Independent Submission
Request for Comments: 5412
Category: Historic
ISSN: 2070-1721

P. Calhoun
R. Suri
N. Cam-Winget
Cisco Systems, Inc.
M. Williams
GWhiz Arts & Sciences
S. Hares
B. O'Hara
S.Kelly

February 2010

Lightweight Access Point Protocol

Abstract

In recent years, there has been a shift in wireless LAN (WLAN) product architectures from autonomous access points to centralized control of lightweight access points. The general goal has been to move most of the traditional wireless functionality such as access control (user authentication and authorization), mobility, and radio management out of the access point into a centralized controller.

The IETF's CAPWAP (Control and Provisioning of Wireless Access Points) WG has identified that a standards-based protocol is necessary between a wireless Access Controller and Wireless Termination Points (the latter are also commonly referred to as Lightweight Access Points). This specification defines the Lightweight Access Point Protocol (LWAPP), which addresses the CAPWAP's (Control and Provisioning of Wireless Access Points) protocol requirements. Although the LWAPP protocol is designed to be flexible enough to be used for a variety of wireless technologies, this specific document describes the base protocol and an extension that allows it to be used with the IEEE's 802.11 wireless LAN protocol.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for the historical record.

This document defines a Historic Document for the Internet community. This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5412.

IESG Note

This RFC documents the LWAPP protocol as it was when submitted to the IETF as a basis for further work in the CAPWAP Working Group, and therefore it may resemble the CAPWAP protocol specification in RFC 5415 as well as other IETF work. This RFC is being published solely for the historical record. The protocol described in this RFC has not been thoroughly reviewed and may contain errors and omissions.

RFC 5415 documents the standards track solution for the CAPWAP Working Group and obsoletes any and all mechanisms defined in this RFC. This RFC is not a candidate for any level of Internet Standard and should not be used as a basis for any sort of Internet deployment.

Copyright Notice

Table of Contents

1. Introduction

Unlike wired network elements, Wireless Termination Points (WTPs) require a set of dynamic management and control functions related to their primary task of connecting the wireless and wired mediums. Today, protocols for managing WTPs are either manual static configuration via HTTP, proprietary Layer 2-specific, or non-existent (if the WTPs are self-contained). The emergence of simple 802.11 WTPs that are managed by a WLAN appliance or switch (also known as an Access Controller, or AC) suggests that having a standardized, interoperable protocol could radically simplify the deployment and management of wireless networks. In many cases, the overall control and management functions themselves are generic and could apply to an AP for any wireless Layer 2 (L2) protocol. Being independent of specific wireless Layer 2 technologies, such a protocol could better support interoperability between Layer 2 devices and enable smoother intertechnology handovers.

The details of how these functions would be implemented are dependent on the particular Layer 2 wireless technology. Such a protocol would need provisions for binding to specific technologies.

LWAPP assumes a network configuration that consists of multiple WTPs communicating either via Layer 2 (Medium Access Control (MAC)) or Layer 3 (IP) to an AC. The WTPs can be considered as remote radio frequency (RF) interfaces, being controlled by the AC. The AC forwards all L2 frames it wants to transmit to a WTP via the LWAPP protocol. Packets from mobile nodes are forwarded by the WTP to the AC, also via this protocol. Figure 1 illustrates this arrangement as applied to an IEEE 802.11 binding.

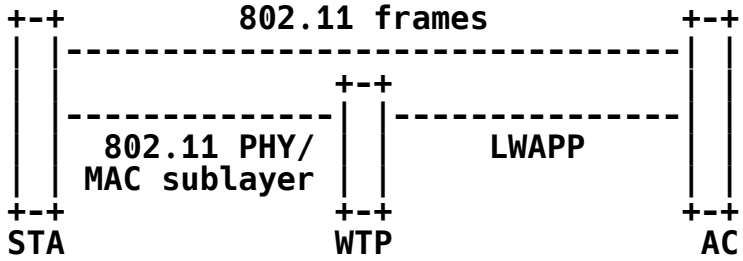


Figure 1: LWAPP Architecture

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

This document describes the Lightweight Access Point Protocol (LWAPP), allowing an AC to manage a collection of WTPs. 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. Centralization of the bridging, forwarding, authentication, and policy enforcement functions for a wireless network. Optionally, the AC may also provide centralized encryption of user traffic. This will permit reduced cost and higher efficiency when applying the capabilities of network processing silicon to the wireless network, as it has already been applied to wired LANs.

2. Permit shifting of the higher-level protocol processing burden away from the WTP. This leaves the computing resource of the WTP to the timing-critical applications of wireless control and access. This makes the most efficient use of the computing power available in WTPs that are the subject of severe cost pressure.

3. Providing a generic encapsulation and transport mechanism, the protocol may be applied to other access point types in the future by adding the binding.

The LWAPP protocol concerns itself solely with the interface between the WTP and the AC. Inter-AC, or mobile-to-AC communication is strictly outside the scope of this document.

1.1. 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 [1].

2. Protocol Overview

LWAPP is a generic protocol defining how Wireless Termination Points communicate with Access Controllers. Wireless Termination Points and Access Controllers may communicate either by means of Layer 2 protocols or by means of a routed IP network.

LWAPP messages and procedures defined in this document apply to both types of transports unless specified otherwise. Transport independence is achieved by defining formats for both MAC-level and IP-level transport (see Section 3). Also defined are framing, fragmentation/reassembly, and multiplexing services to LWAPP for each transport type.

The LWAPP Transport layer carries two types of payload. LWAPP data messages are forwarded wireless frames. LWAPP control messages are management messages exchanged between a WTP and an AC. The LWAPP transport header defines the "C-bit", which is used to distinguish data and control traffic. When used over IP, the LWAPP data and control traffic are also sent over separate UDP ports. Since both data and control frames can exceed Path Maximum Transmission Unit (PMTU), the payload of an LWAPP data or control message can be fragmented. The fragmentation behavior is highly dependent upon the lower-layer transport and is defined in Section 3.

The Lightweight Access Protocol (LWAPP) begins with a discovery phase. The WTPs send a Discovery Request frame, causing any Access Controller (AC), receiving that frame to respond with a Discovery Response. From the Discovery Responses received, a WTP will select an AC with which to associate, using the Join Request and Join Response. The Join Request also provides an MTU discovery mechanism, to determine whether there is support for the transport of large frames between the WTP and its AC. If support for large frames is not present, the LWAPP frames will be fragmented to the maximum length discovered to be supported by the network.

Once the WTP and the AC have joined, a configuration exchange is accomplished that will cause both devices to agree on version information. During this exchange, the WTP may receive provisioning settings. For the 802.11 binding, this information would typically include a 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 WTP is capable of operating more than one 802.11 MAC and Physical Layer (PHY) simultaneously) to be used. Finally, the WTPs are enabled for operation.

When the WTP and AC have completed the version and provision exchange and the WTP is enabled, the LWAPP encapsulates the wireless frames sent between them. LWAPP will fragment its packets, if the size of the encapsulated wireless user data (Data) or protocol control (Management) frames cause the resultant LWAPP packet to exceed the MTU supported between the WTP and AC. 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 AC to the WTP for the management of devices that are communicating with the WTP. This may include the creation of local data structures in the WTP for the managed devices and the collection of statistical information about the communication between the WTP and the 802.11 devices. LWAPP provides the ability for the AC to obtain any statistical information collected by the WTP.

LWAPP also provides for a keepalive feature that preserves the communication channel between the WTP and AC. If the AC fails to appear alive, the WTP will try to discover a new AC to communicate through.

This document uses terminology defined in [5].

2.1. Wireless Binding Definition

This draft standard specifies a protocol independent of a specific wireless access point radio technology. Elements of the protocol are designed to accommodate specific needs of each wireless technology in a standard way. Implementation of this standard for a particular wireless technology must follow the binding requirements defined for that technology. This specification includes a binding for the IEEE 802.11 (see Section 11).

When defining a binding for other technologies, the authors MUST include any necessary definitions for technology-specific messages and all technology-specific message elements for those messages. At a minimum, a binding MUST provide the definition for a binding-specific Statistics message element, which is carried in the WTP Event Request message, and Add Mobile message element, which is carried in the Mobile Configure Request. If any technology-specific message elements are required for any of the existing LWAPP messages defined in this specification, they MUST also be defined in the technology-binding document.

The naming of binding-specific message elements MUST begin with the name of the technology type, e.g., the binding for IEEE 802.11, provided in this standard, begins with "IEEE 802.11".

2.2. LWAPP State Machine Definition

The following state diagram represents the life cycle of a WTP-AC session:

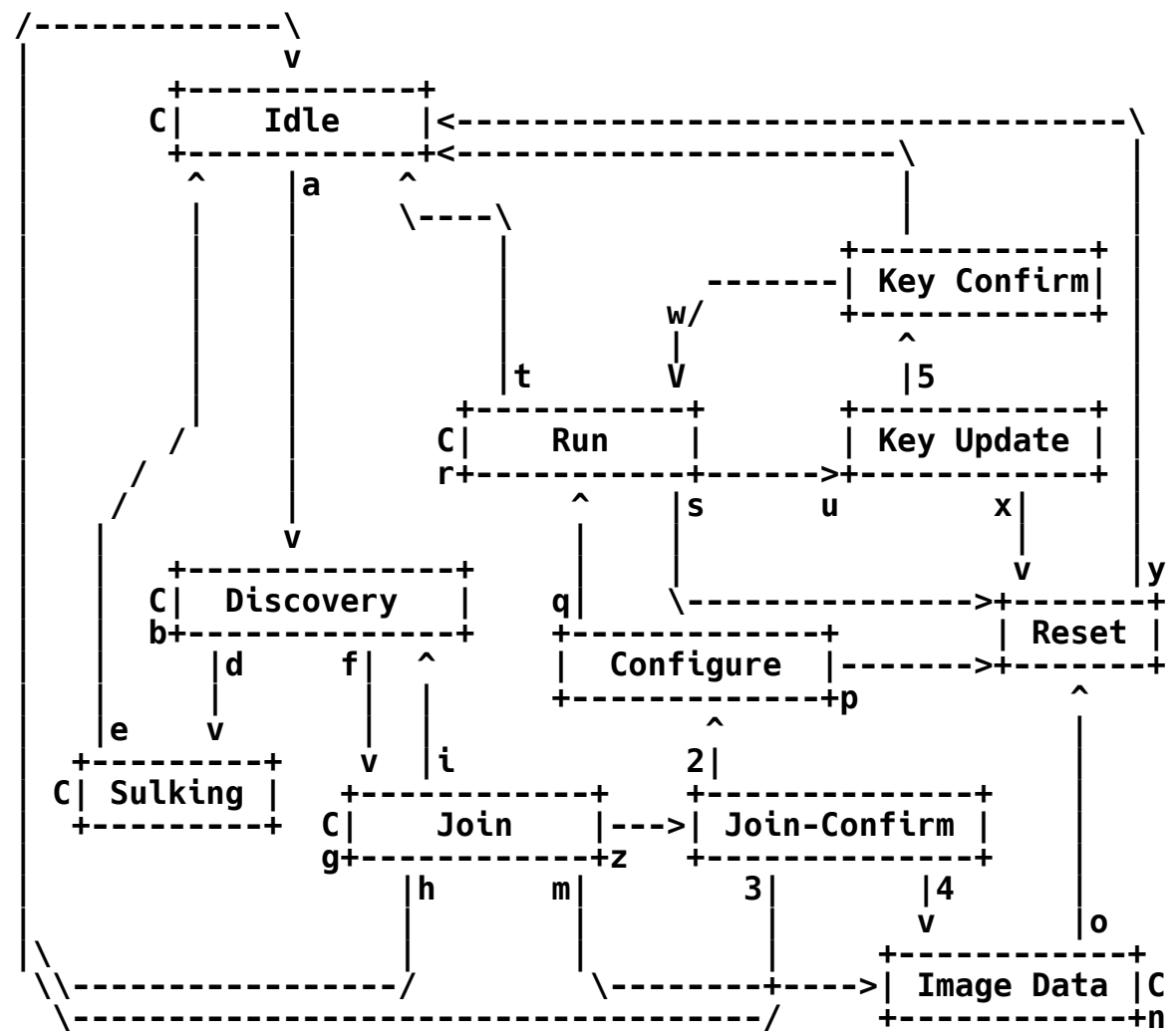


Figure 2: LWAPP State Machine

The LWAPP state machine, depicted above, is used by both the AC and the WTP. For every state defined, only certain messages are permitted to be sent and received. In all of the LWAPP control messages defined in this document, the state for which each command is valid is specified.

Note that in the state diagram figure above, the 'C' character is used to represent a condition that causes the state to remain the same.

The following text discusses the various state transitions, and the events that cause them.

Idle to Discovery (a): This is the initialization state.

WTP: The WTP enters the Discovery state prior to transmitting the first Discovery Request (see Section 5.1). Upon entering this state, the WTP sets the DiscoveryInterval timer (see Section 12). The WTP resets the DiscoveryCount counter to zero (0) (see Section 13). The WTP also clears all information from ACs (e.g., AC Addresses) it may have received during a previous discovery phase.

AC: The AC does not need to maintain state information for the WTP upon reception of the Discovery Request, but it MUST respond with a Discovery Response (see Section 5.2).

Discovery to Discovery (b): This is the state the WTP uses to determine to which AC it wishes to connect.

WTP: This event occurs when the DiscoveryInterval timer expires. The WTP transmits a Discovery Request to every AC to which the WTP hasn't received a response. For every transition to this event, the WTP increments the DisoveryCount counter. See Section 5.1 for more information on how the WTP knows to which ACs it should transmit the Discovery Requests. The WTP restarts the DiscoveryInterval timer.

AC: This is a noop.

Discovery to Sulking (d): This state occurs on a WTP when Discovery or connectivity to the AC fails.

WTP: The WTP enters this state when the DiscoveryInterval timer expires and the DiscoveryCount variable is equal to the MaxDiscoveries variable (see Section 13). Upon entering this state, the WTP will start the SilentInterval timer. While in the Sulking state, all LWAPP messages received are ignored.

AC: This is a noop.

Sulking to Idle (e): This state occurs on a WTP when it must restart the discovery phase.

WTP: The WTP enters this state when the SilentInterval timer (see Section 12) expires.

AC: This is a noop.

Discovery to Join (f): This state is used by the WTP to confirm its commitment to an AC that it wishes to be provided service.

WTP: The WTP selects the best AC based on the information it gathered during the discovery phase. It then transmits a Join Request (see Section 6.1) to its preferred AC. The WTP starts the WaitJoin timer (see Section 12).

AC: The AC enters this state for the given WTP upon reception of a Join Request. The AC processes the request and responds with a Join Response.

Join to Join (g): This state transition occurs during the join phase.

WTP: The WTP enters this state when the WaitJoin timer expires, and the underlying transport requires LWAPP MTU detection (Section 3).

AC: This state occurs when the AC receives a retransmission of a Join Request. The WTP processes the request and responds with the Join Response.

Join to Idle (h): This state is used when the join process has failed.

WTP: This state transition occurs if the WTP is configured to use pre-shared key (PSK) security and receives a Join Response that includes an invalid PSK-MIC (Message Integrity Check) message element.

AC: The AC enters this state when it transmits an unsuccessful Join Response.

Join to Discovery (i): This state is used when the join process has failed.

WTP: The WTP enters this state when it receives an unsuccessful Join Response. Upon entering this state, the WTP sets the DiscoveryInterval timer (see Section 12). The WTP resets the DiscoveryCount counter to zero (0) (see Section 13). This state transition may also occur if the PSK-MIC (see Section 6.2.9) message element is invalid.

AC: This state transition is invalid.

Join to Join-Confirm (z): This state is used to provide key confirmation during the join process.

WTP: This state is entered when the WTP receives a Join Response. In the event that certificate-based security is utilized, this transition will occur if the Certificate message element is present and valid in the Join Response. For pre-shared key security, the Join Response must include a valid and authenticated PSK-MIC message element. The WTP MUST respond with a Join ACK, which is used to provide key confirmation.

AC: The AC enters this state when it receives a valid Join ACK. For certificate-based security, the Join ACK MUST include the WNonce message element. For pre-shared key security, the message must include a valid PSK-MIC message element. The AC MUST respond with a Join Confirm message, which includes the Session Key message element.

Join-Confirm to Idle (3): This state is used when the join process has failed.

WTP: This state transition occurs when the WTP receives an invalid Join Confirm.

AC: The AC enters this state when it receives an invalid Join ACK.

Join-Confirm to Configure (2): This state is used by the WTP and the AC to exchange configuration information.

WTP: The WTP enters this state when it receives a successful Join Confirm and determines that its version number and the version number advertised by the AC are the same. The WTP transmits the Configure Request (see Section 7.2) message to the AC with a snapshot of its current configuration. The WTP also starts the ResponseTimeout timer (see Section 12).

AC: This state transition occurs when the AC receives the Configure Request from the WTP. The AC must transmit a Configure Response (see Section 7.3) to the WTP, and may include specific message elements to override the WTP's configuration.

Join-Confirm to Image Data (4): This state is used by the WTP and the AC to download executable firmware.

WTP: The WTP enters this state when it receives a successful Join Confirm, and determines that its version number and the version number advertised by the AC are different. The WTP transmits the Image Data Request (see Section 8.1) message requesting that the AC's latest firmware be initiated.

AC: This state transition occurs when the AC receives the Image Data Request from the WTP. The AC must transmit an Image Data Response (see Section 8.2) to the WTP, which includes a portion of the firmware.

Image Data to Image Data (n): This state is used by the WTP and the AC during the firmware download phase.

WTP: The WTP enters this state when it receives an Image Data Response that indicates that the AC has more data to send.

AC: This state transition occurs when the AC receives the Image Data Request from the WTP while already in this state, and it detects that the firmware download has not completed.

Image Data to Reset (o): This state is used when the firmware download is completed.

WTP: The WTP enters this state when it receives an Image Data Response that indicates that the AC has no more data to send, or if the underlying LWAPP transport indicates a link failure. At this point, the WTP reboots itself.

AC: This state transition occurs when the AC receives the Image Data Request from the WTP while already in this state, and it detects that the firmware download has completed or if the underlying LWAPP transport indicates a link failure. Note that the AC itself does not reset, but it places the specific WTP's context it is communicating with in the reset state: meaning that it clears all state associated with the WTP.

Configure to Reset (p): This state transition occurs if the configure phase fails.

WTP: The WTP enters this state when the reliable transport fails to deliver the Configure Request, or if the ResponseTimeout timer (see Section 12) expires.

AC: This state transition occurs if the AC is unable to transmit the Configure Response to a specific WTP. Note that the AC itself does not reset, but it places the specific WTP's context it is communicating with in the reset state: meaning that it clears all state associated with the WTP.

Configure to Run (q): This state transition occurs when the WTP and AC enter their normal state of operation.

WTP: The WTP enters this state when it receives a successful Configure Response from the AC. The WTP initializes the HeartBeat timer (see Section 12), and transmits the Change State Event Request message (see Section 7.6).

AC: This state transition occurs when the AC receives the Change State Event Request (see Section 7.6) from the WTP. The AC responds with a Change State Event Response (see Section 7.7) message. The AC must start the Session ID and NeighborDead timers (see Section 12).

Run to Run (r): This is the normal state of operation.

WTP: This is the WTP's normal state of operation, and there are many events that cause this to occur:

Configuration Update: The WTP receives a Configuration Update Request (see Section 7.4). The WTP MUST respond with a Configuration Update Response (see Section 7.5).

Change State Event: The WTP receives a Change State Event Response, or determines that it must initiate a Change State Event Request, as a result of a failure or change in the state of a radio.

Echo Request: The WTP receives an Echo Request message (Section 6.5), to which it MUST respond with an Echo Response (see Section 6.6).

Clear Config Indication: The WTP receives a Clear Config Indication message (Section 7.8). The WTP MUST reset its configuration back to manufacturer defaults.

WTP Event: The WTP generates a WTP Event Request to send information to the AC (Section 8.5). The WTP receives a WTP Event Response from the AC (Section 8.6).

Data Transfer: The WTP generates a Data Transfer Request to the AC (Section 8.7). The WTP receives a Data Transfer Response from the AC (Section 8.8).

WLAN Config Request: The WTP receives a WLAN Config Request message (Section 11.8.1), to which it MUST respond with a WLAN Config Response (see Section 11.8.2).

Mobile Config Request: The WTP receives an Mobile Config Request message (Section 9.1), to which it MUST respond with a Mobile Config Response (see Section 9.2).

AC: This is the AC's normal state of operation, and there are many events that cause this to occur:

Configuration Update: The AC sends a Configuration Update Request (see Section 7.4) to the WTP to update its configuration. The AC receives a Configuration Update Response (see Section 7.5) from the WTP.

Change State Event: The AC receives a Change State Event Request (see Section 7.6), to which it MUST respond with the Change State Event Response (see Section 7.7).

Echo: The AC sends an Echo Request message (Section 6.5) or receives the associated Echo Response (see Section 6.6) from the WTP.

Clear Config Indication: The AC sends a Clear Config Indication message (Section 7.8).

WLAN Config: The AC sends a WLAN Config Request message (Section 11.8.1) or receives the associated WLAN Config Response (see Section 11.8.2) from the WTP.

Mobile Config: The AC sends a Mobile Config Request message (Section 9.1) or receives the associated Mobile Config Response (see Section 9.2) from the WTP.

Data Transfer: The AC receives a Data Transfer Request from the AC (see Section 8.7) and MUST generate the associated Data Transfer Response message (see Section 8.8).

WTP Event: The AC receives a WTP Event Request from the AC (see Section 8.5) and MUST generate the associated WTP Event Response message (see Section 8.6).

Run to Reset (s): This event occurs when the AC wishes for the WTP to reboot.

WTP: The WTP enters this state when it receives a Reset Request (see Section 8.3). It must respond with a Reset Response (see Section 8.4), and once the reliable transport acknowledgement has been received, it must reboot itself.

AC: This state transition occurs either through some administrative action, or via some internal event on the AC that causes it to request that the WTP disconnect. Note that the AC itself does not reset, but it places the specific WTPs context it is communicating with in the reset state.

Run to Idle (t): This event occurs when an error occurs in the communication between the WTP and the AC.

WTP: The WTP enters this state when the underlying reliable transport is unable to transmit a message within the RetransmitInterval timer (see Section 12), and the maximum number of RetransmitCount counter has reached the MaxRetransmit variable (see Section 13).

AC: The AC enters this state when the underlying reliable transport in unable to transmit a message within the RetransmitInterval timer (see Section 12), and the maximum number of RetransmitCount counter has reached the MaxRetransmit variable (see Section 13).

Run to Key Update (u): This event occurs when the WTP and the AC are to exchange new keying material, with which it must use to protect all future messages.

WTP: This state transition occurs when the KeyLifetime timer expires (see Section 12).

AC: The WTP enters this state when it receives a Key Update Request (see Section 6.7).

Key Update to Key Confirm (w): This event occurs during the rekey phase and is used to complete the loop.

WTP: This state transition occurs when the WTP receives the Key Update Response. The WTP MUST only accept the message if it is authentic. The WTP responds to this response with a Key Update ACK.

AC: The AC enters this state when it receives an authenticated Key Update ACK message.

Key Confirm to Run (5): This event occurs when the rekey exchange phase is completed.

WTP: This state transition occurs when the WTP receives the Key Update Confirm. The newly derived encryption key and Initialization Vector (IV) must be plumbed into the crypto module after validating the message's authentication.

AC: The AC enters this state when it transmits the Key Update Confirm message. The newly derived encryption key and IV must be plumbed into the crypto module after transmitting a Key Update Confirm message.

Key Update to Reset (x): This event occurs when the key exchange phase times out.

WTP: This state transition occurs when the WTP does not receive a Key Update Response from the AC.

AC: The AC enters this state when it is unable to process a Key Update Request.

Reset to Idle (y): This event occurs when the state machine is restarted.

WTP: The WTP reboots itself. After rebooting, the WTP will start its LWAPP state machine in the Idle state.

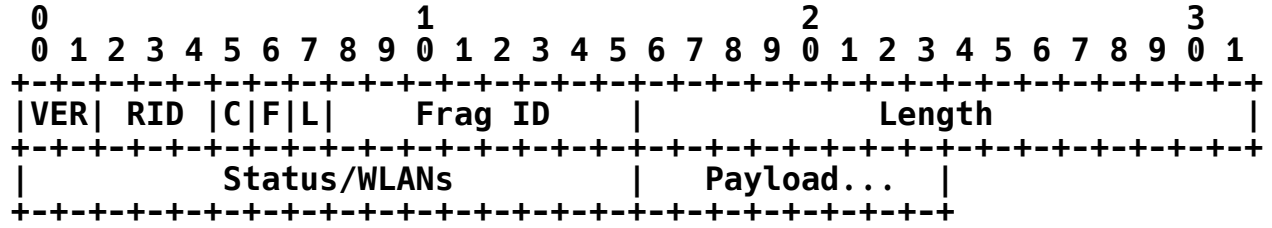
AC: The AC clears out any state associated with the WTP. The AC generally does this as a result of the reliable link layer timing out.

3. LWAPP Transport Layers

The LWAPP protocol can operate at Layer 2 or 3. For Layer 2 support, the LWAPP messages are carried in a native Ethernet frame. As such, the protocol is not routable and depends upon Layer 2 connectivity between the WTP and the AC. Layer 3 support is provided by encapsulating the LWAPP messages within UDP.

3.1. LWAPP Transport Header

All LWAPP protocol packets are encapsulated using a common header format, regardless of the transport used to carry the frames. However, certain flags are not applicable for a given transport, and it is therefore necessary to refer to the specific transport section in order to determine which flags are valid.



3.1.1. VER Field

A 2-bit field that contains the version of LWAPP used in this packet. The value for this document is 0.

3.1.2. RID Field

A 3-bit field that contains the Radio ID number for this packet. WTPs with multiple radios but a single MAC address use this field to indicate which radio is associated with the packet.

3.1.3. C Bit

The control message 'C' bit indicates whether this packet carries a data or control message. When this bit is zero (0), the packet carries an LWAPP data message in the payload (see Section 4.1). When this bit is one (1), the packet carries an LWAPP control message as defined in Section 4.2 for consumption by the addressed destination.

3.1.4. F Bit

The Fragment 'F' bit indicates whether this packet is a fragment. When this bit is one (1), the packet is a fragment and MUST be combined with the other corresponding fragments to reassemble the complete information exchanged between the WTP and AC.

3.1.5. L Bit

The Not Last '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 the WTP and AC. When this bit is 1, the packet is not the last fragment. When this bit is 0, the packet is the last fragment.

3.1.6. Fragment ID

An 8-bit field whose value is assigned to each group of fragments making up a complete set. The Fragment ID space is managed individually for every WTP/AC pair. 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 per frame.

3.1.7. Length

The 16-bit length field contains the number of bytes in the Payload. The field is encoded as an unsigned number. If the LWAPP packet is encrypted, the length field includes the Advanced Encryption Standard Counter with CBC-MAC (AES-CCM) MIC (see Section 10.2 for more information).

