IEEE 802.11
Wireless Access Method and Physical Specification

Title: Draft Inter Access Point Protocol (IAPP) Specification.

Prepared by:

Wim Diepstraten
Lucent Technologies
Nieuwegein The Netherlands
Tel: (31)-3060-97482
Fax: (31)-3060-97556
Email: WDiepstraten@Lucent.com

Mike Trompower
Aironet Wireless Communications, Inc.
Akron, Ohio
Tel: (330) 665-7920
Fax: (330) 665-7301
Email: mtrom@aironet.com

Abstract: This paper introduces the IAPP protocol specification as has been prepared by Aironet, Digital Ocean and Lucent Technologies.
It is addressing a system interoperability issue that has not been covered by the 802.11 standard, which is limited to the "over the air" interface, by specifying an "Inter Access Point Protocol" (IAPP) to allow communication between AP's over the Distribution System.

Request for comments:

You are invited to comment on the draft specification, which will be considered for inclusion in the next revision of this document.

Document Maintenance provisions:

This specification is currently under development and this document is subject to change without notification.

To receive the latest version of the IAPP specification or to provide suggestions or improvements, please contact the following:

Aironet Wireless Communications, Inc.:
Michael Trompower
mtrom@aironet.com

Lucent Technologies:
Henri Moelard
moelard@lucent.com

Wim Diepstraten
WDiepstraten@Lucent.com

Lucent Technologies
Bell Labs Innovations

Inter Access Point Protocol

IAPP Functional Specifications

Revision 1.1

Table of Contents

0.0 Revision History

Revision	Date	Description
1.1	09 Jul 96	Editorial corrections, added DO logo
1.0	25 Jun 96	Initial Release

This specification is currently under development and this document is subject to change without notification.

To receive the latest version of the IAPP specification or to provide suggestions or improvements, please contact the following:

Aironet Wireless Communications, Inc.:
Michael Trompower
mtrom@aironet.com

Lucent Technologies:
Henri Moelard
moelard@lucent.com

1.0 Overview

A typical IEEE 802.11 wireless LAN system consists of a collection of wireless LAN adapters, and Access Points interconnected via a distribution system. The IEEE 802.11 standard focuses on the over-the-air interactions of wireless LAN products and does not provide a complete product specification for a wireless LAN system. This document focuses on specifying those aspects of the system that are not fully defined by the IEEE 802.11 draft standard.

Figure 1 shows the system architecture for an 802.11 system. Stations are associated with a particular Access Point. A group of stations and their AP is called a Basic Service Set (BSS). To extend the wireless coverage area, multiple BSS are connected by a Distribution System to form an Extended Service Set (ESS). The ESS can be viewed as a single logical network. Stations from any BSS can communicate with stations from any other BSS. In addition, direct communication is possible between any wireless station and any station in the distribution system if an Integration Service is present in the APs. For example, the Integration service will allow a station in a BSS to communicate with a server that is a node in the Distribution System.

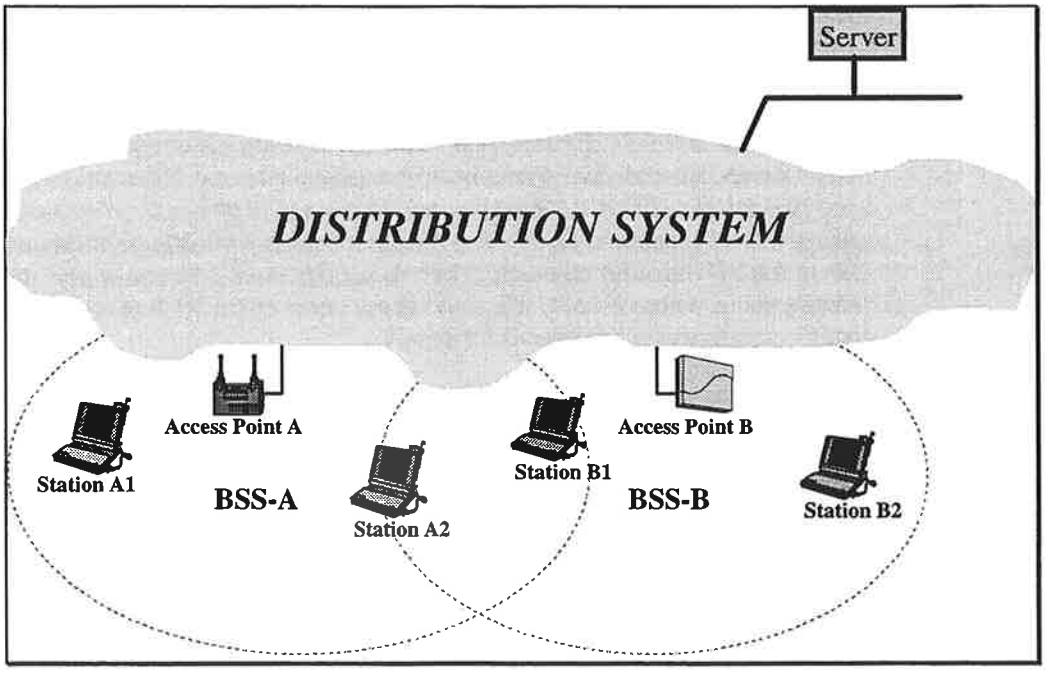

Figure 1 - Wireless LAN System Architecture

The internals of the Distribution System are not defined by IEEE 802.11 and there is no exposed interface to the Distribution System. The integration between the distribution system and IEEE 802.11 networks is handled entirely in the Access Point and is transparent to the applications and network software running on both ends. Figure 2 provides a pictorial view of the applicable protocol stackup.

