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

Sponsored by the
LAN/MAN Standards Committee
of the
IEEE Computer Society

Introduction

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

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

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

Stuart Kerry, *Chair*
David Bagby, *Chair, Task Group f*
Bob O'Hara, *Editor, Task Group f*

Put working group member names here

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

Contents

Figures

Tables

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-Access Point Protocol (IAPP) 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 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, 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.

Deleted: AP

Deleted: (IAPP)

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 station (STA) has a single association at a given time is unlikely to be achieved.

As 802.11 systems have grown in popularity, 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.

Deleted: mobile

Deleted: this limitation has become an impediment to WLAN market growth. At the same time,

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 APs to interoperate on a common DS, using the Transmission Control Protocol over IP (TCP/IP) or 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 about one another. The devices in a network that might use the IAPP are 802.11

Deleted: conformant

Deleted: u

Deleted: d

Deleted: p

APs. Other devices in a network that are affected by the operation of the IAPP are layer 2 networking devices, such as bridges and switches.

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

Deleted: a registration service

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

Deleted: to register as part of an ESS,

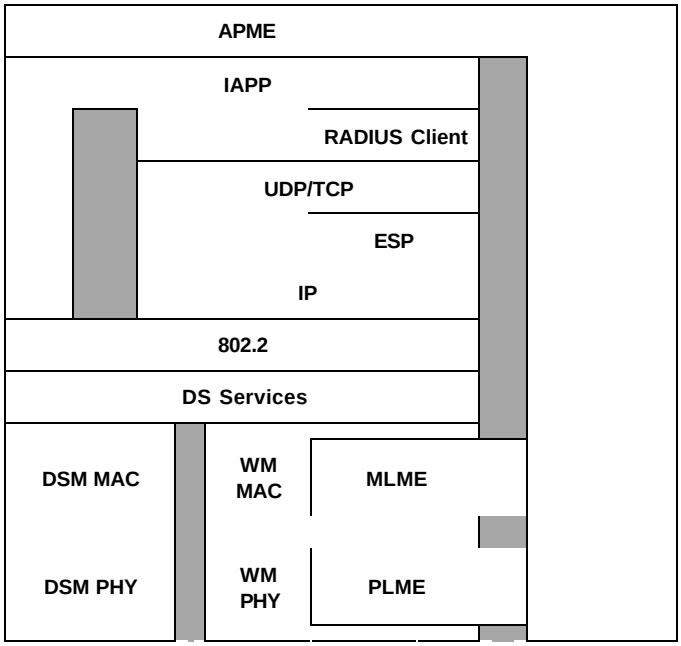


Figure 1 - AP Architecture with IAPP

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

Deleted: station
Deleted: ,
Deleted: 802.11
Deleted: station
Deleted: 802.11
Deleted: station
Deleted: station
Deleted: station
Deleted: 802.11
Deleted: station
Deleted: station
Deleted: station

be delivered to it. A STA can meet the local IP address requirement in many ways. Two mechanisms for a STA to accomplish this are to renew a Dynamic Host Configuration Protocol (DHCP) lease for its IP address or to use Mobile IP. Other mechanisms are possible that meet this requirement.

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

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

IAPP transactions are over the DS. Hence, IAPP is independent of the security scheme defined in ISO/IEC 8802-11:1999.

This recommended practice makes use of the IETF RFCs listed in clause 2 to implement many of its functions. It also relies on a STA making use of the 802.11 Reassociation Request frame when roaming from one AP to another, in order to provide the most complete services to the APs using the IAPP. When a STA uses the 802.11 Association Request, rather than the Reassociation Request, the IAPP may not be able to notify the AP at which the STA was previously associated of the new association. This may result in the old AP (indicated in the "current AP" field of the reassociation request frame) maintaining context for the STA that has roamed to a new AP for a longer time than is strictly necessary. 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 STA association requirement of 802.11.

1.4 Inter-AP Security Risks

Inter-AP communications present three opportunities to an attacker. The attacker can use IAPP as a Denial-of-Service (DoS) attack against a STA state in its AP. It can capture MOVE packets to gather information on the STA that is roaming. It can act as a rogue AP in the ESS.

A Bogus MOVE or ADD-Notify might cause an AP to drop all state it has with a STA. Since these IAPP packets are transmitted over IP, they could be introduced anywhere, from any device that has the necessary knowledge. This attack can best be eliminated by providing packet authentication to all MOVE and ADDs. The protection for the MOVEs can be provided by an IPsec (ESP, RFC 2406) pair-wise Security Associations (SA). The protection for the ADDs requires a group IPsec Security Association. The content of the MOVE can be encrypted by the same IPsec pair-wise SAs, protecting it from scrutiny of an attacker.

The use of IPsec with RADIUS for the Key Management provides for discovery of Rogue APs. The use of IPsec for IAPP MOVEs prevents a STA from roaming from a Rogue AP to a valid AP in the ESS. It also blocks the move of the STA context information to a Rogue AP if the STA roams to it. The RADIUS Access-Request provides the RADIUS server with knowledge of the presence of a Rogue AP

Deleted: station

Deleted: station

Deleted: station

Deleted: station

Deleted: station

Deleted: All the IAPP transactions can make use of the security schemes employed over the distribution system medium (DSM).

Deleted: station

Deleted: station

Deleted: station

Deleted: station

Deleted: station

Formatted: Bullets and Numbering

Deleted: Where 802.1X is used for authentication, use of the Association Request instead of the Reassociation Request will result in a re-authentication, potentially disrupting connectivity.

2 References

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

IEEE Standard 802.11-1999[1]
IEEE Standard 802.1X-2001 Port Based Network Access Control[1]
IEEE Standard 802.2-1998 Logical Link Control[1]
RFC 768 – User Datagram Protocol[2]
RFC 791 – Internet Protocol[2]
RFC 1112 - Host extensions for IP multicasting[2]
RFC 1305 – Network Time Protocol version 3 specification[2]
RFC 1812 – Requirements for IP version 4 Routers[2]
RFC 2131 – Dynamic Host Configuration Protocol[2]
RFC 2181 - Clarifications to the DNS Specification[2]
RFC 2401 - Security Architecture for the Internet Protocol[2]
RFC 2406 - IP Encapsulating Security Payload (ESP)[2]
RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP[2]
RFC 2411 – IP Security Document Roadmap[2]
RFC 2548 - Microsoft Vendor-specific RADIUS Attributes[2]
RFC 2857 - The Use of HMAC-RIPEMD-160-96 within ESP and AH[2]
RFC 2865 - Remote Authentication Dial In User Service (RADIUS)[2]
RFC 2869 - RADIUS Extensions[2]
RFC 3162 – RADIUS in IPv6[2]

Deleted: 0
Deleted: 0

[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)

3 Definitions, abbreviations, and acronyms

AAA	Authentication, Authorization, and Accounting
AP	Access Point
APME	Access Point Management Entity
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
DHCP	Dynamic Host Configuration Protocol
DS	Distribution System
DSM	Distribution System Medium
ESP	IP Encapsulating Security Payload
ESS	Extended Service Set
IANA	Internet Assigned Numbers Authority
IAPP	Inter-Access Point Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
LLC	Logical Link Co ntrol
MAC	Medium Access Control
MLME	MAC Layer Management Entity
PAE	Port Access Entity
PHY	Physical layer
PLME	PHY Layer Management Entity
RADIUS	Remote Authentication Dial In User Service
SA	Security Association
SAP	Service Access Point
SME	Station Management Entity
SPI	Security Parameter Index
SSID	Service Set Identifier
STA	Station
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VSA	Vendor-specific attribute
WM	Wireless Medium
XID	Exchange Identifier

4 IAPP Service definition

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

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

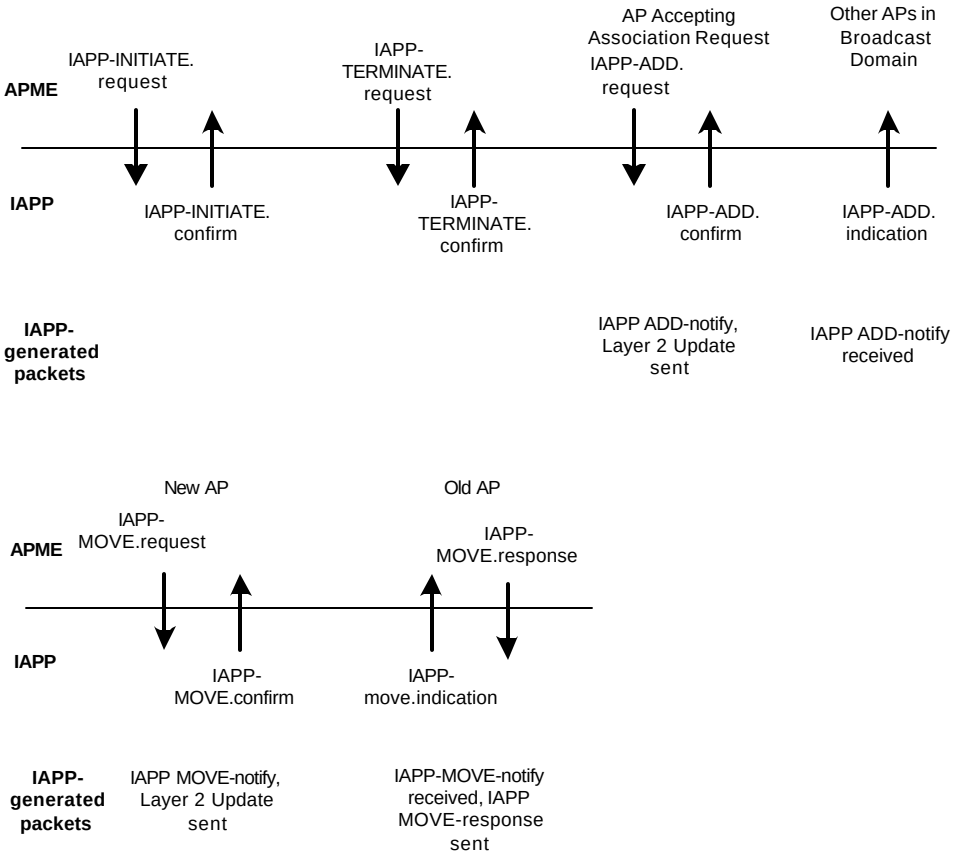


Figure 2 - Primitive Relationships

4.1 IAPP-INITIATE.request

4.1.1 Function

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

4.1.2 Semantics of the service primitive

The IAPP-INITIATE.request has the following semantics.

```
IAPP-INITIATE.request {
                    TCP Port,
                    UDP Port,
                    Shared Secret,
                    IP Address,
                    BSSID Secret
                    }
```

The UDP Port parameter is the UDP port number to be opened for the IAPP for transmission and reception of IAPP packets.

The TCP Port parameter is the TCP port number that the IAPP entity opens to listen for new IAPP TCP connections from the IAPP entities of other APs.

The Shared Secret is used to provide confidentiality of hidden attributes, and integrity and authentication for the communication between the RADIUS server and the AP. See 5.3.