3.1.8. Status and WLANS

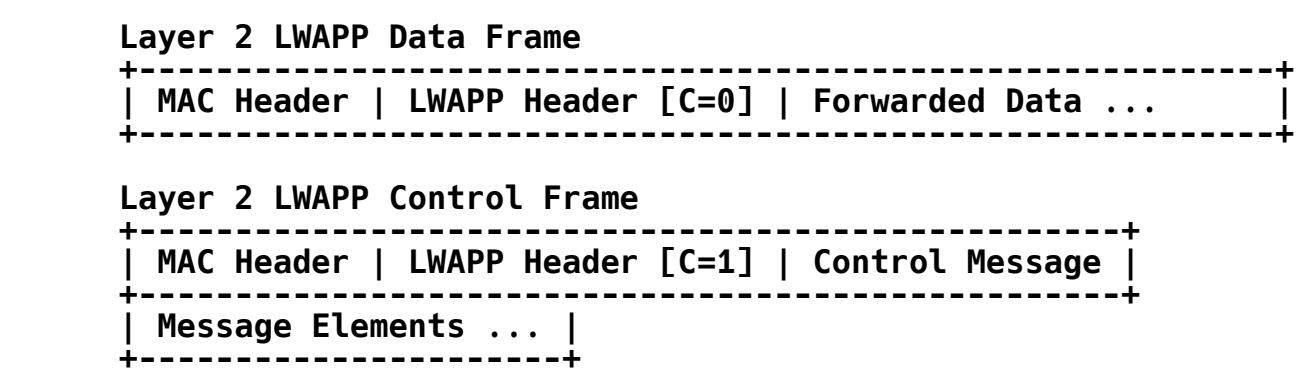
The interpretation of this 16-bit field is binding-specific. Refer to the transport portion of the binding for a wireless technology for the specification.

3.1.9. Payload

This field contains the header for an LWAPP data message or LWAPP control message, followed by the data associated with that message.

3.2. Using IEEE 802.3 MAC as LWAPP Transport

This section describes how the LWAPP protocol is provided over native Ethernet frames. An LWAPP packet is formed from the MAC frame header, followed by the LWAPP message header. The following figure provides an example of the frame formats used when LWAPP is used over the IEEE 802.3 transport.



3.2.1. Framing

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.

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.

Ethertype

The Ethertype field is set to 0x88bb.

3.2.2. AC Discovery

When run over IEEE 802.3, LWAPP messages are distributed to a specific MAC-level broadcast domain. The AC discovery mechanism used with this transport is for a WTP to transmit a Discovery Request message to a broadcast destination MAC address. The ACs will receive this message and reply based on their policy.

3.2.3. LWAPP Message Header Format over IEEE 802.3 MAC Transport

All of the fields described in Section 3.1 are used when LWAPP uses the IEEE 802.3 MAC transport.

3.2.4. Fragmentation/Reassembly

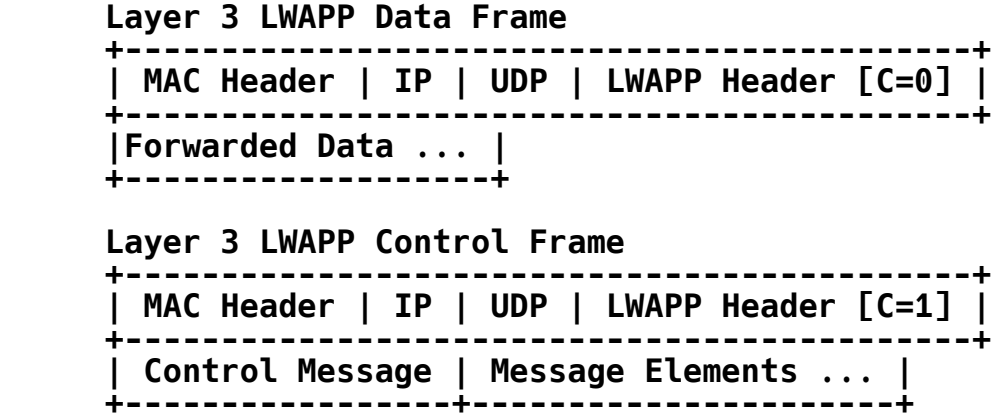
Fragmentation at the MAC layer is managed using the F, L, and Frag ID fields of the LWAPP message header. The LWAPP protocol only allows a single packet to be fragmented into 2, which is sufficient for a frame that exceeds MTU due to LWAPP encapsulation. When used with Layer 2 (Ethernet) transport, both fragments MUST include the LWAPP header.

3.2.5. Multiplexing

LWAPP control messages and data messages are distinguished by the 'C' bit in the LWAPP message header.

3.3. Using IP/UDP as LWAPP Transport

This section defines how LWAPP makes use of IP/UDP transport between the WTP and the AC. When this transport is used, the MAC layer is controlled by the IP stack, and there are therefore no special MAC-layer requirements. The following figure provides an example of the frame formats used when LWAPP is used over the IP/UDP transport. IP stacks can be either IPv4 or IPv6.



3.3.1. Framing

Communication between the WTP and AC is established according to the standard UDP client/server model. The connection is initiated by the WTP (client) to the well-known UDP port of the AC (server) used for control messages. This UDP port number of the AC is 12222 for LWAPP data and 12223 for LWAPP control frames.

3.3.2. AC Discovery

When LWAPP is run over routed IP networks, the WTP and the AC do not need to reside in the same IP subnet (broadcast domain). However, in the event the peers reside on separate subnets, there must exist a mechanism for the WTP to discover the AC.

As the WTP attempts to establish communication with the AC, it sends the Discovery Request message and receives the corresponding response message from the AC. The WTP must send the Discovery Request message to either the limited broadcast IP address (255.255.255.255), a well known multicast address, or the unicast IP address of the AC. Upon receipt of the message, the AC issues a Discovery Response message to the unicast IP address of the WTP, regardless of whether a Discovery Request was sent as a broadcast, multicast, or unicast message.

Whether the WTP uses a limited IP broadcast, multicast or unicast IP address is implementation-dependent.

In order for a WTP to transmit a Discovery Request to a unicast address, the WTP must first obtain the IP address of the AC. Any static configuration of an AC's IP address on the WTP non-volatile storage is implementation-dependent. However, additional dynamic schemes are possible: for example:

DHCP: A comma-delimited, ASCII-encoded list of AC IP addresses is embedded inside a DHCP vendor-specific option 43 extension. An example of the actual format of the vendor-specific payload for IPv4 is of the form "10.1.1.1, 10.1.1.2".

DNS: The DNS name "LWAPP-AC-Address" MAY be resolvable to one or more AC addresses.

3.3.3. LWAPP Message Header Format over IP/UDP Transport

All of the fields described in Section 3.1 are used when LWAPP uses the IPv4/UDP or IPv6/UDP transport, with the following exceptions.

3.3.3.1. F Bit

This flag field is not used with this transport, and MUST be set to zero.

3.3.3.2. L Bit

This flag field is not used with this transport, and MUST be set to zero.

3.3.3.3. Frag ID

This field is not used with this transport, and MUST be set to zero.

3.3.4. Fragmentation/Reassembly for IPv4

When LWAPP is implemented at L3, the transport layer uses IP fragmentation to fragment and reassemble LWAPP messages that are longer than the MTU size used by either the WTP or AC. The details of IP fragmentation are covered in [8]. When used with the IP transport, only the first fragment would include the LWAPP header.

3.3.5. Fragmentation/Reassembly for IPv6

IPv6 does MTU discovery so fragmentation and re-assembly is not necessary for UDP packets.

3.3.6. Multiplexing

LWAPP messages convey control information between WTP and AC, as well as binding specific data frames or binding specific management frames. As such, LWAPP messages need to be multiplexed in the transport sub-layer and be delivered to the proper software entities in the endpoints of the protocol. However, the 'C' bit is still used to differentiate between data and control frames.

In case of Layer 3 connection, multiplexing is achieved by use of different UDP ports for control and data packets (see Section 3.3.1).

As part of the Join procedure, the WTP and AC may negotiate different IP Addresses for data or control messages. The IP address returned in the AP Manager Control IP Address message element is used to inform the WTP with the IP address to which it must send all control frames. The AP Manager Data IP Address message element MAY be present only if the AC has a different IP address that the WTP is to use to send its data LWAPP frames.

In the event the WTP and AC are separated by a NAT, with the WTP using private IP address space, it is the responsibility of the NAT to manage appropriate UDP port mapping.

4. LWAPP Packet Definitions

This section contains the packet types and format. The LWAPP protocol is designed to be transport-agnostic by specifying packet formats for both MAC frames and IP packets. An LWAPP packet consists of an LWAPP Transport Layer packet header followed by an LWAPP message.

Transport details can be found in Section 3.

4.1. LWAPP Data Messages

An LWAPP data message is a forwarded wireless frame. When forwarding wireless frames, the sender simply encapsulates the wireless frame in an LWAPP data packet, using the appropriate transport rules defined in Section 3.

In the event that the encapsulated frame would exceed the transport layer's MTU, the sender is responsible for the fragmentation of the frame, as specified in the transport-specific section of Section 3.

The actual format of the encapsulated LWAPP data frame is subject to the rules defined under the specific wireless technology binding.

4.2. LWAPP Control Messages Overview

The LWAPP Control protocol provides a control channel between the WTP and the AC. The control channel is the series of control messages between the WTP and AC, associated with a session ID and key. Control messages are divided into the following distinct message types:

Discovery: LWAPP Discovery messages are used to identify potential ACs, their load and capabilities.

Control Channel Management: Messages that fall within this classification are used for the discovery of ACs by the WTPs as well as the establishment and maintenance of an LWAPP control channel.

WTP Configuration: The WTP Configuration messages are used by the AC to push a specific configuration to the WTPs with which it has a control channel. Messages that deal with the retrieval of statistics from the WTP also fall in this category.

Mobile Session Management: Mobile Session Management messages are used by the AC to push specific mobile policies to the WTP.

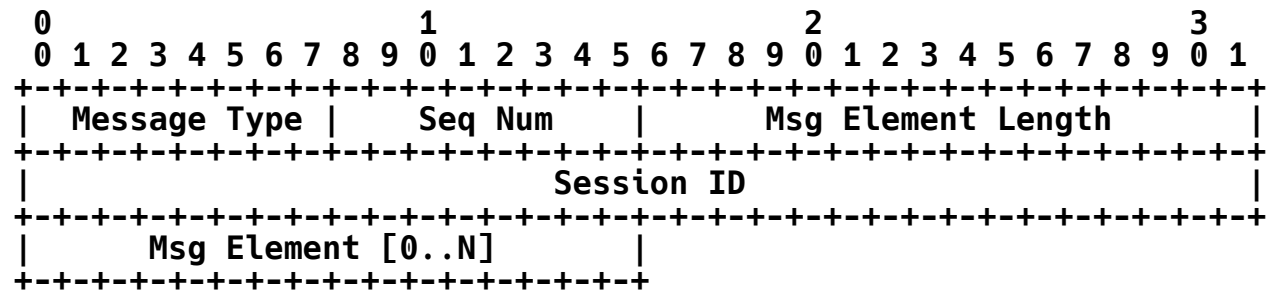
Firmware Management: Messages in this category are used by the AC to push a new firmware image down to the WTP.

Control Channel, WTP Configuration, and Mobile Session Management MUST be implemented. Firmware Management MAY be implemented.

In addition, technology-specific bindings may introduce new control channel commands that depart from the above list.

4.2.1. Control Message Format

All LWAPP control messages are sent encapsulated within the LWAPP header (see Section 3.1). Immediately following the header is the LWAPP control header, which has the following format:



4.2.1.1. Message Type

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

Description	Value
Discovery Request	1
Discovery Response	2
Join Request	3
Join Response	4
Join ACK	5
Join Confirm	6
Unused	7-9
Configure Request	10
Configure Response	11
Configuration Update Request	12
Configuration Update Response	13
WTP Event Request	14
WTP Event Response	15
Change State Event Request	16
Change State Event Response	17
Unused	18-21
Echo Request	22
Echo Response	23
Image Data Request	24
Image Data Response	25
Reset Request	26
Reset Response	27
Unused	28-29
Key Update Request	30
Key Update Response	31
Primary Discovery Request	32

Primary Discovery Response	33
Data Transfer Request	34
Data Transfer Response	35
Clear Config Indication	36
WLAN Config Request	37
WLAN Config Response	38
Mobile Config Request	39
Mobile Config Response	40

4.2.1.2. 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.

When an LWAPP control frame is sent, its internal sequence number counter is monotonically incremented, ensuring that no two requests pending have the same sequence number. This field will wrap back to zero.

4.2.1.3. Message Element Length

The length field indicates the number of bytes following the Session ID field. If the LWAPP packet is encrypted, the length field includes the AES-CCM MIC (see Section 10.2 for more information).

4.2.1.4. Session ID

The Session ID is a 32-bit unsigned integer that is used to identify the security context for encrypted exchanges between the WTP and the AC. Note that a Session ID is a random value that MUST be unique between a given AC and any of the WTPs with which it may be communicating.

4.2.1.5. Message Element [0..N]

The message element(s) carry the information pertinent to each of the control message types. Every control message in this specification specifies which message elements are permitted.

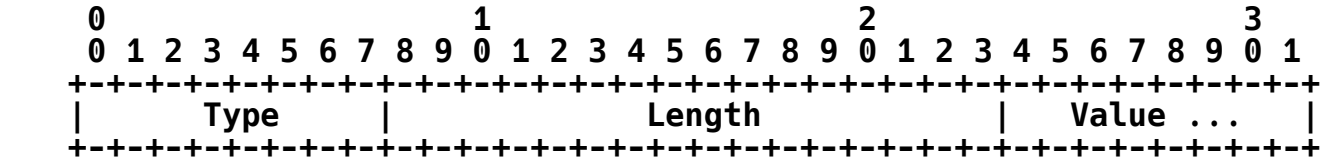
4.2.2. Message Element Format

The message element is used to carry information pertinent to a control message. Every message element is identified by the Type field, whose numbering space is managed via IANA (see Section 16). The total length of the message elements is indicated in the Message Element Length field.

All of the message element definitions in this document use a diagram similar to the one below in order to depict their formats. Note that in order to simplify this specification, these diagrams do not include the header fields (Type and Length). However, in each message element description, the header's field values will be defined.

Note that additional message elements may be defined in separate IETF documents.

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



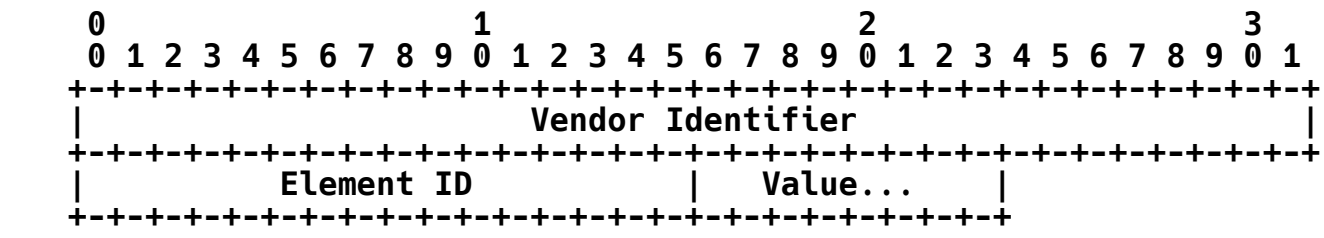
where Type (8 bits) identifies the character of the information carried in the Value field and Length (16 bits) indicates the number of bytes in the Value field.

4.2.2.1. Generic Message Elements

This section includes message elements that are not bound to a specific control message.

4.2.2.1.1. Vendor Specific

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



Type: 104 for Vendor Specific

Length: >= 7

Vendor Identifier: A 32-bit value containing the IANA-assigned "SMI Network Management Private Enterprise Codes" [13].

Element ID: A 16-bit Element Identifier that is managed by the vendor.

Value: The value associated with the vendor-specific element.

4.2.3. Quality of Service

It is recommended that LWAPP control messages be sent by both the AC and the WTP with an appropriate Quality-of-Service precedence value, ensuring that congestion in the network minimizes occurrences of LWAPP control channel disconnects. Therefore, a Quality-of-Service-enabled LWAPP device should use:

802.1P: The precedence value of 7 SHOULD be used.

DSCP: The Differentiated Services Code Point (DSCP) tag value of 46 SHOULD be used.

5. LWAPP Discovery Operations

The Discovery messages are used by a WTP to determine which ACs are available to provide service, as well as the capabilities and load of the ACs.

5.1. Discovery Request

The Discovery Request is used by the WTP to automatically discover potential ACs available in the network. A WTP must transmit this command even if it has a statically configured AC, as it is a required step in the LWAPP state machine.

Discovery Requests MUST be sent by a WTP in the Discover state after waiting for a random delay less of than MaxDiscoveryInterval, after a WTP first comes up or is (re)initialized. A WTP 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 WTP Discoveries. An example of this occurring would be when many WTPs are powered on at the same time.

Discovery Requests MUST be sent by a WTP when no Echo Responses are received for NeighborDeadInterval and the WTP returns to the Idle state. Discovery Requests are sent after NeighborDeadInterval, they MUST be sent after waiting for a random delay less than

MaxDiscoveryInterval. A WTP 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 WTP enters the Sulking state and MUST wait for an interval equal to SilentInterval before sending further Discovery Requests.

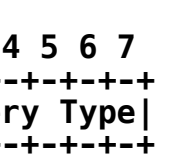
The Discovery Request message may be sent as a unicast, broadcast, or multicast message.

Upon receiving a Discovery Request, the AC will respond with a Discovery Response sent to the address in the source address of the received Discovery Request.

The following subsections define the message elements that MUST be included in this LWAPP operation.

5.1.1. Discovery Type

The Discovery message element is used to configure a WTP to operate in a specific mode.



Type: 58 for Discovery Type

Length: 1

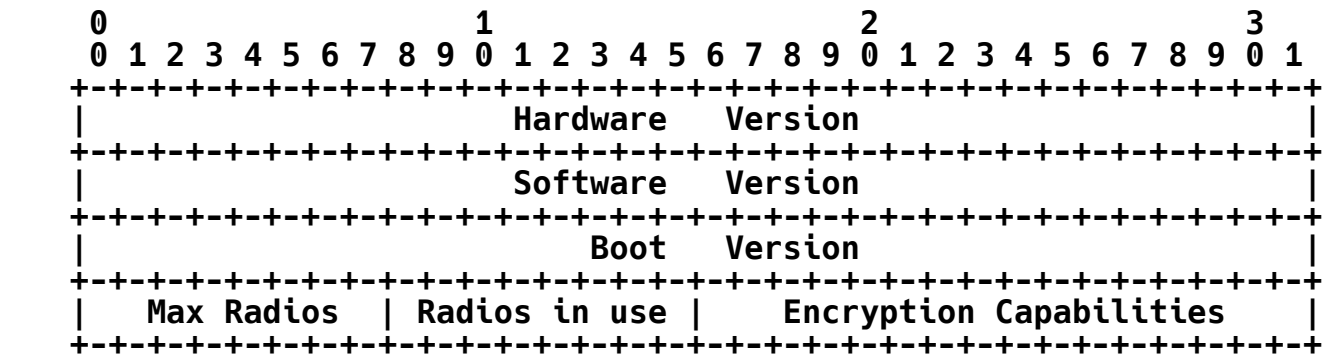
Discovery Type: An 8-bit value indicating how the AC was discovered. The following values are supported:

0 - Broadcast

1 - Configured

5.1.2. WTP Descriptor

The WTP Descriptor message element is used by the WTP to communicate its current hardware/firmware configuration. The value contains the following fields.



Type: 3 for WTP Descriptor

Length: 16

Hardware Version: A 32-bit integer representing the WTP's hardware version number.

Software Version: A 32-bit integer representing the WTP's Firmware version number.

Boot Version: A 32-bit integer representing the WTP's boot loader's version number.

Max Radios: An 8-bit value representing the number of radios (where each radio is identified via the RID field) supported by the WTP.

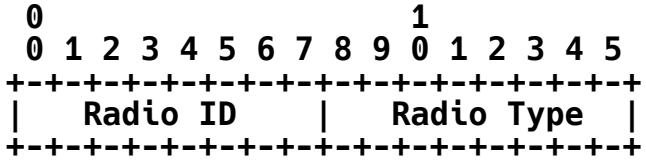
Radios in Use: An 8-bit value representing the number of radios present in the WTP.

Encryption Capabilities: This 16-bit field is used by the WTP to communicate its capabilities to the AC. Since most WTPs support link-layer encryption, the AC may make use of these services. There are binding-dependent encryption capabilites. A WTP that does not have any encryption capabilities would set this field to zero (0). Refer to the specific binding for the specification.

5.1.3. WTP Radio Information

The WTP Radio Information message element is used to communicate the radio information in a specific slot. The Discovery Request MUST include one such message element per radio in the WTP. The Radio-Type field is used by the AC in order to determine which technology-specific binding is to be used with the WTP.

The value contains two fields, as shown:



Type: 4 for WTP Radio Information

Length: 2

Radio ID: The Radio Identifier, typically refers to some interface index on the WTP.

Radio Type: The type of radio present. The following values are supported:

1 - 802.11bg: An 802.11bg radio.

2 - 802.11a: An 802.11a radio.

3 - 802.16: An 802.16 radio.

4 - Ultra Wideband: A UWB radio.

7 - all: Used to specify all radios in the WTP.

5.2. Discovery Response

The Discovery Response is a mechanism by which an AC advertises its services to requesting WTPs.

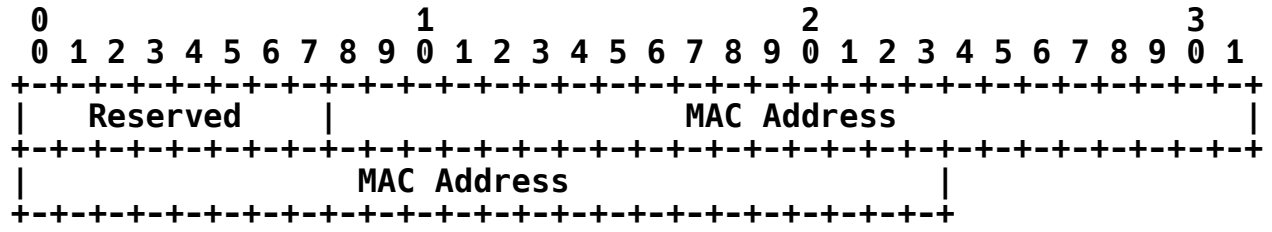
Discovery Responses are sent by an AC after receiving a Discovery Request.

When a WTP receives a Discovery Response, it MUST wait for an interval not less than DiscoveryInterval for receipt of additional Discovery Responses. After the DiscoveryInterval elapses, the WTP enters the Joining state and will select one of the ACs that sent a Discovery Response and send a Join Request to that AC.

The following subsections define the message elements that MUST be included in this LWAPP operation.

5.2.1. AC Address

The AC Address message element is used to communicate the identity of the AC. The value contains two fields, as shown:



Type: 2 for AC Address

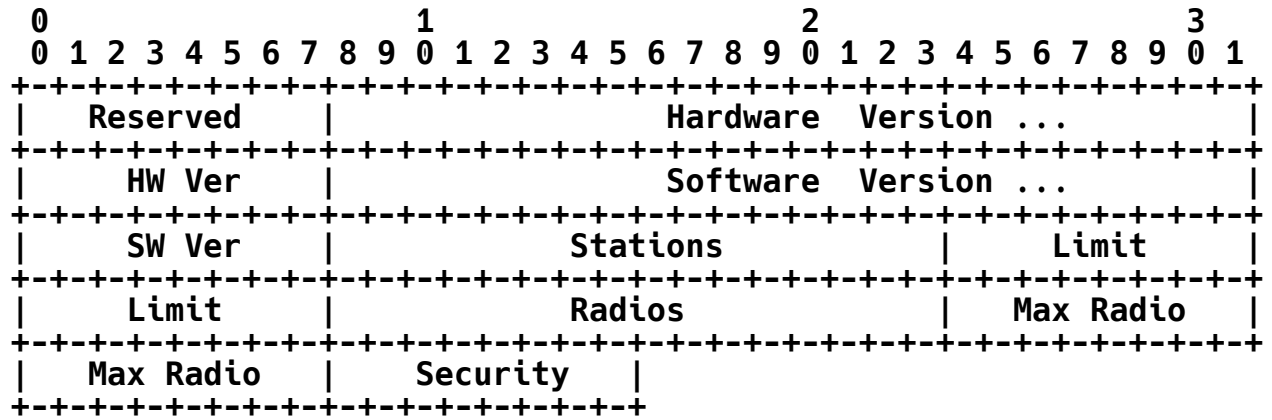
Length: 7

Reserved: MUST be set to zero

MAC Address: The MAC address of the AC

5.2.2. AC Descriptor

The AC Descriptor message element is used by the AC to communicate its current state. The value contains the following fields:



Type: 6 for AC Descriptor

Length: 17

Reserved: MUST be set to zero

Hardware Version: A 32-bit integer representing the AC's hardware version number.

Software Version: A 32-bit integer representing the AC's Firmware version number.

Stations: A 16-bit integer representing the number of mobile stations currently associated with the AC.

Limit: A 16-bit integer representing the maximum number of stations supported by the AC.

Radios: A 16-bit integer representing the number of WTPs currently attached to the AC.

Max Radio: A 16-bit integer representing the maximum number of WTPs supported by the AC.

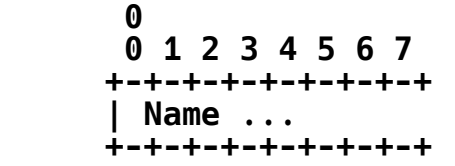
Security: An 8-bit bitmask specifying the security schemes supported by the AC. The following values are supported (see Section 10):

1 - X.509 Certificate-Based

2 - Pre-Shared Secret

5.2.3. AC Name

The AC Name message element contains an ASCII representation of the AC's identity. The value is a variable-length byte string. The string is NOT zero terminated.



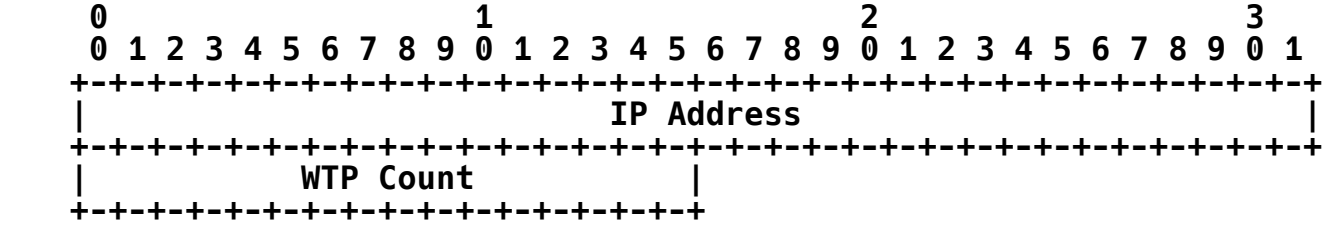
Type: 31 for AC Name

Length: > 0

Name: A variable-length ASCII string containing the AC's name.

5.2.4. WTP Manager Control IPv4 Address

The WTP Manager Control IPv4 Address message element is sent by the AC to the WTP during the discovery process and is used by the AC to provide the interfaces available on the AC, and their current load. This message element is useful for the WTP to perform load balancing across multiple interfaces.



