Abstract

While conventional wisdom has it that wireless Access Points are strictly Layer 2 bridges, such devices today perform some higher functions that are performed by routers or switches in wired networks in addition to bridging between wired and wireless networks. For example, in 802.11 networks, Access Points can function as Network Access Servers. For this reason, Access Points have IP addresses and can function as IP devices.

This document describes the Light Weight Access Point Protocol (LWAPP) which is an IP protocol allowing a router or switch to interoperably control and manage a collection of wireless Access Points. The protocol is independent of wireless Layer 2 technology, but an 802.11 binding is provided.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [KEYWORDS].
1. Introduction

Wireless Access Points already perform a few functions that require IP level service, and so they are not strictly Layer 2 devices, conventional wisdom to the contrary. However, unlike wired network elements, Access Points require an additional set of management and control functions related to their primary function of bridging between the wireless and wired medium. The details of how these functions are implemented are naturally dependent on the particular Layer 2 wireless protocol, but in many cases the overall control and management functions themselves are generic and could apply to any wireless Layer 2 protocol. Today, protocols for managing access points are either Layer 2 specific or non-existent (if the Access Points are self-contained). The emergence of simple Access Points in 802.11 that are managed by a router or switch suggests that having a standardized, interoperable protocol could radically simplify the deployment and management of wireless networks, a trend that could become more important in new wireless Layer 2 protocols. Such a protocol could also better support interoperability between Layer 2 devices supporting different wireless Layer 2 technologies, allowing smoother intertechnology handovers.

Security is another aspect of Access Point management that is not well served by existing solutions. Provisioning Access Points with security credentials, and managing which Access Points are authorized to provide service are today handled by proprietary solutions. Allowing these functions to be performed from a centralized router or switch in an interoperable fashion increases managability and allows network operators to more tightly control their wireless network infrastructure.

This document describes the Light Weight Access Point Protocol, an inter-operable IP protocol allowing a router or switch to manage a collection of Access Points. The protocol is defined to be independent of Layer 2 technology, but an 802.11 binding is provided for use in growing 802.11 wireless LAN networks.

Goals

The following are goals for this protocol:

1. Reduction of the amount of protocol code being executed at the light weight AP, to apply the computing resource of the AP to the application of wireless access, rather than bridge forwarding and filtering. This makes the most efficient use of the computing power available in APs that are the subject of severe cost pressure.

2. Centralization of the bridging, forwarding and policy enforcement functions for a WLAN, to apply the capabilities of network processing silicon to the WLAN, as it has already been applied to wired LANs.

3. Providing a generic encapsulation and transport mechanism, the protocol may be applied to other access protocols in the future.

1.1 Protocol Overview

The Light Weight Access Protocol (LWAPP) begins with a discovery phase, whereby the APs send a Discovery Request frame, causing any Access Router (AR) receiving that frame to respond with a Discovery Reply. From the Discovery Replies received, an Access Point (AP) will select an AR with which to associate, using the Join Request and Join
Reply. The Join Request also provides an MTU discovery mechanism, to determine whether there is support for the transport of jumbo frames between the AP and its AR. If support for jumbo frames is not present, the LWAPP frames will be fragmented to the maximum length discovered to be supported by the layer 2 network.

Once the AP and the AR have joined, a configuration exchange is accomplished that will upgrade the version of the code running on the AP to match that of the AR, if necessary, and will provision the APs. The provisioning of APs includes the typical name (802.11 Service Set Identifier, SSID), and security parameters, the data rates to be advertised as well as the radio channel (channels, if the AP is capable of operating more than one 802.11 MAC and PHY simultaneously) to be used. Finally, the APs are enabled for operation.

When the AP and AR have one or more WLANs provisioned and enabled, the LWAPP encapsulates the 802.11 Data and Management frames, to transport them between the AP and AR. LWAPP will fragment its packets, if the size of the encapsulated 802.11 Data or Management frames causes the resultant LWAPP packet to exceed the MTU supported between the AP and AR. Fragmented LWAPP packets are reassembled to reconstitute the original encapsulated payload.

In addition to the functions thus far described, LWAPP also provides for the delivery of commands from the AR to the AP for the management of 802.11 devices that are communicating with the AP. This may include the creation of local data structures in the AP for the 802.11 devices and the collection of statistical information about the communication between the AP and the 802.11 devices. LWAPP provides the ability for the AR to obtain any statistical information collected by the AP.

### 1.2 Definitions

This Document uses terminology defined in [TERMS]

### 2. LWAPP Packet Format

The packet format for LWAPP is described herein as if it is carried in a native Ethernet frame. As such, it is not routable and depends upon the layer 2 connectivity between AP and AR. However, it is also possible that any other layer 2 or layer 3 transport protocol could be used to carry LWAPP packets.

#### 2.1 Header Fields

##### 2.1.1 Source Address

A MAC address belonging to the interface from which this message is sent. If multiple source addresses are configured on an interface, then the one chosen is implementation dependent.

##### 2.1.2 Destination Address

A MAC address belonging to the interface to which this message is to be sent. This destination address MAY be either an individual address or a multicast address, if more than one destination interface is intended.

##### 2.1.3 Ethertype


The Ethertype field is set to 0x88bb.

### 2.2 LWAPP Message Format

<table>
<thead>
<tr>
<th>VER</th>
<th>RID</th>
<th>D</th>
<th>F</th>
<th>L</th>
<th>Frag ID</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 2.2.1 Flags Field

The first byte contains several flag fields.

### 2.2.2 VER field

The VER field identifies the LWAPP protocol version carried in this packet. For this version of the protocol, the value of this field is 0.

### 2.2.3 RID

The RID field contains the Radio Identifier. For APs that contain more than one radio, this field is used to identify each Radio.

### 2.2.4 D Bit

The D bit indicates whether this packet carries data or control information. When this bit is 0, the packet carries an encapsulated data frame. When this bit is 1, the packet carries control information for consumption by the addressed destination.

### 2.2.5 F Bit

The F bit indicates whether this packet is a fragment. When this bit is 1, the packet is a fragment and MUST be combined with the other corresponding fragments to reassemble the complete information exchanged between the AP and AR.

