Network Working Group
Request for Comments: 5416
Category: Standards Track

P. Calhoun, Ed.
Cisco Systems, Inc.
M. Montemurro, Ed.
Research In Motion
D. Stanley, Ed.
Aruba Networks

March 2009

Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Abstract

Wireless LAN product architectures have evolved from single autonomous access points to systems consisting of a centralized Access Controller (AC) and Wireless Termination Points (WTPs). The general goal of centralized control architectures is to move access control, including user authentication and authorization, mobility management, and radio management from the single access point to a centralized controller.

This specification defines the Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Binding Specification for use with the IEEE 802.11 Wireless Local Area Network protocol.

Table of Contents

1. Introduction

The CAPWAP protocol [RFC5415] defines an extensible protocol to allow an Access Controller to manage wireless agnostic Wireless Termination Points. The CAPWAP protocol itself does not include any specific wireless technologies; instead, it relies on a binding specification to extend the technology to a particular wireless technology.

This specification defines the Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Binding Specification for use with the IEEE 802.11 Wireless Local Area Network protocol. Use of CAPWAP control message fields, new control messages, and message elements are defined. The minimum required definitions for a binding-specific Statistics message element, Station message element, and WTP Radio Information message element are included.

Note that this binding only supports the IEEE 802.11-2007 specification. Of note, this binding does not support the ad hoc network mode defined in the IEEE 802.11-2007 standard. This specification also does not cover the use of data frames with the four-address format, commonly referred to as Wireless Bridges, whose use is not specified in the IEEE 802.11-2007 standard. This protocol specification does not currently officially support IEEE 802.11n. That said, the protocol does allow a WTP to advertise support for an IEEE 802.11n radio; however, the protocol does not allow for any of the protocol’s additional features to be configured and/or used. New IEEE protocol specifications published outside of this document (e.g., IEEE 802.11v, IEEE 802.11r) are also not supported through this binding, and in addition to IEEE 802.11n, must be addressed either through a separate CAPWAP binding, or an update to this binding.

In order to address immediate market needs for standards still being developed by the IEEE 802.11 standards body, the WiFi Alliance created interim pseudo-standards specifications. Two such specifications are widely used in the industry, namely the WiFi Protect Access [WPA] and the WiFi MultiMedia [WMM] specifications. Given their widespread adoption, this CAPWAP binding requires the use of these two specifications.

1.1. Goals

The goals of this CAPWAP protocol binding are to make the capabilities of the CAPWAP protocol available for use in conjunction with IEEE 802.11 wireless networks. The capabilities to be made available can be summarized as:

1. To centralize the authentication and policy enforcement functions for an IEEE 802.11 wireless network. The AC may also provide centralized bridging, forwarding, and encryption of user traffic. Centralization of these functions will enable reduced cost and higher efficiency by applying the capabilities of network processing silicon to the wireless network, as in wired LANs.

2. To enable shifting of the higher-level protocol processing from the WTP. This leaves the time-critical applications of wireless control and access in the WTP, making efficient use of the computing power available in WTPs that are subject to severe cost pressure.

The CAPWAP protocol binding extensions defined herein apply solely to the interface between the WTP and the AC. Inter-AC and station-to-AC communication are strictly outside the scope of this document.

1.2. 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 [RFC2119].

1.3. Terminology

This section contains definitions for terms used frequently throughout this document. However, many additional definitions can be found in [IEEE.802-11.2007].

Access Controller (AC): The network entity that provides WTP access to the network infrastructure in the data plane, control plane, management plane, or a combination therein.

Basic Service Set (BSS): A set of stations controlled by a single coordination function.

Distribution: The service that, by using association information, delivers medium access control (MAC) service data units (MSDUs) within the distribution system (DS).