Type: 99 for WTP Manager Control IPv4 Address

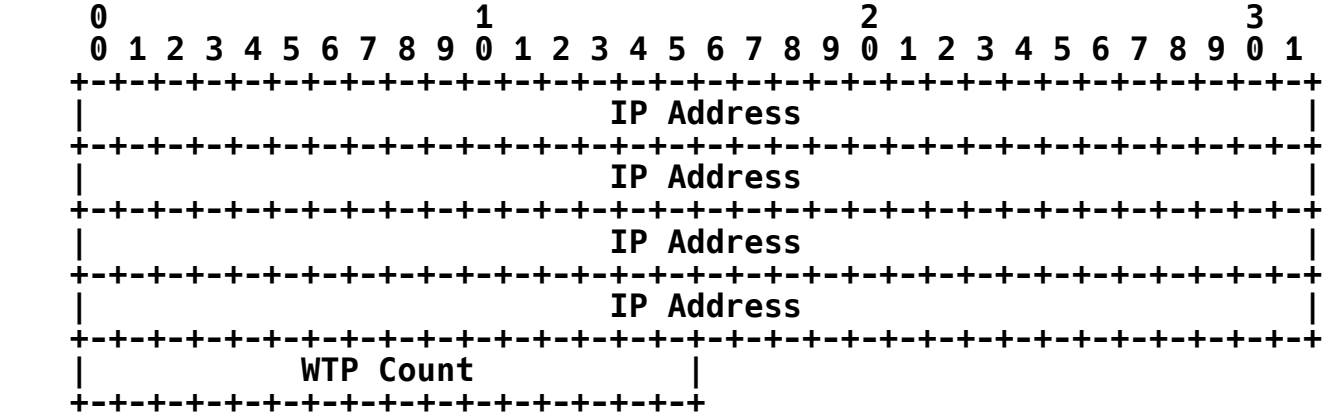
Length: 6

IP Address: The IP address of an interface.

WTP Count: The number of WTPs currently connected to the interface.

5.2.5. WTP Manager Control IPv6 Address

The WTP Manager Control IPv6 Address message element is sent by the AC to the WTP during the discovery process and is used by the AC to provide the interfaces available on the AC, and their current load. This message element is useful for the WTP to perform load balancing across multiple interfaces.



Type: 137 for WTP Manager Control IPv6 Address

Length: 6

IP Address: The IP address of an interface.

WTP Count: The number of WTPs currently connected to the interface.

5.3. Primary Discovery Request

The Primary Discovery Request is sent by the WTP in order to determine whether its preferred (or primary) AC is available.

Primary Discovery Requests are sent by a WTP when it has a primary AC configured, and is connected to another AC. This generally occurs as a result of a failover, and is used by the WTP as a means to discover when its primary AC becomes available. As a consequence, this message is only sent by a WTP when it is in the Run state.

The frequency of the Primary Discovery Requests should be no more often than the sending of the Echo Request message.

Upon receiving a Discovery Request, the AC will respond with a Primary Discovery Response sent to the address in the source address of the received Primary Discovery Request.

The following subsections define the message elements that MUST be included in this LWAPP operation.

5.3.1. Discovery Type

The Discovery Type message element is defined in Section 5.1.1.

5.3.2. WTP Descriptor

The WTP Descriptor message element is defined in Section 5.1.2.

5.3.3. WTP Radio Information

A WTP Radio Information message element must be present for every radio in the WTP. This message element is defined in Section 5.1.3.

5.4. Primary Discovery Response

The Primary Discovery Response is a mechanism by which an AC advertises its availability and services to requesting WTPs that are configured to have the AC as its primary AC.

Primary Discovery Responses are sent by an AC after receiving a Primary Discovery Request.

When a WTP receives a Primary Discovery Response, it may opt to establish an LWAPP connection to its primary AC, based on the configuration of the WTP Fallback Status message element on the WTP.

The following subsections define the message elements that MUST be included in this LWAPP operation.

5.4.1. AC Descriptor

The Discovery Type message element is defined in Section 5.2.2.

5.4.2. AC Name

The AC Name message element is defined in Section 5.2.3.

5.4.3. WTP Manager Control IPv4 Address

A WTP Radio Information message element MAY be present for every radio in the WTP that is reachable via IPv4. This message element is defined in Section 5.2.4.

5.4.4. WTP Manager Control IPv6 Address

A WTP Radio Information message element must be present for every radio in the WTP that is reachable via IPv6. This message element is defined in Section 5.2.5.

6. Control Channel Management

The Control Channel Management messages are used by the WTP and AC to create and maintain a channel of communication on which various other commands may be transmitted, such as configuration, firmware update, etc.

6.1. Join Request

The Join Request is used by a WTP to inform an AC that it wishes to provide services through it.

Join Requests are sent by a WTP in the Joining state after receiving one or more Discovery Responses. The Join Request is also used as an MTU discovery mechanism by the WTP. The WTP issues a Join Request with a Test message element, bringing the total size of the message to exceed MTU.

If the transport used does not provide MTU path discovery, the initial Join Request is padded with the Test message element to 1596 bytes. If a Join Response is received, the WTP can forward frames without requiring any fragmentation. If no Join Response is received, it issues a second Join Request padded with the Test payload to a total of 1500 bytes. The WTP continues to cycle from large (1596) to small (1500) packets until a Join Response has been received, or until both packets' sizes have been retransmitted 3 times. If the Join Response is not received after the maximum number of retransmissions, the WTP MUST abandon the AC and restart the discovery phase.

When an AC receives a Join Request, it will respond with a Join Response. If the certificate-based security mechanism is used, the AC validates the certificate found in the request. If valid, the AC generates a session key that will be used to secure the control frames it exchanges with the WTP. When the AC issues the Join Response, the AC creates a context for the session with the WTP.

If the pre-shared session key security mechanism is used, the AC saves the WTP's nonce, found in the WNonce message element, and creates its own nonce, which it includes in the ANonce message element. Finally, the AC creates the PSK-MIC, which is computed using a key that is derived from the PSK.

A Join Request that includes both a WNonce and a Certificate message element MUST be considered invalid.

Details on the key generation are found in Section 10.

The following subsections define the message elements that MUST be included in this LWAPP operation.

6.1.1. WTP Descriptor

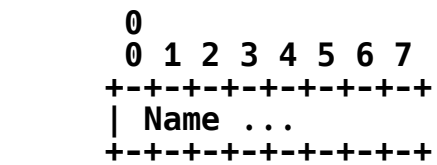
The WTP Descriptor message element is defined in Section 5.1.2.

6.1.2. AC Address

The AC Address message element is defined in Section 5.2.1.

6.1.3. WTP Name

The WTP Name message element value is a variable-length byte string. The string is NOT zero terminated.



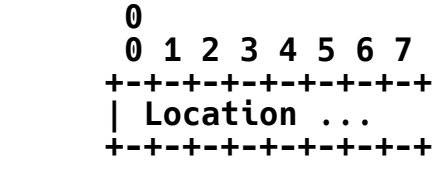
Type: 5 for WTP Name

Length: > 0

Name: A non-zero-terminated string containing the WTP's name.

6.1.4. 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.



Type: 35 for Location Data

Length: > 0

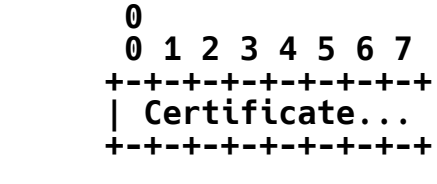
Location: A non-zero-terminated string containing the WTP's location.

6.1.5. WTP Radio Information

A WTP Radio Information message element must be present for every radio in the WTP. This message element is defined in Section 5.1.3.

6.1.6. Certificate

The Certificate message element value is a byte string containing a DER-encoded x.509v3 certificate. This message element is only included if the LWAPP security type used between the WTP and the AC makes use of certificates (see Section 10 for more information).



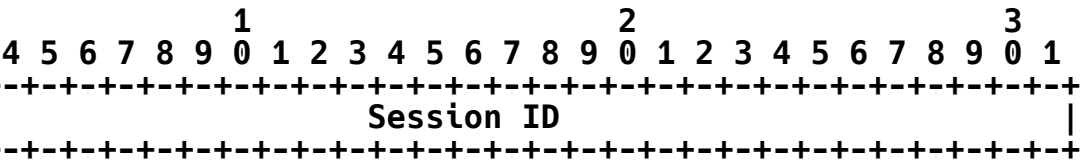
Type: 44 for Certificate

Length: > 0

Certificate: A non-zero-terminated string containing the device's certificate.

6.1.7. Session ID

The Session ID message element value contains a randomly generated [4] unsigned 32-bit integer.



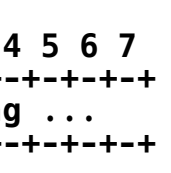
Type: 45 for Session ID

Length: 4

Session ID: 32-bit random session identifier.

6.1.8. Test

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



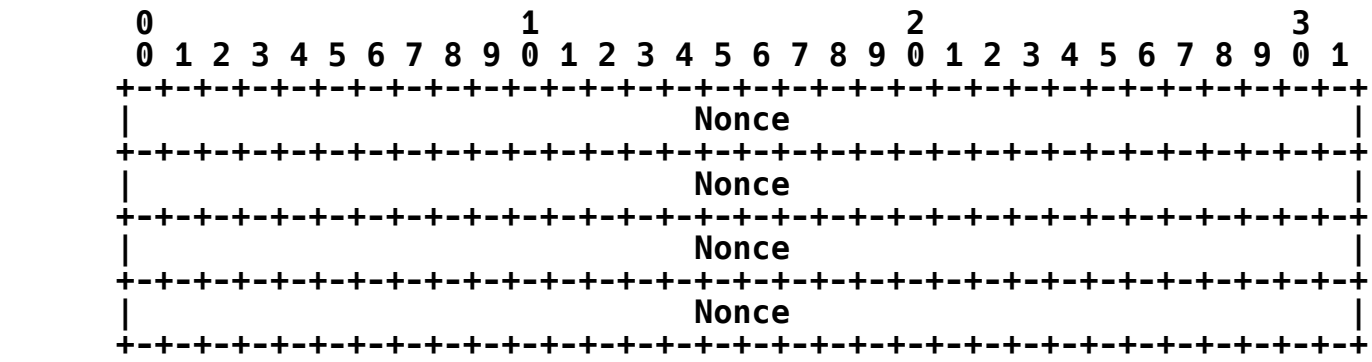
Type: 18 for Test

Length: > 0

Padding: A variable-length pad.

6.1.9. XNonce

The XNonce is used by the WTP to communicate its random nonce during the join or rekey phase. See Section 10 for more information.



Type: 111 for XNonce

Length: 16

Nonce: 1 16-octet random nonce.

6.2. Join Response

The Join Response is sent by the AC to indicate to a WTP whether it is capable and willing to provide service to it.

Join Responses are sent by the AC after receiving a Join Request. Once the Join Response has been sent, the Heartbeat timer is initiated for the session to EchoInterval. Expiration of the timer will result in deletion of the AC-WTP session. The timer is refreshed upon receipt of the Echo Request.

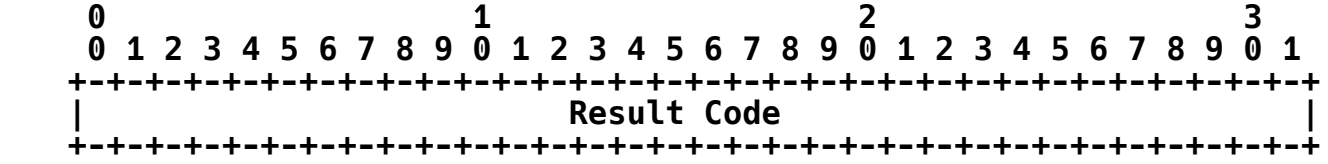
If the security method used is certificate-based, when a WTP receives a Join Response, it enters the Joined state and initiates either a Configure Request or Image Data to the AC to which it is now joined. Upon entering the Joined state, the WTP begins timing an interval equal to NeighborDeadInterval. Expiration of the timer will result in the transmission of the Echo Request.

If the security method used is pre-shared-secret-based, when a WTP receives a Join Response that includes a valid PSK-MIC message element, it responds with a Join ACK that also MUST include a locally computed PSK-MIC message element.

The following subsections define the message elements that MUST be included in this LWAPP operation.

6.2.1. 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. The Result Code is included in a successful Join Response.



Type: 2 for Result Code

Length: 4

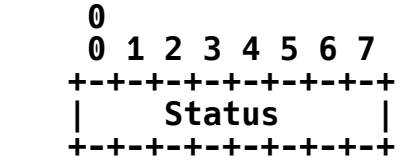
Result Code: The following values are defined:

0 Success

1 Failure (AC List message element MUST be present)

6.2.2. Status

The Status message element is sent by the AC to the WTP in a non-successful Join Response message. This message element is used to indicate the reason for the failure and should only be accompanied with a Result Code message element that indicates a failure.



Type: 60 for Status

Length: 1

Status: The Status field indicates the reason for an LWAPP failure. The following values are supported:

1 - Reserved - do not use

2 - Resource Depletion

3 - Unknown Source

4 - Incorrect Data

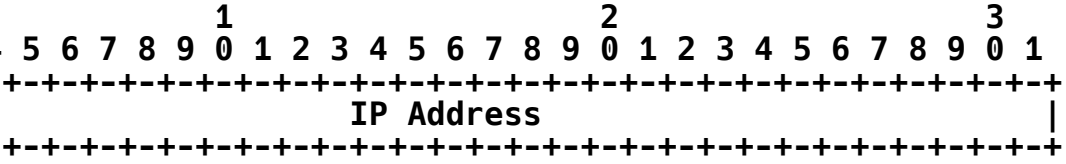
6.2.3. Certificate

The Certificate message element is defined in Section 6.1.6. Note this message element is only included if the WTP and the AC make use of certificate-based security as defined in Section 10.

6.2.4. WTP Manager Data IPv4 Address

The WTP Manager Data IPv4 Address message element is optionally sent by the AC to the WTP during the join phase. If present, the IP Address contained in this message element is the address the WTP is to use when sending any of its LWAPP data frames.

Note that this message element is only valid when LWAPP uses the IP/UDP Layer 3 transport.



Type: 138 for WTP Manager Data IPv4 Address

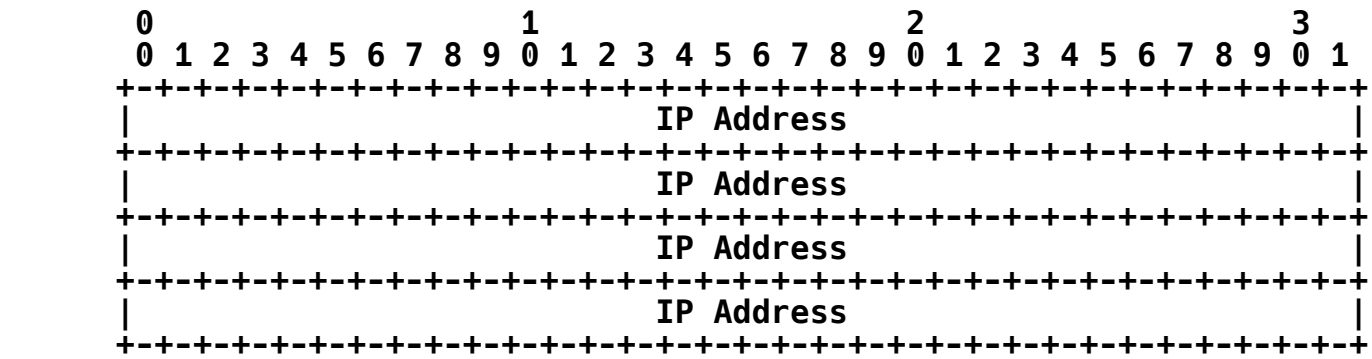
Length: 4

IP Address: The IP address of an interface.

6.2.5. WTP Manager Data IPv6 Address

The WTP Manager Data IPv6 Address message element is optionally sent by the AC to the WTP during the join phase. If present, the IP Address contained in this message element is the address the WTP is to use when sending any of its LWAPP data frames.

Note that this message element is only valid when LWAPP uses the IP/UDP Layer 3 transport.



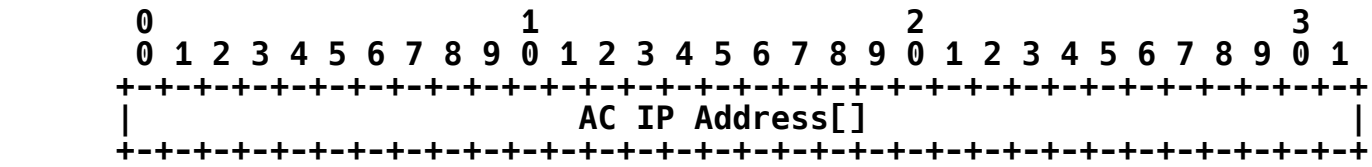
Type: 139 for WTP Manager Data IPv6 Address

Length: 4

IP Address: The IP address of an interface.

6.2.6. AC IPv4 List

The AC List message element is used to configure a WTP with the latest list of ACs in a cluster. This message element MUST be included if the Join Response returns a failure indicating that the AC cannot handle the WTP at this time, allowing the WTP to find an alternate AC to which to connect.



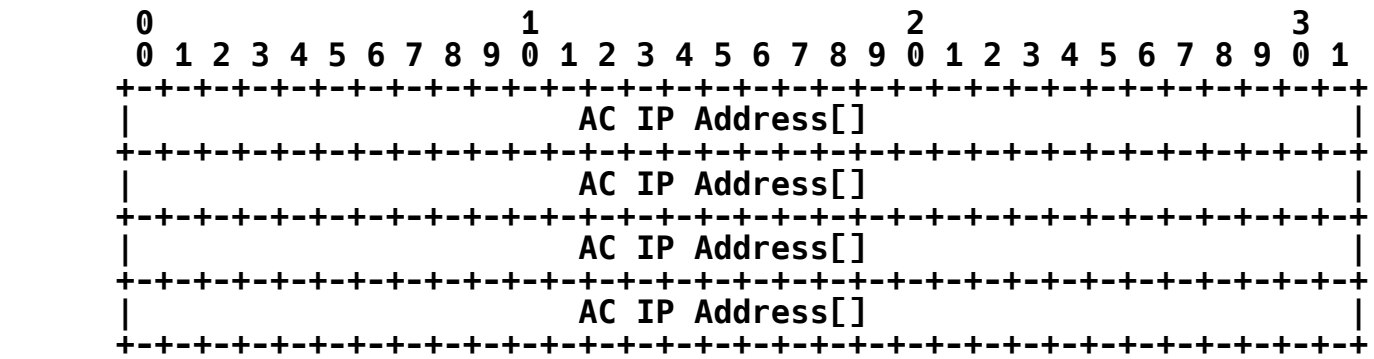
Type: 59 for AC List

Length: >= 4

AC IP Address: An array of 32-bit integers containing an AC's IPv4 Address.

6.2.7. AC IPv6 List

The AC List message element is used to configure a WTP with the latest list of ACs in a cluster. This message element MUST be included if the Join Response returns a failure indicating that the AC cannot handle the WTP at this time, allowing the WTP to find an alternate AC to which to connect.



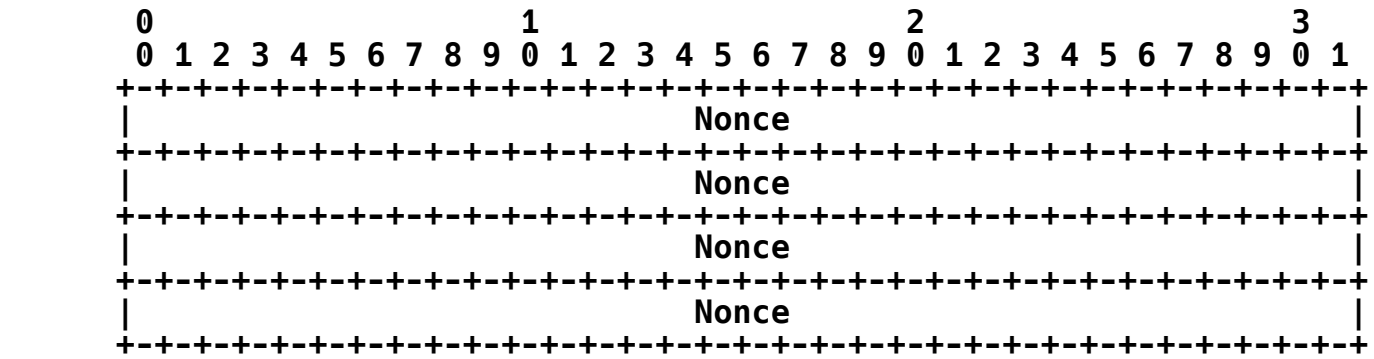
Type: 141 for AC List

Length: >= 4

AC IP Address: An array of 32-bit integers containing an AC's IPv6 Address.

6.2.8. ANonce

The ANonce message element is sent by an AC during the join or rekey phase. The contents of the ANonce are encrypted as described in Section 10 for more information.



Type: 108 for ANonce

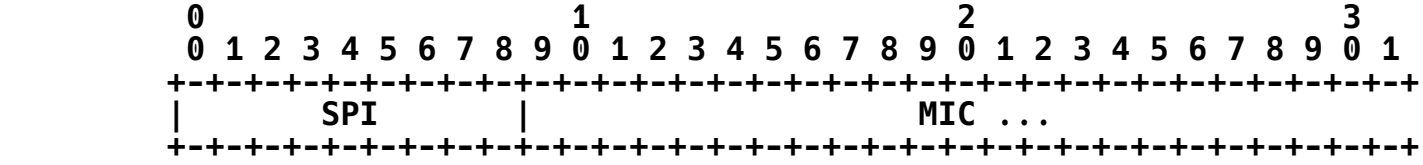
Length: 16

Nonce: An encrypted, 16-octet random nonce.

6.2.9. PSK-MIC

The PSK-MIC message element includes a message integrity check, whose purpose is to provide confirmation to the peer that the sender has the proper session key. This message element is only included if the security method used between the WTP and the AC is the pre-shared secret mechanism. See Section 10 for more information.

When present, the PSK-MIC message element MUST be the last message element in the message. The MIC is computed over the complete LWAPP packet, from the LWAPP control header as defined in Section 4.2.1 to the end of the packet (which MUST be this PSK-MIC message element). The MIC field in this message element and the Sequence Number field in the LWAPP control header MUST be set to zeroes prior to computing the MIC. The length field in the LWAPP control header must already include this message element prior to computing the MIC.



Type: 109 for PSK-MIC

Length: > 1

SPI: The Security Parameter Index (SPI) field specifies the cryptographic algorithm used to create the message integrity check. The following values are supported:

0 - Unused

1 - HMAC-SHA-1 (RFC 2104 [15])

MIC: A 20-octet Message Integrity Check.

6.3. Join ACK

The Join ACK message is sent by the WTP upon receiving a Join Response, which has a valid PSK-MIC message element, as a means of providing key confirmation to the AC. The Join ACK is only used in the case where the WTP makes use of the pre-shared key LWAPP mode (see Section 10 for more information).

Note that the AC should never receive this message unless the security method used between the WTP and the AC is pre-shared-secret-based.

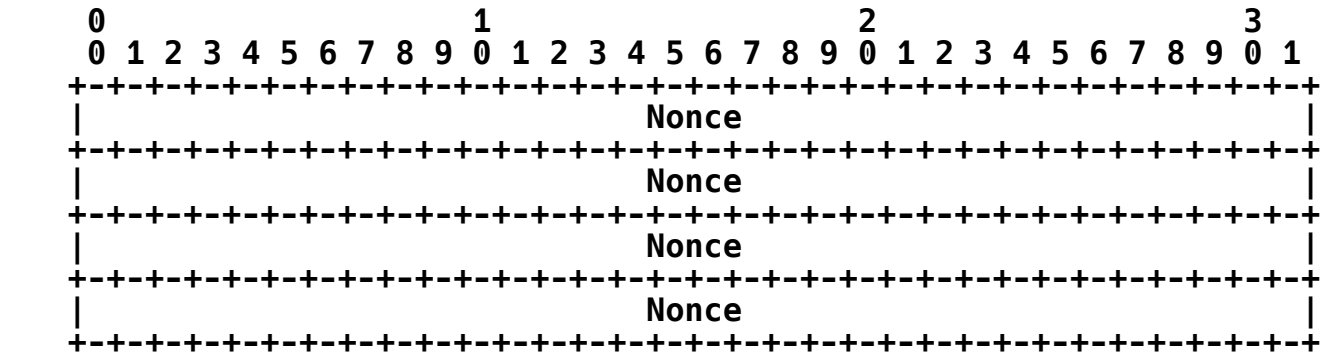
The following subsections define the message elements that MUST be included in this LWAPP operation.

6.3.1. Session ID

The Session ID message element is defined in Section 6.1.7.

6.3.2. WNonce

The WNonce message element is sent by a WTP during the join or rekey phase. The contents of the ANonce are encrypted as described in Section 10 for more information.



Type: 107 for WNonce

Length: 16

Nonce: An encrypted, 16-octet random nonce.

6.3.3. PSK-MIC

The PSK-MIC message element is defined in Section 6.2.9.

6.4. Join Confirm

The Join Confirm message is sent by the AC upon receiving a Join ACK, which has a valid PSK-MIC message element, as a means of providing key confirmation to the WTP. The Join Confirm is only used in the case where the WTP makes use of the pre-shared key LWAPP mode (see Section 10 for more information).

If the security method used is pre-shared-key-based, when a WTP receives a Join Confirm, it enters the Joined state and initiates either a Configure Request or Image Data to the AC to which it is now

joined. Upon entering the Joined state, the WTP begins timing an interval equal to NeighborDeadInterval. Expiration of the timer will result in the transmission of the Echo Request.

This message is never received, or sent, when the security type used between the WTP and the AC is certificated-based.

The following subsections define the message elements that MUST be included in this LWAPP operation.

6.4.1. Session ID

The Session ID message element is defined in Section 6.1.7.

6.4.2. PSK-MIC

The PSK-MIC message element is defined in Section 6.2.9.

6.5. Echo Request

The Echo Request message is a keepalive mechanism for the LWAPP control message.

Echo Requests are sent periodically by a WTP in the Run state (see Figure 2) to determine the state of the connection between the WTP and the AC. The Echo Request is sent by the WTP when the Heartbeat timer expires, and it MUST start its NeighborDeadInterval timer.

The Echo Request carries no message elements.

When an AC receives an Echo Request, it responds with an Echo Response.

6.6. Echo Response

The Echo Response acknowledges the Echo Request, and is only accepted while in the Run state (see Figure 2).

Echo Responses are sent by an AC after receiving an Echo Request. After transmitting the Echo Response, the AC should reset its Heartbeat timer to expire in the value configured for EchoInterval. If another Echo request is not received by the AC when the timer expires, the AC SHOULD consider the WTP to no longer be reachable.

The Echo Response carries no message elements.

When a WTP receives an Echo Response it stops the NeighborDeadInterval timer, and starts the Heartbeat timer to EchoInterval.

If the NeighborDeadInterval timer expires prior to receiving an Echo Response, the WTP enters the Idle state.

6.7. Key Update Request

The Key Update Request is used by the WTP to initiate the rekeying phase. This message is sent by a WTP when in the Run state and MUST include a new unique Session Identifier. This message MUST also include a unique nonce in the XNonce message element, which is used to protect against replay attacks (see Section 10).

The following subsections define the message elements that MUST be included in this LWAPP operation.

6.7.1. Session ID

The Session ID message element is defined in Section 6.1.7.

6.7.2. XNonce

The XNonce message element is defined in Section 6.1.9.

6.8. Key Update Response

The Key Update Response is sent by the AC in response to the request message, and includes an encrypted ANonce, which is used to derive new session keys. This message MUST include a Session Identifier message element, whose value MUST be identical to the one found in the Key Update Request.

The AC MUST include a PSK-MIC message element, which provides message integrity over the whole message.

The following subsections define the message elements that MUST be included in this LWAPP operation.

6.8.1. Session ID

The Session ID message element is defined in Section 6.1.7.

6.8.2. ANonce

The ANonce message element is defined in Section 6.2.8.

