.
- AP to acknowledge with an Association response.
- The Distribution System should from then on, direct all traffic for that station via the new AP.



Handover process

It is possible that the "Previous AP" has still traffic buffered for the subject station. It is an issue what to do with this buffered traffic.
In general there are two methods:

- Flush the buffer at the "Previous AP", and rely on higher layer recovery to retransmit the lost data. (Only applicable when re-associating occurs in the middle of an active communication like a file transfer)
- Transfer the buffered data to the new AP, before any new traffic is being accepted by that AP for that station (to prevent sequencing problems).
  This will make the IAPP more complicated.

It should be recognised however that there may be situations that it is better not to recover the buffered data, because it may be "too old", because higher layer protocols have already started a recovery (by retransmission). This can for instance be the case, when for whatever reason a connection is temporarily but suddenly lost, without having a better AP available (elevator example).

As also concluded above seamless handoff should not mean that no traffic may be lost at the MAC layer. Therefore the best solution would be to discard any buffered traffic still present at the Previous-AP, and flush these buffers at re-association.

Please note that the above procedure assumes that a buffer flushing strategy is being used.

A more general approach would be when the IAPP would contain functions that allow recovery of the data that was still buffered in the Previous-AP. This could however be left to the vendor whether the IAPP implements a flushing or a recovery strategy.
This may however require different timing of the IAPP events.
For instance in the flushing strategy, it is best to notify the DS of the reassociation before the Previous-AP is notified, because that minimizes the probability of loosing a frame comming from the DS during the process. This may be different for the "Recovery strategy" because it needs to assure that frame sequencing needs to be maintained.

Functions and frame formats.

The DFWMAC has specified two frames for MAC to MAC communication. These are the x-Request and x-Response frames. A number of frames can be specified where the functionality is determined by elements in the Request and Response frames. Multiple elements can be included in a single frame, and they define the functionality of the frame.

Association related Frame formats

The purpose of the Association function is to associate the station to an AP, so that any traffic that needs the Infrastructure (including the AP) to reach the final destination, can access this via that AP.

A Request frame containing an Associate element is to be defined to which the AP will respond with a Response frame containing the Associate element. This will have the following general form (which also applies to the Reassociate function):

Request {Element type=Associate, Associate parameters} with parameters: *{Previous-AP-Address, Original-AP-Address,}*

Note that the Previous-AP-Address and Original-AP-Address do not need to be present in an Associate. They would be needed in a Re-Associate.

The AP will respond with the following:

Response {Element type=Associate Response, Associate Response parameters} with parameters: *{Station ID, AP-Address}*

The Station ID (SID) is used particularly to allow stations using one of the power conservation modes to interpret the virtual bitmap in the (D)TIM field. It will also be used in a Poll frame to retrieve buffered frames.

The *PM-Mode* indicates the Power Management operating mode of the station.
The *Previous-AP-Address* is the IEEE address of the previous AP associated to.
The *Original-AP-Address* is the address of the AP with which the initial Associate was accomplished. These fields are absent or are zero, when it is an (initial) Associate. This is the kind of information that provides some of the "hooks" to allow Reassociation across Routers, and would allow some sort of a tunneling scheme similar to the mobile IP approach.
The issue is what additional hooks are needed to support handoff via different DS's. Please note that the IAPP is not part of the MAC, but the MAC will need to supply some of the parameters as discussed to support the handoff.

IAPP function requirement

The IAPP will not be part of the MAC, and will further be DS dependent. We do however need to specify the MAC/IAPP interface, and the minimum functionality required.
Minimum functional requirements:
The following functions seem needed between the New-AP and Previous-AP over the DS.

- Remote dis-associate — Dis-associate the station at the Previous-AP.
- Confirm dis-associate — Response from Previous-AP

The following function is needed between the New-AP and the DS.

- Notify Association to the DS — Communicate new association with the DS, which should replace the previous "Station Location" information in the DS.

Please note that multiple exchanges may be needed to obtain this functionality.
Per DS this will translate into a number of frame formats and associated parameters that need to be specified. For a MAC level bridge based DS, the only parameter needed for the latter function is I think the stations 48 bit IEEE address.

Additional functions are needed to support the traffic recovery strategy. Parameters in the "Remote dis-associate" could control the buffer control function at the Previous-AP.
In addition an interface needs to be specified between the MAC and IAPP to support the functionality.

It is an issue what information needs to be provided to perform this functionality for especially a Router based DS.
One of the parameters that might play a role here could be the Initial-AP, which identifies the AP with which the initial association is being performed.

Conclusion :

- An Inter Access Point Protocol (IAPP) is needed to provide for communication between AP's and between an AP and the DS to provide part of the functionality required for Handoff.
- Several IAPP's need to be standardized to allow multi vendor AP compatibility.
- As a minimum 802.11 should be responsible for a MAC level bridge based DS configuration IAPP standard.
- The algorithms used to start the scanning process do not need to be standardized and can be vendor specific.
- For a user, seamless communication means that temporary traffic disruptions are tolerable, but the communication sessions/connections should be maintained, so that no user intervention is needed to restore communication.
- A mobility requirement for Network Operating Systems is that they should allow for a relative high communication disruption tolerance.
- Frames required for (re-)Association function have been defined.
- A minimum set of functions for the IAPP have been defined, but need further refinement.

Issue's:

- What organization will be responsible for the IAPP standardization
- Does the standard need to specify performance limits for the scanning and subsequent handoff process.
- What strategy should be used for handling the buffered traffic that still resides at the Previous-AP (flushing or recovery strategy). This will have effec on the MAC to IAPP interface.
- What information needs to be provided from the MAC to the IAPP to provide the necessary hooks for handoff across a variety of DS's.
- The interface between the MAC and IAPP needs to be defined in the standard.

References:

[1] DFWMAC Distributed Foundation Wireless MAC Protocol", W. Diepstraten NCR-WCND-Utrecht, G. Ennis Symbol Technologies, P. Belanger Xircom; Novenber 93, IEEE P802-93/190. See also P802.11-93/191, P802.11-93/192, P802.11-93/193.