

3 **Draft**
4 **Recommended Practice for Multi-Vendor Access Point**
5 **Interoperability via an Inter-Access Point Protocol**
6 **Across Distribution Systems Supporting IEEE 802.11**
7 **Operation**

8 Sponsored by the
9 LAN/MAN Standards Committee
10 of the
11 IEEE Computer Society

12
13 Copyright © 2002 by the Institute of Electrical and Electronics Engineers, Inc.
14 345 East 47th Street
15 New York, NY 10017, USA
16 All rights reserved.

17 This is an unapproved draft of a proposed IEEE Recommended Practice, subject to change. Permission is hereby
18 granted for IEEE Standards Committee participants to reproduce this document for purposes of IEEE standardization
19 activities. If this document is to be submitted to ISO or IEC, notification shall be given to the IEEE Copyright
20 Administrator. Permission is also granted for member bodies and technical committees of ISO and IEC to reproduce
21 this document for purposes of developing a national position. Other entities seeking permission to reproduce this
22 document for standardization or other activities, or to reproduce portions of this document for these or other uses,
23 must contact the IEEE Standards Department for the appropriate license. Use of information contained in this
24 unapproved draft is at your own risk.

25 IEEE Standards Department
26 Copyright and Permissions
27 445 Hoes Lane, P.O. Box 1331
28 Piscataway, NJ 08855-1331, USA
29

1 Introduction

2 (This introduction is not part of IEEE P802.11f, Recommended Practice for Multi-Vendor Access Point Interoperability
3 via Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation.)

4 See 9.3 of the *IEEE Standards Style Manual* for information on the Introduction. Use the **heading 1** style for the
5 Introduction and the **paragraph** style for succeeding paragraphs of text. (See Clauses 1-3 in this template for
6 information about styles.)

7 *At the time this standard was completed, the working group had the following membership:*

8
9 *Stuart Kerry, Chair*

10 *David Bagby, Chair, Task Group f*

11 *Bob O'Hara, Editor, Task Group f*

12

*Put working group member
names here*

1 *The following persons were on the balloting committee: (To be provided by IEEE editor at time of publication.)*

2

1	Contents	
2	Introduction	ii
3	1 Overview.....	1
4	1.1 Scope	1
5	1.2 Purpose	1
6	1.3 Inter-AP recommended practice overview.....	1
7	2 References	4
8	3 Definitions, abbreviations, and acronyms	5
9	4 IAPP Service definition	6
10	4.1 IAPP-INITIATE.request.....	7
11	4.2 IAPP-INITIATE.confirm.....	8
12	4.3 IAPP-TERMINATE.request.....	9
13	4.4 IAPP-TERMINATE.confirm.....	9
14	4.5 IAPP-ADD.request.....	10
15	4.6 IAPP-ADD.confirm.....	11
16	4.7 IAPP-ADD.indication	11
17	4.8 IAPP-MOVE.request.....	12
18	4.9 IAPP-MOVE.confirm.....	13
19	4.10 IAPP-MOVE.indication.....	14
20	4.11 IAPP-MOVE.response.....	15
21	5 Operation of the IAPP	16
22	5.1 IAPP Protocol Overview.....	16
23	5.2 Formation and maintenance of the ESS, the Registration Service	17
24	5.3 RADIUS Protocol Usage	18
25	5.4 Support for 802.11 authentication	20
26	5.5 AP to AP Interactions.....	20
27	5.6 AP specific MIB.....	21
28	5.7 Single station association	21
29	6 Packet Formats	22
30	6.1 General IAPP Packet Format	22
31	6.2 ADD-notify Packet	23
32	6.3 Layer 2 Update Frame	23
33	6.4 MOVE-notify Packet	24
34	6.5 MOVE-response Packet.....	25
35	6.6 Send-Security-Block packet.....	25
36	6.7 ACK-Security-Block packet.....	27
37	Annex A, Management Information Base.....	29
38	Annex B, Context Transfer.....	36
39	B.1 Introduction.....	36
40	B.2 Terminology	36
41	B.3 Context transfer model.....	37
42	B.5 Security considerations	40
43	B.6 References	41
44	Appendix A - Table of Attributes	42

45

1 Figures

2	Figure 1 - AP Architecture with IAPP.....	2
3	Figure 2 - Primitive Relationships	7
4	Figure 3 - IAPP Message Exchange During STA Reassociation.....	17
5	Figure 4 - Send-Security-Block Data Field Format	19
6	Figure 5 - General IAPP Packet Format	22
7	Figure 6 - ADD-notify Data Field Format	23
8	Figure 7 - Layer 2 Update Frame Format	24
9	Figure 8 - MOVE-notify Data Field Format.....	24
10	Figure 9 - Information Element Format.....	25
11	Figure 10 - MOVE-response Data Field Format	25
12	Figure 11 - Send-Security-Block Data Field Format	26
13	Figure 12 - Send-Security-Block Data Field Format	27

14 Tables

15	Table 1 - RADIUS Access-Request Attributes	18
16	Table 2 - RADIUS Access-Accept Attributes.....	19
17	Table 3 - Information Elements in the Send-Security-Block Packet.....	20
18	Table 4 - Command field values	22
19	Table 5 - MOVE-notify Status Values	25
20	Table 6 - Information Elements in the Send-Security-Block Packet.....	26
21	Table 7 - ESP Transform Identifiers	27
22	Table 8 - ESP Authentication Algorithm Identifiers	27

23

24

Draft

Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation

1 Overview

1.1 Scope

The scope of this document is to describe recommended practices for implementation of an Inter-AP Protocol on a Distribution System (DS) supporting ISO/IEC 8802-11:1999, IEEE Standard 802.11, wireless LAN (WLAN) links. The recommended DS utilizes an Inter-Access Point Protocol (IAPP) that provides the necessary capabilities to achieve multi-vendor Access Point (AP) interoperability within the DS. This IAPP is described for a DS consisting of IEEE 802 LAN components utilizing an Internet Engineering Task Force (IETF) Internet Protocol (IP) environment. Throughout this recommended practice, the terms ISO/IEC 8802-11:1999, IEEE 802.11, and IEEE Std. 802.11-1999 are used interchangeably to refer to the same document, ISO/IEC 8802-11:1999 and its amendments and supplements published at the time this recommended practice was adopted.

1.2 Purpose

IEEE 802.11 specifies the MAC and PHY layers of a WLAN system and includes the basic architecture of such systems, including the concepts of APs and DSs. Implementations of these concepts were purposely not defined by 802.11 because there are many ways to create a WLAN system. Additionally, many of the possible implementation approaches involve higher network layers. While this leaves great flexibility in DS and AP functional design, the associated cost is that physical AP devices are unlikely to interoperate across a DS. In particular, the enforcement of the restriction that a mobile station has a single association at a given time is unlikely to be achieved.

As 802.11 systems have grown in popularity, this limitation has become an impediment to WLAN market growth. At the same time, it has become clear that there are a small number of DS environments that comprise the bulk of the commercial and private WLAN system installations.

This recommended practice specifies the information to be exchanged between APs amongst themselves and higher layer management entities to support the 802.11 DS functions. The information exchanges are specified for DSs built on the IETF IP in a manner sufficient to enable the interoperation of DSs containing APs from different vendors that adhere to the recommended practice.

1.3 Inter-AP recommended practice overview

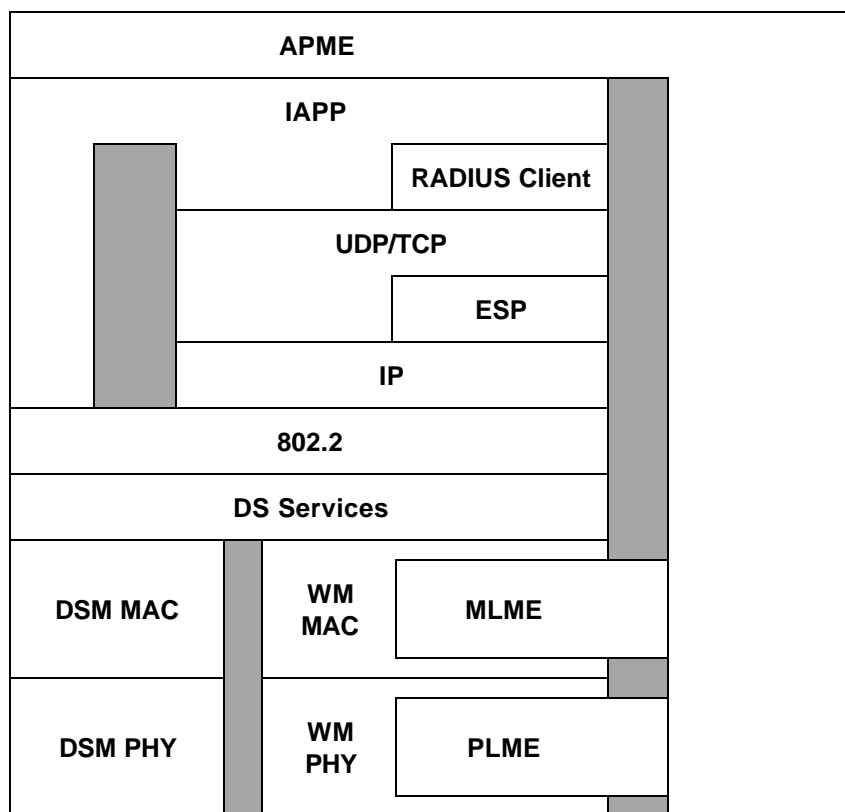
This recommended practice describes a service access point (SAP), service primitives, a set of functions and a protocol that will allow conformant APs to interoperate on a common DS, using the user datagram protocol over IP (UDP/IP) to carry IAPP packets between APs, as well as describing the use of the RADIUS Protocol, so APs may obtain information

1 about one another. The devices in a network that might use the IAPP are 802.11 APs. Other devices in a network that are
2 affected by the operation of the IAPP are layer 2 networking devices, such as bridges and switches.

3 Throughout this recommended practice, reference is made to an “AP management entity” (APME). These are references to
4 a function that is external to the IAPP, though likely still a function of the AP device. Typically, this management entity is
5 the main operational program of the AP, implementing an AP manufacturer’s proprietary features and algorithms, and
6 incorporating the station management entity (SME) of 802.11. Figure 1 depicts an architecture of a typical AP in which the
7 IAPP operates. The IAPP services are accessed by the APME through the IAPP SAP. The IAPP SAP is shown in Figure
8 1, as the line between the APME and the IAPP blocks. IAPP service primitives are defined that allow the AP management
9 entity to cause the IAPP to perform some function or to communicate with other APs in the DS or a registration service.
10 Other service primitives indicate to the AP management entity that operations have taken place at other APs in the DS that
11 can have an effect on information local to the AP.

12 The invocation of some IAPP service primitives relies on the RADIUS protocol to implement certain functions that are
13 required for the correct and secure operation of the IAPP. In particular, the IAPP entity must be able to find and use a
14 RADIUS server to register as part of an ESS, to look up the IP addresses of other APs in the ESS when given the BSSIDs
15 of those other APs, and to obtain security information to protect the content of certain IAPP packets.

16



17 **Figure 1 - AP Architecture with IAPP**

18 The IAPP is not a routing protocol. The IAPP does not deal directly with the delivery of 802.11 data frames to the station,
19 instead the DS utilizes existing network functionality for data frame delivery. The data delivery service of the DS will
20 function as desired when the 802.11 stations maintain a network layer address, e.g., IP address, or addresses that are valid
21 for their point of connection to the network, i.e., when an 802.11 station associates or reassociates, the station must
22 ascertain that its network layer address(es) is configured such that the normal routing functions of the network attaching
23 to the BSS will correctly deliver the station’s traffic to the BSS to which it is associated. If the mobile device incorporating
24 the 802.11 station determines that the network layer address(es) is not configured so as to allow the normal routing
25 functions of the network to deliver the station’s traffic to the BSS to which it is associated, the station must obtain such an

1 address(es), before any network traffic can be delivered to it. A station can meet the local IP address requirement in many
2 ways. Two mechanisms for a station to accomplish this are to renew a Dynamic Host Configuration Protocol (DHCP) lease
3 for its IP address or to use Mobile IP. Other mechanisms are possible that meet this requirement.

4 With the requirement that stations maintain a valid network layer address, APs function much the same as 802.1D bridges.
5 Additionally, the IAPP supports the following functions:

- 6 • DS Services, as defined in ISO/IEC 8802-11:1999
- 7 • Address mapping of wireless medium addresses of APs (their BSSID) to DS network layer addresses (IP
8 addresses)
- 9 • Evolution of the IAPP through multiple versions
- 10 • Formation of a DS
- 11 • Maintenance of the DS
- 12 • Enforcement of the restriction of ISO/IEC 8802-11:1999 that a station may have only a single association at any
13 given time
- 14 • Transfer of station context information between APs

15 IAPP transactions are over the DS. Hence IAPP is independent of the security scheme defined in ISO/IEC 8802-11:1999.
16 All the IAPP transactions can make use of the security schemes employed over the distribution system medium (DSM).

17 This recommended practice makes use of the IETF RFCs listed in clause 2 to implement many of its functions. It also relies
18 on a station making use of the 802.11 Reassociation Request frame when roaming from one AP to another, in order to
19 provide the most complete services to the APs using the IAPP. When a station uses the 802.11 Association Request,
20 rather than the Reassociation Request, the IAPP may not be able to notify the AP at which the station was previously
21 associated of the new association. This may result in the old AP (indicated in the "current AP" field of the reassociation
22 request frame) maintaining context for the station that has roamed to a new AP for a longer time than is strictly necessary.
23 This may cause undue waste of resources at the old AP, as well as limiting the ability of the IAPP to help enforce the single
24 station association requirement of 802.11. Where 802.1X is used for authentication, use of the Association Request
25 instead of the Reassociation Request will result in a re-authentication, potentially disrupting connectivity.