6.8.3. PSK-MIC

The PSK-MIC message element is defined in Section 6.2.9.

6.9. Key Update ACK

The Key Update ACK is sent by the WTP and includes an encrypted version of the WTP's nonce, which is used in the key derivation process. The session keys derived are then used as new LWAPP control message encryption keys (see Section 10).

The WTP MUST include a PSK-MIC message element, which provides message integrity over the whole message.

The following subsections define the message elements that MUST be included in this LWAPP operation.

6.9.1. WNonce

The WNonce message element is defined in Section 6.3.2.

6.9.2. PSK-MIC

The PSK-MIC message element is defined in Section 6.2.9.

6.10. Key Update Confirm

The Key Update Confirm closes the rekeying loop, and allows the WTP to recognize that the AC has received and processed the Key Update messages. At this point, the WTP updates its session key in its crypto engine, and the associated Initialization Vector, ensuring that all future LWAPP control frames are encrypted with the newly derived encryption key.

The WTP MUST include a PSK-MIC message element, which provides message integrity over the whole message.

The following subsections define the message elements that MUST be included in this LWAPP operation.

6.10.1. PSK-MIC

The PSK-MIC message element is defined in Section 6.2.9.

6.11. Key Update Trigger

The Key Update Trigger is used by the AC to request that a Key Update Request be initiated by the WTP.

Key Update Triggers are sent by an AC in the Run state to inform the WTP to initiate a Key Update Request message.

When a WTP receives a Key Update Trigger, it generates a Key Update Request.

The following subsections define the message elements that MUST be included in this LWAPP operation.

6.11.1. Session ID

The Session ID message element is defined in Section 6.1.7.

7. WTP Configuration Management

The Wireless Termination Point Configuration messages are used to exchange configuration between the AC and the WTP.

7.1. Configuration Consistency

The LWAPP protocol provides flexibility in how WTP configuration is managed. To put it simply, a WTP has one of two options:

1. The WTP retains no configuration and simply abides by the configuration provided by the AC.

2. The WTP retains the configuration of parameters provided by the AC that are non-default values.

If the WTP opts to save configuration locally, the LWAPP protocol state machine defines the "Configure" state, which is used during the initial binding WTP-AC phase, which allows for configuration exchange. During this period, the WTP sends its current configuration overrides to the AC via the Configure Request message. A configuration override is a parameter that is non-default. One example is that in the LWAPP protocol, the default antenna configuration is an internal-omni antenna. However, a WTP that either has no internal antennas, or has been explicitely configured by the AC to use external antennas would send its antenna configuration during the configure phase, allowing the AC to become aware of the WTP's current configuration.

Once the WTP has provided its configuration to the AC, the AC sends down its own configuration. This allows the WTP to inherit the configuration and policies on the AC.

An LWAPP AC maintains a copy of each active WTP's configuration. There is no need for versioning or other means to identify configuration changes. If a WTP becomes inactive, the AC MAY delete the configuration associated with it. If a WTP were to fail, and connect to a new AC, it would provide its overridden configuration parameters, allowing the new AC to be aware of the WTP's configuration.

As a consequence, this model allows for resiliency, whereby in light of an AC failure, another AC could provide service to the WTP. In this scenario, the new AC would be automatically updated on any possible WTP configuration changes -- eliminating the need for Inter-AC communication or the need for all ACs to be aware of the configuration of all WTPs in the network.

Once the LWAPP protocol enters the Run state, the WTPs begin to provide service. However, it is quite common for administrators to require that configuration changes be made while the network is operational. Therefore, the Configuration Update Request is sent by the AC to the WTP in order to make these changes at run-time.

7.2. Configure Request

The Configure Request message is sent by a WTP to send its current configuration to its AC.

Configure Requests are sent by a WTP after receiving a Join Response, while in the Configure state.

The Configure Request carries binding-specific message elements. Refer to the appropriate binding for the definition of this structure.

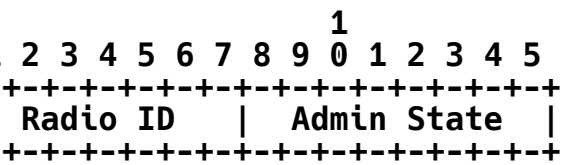
When an AC receives a Configure Request, it will act upon the content of the packet and respond to the WTP with a Configure Response.

The Configure Request includes multiple Administrative State message elements. There is one such message element for the WTP, and then one per radio in the WTP.

The following subsections define the message elements that MUST be included in this LWAPP operation.

7.2.1. Administrative State

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



Type: 27 for Administrative State

Length: 2

Radio ID: An 8-bit value representing the radio to configure. The Radio ID field may also include the value of 0xff, which is used to identify the WTP itself. Therefore, if an AC wishes to change the administrative state of a WTP, it would include 0xff in the Radio ID field.

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

1 - Enabled

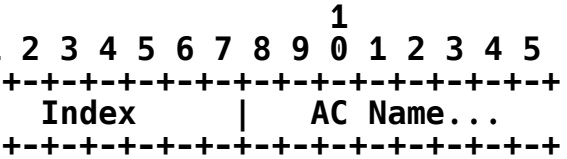
2 - Disabled

7.2.2. AC Name

The AC Name message element is defined in Section 5.2.3.

7.2.3. AC Name with Index

The AC Name with Index message element is sent by the AC to the WTP to configure preferred ACs. The number of instances where this message element would be present is equal to the number of ACs configured on the WTP.



Type: 90 for AC Name with Index

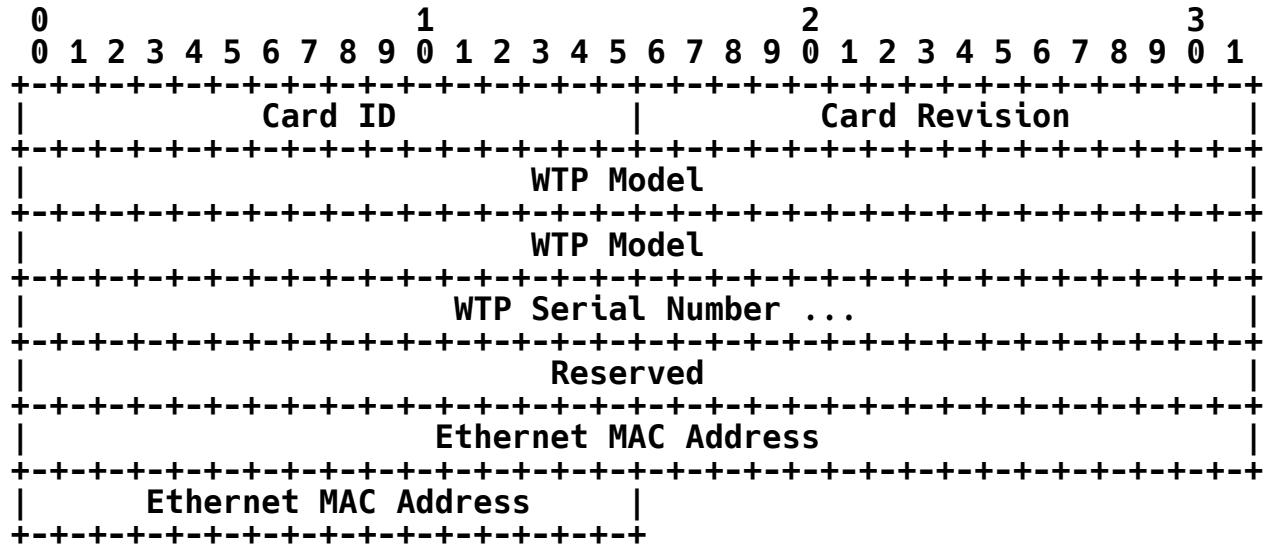
Length: 5

Index: The index of the preferred server (e.g., 1=primary, 2=secondary).

AC Name: A variable-length ASCII string containing the AC's name.

7.2.4. WTP Board Data

The WTP Board Data message element is sent by the WTP to the AC and contains information about the hardware present.



Type: 50 for WTP Board Data

Length: 26

Card ID: A hardware identifier.

Card Revision: 4-byte Revision of the card.

WTP Model: 8-byte WTP Model Number.

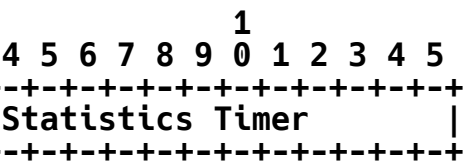
WTP Serial Number: 24-byte WTP Serial Number.

Reserved: A 4-byte reserved field that MUST be set to zero (0).

Ethernet MAC Address: MAC address of the WTP's Ethernet interface.

7.2.5. Statistics Timer

The Statistics Timer message element value is used by the AC to inform the WTP of the frequency that it expects to receive updated statistics.



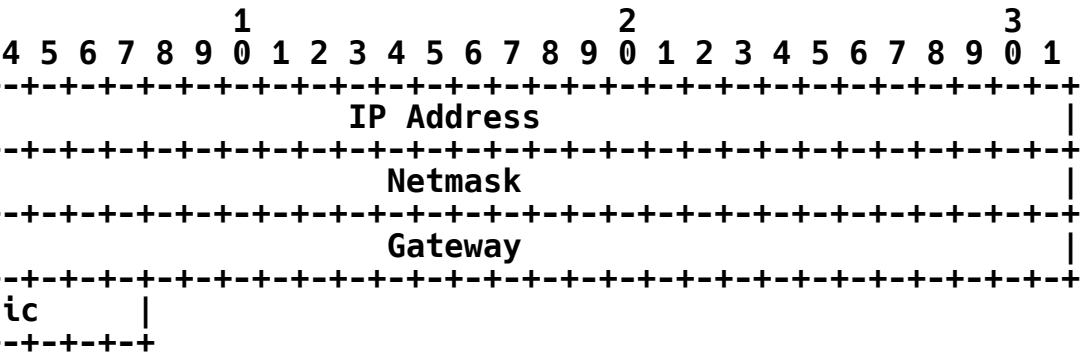
Type: 37 for Statistics Timer

Length: 2

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

7.2.6. WTP Static IP Address Information

The WTP Static IP Address Information message element is used by an AC to configure or clear a previously configured static IP address on a WTP.



Type: 82 for WTP Static IP Address Information

Length: 13

IP Address: The IP address to assign to the WTP.

Netmask: The IP Netmask.

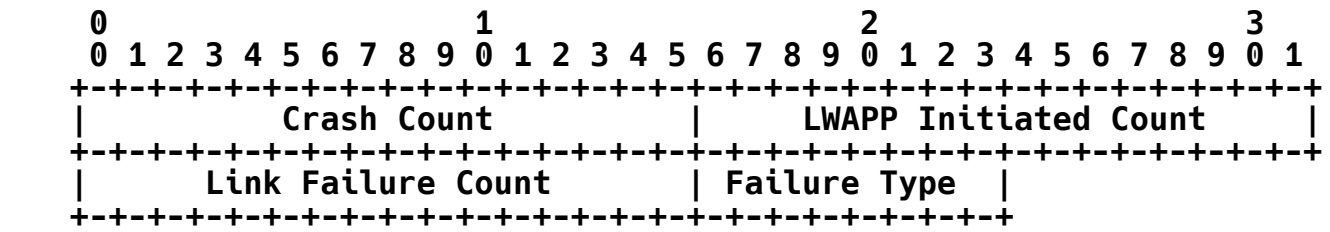
Gateway: The IP address of the gateway.

Netmask: The IP Netmask.

Static: An 8-bit Boolean stating whether or not the WTP should use a static IP address. A value of zero disables the static IP address, while a value of one enables it.

7.2.7. WTP Reboot Statistics

The WTP Reboot Statistics message element is sent by the WTP to the AC to communicate information about reasons why reboots have occurred.



Type: 67 for WTP Reboot Statistics

Length: 7

Crash Count: The number of reboots that have occurred due to a WTP crash.

LWAPP Initiated Count: The number of reboots that have occurred at the request of some LWAPP message, such as a change in configuration that required a reboot or an explicit LWAPP reset request.

Link Failure Count: The number of times that an LWAPP connection with an AC has failed.

Failure Type: The last WTP failure. The following values are supported:

0 - Link Failure

1 - LWAPP Initiated

2 - WTP Crash

7.3. Configure Response

The Configure Response message is sent by an AC and provides an opportunity for the AC to override a WTP's requested configuration.

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

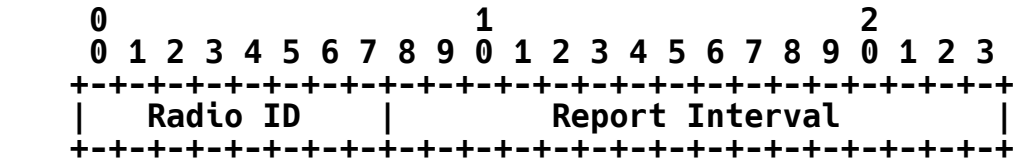
The Configure Response carries binding-specific message elements. Refer to the appropriate binding for the definition of this structure.

When a WTP receives a Configure Response, it acts upon the content of the packet, as appropriate. If the Configure Response message includes a Change State Event message element that causes a change in the operational state of one of the Radios, the WTP will transmit a Change State Event to the AC as an acknowledgement of the change in state.

The following subsections define the message elements that MUST be included in this LWAPP operation.

7.3.1. Decryption Error Report Period

The Decryption Error Report Period message element value is used by the AC to inform the WTP of how frequently it should send decryption error report messages.



Type: 38 for Decryption Error Report Period

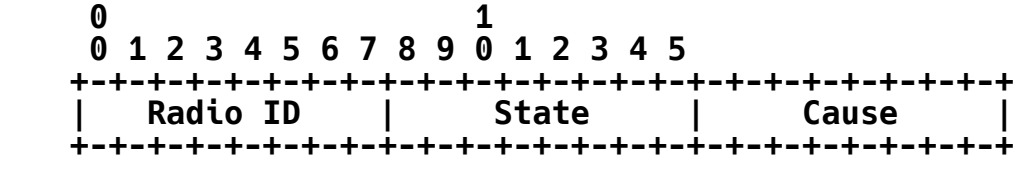
Length: 3

Radio ID: The Radio Identifier: typically refers to some interface index on the WTP.

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

7.3.2. Change State Event

The WTP Radio Information message element is used to communicate the operational state of a radio. The value contains two fields, as shown.



Type: 26 for Change State Event

Length: 3

Radio ID: The Radio Identifier: typically refers to some interface index on the WTP.

State: An 8-bit Boolean value representing the state of the radio. A value of one disables the radio, while a value of two enables it.

Cause: In the event of a radio being inoperable, the Cause field would contain the reason the radio is out of service. The following values are supported:

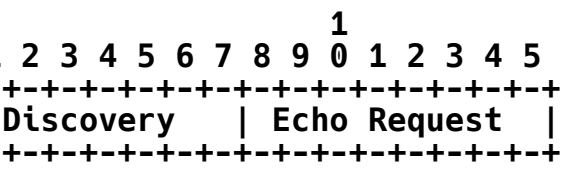
0 - Normal

1 - Radio Failure

2 - Software Failure

7.3.3. LWAPP Timers

The LWAPP Timers message element is used by an AC to configure LWAPP timers on a WTP.



Type: 68 for LWAPP Timers

Length: 2

Discovery: The number of seconds between LWAPP Discovery packets when the WTP is in the discovery mode.

Echo Request: The number of seconds between WTP Echo Request LWAPP messages.

7.3.4. AC IPv4 List

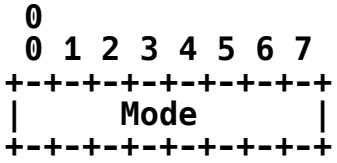
The AC List message element is defined in Section 6.2.6.

7.3.5. AC IPv6 List

The AC List message element is defined in Section 6.2.7.

7.3.6. WTP Fallback

The WTP Fallback message element is sent by the AC to the WTP to enable or disable automatic LWAPP fallback in the event that a WTP detects its preferred AC, and is not currently connected to it.



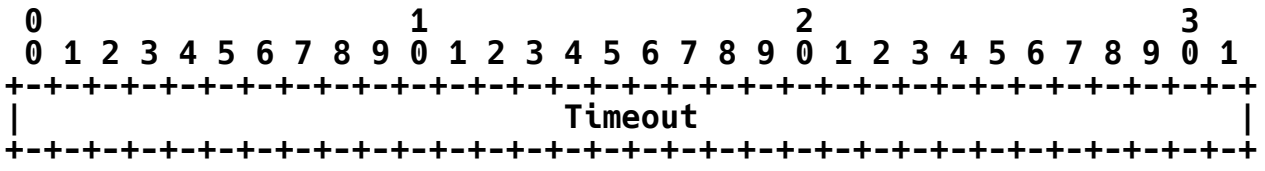
Type: 91 for WTP Fallback

Length: 1

Mode: The 8-bit Boolean value indicates the status of automatic LWAPP fallback on the WTP. A value of zero disables the fallback feature, while a value of one enables it. When enabled, if the WTP detects that its primary AC is available, and it is not connected to it, it SHOULD automatically disconnect from its current AC and reconnect to its primary. If disabled, the WTP will only reconnect to its primary through manual intervention (e.g., through the Reset Request command).

7.3.7. Idle Timeout

The Idle Timeout message element is sent by the AC to the WTP to provide it with the idle timeout that it should enforce on its active mobile station entries.



Type: 97 for Idle Timeout

Length: 4

Timeout: The current idle timeout to be enforced by the WTP.

7.4. Configuration Update Request

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

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

The following subsections define the message elements introduced by this LWAPP operation.

7.4.1. WTP Name

The WTP Name message element is defined in Section 6.1.3.

7.4.2. Change State Event

The Change State Event message element is defined in Section 7.3.2.

7.4.3. Administrative State

The Administrative State message element is defined in Section 7.2.1.

7.4.4. Statistics Timer

The Statistics Timer message element is defined in Section 7.2.5.

7.4.5. Location Data

The Location Data message element is defined in Section 6.1.4.

7.4.6. Decryption Error Report Period

The Decryption Error Report Period message element is defined in Section 7.3.1.

7.4.7. AC IPv4 List

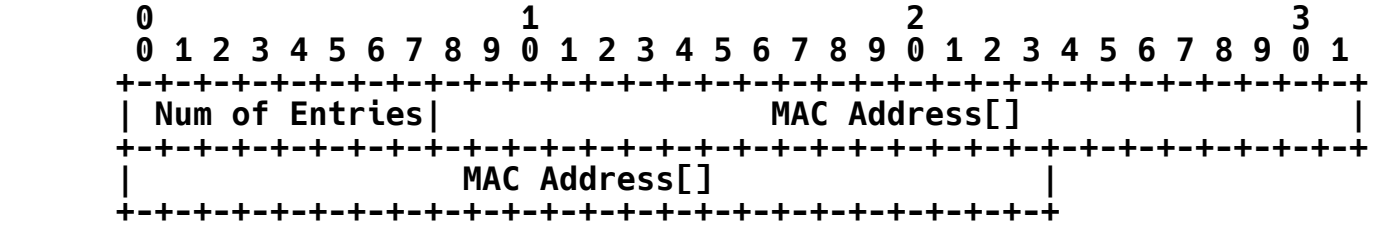
The AC List message element is defined in Section 6.2.6.

7.4.8. AC IPv6 List

The AC List message element is defined in Section 6.2.7.

7.4.9. Add Blacklist Entry

The Add Blacklist Entry message element is used by an AC to add a blacklist entry on a WTP, ensuring that the WTP no longer provides any service to the MAC addresses provided in the message. The MAC addresses provided in this message element are not expected to be saved in non-volative memory on the WTP.



Type: 65 for Add Blacklist Entry

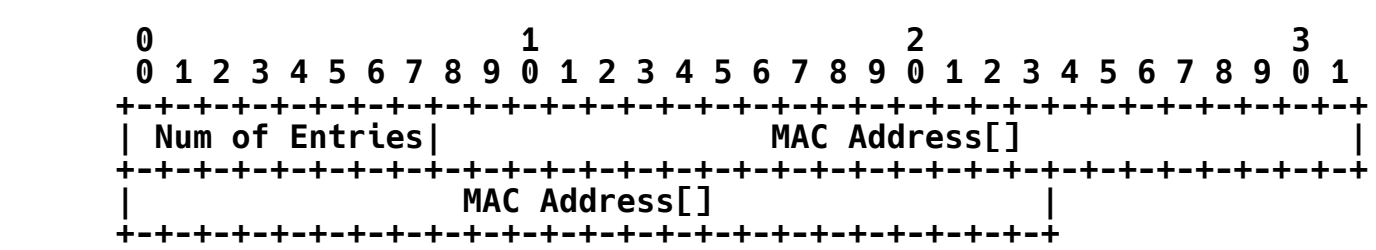
Length: >= 7

Num of Entries: The number of MAC addresses in the array.

MAC Address: An array of MAC addresses to add to the blacklist entry.

7.4.10. Delete Blacklist Entry

The Delete Blacklist Entry message element is used by an AC to delete a previously added blacklist entry on a WTP, ensuring that the WTP provides service to the MAC addresses provided in the message.



Type: 66 for Delete Blacklist Entry

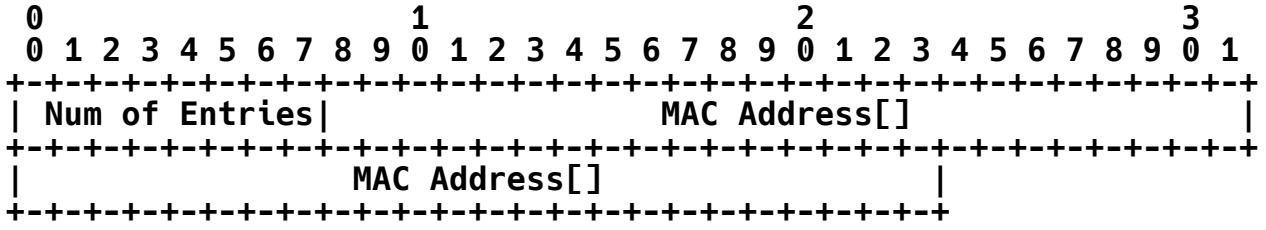
Length: >= 7

Num of Entries: The number of MAC addresses in the array.

MAC Address: An array of MAC addresses to delete from the blacklist entry.

7.4.11. Add Static Blacklist Entry

The Add Static Blacklist Entry message element is used by an AC to add a permanent Blacklist Entry on a WTP, ensuring that the WTP no longer provides any service to the MAC addresses provided in the message. The MAC addresses provided in this message element are expected to be saved in non-volative memory on the WTP.



Type: 70 for Delete Blacklist Entry

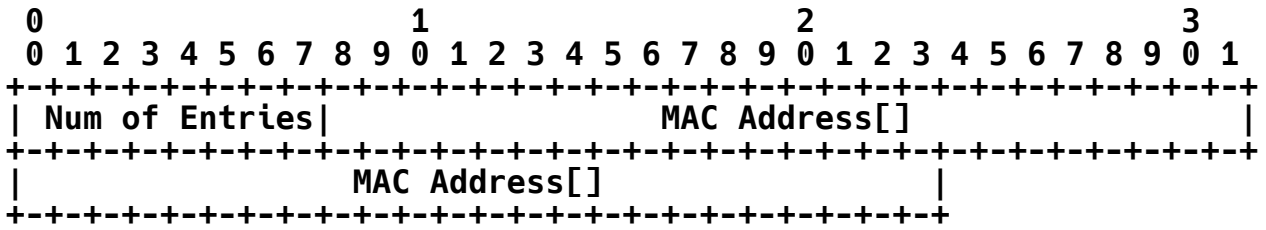
Length: >= 7

Num of Entries: The number of MAC addresses in the array.

MAC Address: An array of MAC addresses to add to the permanent blacklist entry.

7.4.12. Delete Static Blacklist Entry

The Delete Static Blacklist Entry message element is used by an AC to delete a previously added static blacklist entry on a WTP, ensuring that the WTP provides service to the MAC addresses provided in the message.



Type: 71 for Delete Blacklist Entry

Length: >= 7

Num of Entries: The number of MAC addresses in the array.

MAC Address: An array of MAC addresses to delete from the static blacklist entry.

7.4.13. LWAPP Timers

The LWAPP Timers message element is defined in Section 7.3.3.

7.4.14. AC Name with Index

The AC Name with Index message element is defined in Section 7.2.3.

7.4.15. WTP Fallback

The WTP Fallback message element is defined in Section 7.3.6.

7.4.16. Idle Timeout

The Idle Timeout message element is defined in Section 7.3.7.

7.5. Configuration Update Response

The Configuration Update Response is the acknowledgement message for the Configuration Update Request.

Configuration Update Responses are sent by a WTP after receiving a Configuration Update Request.

When an AC receives a Configure Update Response, the result code indicates if the WTP successfully accepted the configuration.

The following subsections define the message elements that must be present in this LWAPP operation.

7.5.1. Result Code

The Result Code message element is defined in Section 6.2.1.

7.6. Change State Event Request

The Change State Event is used by the WTP to inform the AC of a change in the operational state.

The Change State Event message is sent by the WTP when it receives a Configuration Response that includes a Change State Event message element. It is also sent in the event that the WTP detects an operational failure with a radio. The Change State Event may be sent in either the Configure or Run state (see Figure 2).

When an AC receives a Change State Event it will respond with a Change State Event Response and make any necessary modifications to internal WTP data structures.

The following subsections define the message elements that must be present in this LWAPP operation.

7.6.1. Change State Event

The Change State Event message element is defined in Section 7.3.2.

7.7. Change State Event Response

The Change State Event Response acknowledges the Change State Event.

Change State Event Responses are sent by a WTP after receiving a Change State Event.

The Change State Event Response carries no message elements. Its purpose is to acknowledge the receipt of the Change State Event.

The WTP does not need to perform any special processing of the Change State Event Response message.

7.8. Clear Config Indication

The Clear Config Indication is used to reset a WTP's configuration.

The Clear Config Indication is sent by an AC to request that a WTP reset its configuration to manufacturing defaults. The Clear Config Indication message is sent while in the Run LWAPP state.

The Reset Request carries no message elements.

When a WTP receives a Clear Config Indication, it will reset its configuration to manufacturing defaults.

8. Device Management Operations

This section defines LWAPP operations responsible for debugging, gathering statistics, logging, and firmware management.

8.1. Image Data Request

The Image Data Request is used to update firmware on the WTP. This message and its companion response are used by the AC to ensure that the image being run on each WTP is appropriate.

Image Data Requests are exchanged between the WTP and the AC to download a new program image to a WTP.

When a WTP or AC receives an Image Data Request, it will respond with

an Image Data Response.

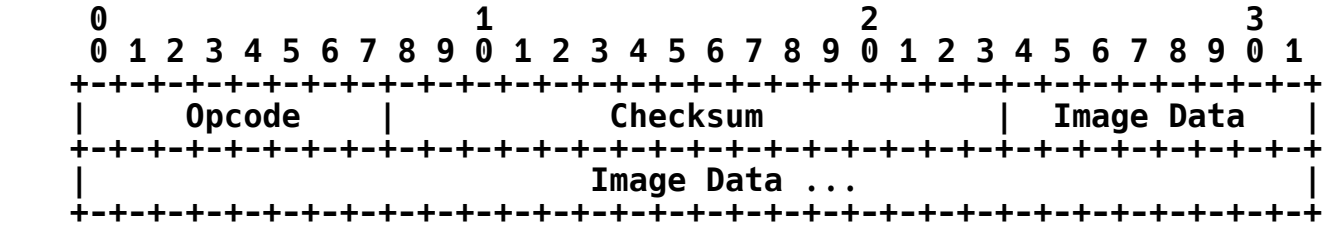
The format of the Image Data and Image Download message elements are described in the following subsections.