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

The BSSID Secret is used to provide integrity, authentication and confidentiality of the security block sent between the RADIUS server and the AP. See 5.3

4.1.3 When generated

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

4.1.4 Effect of receipt

Upon receipt of this service primitive from an APME, the IAPP entity sends the RADIUS Initiate-Request and receives the RADIUS Initiate-Accept or Initiate-Reject. If the Initiate-Accept is received, then the IAPP entity initializes its data structures, functions, and protocols. The port for the IAPP should be opened by the IAPP entity at this time. The previous information in any IAPP data structures is lost. If an Initiate-Reject is received, the IAPP does not start.

4.2 IAPP-INITIATE.confirm

4.2.1 Function

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

4.2.2 Semantics of the service primitive

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

```
IAPP-INITIATE.confirm {
                    Status
                    }
```

The Status parameter indicates the result of the corresponding IAPP-INITIATE.request. The allowable value for the Status parameter are SUCCESSFUL, RUNNING, and FAILURE. SUCCESSFUL status should be returned if the IAPP entity is able to complete its initialization and open the requested port for the IAPP. RUNNING status should be returned if the IAPP entity receives an IAPP-INITIATE.request when the entity is already running. When RUNNING status has been returned, the IAPP ignored the parameters from the corresponding IAPP-INITIATE.request and the operation of the IAPP was unaffected. FAILURE status should be returned otherwise.

4.2.3 When generated

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

4.2.4 Effect of receipt

Upon receipt of the IAPP-INITIATE.confirm(Status=SUCCESSFUL) corresponding to a previously issued IAPP-INITIATE.request, an APME should initialize the operation of the AP by issuing an 802.11 MLME-START.request primitive to the local 802.11 MLME. The APME should not issue an 802.11 MLME-START.request until an IAPP-INITIATE.confirm(Status=SUCCESSFUL) is received, i.e., to ensure that all associations in this BSS are reported to the ESS using IAPP, the AP should not begin operating until after the IAPP-INITIATE.confirm(Status=SUCCESSFUL) is received.

Deleted: the BSS of the AP should not be operating until the IAPP-INITIATE.confirm is received

4.3 IAPP-TERMINATE.request

4.3.1 Function

This service primitive causes the IAPP entity to cease operation of the IAPP functions and protocol.

4.3.2 Semantics of the service primitive

The IAPP-TERMINATE.request primitive has the following semantics.

```
IAPP-TERMINATE.request {
                        }
```

4.3.3 When generated

This service primitive is generated by an APME when it is desired to terminate the operation of the IAPP entity. The APME should terminate operation of the local BSS, including disassociation of any associated STAs and ceasing of beacon transmissions, prior to terminating IAPP operation. The sole or final action by the APME in termination of local BSS operation should be issuance of an MLME-RESET.request. The IAPP-TERMINATE.request should be generated upon receipt of the corresponding MLME-RESET.confirm.

Deleted: The AP should disassociate any stations with which it is associated and cease accepting new associations before this primitive is invoked. The MLME-RESET.request primitive should be issued to the local 802.11 MLME to prevent further sending of Beacon frames before this primitive is invoked.

4.3.4 Effect of receipt

The UDP and TCP ports for the IAPP should be closed and the IAPP entity should cease operations.

4.4 IAPP-TERMINATE.confirm

4.4.1 Function

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

4.4.2 Semantics of the service primitive

The IAPP-TERMINATE.confirm primitive has the following semantics.

```
IAPP-TERMINATE.confirm {
                        Status
                        }
```

The Status parameter indicates the result of the corresponding IAPP-TERMINATE.request. The allowable value for the Status parameter is SUCCESSFUL.

4.4.3 When generated

This service primitive is generated by the IAPP entity when the actions begun by an IAPP-TERMINATE.request are completed.

4.4.4 Effect of receipt

Upon receipt of the IAPP-TERMINATE.confirm corresponding to a previously issued IAPP-TERMINATE.request, the APME should make no further service requests to the IAPP SAP without starting the IAPP entity again, using the IAPP-INITIATE.request primitive. Furthermore, the APME should not issue an MLME-START.request primitive prior to receipt of the subsequent IAPP-INITIATE.confirm primitive which indicates that the IAPP has been restarted successfully.

4.5 IAPP-ADD.request

4.5.1 Function

This service primitive is used when a STA associates with the AP using an 802.11 association request frame. The function of the IAPP-ADD.request primitive is two-fold. One purpose of this primitive is to cause the forwarding tables of layer 2 internetworking devices, e.g. bridges and switches, to be updated. This updates the layer 2 internetworking devices before a transmission from the associating STA, which might occur some arbitrary amount of time after the association. The second purpose of this primitive is to notify other APs within the multicast domain, i.e., that portion of a network in which a layer two frame addressed to a multicast address can be received, of the STA's new association, to allow those APs to clean up context information left behind by STAs that do not properly reassociate when moving from one AP to another.

Deleted: station

Deleted: broadcast

Deleted: station

4.5.2 Semantics of the service primitive

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

```
IAPP-ADD.request {
                        MAC Address,
                        Sequence Number,
                        Timeout
                        }
```

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

Deleted: station

The Sequence Number is the value of the 802.11 Sequence Number field of the Association Request frame received from the associating STA. The sequence number is provided to aid the APME in other APs in the determination of whether the association represented by this IAPP-ADD.request is the most recent association for the STA identified by the MAC Address. The 802.11 sequence number may be an ambiguous indication of the most recent association. But, this information may be useful to an algorithm making a determination of the location of the most recent association of a STA.

Deleted: station

Deleted: station

Deleted: is not

Deleted: un

Deleted: this

The Timeout parameter is the value, in seconds that the IAPP-ADD.confirm primitive will be generated with a status of TIMEOUT, if both the ADD-notify packet (see 6.2) and the Layer 2 Update frame (see 6.3) have not been sent. The

TIMEOUT status will not be generated by the IAPP-ADD.confirm only when both the ADD-notify packet and Layer 2 Update frame have been transmitted before the expiration of the period indicated by the Timeout parameter.

4.5.3 When generated

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

Deleted: an

4.5.4 Effect of receipt

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

1) The IAPP entity sends a Layer 2 Update frame to the DS, addressed such that it will cause forwarding tables in layer 2 devices that receive the frame to be updated so that all future traffic received by those layer 2 devices is forwarded to the port on which the frame was received,

2) The IAPP entity notifies the APs in the local multicast domain of the DS of the association between the AP and STA by sending an IAPP ADD-notify packet to the IAPP IP multicast address. See RFC 1112.

Deleted: the
Deleted: any
Deleted: bridges
Deleted: broadcast
Deleted: station
Deleted: subnet broadcast

4.6 IAPP-ADD.confirm

4.6.1 Function

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

4.6.2 Semantics of the service primitive

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

```
IAPP-ADD.confirm {
                    Status
                    }
```

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

4.6.3 When generated

This service primitive is generated upon completion of the actions of the IAPP-ADD.request or expiration of the timeout specified in the corresponding IAPP-ADD.request primitive.

4.6.4 Effect of receipt

Upon receipt of this service primitive by an APME with Status=SUCCESSFUL, the APME should cause the DS Services to begin forwarding frames for the associated STA. Receipt of this primitive with Status=TIMEOUT should cause the APME to attempt to determine the cause of the failure to send the ADD-notify packet and Layer 2 Update frames and possibly invoke the IAPP-ADD.request again. When Status=FAIL, the STA's association should be denied or the STA disassociated.

Deleted:
Deleted: station

4.7 IAPP-ADD.indication

4.7.1 Function

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

Deleted: mobile station

4.7.2 Semantics of the service primitive

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

```
IAPP-ADD.indication {
                    MAC Address,
                    Sequence Number
                    }
```

The MAC Address is the address of the STA received in the IAPP ADD-notify packet.

Deleted: mobile station

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

Deleted: station

Deleted: station

4.7.3 When generated

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

4.7.4 Effect of receipt

Upon receipt of this service primitive the APME should determine if the STA indicated by the MAC Address is shown to be associated with the AP receiving the IAPP-ADD.indication, with a sequence number older than that in the IAPP ADD-notify packet. If so, this service primitive should cause the generation of an 802.11 MLME-DISASSOCIATE.request by the APME. If the sequence number received in the IAPP ADD-notify packet is older than that received from the STA when it associated with the AP receiving the IAPP ADD-notify packet, the APME should ignore the indicated association and issue an IAPP-ADD.request.

Deleted: station

Deleted: station

Deleted: to ensure that layer two devices are properly informed of the location of t he station's most recent association

Implementers of STA MAC entities are advised of the importance of continuing the sequential assignment of sequence numbers for outgoing MPDUs and MMPDUs throughout STA operation, as required by 802.11. A discontinuity in the sequence numbering at the time of reassociation could cause roaming in an IAPP environment to be unreliable.

Deleted: station

Deleted: management frames

Deleted: station

Deleted: -1999

4.8 IAPP-MOVE.request

4.8.1 Function

This primitive should be issued by the APME when it receives an MLME-REASSOCIATE.indication from the MLME indicating 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 newly reassociated STA, and will notify the DS of the new reassociation between the AP and STA. An attempt to send an IAPP MOVE-notify packet to the AP with which the reassociating STA was previously associated will also be made.

Deleted: is

Deleted: station

Deleted: station

Deleted: station

4.8.2 Semantics of the service primitive

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

```
IAPP-MOVE.request {
                    MAC Address,
                    Sequence Number,
                    Old AP,
                    Context Block,
                    Timeout
                    }
```

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

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

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

The Context Block is the context to be sent to the Old AP. Otherwise, the Context Block is null. The Context Block is a container for information defined in 802.11 that is to be forwarded from one AP to another upon the reassociation of a STA.

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

4.8.3 When generated

This service primitive is generated by an APME when the MLME receives an 802.11 MLME-REASSOCIATE.indication from the local AP.

4.8.4 Effect of receipt

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

1) The IAPP entity determines the DSM layer 3 address of the AP identified by the old BSSID presented in the reassociation request and the security information needed to communicate with that AP using the methods described in clause 5.

2) The IAPP entity requests any context stored at the AP with which the STA was previously associated to be forwarded to the AP with which the STA is currently associated by sending an IAPP MOVE-notify packet to the old AP.

4.9 IAPP-MOVE.confirm

4.9.1 Function

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

4.9.2 Semantics of the service primitive

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

```
IAPP-MOVE.confirm {
```

Deleted: station

Deleted: station

Deleted: station

Deleted: station

Deleted: by other

Deleted: standards

Deleted: mobile station

Deleted: generates

Deleted: <#>The IAPP entity sends a Layer 2 Update frame to the DS, addressed such that it will cause the forwarding tables in any bridges that receive the frame to be updated so that all future traffic received by those bridges is forwarded to the port on which the frame was received.¶

Formatted: Bullets and Numbering

Deleted: station

Deleted: station

MAC Address,
Sequence Number,
Old AP,
New BSSID,
Context Block,
Status
}

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

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

Old AP is the MAC address of the AP with which the reassociating STA was last associated. This value is obtained by the IAPP from the received MOVE-notify packet.

The New BSSID parameter is the WM MAC address of the AP with which the STA has reassociated.