### 2.2.6 L Bit

The L bit is valid only if the ‘F’ bit is set and indicates whether the packet contains the last fragment of a fragmented exchange between AP and AR. When this bit is 1, the packet is not the last fragment. When this bit is 0, the packet is the last fragment.

### 2.2.7 Fragment ID

The Fragment ID is a value assigned to each group of fragments making up a complete set. The value of Fragment ID is incremented with each new set of fragments. The Fragment ID wraps to zero after the maximum value has been used to identify a set of fragments. LWAPP only supports up to 2 fragments.

### 2.2.8 Length

The value of this field is unsigned and indicates the number of bytes in
the Payload field.

2.2.9 Control/Status

The interpretation of this field depends on the direction of transmission of the packet.

2.2.9.1 Status

When an LWAPP packet is transmitted from an AP to a AR, this field indicates link layer information associated with the frame. When the D bit is 0, this field is transmitted as zero and ignored on reception.

For 802.11, the signal strength and signal to noise ratio with which an 802.11 frame was received, encoded in the following manner:

```
0                   1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     RSSI      |     SNR       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

2.2.9.1.1 RSSI

RSSI is a signed, 8-bit value. It is the received signal strength indication, in dBm.

2.2.9.1.2 SNR

SNR is a signed, 8-bit value. It is the signal to noise ratio of the received 802.11 frame, in dB.

2.2.9.2 Control

When an LWAPP packet is transmitted from an AR to an AP, this field indicates on which WLANs the encapsulated 802.11 frame is to be transmitted. This is a bit field, where bit N indicates that the 802.11 frame is to be transmitted on 802.11 WLAN N.

The Control field is encoded in the following manner:

```
0                   1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        WLAN Number(s)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

2.2.10 Payload

The Payload field contains data equal in size to the value of the Length field, found within the LWAPP header.

2.3 LWAPP Control Messages

The LWAPP Control Messages are used to communicate between the AR and the AP. The following state diagram represents the lifecycle of an AP-AR session:

```
+----------------------------------+-
| Idle |                             |
```
Each of the states above correspond to an LWAPP control message type, defined later in this document.

2.4 Control Message Format

All LWAPP control messages are sent encapsulated within the LWAPP header (see Section 2.5) with the following header values:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Msg Type   |    Seq Num    |      Msg Element Length       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Session ID                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Msg Element [0..N]       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

2.4.1 Message Type

The Message Type field identifies the function of the LWAPP control message. The valid values for Message Type are the following:

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery Request</td>
<td>1</td>
</tr>
<tr>
<td>Discovery Reply</td>
<td>2</td>
</tr>
<tr>
<td>Join Request</td>
<td>3</td>
</tr>
<tr>
<td>Join Reply</td>
<td>4</td>
</tr>
<tr>
<td>Configure Request</td>
<td>5</td>
</tr>
<tr>
<td>Configure Response</td>
<td>6</td>
</tr>
<tr>
<td>Configuration Update Request</td>
<td>7</td>
</tr>
<tr>
<td>Configuration Update Response</td>
<td>8</td>
</tr>
<tr>
<td>Statistics Report</td>
<td>9</td>
</tr>
<tr>
<td>Statistics Report Response</td>
<td>10</td>
</tr>
<tr>
<td>Reserved</td>
<td>11-16</td>
</tr>
<tr>
<td>Echo Request</td>
<td>17</td>
</tr>
<tr>
<td>Echo Response</td>
<td>18</td>
</tr>
<tr>
<td>Image Data Request</td>
<td>19</td>
</tr>
<tr>
<td>Image Data Response</td>
<td>20</td>
</tr>
<tr>
<td>Reset Request</td>
<td>21</td>
</tr>
<tr>
<td>Reset Response</td>
<td>22</td>
</tr>
<tr>
<td>Key Update Request</td>
<td>23</td>
</tr>
<tr>
<td>Key Update Response</td>
<td>24</td>
</tr>
</tbody>
</table>

2.4.2 Sequence Number
The Sequence Number Field is an identifier value to match request/response packet exchanges. When an LWAPP packet with a request message type is received, the value of the sequence number field is copied into the corresponding response packet.

2.4.3 Msg Element Length

The Length field indicates the number of bytes following the Session ID field.

2.4.4 Session ID

The Session ID is a 32-bit unsigned integer that is used to identify the security context for encrypted exchanges between the AP and the AR.

2.4.5 Message Element[0..N]

The message element(s) carry the information pertinent to each of the control message types. The total length of the message elements is indicated in the Msg Element Length field.

The format of a message element uses the standard TLV format shown here:

```
+---------------------------------+
|      Type     |             Length            |   Value ...   |
|---------------------------------|
```

Where Type identifies the character of the information carried in the Value field and Length indicates the number of bytes in the Value field.

Section 4.0 contains the supported message elements.

3. Message exchanges

3.1 Discovery Requests

3.1.1 Sending Discovery Requests

Discovery Requests MUST be sent by an AP in the Discover state after waiting for a random delay less than MaxDiscoveryInterval, after an AP first comes up or is (re)initialed. An AP MUST send no more than a maximum of MaxDiscoveries discoveries, waiting for a random delay less than MaxDiscoveryInterval between each successive discovery.

This is to prevent an explosion of AP Discoveries. An example of this occurring would be when many APs are powered on at the same time.

Discovery requests MUST be sent by an AP when no echo responses are received for NeighborDeadInterval and the AP returns to the discover state. Discovery requests are sent after NeighborDeadInterval, they MUST be sent after waiting for a random delay less than MaxDiscoveryInterval. An AP MAY send up to a maximum of MaxDiscoveries discoveries, waiting for a random delay less than MaxDiscoveryInterval between each successive discovery.

If a discovery response is not received after sending the maximum number of discovery requests, the AP enters the Sulking state and MUST wait for
an interval equal to SilentInterval before sending further discovery requests.

3.1.2 Format of a Discovery Request

The Discovery Request carries the following message elements:

- AP Payload
- Radio Payload (one for each radio in the AP)

3.1.3 Receiving Discovery Requests

Upon receiving a discovery request, the AR will respond with a Discovery Reply sent to the address in the source address of the received discovery request.

3.2 Discovery Reply

3.2.1 Sending Discovery Replies

Discovery Replies are sent by an AR after receiving a Discovery Request.