8.1.1. Image Download

The Image Download message element is sent by the WTP to the AC and contains the image filename. The value is a variable-length byte string. The string is NOT zero terminated.

8.1.2. Image Data

The Image Data message element is present when sent by the AC and contains the following fields.



Type: 33 for Image Data

Length: >= 5

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.

Checksum: A 16-bit value containing a checksum of the Image Data that follows.

Image Data: The Image Data field contains 1024 characters, unless the payload being sent is the last one (end of file).

8.2. Image Data Response

The Image Data Response acknowledges the Image Data Request.

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

The Image Data Response carries no message elements.

No action is necessary on receipt.

8.3. Reset Request

The Reset Request is used to cause a WTP to reboot.

Reset Requests are sent by an AC to cause a WTP to reinitialize its operation.

The Reset Request carries no message elements.

When a WTP receives a Reset Request it will respond with a Reset Response and then reinitialize itself.

8.4. Reset Response

The Reset Response acknowledges the Reset Request.

Reset Responses are sent by a WTP after receiving a Reset Request.

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

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

8.5. WTP Event Request

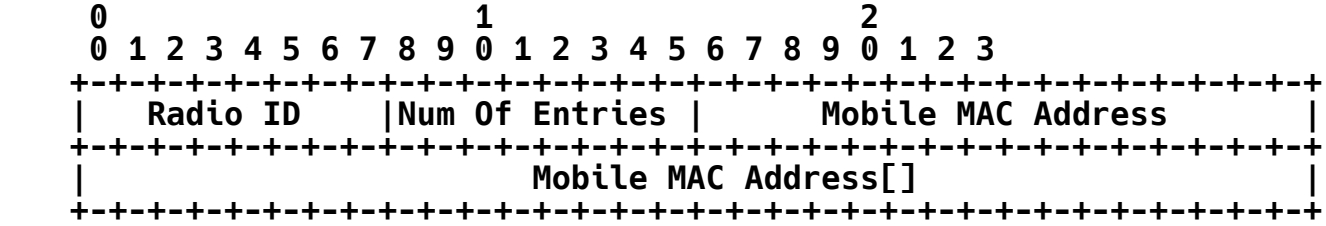
The WTP Event Request is used by a WTP to send information to its AC. These types of events may be periodical, or some asynchronous event on the WTP. For instance, a WTP collects statistics and uses the WTP Event Request to transmit this information to the AC.

When an AC receives a WTP Event Request, it will respond with a WTP Event Request.

The WTP Event Request message MUST contain one of the following message element described in the next subsections, or a message element that is defined for a specific technology.

8.5.1. Decryption Error Report

The Decryption Error Report message element value is used by the WTP to inform the AC of decryption errors that have occurred since the last report.



Type: 39 for Decryption Error Report

Length: >= 8

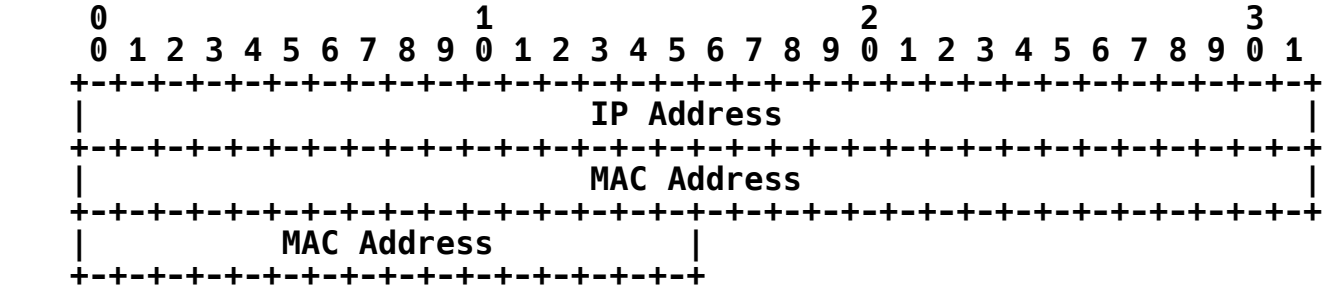
Radio ID: The Radio Identifier, typically refers to some interface index on the WTP.

Num Of Entries: An 8-bit unsigned integer indicating the number of mobile MAC addresses.

Mobile MAC Address: An array of mobile station MAC addresses that have caused decryption errors.

8.5.2. Duplicate IPv4 Address

The Duplicate IPv4 Address message element is used by a WTP to inform an AC that it has detected another host using the same IP address it is currently using.



Type: 77 for Duplicate IPv4 Address

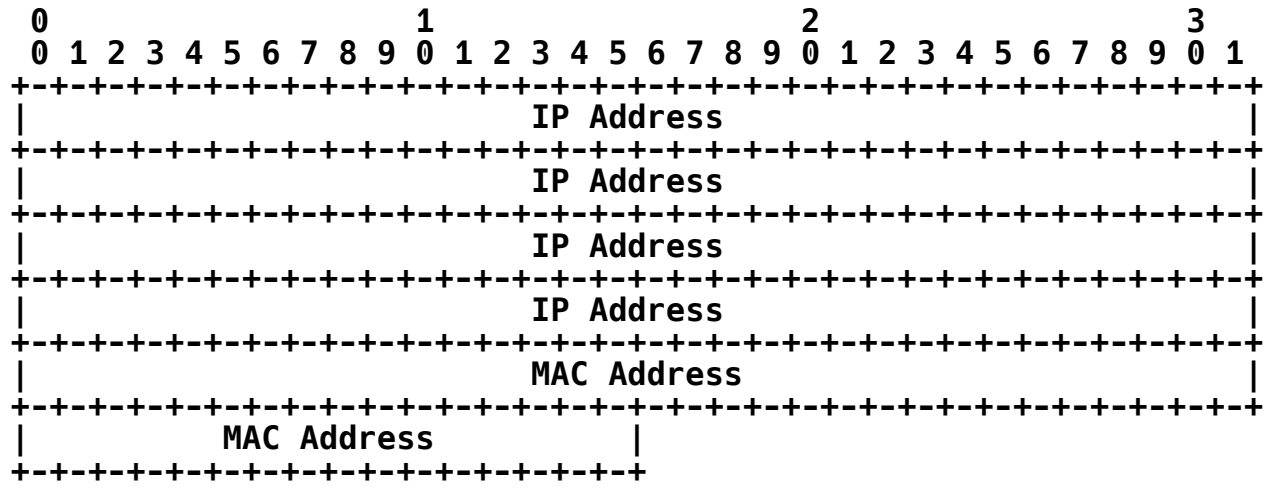
Length: 10

IP Address: The IP address currently used by the WTP.

MAC Address: The MAC address of the offending device.

8.5.3. Duplicate IPv6 Address

The Duplicate IPv6 Address message element is used by a WTP to inform an AC that it has detected another host using the same IP address it is currently using.



Type: 77 for Duplicate IPv6 Address

Length: 10

IP Address: The IP address currently used by the WTP.

MAC Address: The MAC address of the offending device.

8.6. WTP Event Response

The WTP Event Response acknowledges the WTP Event Request.

WTP Event Responses are sent by an AC after receiving a WTP Event Request.

The WTP Event Response carries no message elements.

8.7. Data Transfer Request

The Data Transfer Request is used to upload debug information from the WTP to the AC.

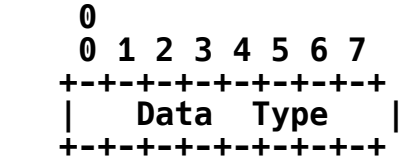
Data Transfer Requests are sent by the WTP to the AC when it determines that it has important information to send to the AC. For instance, if the WTP detects that its previous reboot was caused by a system crash, it would want to send the crash file to the AC. The remote debugger function in the WTP also uses the Data Transfer Request in order to send console output to the AC for debugging purposes.

When an AC receives a Data Transfer Request, it will respond with a Data Transfer Response. The AC may log the information received as it sees fit.

The Data Transfer Request message MUST contain ONE of the following message element described in the next subsection.

8.7.1. Data Transfer Mode

The Data Transfer Mode message element is used by the AC to request information from the WTP for debugging purposes.



Type: 52 for Data Transfer Mode

Length: 1

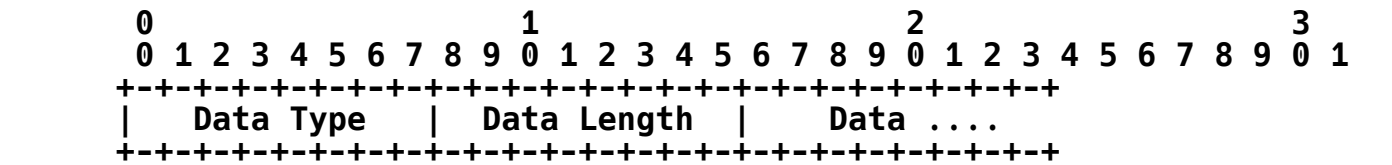
Data Type: An 8-bit value describing the type of information being requested. The following values are supported:

1 - WTP Crash Data

2 - WTP Memory Dump

8.7.2. Data Transfer Data

The Data Transfer Data message element is used by the WTP to provide information to the AC for debugging purposes.



Type: 53 for Data Transfer Data

Length: >= 3

Data Type: An 8-bit value describing the type of information being sent. The following values are supported:

1 - WTP Crash Data

2 - WTP Memory Dump

Data Length: Length of data field.

Data: Debug information.

8.8. Data Transfer Response

The Data Transfer Response acknowledges the Data Transfer Request.

A Data Transfer Response is sent in response to a Data Transfer Request. Its purpose is to acknowledge the receipt of the Data Transfer Request packet.

The Data Transfer Response carries no message elements.

Upon receipt of a Data Transfer Response, the WTP transmits more information, if any is available.

9. Mobile Session Management

Messages in this section are used by the AC to create, modify, or delete mobile station session state on the WTPs.

9.1. Mobile Config Request

The Mobile Config Request message is used to create, modify, or delete mobile session state on a WTP. The message is sent by the AC to the WTP, and may contain one or more message elements. The

message elements for this LWAPP control message include information that is generally highly technology-specific. Therefore, please refer to the appropriate binding section or document for the definitions of the messages elements that may be used in this control message.

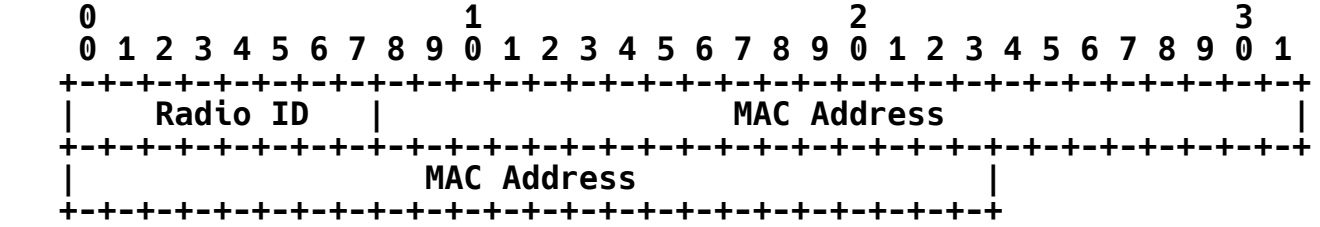
This section defines the format of the Delete Mobile message element, since it does not contain any technology-specific information.

9.1.1. Delete Mobile

The Delete Mobile message element is used by the AC to inform a WTP that it should no longer provide service to a particular mobile station. The WTP must terminate service immediately upon receiving this message element.

The transmission of a Delete Mobile message element could occur for various reasons, including administrative reasons, as a result of the fact that the mobile has roamed to another WTP, etc.

Once access has been terminated for a given station, any future packets received from the mobile must result in a deauthenticate message, as specified in [6].



Type: 30 for Delete Mobile

Length: 7

Radio ID: An 8-bit value representing the radio

MAC Address: The mobile station's MAC address

9.2. Mobile Config Response

The Mobile Configuration Response is used to acknowledge a previously received Mobile Configuration Request, and includes a Result Code message element that indicates whether an error occurred on the WTP.

This message requires no special processing and is only used to acknowledge the Mobile Configuration Request.

The Data Transfer Request message MUST contain the message elements described in the next subsection.

9.2.1. Result Code

The Result Code message element is defined in Section 6.2.1.

10. LWAPP Security

Note: This version only defines a certificate and a shared-secret-based mechanism to secure control LWAPP traffic exchanged between the WTP and the AC.

10.1. Securing WTP-AC Communications

While it is generally straightforward to produce network installations in which the communications medium between the WTP and AC is not accessible to the casual user (e.g., these LAN segments are isolated, and no RJ45 or other access ports exist between the WTP and the AC), 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 AC-WTP communications. While an in-depth security analysis of threats and risks to these communications 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:

- WTP-AC communications take place over a wired connection that 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 WTP and AC are intermediaries is required, this may be provided via IPsec [14].

- privacy and authentication for at least some WTP-AC control traffic is required (e.g., Wired Equivalent Privacy (WEP) keys for user sessions, passed from the AC to the WTP).

- the AC can be trusted to generate strong cryptographic keys.

The AC-WTP traffic can be considered to consist of two types: data traffic (e.g., to or from an end user), and control traffic, which is strictly between the AC and WTP. 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 AES-CCM, described in [3]. This encapsulation provides for strong AES-based authentication and encryption [2]. The exchange of cryptographic keys used for CCM is described below.

10.2. LWAPP Frame Encryption

While the LWAPP protocol uses AES-CCM to encrypt control traffic, it is important to note that not all control frames are encrypted. The LWAPP discovery and join phase are not encrypted. The Discovery messages are sent in the clear since there does not exist a security association between the WTP and the AC during the discovery phase. The join phase is an authenticated exchange used to negotiate symmetric session keys (see Section 10.3).

Once the join phase has been successfully completed, the LWAPP state machine Figure 2 will move to the Configure state, at which time all LWAPP control frames are encrypted using AES-CCM.

Encryption of a control message begins at the Message Element field: meaning the Msg Type, Seq Num, Msg Element Length, and Session ID fields are left intact (see Section 4.2.1).

The AES-CCM 12-byte authentication data is appended to the end of the message. The authentication data is calculated from the start of the LWAPP packet and includes the complete LWAPP control header (see Section 4.2.1).

The AES-CCM block cipher protocol requires an initialization vector. The LWAPP protocol requires that the WTP and the AC maintain two separate IVs, one for transmission and one for reception. The IV derived during the key exchange phase by both the WTP and the AC is used as the base for all encrypted packets with a new key.

10.3. Authenticated Key Exchange

This section describes the key management component of the LWAPP protocol. There are two modes supported by LWAPP: certificate and pre-shared key.

10.3.1. Terminology

This section details the key management protocol that makes use of pre-shared secrets.

The following notations are used throughout this section:

- PSK - the pre-shared key shared between the WTP and the AC.
- Kpriv - the private key of a public-private key pair.
- Kpub - the public key of the pair.
- SessionID - a randomly generated LWAPP session identifier, provided by the WTP in the Join Request.
- E-x{Kpub, M} - RSA encryption of M using X's public key.
- D-x{Kpriv, C} - RSA decryption of C using X's private key.
- AES-CMAC(key, packet) - A message integrity check, using AES-CMAC and key, of the complete LWAPP packet, with the Sequence Number field and the payload of the PSK-MIC message element set to zero.
- AES-E(key, plaintext) - Plaintext is encrypted with key, using AES.
- AES-D(key, ciphertext) - ciphertext is decrypted with key, using AES.
- Certificate-AC - AC's Certificate.
- Certificate-WTP - WTP's Certificate.
- WTP-MAC - The WTP's MAC address.

- AC-MAC - The AC's MAC address.
- RK0 - the root key, which is created through a Key Derivation Function (KDF) function.
- RK0E - the root Encryption key, derived from RK0.
- RK0M - the root MIC key, derived from RK0.
- SK1 - the session key.
- SK1C - the session confirmation key, derived from SK.
- SK1E - the session encryption key, derived from SK.
- SK1W - the session keywrap key, derived from SK (see RFC 3394 [9]).
- WNonce - The WTP's randomly generated nonce.
- ANonce - The AC's randomly generated nonce.
- EWNonce - The payload of the WNonce message element, which includes the WNonce.
- EANonce - The payload of the ANonce message element, which includes the ANonce.

10.3.2. Initial Key Generation

The AC and WTP accomplish mutual authentication and a cryptographic key exchange in a dual round trip using the Join Request, Join Response, Join ACK, and Join Confirm (see Section 6.1).

The following text describes the exchange between the WTP and the AC that creates a session key, which is used to secure LWAPP control messages.

- The WTP creates a Join Request using the following process:
  - If certificate-based security is used, the WTP adds the Certificate message element (see Section 6.1.6) with its contents set to Certificate-WTP.
  - The WTP adds the Session ID message element (see Section 6.1.7) with the contents set to a randomly generated session identifier (see RFC 1750 [4]). The WTP MUST save the Session ID in order to validate the Join Response.

- The WTP creates a random nonce, included in the XNonce message element (see Section 6.1.9). The WTP MUST save the XNonce to validate the Join Response.
- The WTP transmits the Join Request to the AC.

- Upon receiving the Join Request, the AC uses the following process:
  - The AC creates the Join Response, and ensures that the Session ID message element matches the value found in the Join Request.
  - If certificate-based security is used, the AC:
    - adds the Certificate-AC to the Certificate message element.
    - creates a random 'AC Nonce' and encrypts it using the following algorithm E-wtp(Kpub, XNonce XOR 'AC Nonce'). The encrypted contents are added to the ANonce's message element payload.
  - If a pre-shared-key-based security is used, the AC:
    - creates RK0 through the following algorithm: RK0 = KDF-256{PSK, "LWAPP PSK Top K0" || Session ID || WTP-MAC || AC-MAC}, where WTP-MAC is the WTP's MAC address in the form "xx:xx:xx:xx:xx:xx". Similarly, the AC-MAC is an ASCII encoding of the AC's MAC address, of the form "xx:xx:xx:xx:xx:xx". The resulting K0 is split into the following:
      - The first 16 octets are known as RK0E, and are used as an encryption key.
      - The second 16 octets are known as RK0M, and are used for MIC'ing purposes.
    - The AC creates a random 'AC Nonce' and encrypts it using the following algorithm: AES-E(RK0E, XNonce XOR 'AC Nonce'). The encrypted contents are added to the ANonce's message element payload.
    - The AC adds a MIC to the contents of the Join Response using AES-CMAC(RK0M, Join Response) and adds the resulting hash to the PSK-MIC (Section 6.2.9) message element.

- Upon receiving the Join Response, the WTP uses the following process:

- If a pre-shared key is used, the WTP authenticates the Join Response's PSK-MIC message element. If authentication fails, the packet is dropped.
- The WTP decrypts the ANonce message element and XOR's the value with XNonce to retrieve the 'AC Nonce'. The ANonce payload is referred to as ciphertext below:
  - If a pre-shared key is used, use AES-D(RK0E, ciphertext). The 'AC Nonce' is then recovered using XNonce XOR plaintext.
  - If certificates are used, use d-wtp(Kpriv, ciphertext). The 'AC Nonce' is then recovered using XNonce XOR plaintext.
- The WTP creates a random 'WTP Nonce'.
- The WTP uses the KDF function to create a 64-octet session key (SK). The KDF function used is as follows: KDF-512{'WTP Nonce' || 'AC Nonce', "LWAPP Key Generation", WTP-MAC || AC-MAC}. The KDF function is defined in [7].
- SK is then broken down into three separate session keys with different purposes:
  - The first 16 octets are known as SK1C, and are used as a confirmation key.
  - The second 16 octets are known as SK1E, and are as the encryption key.
  - The third 16 octets are known as SK1D, and are used as the keywrap key.
  - The fourth 16 octets are known as IV, and are used as the Initialization Vector during encryption.
- The WTP creates the Join ACK message.
- If certificate-based security is used, the AC:
  - encrypts the 'WTP Nonce' using the following algorithm: E-ac(Kpub, 'WTP Nonce'). The encrypted contents are added to the WNonce's message element payload.
- If a pre-shared-key-based security is used, the AC:

- encrypts the 'WTP Nonce' using the following algorithm: AES-E(RK0E, 'WTP Nonce'). The encrypted contents are added to the WNonce's message element payload.

- The WTP adds a MIC to the contents of the Join ACK using AES-CMAC(SK1M, Join ACK) and adds the resulting hash to the PSK-MIC (Section 6.2.9) message element.

- The WTP then transmits the Join ACK to the AC.

- Upon receiving the Join ACK, the AC uses the following process:

  - The AC authenticates the Join ACK through the PSK-MIC message element. If authentic, the AC decrypts the WNonce message element to retrieve the 'WTP Nonce'. If the Join ACK cannot be authenticated, the packet is dropped.

  - The AC decrypts the WNonce message element to retrieve the 'WTP Nonce'. The WNonce payload is referred to as ciphertext below:

    - If a pre-shared key is used, use AES-D(RK0E, ciphertext). The plaintext is then considered the 'WTP Nonce'.

    - If certificates are used, use d-ac(Kpriv, ciphertext). The plaintext is then considered the 'WTP Nonce'.

  - The AC then uses the KDF function to create a 64-octet session key (SK). The KDF function used is as follows: KDF-512{'WTP Nonce' || 'AC Nonce', "LWAPP Key Generation", WTP-MAC || AC-MAC}. The KDF function is defined in [7]. The SK is split into SK1C, SK1E, SK1D, and IV, as previously noted.

  - The AC creates the Join Confirm.

  - The AC adds a MIC to the contents of the Join Confirm using AES-CMAC(SK1M, Join Confirm) and adds the resulting hash to the MIC (Section 6.2.9) message element.

  - The AC then transmits the Join Confirm to the WTP.

- Upon receiving the Join Confirm, the WTP uses the following process:

  - The WTP authenticates the Join Confirm through the PSK-MIC message element. If the Join Confirm cannot be authenticated, the packet is dropped.

- SK1E is now plumbed into the AC and WTP's crypto engine as the AES-CCM LWAPP control encryption session key. Furthermore, the random IV is used as the base Initialization Vector. From this point on, all control protocol payloads between the WTP and AC are encrypted and authenticated using the new session key.

10.3.3. Refreshing Cryptographic Keys

Since AC-WTP 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". When the key lifetime reaches 95% of the configured value, identified in the KeyLifetime timer (see Section 12), the rekeying will proceed as follows:

- The WTP creates RK0 through the previously defined KDF algorithm: RK0 = KDF-256{SK1D, "LWAPP PSK Top K0" || Session ID || WTP-MAC || AC-MAC}. Note that the difference in this specific instance is that SK1D that was previously generated is used instead of the PSK. Note this is used in both the certificate and pre-shared key modes. The resulting RK0 creates RK0E, RK0M.

- The remaining steps used are identical to the join process, with the exception that the rekey messages are used instead of join messages, and the fact that the messages are encrypted using the previously created SK1E. This means the Join Request is replaced with the Rekey Request, the Join Response is replaced with the Rekey Response, etc. The two differences between the rekey and the join process are:

  - The Certificate-WTP and Certificate-AC are not included in the Rekey-Request and Rekey-Response, respectively.

  - Regardless of whether certificates or pre-shared keys were used in the initial key derivation, the process now uses the pre-shared key mode only, using SK1D as the "PSK".

- The Key Update Request is sent to the AC.

- The newly created SK1E is now plumbed into the AC and WTP's crypto engine as the AES-CCM LWAPP control encryption session key. Furthermore, the new random IV is used as the base Initialization Vector. From this point on, all control protocol payloads between the WTP and AC are encrypted and authenticated using the new session key.

If either the WTP or the AC do not receive an expected response by the time the ResponseTimeout timer expires (see Section 12), the WTP MUST delete the new and old session information, and reset the state machine to the Idle state.

Following a rekey process, both the WTP and the AC keep the previous encryption for 5-10 seconds in order to be able to process packets that arrive out of order.

10.4. Certificate Usage

Validation of the certificates by the AC and WTP is required so that only an AC may perform the functions of an AC and that only a WTP may perform the functions of a WTP. This restriction of functions to the AC or WTP requires that the certificates used by the AC MUST be distinguishable from the certificate used by the WTP. To accomplish this differentiation, the x.509v3 certificates MUST include the Extensions field [10] and MUST include the NetscapeComment [11] extension.

For an AC, the value of the NetscapeComment extension MUST be the string "CAPWAP AC Device Certificate". For a WTP, the value of the NetscapeComment extension MUST be the string "CAPWAP WTP Device Certificate".

Part of the LWAPP certificate validation process includes ensuring that the proper string is included in the NetscapeComment extension, and only allowing the LWAPP session to be established if the extension does not represent the same role as the device validating the certificate. For instance, a WTP MUST NOT accept a certificate whose NetscapeComment field is set to "CAPWAP WTP Device Certificate".

11. IEEE 802.11 Binding

This section defines the extensions required for the LWAPP protocol to be used with the IEEE 802.11 protocol.

11.1. Division of Labor

The LWAPP protocol, when used with IEEE 802.11 devices, requires a specific behavior from the WTP and the AC, specifically in terms of which 802.11 protocol functions are handled.

For both the Split and Local MAC approaches, the CAPWAP functions, as defined in the taxonomy specification, reside in the AC.

11.1.1. Split MAC

This section shows the division of labor between the WTP and the AC in a Split MAC architecture. Figure 3 shows the clear separation of functionality among LWAPP components.

Function	Location
Distribution Service	AC
Integration Service	AC
Beacon Generation	WTP
Probe Response	WTP
Power Mgmt/Packet Buffering	WTP
Fragmentation/Defragmentation	WTP
Assoc/Disassoc/Reassoc	AC
802.11e	
Classifying	AC
Scheduling	WTP/AC
Queuing	WTP
802.11i	
802.1X/EAP	AC
Key Management	AC
802.11 Encryption/Decryption	WTP or AC

Figure 3: Mapping of 802.11 Functions for Split MAC Architecture

The Distribution and Integration services reside on the AC, and therefore all user data is tunneled between the WTP and the AC. As noted above, all real-time 802.11 services, including the control protocol and the beacon and Probe Response frames, are handled on the WTP.

All remaining 802.11 MAC management frames are supported on the AC, including the Association Request, which allows the AC to be involved in the access policy enforcement portion of the 802.11 protocol. The 802.1X and 802.11i key management function are also located on the AC.

While the admission control component of 802.11e resides on the AC, the real-time scheduling and queuing functions are on the WTP. Note that this does not exclude the AC from providing additional policing and scheduling functionality.

Note that in the following figure, the use of '(-)' indicates that processing of the frames is done on the WTP.