1 2 References

2 The following standards contain provisions which, through references in this text, constitute provisions of this standard.
3 At the time of publication, the editions indicated were valid. All standards are subject to revision.

- 4 IEEE Standard 802.11-1999¹
- 5 IEEE Standard 802.1X-2001 Port Based Network Access Control¹
- 6 IEEE Standard 802.2-1998 Logical Link Control¹
- 7 RFC0768 – User Datagram Protocol²
- 8 RFC0791 – Internet Protocol²
- 9 RFC1812 – Requirements for IP version 4 Routers²
- 10 RFC2131 – Dynamic Host Configuration Protocol²
- 11 RFC2181 - Clarifications to the DNS Specification²
- 12 RFC2401 - Security Architecture for the Internet Protocol²
- 13 RFC2406 - IP Encapsulating Security Payload (ESP)²
- 14 RFC2411 – IP Security Document Roadmap²
- 15 RFC2865 - Remote Authentication Dial In User Service (RADIUS)²
- 16 RFC2869 - RADIUS Extensions²

¹ IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (<http://www.standards.ieee.org/>).

² Requests for Comments (RFCs) are available from the Internet Engineering Task Force (IETF) (www.ietf.org)

1 **3 Definitions, abbreviations, and acronyms**

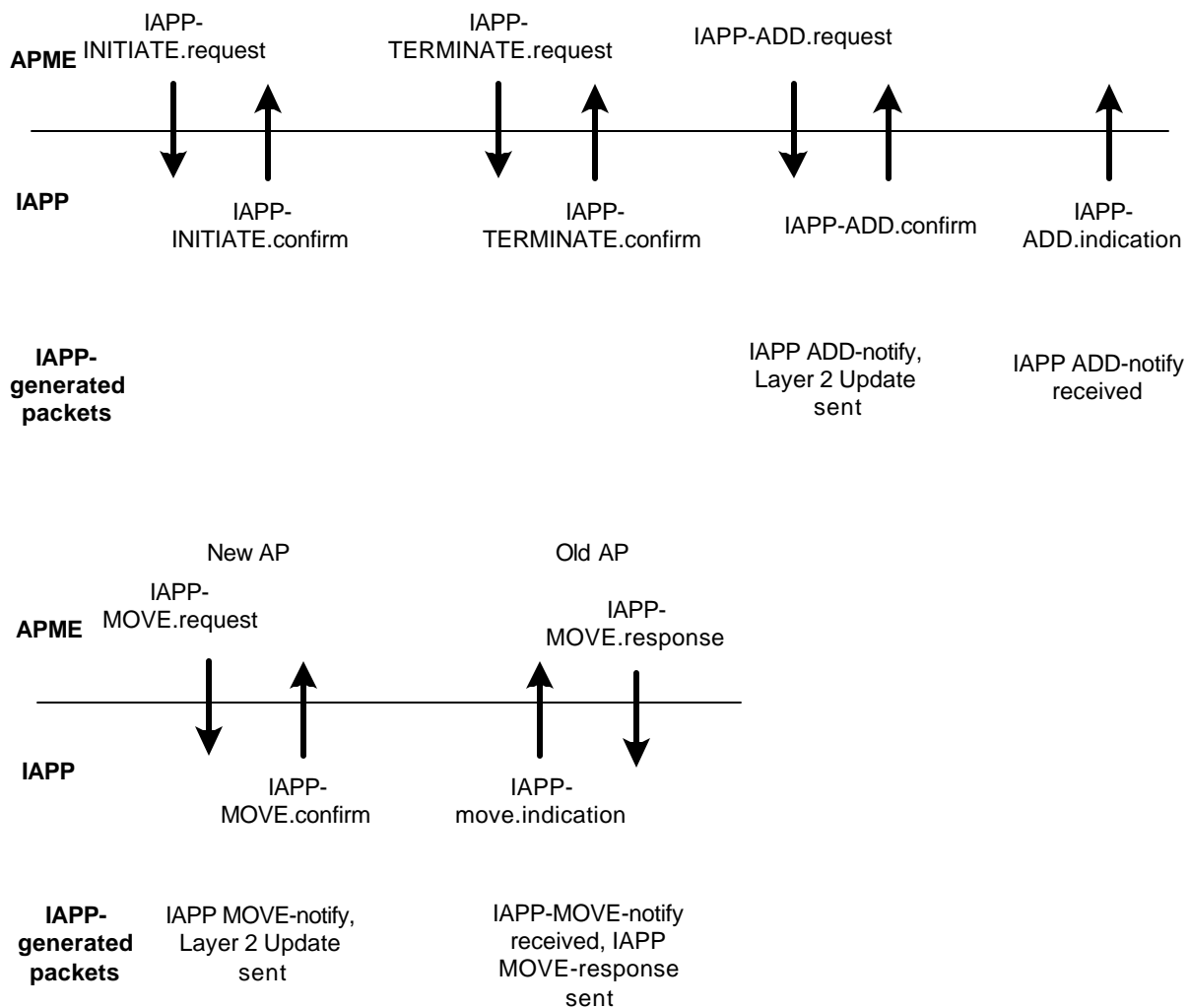
2	AP	Access Point
3	APME	Access Point Management Entity
4	BSS	Basic Service Set
5	BSSID	Basic Service Set Identifier
6	DHCP	Dynamic Host Configuration Protocol
7	DS	Distribution System
8	DSM	Distribution System Medium
9	ESP	IP Encapsulating Security Payload
10	ESS	Extended Service Set
11	IANA	Internet Assigned Numbers Authority
12	IAPP	Inter-Access Point Protocol
13	IETF	Internet Engineering Task Force
14	IP	Internet Protocol
15	IPsec	Internet Protocol Security
16	LLC	Logical Link Control
17	MAC	Medium Access Control
18	MLME	MAC Layer Management Entity
19	PAE	Port Access Entity
20	PHY	Physical layer
21	PLME	PHY Layer Management Entity
22	RADIUS	Remote Authentication Dial In User Service
23	SA	Security Association
24	SAP	Service Access Point
25	SME	Station Management Entity
26	SPI	Security Parameter Index
27	SSID	Service Set Identifier
28	TCP	Transmission Control Protocol
29	UDP	User Datagram Protocol
30	URL	Uniform Resource Locator
31	WM	Wireless Medium
32	XID	Exchange Identifier

1 **4 IAPP Service definition**

2 The IAPP entity provides services to an AP in which it resides through the IAPP SAP. The SAP allows the management
3 entity of the AP (APME) to invoke IAPP services and receive indications of service invocations at other APs in a single
4 ESS. This clause defines the services that are available at the SAP. There are four service types that exist at the SAP.
5 They are requests, confirms, indications, and responses. Service requests and responses are submitted to the IAPP entity
6 by the entity at the next higher layer. In this document, the next higher layer is the APME. Service confirms and
7 indications are delivered by the IAPP entity to the entity at the next higher layer.

8 This clause provides an abstract description of the services that an implementation should provide in order to interoperate
9 with other implementations of the IAPP. This is not an exposed interface. A diagram of the relationships between the
10 primitives is shown in Figure 2.

11



1
2

Figure 2 - Primitive Relationships

3 **4.1 IAPP-INITIATE.request**

4 **4.1.1 Function**

5 This service primitive causes the AP to initialize the IAPP entity, including its data structures, functions, and protocol.

6 **4.1.2 Semantics of the service primitive**

7 The IAPP-INITIATE.request has the following semantics.

8
9 IAPP-INITIATE.request {
10 Port,
11 Shared Secret,

```

1         IP Address,
2         BSSID Secret
3     }

```

4 The Port parameter is the UDP and TCP port number to be opened for the IAPP for transmission and receipt of IAPP
5 packets.

6 The Shared Secret is used to protect communication between the RADIUS server and the AP.

7 The IP address is the IP address or fully qualified domain name of the RADIUS server.

8 The BSSID Secret is used to protect the security block sent between the RADIUS server and the AP.

9 **4.1.3 When generated**

10 This service primitive is generated by an APME to initiate the operation of the IAPP. At the time the IAPP-
11 INITIATE.request is generated, the BSS controlled by this AP should not be operating, and no stations should be
12 associated with this AP. If necessary, the APME can issue an 802.11 MLME-RESET.request prior to generation of the
13 IAPP-INITIATE.request.

14 **4.1.4 Effect of receipt**

15 Upon receipt of this service primitive from an APME, the IAPP entity initializes its data structures, functions, and
16 protocols. The port for the IAPP should be opened by the IAPP entity at this time. The previous information in any IAPP
17 data structures is lost.

18 **4.2 IAPP-INITIATE.confirm**

19 **4.2.1 Function**

20 This service primitive notifies an APME that the actions begun by an IAPP-INITIATE.request have been completed.

21 **4.2.2 Semantics of the service primitive**

22 The IAPP-INITIATE.confirm primitive has the following semantics.

```

23 IAPP-INITIATE.confirm {
24     Status
25 }
26

```

27 The Status parameter indicates the result of the corresponding IAPP-INITIATE.request. The allowable value for the Status
28 parameter are SUCCESSFUL, RUNNING, and FAILURE. SUCCESSFUL status should be returned if the IAPP entity is able
29 to complete its initialization and open the requested port for the IAPP. RUNNING status should be returned if the IAPP
30 entity receives an IAPP-INITIATE.request when the entity is already running. FAILURE status should be returned
31 otherwise.

32 **4.2.3 When generated**

33 This service primitive is generated when the actions begun by an IAPP-INITIATE.request are completed or the invocation
34 of that primitive has failed.

35 **4.2.4 Effect of receipt**

36 Upon receipt of the IAPP-INITIATE.confirm(Status=SUCCESS) corresponding to a previously issued IAPP-
37 INITIATE.request, an APME should initialize the operation of the AP by issuing an 802.11 MLME-START.request

1 INITIATE.request primitive. Furthermore, the APME should not issue an MLME-START.request primitive prior to receipt
2 of the subsequent IAPP-INITIATE.confirm primitive which indicates that the IAPP has been restarted successfully.

3 **4.5 IAPP-ADD.request**

4 **4.5.1 Function**

5 This service primitive is used when a station associates with the AP using an 802.11 association request frame. The
6 function of the IAPP-ADD.request primitive is two-fold. One purpose of this primitive is to cause the forwarding tables of
7 layer 2 internetworking devices to be updated. The second purpose of this primitive is to notify other APs within the
8 broadcast domain of the station's new association.

9 **4.5.2 Semantics of the service primitive**

10 The IAPP-ADD.request primitive has the following semantics.

```
11  
12 IAPP-ADD.request {  
13     MAC Address,  
14     Sequence Number,  
15     Timeout  
16 }
```

17 The MAC Address is the address of the station that recently has successfully associated with the AP.

18 The Sequence Number is the value of the 802.11 Sequence Number field of the Association Request frame received from
19 the associating station. The sequence number is provided to aid the APME in other APs in the determination of whether
20 the association represented by this IAPP-ADD.request is the most recent association for the station identified by the
21 MAC Address. The 802.11 sequence number is not an unambiguous indication of the most recent association. But, this
22 information may be useful to an algorithm making this determination.

23 The Timeout parameter is the value, in seconds that the IAPP-ADD.confirm primitive will be generated with a status of
24 TIMEOUT, if both the ADD-notify packet (see 6.2) and the Layer 2 Update frame (see 6.3) have not been sent. The
25 TIMEOUT status will not be generated by the IAPP-ADD.confirm only when both the ADD-notify packet and Layer 2
26 Update frame have been transmitted before the expiration of the period indicated by the Timeout parameter.

27 **4.5.3 When generated**

28 This service primitive should be generated by an APME when an AP generates an 802.11 MLME-ASSOCIATE.indication.

29 **4.5.4 Effect of receipt**

30 Receipt of this service primitive should cause the following actions to occur:

- 31 1) The IAPP entity sends a Layer 2 Update frame to the DS, addressed such that it will cause the forwarding tables
32 in any layer 2 devices that receive the frame to be updated so that all future traffic received by those bridges is
33 forwarded to the port on which the frame was received,
- 34 2) The IAPP entity notifies the APs in the local broadcast domain of the DS of the association between the AP and
35 station by sending an IAPP ADD-notify packet to the subnet broadcast address.

1 **4.6 IAPP-ADD.confirm**

2 **4.6.1 Function**

3 This service primitive is used to confirm that the actions initiated by an IAPP-ADD.request have been completed and
4 inform an APME of the status of those actions.

5 **4.6.2 Semantics of the service primitive**

6 The IAPP-ADD.confirm primitive has the following semantics.

```
7  
8 IAPP-ADD.confirm {  
9     Status  
10 }
```

11 The Status parameter indicates the success or failure of the corresponding IAPP-ADD.request. The allowable values for
12 this parameter are SUCCESSFUL, FAIL and TIMEOUT. SUCCESSFUL status indicates that the corresponding IAPP-
13 ADD.request was able to send both the IAPP ADD-notify packet and Layer 2 Update frame before the timeout expired.
14 FAIL indicates that for some reason, the IAPP ADD-notify packet and the Layer2 Update frame could not be sent at all.
15 TIMEOUT status indicates that one or both of the ADD-notify packet and Layer 2 Update frame were not sent before the
16 timeout expired.

17 **4.6.3 When generated**

18 This service primitive is generated upon completion of the actions of the IAPP-ADD.request.

19 **4.6.4 Effect of receipt**

20 Upon receipt of this service primitive by an APME, the APME should cause the DS Services to begin forwarding frames
21 for the associated station.

22 **4.7 IAPP-ADD.indication**

23 **4.7.1 Function**

24 The IAPP-ADD.indication primitive is used to indicate to an APME that an association relationship has been established
25 between a mobile station and another AP in the DS.