Distribution System Service (DSS): The set of services provided by the distribution system (DS) that enable the medium access control (MAC) layer to transport MAC service data units (MSDUs) between stations that are not in direct communication with each other over a single instance of the wireless medium (WM). These services include the transport of MSDUs between the access points (APs) of basic service sets (BSSs) within an extended service set (ESS), transport of MSDUs between portals and BSSs within an ESS, and transport of MSDUs between stations in the same BSS in cases where the MSDU has a multicast or broadcast destination address, or where the destination is an individual address but the station sending the MSDU chooses to involve the DSS. DSSs are provided between pairs of IEEE 802.11 MACs.

Integration: The service that enables delivery of medium access control (MAC) service data units (MSDUs) between the distribution system (DS) and an existing, non-IEEE 802.11 local area network (via a portal).

Station (STA): A device that contains an IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).

Portal: The logical point at which medium access control (MAC) service data units (MSDUs) from a non-IEEE 802.11 local area network (LAN) enter the distribution system (DS) of an extended service set (ESS).

WLAN: In this document, WLAN refers to a logical component instantiated on a WTP device. A single physical WTP may operate a number of WLANs. Each Basic Service Set Identifier (BSSID) and its constituent wireless terminal radios is denoted as a distinct WLAN on a physical WTP.

Wireless Termination Point (WTP): The physical or network entity that contains an IEEE 802.11 RF antenna and wireless PHY to transmit and receive station traffic for wireless access networks.

2. IEEE 802.11 Binding

This section describes use of the CAPWAP protocol with the IEEE 802.11 Wireless Local Area Network protocol, including Local and Split MAC operation, Group Key Refresh, Basic Service Set Identification (BSSID) to WLAN Mapping, IEEE 802.11 MAC management frame Quality of Service (Qos) tagging and Run State operation.

2.1. CAPWAP Wireless Binding Identifier

The CAPWAP Header, defined in Section 4.3 of [RFC5415] requires that all CAPWAP binding specifications have a Wireless Binding Identifier (WBID) assigned. This document, which defines the IEEE 802.11 binding, uses the value one (1).

2.2. Split MAC and Local MAC Functionality

The CAPWAP protocol, when used with IEEE 802.11 devices, requires specific behavior from the WTP and the AC to support the required IEEE 802.11 protocol functions.

For both the Split and Local MAC approaches, the CAPWAP functions, as defined in the taxonomy specification [RFC4118], reside in the AC.

To provide system component interoperability, the WTP and AC MUST support 802.11 encryption/decryption at the WTP. The WTP and AC MAY support 802.11 encryption/decryption at the AC.

2.2.1. Split MAC

This section shows the division of labor between the WTP and the AC in a Split MAC architecture. Figure 1 shows the separation of functionality between CAPWAP components.

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

Figure 1: Mapping of 802.11 Functions for Split MAC Architecture

In a 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 IEEE 802.11 services, including the Beacon and Probe Response frames, are handled on the WTP.

All remaining IEEE 802.11 MAC management frames are supported on the AC, including the Association Request frame that allows the AC to be involved in the access policy enforcement portion of the IEEE 802.11 protocol. The IEEE 802.1X [IEEE.802-1X.2004], Extensible Authentication Protocol (EAP) [RFC3748] and IEEE Robust Security Network Association (RSNA) Key Management [IEEE.802-11.2007] functions are also located on the AC. This implies that the Authentication, Authorization, and Accounting (AAA) client also resides on the AC.

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

Note that in the following figure, the use of '(-)' indicates that processing of the frames is done on the WTP. This figure represents a case where encryption services are provided by the AC.

```
             Client                      WTP                          AC

                      Beacon
             <-----------------------------
                   Probe Request
             ----------------------------( - )------------------------->
                   Probe Response
             <-----------------------------
                              802.11 AUTH/Association
             <--------------------------------------------------------->
                                        Station Configuration Request
                                          [Add Station (Station MAC
                                          Address), IEEE 802.11 Add
                                          Station (WLAN ID), IEEE
                                          802.11 Session Key(Flag=A)]
                                            <-------------------------->
                    802.1X Authentication & 802.11 Key Exchange
             <--------------------------------------------------------->
                                        Station Configuration Request
                                          [Add Station(Station MAC
                                          Address), IEEE 802.11 Add
                                          Station (WLAN ID), IEEE 802.11
                                          Station Session Key(Flag=C)]
                                            <-------------------------->
                               802.11 Action Frames
             <--------------------------------------------------------->
                                   802.11 DATA (1)
             <---------------------------( - )------------------------->
```