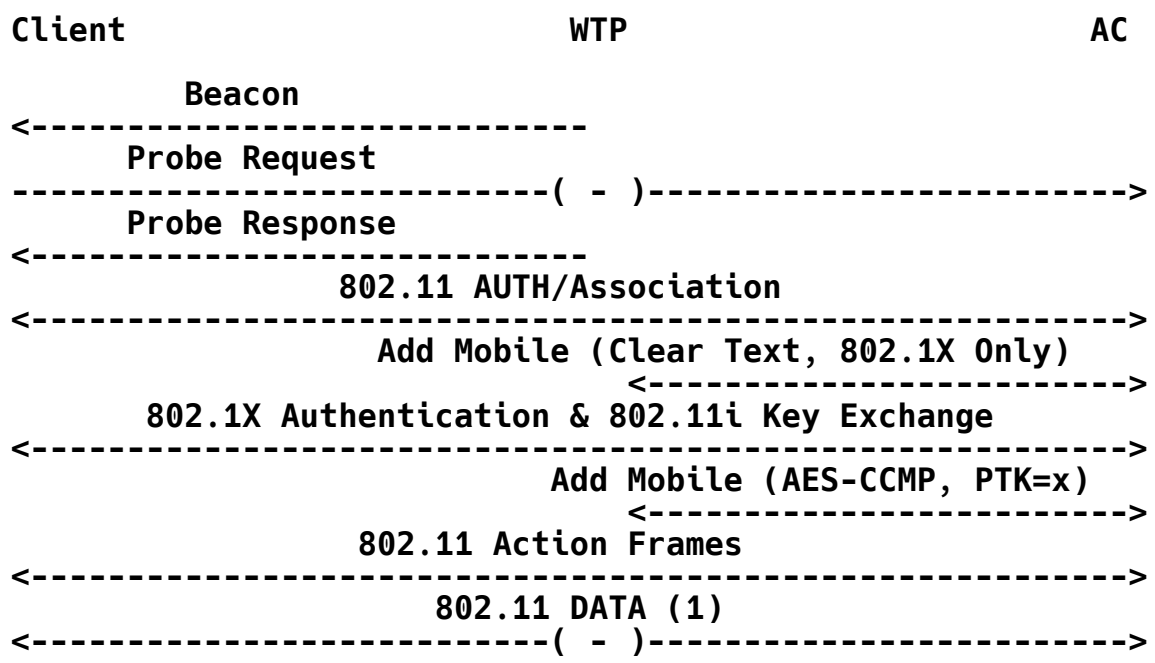


Figure 4: Split MAC Message Flow

Figure 4 provides an illustration of the division of labor in a Split MAC architecture. In this example, a WLAN has been created that is configured for 802.11i, using AES-CCMP for privacy. The following process occurs:

- The WTP generates the 802.11 beacon frames, using information provided to it through the Add WLAN (see Section 11.8.1.1) message element.
- The WTP processes the Probe Request and responds with a corresponding Probe Response. The problem request is then forwarded to the AC for optional processing.
- The WTP forwards the 802.11 Authentication and Association frames to the AC, which is responsible for responding to the client.
- Once the association is complete, the AC transmits an LWAPP Add Mobile Request to the WTP (see Section 11.7.1.1). In the above example, the WLAN is configured for 802.1X, and therefore the '802.1X only' policy bit is enabled.
- If the WTP is providing encryption/decryption services, once the client has completed the 802.11i key exchange, the AC transmits another Add Mobile Request to the WTP, stating the security policy to enforce for the client (in this case AES-CCMP), as well as the

encryption key to use. If encryption/decryption is handled in the AC, the Add Mobile Request would have the encryption policy set to "Clear Text".

- The WTP forwards any 802.11 Action frames received to the AC.
- All client data frames are tunneled between the WTP and the AC. Note that the WTP is responsible for encrypting and decrypting frames, if it was indicated in the Add Mobile Request.

11.1.2. Local MAC

This section shows the division of labor between the WTP and the AC in a Local MAC architecture. Figure 5 shows the clear separation of functionality among LWAPP components.

Function	Location
Distribution Service	WTP
Integration Service	WTP
Beacon Generation	WTP
Probe Response	WTP
Power Mgmt/Packet Buffering	WTP
Fragmentation/Defragmentation	WTP
Assoc/Disassoc/Reassoc	WTP
802.11e	
Classifying	WTP
Scheduling	WTP
Queuing	WTP
802.11i	
802.1X/EAP	AC
Key Management	AC
802.11 Encryption/Decryption	WTP

Figure 5: Mapping of 802.11 Functions for Local AP Architecture

Given that Distribution and Integration Services exist on the WTP, client data frames are not forwarded to the AC, with the exception listed in the following paragraphs.

While the MAC is terminated on the WTP, it is necessary for the AC to be aware of mobility events within the WTPs. As a consequence, the WTP MUST forward the 802.11 Association Requests to the AC, and the AC MAY reply with a failed Association Response if it deems it necessary.

The 802.1X and 802.11i Key Management function resides in the AC. Therefore, the WTP MUST forward all 802.1X/Key Management frames to the AC and forward the associated responses to the station.

Note that in the following figure, the use of '(-)' indicates that processing of the frames is done on the WTP.

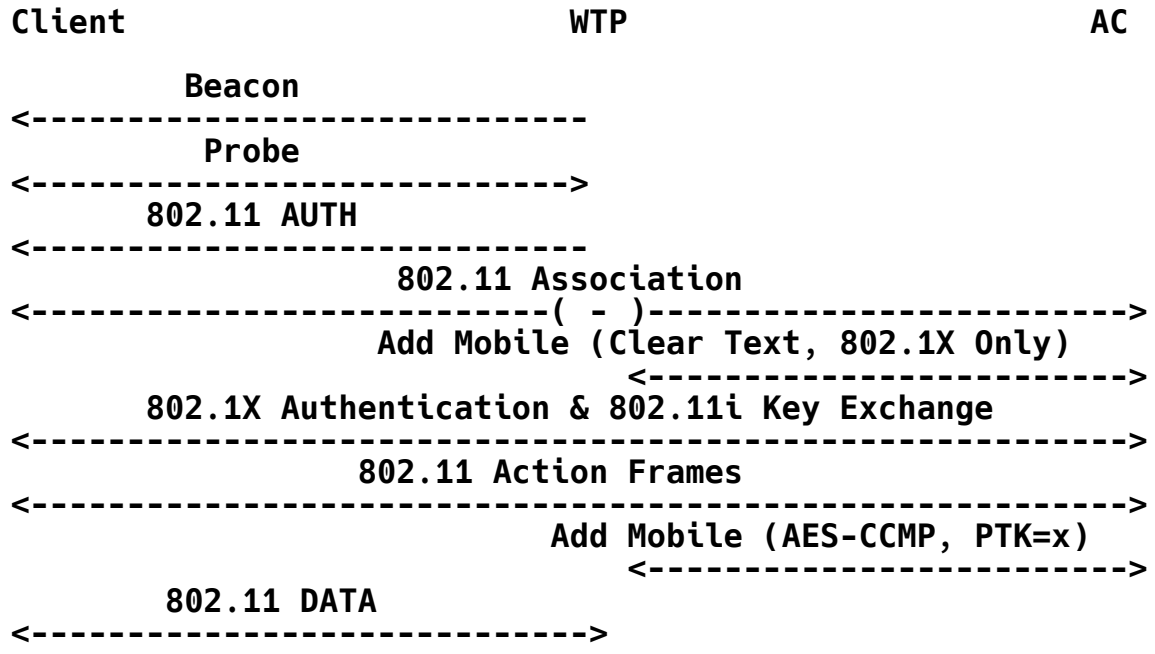


Figure 6: Local MAC Message Flow

Figure 6 provides an illustration of the division of labor in a Local MAC architecture. In this example, a WLAN has been created that is configured for 802.11i, using AES-CCMP for privacy. The following process occurs:

- The WTP generates the 802.11 beacon frames, using information provided to it through the Add WLAN (see Section 11.8.1.1) message element.
- The WTP processes the Probe Request and responds with a corresponding Probe Response.
- The WTP forwards the 802.11 Authentication and Association frames to the AC, which is responsible for responding to the client.

- Once the association is complete, the AC transmits an LWAPP Add Mobile Request to the WTP (see Section 11.7.1.1. In the above example, the WLAN is configured for 802.1X, and therefore the '802.1X only' policy bit is enabled.

- The WTP forwards all 802.1X and 802.11i key exchange messages to the AC for processing.

- The AC transmits another Add Mobile Request to the WTP, stating the security policy to enforce for the client (in this case, AES-CCMP), as well as the encryption key to use. The Add Mobile Request MAY include a VLAN name, which when present is used by the WTP to identify the VLAN on which the user's data frames are to be bridged.

- The WTP forwards any 802.11 Action frames received to the AC.

- The WTP locally bridges all client data frames, and provides the necessary encryption and decryption services.

11.2. Roaming Behavior and 802.11 Security

It is important that LWAPP implementations react properly to mobile devices associating to the networks in how they generate Add Mobile and Delete Mobile messages. This section expands upon the examples provided in the previous section, and describes how the LWAPP control protocol is used in order to provide secure roaming.

Once a client has successfully associated with the network in a secure fashion, it is likely to attempt to roam to another access point. Figure 7 shows an example of a currently associated station moving from its "Old WTP" to a new "WTP". The figure is useful for multiple different security policies, including standard 802.1X and dynamic WEP keys, WPA or even WPA2 both with key caching (where the 802.1x exchange would be bypassed) and without.

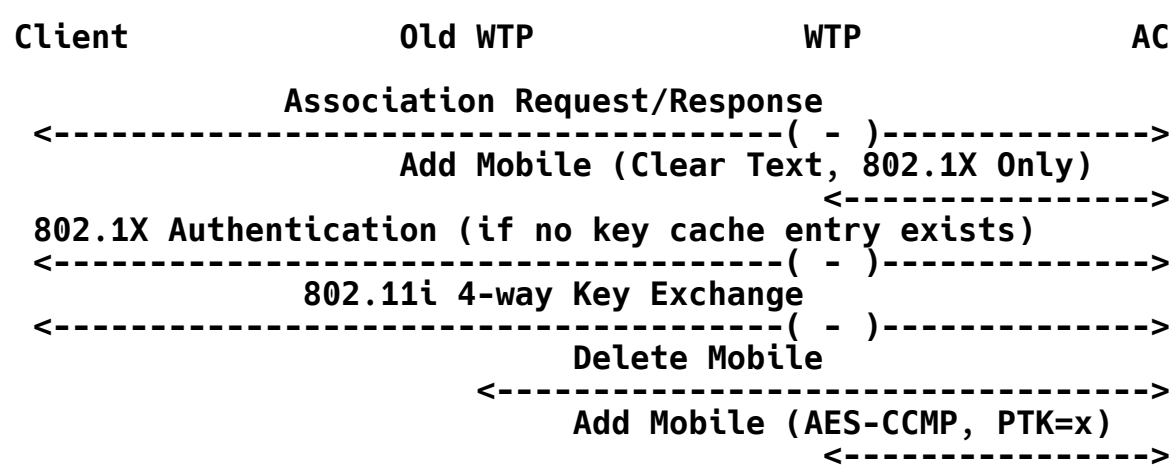


Figure 7: Client Roaming Example

11.3. Transport-Specific Bindings

All LWAPP transports have the following IEEE 802.11 specific bindings:

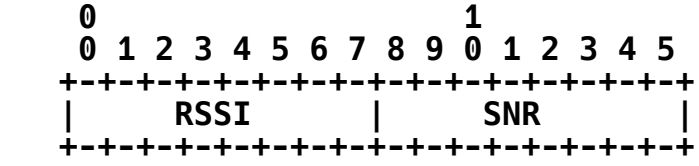
11.3.1. Status and WLANS Field

The interpretation of this 16-bit field depends on the direction of transmission of the packet. Refer to the figure in Section 3.1.

Status

When an LWAPP packet is transmitted from a WTP to an AC, this field is called the Status field and indicates radio resource information associated with the frame. When the message is an LWAPP control message this field is transmitted as zero.

The Status field is divided into the signal strength and signal-to-noise ratio with which an IEEE 802.11 frame was received, encoded in the following manner:

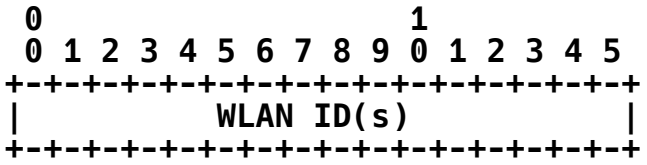


RSSI: RSSI is a signed, 8-bit value. It is the received signal strength indication, in dBm.

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

WLANs field: When an LWAPP data message is transmitted from an AC to a WTP, this 16-bit field indicates on which WLANs the encapsulated IEEE 802.11 frame is to be transmitted. For unicast packets, this field is not used by the WTP. For broadcast or multicast packets, the WTP might require this information if it provides encryption services.

Given that a single broadcast or multicast packet might need to be sent to multiple wireless LANs (presumably each with a different broadcast key), this field is defined as a bit field. A bit set indicates a WLAN ID (see Section 11.8.1.1), which will be sent the data. The WLANS field is encoded in the following manner:



11.4. BSSID to WLAN ID Mapping

The LWAPP protocol makes assumptions regarding the BSSIDs used on the WTP. It is a requirement for the WTP to use a contiguous block of BSSIDs. The WLAN Identifier field, which is managed by the AC, is used as an offset into the BSSID list.

For instance, if a WTP had a base BSSID address of 00:01:02:00:00:00, and the AC sent an Add WLAN message with a WLAN Identifier of 2 (see Section 11.8.1.1), the BSSID for the specific WLAN on the WTP would be 00:01:02:00:00:02.

The WTP communicates the maximum number of BSSIDs that it supports during the Config Request within the IEEE 802.11 WTP WLAN Radio Configuration message element (see Section 11.9.1).

11.5. Quality of Service

It is recommended that 802.11 MAC management be sent by both the AC and the WTP with appropriate Quality-of-Service (QoS) values, ensuring that congestion in the network minimizes occurrences of packet loss. Therefore, a QoS-enabled LWAPP device should use:

802.1P: The precedence value of 6 SHOULD be used for all 802.11 MAC management messages, except for Probe Requests, which SHOULD use 4.

DSCP: The DSCP tag value of 46 SHOULD be used for all 802.11 MAC management messages, except for Probe Requests, which SHOULD use 34.

11.6. Data Message Bindings

There are no LWAPP data message bindings for IEEE 802.11.

11.7. Control Message Bindings

The IEEE 802.11 binding has the following control message definitions.

11.7.1. Mobile Config Request

This section contains the 802.11-specific message elements that are used with the Mobile Config Request.

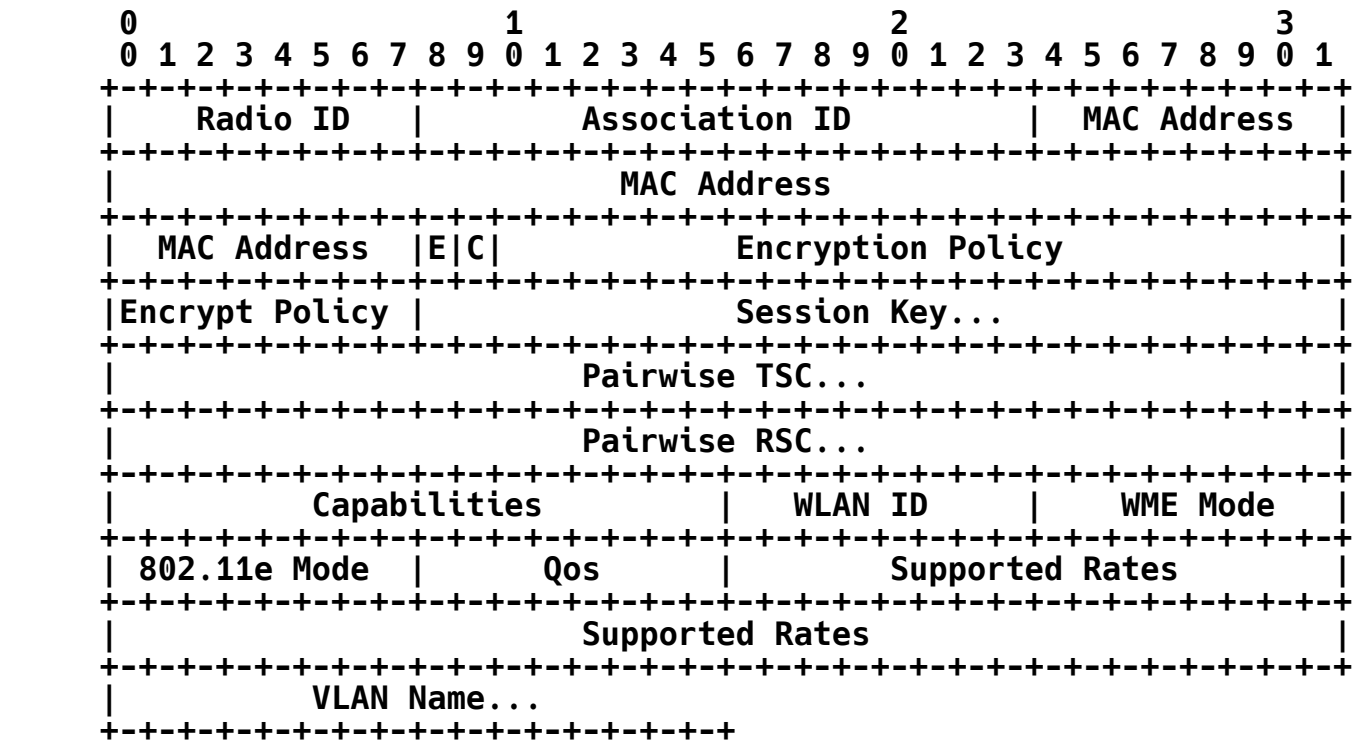
11.7.1.1. Add Mobile

The Add Mobile Request is used by the AC to inform a WTP that it should forward traffic from a particular mobile station. The Add Mobile Request may also include security parameters that must be enforced by the WTP for the particular mobile.

When the AC sends an Add Mobile Request, it includes any security parameters that may be required. An AC that wishes to update a mobile's policy on a WTP may do so by simply sending a new Add Mobile message element.

When a WTP receives an Add Mobile message element, it must first override any existing state it may have for the mobile station in question. The latest Add Mobile overrides any previously received messages. If the Add Mobile message element's EAP-Only bit is set, the WTP MUST drop all 802.11 packets that do not contain EAP packets. Note that when EAP Only is set, the Encryption Policy field MAY have additional values, and therefore it is possible to inform a WTP to only accept encrypted EAP packets. Once the mobile station has successfully completed EAP authentication, the AC must send a new Add Mobile message element to push the session key down to the WTP as well as to remove the EAP Only restriction.

If the QoS field is set, the WTP MUST observe and provide policing of the 802.11e priority tag to ensure that it does not exceed the value provided by the AC.



Type: 29 for Add Mobile

Length: 36

Radio ID: An 8-bit value representing the radio.

Association ID: A 16-bit value specifying the 802.11 Association Identifier.

MAC Address: The mobile station's MAC address.

E: The 1-bit field is set by the AC to inform the WTP that it MUST NOT accept any 802.11 data frames, other than 802.1X frames. This is the equivalent of the WTP's 802.1X port for the mobile station to be in the closed state. When set, the WTP MUST drop any non-802.1X packets it receives from the mobile station.

C: The 1-bit field is set by the AC to inform the WTP that encryption services will be provided by the AC. When set, the WTP SHOULD police frames received from stations to ensure that they comply to the stated encryption policy, but does not need to take specific cryptographic action on the frame. Similarly, for transmitted frames, the WTP only needs to forward already encrypted frames.

Encryption Policy: The policy field informs the WTP how to handle packets from/to the mobile station. The following values are supported:

- 0 - Encrypt WEP 104: All packets to/from the mobile station must be encrypted using a standard 104-bit WEP.
- 1 - Clear Text: All packets to/from the mobile station do not require any additional crypto processing by the WTP.
- 2 - Encrypt WEP 40: All packets to/from the mobile station must be encrypted using a standard 40-bit WEP.
- 3 - Encrypt WEP 128: All packets to/from the mobile station must be encrypted using a standard 128-bit WEP.
- 4 - Encrypt AES-CCMP 128: All packets to/from the mobile station must be encrypted using a 128-bit AES-CCMP [7].
- 5 - Encrypt TKIP-MIC: All packets to/from the mobile station must be encrypted using Temporal Key Integrity Protocol (TKIP) and authenticated using Michael [16].

Session Key: A 32-octet session key the WTP is to use when encrypting traffic to or decrypting traffic from the mobile station. The type of key is determined based on the Encryption Policy field.

Pairwise TSC: The TKIP Sequence Counter (TSC) to use for unicast packets transmitted to the mobile.

Pairwise RSC: The Receive Sequence Counter (RSC) to use for unicast packets received from the mobile.

Capabilities: A 16-bit field containing the 802.11 capabilities to use with the mobile.

WLAN ID: An 8-bit value specifying the WLAN Identifier.

WME Mode: An 8-bit Boolean used to identify whether the station is WME capable. A value of zero is used to indicate that the station is not Wireless Multimedia Extension (WME) capable, while a value of one means that the station is WME capable.

802.11e Mode: An 8-bit Boolean used to identify whether the station is 802.11e-capable. A value of zero is used to indicate that the station is not 802.11e-capable, while a value of one means that the station is 802.11e-capable.

QoS: An 8-bit value specifying the QoS policy to enforce for the station. The following values are supported: PRC: TO CHECK

0 - Silver (Best Effort)

1 - Gold (Video)

2 - Platinum (Voice)

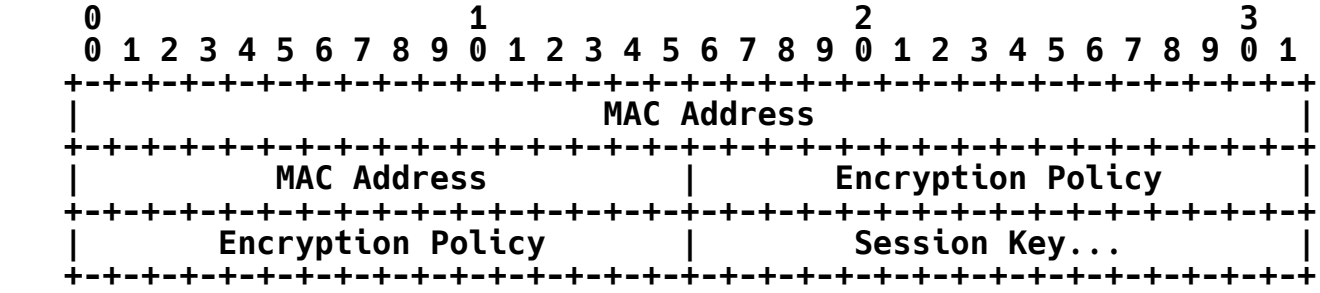
3 - Bronze (Background)

Supported Rates: The supported rates to be used with the mobile station.

VLAN Name: An optional variable string containing the VLAN Name on which the WTP is to locally bridge user data. Note that this field is only valid with Local MAC WTPs.

11.7.1.2. IEEE 802.11 Mobile Session Key

The Mobile Session Key Payload message element is sent when the AC determines that encryption of a mobile station must be performed in the WTP. This message element MUST NOT be present without the Add Mobile message element, and MUST NOT be sent if the WTP had not specifically advertised support for the requested encryption scheme (see Section 11.7.1.1).



Type: 105 for IEEE 802.11 Mobile Session Key

Length: >= 11

MAC Address: The mobile station's MAC address.

Encryption Policy: The policy field informs the WTP how to handle packets from/to the mobile station. The following values are supported:

0 - Encrypt WEP 104: All packets to/from the mobile station must be encrypted using a standard 104-bit WEP.

1 - Clear Text: All packets to/from the mobile station do not require any additional crypto processing by the WTP.

2 - Encrypt WEP 40: All packets to/from the mobile station must be encrypted using a standard 40-bit WEP.

3 - Encrypt WEP 128: All packets to/from the mobile station must be encrypted using a standard 128-bit WEP.

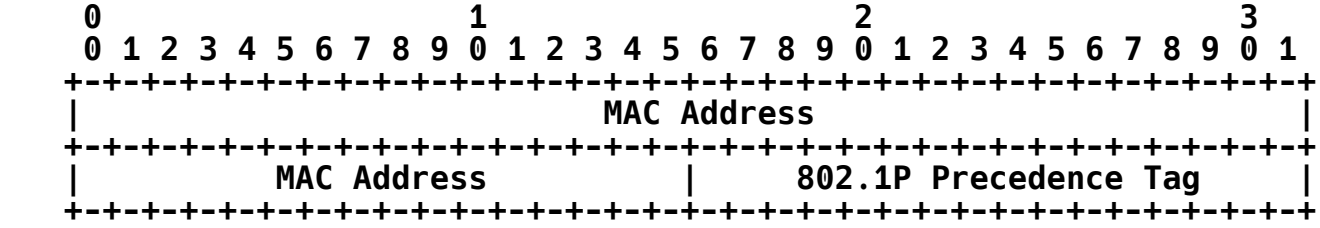
4 - Encrypt AES-CCMP 128: All packets to/from the mobile station must be encrypted using a 128-bit AES-CCMP [7].

5 - Encrypt TKIP-MIC: All packets to/from the mobile station must be encrypted using TKIP and authenticated using Michael [16].

Session Key: The session key the WTP is to use when encrypting traffic to/from the mobile station.

11.7.1.3. Station QoS Profile

The Station QoS Profile Payload message element contains the maximum 802.11e priority tag that may be used by the station. Any packets received that exceed the value encoded in this message element must either be dropped or tagged using the maximum value permitted to the user. The priority tag must be between zero (0) and seven (7).



Type: 140 for IEEE 802.11 Station QoS Profile

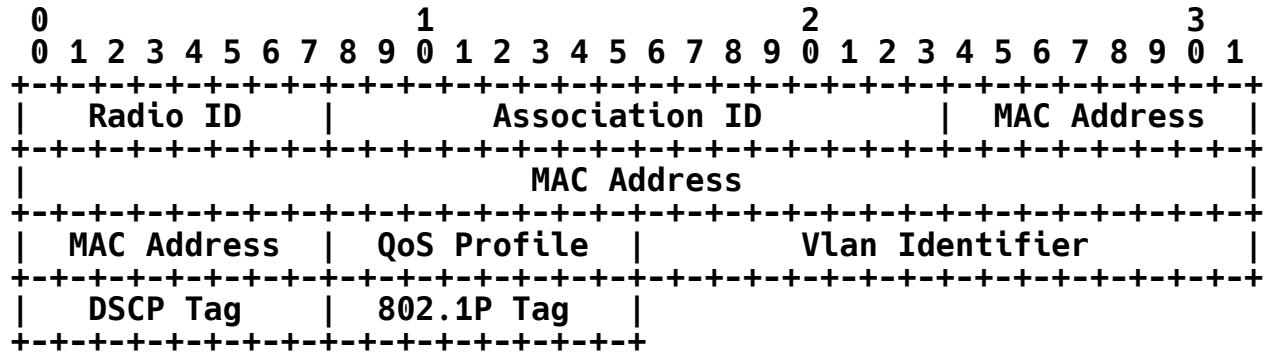
Length: 12

MAC Address: The mobile station's MAC address.

802.1P Precedence Tag: The maximum 802.1P precedence value that the WTP will allow in the Traffic Identifier (TID) field in the extended 802.11e QoS Data header.

11.7.1.4. IEEE 802.11 Update Mobile QoS

The Update Mobile QoS message element is used to change the Quality-of-Service policy on the WTP for a given mobile station.



Type: 106 for IEEE 802.11 Update Mobile QoS

Length: 14

Radio ID: The Radio Identifier, typically refers to some interface index on the WTP.

Association ID: The 802.11 Association Identifier.

MAC Address: The mobile station's MAC address.

QoS Profile: An 8-bit value specifying the QoS policy to enforce for the station. The following values are supported:

0 - Silver (Best Effort)

1 - Gold (Video)

2 - Platinum (Voice)

3 - Bronze (Background)

VLAN Identifier: PRC.

DSCP Tag: The DSCP label to use if packets are to be DSCP tagged.