26 **4.7.2 Semantics of the service primitive**

27 The IAPP-ADD.indication primitive has the following semantics.

```
28  
29 IAPP-ADD.indication {  
30     MAC Address,  
31     Sequence Number  
32 }
```

33 The MAC Address is the address of the mobile station received in the IAPP ADD-notify packet.

34 The Sequence Number is the value of the 802.11 Sequence Number field of the Association Request frame received from
35 the associating station. The sequence number is provided to aid the APME in the determination of whether the
36 association represented by this IAPP-ADD.indication is the most recent association for the station identified by the MAC
37 Address. The 802.11 sequence number is not an unambiguous indication of the most recent association. But, this
38 information may be useful to an algorithm making this determination.

1 **4.7.3 When generated**

2 This service primitive is generated upon receipt of an IAPP ADD-notify packet from the DS.

3 **4.7.4 Effect of receipt**

4 Upon receipt of this service primitive the APME should determine if the station indicated by the MAC Address is shown
5 to be associated with the AP receiving the IAPP-ADD.indication, with a sequence number older than that in the IAPP
6 ADD-notify packet. If so, this service primitive should cause the generation of an 802.11 MLME-DISASSOCIATE.request
7 by the APME. If the sequence number received in the IAPP ADD-notify packet is older than that received from the station
8 when it associated with the AP receiving the IAPP ADD-notify packet, the APME should ignore the indicated association
9 and issue an IAPP-ADD.request to ensure that layer two devices are properly informed of the location of the station's
10 most recent association.

11 Implementers of station MAC entities are advised of the importance of continuing the sequential assignment of sequence
12 numbers for management frames throughout station operation, as required by 802.11-1999. A discontinuity in the
13 sequence numbering at the time of reassociation could cause roaming in an IAPP environment to be unreliable.

14 **4.8 IAPP-MOVE.request**

15 **4.8.1 Function**

16 This primitive is issued by the APME when it receives an MLME-REASSOCIATE.indication from the MLME indicating
17 that an STA has reassociated with the AP. It causes a frame to be sent to the DS that will update forwarding tables for the
18 newly reassociated station, and will notify the DS of the new reassociation between the AP and station. An attempt to
19 send an IAPP MOVE-notify packet to the AP with which the reassociating station was previously associated will also be
20 made.

21 **4.8.2 Semantics of the service primitive**

22 The IAPP-MOVE.request primitive has the following semantics.

```
23  
24   IAPP-MOVE.request {  
25       MAC Address,  
26       Sequence Number,  
27       Old AP,  
28       Context Block,  
29       Timeout  
30       }
```

31 The MAC Address is the address of the station that recently has successfully reassociated with the AP.

32 The Sequence Number is the value of the 802.11 Sequence Number field of the Reassociation Request frame received from
33 the reassociating station. The sequence number is provided to aid the APME in other APs in the determination of whether
34 the association represented by this IAPP-MOVE.request is the most recent association for the station identified by the
35 MAC Address. The 802.11 sequence number is not an unambiguous indication of the most recent association. But, this
36 information may be useful to an algorithm making this determination.

37 Old AP is the MAC address of the AP with which the reassociating station was last associated. This value is obtained by
38 the APME from the Current AP Address field of the 802.11 Reassociation Request frame.

39 The Context Block is the context to be sent to the Old AP. Otherwise, the Context Block is null. The Context Block is a
40 container for information defined by other 802.11 standards that is to be forwarded from one AP to another upon the
41 reassociation of a mobile station.

1 The Timeout parameter value is the number of seconds expected for both the IAPP MOVE-notify packet and the Layer 2
2 Update frame to be sent and the IAPP MOVE-response packet received. Failure to send both messages and receive a
3 response in this time results in the IAPP-MOVE.confirm primitive being generated with a status of TIMEOUT.

4 **4.8.3 When generated**

5 This service primitive is generated by an APME when the MLME generates an 802.11 MLME-REASSOCIATE.indication.

6 **4.8.4 Effect of receipt**

7 Receipt of this service primitive should cause the following actions to occur:

- 8 1) The IAPP entity determines the DSM layer 3 address of old BSSID presented in the reassociation request and the
9 security information needed to communicate with that AP using the methods described in clause 5.
- 10 2) The IAPP entity sends a Layer 2 Update frame to the DS, addressed such that it will cause the forwarding tables
11 in any bridges that receive the frame to be updated so that all future traffic received by those bridges is forwarded
12 to the port on which the frame was received,
- 13 3) The IAPP entity requests any context stored at the AP with which the station was previously associated to be
14 forwarded to the AP with which the station is currently associated by sending an IAPP MOVE-notify packet to
15 the old AP.

16 **4.9 IAPP-MOVE.confirm**

17 **4.9.1 Function**

18 This service primitive is used to confirm that the actions initiated by an IAPP-MOVE.request have been completed and
19 inform an APME of the status of those actions.

20 **4.9.2 Semantics of the service primitive**

21 The IAPP-MOVE.confirm primitive has the following semantics.

```
22  
23 IAPP-MOVE.confirm {  
24     MAC Address,  
25     Sequence Number,  
26     Old AP,  
27     Context Block,  
28     Status  
29 }
```

30 The MAC Address is the address of the station from the corresponding IAPP-MOVE.request.

31 The Sequence Number is the value of the 802.11 Sequence Number field of the Reassociation Request frame received from
32 the reassociating station.

33 Old AP is the MAC address of the AP with which the reassociating station was last associated. This value is obtained by
34 the APME from the Current AP Address field of the 802.11 Reassociation Request frame.

35 The Context Block is the context returned by the Old AP, if the Status is SUCCESSFUL. Otherwise, the Context Block is
36 null. The Context Block is a container for information defined by other 802.11 standards that is to be forwarded from one
37 AP to another upon the reassociation of a mobile station. If the Old AP does not return any context information, the
38 Context Block can be null, even when the status is SUCCESSFUL.

1 The Status parameter indicates the result of the corresponding IAPP-MOVE.request. The allowable values for this
 2 parameter are SUCCESSFUL, STALE_MOVE, and TIMEOUT. The TIMEOUT status indicates the corresponding IAPP-
 3 MOVE.request primitive was not able to complete the transmission of both the IAPP MOVE-notify packet and IAPP Layer
 4 2 Update frame, as well as receive the IAPP MOVE-response packet before the timeout parameter of the IAPP-
 5 MOVE.request primitive expired. The STALE_MOVE status indicates that the corresponding IAPP-MOVE.request did not
 6 complete successfully, because the IAPP MOVE-response packet returned by the Old AP contained a status value
 7 indicating a stale move.

8 **4.9.3 When generated**

9 This service primitive is generated upon receipt of context information from the Old AP in an IAPP MOVE-response packet
 10 as a result of the Old AP's use of the IAPP-MOVE.response primitive or expiration of the timeout specified in the
 11 corresponding IAPP-MOVE.request primitive.

12 **4.9.4 Effect of receipt**

13 Upon receipt of this service primitive by an APME with SUCCESSFUL status, the APME should cause the DS services to
 14 begin forwarding frames for the reassociated station. Completion of the IAPP-MOVE.request includes receipt of station
 15 context from the Old AP, when the Status is SUCCESSFUL. When the Status is not SUCCESSFUL, the APME should
 16 disassociate the station indicated by the MAC Address parameter, using the 802.11 MLME-DISASSOCIATE.request
 17 primitive.

18 **4.10 IAPP-MOVE.indication**

19 **4.10.1 Function**

20 This service primitive is used to indicate that a station has reassociated with another AP.

21 **4.10.2 Semantics of the service primitive**

22 The IAPP-MOVE.indication primitive has the following semantics.

```
23 IAPP-MOVE.indication {
24     MAC Address,
25     Sequence Number,
26     AP Address,
27     Context Block
28 }
29
```

30 The MAC Address is the address of the 802.11 station that has reassociated with the AP that sent the IAPP MOVE-notify
 31 packet.

32 The Sequence Number is the value of the 802.11 Sequence Number field of the Reassociation Request frame received from
 33 the reassociating station. The sequence number is provided to aid the APME in the determination of whether the
 34 association represented by this IAPP-ADD.request is the most recent association for the station identified by the MAC
 35 Address. The 802.11 sequence number is not an unambiguous indication of the most recent association. But, this
 36 information may be useful to an algorithm making this determination.

37 The AP Address is the DSM IP address of the AP sending the IAPP MOVE-notify packet.

38 The Context Block is the context sent by the AP indicated by the AP Address. Otherwise, the Context Block is null. The
 39 Context Block is a container for information defined by other 802.11 standards that is to be forwarded from one AP to
 40 another upon the reassociation of a mobile station.

1 **4.10.3 When generated**

2 This service primitive is generated when an IAPP MOVE-notify packet is received.

3 **4.10.4 Effect of receipt**

4 Upon receipt of this service primitive with a sequence number indicating a more recent association than that at the
5 receiving AP (if any), the AP should forward any relevant context related to the reassocated station to the AP with which
6 the station is now associated by using the IAPP-MOVE.response primitive and process any context received in the
7 Context Block received. "Relevant" context for a station is defined as those information elements that other 802.11
8 standards require to be forwarded when a station reassociates. If the received sequence number does not represent a more
9 recent association than that at the current AP, the AP should ignore the indicated reassocated station, the APME should issue
10 an IAPP-MOVE.response with a status of STALE_MOVE, and the APME should issue an IAPP-MOVE.request of its own
11 to ensure that all layer 2 devices are properly informed of the correct location of the station's most recent association.

12 **4.11 IAPP-MOVE.response**

13 **4.11.1 Function**

14 This service primitive is used to send any relevant context resident in the AP issuing this primitive to another AP when a
15 station has reassocated with that other AP. "Relevant" context for a station is defined as those information elements that
16 other 802.11 standards require to be forwarded when a station reassociates.

17 **4.11.2 Semantics of the service primitive**

18 The IAPP-MOVE.response primitive has the following semantics.

```
19  
20 IAPP-MOVE.response {  
21     MAC Address,  
22     Sequence Number,  
23     AP Address,  
24     Context Block,  
25     Status  
26 }
```

27 The MAC Address is the address of the 802.11 station that has reassocated with the AP identified by the AP Address.

28 The Sequence Number is the value of the 802.11 Sequence Number field of the Reassociation Request frame received from
29 the reassocating station.

30 The AP Address is the MAC address of the AP where the 802.11 station has reassocated.

31 The Context Block is the context for the reassocated station. The Context Block may be null.

32 The Status parameter indicates the result of the corresponding IAPP-MOVE.indication. The allowable values for this
33 parameter are SUCCESSFUL and STALE_MOVE. STALE_MOVE should be used to indicate that the AP receiving the
34 IAPP-MOVE.indication has a current association with the station indicated by the MAC Address parameter with a more
35 recent sequence number than that in the IAPP-MOVE.indication.

36 **4.11.3 When generated**

37 This service primitive should be generated by the APME when an IAPP-MOVE.indication is received.

1 4.11.4 Effect of receipt

2 Upon receipt of this service primitive, the AP forwards all relevant context related to the reassociated station and the
3 Status to the peer IAPP entity in the AP with which the station is now associated by sending the IAPP MOVE-response
4 packet. Any context for the station identified by the MAC Address parameter may be discarded upon receipt of this
5 response.

6 5 Operation of the IAPP

7 The IAPP is a communication protocol, used by the management entity of an AP to communicate with other APs, when
8 various local events occur in the AP. It is a part of a communication system comprising APs, mobile stations, an arbitrarily
9 connected DS, and RADIUS infrastructure containing one or more RADIUS servers. The RADIUS servers provide two
10 functions, mapping the BSSID of an AP to its IP address on the DSM and distribution of keys to the APs to allow the
11 encryption of the communications between the APs. The function of the IAPP is to facilitate the creation and maintenance
12 of the ESS, support the mobility of 802.11 stations, and enable APs to enforce the requirement of a single association for
13 each mobile station at a given time, as stated in ISO/IEC 8802-11:1999. IAPP also removes the need for reauthentication
14 with 802.1X when moving between access points, enabling seamless connectivity, and reducing the load on the backend
15 authentication server.

16 5.1 IAPP Protocol Overview

17 IAPP supports two protocol sequences. One is initiated by an associate request to an Access Point, and the other is
18 initiated by a reassociate request.

19 5.1.1 Actions triggered by an associate request

20 When an AP receives an associate request it should send an IAPP-ADD Packet and a Level 2 Update Frame. The IAPP-
21 ADD is an IP packet with destination-IP-address of the subnet broadcast address, the source IP and MAC address of the
22 AP. The message body contains the MAC address of the STA. On receiving this message the AP should check its
23 association table and remove an association with the STA if it exists. Note that purpose of the IAPP-ADD message is to
24 remove stale associations, not to modify the learning table. The learning table update is done by Layer 2 Update frame
25 (see sec.6.3). This frame has the source MAC address of the associating STA. This frame is used by receiving APs to
26 update their learning table.

27 5.1.2 Actions triggered by a reassociate request

28 When an AP receives an associate request it should send an Move-Notify to the old-AP and get back a Move-Response
29 from the old-AP. The Move-Response carries the Context block for the STA association to the old-STA, allowing the new-
30 STA to replicate the prior connection context without reauthenticating. This is commonly called a fast-handoff.

31 The Move-Notify and Move-Response are IP packets carried in a TCP session between APs. The IP address of the old-
32 AP must be found by mapping the BSSID from the reassociate message to its IP address. This mapping is done using a
33 RADIUS exchange. For this exchange any standard RADIUS server should work.

34 If it is desired to encrypt the Move-Response packet, then the RADIUS Reply to the new AP will include, in addition to the
35 IP address of the old-AP, reply items with Security Block for both the new and old AP. The security Blocks each contain a
36 shared secret for AP-AP connection, and are encrypted using the AP's password in the RADIUS registry. The RADIUS
37 server would have to have an add-on to create the Security Block.

38 The new-AP sends the security block for the old-AP, which it received from the RADIUS Server, as a Send-Security-Block
39 packet. This is the first message in the IAPP TCP exchange between the APs. The old-AP returns ACK-Security-Block
40 packet. At this point both APs have the shared secret and it is used to encrypt all further packets for this exchange
41 between the APs are encrypted. Figure 3 is an overview of the protocol triggered by the reassociate request.