Figure 2: Split MAC Message Flow

Figure 2 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 IEEE 802.11, using 802.1X-based end user authentication and Advanced Encryption Standard-Counter Mode with CBC-MAC Protocol (AES-CCMP) link layer encryption (CCMP, see [FIPS.197.2001]). The following process occurs:

- The WTP generates the IEEE 802.11 Beacon frames, using information provided to it through the IEEE 802.11 Add WLAN (see Section 6.1) message element, including the Robust Security Network Information Element (RSNIE), which indicates support of 802.1X and AES-CCMP.

- The WTP processes the Probe Request frame and responds with a corresponding Probe Response frame. The Probe Request frame is then forwarded to the AC for optional processing.

- The WTP forwards the IEEEE 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 a Station Configuration Request message, which includes an Add Station message element, to the WTP (see Section 4.6.8 in [RFC5415]). In the above example, the WLAN was configured for IEEE 802.1X, and therefore the IEEE 802.11 Station Session Key is included with the flag field's 'A' bit set.

- If the WTP is providing encryption/decryption services, once the client has completed the IEEE 802.11 key exchange, the AC transmits another Station Configuration Request message, which includes:

  - An Add Station message element.

  - An IEEE 802.11 Add Station message element, which includes the WLAN Identifier with which the station has associated.

  - An IEEE 802.11 Station Session Key message element, which includes the pairwise encryption key.

  - An IEEE 802.11 Information Element message element, which includes the Robust Security Network Information Element (RSNIE) to the WTP, stating the security policy to enforce for the client (in this case AES-CCMP).

- If the WTP is providing encryption/decryption services, once the client has completed the IEEE 802.11 key exchange, the AC transmits another Station Configuration Request message, which includes:

  - An Add Station message element.

  - An IEEE 802.11 Add Station message element, which includes the WLAN Identifier with which the station has associated.

  - An IEEE 802.11 Station Session Key message element, which includes the pairwise encryption key.

  - An IEEE 802.11 Information Element message element, which includes the Robust Security Network Information Element (RSNIE) to the WTP, stating the security policy to enforce for the client (in this case AES-CCMP).

- If the AC is providing encryption/decryption services, once the client has completed the IEEE 802.11 key exchange, the AC transmits another Station Configuration Request message, which includes:

    - An Add Station message element.

    - An IEEE 802.11 Add Station message element, which includes the WLAN Identifier with which the station has associated.

    - An IEEE 802.11 Station Session Key message element with the flag field’s ’C’ bit enabled (indicating that the AC will provide crypto services).

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

- All IEEE 802.11 station data frames are tunneled between the WTP and the AC.

Note that during the EAP over LAN (EAPOL)-Key exchange between the Station and the AC, the Receive Sequence Counter (RSC) field for the Group Key (GTK) needs to be included in the frame. The value of zero (0) is used by the AC during this exchange. Additional details are available in Section 9.1.

The WTP SHALL include the IEEE 802.11 MAC header contents in all frames transmitted to the AC.

When 802.11 encryption/decryption is performed at the WTP, the WTP MUST decrypt the uplink frames, MUST set the Protected Frame field to 0, and MUST make the frame format consistent with that of an unprotected 802.11 frame prior to transmitting the frames to the AC. The fields added to an 802.11 protected frame (i.e., Initialization Vector/Extended Initialization Vector (IV/EIV), Message Integrity Code (MIC), and Integrity Check Value (ICV)) MUST be stripped off prior to transmission from the WTP to AC. For downlink frames, the Protected Frame field MUST be set to 0 by the AC as the frame being sent is unencrypted. The WTP MUST apply the required protection policy for the WLAN, and set the Protected Frame field on transmission over the air. The Protected Frame field always needs to accurately indicate the status of the 802.11 frame that is carrying it.