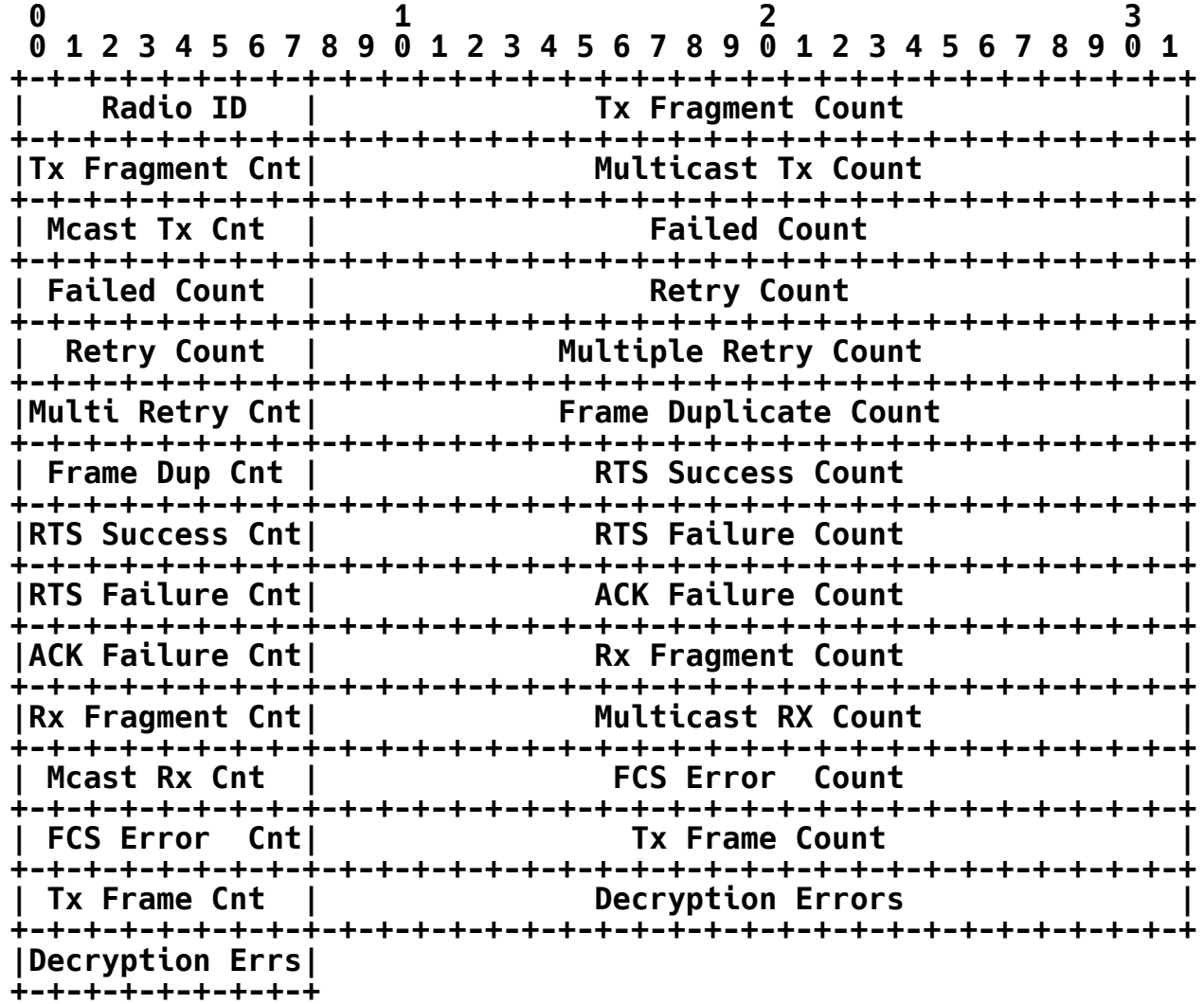
802.1P Tag: The 802.1P precedence value to use if packets are to be 802.1P-tagged.

11.7.2. WTP Event Request

This section contains the 802.11-specific message elements that are used with the WTP Event Request message.

11.7.2.1. IEEE 802.11 Statistics

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



Type: 38 for Statistics

Length: 57

Radio ID: An 8-bit value representing the radio.

Tx Fragment Count: A 32-bit value representing the number of fragmented frames transmitted.

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

Failed Count: A 32-bit value representing the transmit excessive retries.

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

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

Frame Duplicate Count: A 32-bit value representing the duplicate frames received.

RTS Success Count: A 32-bit value representing the number of successfully transmitted Ready To Send (RTS).

RTS Failure Count: A 32-bit value representing the failed transmitted RTS.

ACK Failure Count: A 32-bit value representing the number of failed acknowledgements.

Rx Fragment Count: A 32-bit value representing the number of fragmented frames received.

Multicast RX Count: A 32-bit value representing the number of multicast frames received.

FCS Error Count: A 32-bit value representing the number of Frame Check Sequence (FCS) failures.

Decryption Errors: A 32-bit value representing the number of Decryption errors that occurred on the WTP. Note that this field is only valid in cases where the WTP provides encryption/ decryption services.

11.8. 802.11 Control Messages

This section will define LWAPP control messages that are specific to the IEEE 802.11 binding.

11.8.1. IEEE 802.11 WLAN Config Request

The IEEE 802.11 WLAN Configuration Request is sent by the AC to the WTP in order to change services provided by the WTP. This control message is used to either create, update, or delete a WLAN on the WTP.

The IEEE 802.11 WLAN Configuration Request is sent as a result of either some manual administrative process (e.g., deleting a WLAN), or automatically to create a WLAN on a WTP. When sent automatically to create a WLAN, this control message is sent after the LWAPP Configuration Request message has been received by the WTP.

Upon receiving this control message, the WTP will modify the necessary services, and transmit an IEEE 802.11 WLAN Configuration Response.

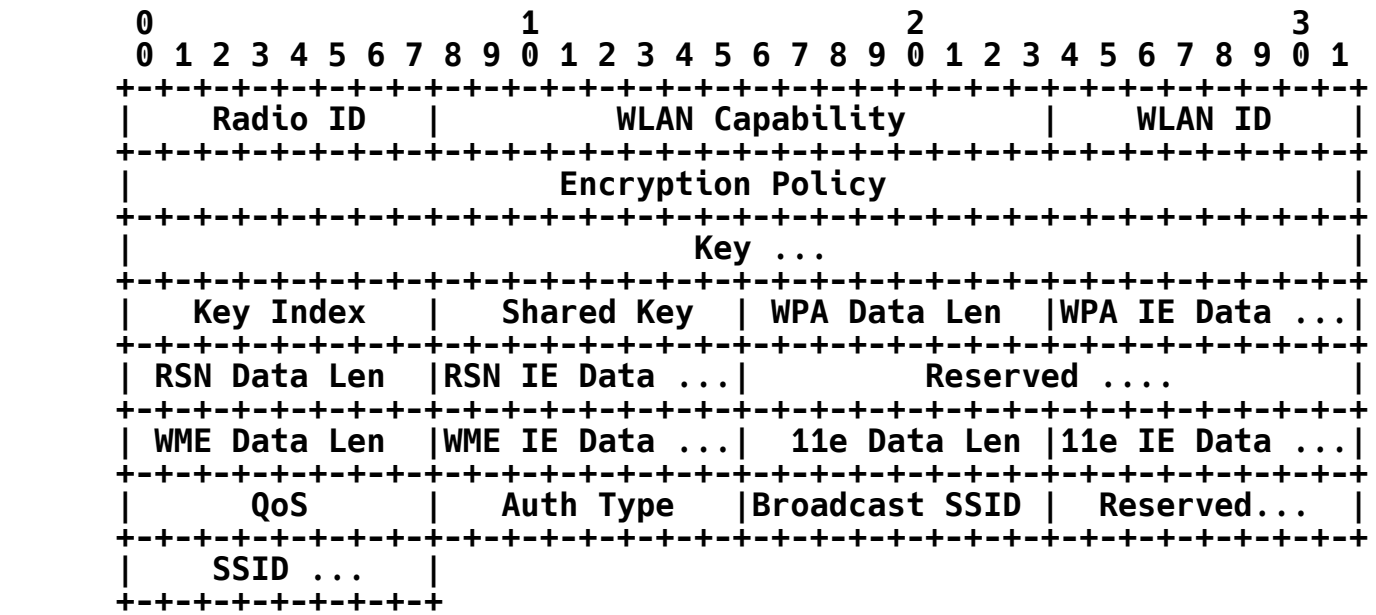
An WTP MAY provide service for more than one WLAN: therefore, every WLAN is identified through a numerical index. For instance, a WTP that is capable of supporting up to 16 SSIDs could accept up to 16 IEEE 802.11 WLAN Configuration Request messages that include the Add WLAN message element.

Since the index is the primary identifier for a WLAN, an AC SHOULD attempt to ensure that the same WLAN is identified through the same index number on all of its WTPs. An AC that does not follow this approach MUST find some other means of maintaining a WLAN Identifier to SSID mapping table.

The following subsections define the message elements that are of value for this LWAPP operation. Only one message MUST be present.

11.8.1.1. IEEE 802.11 Add WLAN

The Add WLAN message element is used by the AC to define a wireless LAN on the WTP. The value contains the following format:



Type: 7 for IEEE 802.11 Add WLAN

Length: >= 298

Radio ID: An 8-bit value representing the radio.

WLAN Capability: A 16-bit value containing the capabilities to be advertised by the WTP within the Probe and Beacon messages.

WLAN ID: A 16-bit value specifying the WLAN Identifier.

Encryption Policy: A 32-bit value specifying the encryption scheme to apply to traffic to and from the mobile station.

The following values are supported:

0 - Encrypt WEP 104: All packets to/from the mobile station must be encrypted using a standard 104-bit WEP.

1 - Clear Text: All packets to/from the mobile station do not require any additional crypto processing by the WTP.

2 - Encrypt WEP 40: All packets to/from the mobile station must be encrypted using a standard 40-bit WEP.

3 - Encrypt WEP 128: All packets to/from the mobile station must be encrypted using a standard 128-bit WEP.

4 - Encrypt AES-CCMP 128: All packets to/from the mobile station must be encrypted using a 128-bit AES-CCMP [7].

5 - Encrypt TKIP-MIC: All packets to/from the mobile station must be encrypted using TKIP and authenticated using Michael [16].

6 - Encrypt CKIP: All packets to/from the mobile station must be encrypted using Cisco TKIP.

Key: A 32-byte session key to use with the encryption policy.

Key-Index: The Key Index associated with the key.

Shared Key: A 1-byte Boolean that specifies whether the key included in the Key field is a shared WEP key. A value of zero is used to state that the key is not a shared WEP key, while a value of one is used to state that the key is a shared WEP key.

WPA Data Len: Length of the WPA Information Element (IE).

WPA IE: A 32-byte field containing the WPA Information Element.

RSN Data Len: Length of the Robust Security Network (RSN) IE.

RSN IE: A 64-byte field containing the RSN Information Element.

Reserved: A 49-byte reserved field, which MUST be set to zero (0).

WME Data Len: Length of the WME IE.

WME IE: A 32-byte field containing the WME Information Element.

DOT11E Data Len: Length of the 802.11e IE.

DOT11E IE: A 32-byte field containing the 802.11e Information Element.

QOS: An 8-bit value specifying the QoS policy to enforce for the station.

The following values are supported:

0 - Silver (Best Effort)

1 - Gold (Video)

2 - Platinum (Voice)

3 - Bronze (Background)

Auth Type: An 8-bit value specifying the station's authentication type.

The following values are supported:

0 - Open System

1 - WEP Shared Key

2 - WPA/WPA2 802.1X

3 - WPA/WPA2 PSK

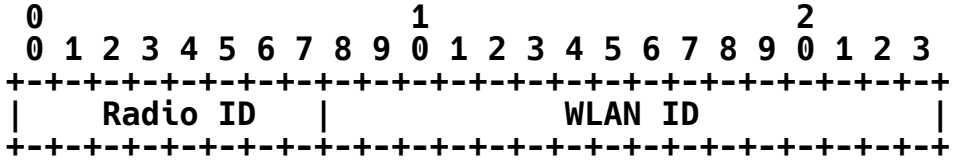
Broadcast SSID: A Boolean indicating whether the SSID is to be broadcast by the WTP. A value of zero disables SSID broadcast, while a value of one enables it.

Reserved: A 40-byte reserved field.

SSID: The SSID attribute is the service set identifier that will be advertised by the WTP for this WLAN.

11.8.1.2. IEEE 802.11 Delete WLAN

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



Type: 28 for IEEE 802.11 Delete WLAN

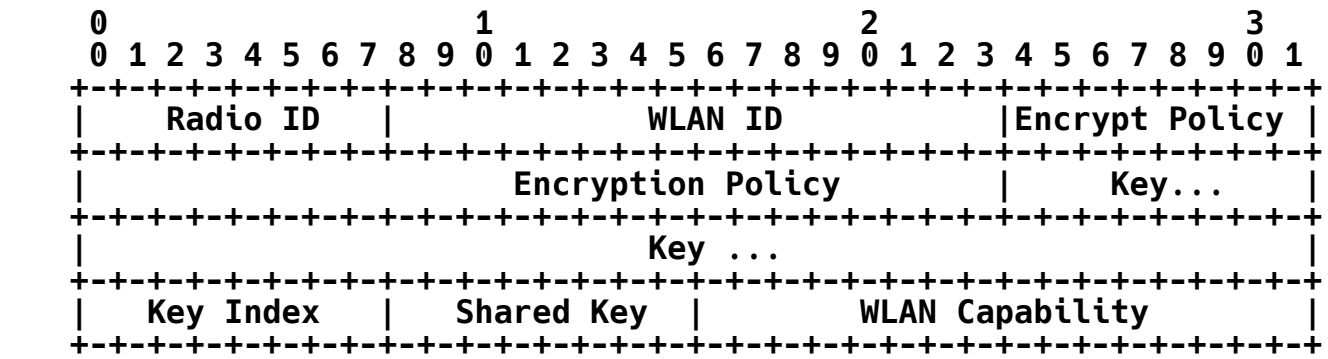
Length: 3

Radio ID: An 8-bit value representing the radio

WLAN ID: A 16-bit value specifying the WLAN Identifier

11.8.1.3. IEEE 802.11 Update WLAN

The Update WLAN message element is used by the AC to define a wireless LAN on the WTP. The value contains the following format:



Type: 34 for IEEE 802.11 Update WLAN

Length: 43

Radio ID: An 8-bit value representing the radio.

WLAN ID: A 16-bit value specifying the WLAN Identifier.

Encryption Policy: A 32-bit value specifying the encryption scheme to apply to traffic to and from the mobile station.

The following values are supported:

0 - Encrypt WEP 104: All packets to/from the mobile station must be encrypted using a standard 104-bit WEP.

1 - Clear Text: All packets to/from the mobile station do not require any additional crypto processing by the WTP.

2 - Encrypt WEP 40: All packets to/from the mobile station must be encrypted using a standard 40-bit WEP.

3 - Encrypt WEP 128: All packets to/from the mobile station must be encrypted using a standard 128-bit WEP.

4 - Encrypt AES-CCMP 128: All packets to/from the mobile station must be encrypted using a 128-bit AES-CCMP [7].

5 - Encrypt TKIP-MIC: All packets to/from the mobile station must be encrypted using TKIP and authenticated using Michael [16].

6 - Encrypt CKIP: All packets to/from the mobile station must be encrypted using Cisco TKIP.

Key: A 32-byte session key to use with the encryption policy.

Key-Index: The Key Index associated with the key.

Shared Key: A 1-byte Boolean that specifies whether the key included in the Key field is a shared WEP key. A value of zero means that the key is not a shared WEP key, while a value of one is used to state that the key is a shared WEP key.

WLAN Capability: A 16-bit value containing the capabilities to be advertised by the WTP within the Probe and Beacon messages.

11.8.2. IEEE 802.11 WLAN Config Response

The IEEE 802.11 WLAN Configuration Response is sent by the WTP to the AC as an acknowledgement of the receipt of an IEEE 802.11 WLAN Configuration Request.

This LWAPP control message does not include any message elements.

11.8.3. IEEE 802.11 WTP Event

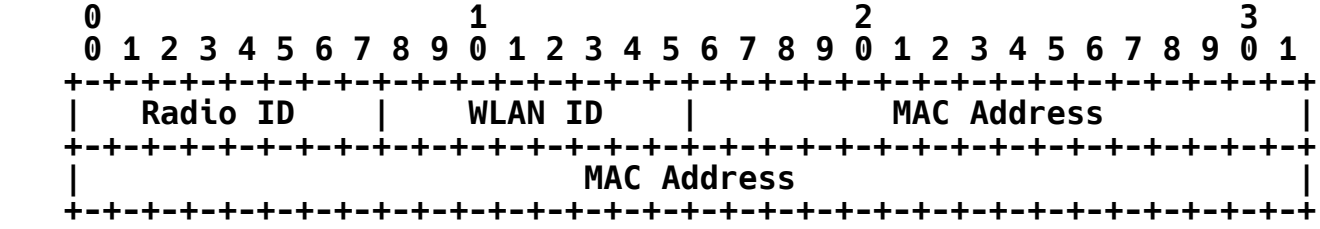
The IEEE 802.11 WTP Event LWAPP message is used by the WTP in order to report asynchronous events to the AC. There is no reply message expected from the AC, except that the message is acknowledged via the reliable transport.

When the AC receives the IEEE 802.11 WTP Event, it will take whatever action is necessary, depending upon the message elements present in the message.

The IEEE 802.11 WTP Event message MUST contain one of the following message elements described in the next subsections.

11.8.3.1. IEEE 802.11 MIC Countermeasures

The MIC Countermeasures message element is sent by the WTP to the AC to indicate the occurrence of a MIC failure.



Type: 61 for IEEE 802.11 MIC Countermeasures

Length: 8

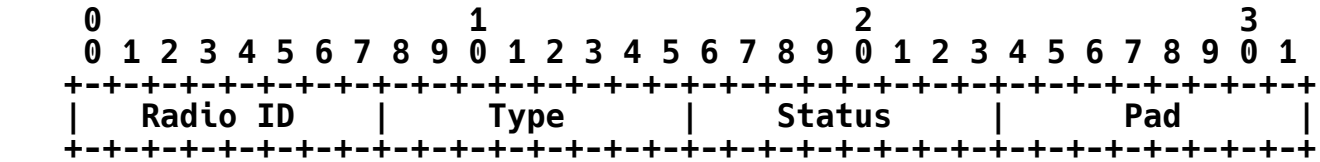
Radio ID: The Radio Identifier, typically refers to some interface index on the WTP.

WLAN ID: This 8-bit unsigned integer includes the WLAN Identifier, on which the MIC failure occurred.

MAC Address: The MAC address of the mobile station that caused the MIC failure.

11.8.3.2. IEEE 802.11 WTP Radio Fail Alarm Indication

The WTP Radio Fail Alarm Indication message element is sent by the WTP to the AC when it detects a radio failure.



Type: 95 for WTP Radio Fail Alarm Indication

Length: 4

Radio ID: The Radio Identifier, typically refers to some interface index on the WTP.

Type: The type of radio failure detected. The following values are supported:

1 - Receiver

2 - Transmitter

Status: An 8-bit Boolean indicating whether the radio failure is being reported or cleared. A value of zero is used to clear the event, while a value of one is used to report the event.

Pad: Reserved field MUST be set to zero (0).

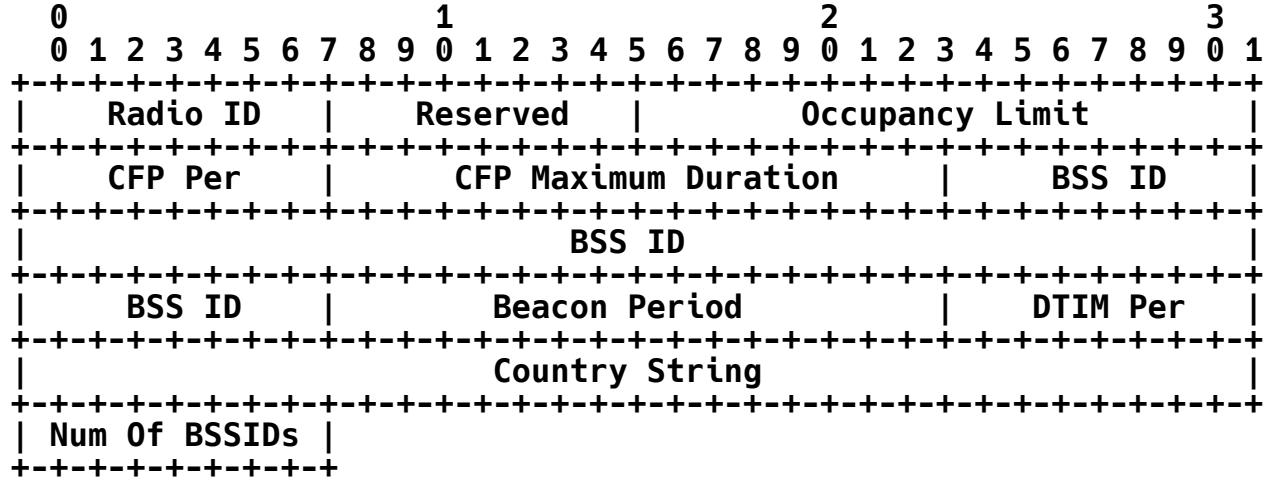
11.9. Message Element Bindings

The IEEE 802.11 Message Element binding has the following definitions:

	Conf Req	Conf Resp	Conf Upd	Add Mobile
IEEE 802.11 WTP WLAN Radio Configuration	X	X	X	
IEEE 802.11 Rate Set		X	X	
IEEE 802.11 Multi-domain Capability	X	X	X	
IEEE 802.11 MAC Operation	X	X	X	
IEEE 802.11 Tx Power	X	X	X	
IEEE 802.11 Tx Power Level	X			
IEEE 802.11 Direct Sequence Control	X	X	X	
IEEE 802.11 OFDM Control	X	X	X	
IEEE 802.11 Supported Rates	X	X		
IEEE 802.11 Antenna	X	X	X	
IEEE 802.11 CFP Status	X		X	
IEEE 802.11 Broadcast Probe Mode		X	X	
IEEE 802.11 WTP Mode and Type	X?		X	
IEEE 802.11 WTP Quality of Service		X	X	
IEEE 802.11 MIC Error Report From Mobile			X	
IEEE 802.11 Update Mobile QoS				X
IEEE 802.11 Mobile Session Key				X

11.9.1. IEEE 802.11 WTP WLAN Radio Configuration

The WTP WLAN radio configuration is used by the AC to configure a Radio on the WTP. The message element value contains the following Fields:



Type: 8 for IEEE 802.11 WTP WLAN Radio Configuration

Length: 20

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

Reserved: MUST be set to zero

Occupancy Limit: This attribute indicates the maximum amount of time, in Time Units (TUs), 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 Distributed Coordination Function (DCF) access to the medium. The default value of this attribute SHOULD be 100, and the maximum value SHOULD be 1000.

CFP Period: The attribute describes the number of DTIM intervals between the start of Contention-Free Periods (CFPs).

CFP Maximum Duration: The attribute describes the maximum duration of the CFP in TU that MAY be generated by the Point Coordination Function (PCF).

BSSID: The WLAN Radio's base MAC address. For WTPs that support more than a single WLAN, the value of the WLAN Identifier is added to the last octet of the BSSID. Therefore, a WTP that supports 16 WLANs MUST have 16 MAC addresses reserved for it, and the last nibble is used to represent the WLAN ID.

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

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.

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,

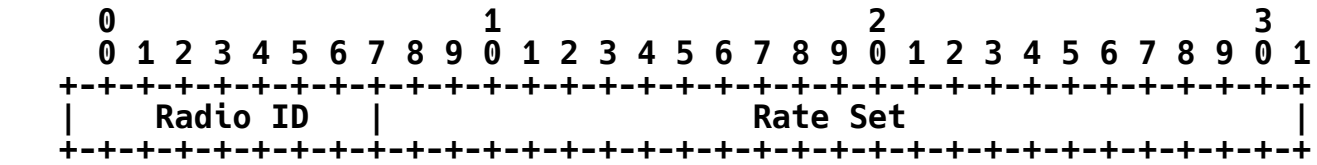
2. an ASCII 'O' character, if the regulations under which the station is operating are for an outdoor environment only, or

3. an ASCII 'I' character, if the regulations under which the station is operating are for an indoor environment only.

Number of BSSIDs: This attribute contains the maximum number of BSSIDs supported by the WTP. This value restricts the number of logical networks supported by the WTP.

11.9.2. IEEE 802.11 Rate Set

The Rate Set message element value is sent by the AC and contains the supported operational rates. It contains the following fields:



Type: 16 for IEEE 802.11 Rate Set

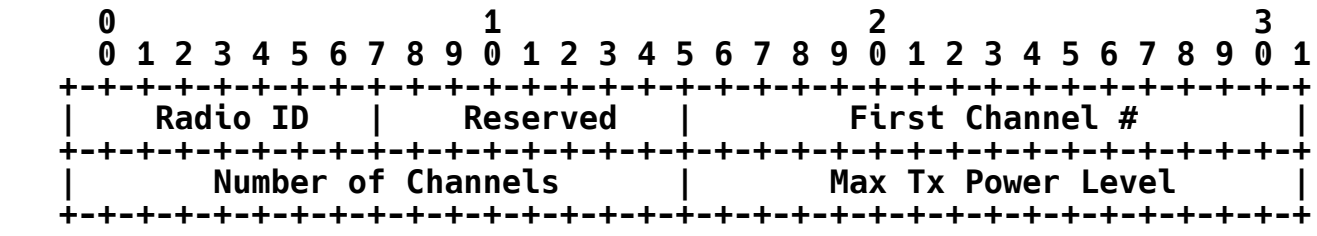
Length: 4

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

Rate Set: The AC generates the Rate Set that the WTP is to include in its Beacon and Probe messages.

11.9.3. IEEE 802.11 Multi-Domain Capability

The Multi-Domain Capability message element is used by the AC to inform the WTP of regulatory limits. The value contains the following fields:



Type: 10 for IEEE 802.11 Multi-Domain Capability

Length: 8

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

Reserved: MUST be set to zero

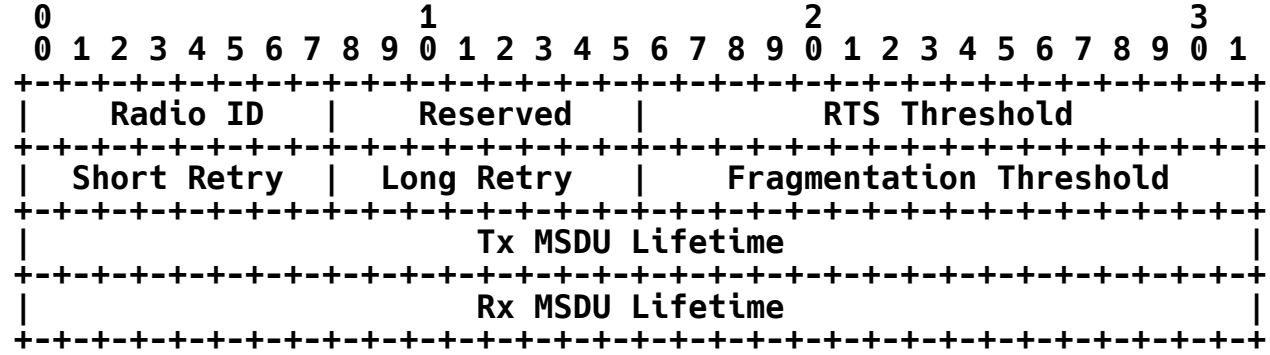
First Channel #: This attribute indicates the value of the lowest channel number in the subband for the associated domain country string.