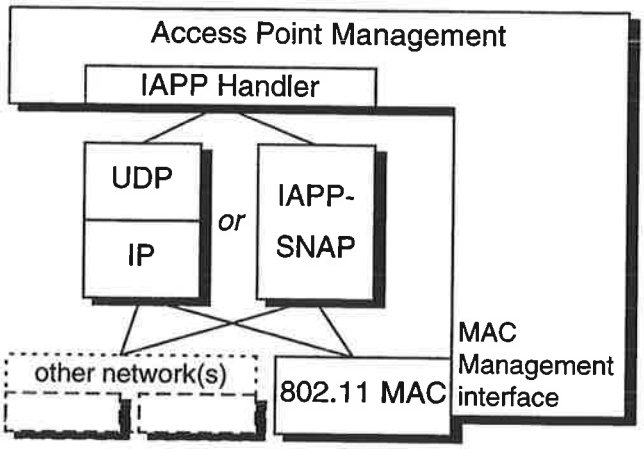

Figure 2 - IAPP protocol stackup

The IEEE 802.11 system supports mobility across BSS boundaries. Stations may move from one BSS to another and maintain their higher level network connections. This mobility is enabled through the use of IEEE 802.11 management frames and an Inter Access Point Protocol (IAPP) that is used to communicate on the distribution system (wired or wireless). The IAPP is implemented on top of IP so that it will work across router boundaries.

The Inter Access Point Protocol (IAPP) builds on the baseline capabilities of the IEEE 802.11 standard to define methods which facilitate interoperability among IEEE 802.11 compliant devices. The IAPP is implemented on top of IP and is an extension to existing management protocols. By specifying how access points will communicate with each other, the IAPP defines methods to handle access point awareness as well as roaming by mobile stations across cells. It is also not the intent of the IAPP to resolve all addressing issues across router boundaries for instance.

In order to allow operation over a wide range of networks, two transfer protocols will be implemented: UDP/IP and 802.2 Sub-Network Access Protocol (SNAP). Whenever an IP address is present in the access point, the UDP/IP will be used. SNAP will be used in cases where an IP address is not assigned to the access points desiring to communicate.

2.0 General Message Format

The IAPP specification allows for great flexibility in implementation by the utilization of messages referred to as Protocol Data Units (PDUs). Each PDU consists of elements which define capabilities. IAPP PDUs contain mandatory elements as well as optional elements. Optional elements are qualified as such in the PDU specifications below. With one exception, PDU-Elements may be inserted in any sequence (this exception is detailed below). The general IAPP PDU format is shown in Table 1.

Field sub-field	Length (octets)	Description
Transfer protocol header(s)	variable	Depending on transfer protocol(s) selected, and type of network.
PDU	variable	The IAPP Protocol Data Unit
Version Number	1	The applicable IAPP version number
PDU-Type	1	Identifies the specific PDU
n * PDU-Element (each consisting of:)	3+Length	PDU data element field(s)
Element-ID	1	Identification of the element
Length	2	Length of the element's Data field (number of octets)
Data	Length	Data of the element

Table 1 - General IAPP PDU format

Figure 3 - General IAPP PDU message

In accordance with appendix B of the RFC791 IP protocol specification, the order of transmission of the header and data described in this document is resolved to the octet level. Whenever a diagram shows a group of octets, the order of transmission of those octets is the normal order in which they are read in English. Whenever an octet represents a numeric quantity, the left most bit in the diagram in the high order or most significant bit. When a multi-octet quantity is transmitted, the most significant octet is transmitted first.

2.1 Transfer Protocol Header(s)

2.1.1 SNAP Header

Field sub-field	Length (octets)	Value (hex)	Description
MAC protocol header(s)	variable		Depending on the type of LAN (802.3, 802.5, 802.11).
SNAP Header	8		The SNAP header
DSAP	1	AA	Destination LLC SAP indicates that this is a SNAP message
SSAP	1	AA	Source LLC SAP indicates that this is a SNAP message
CTRL	1	03	CTRL field indicates an Unnumbered Information frame
PID	5		Protocol Identifier
OUI	3	*TBD*	Organizationally Unique Identifier
Specific ID	2	*TBD*	Specific ID code, allocated to IAPP

Table 2 - SNAP header description

Messages can be specifically addressed to one AP, or be group addressed to all APs. The all APs MAC group address is: 0x(*OUI* OR 0x01-00-00)-*00?-00?-00?*.