When 802.11 encryption/decryption is performed at the AC, the WTP SHALL NOT decrypt the uplink frames prior to transmitting the frames to the AC. The AC and WTP SHALL populate the IEEE 802.11 MAC header fields as described in Figure 3.

MAC header field	Location
Frame Control:	
Version	AC
ToDS	AC
FromDS	AC
Type	AC
SubType	AC
MoreFrag	WTP/AC
Retry	WTP
Pwr Mgmt	-
MoreData	WTP
Protected	WTP/AC
Order	AC
Duration:	WTP
Address 1:	AC
Address 2:	AC
Address 3:	AC
Sequence Ctrl:	WTP
Address 4:	AC
QoS Control:	AC
Frame Body:	AC
FCS:	WTP

Figure 3: Population of the IEEE 802.11 MAC Header Fields for Downlink Frames

When 802.11 encryption/decryption is performed at the AC, the MoreFrag bit is populated at the AC. The Pwr Mgmt bit is not applicable to downlink frames, and is set to 0. Note that the Frame Check Sequence (FCS) field is not included in 802.11 frames exchanged between the WTP and the AC. Upon sending data frames to the AC, the WTP is responsible for validating and stripping the FCS field. Upon receiving data frames from the AC, the WTP is responsible for adding the FCS field, and populating the field as described in [IEEE.802-11.2007].

Note that when the WTP tunnels data packets to the AC (and vice versa), the CAPWAP protocol does not guarantee in-order delivery. When the protocol being transported over IEEE 802.11 is IP, out-of-order delivery is not an issue as IP has no such requirements. However, implementers need to be aware of this protocol characteristic before deciding to use CAPWAP.

2.2.2. Local MAC

This section shows the division of labor between the WTP and the AC in a Local MAC architecture. Figure 4 shows the separation of functionality among CAPWAP components.

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

Figure 4: Mapping of 802.11 Functions for Local AP Architecture

In the Local MAC mode, the integration service exists on the WTP, while the distribution service MAY reside on either the WTP or the AC. When it resides on the AC, station-generated frames are not forwarded to the AC in their native format, but encapsulated as 802.3 frames.

While the MAC is terminated on the WTP, it is necessary for the AC to be aware of mobility events within the WTPs. Thus, the WTP MUST forward the IEEE 802.11 Association Request frames to the AC. The AC MAY reply with a failed Association Response frame if it deems it necessary, and upon receipt of a failed Association Response frame from the AC, the WTP MUST send a Disassociation frame to the station.

The IEEE 802.1X [IEEE.802-1X.2004], EAP, and IEEE RSNA Key Management [IEEE.802-11.2007] functions reside in the AC. Therefore, the WTP MUST forward all IEEE 802.1X, EAP, and RSNA Key Management frames to the AC and forward the corresponding responses to the station. This implies that the AAA client also resides on the AC.

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

```
             Client                        WTP                         AC

                      Beacon
             <-----------------------------
                       Probe
             <---------------------------->
                        802.11 AUTH
             <-----------------------------
                                 802.11 Association
             <---------------------------( - )------------------------->
                                        Station Configuration Request
                                          [Add Station (Station MAC
                                          Address), IEEE 802.11 Add
                                          Station (WLAN ID), IEEE
                                          802.11 Session Key(Flag=A)]
                                            <-------------------------->
                    802.1X Authentication & 802.11 Key Exchange
             <--------------------------------------------------------->
                                        Station Configuration Request
                                          [Add Station(Station MAC
                                          Address), IEEE 802.11 Add
                                          Station (WLAN ID), IEEE 802.11
                                          Station session Key (Key=x),
                                          IEEE 802.11 Information
                                          Element(RSNIE(Pairwise
                                          Cipher=CCMP))]
                                            <-------------------------->
                               802.11 Action Frames
             <--------------------------------------------------------->
                     802.11 DATA
             <----------------------------->
```

Figure 5: Local MAC Message Flow

Figure 5 provides an illustration of the division of labor in a Local MAC architecture. In this example, a WLAN that is configured for IEEE 802.11 has been created using AES-CCMP for privacy. The following process occurs:

- The WTP generates the IEEE 802.11 Beacon frames, using information provided to it through the Add WLAN (see Section 6.1) message element.