Number of Channels: This attribute indicates the value of the total number of channels allowed in the subband for the associated domain country string.

Max Tx Power Level: This attribute indicates the maximum transmit power, in dBm, allowed in the subband for the associated domain country string.

11.9.4. IEEE 802.11 MAC Operation

The MAC Operation message element is sent by the AC to set the 802.11 MAC parameters on the WTP. The value contains the following fields:



Type: 11 for IEEE 802.11 MAC Operation

Length: 16

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

Reserved: MUST be set to zero

RTS Threshold: This attribute indicates the number of octets in a Management Protocol Data Unit (MPDU), below which an RTS/CTS (clear to send) 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 MAC Service Data Unit (MSDU) size MUST have the effect of turning off the RTS/CTS handshake for frames of Data or Management type transmitted by this Station (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.

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.

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.

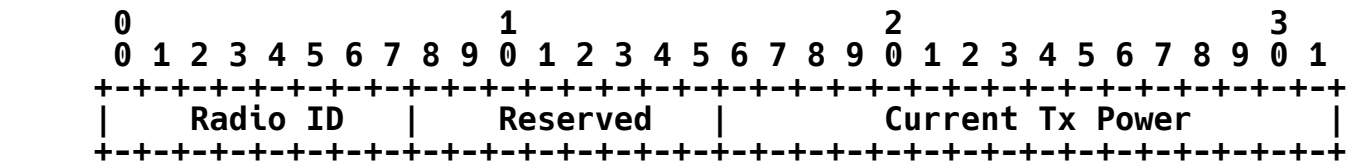
Fragmentation Threshold: This attribute specifies the current maximum size, in octets, of the MPDU that MAY be delivered to the PHY. An MSDU MUST be broken into fragments if its size exceeds the value of this attribute after adding MAC headers and trailers. An MSDU or MAC Management Protocol Data Unit (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.

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.

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.

11.9.5. IEEE 802.11 Tx Power

The Tx Power message element value is bi-directional. When sent by the WTP, it contains the current power level of the radio in question. When sent by the AC, it contains the power level to which the WTP MUST adhere:



Type: 12 for IEEE 802.11 Tx Power

Length: 4

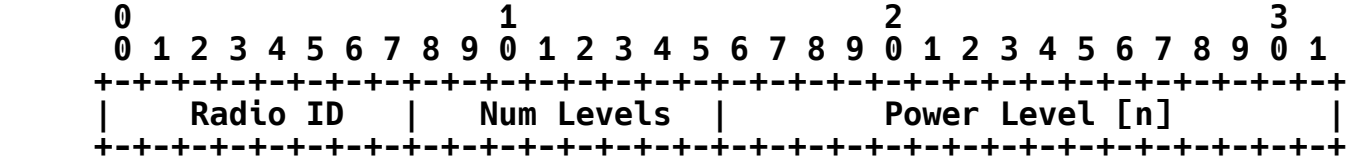
Radio ID: An 8-bit value representing the radio to configure.

Reserved: MUST be set to zero

Current Tx Power: This attribute contains the transmit output power in mW.

11.9.6. IEEE 802.11 Tx Power Level

The Tx Power Level message element is sent by the WTP and contains the different power levels supported. The value contains the following fields:



Type: 13 for IEEE 802.11 Tx Power Level

Length: >= 4

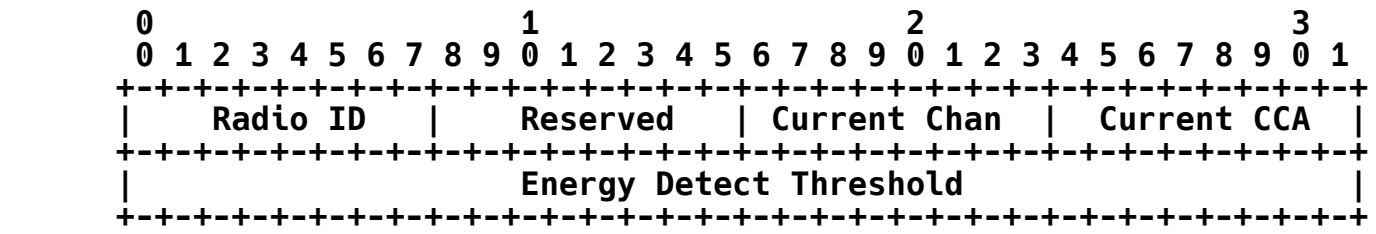
Radio ID: An 8-bit value representing the radio to configure.

Num Levels: The number of power level attributes.

Power Level: Each power level fields contains a supported power level, in mW.

11.9.7. IEEE 802.11 Direct Sequence Control

The Direct Sequence Control message element is a bi-directional element. When sent by the WTP, it contains the current state. When sent by the AC, the WTP MUST adhere to the values. This element is only used for 802.11b radios. The value has the following fields.



Type: 14 for IEEE 802.11 Direct Sequence Control

Length: 8

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

Reserved: MUST be set to zero

Current Channel: This attribute contains the current operating frequency channel of the Direct Sequence Spread Spectrum (DSSS) PHY.

Current CCA: The current Controlled Channel Access (CCA) method in operation. Valid values are:

1 - energy detect only (edonly)

2 - carrier sense only (csonly)

4 - carrier sense and energy detect (edandcs)

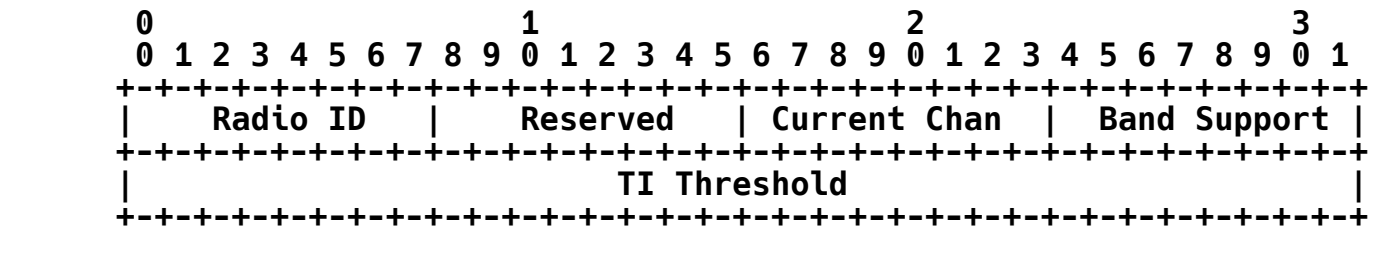
8 - carrier sense with timer (cswithtimer)

16 - high-rate carrier sense and energy detect (hrcsanded)

Energy Detect Threshold: The current Energy Detect Threshold being used by the DSSS PHY.

11.9.8. IEEE 802.11 OFDM Control

The Orthogonal Frequency Division Multiplexing (OFDM) Control message element is a bi-directional element. When sent by the WTP, it contains the current state. When sent by the AC, the WTP MUST adhere to the values. This element is only used for 802.11a radios. The value contains the following fields:



Type: 15 for IEEE 802.11 OFDM Control

Length: 8

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

Reserved: MUST be set to zero

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

Band Supported: The capability of the OFDM PHY implementation to operate in the three U-NII bands. Coded as an integer value of a 3-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

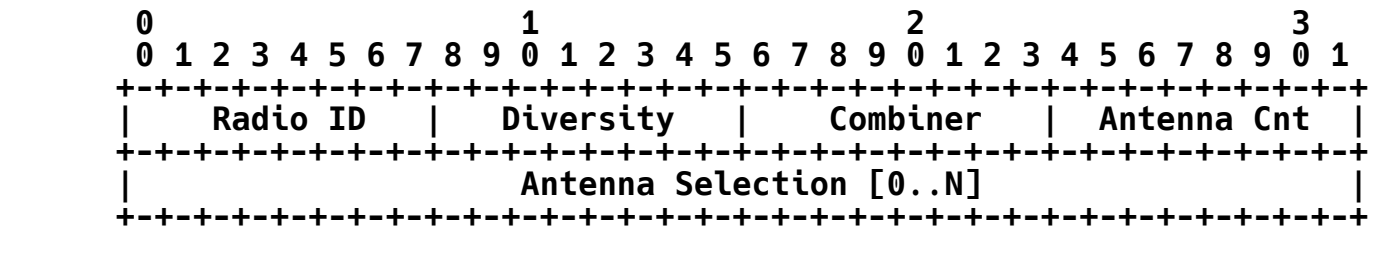
Bit 2 - capable of operating in the upper (5.725-5.825 GHz) U-NII band

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

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.

11.9.9. IEEE 802.11 Antenna

The Antenna message element is communicated by the WTP to the AC to provide information on the antennas available. The AC MAY use this element to reconfigure the WTP's antennas. The value contains the following fields:



Type: 41 for IEEE 802.11 Antenna

Length: >= 8

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

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)

Combiner: An 8-bit value specifying the combiner selection. The following values are supported:

- 1 - Sectorized (Left)
- 2 - Sectorized (Right)
- 3 - Omni
- 4 - Mimo

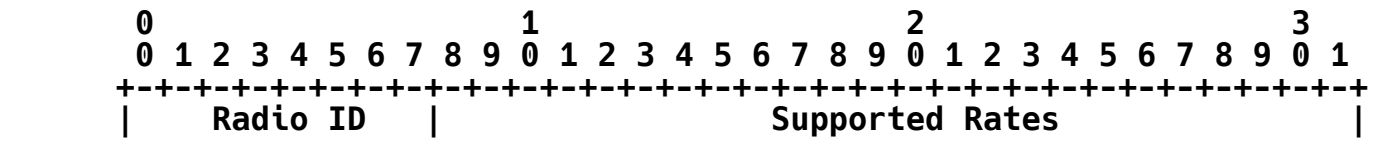
Antenna Count: An 8-bit value specifying the number of Antenna Selection fields.

Antenna Selection: One 8-bit antenna configuration value per antenna in the WTP. The following values are supported:

- 1 - Internal Antenna
- 2 - External Antenna

11.9.10. IEEE 802.11 Supported Rates

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



Type: 16 for IEEE 802.11 Supported Rates

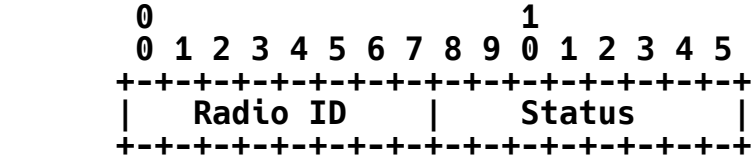
Length: 4

Radio ID: An 8-bit value representing the radio.

Supported Rates: The WTP includes the Supported Rates that its hardware supports. The format is identical to the Rate Set message element.

11.9.11. IEEE 802.11 CFP Status

The CFP Status message element is sent to provide the CF Polling configuration.



Type: 48 for IEEE 802.11 CFP Status

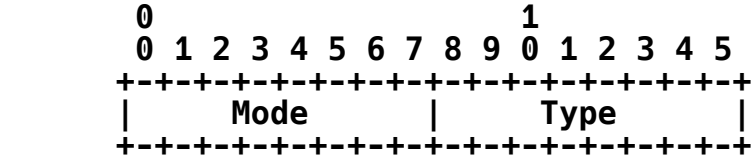
Length: 2

Radio ID: The Radio Identifier, typically refers to some interface index on the WTP.

Status: An 8-bit Boolean containing the status of the CF Polling feature. A value of zero disables CFP Status, while a value of one enables it.

11.9.12. IEEE 802.11 WTP Mode and Type

The WTP Mode and Type message element is used to configure a WTP to operate in a specific mode.



Type: 54 for IEEE 802.11 WTP Mode and Type

Length: 2

Mode: An 8-bit value describing the type of information being sent. The following values are supported:

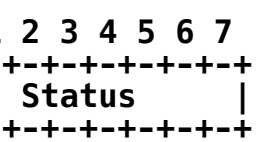
0 - Split MAC

2 - Local MAC

Type: The type field is not currently used.

11.9.13. IEEE 802.11 Broadcast Probe Mode

The Broadcast Probe Mode message element indicates whether a WTP will respond to NULL SSID Probe requests. Since broadcast NULL Probes are not sent to a specific BSSID, the WTP cannot know which SSID the sending station is querying. Therefore, this behavior must be global to the WTP.



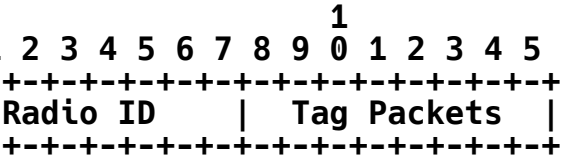
Type: 51 for IEEE 802.11 Broadcast Probe Mode

Length: 1

Status: An 8-bit Boolean indicating the status of whether a WTP shall respond to a NULL SSID Probe request. A value of zero disables the NULL SSID Probe response, while a value of one enables it.

11.9.14. IEEE 802.11 WTP Quality of Service

The WTP Quality of Service message element value is sent by the AC to the WTP to communicate quality-of-service configuration information.



Type: 57 for IEEE 802.11 WTP Quality of Service

Length: 12

Radio ID: The Radio Identifier, typically refers to some interface index on the WTP.

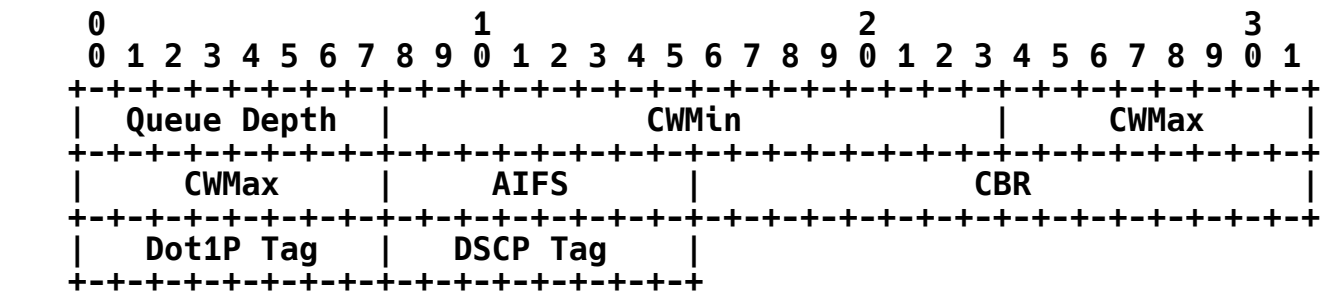
Tag Packets: A value indicating whether LWAPP packets should be tagged for QoS purposes. The following values are currently supported:

0 - Untagged

1 - 802.1P

2 - DSCP

Immediately following the above header is the following data structure. This data structure will be repeated five times, once for every QoS profile. The order of the QoS profiles is Uranium, Platinum, Gold, Silver, and Bronze.



Queue Depth: The number of packets that can be on the specific QoS transmit queue at any given time.

CWMin: The Contention Window minimum value for the QoS transmit queue.

CWMax: The Contention Window maximum value for the QoS transmit queue.

AIFS: The Arbitration Inter Frame Spacing to use for the QoS transmit queue.

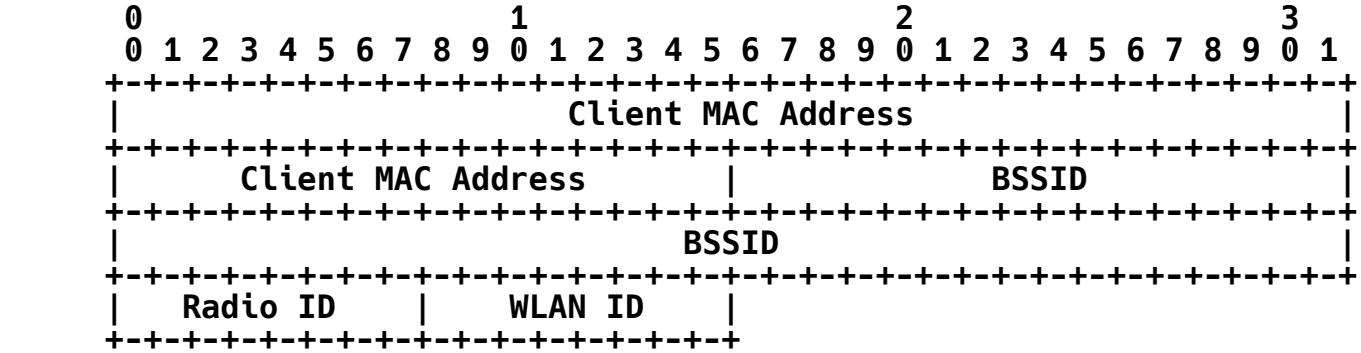
CBR: The Constant Bit Rate (CBR) value to observe for the QoS transmit queue.

Dot1P Tag: The 802.1P precedence value to use if packets are to be 802.1P tagged.

DSCP Tag: The DSCP label to use if packets are to be DSCP tagged.

11.9.15. IEEE 802.11 MIC Error Report From Mobile

The MIC Error Report From Mobile message element is sent by an AC to a WTP when it receives a MIC failure notification via the Error bit in the EAP over LAN (EAPOL)-Key frame.



Type: 79 for IEEE 802.11 MIC Error Report From Mobile

Length: 14

Client MAC Address: The Client MAC address of the station reporting the MIC failure.

BSSID: The BSSID on which the MIC failure is being reported.

Radio ID: The Radio Identifier, typically refers to some interface index on the WTP.

WLAN ID: The WLAN ID on which the MIC failure is being reported.

11.10. IEEE 802.11 Message Element Values

This section lists IEEE 802.11-specific values for any generic LWAPP message elements that include fields whose values are technology-specific.

IEEE 802.11 uses the following values:

4 - Encrypt AES-CCMP 128: WTP supports AES-CCMP, as defined in [7].

5 - Encrypt TKIP-MIC: WTP supports TKIP and Michael, as defined in [16].

12. LWAPP Protocol Timers

A WTP or AC that implements LWAPP discovery MUST implement the following timers.

12.1. 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.

12.2. SilentInterval

The minimum time, in seconds, a WTP MUST wait after failing to receive any responses to its Discovery Requests, before it MAY again send Discovery Requests.

Default: 30

12.3. NeighborDeadInterval

The minimum time, in seconds, a WTP MUST wait without having received Echo Responses to its Echo Requests, before the destination for the Echo Request may be considered dead. Must be no less than 2*EchoInterval seconds and no greater than 240 seconds.

Default: 60

12.4. EchoInterval

The minimum time, in seconds, between sending Echo Requests to the AC with which the WTP has joined.

Default: 30

12.5. DiscoveryInterval

The minimum time, in seconds, that a WTP MUST wait after receiving a Discovery Response, before sending a Join Request.

Default: 5

12.6. RetransmitInterval

The minimum time, in seconds, that a non-acknowledged LWAPP packet will be retransmitted.

Default: 3

12.7. ResponseTimeout

The minimum time, in seconds, in which an LWAPP Request message must be responded to.

Default: 1

12.8. KeyLifetime

The maximum time, in seconds, that an LWAPP session key is valid.

Default: 28800

13. LWAPP Protocol Variables

A WTP or AC 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.

13.1. MaxDiscoveries

The maximum number of Discovery Requests that will be sent after a WTP boots.

Default: 10

13.2. DiscoveryCount

The number of discoveries transmitted by a WTP to a single AC. This is a monotonically increasing counter.

13.3. RetransmitCount

The number of retransmissions for a given LWAPP packet. This is a monotonically increasing counter.

13.4. MaxRetransmit

The maximum number of retransmissions for a given LWAPP packet before the link layer considers the peer dead.

Default: 5

14. NAT Considerations

There are two specific situations where a NAT system may be used in conjunction with LWAPP. The first consists of a configuration where the WTP is behind a NAT system. Given that all communication is initiated by the WTP, and all communication is performed over IP using a single UDP port, the protocol easily traverses NAT systems in this configuration.

The second configuration is one where the AC sits behind a NAT, and there are two main issues that exist in this situation. First, an AC communicates its interfaces and associated WTP load on these interfaces, through the WTP Manager Control IP Address. This message element is currently mandatory, and if NAT compliance became an issue, it would be possible to either:

1. make the WTP Manager Control IP Address optional, allowing the WTP to simply use the known IP address. However, note that this approach would eliminate the ability to perform load balancing of WTP across ACs, and therefore is not the recommended approach.

2. allow an AC to be able to configure a NAT'ed address for every associated AC that would generally be communicated in the WTP Manager Control IP Address message element.

3. require that if a WTP determines that the AC List message element consists of a set of IP addresses that are different from the AC's IP address it is currently communicating with, then assume that NAT is being enforced, and require that the WTP communicate with the original AC's IP address (and ignore the WTP Manager Control IP Address message element(s)).

Another issue related to having an AC behind a NAT system is LWAPP's support for the CAPWAP Objective to allow the control and data plane to be separated. In order to support this requirement, the LWAPP protocol defines the WTP Manager Data IP Address message element, which allows the AC to inform the WTP that the LWAPP data frames are to be forwarded to a separate IP address. This feature MUST be disabled when an AC is behind a NAT. However, there is no easy way to provide some default mechanism that satisfies both the data/

control separation and NAT objectives, as they directly conflict with each other. As a consequence, user intervention will be required to support such networks.

LWAPP has a feature that allows for all of the AC's identities supporting a group of WTPs to be communicated through the AC List message element. This feature must be disabled when the AC is behind a NAT and the IP address that is embedded would be invalid.

The LWAPP protocol has a feature that allows an AC to configure a static IP address on a WTP. The WTP Static IP Address Information message element provides such a function; however, this feature SHOULD NOT be used in NAT'ed environments, unless the administrator is familiar with the internal IP addressing scheme within the WTP's private network, and does not rely on the public address seen by the AC.

When a WTP detects the duplicate address condition, it generates a message to the AC, which includes the Duplicate IP Address message element. Once again, it is important to note that the IP address embedded within this message element would be different from the public IP address seen by the AC.

15. Security Considerations

LWAPP uses either an authenticated key exchange or key agreement mechanism to ensure peer authenticity and establish fresh session keys to protect the LWAPP communications.

The LWAPP protocol defines a join phase, which allows a WTP to bind a session with an AC. During this process, a session key is mutually derived, and secured either through an X.509 certificate or a pre-shared key. The resulting key exchange generates an encryption session key, which is used to encrypt the LWAPP control packets, and a key derivation key.

During the established secure communication, the WTP and AC may rekey using the key update process, which is identical to the join phase, meaning the session keys are mutually derived. However, the exchange described for pre-shared session keys is always used for the key update, with the pre-shared key set to the derivation key created either during the join, or the last key update if one has occurred. The key update results in a new derivation key, which is used in the next key update, as well as an encryption session key to encrypt the LWAPP control packets.

Replay protection of the Join Request is handled through an exchange of nonces during the join (or key update) phase. The Join Request includes an XNonce, which is included in the AC's authenticated Join Reply's encrypted ANonce message element, allowing for the two messages to be bound. Upon receipt of the Join Reply, the WTP generates the WNonce, and generates a set of session keys using a KDF function. One of these keys is used to MIC the Join ACK. The AC responds with a Join Confirm, which must also include a MIC, and therefore be capable of deriving the same set of session keys.

In both the X.509 certificate and pre-shared key modes, an initialization vector is created through the above mentioned KDF function. The IV and the KDF created encryption key are used to encrypt the LWAPP control frames.

Given that authentication in the Join exchange does not occur until the WTP transmits the Join ACK message, it is crucial that an AC not delete any state for a WTP it is servicing until an authentication Join ACK has been received. Otherwise, a potential Denial-of-Service attack exists, whereby sending a spoofed Join Request for a valid WTP would cause the AC to reset the WTP's connection.

It is important to note that Perfect Forward Secrecy is not a requirement for the LWAPP protocol.

Note that the LWAPP protocol does not add any new vulnerabilities to 802.11 infrastructure that makes use of WEP for encryption purposes. However, implementors SHOULD discourage the use of WEP to allow the market to move towards technically sound cryptographic solutions, such as 802.11i.

15.1. Certificate-Based Session Key Establishment

LWAPP uses public key cryptography to ensure trust between the WTP and the AC. One question that periodically arises is why the Join Request is not signed. Signing this request would not be optimal for the following reasons:

1. The Join Request is replayable, so a signature doesn't provide much protection unless the switches keep track of all previous Join Requests from a given WTP.

2. Replay detection is handled during the Join Reply and Join ACK messages.

3. A signed Join Request provides a potential Denial-of-Service attack on the AC, which would have to authenticate each (potentially malicious) message.

The WTP-Certificate that is included in the Join Request MUST be validated by the AC. It is also good practice that the AC perform some form of authorization, ensuring that the WTP in question is allowed to establish an LWAPP session with it.

15.2. PSK-Based Session Key Establishment

Use of a fixed shared secret of limited entropy (for example, a PSK that is relatively short, or was chosen by a human and thus may contain less entropy than its length would imply) may allow an attacker to perform a brute-force or dictionary attack to recover the secret.

It is RECOMMENDED that implementations that allow the administrator to manually configure the PSK also provide a functionality for generating a new random PSK, taking RFC 1750 [4] into account.

Since the key generation does not expose the nonces in plaintext, there are no practical passive attacks possible.

16. Acknowledgements

The authors wish to thank Michael Vakulenko for contributing text that describes how LWAPP can be used over a Layer 3 (IP) network.

The authors would also like to thanks Russ Housley and Charles Clancy for their assistance in providing a security review of the LWAPP specification. Charles' review can be found in [12].

17. References

17.1. Normative References

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

[2] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[3] Whiting, D., Housley, R., and N. Ferguson, "Counter with CBC-MAC (CCM)", RFC 3610, September 2003.

[4] Eastlake, D., 3rd, Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[5] Manner, J., Ed., and M. Kojo, Ed., "Mobility Related Terminology", RFC 3753, June 2004.

[6] "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 Standard 802.11, 2007, <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>

[7] "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 Amendment 6: Medium Access Control (MAC) Security Enhancements", IEEE Standard 802.11i, July 2004, http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[8] Clark, D., "IP datagram reassembly algorithms", RFC 815, July 1982.

[9] Schaad, J. and R. Housley, "Advanced Encryption Standard (AES) Key Wrap Algorithm", RFC 3394, September 2002.

[10] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[11] "Netscape-Defined Certificate Extensions", <http://www.redhat.com/docs/manuals/cert-system/admin/7.1/app_ext.html#35336>.

[12] Clancy, C., "Security Review of the Light-Weight Access Point Protocol", May 2005, <http://www.cs.umd.edu/~clancy/docs/lwapp-review.pdf>.

17.2. Informative References

[13] Reynolds, J., Ed., "Assigned Numbers: RFC 1700 is Replaced by an On-line Database", RFC 3232, January 2002.

[14] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[15] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[16] "WiFi Protected Access (WPA) rev 1.6", April 2003.

Authors' Addresses

Pat R. Calhoun
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
Phone: +1 408-853-5269
EMail: pcalhoun@cisco.com

Rohit Suri
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
Phone: +1 408-853-5548
EMail: rsuri@cisco.com

Nancy Cam-Winget
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
Phone: +1 408-853-0532
EMail: ncamwing@cisco.com

Scott Kelly
EMail: scott@hyperthought.com

Michael Glenn Williams
GWhiz Arts & Sciences
1560 Newbury Road, Suite 1-204
Newbury Park, CA 91320
Phone: +1 805-499-1994
EMail: gwhiz@gwhiz.com

Sue Hares
Phone: +1 734-604-0332
EMail: shares@ndzh.com

Bob O'Hara
EMail: bob.ohara@computer.org