2.1.2 UDP/IP Header

Field sub-field	Length (octets)	Value (hex)	Description
MAC (or link layer) protocol header(s)	Depending on the type of network (DIX-Ethernet, 802.3, 802.5, 802.11, etc.). 802 LANs require RFC 1042 encapsulation.		
IP Header	20		The IP header
Version/IHL	1	45	IP Version (4), and IP Header length (5 32-bit words)
Type	1	00	Type of Service (normal, routine)
Length	2	number of octets	Total length of the IP datagram
Identification	2	00	Identification for fragmentation
Flags/Fragment	2	?	Fragmentation flags, and offset.
TTL	1	?	Time to Live
Protocol	1	11	The UDP protocol number (17)
Header Checksum	2	00??	Checksum of the IP Header
Source Address	4	coded	IP Source Address
Destination Address	4	coded	IP Destination Address
			Note: No options
UDP Header	8		The UDP header
Source Port	2	*TBD*	*Number to be requested from IAB*
Destination Port	2	*TBD*	*Number to be requested from IAB*
Length	2	number of octets	Total length of the UDP datagram
Checksum	2	00??	Checksum of the UDP Header

Table 3 - UDP/IP header description

Messages can be specifically addressed to one AP, or be group addressed to all APs or to an AP management function. The UDP/IP group addressing is achieved as follows:
MAC Destination Address: 0xFFFFFFFFFFFF (broadcast)
IP Destination Address: "All-subnets broadcast"?
(Note: This requires ASB to be enabled on routers)

2.2 Version Number

The PDU will have a single octet used to indicate the IAPP version number. The current defined values are shown in Table 4.

Value (hex)	Version Description
00	reserved
01	initial release
02-FF	reserved

Table 4 - IAPP Version Number description

2.3 PDU Types

The IAPP protocol is implemented using the following PDUs. The PDU type is defined by a single octet according to Table 5.

Value (hex)	PDU Type
00	ANNOUNCE.request
01	ANNOUNCE.response
02	HANDOVER.request
03	HANDOVER.response
04 -FF	reserved

Table 5 - IAPP PDU Types

2.4 PDU-Element Definitions

IAPP functionality is implemented according to the elements shown in Table 6 and described in section 2.5.

ID (hex)	Data field Length	Data (hex)	**Name** Description
00-7F			Generic standard elements
00	1-33	string	**ESSID**
01	6	hex string	**BSSID**
02	6	hex string	**OLD BSSID**
03	6	hex string	**MS-Address**
04	1	see below	**IAPP Capability / Status**
05	2	kμsec	**Periodic Announce Interval**
06	2	seconds	**Station Staleout Time**
07	2	kμsec	**Handover Time-out**
10	1	see below	**PHY-Type**
11	1	see below	**Regulatory-Domain**
12	1	see below	**Channel**
13	2	kμsec	**Beacon-Interval**
80-FF			Reserved for proprietary elements
80	3		**IEEE OUI company identifier**

Table 6 - IAPP element definitions

Note: The high-order bit of the element ID indicates Generic vs Proprietary specific elements:

- 0xxx xxxx = Generic standard elements
- 1xxx xxxx = Proprietary elements

Note: kμsec is a unit of time consisting of 1024 microseconds (μsec) as defined in the 802.11 specification.

As a general procedure, all unrecognized elements will be discarded.

Elements can appear in any order with the following exception: it is required that the IEEE OUI company identifier precede all proprietary elements which pertain to that company (the x80 company identifier element is only required once to preface a block of proprietary elements).

It is also a requirement that all proprietary elements adhere to the 2 byte length field so that proper element boundary determination can be accomplished. (The length field is zero based and will be ordered MSB to LSB). All proprietary elements must also adhere to the RFC791 IP protocol specification data descriptions.

2.5 PDU-Element Descriptions

ESSID (0x00) - a null terminated string which identifies a set of one or more interconnected Basic Service Sets and integrated LANs.

BSSID (0x01) - the MAC address of the particular access point initiating an IAPP message. In the case of HANDOVER exchange, this address is the BSSID of the access point (new AP) with the mobile station has just associated. The address field is a 48 bit address according to IEEE Std 802-1990.

OLD BSSID (0x02) - the MAC address of a referenced access point. In the case of a HANDOVER exchange, this address BSSID of the access point (old AP) from which the station just left. The address field is a 48 bit address according to IEEE Std 802-1990.

MS-Address (0x03) - the MAC address of the mobile station. The address field is a 48 bit address according to IEEE Std 802-1990.

IAPP Capability / Status (0x04) - this single byte element enumerates the current operational mode of the particular access point and/or management function.

Bit position								Description
X								IAPP operation mode 0 = slave mode 1 = master mode
	X							frame forwarding support 0 = not supported / disabled 1 = enabled
		X						WEP support 0 = not supported / disabled 1= enabled
			X					response(s) requested 0 = no response 1 = response desired
				-	-	-	-	undefined / not used

Table 7 - Capability / Status element descriptions

Periodic Announce Interval (0x05) - this two byte field identifies the number of kμsec which will occur between successive ANNOUNCE.response frames. This functionality can be used as an 'alive' indication. A value of 0x0000 in this element is used to indicate the functionality is either disabled or does not exist.

Station Staleout Time (0x06) - this two byte field identifies the number of seconds which will pass before an AP will remove a station from a preauthentication state. A value of 0x0000 in this element indicates that the access point does not support the preauthentication capability (or has it disabled) but forces that any station must use the authentication process each time it associates.