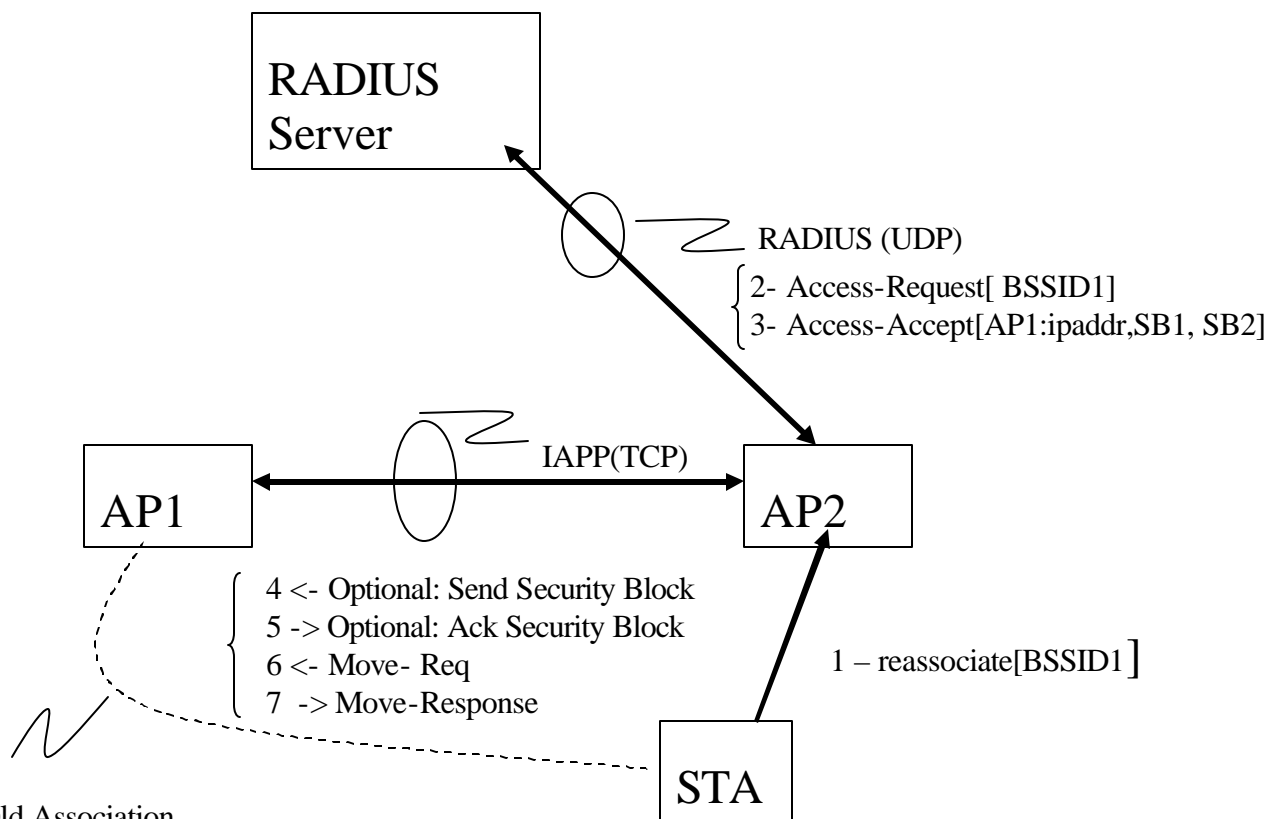


Figure 3 - IAPP Message Exchange During STA Reassociation

5.2 Formation and maintenance of the ESS, the Registration Service

An ESS is a set of Basic Service Sets (BSSs) that form a single LAN, allowing an 802.11 mobile station to move transparently from one BSS to another throughout the ESS. As described in ISO/IEC 8802-11:1999 the initialization of the first AP via the MLME-START.request(BSSType=Infrastructure) establishes the formation of an ESS. Subsequent APs that are interconnected by a common DS and that are started with the same SSID extend the ESS created by the first. IAPP is defined to provide a secure handoff mechanism of mobile STA information between APs in the same ESS. IAPP uses a central RADIUS registry to define AP members of an ESS.

The RADIUS server and the AP RADIUS client must be configured with the shared secret and with each other's IP address. This must be done prior to the first AP in an ESS becoming operational. Each AP acting as a RADIUS client should have its own shared secret with the RADIUS server, different from that of any other AP.

Since the roaming STA sends an 802.11 reassociate frame to the new AP containing the BSSID it is roaming from, each RADIUS server must also be configured with the following information for each BSSID. From an IAPP point of view, this set of BSSID entries defines the members of an ESS.

- a) BSSID,
- b) RADIUS BSSID Secret at least 128 bits in length
- c) IP address or DNS name, and
- d) Cipher suites supported by the AP for the protection of IAPP communications.

1 If an APME is going to use the services of IAPP, additional steps, internal to the AP, are necessary. Before the issuance
 2 of the MLME-START.request(BSSType=Infrastructure) and the receipt of an MLME-
 3 START.confirm(ResultCode=SUCCESS), the APME should issue the IAPP-INITIATE.request.

4 The IAPP entity is invoked by the APME to initiate STA context transfer from the old AP. The IAPP may invoke RADIUS
 5 to obtain mapping of the old BSSID to the DSM IP address of the old AP and the security information with which to secure
 6 the communications with the peer IAPP entity.

7 **5.3 RADIUS Protocol Usage**

8 For the IAPP entity to function correctly, it must have the ability to discover the DSM IP address of the old BSSID in the
 9 ESS using the old BSSID as a lookup key. To implement this capability, the use of the RADIUS Protocol (IETF RFC 2138
 10 and 2869) is recommended. RADIUS is also used to obtain the security information to secure the communication between
 11 IAPP entities. This address mapping and security information may be preloaded or cached.

12 **5.3.1 RADIUS Access-Request**

13 Upon receipt of an IAPP-MOVE.Request primitive, the receiving AP must establish

- 14 a. that the Old BSSID is a valid member of the New BSSID's ESS, and
- 15 b. optionally, a secure channel for communications with the Old BSSID

16 To verify the Old BSSID's identity, and also to obtain the security parameters necessary for establishing a secure
 17 connection with the Old BSSID, the New AP sends a RADIUS Access-Request packet to the RADIUS server. The
 18 RADIUS Access-Request packet contains the following attributes:

19
 20 **Table 1 - RADIUS Access-Request Attributes**

1	User-Name	Old BSSID
2	User-Password	NULL
4	NAS-IP-Address (optional)	New AP's IP Address
6	Service-Type	Call Check (10)
26	Vendor-Specific	The following IEEE 802.11 vendor-specific attributes:
26-802-1 ³	IAPP-Liveliness-Nonce (optional)	A 32-byte nonce used to ensure liveliness of the secure IAPP traffic. This attribute should not be included if secure IAPP communication are not required by the AP.
30	Called-Station-Id	The WM MAC Address of the new BSSID with which the STA is reassociating, in ASCII format, with octet values separated by a "-". Example: "00-10-A4-23-19-C0". The SSID SHOULD be appended to the WM MAC address, separated from the MAC address with a ":". Example "00-10-A4-23-19-C0:AP1".
32	NAS-Identifier (optional)	New BSSID's NAS Identifier
61	NAS-Port-Type	new value assigned for IAPP ³
80	Message-Authenticator	The RADIUS message's authenticator

21 Per RFC 2865, other RADIUS attributes may be included in the Access-Request packet in addition to the ones listed above.

³ Editor's Note: This value will be applied for and inserted when received.

5.3.2 RADIUS Access-Accept

Upon receipt of an Access-Request from the New BSSID, the RADIUS Server will verify that the Old BSSID is a valid member of the ESS of which the New BSSID is a member. If the RADIUS Server determines that the Old AP and New AP should be able to communicate with each other via IAPP, the RADIUS Server will respond to the New AP's Access-Request packet with an Access-Accept packet. The RADIUS Access-Accept packet both confirms that the Old BSSID is a valid member of the ESS, and also provides both the Old and New AP with the appropriate security information for establishing a secure communications channel.

When the RADIUS server responds with Access-Accept, the Access-Accept packet should contain the following attributes:

Table 2 - RADIUS Access-Accept Attributes

1	User-Name	Old BSSID
8	Framed-IP-Address	Old BSSID's IP Address
26	Vendor-Specific	The following IEEE 802.11 vendor-specific attributes:
26-802-2 ³	New -BSSID-Security-Block (optional)	Security Block encrypted using new BSSID's user-password, to be decrypted and used by the new BSSID
26-802-3 ³	Old-BSSID-Security-Block (optional)	Security Block encrypted using old BSSID's user-password, to be sent via IAPP from the new BSSID to the old BSSID, and decrypted and used by the old BSSID
80	Message-Authenticator	The RADIUS message's authenticator

Per RFC 2865, other RADIUS attributes may be included in the Access-Accept packet in addition to the ones listed above.

The data field of new AP security block carries the security information needed by the new AP to decrypt and encrypt ESP packets. The format of the data field for this packet is shown in 7.

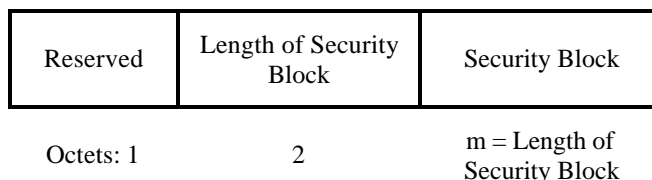


Figure 4 - Send-Security-Block Data Field Format

The Reserved field is reserved in this version of the protocol and should be sent with a value of zero. The Reserved field should be ignored on reception. The Length of Security Block is a 16-bit integer that indicates the number of octets in the Security Block field. The Security Block is a variable length field that contains the security information from the RADIUS Server for the new AP. The content of the Security Block should be interpreted by the IAPP.

The Security Block is a series of information elements. This block is encrypted with the new AP's RADIUS BSSID Secret, using the AP's configured cipher. The old AP has to decrypt it first before processing it. The format of the Information Element is shown in Figure 9. Information elements are defined to have a common general format consisting of a 2 octet Element ID field, a 2 octet length field, and a variable-length element-specific information field. Each element is assigned a unique Element ID as defined below. The Length field specifies the number of octets in the Information field.

ID	Length	Information
----	--------	-------------

8	Date/Time stamp
8	Security lifetime in seconds
32	ACK nonce
1	ESP transform number
1	ESP authentication number
4	SPI used to identify ESP SA to the old AP
Variable	key used by ESP Transform for ESP packets to the old AP
Variable	key used by ESP Authentication for ESP packets to the old AP
4	SPI used to identify ESP SA from the old AP
Variable	key used by ESP Transform for ESP packets from the old AP
Variable	key used by ESP Authentication for ESP packets from the old AP

Table 3 - Information Elements in the Send-Security-Block Packet

5.3.3 RADIUS Access-Reject

As described in 5.2.2, upon receipt of an Access-Request from the New AP, the RADIUS Server will verify that the Old BSSID is a valid member of the ESS. If the RADIUS Server determines that the Old BSSID and New AP should NOT be able to communicate with each other via IAPP, the RADIUS Server will respond to the AP's Access-Request packet with a RADIUS Access-Reject. The RADIUS Access-Reject packet instructs the New AP to issue an MLME-REASSOCIATE.confirm(ResultCode= REFUSED) for the STA that caused the original MLME.REASSOCIATE.request primitive.

IAPP has no special requirements for RADIUS Access-Reject packets.

5.4 Support for 802.11 authentication

There are no requirements from the existing authentication mechanisms of IEEE 802.11-1999 for the IAPP to carry authentication information between APs. However, should other authentication mechanisms be defined that establish a requirement for the IAPP to carry authentication information between APs, that information will be carried in the Context Block of an IAPP MOVE-notify and MOVE-response packets. The cryptographic protection of the information in the Context Block, should such protection be required, will be the responsibility of the standard defining the format of the information element carrying the authentication information. IAPP can be used to move AAA context between access points, as described in Annex B. This enables the transfer of 802.1X context, enabling roaming without re-authentication.

5.5 AP to AP Interactions

5.5.1 Station Move Process

The interaction between APs in an ESS when a STA is added to the STAs associated with an AP as a result of an 802.11 reassociation request frame minimally comprises the exchange of the IAPP MOVE-notify and IAPP MOVE-response messages by the new AP at which the reassociation occurs and the old AP that formerly held the association of the STA, as well as the transmission of a Layer 2 Update frame by the new AP. If security is needed for the IAPP MOVE-notify and IAPP MOVE-response packets, they are wrapped in ESP.

The purpose of exchanging the IAPP MOVE-notify and MOVE-response packets is to allow the new AP and old AP to exchange STA context information. An example of this STA context information is STA security information that may allow faster reauthentication of a STA on reassociation. The purpose of transmitting the Layer 2 Update frame is to cause any layer 2 devices, such as bridges and switches, to update any forwarding information they may hold regarding the STA identified by the MAC address in the SA field of the frame, so that frames destined for the STA are delivered to a point in the DS where the new AP can forward these frames into the BSS containing the STA.

The SPIs and keys for the Security Associations (SAs) for ESP are created by the RADIUS Server and sent to the new AP as the New-BSSID-Security-Block and Old-BSSID-Security-Block RADIUS Attributes. The new AP decrypts the New-

1 BSSID-Security-Block using the configured cipher and its RADIUS BSSID Secret. The new AP creates the SAs from the
2 information in the Security Block and if it caches these SAs, uses the lifetime to remove the SAs from its cache.