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

The Status parameter indicates the result of the corresponding IAPP-MOVE.request. The allowable values for this parameter are SUCCESSFUL, STALE_MOVE, MOVE_DENIED, NOT_OPERATING, FAIL, and TIMEOUT. The TIMEOUT status indicates the corresponding IAPP-MOVE.request primitive was not able to complete the transmission of both the IAPP MOVE-notify packet and IAPP Layer 2 Update frame, as well as receive the IAPP MOVE-response packet before the timeout parameter of the IAPP-MOVE.request primitive expired. The STALE_MOVE status indicates that the corresponding IAPP-MOVE.request did not completesuccessfully, because the IAPP MOVE-response packet returned by the Old AP contained a status value indicating a stale move. MOVE_DENIED indicates that the AP receiving the IAPP-MOVE.indication either is not able to verify a previous association by the indicated STA or has some other reason to deny the reassociation at the AP that sent the IAPP Move-notify packet. NOT_OPERATING indicates that the IAPP-MOVE.request was invoked either before an IAPP-INITIATE.request was invoked or after an IAPP-TERMINATE.request was invoked. FAIL indicates that a RADIUS Access-Reject was received in response to the RADIUS Access-Request sent to the RADUS server to look up the IP address of the Old AP.

4.9.3 When generated

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

4.9.4 Effect of receipt

Upon receipt of this service primitive by an APME with SUCCESSFUL status, the APME should send a Layer 2 Update frame to the DS, addressed such that it will cause the forwarding tables in any bridges that receive the frame to be updated so that all future traffic received by those bridges is forwarded to the port on which the frame was received and should cause the DS services to begin forwarding frames for the reassociated STA. Completion of the IAPP-MOVE.request includes receipt of STA context from the Old AP, when the Status is SUCCESSFUL. When the Status is not SUCCESSFUL, the APME should disassociate the STA indicated by the MAC Address parameter, using the 802.11 MLME-DISASSOCIATE.request primitive with a Reason Code of 1, meaning "Unspecified Reason". Future revisions of the IEEE Std 802.11 may define a new Reason Code that means "Old AP did not verify previous association." Should this Reason Code be defined, it should be used in preference to Reason Code 1.

Deleted: station

Deleted: station

Deleted: station

Deleted: This value is obtained by the APME from the Current AP Address field of the 802.11 Reassociation Request frame.

Deleted: mobile station

Deleted: station

Deleted: station

Deleted: station

4.10 IAPP-MOVE.indication

4.10.1 Function

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

4.10.2 Semantics of the service primitive

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

```
IAPP-MOVE.indication {
                MAC Address,
                New BSSID
                Sequence Number,
                AP Address,
                Context Block
                }
```

The MAC Address is the address of the STA that has reassociated with the AP that sent the IAPP MOVE-notify packet.

The New BSSID parameter is the WM MAC address of the AP sending the IAPP MOVE-notify packet.

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

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

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

4.10.3 When generated

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

4.10.4 Effect of receipt

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

Deleted: station
Deleted: 802.11
Deleted: station
Deleted: station
Deleted: station
Deleted: mobile station
Deleted: station
Deleted: station
Deleted: station
Deleted: station
Deleted: current
Deleted: station

4.11 IAPP-MOVE.response

4.11.1 Function

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

Deleted: station
Deleted: station
Deleted: station

4.11.2 Semantics of the service primitive

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

```
IAPP-MOVE.response {
                    MAC Address,
                    Sequence Number,
                    AP Address,
                    Context Block,
                    Status
                    }
```

The MAC Address is the address of the STA that has reassociated with the AP identified by the AP Address.

Deleted: 802.11
Deleted: station

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

Deleted: station

The AP Address is the DSM IP address of the AP where the STA has reassociated.

Deleted: MAC
Deleted: 802.11

The Context Block is the context for the reassociated STA. The Context Block may be null.

Deleted: station
Deleted: station

The Status parameter indicates the result of the corresponding IAPP-MOVE.indication. The allowable values for this parameter are SUCCESSFUL, MOVE_DENIED, and STALE_MOVE. STALE_MOVE should be used to indicate that the AP receiving the IAPP-MOVE.indication has a current association with the STA indicated by the MAC Address parameter with a more recent sequence number than that in the IAPP-MOVE.indication. MOVE_DENIED should be used to indicate that the AP receiving the IAPP-MOVE.indication either is not able to verify a previous association by the indicated STA or has some other reason to deny the reassociation at the AP that sent the IAPP Move-notify packet.

Deleted: station

4.11.3 When generated

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

4.11.4 Effect of receipt

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

Deleted: station
Deleted: station
Deleted: station
Deleted: receipt

5 Operation of the IAPP

The IAPP is a communication protocol, used by the management entity of an AP to communicate with other APs, when various local events occur in the AP. It is a part of a communication system comprising APs, STAs, an arbitrarily connected DS, and RADIUS infrastructure containing one or more RADIUS servers. The RADIUS servers provide two functions, mapping the BSSID of an AP to its IP address on the DSM and distribution of keys to the APs to allow the encryption of the communications between the APs. The function of the IAPP is to facilitate the creation and maintenance

Deleted: mobile station

of the ESS, support the mobility of STAs, and enable APs to enforce the requirement of a single association for each STA at a given time, as stated in ISO/IEC 8802-11:1999.

5.1 IAPP Protocol Overview

IAPP supports two protocol sequences. One is initiated by invoking the IAPP-ADD.request after the APME receives an MLME-ASSOCIATE.indication, and the other is initiated by invoking the IAPP-MOVE.request after the APME receives an MLME-REASSOCIATE.indication.

5.1.1 Actions triggered by the IAPP-ADD.request

When the IAPP receives an IAPP-ADD.request it should send an IAPP ADD-notify packet and a Layer 2 Update Frame. The IAPP ADD-notify packet is an IP packet with a destination-IP-address of the IAPP IP multicast address, the source IP and MAC address of the AP. The message body contains the MAC address of the STA and the Sequence Number from the Association request sent by the STA. On receiving this message the APME should check its association table and remove an association with the STA if it exists and is determined to be older than the association indicated by the ADD-notify packet. Note that purpose of the IAPP ADD-notify packet is to remove stale associations, not to modify the learning table. The learning table update is done by the Layer 2 Update frame (see sec.6.3). This frame has the source MAC address of the associating STA. This frame is used by receiving APs and other layer 2 devices to update their learning table.

5.1.2 Actions triggered by an IAPP-MOVE.request

When the IAPP receives an IAPP-MOVE.request it should send a n IAPP MOVE-Notify packet to the old AP and get back a MOVE-response from the old AP. The IAPP MOVE-Response carries the Context block for the STA's association from the old AP to the new AP.

The IAPP MOVE-Notify and MOVE-Response are IP packets carried in a TCP session between APs. The IP address of the old-AP must be found by mapping the BSSID from the reassociate message to its IP address. This mapping is done using a RADIUS exchange. For this exchange any standard RADIUS server that supports the Call Check service-type should work.

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

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

Figure 3 - IAPP Message Exchange During STA Reassociation

RADIUS (UDP)
2- Access-Request[BSSID1]
3- Access-Accept[AP1 ipaddr, SB1, SB2]

5.2 Formation and maintenance of the ESS

An ESS is a set of Basic Service Sets (BSSs) that form a single LAN, allowing an STA 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 be able to provide a secure handoff mechanism of STA information between APs in the same ESS. IAPP can use a central RADIUS

Deleted: 802.11…station…mobile station…IAPP also removes the need for reauthentication with 802.1X when moving between access points, enabling seamless connectivity, and reducing the load on the backend authentication server. ... [1]

Deleted: associate request to an Access Point… a reassociate req ... [2]

Deleted: an associate request

Deleted: an AP…associate …-P…Level …-…subnet broadcast …-message … … ... [3]

Deleted: reassociate request

Deleted: an AP…associate n…ove…old-…ove…R…old-ove…old-STA, allowing the new-STA to replicate the prior connection context without reauthenticating. This is commonly called a fast-handoff. ... [4]

Deleted: Move…Move ... [5]

Deleted: Move…R…s ... [6]

Deleted: s…b… …associate re ... [7]

Deleted: , the Registration Service

Deleted:

Deleted: 802.11…mobile station…mobile STA…s ... [8]

registry to define AP members of an ESS. Three levels of support for ESS formation are possible with the IAPP capabilities described here: 1) no administrative or security support; 2) support for dynamic mapping of BSSID to IP addresses; and 3) support for encryption and authentication of IAPP messages. Level one support can be achieved by configuring each AP in the ESS with the BSSID to IP address mapping for all other APs in the ESS. This may be acceptable for a small ESS. Many ESS providers will need levels 2 or 3, which requires RADIUS support. The remainder of this section describes requirements for level 2 and 3 support.

To include RADIUS support, 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, containing the damage caused by the compromise of the key at any single AP to only the compromised AP.

Since the roaming STA sends an 802.11 reassociation request 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 160 bits in length

c) IP address or DNS name, and

d) Cipher suites supported by the AP for the protection of IAPP communications.

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

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

5.3 RADIUS Protocol Usage

For the IAPP entity to function correctly, it must have the ability to discover the DSM IP address of the old BSSID in the ESS using the old BSSID as a lookup key. To implement this capability, the use of the RADIUS Protocol (IETF RFCs 2865 and 2869) is recommended. RADIUS is also used to obtain the security information to secure the communication between IAPP entities. This address mapping and security information may be preloaded or cached.

5.3.1 RADIUS Registration Access-Request

Upon receipt of an IAPP-INITIATE.request primitive, the AP

a) should register as a valid member of the ESS, and

b) may establish a secure channel for broadcast communications all APs in the ESS.

To register the AP's membership in the ESS, and to obtain the security parameters necessary for establishing a secure broadcast connection with all the other APs in the ESS, the AP sends a RADIUS Registration Access-Request packet to the RADIUS server with a Service-Type of IAPP-Register. The Registration Access-Request packet uses the AP's BSSID as the User-Name, the AP's BSSID Secret as the User-Password, and contains the global SSID as a vendor-specific attribute. This enables the RADIUS server to register the BSSID as a part of the ESS, and also to store the AP's BSSID Secret. The Registration Access-Request also contains the list of the AP's supported ESP and AH transforms, which allows the RADIUS server to determine the appropriate common supported ciphersuite(s) to use for the ADD-Notify and MOVE-Notify packets.

Deleted: T

Deleted: reassociate

Deleted: 128

Deleted: and the receipt of an MLME-START.confirm(ResultCode=SUCCESS)

Deleted: ,

Deleted: from

Deleted: 2138

Formatted: Bullets and Numbering

Formatted: Numbered+ Level: 1 + NumberingStyle:a, b, c, … + Start at: 1 + Alignment:Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Bullets and Numbering

The RADIUS Registration Access-Request contains the following attributes:

Table 1 - RADIUS Registration Access-Request Attributes

Attribute Number	Attribute Name	Value
1	User-Name	BSSID. The BSSID should be represented in ASCII format, with octet values separated by a "-". Example: "00-10-A4-23-19-C0".
2	User-Password	BSSID Secret, determined by the AP
4	NAS-IP-Address	AP's IP Address
6	Service-Type	IAPP-Register (number TBD[3])
26	Vendor-Specific	The following IEEE 802.11 vendor-specific attributes:
26-802-4[3]	SSID	The ASCII text SSID which denotes the ESS in which the BSSID is registering
26-802-5[3]	Supported-ESP-Authentication-Algorithms	The list of ISAKMP ESP Authentication IDs corresponding to the ESP Authentication algorithms supported by this AP (see Table 11)
26-802-6[3]	Supported-ESP-Transforms	The list of ISAKMP ESP Transform IDs corresponding to the ESP transforms supported by this AP (See Table 10)
32	NAS-Identifier (optional)	AP's NAS Identifier
80	Message-Authenticator	The RADIUS message's authenticator

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

Formatted: Bullets and Numbering

5.3.2 RADIUS Registration Access-Accept

Upon receipt of a Registration Access-Request from the AP, the RADIUS Server verifies that the AP is a valid member of the ESS. If the RADIUS Server permits the AP entrance into the ESS, it returns a Registration Access-Accept packet. Receipt of a valid RADIUS Registration Access-Accept packet both confirms that the AP is a valid member of the ESS, and also provides the AP with the appropriate security information for establishing a secure group communications channel for IAPP. For key rollover purposes, the parameters obtained by the AP from the RADIUS Registration Access-Accept should be cached for use in sending ADD-Notify packets.