Handover Timeout (0x07) - this two byte field identifies the number of kμsec which a particular access point will wait before attempting to re-initiate a handover sequence.

PHY Type (0x10) - this single byte element is used to identify the 802.11 PHY associated with this BSSID.

Data Value	PHY Type
00	reserved
01	2.4 GHz 802.11 DS PHY
02	2.4 GHz 802.11 FH PHY
03	802.11 IR PHY

Table 8 - PHY Type element description

Regulatory Domain (0x11) - this single byte element is used to identify the current 802.11 regulatory domain under which this BSSID is functioning. The allowed values for this element are those currently defined in the 802.11 specification.

Channel (0x12) - this single byte element is used to identify the current 802.11 channel selection. Depending on the particular PHY type, the data field of this element is encoded according to the following:

PHY-Type	Description	Data Value
01	DS channels (1-12)	1 - 12
02	xx = pattern set (1-3) yyyy = sequence (1-26)	xx0yyyyy
03	IR	

Table 9 - Channel element description

Beacon Interval (0x13) - this two byte element is used to identify the current 802.11 beacon interval in kμsec.

IEEE OUI company identifier (0x80) - this three byte element is used to identify a particular access point manufacturer. Management is handled via the IEEE OUI management office. Current IAPP participants are shown in the following table:

Data Value	Current IAPP Participants
004096	Aironet Wireless Communications, Inc.
08006A	Lucent Technologies
0020CA	Digital Ocean

Table 10 - IAPP participant OUI identifiers

3.0 Announce Protocol

The intention of this protocol is to:

- inform the other access points that a new access point has become active,
- inform other access points and/or network management functions of the continued operation of a particular access point,
- inform the access points of network-wide configuration information,
- allow for a network management function to provide AP coordination.

There are several methods of providing AP coordination using both solicited and unsolicited message schemes. One method is the central control method which involves a network management function which provides coordination of all APs. This function can exist as a task running in a 'master AP' or as a separate entity on the network. A second method is the distributed control method which requires all APs to have some intelligence to chose its operating modes. A third method is the uncoordinated method where a newly powered AP arbitrarily chooses an operating configuration and just informs all other APs of its newly established operation.

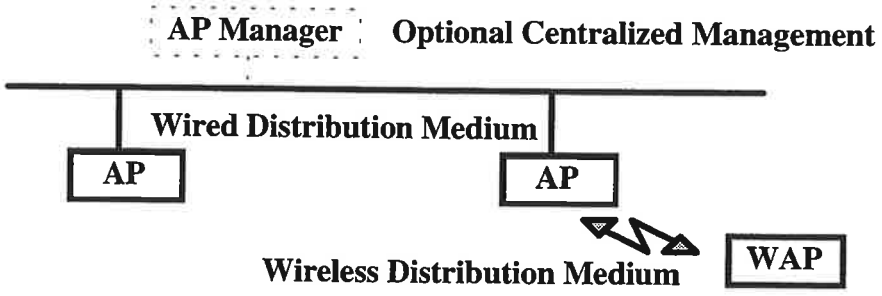

Figure 4 - AP Management Topologies

Since the 802.11 specification does not currently define how wireless AP's will be implemented, the IAPP ANNOUNCE messages will be the means by which a wireless AP will register (a wireless AP does not associate in the 802.11 sense with a wired AP) with another AP. Registration is equivalent to a higher level association. Network topology may require that the message be relayed in order to reach all APs. Normal network operation should facilitate this function. Repeated use of the ANNOUNCE message will maintain the registration status among the APs.

3.1 Announce Procedures

The simplest method, the uncoordinated AP method, requires only informative messages. No formal exchanges among APs are required. A new AP will choose a configuration, either arbitrarily or from a local management function, and send a broadcast ANNOUNCE.response with the reply switch disabled.

An ANNOUNCE.response packet is also used to accomplish the periodic ANNOUNCE function ('alive' indication) which is used to notify all APs and/or a network management (AP management) function of the continued operation of a particular access point. The ANNOUNCE.response packet is also used to provide an update capability for the

distributed control method. The ANNOUNCE.response packet is used in these instances of unsolicited messages because of the mandatory elements which make up this message.

In the central control method, a new AP will send a broadcast ANNOUNCE.request packet to the distribution system. The network management function will respond with an ANNOUNCE.response (with the MASTER bit set in the Control/Status element) packet directed to the new AP. The response packet will contain information which will establish the operating characteristics of the new AP. Once a master AP function has been determined to be functional, all non-master APs shall not respond to any broadcast ANNOUNCE packets.

In the distributed control method, a new AP will send a broadcast ANNOUNCE.request packet to the distribution system. All operating APs will respond with their current operating characteristics (an AP connected to the distribution system has the option of responding for all wireless APs currently registered with it). Each AP will respond with an ANNOUNCE.response packet which informs the new AP of its operating characteristics. The new AP will wait a reasonable amount of time to insure that all APs have time to respond. With the information just gathered, the new AP will determine an operational mode which will not conflict with (or minimally conflicts) with the current APs. The new AP will send a second ANNOUNCE.request (with a no response indication) packet which informs all APs of its operational mode.