3 The new AP sends the old-BSSID-Security-Block to the old AP in the IAPP Send-Security-Block packet. The old AP
4 authenticates and decrypts this Security Block using the configured cipher, HMAC-MD5, and its RADIUS BSSID Secret.
5 The cipher and HMAC keys are derived from the RADIUS BSSID Secret by first expanding the password by:
6 SHA1(password)||SHA1(password||1st SHA1)||... The cipher password is the first N bits and the authentication secret is
7 the next M bits. The new AP creates the SAs from the information in the Security Block and if it caches these SAs, uses
8 the lifetime to remove the SAs from its cache. If the old AP already has SAs with the IP address of the new AP, it checks
9 the date/time stamp received against the date/time stamp used to create the old SAs. If the stamp just received is greater, it
10 removes the old SAs, and uses the new. If the stamps are the same, all the rest of the Security Block content is the same
11 and can be dropped. If the stamp just received is less, this is a reply and MUST be ignored.

12 The old AP takes the New-AP-ACK-Authenticator and sends it to the new AP in the IAPP ACK-Security-Block packet.
13 The new AP authenticates and decrypts the New-AP-ACK-Authenticator using the configured cipher, HMAC-MD5, and
14 its RADIUS BSSID Secret. The same password expansion routine is used here. It compares the nonce in this block with
15 the nonce it received in the New-BSSID-Security-Block. If they are the same, the old AP is ready to receive the IAPP
16 MOVE-notify protected with ESP. If they do not match, there was some attack or failure. The new AP CAN wait to see if
17 another IAPP ACK-Security-Block packet arrives with the proper nonce or the new AP can resend the IAPP Send-Security-
18 Block packet.

19 **5.5.2 Station Add Process**

20 The interaction between APs in an ESS when a STA is added to the STAs associated with an AP as a result of an 802.11
21 association request frame comprises the transmission by the AP at which the association occurs of an IAPP ADD-notify
22 packet and the transmission of a Layer 2 Update frame. The IAPP ADD-notify packet is sent to the subnet limited
23 broadcast address. The Layer 2 Update frame is sent to the MAC broadcast address and uses the MAC address of the
24 STA that has associated as the MAC source address for the frame. See clause 6.2 for further information on the IAPP
25 ADD-notify packet and clause 6.3 for further information on the Layer 2 Update frame.

26 The purpose of transmitting the IAPP ADD-notify packet is to provide an indication to an AP that may have held an older
27 association of a STA that has more recently associated with another AP that the AP holding that older association may
28 discard any context for that STA. This should allow for more efficient management of AP resources. The purpose of
29 transmitting the Layer 2 Update frame is to cause any layer 2 devices, such as bridges and switches, to update any
30 forwarding information they may hold regarding the STA identified by the MAC address in the SA field of the frame, so
31 that frames destined for the STA are delivered to a point in the DS where the new AP can forward these frames into the
32 BSS containing the STA.

33 There is no security provided for the IAPP ADD-notify packet or the Layer 2 Update frame. Neither the IAPP ADD-notify
34 packet nor the Layer 2 Update frame open new potentials for attacks against the WLAN or the mobile STAs that did not
35 exist without the presence of these transmissions.

36 **5.6 AP specific MIB**

37 An SNMP MIB using SMIV2 for the IAPP is defined in Annex A. The MIB contains attributes for the IAPP that are useful
38 in monitoring and diagnosis of the operation of the IAPP.

39 **5.7 Single station association**

40 IEEE 802.11 specifies that each Station may only be associated with a single AP at any given time. (See 802.11-1999
41 subclauses 5.4.2.2 and C.2) When a station changes its association from one AP to another, the station issues a
42 reassociate frame (as specified in the 802.11 standard). Reception of the reassociate frame and granting of the association
43 by the new AP causes the APME in that AP to issue an IAPP-MOVE.request service primitive. This causes an IAPP
44 MOVE-notify packet to be sent to the Old AP, requesting the old AP to remove the station from its table, to forward any
45 stored context for the station, and the new AP to add the station and context to its own table. Thus, the use of the

1 reassociation request frame by the mobile station allows the APs to ensure that there is only a single association for the
2 station.

3 When a roaming station associates with an AP, rather than reassociates, or when the AP holding the roaming station's
4 previous association cannot be found using RADIUS, the AP attempts to enforce the single station association
5 requirement by sending an IAPP ADD-notify packet and the Layer 2 Update frame to the DS. Because this packet is
6 addressed to the subnet-local broadcast address (see 6.2), this packet may not reach all APs in an ESS. In particular, if the
7 ESS spans multiple subnets, neither the ADD-notify packet nor the Layer 2 Update frame is likely to reach the APs on
8 subnets other than the one on which the transmissions originate. If the old AP receives the IAPP ADD-notify packet, it
9 should remove any context stored for the station.

10 6 Packet Formats

11 6.1 General IAPP Packet Format

12 The general format of an IAPP packet is shown in Figure 5. An IAPP packet is carried in the TCP or UDP protocols over IP.
13 The port number assigned to IAPP is TBD.

14

IAPP Version	Command	Identifier	Length	Data
Octets: 1	1	2	2	0-n

15

Figure 5 - General IAPP Packet Format

16 6.1.1 IAPP Version Field

17 The IAPP Version Field indicates the protocol version of the IAPP, and thus the organization of the rest of the packet. The
18 value of the Version field for this protocol is zero. All other values are reserved. A device that receives a packet with a
19 higher revision level than it supports will silently discard the packet.

20

21 6.1.2 Command Field

22 This is an 8-bit integer value that identifies the specific function of the packet. The data field that is specific to that
23 command follows each command field.

24

25

Table 4 - Command field values

26

Value	Command
0	ADD-notify
1	MOVE-notify
2	MOVE-response
3	Send-Security-Block
4	ACK-Security-Block
5-255	Reserved

27

1 6.1.3 Identifier Field

2 The two-octet Identifier aids in matching requests and responses. Any IAPP packet that is sent in response to the receipt
3 of another IAPP packet will copy the value of the Identifier field from the received packet into the Identifier field of the
4 packet sent in response. A duplicate request can be detected if it has the same source IP address and port and Identifier
5 within a short span of time. Duplicate requests should be silently discarded.

6 6.1.4 Length Field

7 The two-octet Length field indicates the length of the entire packet, including the version, command, identifier, length and
8 data fields. Octets outside the range of the Length field MUST be treated as padding and ignored on reception. If the
9 packet is shorter than the Length field indicates, it MUST be silently discarded.

10 6.1.5 Data Field

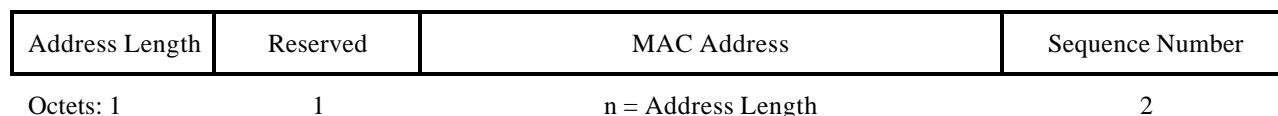
11 The Data Field is a variable length field, the content of which is dependent on the value of the Command field. The content
12 of the Data Field is described in 6.2, 6.4, and 6.5 for each of the packet types.

13 6.2 ADD-notify Packet

14 The ADD-notify packet is sent, using the IAPP over UDP and IP, on the local LAN segment to notify any AP that receives
15 it that the mobile station identified in the packet has associated at the AP sending the packet. The packet is sent to the
16 subnet limited broadcast address (see RFC 1812), so that it will reach every device on the DSM local subnet, even if the
17 LAN is switched.

18 The ADD-notify packet carries the MAC address and sequence number from the mobile station that has associated with
19 the AP. The format of the packet data field is shown in Figure 6.

20



21

Figure 6 - ADD-notify Data Field Format

22 The Address Length is an 8-bit integer that indicates the number of octets in the MAC Address. The Reserved field is
23 reserved in this version of the protocol and should be sent with a value of zero. The Reserved field should be ignored on
24 reception. The length of the Reserved field is one octet, in order to align the MAC Address field on a 16-bit boundary.
25 The MAC Address is the MAC address of the station that has associated. The length of the MAC Address field is equal
26 to the value of the Address Length field. The Sequence Number field contains the integer value of the sequence number
27 of the association request frame received by the AP from the station that has associated. Allowable values for the
28 Sequence number are between 0 and 4095.

29 6.3 Layer 2 Update Frame

30 The Layer 2 Update frame is an 802.2 Type 1 Logical Link Control (LLC) Exchange Identifier (XID) Update response frame.
31 This frame is sent using a MAC source address equal to the MAC address of the mobile station that has associated, so
32 that any layer 2 devices, e.g., bridges, switches and other APs, can update their forwarding tables with the correct port to
33 reach the new location of the mobile station. The format of an XID Update frame carried over 802.3 is shown in Figure 7.
34 The 802.3 MAC header is shown as an example only. Other MAC protocols than 802.3 may be used.

35

MAC DA	MAC SA	Length	DSAP	SSAP	Control	XID Information Field
Octets: 6	6	2	1	1	1	3

Figure 7 - Layer 2 Update Frame Format

The MAC DA is the broadcast MAC address. The MAC SA is the MAC address of the mobile station that has just associated or reassociated. The Length field is the length of the information following this field, eight octets. The value of both the DSAP and SSAP is null. The Control field and XID Information field are defined in IEEE Standard 802.2.

6.4 MOVE-notify Packet

The MOVE-notify packet is sent using the IAPP, over TCP and IP. This packet is sent from the AP directly to the old AP with which the reassociating mobile station was previously associated. TCP is used, rather than UDP, because of its defined retransmission behavior and the need for the exchange to be reliable.

The data field of the MOVE-notify packet carries the MAC address and sequence number from the mobile station that has reassociated with the AP sending the packet. The format of the data field for this packet is shown in Figure 8.

Address Length	Reserved	MAC Address	Sequence Number	Length of Context Block	Context Block
Octets: 1	1	n = Address Length	2	2	m = Length of Context Block

Figure 8 - MOVE-notify Data Field Format

The Address Length is an 8-bit integer that indicates the number of octets in the MAC Address. The Reserved field is reserved in this version of the protocol and should be sent with a value of zero. The Reserved field should be ignored on reception. The MAC Address is the MAC address of the station that has reassociated. The Sequence Number field contains the integer value of the sequence number of the reassociation request frame received by the AP from the station that has associated. Allowable values for the Sequence number are between 0 and 4095. The Length of Context Block is a 16-bit integer that indicates the number of octets in the Context Block field. The Context Block is a variable length field that contains the context information being forwarded for the reassociated station indicated by the MAC Address. The content of the Context Block should not be interpreted by the IAPP.

The Context Block is a container for information defined in other 802.11 standards that needs to be forwarded from one AP to another upon reassociation of a mobile station. The Context Block is a series of information elements. The format of the Information Element is shown in Figure 9. The element identifiers and format of the information element content are defined by the standards that use the IAPP to transfer context from one AP to another. Information elements are defined to have a common general format consisting of a 2 octet Element ID field, a 2 octet length field, and a variable-length element-specific information field. Each element is assigned a unique Element ID as defined in the standards that use the IAPP to transfer context between APs. The Length field specifies the number of octets in the Information field.

Users of the IAPP service should ignore information elements, the element identifier of which they do not understand, rather than discarding the entire IAPP MOVE-notify packet.

Element Identifier	Length	Information
Octets: 2	2	n = Length

1 **Figure 9 - Information Element Format**

2 **6.5 MOVE-response Packet**

3 The MOVE-response packet is sent using the IAPP, over TCP and IP. This packet is sent directly to the AP from which the
4 MOVE-notify packet was received. TCP is used, rather than UDP, because of its defined retransmission behavior and the
5 need for the exchange to be reliable.

6 The data field of the MOVE-response packet carries the MAC address of the reassociated station and the context
7 information pertaining to that station. The format of the data field for this packet is shown in Figure 10.

Address Length	Status	MAC Address	Sequence Number	Length of Context Block	Context Block
Octets: 1	1	n = Address Length	2	2	m = Length of Context Block

8
9 **Figure 10 - MOVE-response Data Field Format**

10 The Address Length is an 8-bit integer that indicates the number of octets in the MAC Address. The Status field is an 8-
11 bit integer that indicates the status resulting from the receipt of the MOVE-notify packet. The allowable values for the
12 Status field are shown in Table 5. The MAC Address is the MAC address of the station that has reassociated. The
13 Sequence Number field contains the integer value of the sequence number from the MOVE-notify packet that caused the
14 generation of this packet. The Length of Context Block is a 16-bit integer that indicates the number of octets in the Context
15 Block field. The Context Block is a variable length field that contains the context information being forwarded for the
16 reassociated station indicated by the MAC Address. The content of the Context Block should not be interpreted by the
17 IAPP.

Status Value	Definition
0	Successful
1	Stale move
2-255	Reserved

18
19 **Table 5 - MOVE-notify Status Values**

20 **6.6 Send-Security-Block packet**

21 The Send-Security-Block packet is sent using the IAPP, over TCP and IP. This packet is sent from the AP directly to the
22 old AP with which the reassociating mobile station was previously associated. TCP is used, rather than UDP, because of
23 its defined retransmission behavior and the need for the exchange to be reliable.

24 The data field of the Send-Security-Block packet carries the security information needed by the old AP to decrypt and
25 encrypt ESP packets. The format of the data field for this packet is shown in Figure 11.

Reserved	Length of Security Block	Security Block	Authentication Block
Octets: 1	2	m = Length of Security Block	16

Figure 11 - Send-Security-Block Data Field Format

The Reserved field is reserved in this version of the protocol and should be sent with a value of zero. The Reserved field should be ignored on reception. The Length of Security Block is a 16-bit integer that indicates the number of octets in the Security Block field. The Security Block is a variable length field that contains the security information being forwarded from the RADIUS Server through the AP to the old AP. The Authentication Block is a 16 byte field that contains the result of an HMAC-MD5 hash of the Security Block. The content of the Security Block should be interpreted by the IAPP.

The Security Block is a series of information elements. This block is encrypted with the old AP’s RADIUS BSSID Secret, using the AP’s configured cipher. The old AP has to authenticate and decrypt it first before processing it. The format of the Information Element is shown in Figure 9. Information elements are defined to have a common general format consisting of a 2 octet Element ID field, a 2 octet length field, and a variable-length element-specific information field. Each element is assigned a unique Element ID as defined below. The Length field specifies the number of octets in the Information field.