- The WTP processes a Probe Request frame and responds with a corresponding Probe Response frame.

- The WTP forwards the IEEE 802.11 Authentication and Association frames to the AC.

- Once the association is complete, the AC transmits a Station Configuration Request message, which includes the Add Station message element, to the WTP (see Section 4.6.8 in [RFC5415]). In the above example, the WLAN was configured for IEEE 802.1X, and therefore the IEEE 802.11 Station Session Key is included with the flag field’s ’A’ bit set.

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

- The AC transmits another Station Configuration Request message, which includes:

    - An Add Station message element, which MAY include a Virtual LAN (VLAN) [IEEE.802-1Q.2005] name, which when present is used by the WTP to identify the VLAN on which the user’s data frames are to be bridged.

    - An IEEE 802.11 Add Station message element, which includes the WLAN Identifier with which the station has associated.

    - An IEEE 802.11 Station Session Key message element, which includes the pairwise encryption key.

    - An IEEE 802.11 Information Element message element, which includes the RSNIE to the WTP, stating the security policy to enforce for the client (in this case AES-CCMP).

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

- The WTP MAY locally bridge client data frames (and provide the necessary encryption and decryption services). The WTP MAY also tunnel client data frames to the AC, using 802.3 frame tunnel mode or 802.11 frame tunnel mode.

2.3. Roaming Behavior

This section expands upon the examples provided in the previous section, and describes how the CAPWAP control protocol is used 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 WTP. Figure 6 shows an example of a currently associated station moving from its "Old WTP" to a "New WTP". The figure is valid for multiple different security policies, including IEEE 802.1X and Wireless Protected Access (WPA) or Wireless Protected Access 2 (WPA2) [WPA].

In the event that key caching was employed, the 802.1X Authentication step would be eliminated. Note that the example represents one where crypto services are provided by the WTP, so in a case where the AC provided this function the last Station Configuration Request would be different.

```
            Client                  Old WTP            New WTP          AC

                          Association Request/Response
             <--------------------------------------( - )-------------->
                                        Station Configuration Request
                                          [Add Station (Station MAC
                                          Address), IEEE 802.11 Add
                                          Station (WLAN ID), IEEE
                                          802.11 Session Key(Flag=A)]
                                                      <---------------->
             802.1X Authentication (if no key cache entry exists)
             <--------------------------------------( - )-------------->
                           802.11 4-way Key Exchange
             <--------------------------------------( - )-------------->
                                Station Configuration Request
                                  [Delete Station]
                                    <---------------------------------->
                                        Station Configuration Request
                                          [Add Station(Station MAC
                                          Address), IEEE 802.11 Add
                                          Station (WLAN ID), IEEE 802.11
                                          Station session Key (Key=x),
                                          IEEE 802.11 Information
                                          Element(RSNIE(Pairwise
                                          Cipher=CCMP))]
                                                      <---------------->
```

Figure 6: Client Roaming Example

2.4. Group Key Refresh

Periodically, the Group Key (GTK) for the BSS needs to be updated. The AC uses an EAPOL-Key frame to update the group key for each STA in the BSS. While the AC is updating the GTK, each Layer 2 (L2) broadcast frame transmitted to the BSS needs to be duplicated and transmitted using both the current GTK and the new GTK. Once the GTK update process has completed, broadcast frames transmitted to the BSS will be encrypted using the new GTK.