3.2 Announce PDUs

The Announce-AP messages between access points are:

- ANNOUNCE.request (from new access point to all access points or a network management function),
- ANNOUNCE.response (from a network management function or all access points to new access point or from an existing AP to all access points and/or network management function).

The valid ANNOUNCE message exchanges are as follows:

I. The uncoordinated AP method requires that a single ANNOUNCE.response message be sent from the new AP to all existing APs. This allows a new AP to identify itself and its operational status. This message is a general broadcast sent from a new AP with the response switch disabled.

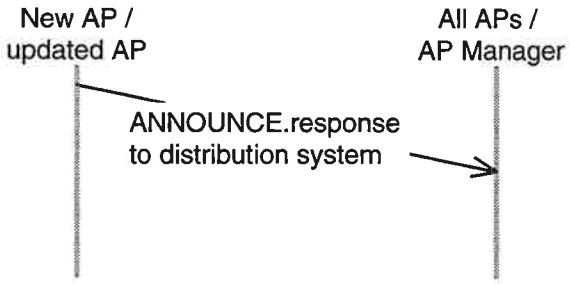

Figure 5 - ANNOUNCE exchange

II. The central control Method begins with an ANNOUNCE.request message with the response switch enabled from the new AP. The AP management function will

respond with an ANNOUNCE.response (with the MASTER bit set). All existing APs will not respond. This response will contain the operational state with which the new AP will establish operation.

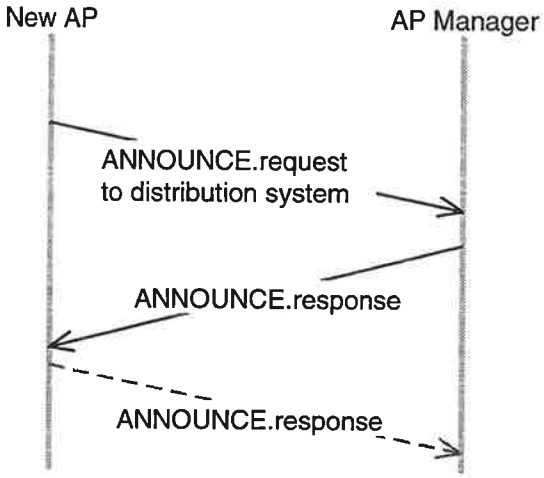

Figure 6 - ANNOUNCE exchange

Optionally, the Response Desired switch could be enabled in the ANNOUNCE.response message from the AP management function. This will generate a new ANNOUNCE.response (with the response switch disabled) from the new AP which contains its current operating state.

III. In the central control method, the AP management function could query the current status of each AP by generating an ANNOUNCE.request message with the response desired switch enabled. Depending upon addressing, the addressed AP or all APs will respond with their current operational status.

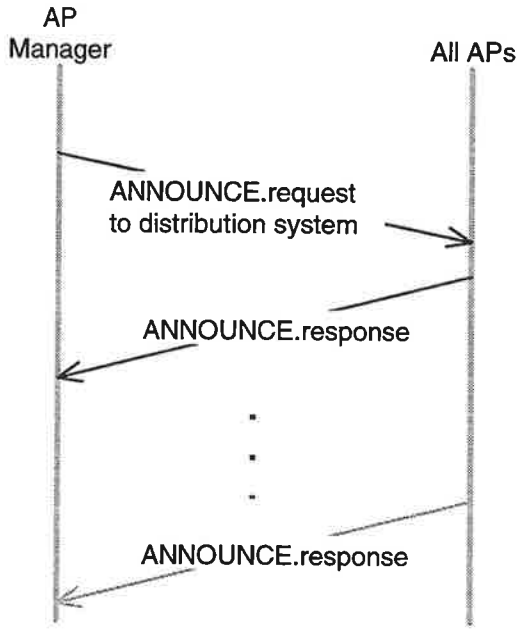

Figure 7 - ANNOUNCE exchange

IV. Under distributed control operation, the new AP will generate an ANNOUNCE.request with the response desired switch enabled. Each AP will respond with an ANNOUNCE.response message. After an appropriate time interval which assures that all current APs will have time to respond, the new AP will then respond with an ANNOUNCE.response message informing all existing APs of its operational status.

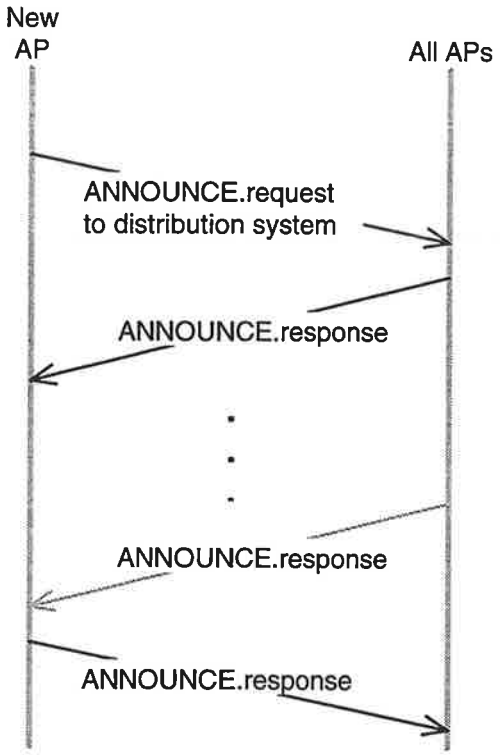

Figure 8 - ANNOUNCE exchange

3.2.1 ANNOUNCE.request

Mandatory element fields are shown below. The value in the length column includes all fields associated with the element.