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

Table 2 - RADIUS Registration Access-Accept Attributes

Attribute Number	Attribute Name	Value
1	User-Name	BSSID
6	Service-Type	IAPP-Register (number TBD[3])
26	Vendor-Specific	The following IEEE 802.11 vendor-specific attributes (optional):
26-802-7[3]	ESS-New-ESP-Transform-Key	The ESP Transform key used to encrypt ADD-Notify packets when sending
26-802-8[3]	ESS-New-ESP-Authentication-Key	The ESP Authentication key used to authenticate ADD-Notify packets when sending
26-802-9[3]	ESS-Old-ESP-Transform-Key	The ESP Transform key that can be used to decrypt ADD-Notify packets when receiving, if the New-ESP-Transform-Key does not work
26-802-10[3]	ESS-Old-ESP-Authentication-Key	The ESP Authentication key that can be used to authenticate ADD-Notify packets when receiving, if the New-ESP-Authentication-Key does not work
26-802-11[3]	ESS-ESP-Transform-ID	ESP Transform ID of the algorithm to use when encrypting/decrypting ADD-Notify packets
26-802-12[3]	ESS-ESP-Authentication-ID	ESP Authentication ID of the algorithm to use when encrypting/decrypting ADD-Notify packets
26-802-13[3]	ESS-ESP-SPI	SPI used to identify ESP group SA

27	Session-Timeout	Number of seconds until the AP should reissue the Registration Access-Request packet to the RADIUS Server to obtain new keying information
80	Message-Authenticator	The RADIUS message's authenticator

The ESS-New-ESP-Transform-Key, ESS-New-ESP-Authentication-Key, ESS-Old-ESP-Transform-Key, and ESS-Old-ESP-Authentication-Key attributes are encrypted as described for the MS-MPPE-Send-Key attribute in RFC 2548.

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

5.3.3 RADIUS Registration Access-Reject

As described in 5.3.2, upon receipt of a Registration Access-Request from the AP, the RADIUS Server will verify that the AP is a valid member of the ESS. A Registration Access-Reject may be issued due to an AP not supporting the ESP Transform or ESP Authentication algorithm selected for use in securing the ADD-Notify, or for other RADIUS configuration reasons not discussed here.

If the RADIUS Server determines that the AP is not a valid member of the ESS, the RADIUS Server will respond to the AP's Registration Access-Request packet with an RADIUS Registration Access-Reject. The RADIUS Registration Access-Reject packet instructs the AP to issue IAPP-INITIATE.confirm (ResultCode= FAILURE).

5.3.4 RADIUS Access-Request

Upon receipt of an IAPP-MOVE.request primitive, the receiving AP

a) must establish that the Old BSSID is a valid member of the New BSSID's ESS, and

b) may establish a secure channel for communications with the Old BSSID

To verify the Old BSSID's identity, and also to obtain the security parameters necessary for establishing a secure connection with the Old BSSID, the New AP sends a RADIUS Access-Request packet to the RADIUS server. The RADIUS Access-Request packet is used to verify the identity of the Old AP, and to establish the communications parameters between the New AP and the Old AP. The parameters obtained in the RADIUS Access-Accept are used to communicate with the Old AP, and can be cached for use upon receipt of future IAPP-MOVE.request primitives. It is important to note that this RADIUS Access-Accept verifies the old BSSID, and does not authenticate the STA.

The RADIUS Access-Request contains the following attributes:

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Deleted: R

Deleted: must establish

Formatted: Bullets and Numbering

Deleted: optionally

Deleted: ,

Table 3 - RADIUS Access-Request Attributes

Attribute Number	Attribute Name	Value
1	User-Name	Old BSSID. The Old BSSID should be represented in ASCII format, with octet values separated by a "-". Example: "00-10-A4-23-19-C0".
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 communications 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:Company WLAN".
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

Deleted: Attribute Number
Deleted: Attribute Name [Size]
Deleted: Value
Deleted: SHOULD
Deleted: AP1

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

Formatted: Bullets and Numbering

5.3.5 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 4 - RADIUS Access-Accept Attributes

Attribute Number	Attribute Name	Value
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

Deleted: Attribute
Formatted: Left
Formatted: Left
Formatted: Left
Formatted: Left
Formatted: Left
Formatted: Left

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

The New-BSSID-Security-Block VSA carries the security information needed by the new AP to decrypt and encrypt ESP packets. The New-BSSID-Security-Block is defined in 5.3.7.2.

Deleted: data field of new AP security block
Deleted: The format of the data field for this packet is shown in 7.

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

5.3.6 RADIUS Access-Reject

As described in 5.3.5, 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.

5.3.7 IAPP RADIUS vendor-specific attributes

Table 5 contains a list of the RADIUS Vendor-Specific Attributes (VSAs) used by the IAPP. The IEEE 802.11 vendor code is TBD[4].

Per RFC 2865, RADIUS Vendor-Specific Attributes should have the following form:

RADIUS Attribute Type (26)	Attribute Length	Vendor-ID (TBD[5])	Vendor Type	Vendor Length	Attribute Data
Octets: 1	1	4	1	1	n

Figure 4 - RADIUS Vendor-Specific Attribute Format

Table 5 - IAPP RADIUS Vendor-Specific Attributes

Vendor Type	Attribute Name	Description
1	IAPP-Liveliness-Nonce	A 32-byte nonce used to ensure liveliness of the secure IAPP traffic. This attribute should not be included if secure IAPP communications are not required by the AP.
2	New-BSSID-Security-Block	Security Block encrypted using new BSSID's user-password, to be decrypted and used by the new BSSID
3	Old-BSSID-Security-Block	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
4	SSID	The ASCII text SSID which denotes the ESS in which the AP is registering its BSSID
5	Supported-ESP-Authentication-Algorithms	The list of ISAKMP ESP Authentication IDs corresponding to the ESP Authentication algorithms supported by this AP (see Table 8)
6	Supported-ESP-Transforms	The list of ISAKMP ESP Transform IDs corresponding to the ESP transforms supported by this AP (See Table 7)
7	ESS-New-ESP-Transform-Key	The ESP Transform key used to encrypt ADD-Notify packets when sending
8	ESS-New-ESP-Authentication-Key	The ESP Authentication key used to authenticate ADD-Notify packets when sending
9	ESS-Old-ESP-Transform-Key	The ESP Transform key that can be used to decrypt ADD-Notify packets when receiving, if the New-ESP-Transform-Key does not work
10	ESS-Old-ESP-Authentication-Key	The ESP Authentication key that can be used to authenticate ADD-Notify packets when receiving, if the New-ESP-Authentication-Key does not work

[4] Vendor code has been requested from IANA and will be entered upon receipt.
[5] Vendor code has been requested from IANA and will be entered upon receipt.

Deleted: ¶
Length of Security Block [9]
Formatted: Bullets and Numbering
Field CodeChanged
Formatted: Font: 10 pt
Formatted: Heading3
Formatted: Caption

11	ESS-ESP-Transform-ID	ESP Transform ID of the algorithm to use when encrypting/decrypting ADD-Notify packets
12	ESS-ESP-Authentication-ID	ESP Authentication ID of the algorithm to use when encrypting/decrypting ADD-Notify packets
13	ESS-ESP-SPI	SPI used to identify ESP group SA.
14	New-BSSID-Security-Block-IV	A 4-byte nonce used as the initialization vector to encrypt and decrypt the New-BSSID-Security-Block attribute

Formatted: Bullets and Numbering

5.3.7.1 IAPP-Liveliness-Nonce

The IAPP-Liveliness-Nonce VSA is a 32-byte nonce used to ensure liveliness of the secure IAPP traffic. This attribute should not be included if secure IAPP communications are not required by the AP.

Formatted: Bullets and Numbering

5.3.7.2 New-BSSID-Security-Block

The New-BSSID-Security-Block is a Security Block encrypted using new BSSID's user-password, to be decrypted and used by the new BSSID. It is a variable length attribute that contains the security information from the RADIUS Server for the new AP. The content of the Security Block should be interpreted by the new AP, and should not be passed on to other APs.

The Security Block is a series of information elements. This block is encrypted with the new AP's RADIUS BSSID Secret, using the ESP Transform algorithm given to it in the ESS-ESP-Transform-ID attribute of the RADIUS Registration Access-Accept packet. The new AP authenticates this Security Block using the ESS-ESP-Authentication-ID algorithm, and decrypts it using the ESS-ESP-Transform-ID cipher (with New-BSSID-Security-Block-IV as IV) and its RADIUS BSSID Secret as the decryption key. The transform and authentication keys are derived from the RADIUS BSSID Secret by first expanding the secret by: SHA1(secret)||SHA1(secret||1st SHA1)||…. The transform key is the first N bits and the authentication key is the next M bits (the values of N and M are dependent on the cipher suite). The new AP creates the SAs from the information in the Security Block and if it caches these SAs, uses the lifetime to remove the SAs from its cache. 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.

Table 6 - Information Elements in the New-BSSID-Security-Block

Element ID	Length	Information
2	8	Security lifetime in seconds
3	32	ACK nonce
4	1	ESP transform number
5	1	ESP authentication number
6	4	SPI used to identify ESP SA to the old AP
7	Variable	key used by ESP Transform for ESP packets to the old AP
8	Variable	key used by ESP Authentication for ESP packets to the old AP
9	4	SPI used to identify ESP SA from the old AP
10	Variable	key used by ESP Transform for ESP packets from the old AP
11	Variable	key used by ESP Authentication for ESP packets from the old AP

Formatted: Bullets and Numbering

5.3.7.3 Old-BSSID-Security-Block

The Old-BSSID-Security-Block is a Security Block encrypted using old BSSID's user-password, to be decrypted and used by the old AP. It is a variable length attribute that contains the security information from the RADIUS Server for the old AP. The content of the Security Block should not be interpreted by the new AP, but should not be passed on to the old AP. The contents of the Old-BSSID-Security-Block attribute are defined in 6.6.

5.3.7.4 SSID

Formatted: Bullets and Numbering

The SSID VSA is the ASCII text string SSID which denotes the ESS in which the AP is registering its BSSID. Since RADIUS VSAs have a separate length value, the SSID is not null-terminated.

Formatted: Bullets and Numbering

5.3.7.5 Supported-ESP-Authentication-Algorithms

The Supported-ESP-Authentication-Algorithms VSA is a list of consecutive one-byte values that are ISAKMP ESP Authentication IDs corresponding to the ESP Authentication algorithms supported by this AP (see Table 11 for values).