ID	Length	Information
	6 or 8	Old BSSID
	8	Date/Time stamp
	8	Security lifetime in seconds
	48	ACK nonce
	1	ESP transform number
	1	ESP authentication number
	4	SPI used to identify ESP SA from new AP
	Variable	key used by ESP Transform for ESP packets from the new AP
	Variable	key used by ESP Authentication for ESP packets from the new AP
	4	SPI used to identify ESP SA to the new AP
	Variable	key used by ESP Transform for ESP packets to the new AP
	Variable	key used by ESP Authentication for ESP packets to the new AP

Table 6 - Information Elements in the Send-Security-Block Packet

The ESP Transform and Authentication algorithms are defined by IANA at <http://www.iana.org/assignments/isakmp-registry>. The values as of the last update of 2001 September 6 are:

Transform Identifier	Value	Reference
RESERVED	0	[RFC2407]
ESP_DES_IV64	1	[RFC2407]
ESP_DES	2	[RFC2407]
ESP_3DES	3	[RFC2407]
ESP_RC5	4	[RFC2407]
ESP_IDEA	5	[RFC2407]
ESP_CAST	6	[RFC2407]
ESP_BLOWFISH	7	[RFC2407]
ESP_3IDEA	8	[RFC2407]
ESP_DES_IV32	9	[RFC2407]
ESP_RC4	10	[RFC2407]
ESP_NULL	11	[RFC2407]
ESP_AES	12	[Leech]

Table 7 - ESP Transform Identifiers

The values 249-255 are reserved for private use amongst cooperating systems.

Transform Identifier	Value	Reference
RESERVED	0	[RFC2407]
HMAC-MD5	1	[RFC2407]
HMAC-SHA	2	[RFC2407]
DES-MAC	3	[RFC2407]
KPDK	4	[RFC2407]
HMAC-SHA2-256	5	[Leech]
HMAC-SHA2-384	6	[Leech]
HMAC-SHA2-512	7	[Leech]
HMAC-RIPEMD	8	[RFC2857]

Table 8 - ESP Authentication Algorithm Identifiers

Values 5-61439 are reserved to IANA. Values 61440-65535 are for private use.

6.7 ACK-Security-Block packet

ACK-Security-Block packet is sent using the IAPP, over TCP and IP. This packet is sent from the old AP with which the reassociating mobile station was previously associated directly to the new AP. TCP is used, rather than UDP, because of its defined retransmission behavior and the need for the exchange to be reliable.

The data field of the ACK-Security-Block packet carries the New AP ack authentication Information element that the old AP received in the Security Block. The format of the data field for this packet is shown in Figure 12.

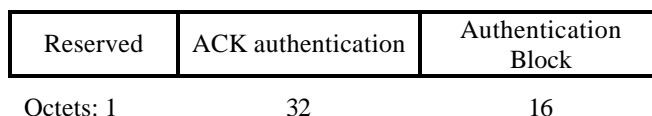


Figure 12 - Send-Security-Block Data Field Format

The Reserved field is reserved in this version of the protocol and should be sent with a value of zero. The Reserved field should be ignored on reception. The ACK authentication is a 32 byte field that contains an encrypted nonce that the new

- 1 AP received from the RADIUS Server. The Authentication Block is a 16 byte field that contains the result of an HMAC-
- 2 MD5 hash of the ACK authentication. The content of the ACK authentication should be interpreted by the IAPP. The
- 3 ACK authentication is encrypted with the new AP's RADIUS BSSID Secret, using the AP's configured cipher. The new
- 4 AP has to authenticate and decrypt it first before processing it.

- 5 There is only one element. This is the 256 bit nonce the new AP sent to the RADIUS Server in the RADIUS-Access-
- 6 Request message. This nonce protects the new AP from spoofed ACK-Security-Block packets.

1
2 **Annex A, Management Information Base**

3 **(Normative)**

```

4
5
6 -- *****
7 -- * IEEE 802.11f Inter-AP Protocol Management Information Base
8 -- *****
9
10 IEEE802dot11f-MIB DEFINITIONS ::= BEGIN
11     IMPORTS
12         MODULE-IDENTITY, OBJECT-TYPE,
13         NOTIFICATION-TYPE, Integer32, Counter32 FROM SNMPv2-SMI
14
15         DisplayString , MacAddress, RowStatus,
16         TruthValue                                     FROM SNMPv2-TC
17
18         MODULE-COMPLIANCE, OBJECT-GROUP,
19         NOTIFICATION-GROUP                             FROM SNMPv2-CONF
20
21         ifIndex                                       FROM RFC1213-MIB;
22
23 -- *****
24 -- * MODULE IDENTITY
25 -- *****
26
27     ieee802dot11f MODULE-IDENTITY
28         LAST-UPDATED "0107020000Z"
29         ORGANIZATION "IEEE 802.11"
30         CONTACT-INFO
31             "WG E-mail: stds-802-11@ieee.org
32
33             Chair: Stuart J. Kerry
34             Postal: Philips Semiconductors, Inc.
35                 1109 McKay Drive
36                 M/S 48 SJ
37                 San Jose, CA 95130-1706 USA
38             Tel: +1 408 474 7356
39             Fax: +1 408 474 7247
40             E-mail: stuart.kerry@philips.com
41
42             Editor: Bob O'Hara
43             Postal: Informed Technology, Inc.
44                 1750 Nantucket Circle, Suite 138
45                 Santa Clara, CA 95054 USA
46             Tel: +1 408 986 9596
47             Fax: +1 408 727 2654
48             E-mail: bob@informed-technology.com"
49
50     DESCRIPTION
51         "The MIB module for IEEE 802.11f IAPP entities.
52         iso(1).member-body(2).us(840).ieee802dot11(10036).iapp(6)"
53         ::= { 1 2 840 10036 6 }
54
55 -- *****

```

```

1  -- * Major sections
2  -- *****
3  -- IAPP diagnostic attributes
4  --   DEFINED AS "The iappdiagnostics object class provides the necessary
5  --   support at an 802.11 AP to manage and diagnose the IAPP processes
6  --   and protocol in the AP such that the AP may work cooperatively as
7  --   a part of an IEEE 802.11 network.";
8
9  iappdiagnostics OBJECT IDENTIFIER ::= {ieee802dot11f 1}
10
11 iappAPTable OBJECT-TYPE
12     SYNTAX      SEQUENCE OF iappAPTableEntry
13     MAX-ACCESS not-accessible
14     STATUS      current
15     DESCRIPTION
16         "The (conceptual) table listing the other APs with
17         which the AP has communicated via IAPP."
18     ::= { iappdiagnostics 1 }
19
20 iappAPTableEntry OBJECT-TYPE
21     SYNTAX      iappDiagnosticTableEntry
22     MAX-ACCESS not-accessible
23     STATUS      current
24     DESCRIPTION
25         "An entry (conceptual row) representing another AP
26         with which the AP has communicated via IAPP."
27     INDEX       { iappDiagnosticTableIndex }
28     ::= { iappDiagnosticTable 1 }
29
30 iappAPTableEntry ::= SEQUENCE {
31     iappAPTableIndex          Integer32,
32     iappAPIPAddress           IpAddress,
33     iappAPMACAddress          MacAddress,
34     iappClientServerPortNumber Integer32,
35     iappAPRoundTripTime       TimeTicks,
36     iappAPRTO                 TimeTicks,
37     iappMoveNotifySent        Counter32,
38     iappMoveNotifyRetransmissions Counter32,
39     iappMoveNotifyReceived     Counter32,
40     iappMoveResponseSent      Counter32,
41     iappMoveResponseReceived   Counter32,
42     iappMoveNotifyMalformed    Counter32,
43     iappMoveNotifyUnAuthentic  Counter32,
44     iappMoveResponseMalformed  Counter32,
45     iappMoveResponseUnAuthentic Counter32,
46     iappMoveNotifyBadService   Counter32,
47     iappMoveResponseBadService Counter32,
48     iappMoveNotifyPendingRequests Gauge32,
49     iappMoveResponsePendingResponses Gauge32,
50     iappMoveNotifyTimeouts     Counter32,
51     iappUnknownType           Counter32,
52     iappMoveNotifyPacketsDropped Counter32,
53     iappMoveResponsePacketsDropped Counter32
54 }
55
56 iappAPTableIndex OBJECT-TYPE
57     SYNTAX      Integer32 (1..2147483647)

```

Inter-Access Point Protocol

```

1      MAX-ACCESS not-accessible
2      STATUS      current
3      DESCRIPTION
4          "A number uniquely identifying each other AP
5          with which this AP has communicated via IAPP."
6      ::= { iappAPTableEntry 1 }
7
8  iappAPIPAddress OBJECT-TYPE
9      SYNTAX      IPAddress
10     MAX-ACCESS read-only
11     STATUS      current
12     DESCRIPTION
13         "The IP address of the AP
14         referred to in this table entry."
15     ::= { iappAPTableEntry 2 }
16
17  iappAPMACAddress OBJECT-TYPE
18     SYNTAX      MacAddress
19     MAX-ACCESS read-only
20     STATUS      current
21     DESCRIPTION
22         "The MAC address of the AP
23         referred to in this table entry."
24     ::= { iappAPTableEntry 3 }
25
26
27  iappClientServerPortNumber OBJECT-TYPE
28     SYNTAX      Integer32 (0..65535)
29     MAX-ACCESS read-only
30     STATUS      current
31     DESCRIPTION
32         "The UDP port the AP is using to send
33         to the other AP"
34     ::= { iappAPTableEntry 4 }
35
36  iappAPRoundTripTime OBJECT-TYPE
37     SYNTAX      TimeTicks
38     MAX-ACCESS read-only
39     STATUS      current
40     DESCRIPTION
41         "The time interval (in hundredths of a second) between
42         the most recent Move-Notify sent by this AP and the
43         Move-Response that matched it from the other AP."
44     ::= { iappAPTableEntry 5 }
45
46  iappAPRTO OBJECT-TYPE
47     SYNTAX      TimeTicks
48     MAX-ACCESS read-only
49     STATUS      current
50     DESCRIPTION
51         "The Round Trip Timeout (RTO) (in hundredths of a second)
52         between this AP and the other AP."
53     ::= { iappAPTableEntry 6 }
54
55  -- Request/Response statistics
56  --
57  -- TotalIncomingPackets = MoveNotifyReceived + MoveResponseReceived + UnknownTypes

```

Inter-Access Point Protocol

```

1  --
2  -- TotalIncomingPackets - Malformed - Unauthentic -
3  -- UnknownTypes - PacketsDropped = Successfully received
4  --
5
6  iappMoveNotifySent OBJECT-TYPE
7      SYNTAX Counter32
8      MAX-ACCESS read-only
9      STATUS current
10     DESCRIPTION
11         "The number of Move-Notify packets sent to this AP.
12         This does not include retransmissions."
13     ::= { iappAPTableEntry 7 }
14
15  iappMoveNotifyRetransmissions OBJECT-TYPE
16     SYNTAX Counter32
17     MAX-ACCESS read-only
18     STATUS current
19     DESCRIPTION
20         "The number of Move-Notify packets
21         retransmitted to this AP."
22     ::= { iappAPTableEntry 8 }
23
24  iappMoveNotifyReceived OBJECT-TYPE
25     SYNTAX Counter32
26     MAX-ACCESS read-only
27     STATUS current
28     DESCRIPTION
29         "The number of Move-Notify packets
30         (valid or invalid) received from this AP."
31     ::= { iappAPTableEntry 9 }
32
33  iappMoveResponseSent OBJECT-TYPE
34     SYNTAX Counter32
35     MAX-ACCESS read-only
36     STATUS current
37     DESCRIPTION
38         "The number of Move-Response packets sent to this AP."
39     ::= { iappAPTableEntry 10 }
40
41  iappMoveResponseReceived OBJECT-TYPE
42     SYNTAX Counter32
43     MAX-ACCESS read-only
44     STATUS current
45     DESCRIPTION
46         "The number of Move-Response packets
47         (valid or invalid) received from this AP."
48     ::= { iappAPTableEntry 11 }
49
50  iappMoveNotifyMalformed OBJECT-TYPE
51     SYNTAX Counter32
52     MAX-ACCESS read-only
53     STATUS current
54     DESCRIPTION
55         "The number of malformed Move-Notify
56         packets received from this AP.
57         Malformed packets include packets with

```

```
1         an invalid length. Unauthenticated packets
2         or unknown types are not
3         included as malformed packets."
4     ::= { iappAPTableEntry 12 }
5
6 iappMoveNotifyUnAuthentic OBJECT-TYPE
7     SYNTAX Counter32
8     MAX-ACCESS read-only
9     STATUS current
10    DESCRIPTION
11        "The number of Move-Notify packets
12        failing authentication, received from this AP."
13    ::= { iappAPTableEntry 13 }
14
15 iappMoveResponseMalformed OBJECT-TYPE
16     SYNTAX Counter32
17     MAX-ACCESS read-only
18     STATUS current
19     DESCRIPTION
20        "The number of malformed Move-Response
21        packets received from this AP.
22        Malformed packets include packets with
23        an invalid length. Unauthenticated packets
24        or unknown types are not
25        included as malformed packets."
26    ::= { iappAPTableEntry 14 }
27
28 iappMoveResponseUnAuthentic OBJECT-TYPE
29     SYNTAX Counter32
30     MAX-ACCESS read-only
31     STATUS current
32     DESCRIPTION
33        "The number of Move-Response packets
34        failing authentication, received from this AP."
35    ::= { iappAPTableEntry 15 }
36
37 iappMoveNotifyBadService OBJECT-TYPE
38     SYNTAX Counter32
39     MAX-ACCESS read-only
40     STATUS current
41     DESCRIPTION
42        "The number of Move-Notify packets
43        received from this AP which could not be acted
44        upon, due to inclusion of an unavailable service.
45        Malformed or unauthentic packets are not included
46        in this count."
47    ::= { iappAPTableEntry 16 }
48
49 iappMoveResponseBadService OBJECT-TYPE
50     SYNTAX Counter32
51     MAX-ACCESS read-only
52     STATUS current
53     DESCRIPTION
54        "The number of Move-Response packets
55        received from this AP which could not be acted
56        upon, due to requesting an unavailable service.
57        Malformed or unauthentic packets are not included
```