ANNOUNCE.request mandatory elements			
Field sub-field	element #	Length (octets)	Description
Version Number		1	operational version
PDU Type		1	ANNOUNCE.request
ESSID	00	4-36	ESSID text
BSSID	01	9	AP MAC address
Capability	04	4	IAPP capabilities
PHY type	10	4	FH/DS/IR

Table 11 - ANNOUNCE.request mandatory elements

Optional element fields are shown below. The value in the length column includes all fields associated with the element.

ANNOUNCE.request optional elements			
Field sub-field	element #	Length (octets)	Description
Reg Domain	11	4	Regulatory Domain in operation
Channel	12	4	Channel of operation
Beacon Int	13	5	Current Beacon interval
Prop Name	80	6	IEEE OUI company identifier
			all other proprietary elements

Table 12 - ANNOUNCE.request optional elements

Source = New AP
Destination = All APs, AP management

3.2.2 ANNOUNCE.response

Mandatory elements are shown below. The value in the length column includes all fields associated with the element.

ANNOUNCE.response mandatory elements			
Field sub-field	element #	Length (octets)	Description
Version Number		1	operational version
PDU Type		1	ANNOUNCE.response
ESSID	00	4-36	ESSID text
BSSID	01	9	AP MAC address
Capability	04	4	IAPP capabilities
Announce Int	05	5	Periodic ANNOUNCE Interval
Staleout	06	5	Station Staleout Time
Handover Timeout	07	5	Handover Timeout
PHY type	10	4	FH/DS/IR
Reg Domain	11	4	Regulatory Domain in operation
Channel	12	4	Current DS Channel / FH Set
Beacon Int	13	5	Current Beacon interval

Table 13 - ANNOUNCE.response mandatory elements

Optional element fields are shown below. The value in the length column includes all fields associated with the element.

ANNOUNCE.response optional elements			
Field sub-field	element #	Length (octets)	Description
Prop Name	80	6	IEEE OUI company identifier
			all other proprietary elements

Table 14 - ANNOUNCE.response optional elements

Source = The "master" AP / individual APs
Destination = New AP / All APs?

4.0 Handover Protocol

The intention of this protocol is to:

- inform the old access point that a station is taken over by another access point;
  - to release the resources that the old access point had assigned to support the station,
  - update its filter table to forward frames destined for the station appropriately,
  - discard or forward frames buffered in the old access point for the station,
- update filter tables of intermediate MAC-bridges to forward frames destined for the station appropriately.

4.1 Handover Procedures

4.1.1 Normal Handover Procedure

The Handover procedure is tied into the IEEE 802.11 Reassociation procedure; it is initiated when an access point receives a Reassociation-request from a mobile station. The Reassociation messages between mobile station and access point (Reassociation-request and Reassociation-response) are part of the IEEE 802.11 MAC protocol.

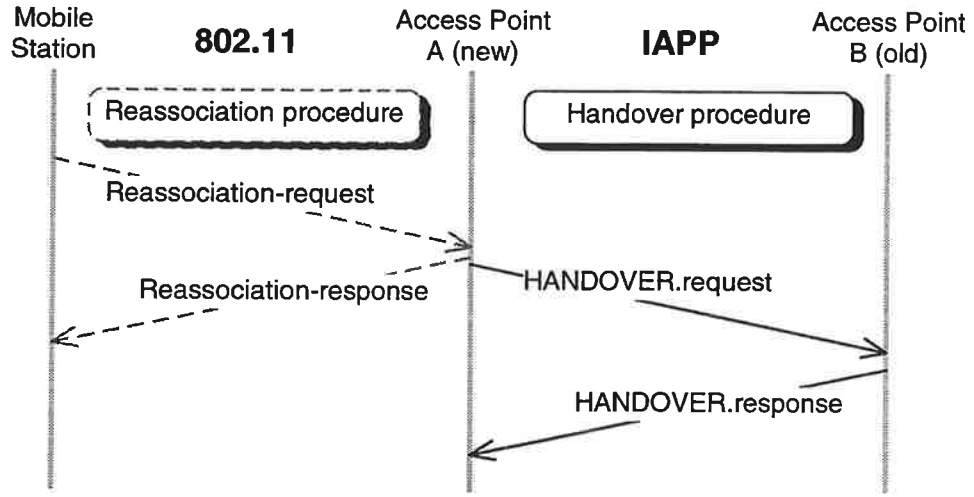

Figure 9 - HANDOVER exchange

The above figure depicts the Reassociation-response being delivered to the mobile station before the HANDOVER.response is received by the new AP. The timing for sending the Reassociation-response is implementation dependent which allows for the Reassociation-response to be delivered after the receipt of the HANDOVER.response. This allows for full implementation flexibility.