3.2.2 Format of a Discovery Reply

The Discovery Reply carries the following message elements:

- AR Payload
- AR Name Payload

3.2.3 Receiving Discovery Replies

When an AP receives a Discovery Reply, it MUST wait for an interval not less than DiscoveryInterval for receipt of additional discovery replies. After the DiscoveryInterval elapses, the AP enters the Joining state and will select one of the ARs that sent a discovery reply and send a Join Request to that AR.

3.3 Join Request

3.3.1 Sending Join Requests

Join Requests are sent by an AP in the Joining state after receiving one or more Discovery Replies. The Join Request is also used as an MTU discovery mechanism by the AP. The AP issues a Join Request with a Test message element, bringing the total size of the message to exceed MTU. If a Join Reply is received, the AP can forward frames without requiring any fragmentation. If no Join Reply is received, it issues a second Join Request with a smaller Test Payload. This continues until a Join Reply has been received. Ideally, the AP SHOULD NOT send more than 3 Join Requests of different sizes before abandoning the AR.

3.3.2 Format of a Join Request

The Join Request carries the following message elements:

- AR Address Payload
- AP Payload
- AP Name Payload
- Location Data
Radio Payload (one for each radio)
Certificate
Session ID
Test

3.3.3 Receiving Join Requests

When an AR receives a Join Request it will respond with a Join Reply. The AR validates the certificate found in the request. If valid, the AR generates a session key which will be used to secure the control frames it exchanges with the AP. When the AR issues the Join Reply, the AR creates a context for the session with the AP.

Details on the key generation is found in appendix A.

3.4 Join Reply

3.4.1 Sending Join Replies

Join Replies are sent by the AR after receiving a Join Request. Once the Join Reply has been sent, the heartbeat timer is initiated for the session. Expiration of the timer will result in delete of the AR-AP session. The timer is refreshed upon receipt of the Echo Request.

3.4.2 Format of a Join Reply

The Join Reply carries the following message elements:

- Result Code
- Certificate
- Session Key

3.4.3 Receiving Join Replies

When an AP receives a Join Reply it enters the Joined state and initiates the Configure Request to the AR to which it is now joined. Upon entering the Joined state, the AP begins timing an interval equal to NeighborDeadInterval. Expiration of the timer will result in the transmission of the Echo Request.

3.5 Configure Request

3.5.1 Sending Configure Requests

Configure Requests are sent by an AP after receiving a Join Reply.

3.5.2 Format of a Configure Request

The Configure Request carries the following message elements:

- Administrative State (for the AP)
- AR Name
- Administrative State (for each radio)
- AP WLAN Radio Configuration (for each radio)
- Multi-domain Capability (for each radio)
- MAC Operation (for each radio)
- PHY TX Power (for each radio)
- PHY TX Power Level (for each Radio)
- PHY DSSS Payload or PHY OFDM Payload (for each radio)
Antenna
Supported Rates

3.5.3 Receiving Configure Requests

When an AR receives a Configure Request it will act upon the content of the packet and respond to the AP with a Configure Response.

3.6 Configure Response

3.6.1 Sending Configure Responses

Configure Responses are sent by an AR after receiving a Configure Request.

3.6.2 Format of a Configure Response

The Configure Response carries the following message elements:

- AP WLAN Radio Configuration (for each radio)
- Operational Rate Set (for each radio)
- Multi-domain Capability (for each radio)
- MAC Operation (for each radio)
- PHY Tx Power (for each Radio)
- PHY DSSS or PHY OFDM Payload (for each radio)
- Antenna (for each radio)

3.6.3 Receiving Configure Responses

When an AP receives a Configure Response it acts upon the content of the packet, as appropriate.

3.7 Configuration Update Request

3.7.1 Sending Configuration Update Requests

Configure Update Requests are sent by the AR to provision the AP while in the Run state. This is used to modify the configuration of the AP while it is operational.

3.7.2 Format of a Configure Command Request

The Configure Command Request carries any message elements, except the following:

- Result Code 1
- AR Address 2
- AP Payload 3
- AR Payload 5
- AP WLAN Radio Configuration 7
- Reserved 16
- Reserved 18-24
- AR Name 30
- Image Download 31
- Image Data 32
- Statistics 37
- Reserved 39-42
- Certificate 43
- Session Key 45
- Reserved 46
3.7.3 Receiving Configuration Update Requests

When an AR receives a Configuration Update Request it will respond with a Configuration Update Reply, with the appropriate Result Code.

3.8 Configuration Update Response

3.8.1 Sending Configuration Update Responses

Configuration Update Responses are sent by an AR after receiving a Configuration Update Request.

3.8.2 Format of a Configuration Update Response

The Configuration Update Response carries the following message elements:

- Result Code

3.8.3 Receiving Configure Command Responses

When an AR receives a Configure Command Response it knows that the configuration was accepted (or not) by the AP.

3.9 Statistics Report

3.9.1 Sending Statistics Reports

Statistics Reports are sent by an AP periodically, based on the configuration, to transfer statistics to the AR.

3.9.2 Format of a Statistics Report

The Statistics Report carries the following message elements:

- Statistics

3.9.3 Receiving Statistics Report

When an AR receives a Statistics Report it will respond with a Statistics Response.

3.10 Statistics Response

3.10.1 Sending Statistics Responses

Statistics Responses are sent by an AP after receiving a Statistics Report.

3.10.2 Format of a Statistics Response

The Statistics Response carries no message elements.

3.10.3 Receiving Statistics Responses
The Statistics Response is simply an acknowledgement of the Statistics Report.

3.11 Echo Request

3.11.1 Sending Echo Requests

Echo Requests are sent by an AP in the Join or Run state to determine the state of the connection between the AP and the AR.

3.11.2 Format of a Echo Request

The Echo Request carries no message elements.

3.11.3 Receiving Echo Requests

When an AR receives an Echo Request it responds with a Echo Reply.

3.12 Echo Response

3.12.1 Sending Echo Responses

Echo Responses are sent by an AR after receiving an Echo Request.

3.12.2 Format of a Echo Response

The Echo Response carries no message elements.

3.12.3 Receiving Echo Responses

When an AP receives an Echo Response it resets the timer that is timing the NeighborDeadInterval. If the NeighborDeadInterval timer expires prior to receiving an Echo Response, the AP enters the Discovery state.