Formatted: Bullets and Numbering

5.3.7.6 Supported-ESP-Transforms

The Supported-ESP-Transforms VSA is a list of consecutive one-byte values that are ISAKMP ESP Transform IDs corresponding to the ESP Transformation algorithms supported by this AP (see Table 10 for values).

Formatted: Bullets and Numbering

5.3.7.7 ESS-New-ESP-Transform-Key

The ESS-New-ESP-Transform-Key VSA contains the ESP Transform key used to encrypt and decrypt ADD-Notify packets transmitted and received by this AP. If a received ADD-Notify packet does not correctly decrypt using the ESS-New-ESP-Transform-Key, the ESS-Old-ESP-Transform-Key should be used to decrypt the ADD-Notify packet.

The contents of this VSA are encrypted as described for the MS-MPPE-Send-Key attribute in RFC 2548.

Formatted: Bullets and Numbering

5.3.7.8 ESS-New-ESP-Authentication-Key

The ESS-New-ESP-Authentication-Key VSA contains the ESP Authentication key used to authenticate ADD-Notify packets transmitted and received by this AP. If a received ADD-Notify packet does not pass authentication using the ESS-New-ESP-Authentication-Key, the ESS-Old-ESP-Authentication-Key should be used to authenticate the ADD-Notify packet.

The contents of this VSA are encrypted as described for the MS-MPPE-Send-Key attribute in RFC 2548.

Formatted: Bullets and Numbering

5.3.7.9 ESS-Old-ESP-Transform-Key

The ESS-Old-ESP-Transform-Key VSA contains the ESP Transform key used only to decrypt ADD-Notify packets received by this AP if the received ADD-Notify packet does not correctly decrypt using the ESS-New-ESP-Transform-Key. This key should never be used to encrypt ADD-Notify packets sent from this AP.

The contents of this VSA are encrypted as described for the MS-MPPE-Send-Key attribute in RFC 2548.

Formatted: Bullets and Numbering

5.3.7.10 ESS-Old-ESP-Authentication-Key

The ESS-Old-ESP-Authentication-Key VSA contains the ESP Authentication key used only to authenticate ADD-Notify packets received by this AP if the received ADD-Notify packet does not pass authentication using the ESS-New-ESP-Authentication-Key. This key should never be used to authenticate ADD-Notify packets sent from this AP.

The contents of this VSA are encrypted as described for the MS-MPPE-Send-Key attribute in RFC 2548.

Formatted: Bullets and Numbering

5.3.7.11 ESS-ESP-Transform-ID

The ESS-ESP-Transform-ID VSA is a one-byte attribute that denotes the ESP Transform algorithm chosen by the RADIUS server for encrypting and decrypting the ADD-Notify packets, using values selected from Table 10. The selected transform algorithm is also used to encrypt and decrypt the New-BSSID-Security-Block and Old-BSSID-Security-Block attributes sent in the RADIUS packets.

5.3.7.12 ESS-ESP-Authentication-ID

The ESS-ESP-Authentication-ID VSA is a one-byte attribute that denotes the ESP Authentication algorithm chosen by the RADIUS server for authenticating the ADD-Notify packets, using values selected from Table 11. The selected authentication algorithm is also used to authenticate the New-BSSID-Security-Block and Old-BSSID-Security-Block attributes sent in the RADIUS packets.

5.3.7.13 ESS-ESP-SPI

The ESS-ESP-SPI VSA is a 4-byte attribute that is the Security Parameter Index which is used by all members of the ESS to lookup the correct group SA for the ADD-Notify packet protection.

5.3.7.14 New-BSSID-Security-Block-IV

The New-BSSID-Security-Block-IV VSA is an 8-byte nonce used as the initialization vector to encrypt and decrypt the New-BSSID-Security-Block attribute.

5.4 Support for 802.11 context transfer

There are no requirements from the existing mechanisms of IEEE 802.11-1999 for the IAPP to carry context information between APs. However, should such mechanisms be defined that establish a requirement for the IAPP to carry context information between APs, that information will be carried in the Context Block of 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.

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

The new AP sends the old-BSSID-Security-Block to the old AP in the IAPP Send-Security-Block packet. The old AP authenticates and decrypts this Security Block using the configured cipher (with Date/Time as IV), HMAC-MD5, and its RADIUS BSSID Secret. The cipher and HMAC keys are derived from the RADIUS BSSID Secret by first expanding the secret by: SHA1(secret)||SHA1(secret||1st SHA1)||…. The cipher key is the first N bits and the authentication key is the next M bits (the values of N and M are dependant on the cipher suite). The new AP creates the SAs from the information in the Security Block and if it caches these SAs, uses 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 the date/time stamp received against the date/time stamp used to create the old SAs. If the stamp just received is greater, it removes the old SAs, and uses the new. If the stamps are the same, all

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

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

Formatted: Bullets and Numbering

Deleted: authentication

Deleted: authentication

Deleted: authentication

Deleted: other authentication

Deleted: authentication

Deleted: an

Deleted: 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.

Deleted: password

Deleted: password

Deleted: password

Deleted: w

Inserted: wy

Deleted: password

Deleted: secret

the rest of the Security Block content is the same and can be dropped. If the stamp just received is less, this is an invalid reply and should be ignored.

Deleted: MUST

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

5.5.2 Station Add Process

The interaction between APs in an ESS as a result of an AP receiving an 802.11 association request frame comprises the transmission by the AP at which the association occurs of an IAPP ADD-notify packet and the transmission of a Layer 2 Update frame. The IAPP ADD-notify packet is sent to the IAPP IP multicast address. The Layer 2 Update frame is sent to the MAC broadcast address and uses the MAC address of the STA that has associated as the MAC source address for the frame. See clause 6.2 for further information on the IAPP ADD-notify packet and clause 6.3 for further information on the Layer 2 Update frame.

Deleted: when a STA is added to the STAs associated with an AP

Deleted: subnet limited broadcast

The purpose of transmitting the IAPP ADD-notify packet is to provide an indication to an AP that may have held an older association of a STA that has more recently associated with another AP that the AP holding that older association may discard any context for that STA. This should allow for more efficient management of AP resources. 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.

There is no security provided for the Layer 2 Update frame. If security is needed for the IAPP ADD-notify packet, it is wrapped in ESP. The Layer 2 Update frame does not open new potentials for attacks against the WLAN or the STAs. However, the ADD-notify is a UDP IP frame that COULD be sent from anywhere in the DS and attack the AP's state for the STA.

The SPI and keys for the Security Association (SA) for ESP are created by the RADIUS Server and sent to the AP as the RADIUS Attributes. The AP creates the SA from the information in the RADIUS response, caches the SA, and uses the registration session timeout to remove the SA from its cache.

At any time, there could be two broadcast SPIs for the ESS, as lifetime expires on each AP and the AP performs a new RADIUS Registration Access-Request/Access-Accept interaction. ADD-Notify packets are always sent with the newest SA, but the old SA might be needed to decrypt a received ADD-Notify.

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

5.6 AP specific MIB

An SNMP MIB using SMIv2 for the IAPP is defined in Annex A. The MIB contains attributes for the IAPP that are useful in monitoring and diagnosis of the operation of the IAPP.

Formatted: Bullets and Numbering

5.7 Single station association

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

Deleted: Station

Deleted: station

Deleted: station

Deleted: reassociate

Deleted: station

context for the STA, and the new AP to add the STA and context to its own table. Thus, the use of the reassociation request frame by the STA allows the APs to ensure that there is only a single association for the STA.

When a roaming STA associates with an AP, rather than reassociates, the AP attempts to enforce the single STA association requirement by sending an IAPP ADD-notify packet and the Layer 2 Update frame to the DS. Because this packet is addressed to the subnet-local broadcast address (see 6.2), this packet may not reach all APs in an ESS. In particular, if the ESS spans multiple subnets, neither the ADD-notify packet nor the Layer 2 Update frame is likely to reach the APs on subnets other than the one on which the transmissions originate. If the old AP receives the IAPP ADD-notify packet, it should remove any context stored for the STA.

Deleted: station
Deleted: station
Deleted: mobile station
Deleted: station
Deleted: station
Deleted: or when the AP holding the roaming station's previous association cannot be found using RADIUS,
Deleted: station
Deleted: station

6 Packet Formats

6.1 General IAPP Packet Format

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. The port number assigned to IAPP is TBD[6].

Formatted Table

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

Figure 5 - General IAPP Packet Format

6.1.1 IAPP Version Field

The IAPP Version Field indicates the protocol version of the IAPP, and thus the organization of the rest of the packet. The value of the Version field for this protocol is zero. All other values are reserved. A device that receives a packet with an IAPP Version level that it does not support should silently discard the packet.

Deleted: higher revision
Deleted: than
Deleted: s
Deleted: will

6.1.2 Command Field

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

Table 7 - Command field values

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

[6] Port numbers have been applied for. As soon as it is received, the "TBD" will be replaced with the actual value(s).

6.1.3 Identifier Field

The two-octet Identifier field aids in matching requests and responses. When sending an IAPP request packet, the value of the Identifier field should be unique, with respect to other outstanding packets. When sending an IAPP response packet the value of the Identifier field will be a copy the value of the Identifier field from the received request packet. The Identifier field can be used to help detect duplicate requests and responses. Duplicate requests and responses should be silently discarded.

6.1.4 Length Field

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

6.1.5 Data Field

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

6.2 ADD-notify Packet

The ADD-notify packet is sent, using the IAPP over UDP and IP, on the local LAN segment to notify any AP that receives it that the STA identified in the packet has associated at the AP sending the packet. The packet is sent to the IAPP IP multicast address (see RFC 1112), so that it will reach every device on the DSM local subnet, even if the LAN is switched.

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

Address Length	Reserved	MAC Address	Sequence Number
Octets: 1	1	n = Address Length	2

Figure 6 - ADD-notify Data Field Format

The Address Length is an 8-bit integer that indicates the number of octets in the MAC Address. This field allows the extension of the IAPP to IEEE 64-bit MAC addresses, when those become generally deployed. 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 the Reserved field is one octet, in order to align the MAC Address field on a 16-bit boundary. The MAC Address is the MAC address of the STA that has associated. The length of the MAC Address field is equal to the value of the Address Length field. The Sequence Number field contains the integer value of the sequence number of the association request frame received by the AP from the STA that has associated. Allowable values for the Sequence number are between 0 and 4095.

6.3 Layer 2 Update Frame

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

Deleted: Any
Deleted: that is sent in response to the receipt of another IAPP packet will
Deleted: into the Identifier field of the packet sent in response
Deleted: A duplicate request can be detected if it has the same source IP address and port and Identifier within a short span of time.
Deleted: MUST
Deleted: MUST
Deleted: mobile station
Deleted: subnet limited broadcast
Deleted: 18
Deleted: mobile station
Deleted: station
Deleted: station
Deleted: mobile
Deleted: station
Deleted: mobile
Deleted: station

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 STA 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.

Deleted: mobile
Deleted: station

6.4 MOVE-notify Packet

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

Deleted: and
Deleted: mobile
Deleted: station

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

Deleted: mobile
Deleted: station

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 STA that has requested reassociation. The Sequence Number field contains the integer value of the sequence number of the reassociation request frame received by the AP from the STA that has requested reassociation. 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 STA indicated by the MAC Address. The content of the Context Block should not be interpreted by the IAPP.