From the time the Reassociation-request is sent until receipt of the Reassociation-response, the mobile station must not send any data frames.
If during the Handover procedure a (retried) Reassociation-request is received from the (same) mobile station, the 802.11 Reassociation procedure is completed normally, but no additional HANDOVER sequence will be initiated.

4.1.2 Handover Retransmission

The new access point (A) is responsible for recovery of the Handover procedure. If the HANDOVER.response is not received within a certain time as established by the Handover timeout as identified by element 0x07, the HANDOVER.request is retransmitted over the distribution system. The Handover timeout can be set by a local management function or via a global access point management function which accounts for any distribution system structure dependencies.

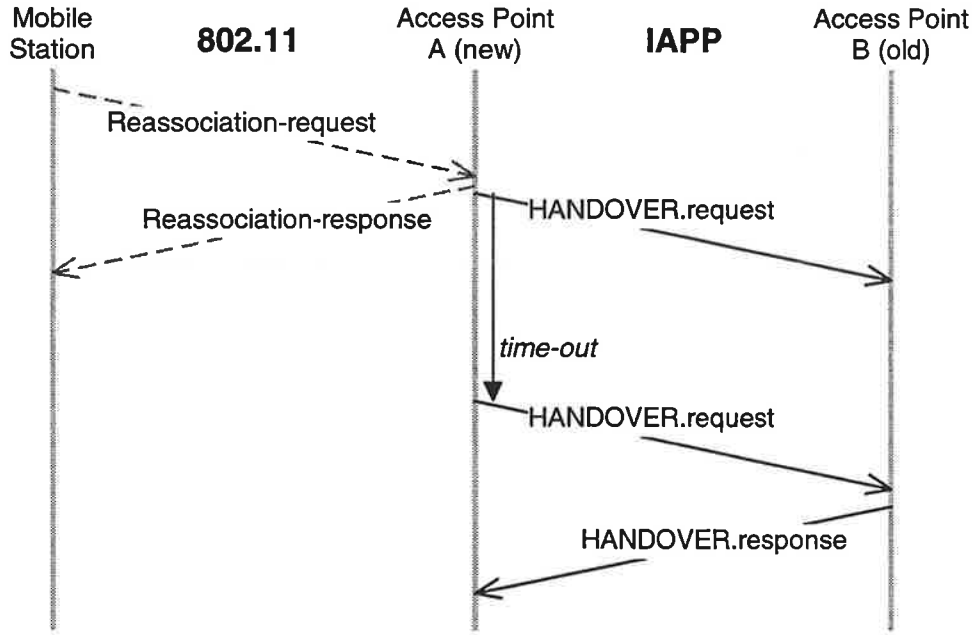

Figure 10 - HANDOVER exchange

If no HANDOVER.response is received at all (after x retries), the Reassociation procedure is completed by the new access point. The number of retries is determined by a local management function and will vary according to particular implementations.

This behavior ensures that if the old access point is not reachable (it died, got disconnected, is on the other side of a router or gateway, or the distribution system is temporarily out of service), the MAC services of the mobile station can continue.

4.1.3 Handover Network Recovery

After a handover has failed (due to e.g. a temporary distribution system outage), filter tables of intermediate bridges may not be up-to-date on the location of the mobile station. This can be recovered, by regularly sending a message on behalf of the mobile station onto the distribution system.
Using the HANDOVER.request to the old access point as 'recover' message has the following advantages:

- the association between the mobile station and the old access point is cleaned-up, in case it would still exist and one of the messages gets through;
- the recovery can be stopped when the old access point sends a response (which is likely if the handover failure was caused by a temporary network outage);
- it traverses only that part of the distribution system that possibly needs updating;
- a unicast frame is not likely to be filtered (as a multicast/broadcast may);

- no new frame type is introduced.