In the case of Split MAC, the AC needs to duplicate all broadcast packets and update the key index so that the packet is transmitted using both the current and new GTK to ensure that all STAs in the BSS receive the broadcast frames. In the case of Local MAC, the WTP needs to duplicate and transmit broadcast frames using the appropriate index to ensure that all STAs in the BSS continue to receive broadcast frames.

The Group Key update procedure is shown in the following figure. The AC will signal the update to the GTK using an IEEE 802.11 Configuration Request message, including an IEEE 802.11 Update WLAN message element with the new GTK, its index, the Transmit Sequence Counter (TSC) for the Group Key and the Key Status set to 3 (begin GTK update). The AC will then begin updating the GTK for each STA. During this time, the AC (for Split MAC) or WTP (for Local MAC) MUST duplicate broadcast packets and transmit them encrypted with both the current and new GTK. When the AC has completed the GTK update to all STAs in the BSS, the AC MUST transmit an IEEE 802.11 Configuration Request message including an IEEE 802.11 Update WLAN message element containing the new GTK, its index, and the Key Status set to 4 (GTK update complete).

```
        Client           WTP                                          AC

                         IEEE 802.11 WLAN Configuration Request [Update
                           WLAN (GTK, GTK Index, GTK Start,
                           Group TSC) ]
                         <---------------------------------------------
                               802.1X EAPoL (GTK Message 1)
        <-------------( - )-------------------------------------------
                               802.1X EAPoL (GTK Message 2)
        -------------( - )------------------------------------------->
                         IEEE 802.11 WLAN Configuration Request [ Update
                           WLAN (GTK Index, GTK Complete) ]
                         <---------------------------------------------
```

Figure 7: Group Key Update Procedure

2.5. BSSID to WLAN ID Mapping

The CAPWAP protocol binding enables the WTP to assign BSSIDs upon creation of a WLAN (see Section 6.1). While manufacturers are free to assign BSSIDs using any arbitrary mechanism, it is advised that where possible the BSSIDs are assigned as a contiguous block.

When assigned as a block, implementations can still assign any of the available BSSIDs to any WLAN. One possible method is for the WTP to assign the address using the following algorithm: base BSSID address + WLAN ID.

The WTP communicates the maximum number of BSSIDs that it supports during configuration via the IEEE 802.11 WTP WLAN Radio Configuration message element (see Section 6.23).

2.6. CAPWAP Data Channel QoS Behavior

The CAPWAP IEEE 802.11 binding specification provides procedures to allow for the WTP to enforce Quality of Service on IEEE 802.11 Data Frames and MAC Management messages.

2.6.1. IEEE 802.11 Data Frames

When the WLAN is created on the WTP, a default Quality of Service policy is established through the IEEE 802.11 WTP Quality of Service message element (see Section 6.22). This default policy will cause the WTP to use the default QoS values for any station associated with the WLAN in question. The AC MAY also override the policy for a given station by sending the IEEE 802.11 Update Station QoS message element (see Section 6.20), known as a station-specific QoS policy.

Beyond the default, and per station QoS policy, the IEEE 802.11 protocol also allows a station to request special QoS treatment for a specific flow through the Traffic Specification (TSPEC) Information Elements found in the IEEE 802.11-2007’s QoS Action Frame. Alternatively, stations MAY also use the WiFi Alliance’s WMM specification instead to request QoS treatment for a flow (see [WMM]). This requires the WTP to observe the Status Code in the IEEE 802.11-2007 and WMM QoS Action Add Traffic System (ADDTS) responses from the AC, and provide the services requested in the TSPEC Information Element. Similarly, the WTP MUST observe the Reason Code Information Element in the IEEE 802.11-2007 and WMM QoS Action DELTS responses from the AC by removing the policy associated with the TSPEC.

The IEEE 802.11 WTP Quality of Service message element’s Tagging Policy field indicates how the packets are to be tagged, known as the Tagging Policy. There are five bits defined, two of which are used to indicate the type of QoS to be used by the WTP. The first is the ’P’ bit, which is set to inform the WTP it is to use the 802.1p QoS mechanism. When set, the ’Q’ bit is used to inform the WTP which 802.1p priority values it is to use.