3.13 Image Data Request

3.13.1 Sending Image Data Requests

Image Data Requests are exchanged between the AP and the AR to download a new program image to an AP.

3.13.2 Format of a Image Data Request

When sent by the AP, the Image Data Request contains the following message elements:

   Image Download

When sent by the AR, the Image Data Request contains the following message elements:

   Image Data

3.13.3 Receiving Image Data Requests

When an AP or AR receives an Image Data Request it will respond with a Image Data Reply.
3.14 Image Data Response

3.14.1 Sending Image Data Responses

Image Data Responses are sent in response to Image Data Request. Its purpose is to acknowledge the receipt of the Image Data Request packet.

3.14.2 Format of an Image Data Response

The Image Data Response carries no message elements.

3.14.3 Receiving Image Data Responses

No action is necessary.

3.15 Reset Request

3.15.1 Sending Reset Requests

Reset Requests are sent by an AR to cause an AP to reinitialize its operation.

3.15.2 Format of a Reset Request

The Reset Request carries no message elements.

3.15.3 Receiving Reset Requests

When an AP receives a Reset Request it will respond with a Reset Reply and then reinitialize itself.

3.16 Reset Response

3.16.1 Sending Reset Responses

Reset Responses are sent by an AP after receiving a Reset Request.

3.16.2 Format of a Reset Response

The Reset Response carries no message elements. Its purpose is to acknowledge the receipt of the Reset Request.

3.16.3 Receiving Reset Responses

When an AP receives a Reset Response it is notified that the AP will now reinitialize its operation.

3.17 Key Update Request

3.17.1 Sending Key Update Requests

Key Update Requests are sent by an AP in the Run state to update a session key. The Session ID message element MUST include a new session identifier.

3.17.2 Format of a Key Update Request
The Key Update Request carries the following message elements:

- Session ID

### 3.17.3 Receiving Key Update Requests

When a AR receives a Key Update Request it generates a new key (see appendix A) and responds with a Key Update Response.

### 3.18 Key Update Response

#### 3.18.1 Sending Key Update Responses

Key Update Responses are sent by a AR after receiving a Key Update Request. The Key Update Responses is secured using public key cryptography.

#### 3.18.2 Format of a Discovery Response

The Key Update Response carries the following message elements:

- Session Key

#### 3.18.3 Receiving Key Update Responses

When an AP receives a Key Update Response it will use the information contained in the Session Key message element to determine the keying material used to encrypt the LWAPP communications between the AP and the AR.

### 4. LWAPP Message Elements

As previously specified, the LWAPP messages MAY include a message element. The supported message elements are defined in this section.

The allowable values for the Type field are the following:

<table>
<thead>
<tr>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result Code</td>
<td>1</td>
</tr>
<tr>
<td>AR Address</td>
<td>2</td>
</tr>
<tr>
<td>AP Payload</td>
<td>3</td>
</tr>
<tr>
<td>AP Name</td>
<td>4</td>
</tr>
<tr>
<td>AR Payload</td>
<td>5</td>
</tr>
<tr>
<td>Reserved</td>
<td>6</td>
</tr>
<tr>
<td>AP WLAN Radio Configuration</td>
<td>7</td>
</tr>
<tr>
<td>Rate Set</td>
<td>8</td>
</tr>
<tr>
<td>Multi-domain capability</td>
<td>9</td>
</tr>
<tr>
<td>MAC Operation</td>
<td>10</td>
</tr>
<tr>
<td>Reserved</td>
<td>11</td>
</tr>
<tr>
<td>Tx Power Level</td>
<td>12</td>
</tr>
<tr>
<td>Direct Sequence Control</td>
<td>13</td>
</tr>
<tr>
<td>OFDM Control</td>
<td>14</td>
</tr>
<tr>
<td>Supported Rates</td>
<td>15</td>
</tr>
<tr>
<td>Reserved</td>
<td>16</td>
</tr>
<tr>
<td>Test</td>
<td>17</td>
</tr>
<tr>
<td>Reserved</td>
<td>18-25</td>
</tr>
<tr>
<td>Administrative State</td>
<td>26</td>
</tr>
<tr>
<td>Delete WLAN</td>
<td>27</td>
</tr>
<tr>
<td>Reserved</td>
<td>28</td>
</tr>
</tbody>
</table>
4.1 Result Code

The result code message element value is a 32-bit integer value, indicating the result of the request operation corresponding to the sequence number in the message.

```
+---------+--------+--------+--------+
| 0 1 2 3 | 4 5 6 7 | 8 9 0 1 |
+---------+--------+--------+--------+
```

Result Code

The following values are supported

0 - Success
1 - Failure

4.2 AR Address

The AR address message element is used to communicate the identity of the AR. The value contains two fields, as shown.

```
+---------+--------+--------+--------+
| 0 1 2 3 | 4 5 6 7 | 8 9 0 1 |
+---------+--------+--------+--------+
```

Reserved

MUST be set to zero

4.2.2 MAC Address

The MAC Address of the AR

4.3 AP Payload
The AP payload message element is used by the AP to communicate its current hardware/firmware configuration. The value contains the following fields.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.3.1 Hardware Version
A 32-bit integer representing the AP’s hardware version number

4.3.2 Software Version
A 32-bit integer representing the AP’s firmware version number

4.3.3 Boot Version
A 32-bit integer representing the AP’s boot loader’s version number

4.3.4 Max Radios
An 8-bit value representing the number of radio slots supported by the AP

4.3.5 Radios in use
An 8-bit value representing the number of radios present in the AP

4.4 AP Name
The AP name message element value is a variable length byte string. The string is NOT zero terminated.

4.5 AR Payload
The AR payload message element is used by the AR to communicate its current state. The value contains the following fields.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.3.1 Hardware Version
A 32-bit integer representing the AP’s hardware version number

4.3.2 Software Version
A 32-bit integer representing the AP’s firmware version number

4.3.3 Boot Version
A 32-bit integer representing the AP’s boot loader’s version number

4.3.4 Max Radios
An 8-bit value representing the number of radio slots supported by the AP

4.3.5 Radios in use
An 8-bit value representing the number of radios present in the AP
### 4.5.1 Hardware Version

A 32-bit integer representing the AP’s hardware version number.