Deleted: station
Deleted: ed
Deleted: station
Deleted: ed
Deleted: station

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 STA. 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.

Deleted: mobile
Deleted: station
Deleted: **Error! Reference source not found.**

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

Deleted: , the
Deleted: of which

Element Identifier	Length	Information
Octets: 2	2	n = Length

Figure 9 - Information Element Format

6.5 MOVE-response Packet

The MOVE-response packet is sent using the IAPP, over TCP and IP. This packet is sent directly to the AP from which the MOVE-notify packet was received. 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-response packet carries the MAC address of the reassociated STA and the context information pertaining to that STA. 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

Figure 10 - MOVE-response Data Field Format

The Address Length is an 8-bit integer that indicates the number of octets in the MAC Address. The Status field is an 8-bit integer that indicates the status resulting from the receipt of the MOVE-notify packet. The allowable values for the Status field are shown in . The values for the Status field are derived from the Status parameter of the IAPP-MOVE.response service primitive. The MAC Address is the MAC address of the STA that has reassociated. The Sequence Number field contains the integer value of the sequence number from the MOVE-notify packet that caused the generation of this packet. 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 STA indicated by the MAC Address. The content of the Context Block should not be interpreted by the IAPP.

Table 8 - MOVE-notify Status Values

Status Value	Definition
0	Successful
1	Move denied
2	Stale move
3-255	Reserved

6.6 Send-Security-Block packet

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

Deleted: station
Deleted: station
Deleted: Error! Reference source not found.
Deleted: station
Deleted: station
Deleted: 1
Deleted: 2
Deleted: Table 5 - MOVE-notify Status Values¶
Formatted: Bullets and Numbering
Deleted: mobile
Deleted: station
Deleted:

Initialization Vector	Length of Security Block	Security Block
Octets: 8	2	m = Length of Security Block

Figure 11 - Send-Security-Block Data Field Format

The Initialization Vector is the first 8 bytes of the ACK nonce. 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 new AP to the old 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 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 Authentication Block is a 16 byte field that contains the result of an HMAC-MD5 hash of the Security Block. 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.

Table 9 - Information Elements in the Send-Security-Block Packet

Element ID	Length	Information
12	6 or 8	Old BSSID
1	8	Date/Time stamp
15	6 or 8	New BSSID
16	4 or 16	New BSSID IP address
2	8	Security lifetime in seconds
13	56	New-AP-ACK-Authenticator
4	1	ESP transform identifier
5	1	ESP authentication identifier
6	4	SPI used to identify ESP SA from new AP
7	Variable	key used by ESP Transform for ESP packets from the new AP
8	Variable	key used by ESP Authentication for ESP packets from the new AP
9	4	SPI used to identify ESP SA to the new AP
10	Variable	key used by ESP Transform for ESP packets to the new AP
11	Variable	key used by ESP Authentication for ESP packets to the new AP
14	16	HMAC authentication block

The ESP Transform and Authentication algorithms are defined by IANA at http://www.iana.org/assignments/isakmp-registry. The recommended minimum set of transforms is ESP_DES, as defined in RFC 2407. The recommended minimum set of authentication algorithms is HMAC_MD5 and HMAC_SHA. The values of the identifiers as of the last update of 2001 September 6 are shown in Table 10 and Table 11.

Formatted Table

Formatted: Left

Deleted: 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.

Deleted: The Authentication Block is a 16 byte field that contains the result of an HMAC-MD5 hash of the Security Block.

Deleted: Error! Reference source not found.

Deleted: 48

Deleted: nonce

Deleted: number

Deleted: number

Deleted: Table 6 - Information Elements in the Send-Security-Block Packet¶

Deleted: :

Table 10 - ESP Transform Identifiers

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]
Reserved for private use	249-255	[RFC2407]

Table 11 - ESP Authentication Algorithm Identifiers

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]
RESERVED Reserved for private use	9-61439 61440-65535	

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 STA 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 format of the data field for this packet is shown in Figure 12.

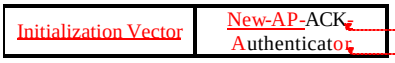


Figure 12 - ACK-Security-Block Data Field Format

The Initialization Vector is an 8-byte value copied from the Date/Time stamp. The New-AP-ACK-Authenticator field carries the content of the New-AP-ACK-Authenticator Information element that the old AP received in the Security Block. The content of the New-AP-ACK-Authenticator should be interpreted by the new AP. The New-AP-ACK-Authenticator

Deleted: Table 7 - ESP Transform Identifiers¶
The values 249-255 are reserved for private use amongst cooperating systems.¶

Deleted: Table 8 - ESP Authentication Algorithm Identifiers¶
Values 5-61439 are reserved to IANA. Values 61440-65535 are for private use.¶

Formatted: Bullets and Numbering

Deleted: mobile

Deleted: station

Deleted: ¶
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.

Deleted: a

Deleted: ion

Deleted: 32

Deleted: Send

Deleted: 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.

Deleted: The ACK authentication is a 32 byte field that contains an encrypted nonce that the new AP received from the RADIUS Server. The Authentication Block is a 16 byte field that contains the result of an HMAC-MD5 hash of the ACK authentication.

Deleted: ACK authentication

Deleted: IAPP

is encrypted with the new AP's RADIUS BSSID Secret, using the AP's configured cipher. The new AP has to authenticate and decrypt it first before processing it. This New-AP-ACK-Authenticator protects the new AP from spoofed ACK-Security-Block packets.

6.8 Information Element Definitions

The information elements defined in this recommended practice are listed in Table 12.

Table 12 - IAPP Information Elements

IAPP Element ID	Description
1	Date/Time stamp
2	Security lifetime
3	ACK nonce (32-byte)
4	ESP transform number
5	ESP authentication number
6	SPI from new AP
7	ESP transform key from new AP
8	ESP authentication key from new AP
9	SPI to new AP
10	ESP transform key to new AP
11	ESP authentication key to new AP
12	Old BSSID
13	New-AP-ACK-Authenticator (48-byte)
14	HMAC authentication block
15	New BSSID
16	New BSSID IP address
17 – 65,534	Reserved for future standardization
65,535	Proprietary Information. This information element must include the 3-byte Organizational Unique Identifier (OUI) from the organization's MAC address allocation as the first three bytes of the information field.

6.8.1 Date/Time stamp

The Date/Time stamp information element contains date and time information in RFC 1305 format. This information element is 8 octets in length.

6.8.2 Security lifetime

The Security lifetime information element contains a value indicating the seconds for the life of the SA. This value is used to compute the local time at which the SA is no longer valid for sending IAPP packets, and may be deleted. Common practice is to keep old SAs available for some limited time to receive packets from other APs.

6.8.3 ACK nonce (32-byte)

The ACK nonce information element is a 32 byte random value created by the RADIUS server, used by the new AP to establish liveness of the old AP. This information element is 4 octets in length.

6.8.4 ESP transform number

The ESP transform number information element is an 8-bit value that identifies the cryptographic algorithm used with ESP. This information element is 1 octet in length.

Deleted: ACK authentication

Deleted: ¶
There is only one element. This is the 256 bit nonce the new AP sent to the RADIUS Server in the RADIUS-Access-Request message.

Deleted: nonce

Formatted: Bullets and Numbering

Formatted: Keep with next

Formatted Table

Formatted: Heading3

Formatted: Normal

Formatted: Heading3

Formatted: Normal

Formatted: Heading3

Formatted: Normal

Formatted: Heading3

Formatted: Normal

6.8.5 ESP authentication number

The ESP authentication number information element is an 8-bit value that identifies the authentication algorithm used with ESP. This information element is 1 octet in length.

6.8.6 SPI from new AP

The SPI from new AP information element is an Index into the SA for IAPP MOVE packets going from the new AP to the old AP. Initially this is a Request, but if this information is cached, it could later be a Response. This information element is 4 octets in length.

6.8.7 ESP transform key from new AP

The ESP transform key from new AP information element is a variable length value that is used by the cryptographic algorithmidentified by the ESP transform number to encrypt information from the new AP to the old AP.

6.8.8 ESP authentication key from new AP

The ESP authentication key from new AP information element is a variable length value that is used by the authentication algorithm identified by the ESP authentication number to authenticate information from the new AP to the old AP.

6.8.9 SPI to new AP

The SPI to new AP information element is an Index into the SA for IAPP MOVE packets going to the new AP from the old AP. Initially this is a Response, but if this information is cached, it could later be a Request. This information element is 4 octets in length.

6.8.10 ESP transform key to new AP

The ESP transform key from new AP information element is a variable length value that is used by the cryptographic algorithm identified by the ESP transform number to encrypt information to the new AP from the old AP.

6.8.11 ESP authentication key to new AP

The ESP authentication key from new AP information element is a variable length value that is used by the authentication algorithm identified by the ESP authentication number to authenticate information to the new AP from the old AP.

6.8.12 Old BSSID

The Old BSSID information element contains the value of the BSSID for the old AP. This information element is variable length, either 6 or 8 octets.

6.8.13 New-AP-ACK-Authenticator (48-byte)

The New-AP-ACK-Authenticator information element contains a date/time stamp, an ACK nonce and an HMAC authentication block.

Table 13 - Content of the New-AP-ACK-Authenticator

Length	Information
8	Date/Time stamp
32	ACK nonce
16	HMAC authentication block

Formatted: Heading3
Formatted: Normal
Formatted: Heading3
Formatted: Normal
Formatted: Heading3
Formatted: Normal
Formatted: Heading3
Formatted: Normal
Formatted: Heading3
Formatted: Normal
Formatted: Heading3
Formatted: Normal
Formatted: Heading3
Formatted: Normal
Formatted: Normal

6.8.14 HMAC authentication block

The HMAC authentication block information element is a value created by performing an HMAC-MD5 operation over other designated fields. The usage of this information element is described in the definition of the particular packets that are authenticated. This information element is 16 octets in length.

6.8.15 New BSSID

The New BSSID information element contains the value of the BSSID for the new AP. This information element is variable length, either 6 or 8 octets.

6.8.16 New BSSID IP address

The New BSSID IP address information element contains the IP address of the new AP. This information element is variable length, either 4 or 8 octets.