The ’D’ bit is set to inform the WTP it is to use the Differentiated Services Code Point (DSCP) QoS mechanism. When set, the ’I’ and ’O’ bits are used to inform the WTP which values it is to use in the inner header, in the station’s original packet, or the outer header, the latter of which is only valid when tunneling is enabled.

When an IEEE 802.11 Update Station QoS message element is received, while the specific 802.1p priority or DSCP values may change for a given station, known as the station specific policy, the original Tagging Policy (the use of the five bits) remains the same.

The use of the DSCP and 802.1p QoS mechanisms are not mutually exclusive. An AC MAY request that a WTP use none, one, or both types of QoS mechanisms at the same time.

2.6.1.1. 802.1p Support

The IEEE 802.11 WTP Quality of Service and IEEE 802.11 Update Station QoS message elements include the "802.1p Tag" field, which is the 802.1p priority value. This value is used by the WTP by adding an 802.1Q header (see [IEEE.802-1Q.2005]) with the priority field set according to the policy provided. Note that this tagging is only valid for interfaces that support 802.1p. The actual treatment does not change for either Split or Local MAC modes, or when tunneling is used. The only exception is when tunneling is used, the 802.1Q header is added to the outer packet (tunneled) header. The IEEE 802.11 standard does not permit the station's packet to include an 802.1Q header. Instead, the QoS mechanisms defined in the IEEE 802.11 standard are used by stations to mark a packet's priority. When the 'P' bit is set in the Tagging Policy, the 'Q' bit has the following behavior:

Q=1: The WTP marks the priority field in the 802.1Q header to either the default or the station-specific 802.1p policy.

Q=0: The WTP marks the priority field in the 802.1Q header to the value found in the User Priority field of the QoS Control field of the IEEE 802.11 header. If the QoS Control field is not present in the IEEE 802.11 header, then the behavior described under 'Q=1' is used.

2.6.1.2. DSCP Support

The IEEE 802.11 WTP Quality of Service and IEEE 802.11 Update Station QoS message elements also provide a "DSCP Tag", which is used by the WTP when the 'D' bit is set to mark the DSCP field of both the IPv4 and IPv6 headers (see [RFC2474]). When DSCP is used, the WTP marks the inner packet (the original packet received by the station) when the 'I' bit is set. Similarly, the WTP marks the outer packet (tunnel header's DSCP field) when the 'O' bit is set.

When the 'D' bit is set, the treatment of the packet differs based on whether the WTP is tunneling the station's packets to the AC. Tunneling does not occur in a Local MAC mode when the AC has communicated that tunneling is not required, as part of the IEEE 802.11 Add WLAN message element, see Section 6.1. In the case where tunneling is not used, the ’I’ and ’O’ bits have the following behaviors:

O=1: This option is invalid when tunneling is not enabled for station data frames.

O=0: This option is invalid when tunneling is not enabled for station data frames.

I=1: The WTP sets the DSCP field in the station’s packet to either the default policy or the station-specific policy if one exists.

I=0: The WTP MUST NOT modify the DSCP field in the station’s packet.

For Split MAC mode, or Local MAC with tunneling enabled, the WTP needs to contend with both the inner packet (the station’s original packet) as well as the tunnel header (added by the WTP). In this mode of operation, the bits are treated as follows:

O=1: The WTP sets the DSCP field in the tunnel header to either the default policy or the station specific policy if one exists.

O=0: The WTP sets the DSCP field in the tunnel header to the value found in the inner packet’s DSCP field. If encryption services are provided by the AC (see Section 6.15), the packet is encrypted; therefore, the WTP cannot access the inner DSCP field, in which case it uses the behavior described when the ’O’ bit is set. This occurs also if the inner packet is not IPv4 or IPv6, and thus does not have a DSCP field.