### 4.5.2 Software Version

A 32-bit integer representing the AP’s Firmware version number.

### 4.5.3 Stations

A 16-bit integer representing the number of mobile stations currently associated with the AR.

### 4.5.4 Limit

A 16-bit integer representing the maximum number of stations supported by the AR.

### 4.5.5 Radios

A 16-bit integer representing the number of APs currently attached to the AR.

### 4.5.6 Max Radio

A 16-bit integer representing the maximum number of APs supported by the AR.

### 4.6 AP WLAN Radio Configuration

The AP WLAN radio configuration is used by the AR to configure a Radio on the AP. The message element value contains the following fields.

```
+---------------------------------------------------------------+
| 0 | 1 | 2 | 3 |
+---------------------------------------------------------------+
| Radio ID | Reserved | Occupancy Limit |
+---------------------------------------------------------------+
| CFP Per  | CFP Maximum Duration | BSS ID |
+---------------------------------------------------------------+
| BSS ID   |                                                      |
+---------------------------------------------------------------+
| BSS ID   | Beacon Period | DTIM Per |
+---------------------------------------------------------------+
| Country String |                                                      |
+---------------------------------------------------------------+
```

#### 4.6.1 Radio ID

An 8-bit value representing the radio to configure.

#### 4.6.2 Reserved

MUST be set to zero.

#### 4.6.3 Occupancy Limit

This attribute indicates the maximum amount of time, in TU, that a point...
coordinator MAY control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value of this attribute SHOULD be 100, and the maximum value SHOULD be 1000

4.6.4 CFP Period

The attribute describes the number of DTIM intervals between the start of CFPs

4.6.5 CFP Maximum Duration

The attribute describes the maximum duration of the CFP in TU that MAY be generated by the PCF

4.6.6 BSSID

The WLAN Radio’s MAC Address

4.6.7 Beacon Period

This attribute specifies the number of TU that a station uses for scheduling Beacon transmissions. This value is transmitted in Beacon and Probe Response frames

4.6.8 DTIM Period

This attribute specifies the number of beacon intervals that elapses between transmission of Beacons frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames

4.6.9 Country Code

This attribute identifies the country in which the station is operating. The first two octets of this string is the two character country code as described in document ISO/IEC 3166-1. The third octet MUST be one of the following:

1. an ASCII space character, if the regulations under which the station is operating encompass all environments in the country,
2. an ASCII ‘O’ character, if the regulations under which the station is operating are for an Outdoor environment only, or
3. an ASCII ‘I’ character, if the regulations under which the station is operating are for an Indoor environment only

4.7 Rate Set

The rate set message element value is sent by the AR and contains the supported operational rates. It contains the following fields.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |                   Rate Set                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

4.7.1 Radio ID
An 8-bit value representing the radio to configure

4.7.2 Rate Set

The AR generates the Rate Set that the AP is to include in its Beacon and Probe messages

4.8 Multi-domain Capability

The multi-domain capability message element is used by the AR to inform the AP of regulatory limits. The value contains the following fields.

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>+-------------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------</td>
</tr>
</tbody>
</table>

4.8.1 Radio ID

An 8-bit value representing the radio to configure

4.8.2 Reserved

MUST be set to zero

4.8.3 First Channel #

This attribute indicates the value of the lowest channel number in the subband for the associated domain country string. The default value of this attribute MUST be zero

4.8.4 Number of Channels

This attribute indicates the value of the total number of channels allowed in the subband for the associated domain country string. The default value of this attribute SHOULD be zero

4.8.5 Max Tx Power Level

This attribute indicates the maximum transmit power, in dBm, allowed in the subband for the associated domain country string. The default value of this attribute SHOULD be zero

4.9 MAC Operation

The MAC operation message element is sent by the AR to set the 802.11 MAC parameters on the AP. The value contains the following fields.

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>+-------------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------</td>
</tr>
</tbody>
</table>
4.9.1 Radio ID

An 8-bit value representing the radio to configure

4.9.2 Reserved

MUST be set to zero

4.9.3 RTS Threshold

This attribute indicates the number of octets in an MPDU, below which an RTS/CTS handshake MUST NOT be performed. An RTS/CTS handshake MUST be performed at the beginning of any frame exchange sequence where the MPDU is of type Data or Management, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size MUST have the effect of turning off the RTS/CTS handshake for frames of Data or Management type transmitted by this STA. Setting this attribute to zero MUST have the effect of turning on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default value of this attribute MUST be 2347

4.9.4 Short Retry

This attribute indicates the maximum number of transmission attempts of a frame, the length of which is less than or equal to RTSThreshold, that MUST be made before a failure condition is indicated. The default value of this attribute MUST be 7

4.9.5 Long Retry

This attribute indicates the maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that MUST be made before a failure condition is indicated. The default value of this attribute MUST be 4

4.9.6 Fragmentation Threshold

This attribute specifies the current maximum size, in octets, of the MPDU that MAY be delivered to the PHY. An MSDU MUST be broken into fragments if its size exceeds the value of this attribute after adding MAC headers and trailers. An MSDU or MMPDU MUST be fragmented when the resulting frame has an individual address in the Address1 field, and the length of the frame is larger than this threshold. The default value for this attribute MUST be the lesser of 2346 or the aMPDUMaxLength of the attached PHY and MUST never exceed the lesser of 2346 or the aMPDUMaxLength of the attached PHY. The value of this attribute MUST never be less than 256

4.9.7 Tx MSDU Lifetime

This attribute specifies the elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU MUST be terminated. The default value of this attribute MUST be 512

4.9.8 Rx MSDU Lifetime
This attribute specifies the elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU MUST be terminated. The default value MUST be 512

4.10 Tx Power Level

The Tx power level message element is sent by the AP and contains the different power levels supported. The value contains the following fields.

<table>
<thead>
<tr>
<th>Radio ID</th>
<th>Num Levels</th>
<th>Power Level [n]</th>
</tr>
</thead>
</table>

4.10.1 Radio ID

An 8-bit value representing the radio to configure

4.10.2 Num Levels

The number of power level attributes

4.10.3 Power Level

Each power level fields contains a supported power level, in mW.