Formatted: Heading3
Formatted: Normal
Formatted: Heading3
Formatted: Heading3
Formatted: Normal

Annex A, Management Information Base

(Normative)

```
-- ************************************************************************
-- * IEEE 802.11f Inter-AP Protocol Management Information Base
-- ************************************************************************

IEEE802dot11f-MIB DEFINITIONS ::= BEGIN
    IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE,
        NOTIFICATION-TYPE,Integer32, Counter32  FROM SNMPv2-SMI

        DisplayString , MacAddress, RowStatus,
        TruthValue                              FROM SNMPv2-TC

        MODULE-COMPLIANCE, OBJECT-GROUP,
        NOTIFICATION-GROUP                      FROM SNMPv2-CONF

        ifIndex                                 FROM RFC1213-MIB;

-- ************************************************************************
-- *  MODULE IDENTITY
-- ************************************************************************

    ieee802dot11f MODULE-IDENTITY
    LAST-UPDATED "0107020000Z"
    ORGANIZATION "IEEE 802.11"
    CONTACT-INFO
           "WG E-mail: stds-802-11@ieee.org

                Chair: Stuart J. Kerry
               Postal: Philips Semiconductors, Inc.
                       1109 McKay Drive
                       M/S 48A SJ
                       San Jose, CA 95130-1706  USA
                  Tel: +1 408 474 7356
                  Fax: +1 408 474 7247
               E-mail: stuart.kerry@philips.com

               Editor: Bob O'Hara
               Postal: Informed Technology, Inc.
                       1750 Nantucket Circle, Suite 138
                       Santa Clara, CA 95054 USA
                  Tel: +1 408 986 9596
                  Fax: +1 408 727 2654
               E-mail: bob@informed-technology.com"

    DESCRIPTION
        "The MIB module for IEEE 802.11f IAPP entities.
        iso(1).member-body(2).us(840).ieee802dot11(10036).iapp(6)"
    ::= { 1 2 840 10036 6 }

-- ************************************************************************
```

Formatted: French (France)

Formatted: French (France)

```
-- *  Major sections
-- ************************************************************************
--  IAPP diagnostic attributes
    --  DEFINED AS “The iappdiagnostics object class provides the necessary
    --  support at an 802.11 AP to manage and diagnose the IAPP processes
    --  and protocol in the AP such that the AP may work cooperatively as
    --  a part of an IEEE 802.11 network.”;

iappdiagnostics OBJECT IDENTIFIER ::= {ieee802dot11f 1}

iappAPTable OBJECT-TYPE
      SYNTAX     SEQUENCE OF IappAPTableEntry
      MAX-ACCESS not-accessible
      STATUS     current
      DESCRIPTION
            "The (conceptual) table listing the other APs with
             which the AP has communicated via IAPP."
      ::= { iappdiagnostics 1 }

IappAPTableEntry OBJECT-TYPE
      SYNTAX     iappDiagnosticTableEntry
      MAX-ACCESS not-accessible
      STATUS     current
      DESCRIPTION
            "An entry (conceptual row) representing another AP
             with which the AP has communicated via IAPP."
      INDEX      { iappDiagnosticTableIndex }
      ::= { iappDiagnosticTable 1 }

iappAPTableEntry ::= SEQUENCE {
      iappAPTableIndex                          Integer32,
      iappAPIPAddress                           IpAddress,
      iappAPMACAddress                          MacAddress,
      iappClientServerPortNumber                Integer32,
      iappAPRoundTripTime                       TimeTicks,
      iappAPRTO                                 TimeTicks,
      iappMoveNotifySent                        Counter32,
      iappMoveNotifyRetransmissions             Counter32,
      iappMoveNotifyReceived                    Counter32,
      iappMoveResponseSent                      Counter32,
      iappMoveResponseReceived                  Counter32,
      iappMoveNotifyMalformed                   Counter32,
      iappMoveNotifyUnAuthentic                 Counter32,
      iappMoveResponseMalformed                 Counter32,
      iappMoveResponseUnAuthentic               Counter32,
      iappMoveNotifyBadService                  Counter32,
      iappMoveResponseBadService                Counter32,
      iappMoveNotifyPendingRequests             Gauge32,
      iappMoveResponsePendingResponses          Gauge32,
      iappMoveNotifyTimeouts                    Counter32,
      iappUnknownType                           Counter32,
      iappMoveNotifyPacketsDropped              Counter32,
      iappMoveResponsePacketsDropped            Counter32
}

iappAPTableIndex OBJECT-TYPE
      SYNTAX     Integer32 (1..2147483647)
```

Deleted: iappAPTableEntry

Deleted: iappAPTableEntry

```
      MAX-ACCESS not-accessible
      STATUS     current
      DESCRIPTION
             "A number uniquely identifying each other AP
             with which this AP has communicated via IAPP."
      ::= { iappAPTableEntry 1 }

iappAPIPAddress OBJECT-TYPE
      SYNTAX     IpAddress
      MAX-ACCESS read-only
      STATUS     current
      DESCRIPTION
            "The IP address of the AP
             referred to in this table entry."
      ::= { iappAPTableEntry 2 }

iappAPMACAddress OBJECT-TYPE
      SYNTAX     MacAddress
      MAX-ACCESS read-only
      STATUS     current
      DESCRIPTION
           "The MAC address of the AP
            referred to in this table entry."
      ::= { iappAPTableEntry 3 }


iappClientServerPortNumber  OBJECT-TYPE
      SYNTAX Integer32 (0..65535)
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
           "The UDP port the AP is using to send
            to the other AP"
      ::= { iappAPTableEntry 4 }

iappAPRoundTripTime  OBJECT-TYPE
      SYNTAX TimeTicks
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
            "The time interval (in hundredths of a second) between
             the most recent Move-Notify sent by this AP and the
             Move-Response that matched it from the other AP."
      ::= { iappAPTableEntry 5 }

iappAPRTO  OBJECT-TYPE
      SYNTAX TimeTicks
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
            "The Round Trip Timeout (RTO) (in hundredths of a second)
             between this AP and the other AP."
      ::= { iappAPTableEntry 6 }

-- Request/Response statistics
--
```

```
--   TotalIncomingPackets   =   MoveNotifyReceived   +   MoveResponseReceived   +
UnknownTypes
--
-- TotalIncomingPackets - Malformed - Unauthentic -
-- UnknownTypes - PacketsDropped = Successfully received
--

iappMoveNotifySent OBJECT-TYPE
      SYNTAX Counter32
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
            "The number of Move-Notify packets sent to this AP.
             This does not include retransmissions."
      ::= { iappAPTableEntry 7 }

iappMoveNotifyRetransmissions OBJECT-TYPE
      SYNTAX Counter32
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
            "The number of Move-Notify packets
             retransmitted to this AP."
      ::= { iappAPTableEntry 8 }

iappMoveNotifyReceived OBJECT-TYPE
      SYNTAX Counter32
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
            "The number of Move-Notify packets
             (valid or invalid) received from this AP."
      ::= { iappAPTableEntry 9 }

iappMoveResponseSent OBJECT-TYPE
      SYNTAX Counter32
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
            "The number of Move-Response packets sent to this AP."
      ::= { iappAPTableEntry  10 }

iappMoveResponseReceived OBJECT-TYPE
      SYNTAX Counter32
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
            "The number of Move-Response packets
             (valid or invalid) received from this AP."
      ::= { iappAPTableEntry 11 }

iappMoveNotifyMalformed OBJECT-TYPE
      SYNTAX Counter32
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
            "The number of malformed Move-Notify
```

```
              packets received from this AP.
              Malformed packets include packets with
              an invalid length. Unauthenticated packets
              or unknown types are not
              included as malformed packets."
       ::= { iappAPTableEntry 12 }

iappMoveNotifyUnAuthentic OBJECT-TYPE
       SYNTAX Counter32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
             "The number of Move-Notify packets
              failing authentication, received from this AP."
       ::= { iappAPTableEntry 13 }

iappMoveResponseMalformed OBJECT-TYPE
       SYNTAX Counter32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
             "The number of malformed Move-Response
              packets received from this AP.
              Malformed packets include packets with
              an invalid length. Unauthenticated packets
              or unknown types are not
              included as malformed packets."
       ::= { iappAPTableEntry 14 }

iappMoveResponseUnAuthentic OBJECT-TYPE
       SYNTAX Counter32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
             "The number of Move-Response packets
              failing authentication, received from this AP."
       ::= { iappAPTableEntry 15 }

iappMoveNotifyBadService OBJECT-TYPE
       SYNTAX Counter32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
             "The number of Move-Notify packets
              received from this AP which could not be acted
              upon, due to inclusion of an unavailable service.
              Malformed or unauthentic packets are not included
              in this count."
       ::= { iappAPTableEntry 16 }

iappMoveResponseBadService OBJECT-TYPE
       SYNTAX Counter32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
             "The number of Move-Response packets
              received from this AP which could not be acted
```

```
              upon, due to requesting an unavailable service.
              Malformed or unauthentic packets are not included
              in this count."
       ::= { iappAPTableEntry 17 }

iappMoveNotifyPendingRequests OBJECT-TYPE
      SYNTAX Gauge32
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
            "The number of Move-Notify packets
             destined for this AP that have not yet timed out
             or received a response. This variable is incremented
             when a Move-Notify is sent and decremented due to
             receipt of a Move-Response, a timeout or retransmission."
      ::= { iappAPTableEntry 18 }

iappMoveNotifyTimeouts OBJECT-TYPE
     SYNTAX Counter32
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION
            "The number of Move-Notify timeouts to this AP.
             After a timeout the AP may retry or
             give up. A retry is counted as a
             retransmit as well as a timeout."
      ::= { iappAPTableEntry 19 }

iappUnknownType OBJECT-TYPE
      SYNTAX Counter32
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
            "The number of IAPP packets of unknown type which
             were received from this AP."
      ::= { iappAPTableEntry 20 }


iappMoveNotifyPacketsDropped OBJECT-TYPE
      SYNTAX Counter32
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
            "The number of Move-Notify packets received from
             this AP and dropped for some other reason.
              Malformed or unauthentic packets, or those
             requesting an unavailable service are not included
             in this count."
      ::= { iappAPTableEntry  21 }

iappMoveResponsePacketsDropped OBJECT-TYPE
      SYNTAX Counter32
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
            "The number of Move-Response packets received from
             this AP and dropped for some other reason, such
```

```
                as arriving after the Timeout window has expired.
                Malformed or unauthentic packets, or those
                requesting an unavailable service are not included
                in this count."
        ::= { iappAPTableEntry  22 }


-- ****************************************************************
-- *   End of IAPP MIB
-- ****************************************************************
END
```

2

Deleted: Annex B, Context Transfer¶
(Informative)¶
The text in this annex has been excerpted from IETF RFC 3162.¶
B.1 Introduction¶
IEEE 802.1X [13] enables authenticated access to IEEE 802 media, including Ethernet, Token Ring, and 802.11 wireless LANs. Although Authentication, Authorization and Accounting (AAA) support is optional within IEEE 802.1X, it is expected that many IEEE 802.1X Authenticators will function as AAA clients. Behavior of IEEE 802.1X Authenticators acting as RADIUS clients is described in [24]. ¶
The IEEE 802 Inter-Access Point Protocol (IAPP), under development within the IEEE 802.11 TGf working group, supports the transfer of context between access points implementing IEEE 802 technology. This annex describes how IAPP can be used to support transfer of authentication, authorization and accounting (AAA) context between devices supporting IEEE 802.1X network port authentication [13].¶
In terms of organization, this document first develops a general model for AAA context transfer. Central to the model is the notion of a "correct" context transfer -- a transfer resulting in the same context on the new access point as would have resulted had a AAA conversation been completed.¶
The circumstances in which "correct" context transfer can be achieved are analyzed -- demonstrating that this can only be achieved in a limited set of circumstances. As a result, it is suggested that context transfer protocols restrict the domain of applicability to scenarios involving a high degree of homogeneity.¶
For example, layer 2 context transfer solutions are most likely to be successful transferring context within media families, such as IE... [10]

Formatted: annex

Page 17: [1] Deleted **Bob O'Hara** **4/13/2002 5:31 PM**

802.11

Page 17: [1] Deleted **Bob O'Hara** **4/13/2002 5:27 PM**

station

Page 17: [1] Deleted **Bob O'Hara** **4/13/2002 5:27 PM**

mobile station

Page 17: [1] Deleted **Bob O'Hara** **3/14/2002 10:40 AM**

IAPP also removes the need for reauthentication with 802.1X when moving between access points, enabling seamless connectivity, and reducing the load on the backend authentication server.