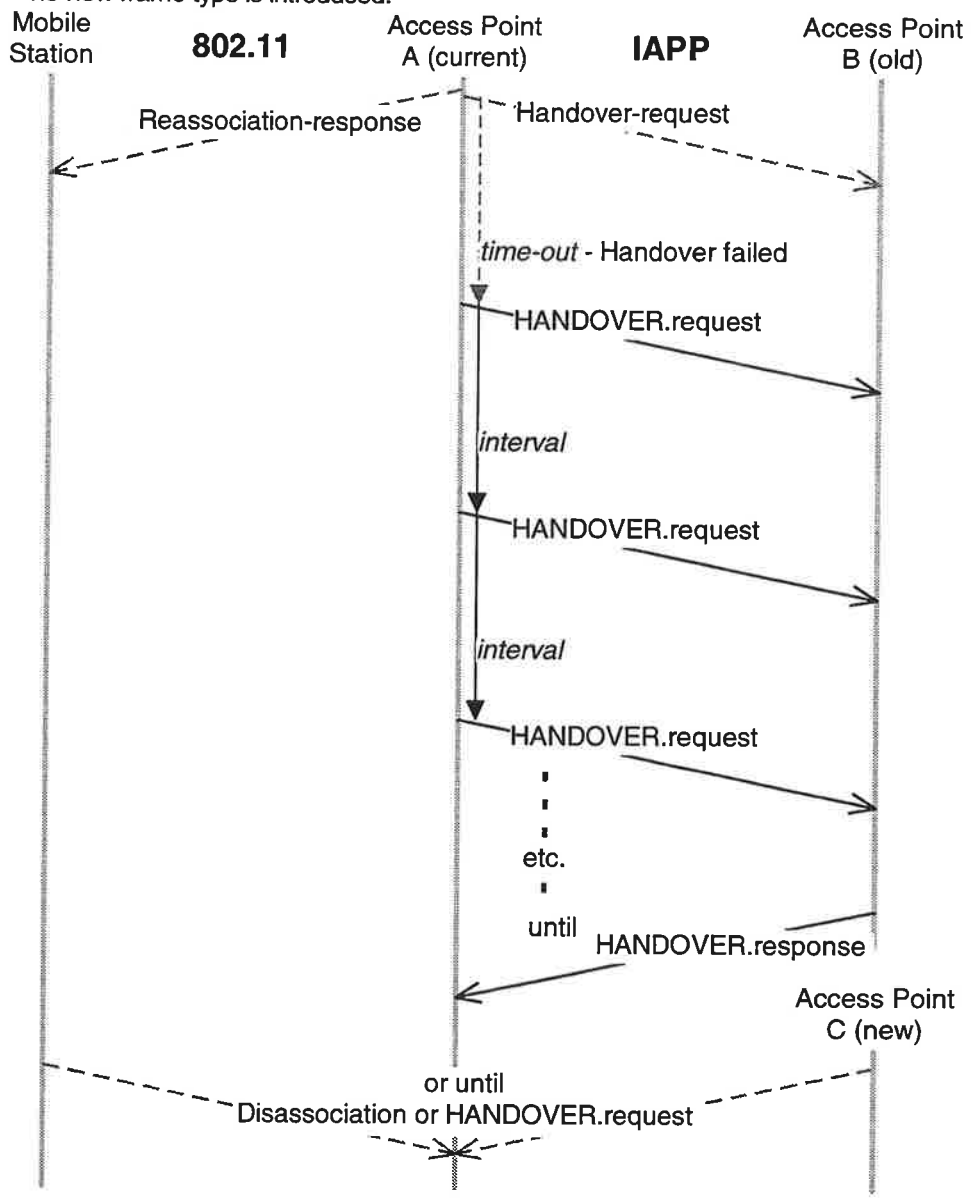

Figure 11 - HANDOVER exchange

4.2 HANDOVER PDUs

The HANDOVER messages between access points are:

- HANDOVER.request (from new access point to old access point),
- HANDOVER.response (from old access point to new access point).

4.2.1 HANDOVER.request

Mandatory element fields are shown below. The value in the length column includes all fields associated with the element.

HANDOVER.request mandatory elements			
Field sub-field	element #	Length (octets)	Description
Version Number		1	operational version
PDU Type		1	HANDOVER.request
ESSID	00	4-36	ESSID text
BSSID	01	9	AP MAC address
OLD BSSID	02	9	old AP MAC address
MS-Address	03	9	Mobile Station address
Capability	04	4	IAPP capabilities

Table 15 - HANDOVER.request mandatory elements

Optional element fields are shown below. The value in the length column includes all fields associated with the element.

HANDOVER.request optional elements			
Field sub-field	element #	Length (octets)	Description
PHY type	10	4	FH/DS/IR
Reg Domain	11	4	Regulatory Domain in operation
Channel	12	4	Current DS Channel / FH Set
Beacon Int	13	5	Current Beacon interval
Prop Name	80	6	IEEE OUI company identifier
			all other proprietary elements

Table 16 - HANDOVER.request optional elements

Source = MAC source address: MAC address of mobile station this handover is done for.
(to get bridge filter tables updated; only on new network segment)
IP source address: New AP
Destination = Old AP

In case of UDP/IP, the ANNOUNCE.request message will provide both the new APs BSSID and its IP address. During a handover, the Reassociation packet will provide only the BSSID of the old AP, therefore, a table look up will be required in order to obtain the IP address of the old AP in order to complete the handover.

4.2.2 HANDOVER.response

Mandatory element fields are shown below. The value in the length column includes all fields associated with the element.

HANDOVER.response mandatory elements			
Field sub-field	element #	Length (octets)	Description
Version Number		1	operational version
PDU Type		1	HANDOVER.response
ESSID	00	4-36	ESSID text
BSSID	01	9	AP MAC address
OLD BSSID	02	9	old AP MAC address
MS-Address	03	9	Mobile Station address
Capability	04	4	IAPP capabilities

Table 17 - HANDOVER.response mandatory elements

Optional element fields are shown below. The value in the length column includes all fields associated with the element.

HANDOVER.response optional elements			
Field sub-field	element #	Length (octets)	Description
PHY type	10	4	FH/DS/IR
Reg Domain	11	4	Regulatory Domain in operation
Channel	12	4	Current DS Channel / FH Set
Beacon Int	13	5	Current Beacon interval
Prop Name	80	6	IEEE OUI company identifier
			all other proprietary elements

Table 18 - HANDOVER.response optional elements

Source = Old AP
Destination = New AP
Note: In case of UDP/IP, MAC address is determined via ARP (not from request).