4.11 Direct Sequence Control

The direct sequence control message element is a bi-directional element. When sent by the AP, it contains the current state. When sent by the AR, the AP MUST adhere to the values. This element is only used for 802.11b radios. The value has the following fields.

<table>
<thead>
<tr>
<th>Radio ID</th>
<th>Reserved</th>
<th>Current Chan</th>
<th>Current CCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy Detect Threshold</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.11.1 Radio ID

An 8-bit value representing the radio to configure

4.11.2 Reserved

MUST be set to zero

4.11.3 Current Channel

This attribute contains the current operating frequency channel of the DSSS PHY.

4.11.4 Current CCA
The current CCA method in operation. Valid values are:
1 - energy detect only (edonly)
2 - carrier sense only (csonly)
4 - carrier sense and energy detect (edandcs)
8 - carrier sense with timer (cswithtimer)
16 - high rate carrier sense and energy detect (hrcsanded)

4.11.5 Energy Detect Threshold
The current Energy Detect Threshold being used by the DSSS PHY

4.12 OFDM Control

The OFDM control message element is a bi-directional element. When sent by the AP, it contains the current state. When sent by the AR, the AP MUST adhere to the values. This element is only used for 802.11a radios. The value contains the following fields.

```
+------------------------------------------+
<table>
<thead>
<tr>
<th>Radio ID</th>
<th>Reserved</th>
<th>Current Chan</th>
<th>Band Support</th>
</tr>
</thead>
</table>
+------------------------------------------+
| TI Threshold                              |
+------------------------------------------+
```

4.12.1 Radio ID
An 8-bit value representing the radio to configure

4.12.2 Reserved
MUST be set to zero

4.12.3 Current Channel
This attribute contains the current operating frequency channel of the OFDM PHY.

4.12.4 Band Supported
The capability of the OFDM PHY implementation to operate in the three U-NII bands. Coded as an integer value of a three bit field as follows:

- Bit 0 - capable of operating in the lower (5.15-5.25 GHz) U-NII band
- Bit 1 - capable of operating in the middle (5.25-5.35 GHz) U-NII band
- Bit 2 - capable of operating in the upper (5.725-5.825 GHz) U-NII band

For example, for an implementation capable of operating in the lower and mid bands this attribute would take the value 3

4.12.5 TI Threshold
The Threshold being used to detect a busy medium (frequency). CCA MUST report a busy medium upon detecting the RSSI above this threshold

4.13 Supported Rates
The supported rates message element is sent by the AP to indicate the rates that it supports. The value contains the following fields.

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+----------------------------------------------------------+
|  Radio ID | Supported Rates                                   |
+----------------------------------------------------------+
```

4.13.1 Radio ID

An 8-bit value representing the radio

4.13.2 Supported Rates

The AP includes the Supported Rates that it's hardware supports. The format is identical to the Rate Set message element

4.14 Test

The test message element is used as padding to perform MTU discovery, and MAY contain any value, of any length.

4.15 Administrative State

The administrative event message element is used to communicate the state of a particular radio. The value contains the following fields.

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+----------------------------------------------------------+
|  Radio ID | Admin State                              |
+----------------------------------------------------------+
```

4.15.1 Radio ID

An 8-bit value representing the radio to configure

4.15.2 Admin State

An 8-bit value representing the administrative state of the radio. The following values are supported:

- 0 - Enabled
- 1 - Disabled

4.16 Delete WLAN

The delete WLAN message element is used to inform the AP that a previously created WLAN is to be deleted. The value contains the following fields.

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+----------------------------------------------------------+
|  Radio ID | WLAN ID                                        |
+----------------------------------------------------------+
```

4.16.1 Radio ID
An 8-bit value representing the radio

4.16.2 WLAN ID

A 16-bit value specifying the WLAN Identifier

4.17 AR Name

The AR name message element contains an ASCII representation of the AR’s identity. The value is a variable length byte string. The string is NOT zero terminated.

4.18 Image Download

The image download message element is sent by the AP to the AR and contains the image filename. The value is a variable length byte string. The string is NOT zero terminated.

4.19 Image Data

The image data message element value contains the following fields.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opcode</td>
<td>Checksum</td>
<td>Image Data</td>
<td></td>
</tr>
<tr>
<td>+--------------------+-----------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.19.1 Opcode

An 8-bit value representing the transfer opcode. The following values are supported:

3 - Image data is included
5 - An error occurred. Transfer is aborted

4.19.2 Checksum

A 16-bit value containing a checksum of the image data that follows

4.19.3 Image Data

A variable length firmware data

4.20 Location Data

The location data message element is a variable length byte string containing user defined location information (e.g. "Next to Fridge"). The string is NOT zero terminated.

4.21 Statistics Timer

The statistics timer message element value is used by the AR to inform the AP of the frequency which it expects to receive updated statistics.
4.21.1 Statistics Timer

A 16-bit unsigned integer indicating the time, in seconds.

4.22 Statistics

The statistics message element is sent by the AP to transmit its current statistics. The value contains the following fields.

4.22.1 Radio ID

An 8-bit value representing the radio.

4.22.2 Tx Fragment Count

A 32-bit value representing the number of fragmented frames transmitted.

4.22.3 Multicast Tx Count
A 32-bit value representing the number of multicast frames transmitted.

4.22.4 Failed Count

A 32-bit value representing the transmit excessive retries.

4.22.5 Retry Count

A 32-bit value representing the number of transmit retries.

4.22.6 Multiple Retry Count

A 32-bit value representing the number of transmits that required more than one retry.

4.22.7 Frame Duplicate Count

A 32-bit value representing the duplicate frames received.

4.22.8 RTS Success Count

A 32-bit value representing the number of successful Ready To Send (RTS).

4.22.9 RTS Failure Count

A 32-bit value representing the failed RTS.

4.22.10 ACK Failure Count

A 32-bit value representing the number of failed acknowledgements.

4.22.11 Rx Fragment Count

A 32-bit value representing the number of fragmented frames received.

4.22.12 Multicast RX Count

A 32-bit value representing the number of multicast frames received.

4.22.13 FCS Error Count

A 32-bit value representing the number of FCS failures.

4.22.14 Reserved

MUST be set to zero

4.23 Antenna

The antenna message element is communicated by the AP to the AR to provide information on the antennas available. The AR MAY use this element to reconfigure the AP’s antennas. The value contains the following fields.

<table>
<thead>
<tr>
<th>Radio ID</th>
<th>Diversity</th>
<th>Reserved</th>
<th>Antenna Cnt</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
<td>+---------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+---------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.23.1 Radio ID

An 8-bit value representing the radio

4.23.2 Diversity

An 8-bit value specifying whether the antenna is to provide receive diversity. The following values are supported:
0 - Disabled
1 - Enabled (may only be true if the antenna can be used as a receive antenna)

4.23.3 Reserved

MUST be set to zero

4.23.4 Antenna Count

An 8-bit value specifying the number of Antenna Selection fields.

4.23.5 Antenna Selection

A 32-bit value representing the antenna type. The following values are supported:
1 - Sectorized (Left)
2 - Sectorized (Right)
3 - Omni

4.24 Certificate

The certificate message element value is a byte string containing a PKCS #5 certificate [PKCS5].

4.25 Session ID

The session ID message element value contains a randomly generated [RANDOM] unsigned 32-bit integer.

4.26 Session Key Payload

The Session Key Payload message element is sent by the AR to the AP and includes the randomly generated session key, which is used to protect the LWAPP control messages. More details are available in appendix A. The value contains the following fields.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
| Session ID                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
| Session Key                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
| Session Key                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
| Session Key                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```
4.26.1 Session ID

A 32-bit value representing the session which this session key is related to.

4.26.2 Session Key

A 128-bit value randomly generated session key [RANDOM]

4.27 WLAN Payload

The WLAN payload message element is used by the AR to define a wireless LAN on the AP. The value contains the following format:

```
0                   1                   2                   3
+-------------------------------+-------------------------------+-------------------------------+-------------------------------+
|       Radio ID          |       WLAN Capability        |       WLAN ID            |
+-------------------------------+-------------------------------+-------------------------------+
|       WLAN ID            |       SSID ...              |
+-------------------------------+-------------------------------+
```

4.27.1 Radio ID

An 8-bit value representing the radio.

4.27.2 WLAN Capability

A 16-bit value containing the capabilities to be advertised by the AP within the Probe and Beacon messages.

4.27.3 WLAN ID

A 16-bit value specifying the WLAN Identifier.

4.27.4 SSID

The SSID attribute is a variable length byte string containing the SSID to be advertised by the AP. The string is NOT zero terminated.

4.28 Vendor Specific Payload

The Vendor Specific Payload is used to communicate vendor specific information between the AP and the AR. The value contains the following format:

```
0                   1                   2                   3
+-------------------------------+-------------------------------+-------------------------------+-------------------------------+
|       Vendor Identifier     |       Element ID             |       Value...              |
+-------------------------------+-------------------------------+-------------------------------+
```

4.28.1 Vendor Identifier
A 32-bit value containing the IANA assigned "SMI Network Management Private Enterprise Codes" [SMI]

4.28.2 Element ID

A 16-bit Element Identifier which is managed by the vendor.

4.28.3 Value

The value associated with the vendor specific element.

4.29 Tx Power

The Tx power message element value is bi-directional. When sent by the AP, it contains the current power level of the radio in question. When sent by the AR, it contains the power level the AP MUST adhere to.

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+</td>
</tr>
</tbody>
</table>

4.29.1 Radio ID

An 8-bit value representing the radio to configure

4.29.2 Reserved

MUST be set to zero

4.29.3 Current Tx Power

This attribute contains the transmit output power in mW

5. LWAPP Configuration Variables

An AP or AR that implements LWAPP discovery MUST allow for the following variables to be configured by system management; default values are specified so as to make it unnecessary to configure any of these variables in many cases.

5.1 MaxDiscoveryInterval

The maximum time allowed between sending discovery requests from the interface, in seconds. Must be no less than 2 seconds and no greater than 180 seconds.

   Default: 20 seconds.

5.2 MaxDiscoveries

The maximum number of discovery requests that will be sent after an AP boots.

   Default: 10

5.3 SilentInterval
The minimum time, in seconds, an AP MUST wait after failing to receive any responses to its discovery requests, before it MAY again send discovery requests.

Default: 30

5.4 NeighborDeadInterval

The minimum time, in seconds, an AP MUST wait without having received echo replies to its echo responses, before the destination for the echo replies may be considered dead. Must be no less than 2*EchoInterval seconds and no greater than 240 seconds.

Default: 60

5.5 EchoInterval

The minimum time, in seconds, between sending echo requests to the AR with which the AP has joined.

Default: 30

5.6 DiscoveryInterval

The minimum time, in seconds, that an AP MUST wait after receiving a discovery reply, before sending a join request.

Default: 5


<table>
<thead>
<tr>
<th>Constant</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAX_RESPONSE_DELAY</td>
<td>2 seconds</td>
</tr>
<tr>
<td>MAX_SOLICITATION_DELAY</td>
<td>1 second</td>
</tr>
<tr>
<td>SOLICITATION_INTERVAL</td>
<td>3 seconds</td>
</tr>
<tr>
<td>MAX_SOLICITATIONS</td>
<td>3 transmissions</td>
</tr>
</tbody>
</table>

7. Security Considerations

LWAPP uses public key cryptography to ensure trust between the AP and the AR. During the Join phase, the AR generates a session key, which is used to secure all future control messages. The AP does not participate in the key generation, but public key cryptography is used to authenticate the resulting key material. A secured delivery mechanism to place the certificate in the devices is required. In order to maximize session key security, the AP and AR periodically update the session keys, which are encrypted using public key cryptography. This ensures that a potentially previously compromised key does not affect the security of communication with new key material.

8. References

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997
9. Acknowledgments

10. Author’s Addresses

Pat Calhoun
Airespace
110 Nortech Parkway
San Jose, CA 95154
Email: pcalhoun@airespace.com
Phone: +1 408-635-2023

Bob O’Hara
Airespace
110 Nortech Parkway
San Jose, CA 95154
Email: bob@airespace.com
Phone: +1 408-635-2025

Scott Kelly
Airespace
110 Nortech Parkway
San Jose, CA 95154
Email: skelly@airespace.com
Phone: +1 408-635-2022

Rohit Suri
Airespace
110 Nortech Parkway
San Jose, CA 95154
Email: rsuri@airespace.com
Phone: +1 408-635-2026

Glen Zorn
Cisco Systems, Inc.
500 108th Avenue N.E., Suite 500
Bellevue, WA 98004
EMail: gwz@cisco.com
Phone: +1 425 438 8218

Daichi Funato
Appendix A: Session Key Generation

Note: This version only defines a certificate based mechanism to secure traffic between the AP and the AR. A shared-secret mechanism will be added in a future version.

A.1 Securing AP-AR communications

While it is generally straightforward to produce network installations in which the communications medium between the AP and AR is not accessible to the casual user (e.g. these LAN segments are isolated, no RJ45 or other access ports exist between the AP and the AR), this will not always be the case. Furthermore, a determined attacker may resort to various more sophisticated monitoring and/or access techniques, thereby compromising the integrity of this connection.