Page 17: [2] Deleted **Bob O'Hara** **3/14/2002 11:04 AM**

associate request to an Access Point

Page 17: [2] Deleted **Bob O'Hara** **3/14/2002 11:05 AM**

a reassociate request

Page 17: [3] Deleted **Bob O'Hara** **3/14/2002 11:05 AM**

an AP

Page 17: [3] Deleted **Bob O'Hara** **3/14/2002 11:05 AM**

associate

Page 17: [3] Deleted **Bob O'Hara** **3/14/2002 10:55 AM**

-

Page 17: [3] Deleted **Bob O'Hara** **3/14/2002 10:56 AM**

P

Page 17: [3] Deleted **Bob O'Hara** **4/13/2002 4:29 PM**

Level

Page 17: [3] Deleted **Bob O'Hara** **3/14/2002 10:57 AM**

-

Page 17: [3] Deleted **Bob O'Hara** **4/23/2002 2:26 PM**

subnet broadcast

Page 17: [3] Deleted **Bob O'Hara** **3/14/2002 10:58 AM**

-

Page 17: [3] Deleted **Bob O'Hara** **3/14/2002 10:58 AM**

message

Page 17: [3] Deleted **Bob O'Hara** **3/14/2002 10:58 AM**

Page 17: [3] Deleted **Bob O'Hara** **3/14/2002 10:58 AM**

Page 17: [4] Deleted **Bob O'Hara** **3/14/2002 11:08 AM**

an AP

Page 17: [4] Deleted **Bob O'Hara** **3/14/2002 11:08 AM**

associate

Page 17: [4] Deleted **Bob O'Hara** **3/14/2002 11:08 AM**

n

Page 17: [4] Deleted **Bob O'Hara** **3/14/2002 11:08 AM**

ove

Page 17: [4] Deleted **Bob O'Hara** **3/14/2002 1:50 PM**

old-

Page 17: [4] Deleted **Bob O'Hara** **3/14/2002 11:09 AM**

ove

Page 17: [4] Deleted **Bob O'Hara** **3/14/2002 1:52 PM**

R

Page 17: [4] Deleted **Bob O'Hara** **3/14/2002 1:50 PM**

old-

Page 17: [4] Deleted **Bob O'Hara** **3/14/2002 11:09 AM**

ove

Page 17: [4] Deleted **Bob O'Hara** **3/14/2002 1:50 PM**

old-STA, allowing the new-STA to replicate the prior connection context without reauthenticating. This is commonly called a fast-handoff.

Page 17: [5] Deleted **Bob O'Hara** **3/14/2002 11:10 AM**

Move

Page 17: [5] Deleted **Bob O'Hara** **3/14/2002 11:10 AM**

Move

Page 17: [6] Deleted **Bob O'Hara** **3/14/2002 11:10 AM**

Move

Page 17: [6] Deleted **Bob O'Hara** **3/14/2002 1:52 PM**

R

Page 17: [6] Deleted **Bob O'Hara** **4/13/2002 4:36 PM**

s

Page 17: [7] Deleted **Bob O'Hara** **4/13/2002 4:36 PM**

s

Page 17: [7] Deleted **Bob O'Hara** **4/13/2002 4:36 PM**

b

Page 17: [7] Deleted **Bob O'Hara** **4/13/2002 4:32 PM**

Page 17: [7] Deleted	Bob O'Hara	4/13/2002 4:28 PM

associate request

Page 17: [8] Deleted	Bob O'Hara	4/13/2002 5:31 PM

802.11

Page 17: [8] Deleted	Bob O'Hara	4/13/2002 5:27 PM

mobile station

Page 17: [8] Deleted	Bob O'Hara	4/13/2002 5:29 PM

mobile STA

Page 17: [8] Deleted	Bob O'Hara	4/23/2002 3:47 PM

s

Page 22: [9] Deleted	Bob O'Hara	4/23/2002 4:30 PM

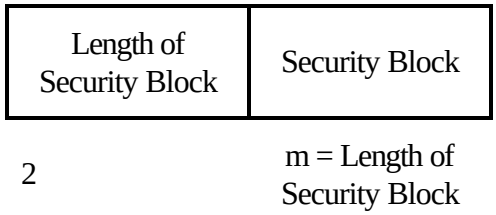


Figure 4 - Send-Security-Block Data Field Format

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 **Error! Reference source not found.**. 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

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

Page 43: [10] Deleted **Bob O'Hara** **4/22/2002 4:57 PM**

Annex B, Context Transfer

(Informative)

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

B.1 Introduction

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

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

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

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

For example, layer 2 context transfer solutions are most likely to be successful transferring context within media families, such as IEEE 802. While the IAPP is expected to be used primarily for transfer of context between IEEE 802.11 access points, it is also possible for it to be used to transfer context between access points supporting other IEEE 802 media, such as IEEE 802.15 or 802.16. Where context transfer between dissimilar media is required, then

higher layer homogeneity is needed. This can be achieved, for example, by restricting applicability to access points supporting Mobile IP.

B.2 Terminology

This document uses the following terms:

Authenticator

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

Authentication Server

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

Port Access Entity (PAE)

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

Supplicant

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

B.3 Context transfer model

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

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

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

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

For the equivalency principle to be satisfied, it is necessary for the new device to be able to process the protocol exchanges from the old device, and for those exchanges to result in the same state on the new device. This requires that the protocol messages completely describe the context to be created on the device, and that the effect of processing these messages not depend on state that exists uniquely on the old device, but may not exist on the new device. For example, a protocol message that describes the state to be attained in terms of deltas from a previous state would not be suitable for use in context transfer, since the effect of the protocol message would differ depending on the previous device state. Similarly, if a protocol message

were conditionally executed based on dynamic data, such as the number of users on the device, then the message might have a different effect on the new device than on the old device.
To a large extent, AAA protocols meet the criteria, since the desired device state is completely described by the authorizations. Conditional execution, if it occurs, is relatively rare and usually confined to the AAA server.
The set of messages that establish service context differ, depending on the AAA protocol that is being considered. Within RADIUS [4]-[6], service context is only established via an Access-Accept. Access-Reject messages do not establish context since their purpose is to deny access. Similarly, Access-Challenge messages do not establish context since they represent an intermediate stage within the authentication conversation. Since only one RADIUS message (Access-Accept) establishes service context, to re-establish context on a new device, to first order it is only necessary to transfer Access-Accept messages to the new device, and process them as if they were sent by the RADIUS server.
Note that since only one RADIUS message type can establish context, the message type need not be included explicitly, since it is implicit. As a result, devices supporting transfer of RADIUS context need only transfer attributes, not the entire RADIUS message.

B.3.1 "Correct" context transfer

Given this model for context establishment, it is worthwhile to examine when the transfer of context between devices produces a "correct" result.
One way to define correctness in a context transfer is that the transfer establishes on the new device the same context as would have been created had the new device completed a AAA conversation with the authentication server. Ideally, a context transfer should only succeed if it is "correct" in this way. If a successful context transfer would establish "incorrect" state, it would be preferable for such a transfer to fail.
Not all AAA and access device configurations are capable of meeting this definition of "correctness". Implicit within our context transfer model is trust between devices transferring context. Since the new device acts on the context transfer as though it had been instructed by a trusted AAA server, it is necessary for the new device to trust the old device.
In transfer of context across administrative domains, such a level of trust may not be possible or appropriate. As a result, a context transfer may fail even in situations where the devices are homogeneous, due to lack of trust between administrative domains.
If the deployment is heterogeneous, it also may be difficult to meet this definition of correctness. In these situations, AAA servers often perform conditional evaluation, in which the authorizations returned in an Access-Accept message are contingent on characteristics of the AAA client or the user. For example, in a heterogeneous deployment, the AAA server might return different authorizations depending on the type of device making the request, in order to make sure that the requested service is consistent with device capabilities.
If differences between the new and old device would result in the AAA server sending a different set of messages to the new device than were sent to the old device, then a context transfer between the devices cannot be carried out correctly.
For example, if some access points within a deployment support dynamic VLANs while others do not, then attributes present in the Access-Request (such as the NAS-IP-Address, NAS-Identifier, Vendor-Identifier, etc.) could be examined to determine when VLAN attributes will be returned, as described in [24].

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

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

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

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

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

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

B.3.2 Context handling

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

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

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

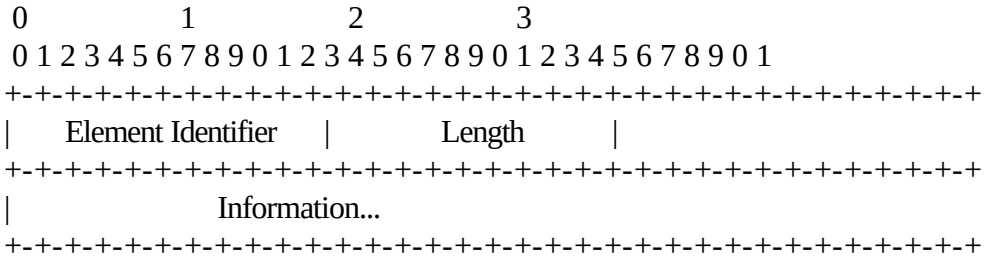
The packaging of AAA protocol messages within individual sub-elements enables compatibility with the definition of correctness described earlier. Within IAPP, a device that receives Information Elements or sub-elements that it does not support will ignore those elements, and process those that it does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

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

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

B.3.3 Information Element format

Within IAPP, Information Elements have the following structure:



Element Identifier

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

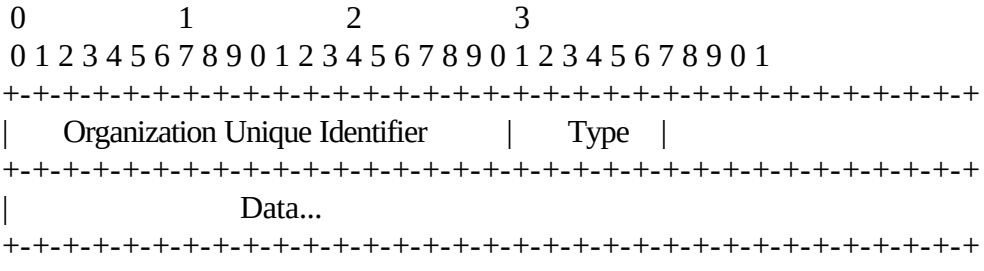
Length

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

Information

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

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



Organization Unique Identifier (OUI)

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

Type

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

RADIUS = (1)

Data

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

B.3.4 Usage guidelines for the RADIUS sub-element

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

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

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

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

B.5 Security considerations

B.5.1 Trust issues

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

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

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

B.5.2 Confidentiality

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

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

B.6 References

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix A - Table of Attributes

The following table provides a guide to which attributes are sent and received as part of IEEE 802.1X authentication, and which attributes are considered part of the "context" to be transferred during roaming. L3 denotes attributes that will be 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]

802.1X	Context	#	Attribute
X	X	11	Filter-Id [4]
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]

802.1X	Context	#	Attribute
		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]
		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]

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