Inter-Access Point Protocol

```

1         in this count."
2     ::= { iappAPTableEntry 17 }
3
4 iappMoveNotifyPendingRequests OBJECT-TYPE
5     SYNTAX Gauge32
6     MAX-ACCESS read-only
7     STATUS current
8     DESCRIPTION
9         "The number of Move-Notify packets
10        destined for this AP that have not yet timed out
11        or received a response. This variable is incremented
12        when a Move-Notify is sent and decremented due to
13        receipt of a Move-Response, a timeout or retransmission."
14    ::= { iappAPTableEntry 18 }
15
16 iappMoveNotifyTimeouts OBJECT-TYPE
17     SYNTAX Counter32
18     MAX-ACCESS read-only
19     STATUS current
20     DESCRIPTION
21         "The number of Move-Notify timeouts to this AP.
22         After a timeout the AP may retry or
23         give up. A retry is counted as a
24         retransmit as well as a timeout."
25    ::= { iappAPTableEntry 19 }
26
27 iappUnknownType OBJECT-TYPE
28     SYNTAX Counter32
29     MAX-ACCESS read-only
30     STATUS current
31     DESCRIPTION
32         "The number of IAPP packets of unknown type which
33         were received from this AP."
34    ::= { iappAPTableEntry 20 }
35
36
37 iappMoveNotifyPacketsDropped OBJECT-TYPE
38     SYNTAX Counter32
39     MAX-ACCESS read-only
40     STATUS current
41     DESCRIPTION
42         "The number of Move-Notify packets received from
43         this AP and dropped for some other reason.
44         Malformed or unauthentic packets, or those
45         requesting an unavailable service are not included
46         in this count."
47    ::= { iappAPTableEntry 21 }
48
49 iappMoveResponsePacketsDropped OBJECT-TYPE
50     SYNTAX Counter32
51     MAX-ACCESS read-only
52     STATUS current
53     DESCRIPTION
54         "The number of Move-Response packets received from
55         this AP and dropped for some other reason, such
56         as arriving after the Timeout window has expired.
57         Malformed or unauthentic packets, or those

```

```
1           requesting an unavailable service are not included
2           in this count."
3       ::= { iappAPTableEntry 22 }
4
5
6 -- *****
7 -- *   End of IAPP MIB
8 -- *****
9 END
10
```

1 **Annex B, Context Transfer**

2 **(Informative)**

3 The text in this annex has been excerpted from IETF RFC 3162.

4 **B.1 Introduction**

5 IEEE 802.1X [13] enables authenticated access to IEEE 802 media, including Ethernet, Token Ring, and 802.11 wireless
6 LANs. Although Authentication, Authorization and Accounting (AAA) support is optional within IEEE 802.1X, it is
7 expected that many IEEE 802.1X Authenticators will function as AAA clients. Behavior of IEEE 802.1X Authenticators
8 acting as RADIUS clients is described in [24].

9 The IEEE 802 Inter-Access Point Protocol (IAPP), under development within the IEEE 802.11 TGF working group, supports
10 the transfer of context between access points implementing IEEE 802 technology. This annex describes how IAPP can be
11 used to support transfer of authentication, authorization and accounting (AAA) context between devices supporting IEEE
12 802.1X network port authentication [13].

13 In terms of organization, this document first develops a general model for AAA context transfer. Central to the model is
14 the notion of a "correct" context transfer -- a transfer resulting in the same context on the new access point as would have
15 resulted had a AAA conversation been completed.

16 The circumstances in which "correct" context transfer can be achieved are analyzed -- demonstrating that this can only be
17 achieved in a limited set of circumstances. As a result, it is suggested that context transfer protocols restrict the domain of
18 applicability to scenarios involving a high degree of homogeneity.

19 For example, layer 2 context transfer solutions are most likely to be successful transferring context within media families,
20 such as IEEE 802. While the IAPP is expected to be used primarily for transfer of context between IEEE 802.11 access
21 points, it is also possible for it to be used to transfer context between access points supporting other IEEE 802 media, such
22 as IEEE 802.15 or 802.16. Where context transfer between dissimilar media is required, then higher layer homogeneity is
23 needed. This can be achieved, for example, by restricting applicability to access points supporting Mobile IP.

24 **B.2 Terminology**

25 This document uses the following terms:

26 **Authenticator**

27 An Authenticator is an entity that requires authentication from the Supplicant. The Authenticator may be
28 connected to the Supplicant at the other end of a point-to-point LAN segment or 802.11 wireless link.

29 **Authentication Server**

30 An Authentication Server is an entity that provides an Authentication Service to an Authenticator. This
31 service verifies from the credentials provided by the Supplicant, the claim of identity made by the Supplicant.

32 **Port Access Entity (PAE)**

33 The protocol entity associated with a physical or virtual (802.11) Port. A given PAE may support the protocol
34 functionality associated with the Authenticator, Supplicant or both.

35 **Supplicant**

36 A Supplicant is an entity that is being authenticated by an Authenticator. The Supplicant may be connected to
37 the Authenticator at one end of a point-to-point LAN segment or 802.11 wireless link.

1 **B.3 Context transfer model**

2 In attempting to transfer context between devices, the first task is to understand how "context" is defined, and what the
3 goal of the context transfer is. For the purpose of this document "context" will refer to the set of state variables defining
4 the service to be provided to the user.

5 To date, a number of protocols have been proposed for defining and managing services provided on a per-user basis.
6 RADIUS, defined in [4]-[6], is a first-generation protocol for Authentication, Authorization and Accounting (AAA).
7 Diameter [25] is a next generation AAA protocol currently under development. COPS [26] is a protocol used to manage the
8 use of policies for QoS, Security, and other policy-based services.

9 In each of these protocols, exchanges are used to establish, and possibly to remove, state from devices. In thinking about
10 transfer of context initially established through such protocols, we would like to propose the "Equivalency Principle":

11 For context established via protocol exchanges, transfer of context to a new device can be accomplished by
12 transferring the protocol exchanges that created the context on the original device, and processing them on the new
13 device. For such a context transfer to be successful, the state created on the new device by processing such an
14 exchange MUST be equivalent to the state that would have been created by having the new device engage in a
15 fresh protocol conversation.

16 For the equivalency principle to be satisfied, it is necessary for the new device to be able to process the protocol
17 exchanges from the old device, and for those exchanges to result in the same state on the new device. This requires that
18 the protocol messages completely describe the context to be created on the device, and that the effect of processing these
19 messages not depend on state that exists uniquely on the old device, but may not exist on the new device.

20 For example, a protocol message that describes the state to be attained in terms of deltas from a previous state would not
21 be suitable for use in context transfer, since the effect of the protocol message would differ depending on the previous
22 device state. Similarly, if a protocol message were conditionally executed based on dynamic data, such as the number of
23 users on the device, then the message might have a different effect on the new device than on the old device.

24 To a large extent, AAA protocols meet the criteria, since the desired device state is completely described by the
25 authorizations. Conditional execution, if it occurs, is relatively rare and usually confined to the AAA server.

26 The set of messages that establish service context differ, depending on the AAA protocol that is being considered.
27 Within RADIUS [4]-[6], service context is only established via an Access-Accept. Access-Reject messages do not
28 establish context since their purpose is to deny access. Similarly, Access-Challenge messages do not establish context
29 since they represent an intermediate stage within the authentication conversation. Since only one RADIUS message
30 (Access-Accept) establishes service context, to re-establish context on a new device, to first order it is only necessary to
31 transfer Access-Accept messages to the new device, and process them as if they were sent by the RADIUS server.

32 Note that since only one RADIUS message type can establish context, the message type need not be included explicitly,
33 since it is implicit. As a result, devices supporting transfer of RADIUS context need only transfer attributes, not the entire
34 RADIUS message.

35 **B.3.1 "Correct" context transfer**

36 Given this model for context establishment, it is worthwhile to examine when the transfer of context between devices
37 produces a "correct" result.

38 One way to define correctness in a context transfer is that the transfer establishes on the new device the same context as
39 would have been created had the new device completed a AAA conversation with the authentication server. Ideally, a
40 context transfer should only succeed if it is "correct" in this way. If a successful context transfer would establish
41 "incorrect" state, it would be preferable for such a transfer to fail.

1 Not all AAA and access device configurations are capable of meeting this definition of "correctness". Implicit within our
2 context transfer model is trust between devices transferring context. Since the new device acts on the context transfer as
3 though it had been instructed by a trusted AAA server, it is necessary for the new device to trust the old device.

4 In transfer of context across administrative domains, such a level of trust may not be possible or appropriate. As a result, a
5 context transfer may fail even in situations where the devices are homogeneous, due to lack of trust between administrative
6 domains.

7 If the deployment is heterogeneous, it also may be difficult to meet this definition of correctness. In these situations, AAA
8 servers often perform conditional evaluation, in which the authorizations returned in an Access-Accept message are
9 contingent on characteristics of the AAA client or the user. For example, in a heterogeneous deployment, the AAA server
10 might return different authorizations depending on the type of device making the request, in order to make sure that the
11 requested service is consistent with device capabilities.

12 If differences between the new and old device would result in the AAA server sending a different set of messages to the
13 new device than were sent to the old device, then a context transfer between the devices cannot be carried out correctly.

14 For example, if some access points within a deployment support dynamic VLANs while others do not, then attributes
15 present in the Access-Request (such as the NAS-IP-Address, NAS-Identifier, Vendor-Identifier, etc.) could be examined to
16 determine when VLAN attributes will be returned, as described in [24].

17 In practice, this limits the situations in which context transfer can be expected to be successful. Where the deployed
18 devices implement the same set of services, it may be possible to transfer context successfully. However, where the
19 supported services differ between devices, or where some devices require vendor specific attributes, the context transfer
20 may not succeed. For example, RFC 2865, section 1.1 states:

21 "A NAS that does not implement a given service MUST NOT implement the RADIUS attributes for that service. For
22 example, a NAS that is unable to offer ARAP service MUST NOT implement the RADIUS attributes for ARAP. A
23 NAS MUST treat a RADIUS access-accept authorizing an unavailable service as an access-reject instead."

24 Obeying the Equivalency Principle, if a new device is provided with RADIUS context for an unavailable service, then it
25 MUST process this context the same way it would handle a RADIUS Access-Accept requesting an unavailable service.
26 This MUST cause the context transfer to fail.

27 Although it may seem somewhat counter-intuitive, failure is indeed the "correct" result. Presumably a correctly configured
28 AAA server would not request that a device carry out a service that it does not implement. This implies that if the new
29 device were to complete a AAA conversation that it would be likely to receive different service instructions than those
30 present in the context transfer. In such a case, failure of the context transfer is the desired result. This will cause the new
31 device to go back to the AAA server in order to receive the appropriate service definition.

32 Thus in practice, context transfer is most likely to be successful within a homogeneous device deployment within a single
33 administrative domain. For example, where all the devices support IEEE 802.1X, success is possible, as long as the same set
34 of security services are supported. For example, it would not be advisable to attempt to transfer context between an 802.11
35 access point implementing WEP to an 802.15 access point without security support. The correct result of such a transfer
36 would be a failure, since if the transfer were blindly carried out, then the user would find themselves moved from a secure
37 to an insecure channel without permission from the AAA server. Thus the definition of an "unsupported service" MUST
38 encompass requests for unavailable security services.

39 In general, context transfers between media with different service models should not be expected to be successful. For
40 example, attempts to transfer context between cellular devices and 802.11 access points cannot be "correct" within this
41 model, unless the cellular access points implement the same set of services as the 802.11 access points. Where the
42 implemented services differ, the correct behavior would be for such context transfers to fail, and for the 802.11 AP to pick
43 up the correct service definition by going back to the AAA server. Thus while attempted context transfers between
44 heterogeneous technologies may fail, context transfers between homogeneous devices have a higher probability of
45 success.

1 **B.3.2 Context handling**

2 AAA is not mandatory to implement for IEEE 802.1X Authenticators. The IEEE 802.1X specification provides guidelines
3 for usage of RADIUS [13], a revised version of which can be found in [24]. However, support for other protocols is
4 feasible. Since a IEEE 802.1X Authenticator may support zero or more AAA protocols and implementation of AAA is non-
5 mandatory, an IEEE 802.1X Authenticator cannot be assumed to implement any particular AAA protocol.

6 Therefore it is important that the context transfer protocol be agnostic with respect to AAA protocols. If two devices
7 share support for a given AAA protocol, then the context transfer mechanism should enable the devices to interoperate.
8 One way to accomplish this is to enable the context transfer mechanism to support multiple AAA protocols within the
9 same message. This allows a device that speaks multiple protocols to interoperate with a device that only supports one of
10 them.

11 Through addition of a AAA Information Element, and unique sub-elements for each AAA protocol, it is possible to
12 support transfer of context for multiple AAA protocols within the same message. Assigning only one Information Element
13 for AAA ensures against exhaustion of the IAPP element space. Since the number of AAA attributes may be substantial,
14 assignment of Information Elements to individual attributes is to be avoided.