In general, a certain level of threat on the local (wired) LAN is expected and accepted in most computing environments. That is, it is expected that in order to provide users with an acceptable level of service and maintain reasonable productivity levels, a certain amount of risk must be tolerated. It is generally believed that a certain perimeter is maintained around such LANs, that an attacker must have access to the building(s) in which such LANs exist, and that they must be able to "plug in" to the LAN in order to access the network.

With these things in mind, we can begin to assess the general security requirements for AR-AP communications. While an in-depth security analysis of threats and risks to these communication is beyond the scope of this document, some discussion of the motivation for various security-related design choices is useful. The assumptions driving the security design thus far include the following:

- AP-AR communications take place over a wired connection which may be accessible to a sophisticated attacker
- Access to this connection is not trivial for an outsider (i.e. someone who does not "belong" in the building) to access
- If authentication and/or privacy of end to end traffic for which the AP and AR are intermediaries is required, this may be provided via IPsec.
- Privacy and authentication for at least some AP-AR control traffic is required (e.g. WEP keys for user sessions, passed from AR to AP)
- The AR can be trusted to generate strong cryptographic keys

AR-AP traffic can be considered to consist of two types: data traffic (e.g. from or to an end user), and control traffic which is strictly
between the AR and AP. Since data traffic may be secured using Ipsec (or some other end-to-end security mechanism), we confine our solution to control traffic. The resulting security consists of two components: an authenticated key exchange, and control traffic security encapsulation. The security encapsulation is accomplished using CCM, described in [ref. here]. This encapsulation provides for strong AES-based authentication and encryption. The exchange of cryptographic keys used for CCM is described below.

A.2 Authenticated Key Exchange

The AR and AP accomplish mutual authentication and a cryptographic key exchange in a single round trip using the JOIN request/response pair. To accomplish this, the AP includes its identity certificate and a randomly-generated session ID which functions as a cryptographic nonce in the JOIN request. The AR verifies the AP’s certificate, and replies with its own identity certificate, and a signed concatenation of the session ID and and encrypted cryptographic session key. This exchange is detailed below.

Before proceeding, we define the following notation:

- **Kpriv** - the private key of a public-private key pair.
- **Kpub** - the public key of the pair
- **M** - a clear-text message
- **C** - a cipher-text message.
- **PKCS1(z)** - the PKCS#1 encapsulation of z
- **E-x{Kpriv, M}** - encryption of M using X’s private key
- **E-x{Kpub, M}** - encryption of M using X’s public key
- **S-x{M}** - a digital signature over M produced by X
- **V-x(S-x, M)** - verification of X’s digital signature over M
- **D-x{Kpriv, C}** - decryption of C using X’s private key
- **D-x{Kpub, C}** - decryption of C using X’s public key

When the AR receives the SessionID value along with the AP’s certificate, it constructs the reply payload as follows:

- Randomly generate enough key material to produce an encryption key and an authentication hash key (xx bytes in length).
  [TBD: detailed key material generation instructions]

- Compute C1 = E-ap{ Kpub , PKCS1(KeyMaterial)}; this encrypts the PKCS#1-encoded key material with the public key of the AP, so that only the AP can decrypt it and determine the session keys.

- Compute S1 = S-ar(SessionID|C1); this computes the AR’s digital signature over the concatenation of the nonce and the encrypted key material, and can be verified using the public key of the AP, "proving" that the AR produced this; this forms the basis of trust for the AP with respect to the source of the session keys.
o AR sends (Certificate-AR, C1, S1, SessionID) to AP

o AP verifies that SessionID matches an outstanding request

o AP verifies authenticity of Certificate-AR

o AP computes V-ar(S1, SessionID|C1), verifying the AR’s signature over the session identifier and the encrypted key material

o AP computes PKCS1(KeyMaterial) = D-ar(Kpriv, C1), decrypting the session keys using its private key; since these were encrypted with the AP’s public key, only the AP can successfully decrypt this.

KeyMaterial is divided into the encryption key and the HMAC key [TBD: say how] From this point on, all control protocol payloads between the AP and AR are encrypted and authenticated. The related payloads are described in the sections above.

A.3 Refreshing Cryptographic Keys

Since AR-AP associations will tend to be relatively long-lived, it is sensible to periodically refresh the encryption and authentication keys; this is referred to as "rekeying". This function is entirely driven at the discretion of the AR. When the key lifetime reaches 95% of the configured value, the rekeying will proceed as follows:

o AP generates a fresh SessionID value, along with fresh keying material

o AP computes C1 = E-ar(Kpub, PKCS1(KeyMaterial)); this encrypts the new key material with the public key of the AR, so that only the AR can determine the session key. This provides a form of forward secrecy, as an attacker who has broken the current AR-AP session key must also have broken the AR’s private RSA key to determine this new value.

o AP constructs a TLV payload of type KEY-UPDATE which contains the new SessionID followed by the encrypted key material (C1) and sends this to AR. Since this is a control payload, it is encrypted and authenticated using the existing session keys.

o AR decrypts the new keys, instantiates the new session, deletes the old session, and sends a KEY-UPDATE-RSP message to the AP using the new session values.

o AP must maintain session state for the original SessionID and keys until it receives the KEY-UPDATE-RSP, at which time it clears the old session.

o If AP does not receive the KEY-UPDATE-RSP within a reasonable period of time (1 minute?), it will resend the original request and reset its response timer. If no response occurs by the time the original session expires, the AP will delete the new and old session information, and initiate the DISCOVER process anew.