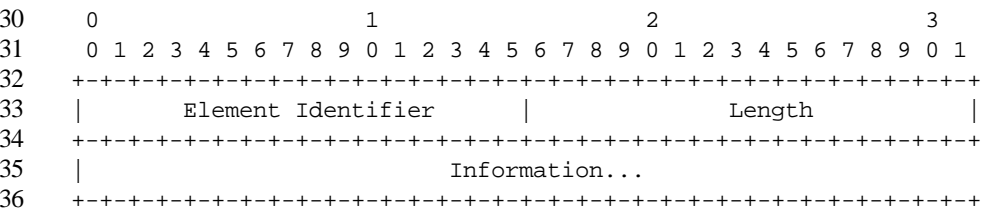
15 The packaging of AAA protocol messages within individual sub-elements enables compatibility with the definition of
16 correctness described earlier. Within IAPP, a device that receives Information Elements or sub-elements that it does not
17 support will ignore those elements, and process those that it does support.

18 However, as described earlier, our model of context transfer requires that if a device supports a AAA protocol, that
19 transferred AAA messages **MUST** be processed according to the rules of the protocol. For RADIUS, this implies that the
20 context transfer **MUST** fail if unavailable services are requested. As a result, individual RADIUS attributes **MUST NOT** be
21 encoded as Information Elements or sub-elements within IAPP. Rather, RADIUS attributes are encoded as a unit within the
22 RADIUS sub-element. This enables the correct processing to occur. While a device may ignore an entire Information
23 Element or sub-element, once the Information Element or sub-element is recognized it must be processed in its entirety.

24 Among other things, this approach enables the context transfer operation to be independent of the supported AAA
25 protocol. For example, a device supporting both Diameter and RADIUS could include sub-elements for both protocols.
26 This would enable transfer of context to a new device supporting either protocol.

27 **B.3.3 Information Element format**

28 Within IAPP, Information Elements have the following structure:



37 **Element Identifier**

38 The Element Identifier field is two octets. It identifies the enclosed Information Element.

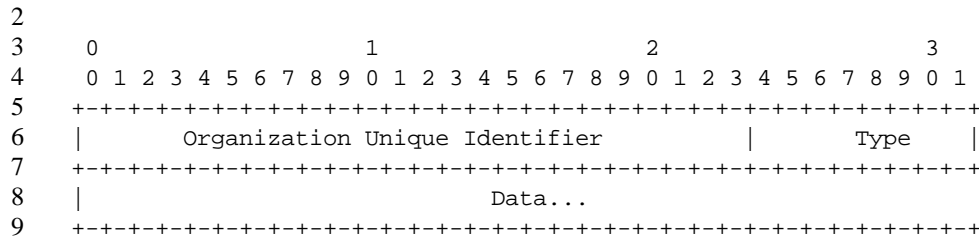
39 **Length**

40 The Length field is two octets. It encodes the length of the Information Element, including the Element Identifier,
41 Length and Information fields.

42 **Information**

43 The Information field is variable length. It encodes the Information Element.

1 AAA sub-elements are encoded within the Information field as follows:



10 Organization Unique Identifier (OUI)

11 The OUI is a three octet field, encoding the Organization Unique Identifier. An OUI of zero is used for standardized
12 sub-elements. Non-zero OUIs can be used to support vendor-specific sub-elements.

13 Type

14 The type field is one octet, and represents the AAA protocol type:

15 RADIUS = (1)

16 Data

17 The Data field is of variable length, and contains the context to be transferred. For RADIUS this consists of a list of
18 attributes.

19 B.3.4 Usage guidelines for the RADIUS sub-element

20 RADIUS context is established solely by Access-Accept messages, and therefore the bulk of RADIUS attributes
21 includable within the RADIUS sub-element are those that may be included within an Access-Accept, as described in [4]-
22 [6]. There are two exceptions: the Acct-Authentic and Acct-Multi-SessionId accounting attributes. The attributes
23 allowable for use with transfers of IEEE 802.1X context are described in Appendix A.

24 Acct-Authentic encodes the authentication technique utilized on the old access point: RADIUS, Local or Remote. A value
25 of RADIUS denotes authentication against a backend RADIUS server; Local means that the user authenticated against the
26 local database on the old device; Remote means that a AAA protocol other than RADIUS was used.

27 Typically, it does not make sense to transfer context of sessions established by local authentication. This violates the
28 Equivalency Principle because context established via local authentication will not in general be the same as the context
29 that would be established by carrying out a conversation with the AAA server. In order to guard against inappropriate
30 context transfers, the new device SHOULD examine the authentication status prior to deciding to accept the context
31 transfer.

32 Acct-Multi-SessionId enables linkage of accounting records from related sessions. As described in [24], it is possible to
33 maintain the same Acct-Multi-SessionId as a user moves between devices. To enable this, it is necessary to include the
34 Acct-Multi-SessionId in the context transfer.

35 B.5 Security considerations

36 B.5.1 Trust issues

37 Implicit within our context transfer model is trust between devices engaging in a context transfer. Since the new device will
38 act on the context transfer as though it had been given the service instructions by a trusted AAA server, it is necessary
39 for the new device to trust the old device.

1 In transfer of context across administrative domains, such a level of trust may not be possible or appropriate. Therefore, it
2 is possible for context transfer to fail even in situations where the devices are homogeneous, due to lack of trust between
3 administrative domains.

4 Another implication of the "Equivalency Principle" is that the context transfer protocol SHOULD provide the same level of
5 security as the AAA protocol whose context is being transferred. For example, where the AAA protocol is using IPsec to
6 provide confidentiality, it does not make sense for the context transfer protocol to use shared secret-based hiding.

7 **B.5.2 Confidentiality**

8 AAA protocol messages may include attributes requiring confidentiality. This includes user passwords, encryption keys,
9 or tunnel passwords. In order to transfer these attributes securely, confidentiality is required. Following the Equivalency
10 Principle, attributes are processed as though they came from the AAA server. This includes security processing. As a
11 result, existing AAA security mechanisms are used in order to ensure confidentiality.

12 This can be accomplished in two ways. As described in [4], RADIUS attributes can be encrypted using the shared secret
13 shared by the new device and the AAA server. Alternatively, if IPsec is supported, encapsulating security payload (ESP)
14 with a non-null transform can be used to provide confidentiality, as described in [23]. In this case, if a shared secret does
15 not exist, then a null shared secret is assumed.

16 **B.6 References**

17 [1] Blunk, L., Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

18 [2] Rivest, R., Dusse, S., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

19 [3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March, 1997.

20 [4] Rigney, C., Rubens, A., Simpson, W., Willens, S., "Remote Authentication Dial In User Service (RADIUS)", RFC 2865,
21 June 2000.

22 [5] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

23 [6] Rigney, C., Willats, W., Calhoun, P., "RADIUS Extensions", RFC 2869, June 2000.

24 [7] IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990.

25 [8] ISO/IEC 10038 Information technology - Telecommunications and information exchange between systems - Local area
26 networks - Media Access Control (MAC) Bridges, (also ANSI/IEEE Std 802.1D- 1993), 1993.

27 [9] ISO/IEC Final CD 15802-3 Information technology - Telecommunications and information exchange between systems -
28 Local and metropolitan area networks - Common specifications - Part 3:Media Access Control (MAC) bridges, (current
29 draft available as IEEE P802.1D/D15).

30 [10] IEEE Standards for Local and Metropolitan Area Networks: Draft Standard for Virtual Bridged Local Area Networks,
31 P802.1Q/D8, January 1998.

32 [11] ISO/IEC 8802-3 Information technology - Telecommunications and information exchange between systems - Local and
33 metropolitan area networks - Common specifications - Part 3: Carrier Sense Multiple Access with Collision Detection
34 (CSMA/CD) Access Method and Physical Layer Specifications, (also ANSI/IEEE Std 802.3- 1996), 1996.

35 [12] IEEE Standards for Local and Metropolitan Area Networks: Demand Priority Access Method, Physical Layer and
36 Repeater Specification For 100 Mb/s Operation, IEEE Std 802.12-1995.

- 1 [13] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Draft
2 802.1X/D11, March 2001.
- 3 [14] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.
- 4 [15] Yergeau, F., "UTF-8, a transformation format of Unicode and ISO 10646", RFC 2044, October 1996.
- 5 [16] Aboba, B., Beadles, M., "The Network Access Identifier", RFC 2486, January 1999.
- 6 [17] Alvestrand, H. and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434,
7 October 1998.
- 8 [18] Dobbertin, H., "The Status of MD5 After a Recent Attack." CryptoBytes Vol.2 No.2, Summer 1996.
- 9 [19] Atkinson, R., "Security Architecture for the Internet Protocol", RFC 1825, August 1995.
- 10 [20] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., Goyret, I., "RADIUS Attributes for Tunnel Protocol Support",
11 RFC 2868, June 2000.
- 12 [21] Zorn, G., Mitton, D., Aboba, B., "RADIUS Accounting Modifications for Tunnel Protocol Support", RFC 2867, June
13 2000.
- 14 [22] Information technology - Telecommunications and information exchange between systems - Local and metropolitan
15 area networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)
16 Specifications, IEEE Std. 802.11-1997, 1997.
- 17 [23] Aboba, B., Zorn, G., Mitton, D., "RADIUS and IPv6", Internet draft (work in progress), draft-aboba-radius-ipv6-10.txt,
18 June 2001.
- 19 [24] Congdon, P., Et al. "IEEE 802.1X Usage Guidelines", Internet draft (work in progress), draft-congdon-radius-8021x-
20 15.txt, July 2001.
- 21 [25] Calhoun, P., Akhtar, H., Arkko, J., Guttman, E., Rubens, A., Zorn, G., draft-ietf-aaa-diameter-08.txt, November 2001
- 22 [26] J. Boyle, R. Cohen, D. Durham, S. Herzog, R. Rajan, A. Sastry, "The **COPS** (Common Open Policy Service) Protocol",
23 RFC 2748, January 2000

24 Appendix A - Table of Attributes

25 The following table provides a guide to which attributes are sent and received as part of IEEE 802.1X authentication, and
26 which attributes are considered part of the "context" to be transferred during roaming. L3 denotes attributes that will be
27 understood only by switches or access points implementing Layer 3 capabilities.

802.1X	Context	#	Attribute
X	X	1	User-Name [4]
		2	User-Password [4]
		3	CHAP-Password [4]
X		4	NAS-IP-Address [4]
X		5	NAS-Port [4]
X	X	6	Service-Type [4]
		7	Framed-Protocol [4]
		8	Framed-IP-Address [4]
		9	Framed-IP-Netmask [4]
L3	X	10	Framed-Routing [4]
X	X	11	Filter-Id [4]

802.1X	Context	#	Attribute
X	X	12	Framed-MTU [4]
		13	Framed-Compression [4]
		14	Login-IP-Host [4]
		15	Login-Service [4]
		16	Login-TCP-Port [4]
X	X	18	Reply-Message [4]
		19	Callback-Number [4]
		20	Callback-Id [4]
L3	X	22	Framed-Route [4]
L3	X	23	Framed-IPX-Network [4]
X	X	24	State [4]
X	X	25	Class [4]
X	X	26	Vendor-Specific [4]
X	X	27	Session-Timeout [4]
X	X	28	Idle-Timeout [4]
X	X	29	Termination-Action [4]
X		30	Called-Station-Id [4]
X		31	Calling-Station-Id [4]
X		32	NAS-Identifier [4]
X		33	Proxy-State [4]
		34	Login-LAT-Service [4]
		35	Login-LAT-Node [4]
		36	Login-LAT-Group [4]
L3	X	37	Framed-AppleTalk-Link [4]
L3	X	38	Framed-AppleTalk-Network [4]
L3	X	39	Framed-AppleTalk-Zone [4]
X		40	Acct-Status-Type [5]
X		41	Acct-Delay-Time [5]
X		42	Acct-Input-Octets [5]
X		43	Acct-Output-Octets [5]
X		44	Acct-Session-Id [5]
X	X	45	Acct-Authentic [5]
X		46	Acct-Session-Time [5]
X		47	Acct-Input-Packets [5]
X		48	Acct-Output-Packets [5]
X		49	Acct-Terminate-Cause [5]
X	X	50	Acct-Multi-Session-Id [5]
		51	Acct-Link-Count [5]
X		52	Acct-Input-Gigawords [6]
X		53	Acct-Output-Gigawords [6]
X		55	Event-Timestamp [6]
		60	CHAP-Challenge [4]
X	X	61	NAS-Port-Type [4]
		62	Port-Limit [4]
		63	Login-LAT-Port [4]
X	X	64	Tunnel-Type [20]
X	X	65	Tunnel-Medium-Type [20]
L3	X	66	Tunnel-Client-Endpoint [20]
L3	X	67	Tunnel-Server-Endpoint [20]
L3	X	68	Acct-Tunnel-Connection [21]
L3	X	69	Tunnel-Password [20]
		70	ARAP-Password [6]

802.1X	Context	#	Attribute
		71	ARAP-Features [6]
		72	ARAP-Zone-Access [6]
		73	ARAP-Security [6]
		74	ARAP-Security-Data [6]
		75	Password-Retry [6]
		76	Prompt [6]
X		77	Connect-Info [6]
X		78	Configuration-Token [6]
X		79	EAP-Message [6]
X		80	Message-Authenticator [6]
X	X	81	Tunnel-Private-Group-ID [20]
L3	X	82	Tunnel-Assignment-ID [20]
X	X	83	Tunnel-Preference [20]
		84	ARAP-Challenge-Response [6]
X		85	Acct-Interim-Interval [6]
X		86	Acct-Tunnel-Packets-Lost [21]
X		87	NAS-Port-Id [6]
		88	Framed-Pool [6]
L3	X	90	Tunnel-Client-Auth-ID [20]
L3	X	91	Tunnel-Server-Auth-ID [20]
X		TBD	NAS-IPv6-Address [23]
		TBD	Framed-Interface-Id [23]
L3	X	TBD	Framed-IPv6-Prefix [23]
		TBD	Login-IPv6-Host [23]
L3	X	TBD	Framed-IPv6-Route [23]
L3	X	TBD	Framed-IPv6-Pool [23]

- 1
- 2 Key
- 3 802.1X = Allowed for use with IEEE 802.1X
- 4 Context = Transferred during roaming if available
- 5 L3 = implemented only on switches/access points with Layer 3 capabilities
- 6