I=1: The WTP sets the DSCP field in the station’s packet to either the default policy or the station-specific policy if one exists. If encryption services are provided by the AC (see Section 6.15), the packet is encrypted; therefore, the WTP cannot access the inner DSCP field, in which case it uses the behavior described when the ’I’ bit is not set. This occurs also if the inner packet is not IPv4 or IPv6, and thus does not have a DSCP field.

I=0: The WTP MUST NOT modify the DSCP field in the station’s packet.

The CAPWAP protocol supports the Explicit Congestion Notification (ECN) bits [RFC3168]. Additional details on ECN support can be found in [RFC5415].

2.6.2. IEEE 802.11 MAC Management Messages

It is recommended that IEEE 802.11 MAC Management frames be sent by both the AC and the WTP with appropriate Quality of Service values, listed below, to ensure that congestion in the network minimizes occurrences of packet loss. Note that the QoS Mechanism specified in the Tagging Policy is used as specified by the AC in the IEEE 802.11 WTP Quality of Service message element (see Section 6.22). However, the station-specific policy is not used for IEEE 802.11 MAC Management frames.

802.1p:	The precedence value of 7 (decimal) SHOULD be used for all IEEE 802.11 MAC management frames, except for Probe Requests, which SHOULD use 4.
DSCP:	All IEEE 802.11 MAC management frames SHOULD use the CS6 per- hop behavior (see [RFC2474]), while IEEE 802.11 Probe Requests should use the Low Drop Assured Forwarding per-hop behavior (see [RFC3246]).

2.7. Run State Operation

The Run state is the normal state of operation for the CAPWAP protocol in both the WTP and the AC.

When the WTP receives a WLAN Configuration Request message (see Section 3.1), it MUST respond with a WLAN Configuration Response message (see Section 3.2), and it remains in the Run state.

When the AC sends a WLAN Configuration Request message (see Section 3.1) or receives the corresponding WLAN Configuration Response message (see Section 3.2) from the WTP, it remains in the Run state.

3. IEEE 802.11 Specific CAPWAP Control Messages

This section defines CAPWAP Control messages that are specific to the IEEE 802.11 binding. Two messages are defined: IEEE 802.11 WLAN Configuration Request and IEEE 802.11 WLAN Configuration Response. See Section 4.5 in [RFC5415] for CAPWAP Control message definitions and the derivation of the Message Type value from the IANA Enterprise number.

The valid message types for IEEE 802.11-specific control messages are listed below. The IANA Enterprise number used with these messages is 13277.

CAPWAP Control Message	Message Type Value
IEEE 802.11 WLAN Configuration Request	3398913
IEEE 802.11 WLAN Configuration Response	3398914

3.1. IEEE 802.11 WLAN Configuration 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 CAPWAP Configuration Update Response message (see Section 8.5 in [RFC5415]) has been received by the AC.

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

A 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 Service Set Identifiers (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 MAY 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 message elements MAY be included in the IEEE 802.11 WLAN Configuration Request message. Only one message element MUST be present.

- IEEE 802.11 Add WLAN, see Section 6.1
- IEEE 802.11 Delete WLAN, see Section 6.4

- IEEE 802.11 Update WLAN, see Section 6.21

The following message element MAY be present.

- IEEE 802.11 Information Element, see Section 6.6

- Vendor-Specific Payload, see [RFC5415]

3.2. IEEE 802.11 WLAN Configuration Response

The IEEE 802.11 WLAN Configuration Response message is sent by the WTP to the AC. It is used to acknowledge receipt of an IEEE 802.11 WLAN Configuration Request message, and to indicate that the requested configuration was successfully applied or that an error related to the processing of the IEEE 802.11 WLAN Configuration Request message occurred on the WTP.

The following message element MUST be included in the IEEE 802.11 WLAN Configuration Response message.

- Result Code, see Section 4.6.34 in [RFC5415]

The following message element MAY be included in the IEEE 802.11 WLAN Configuration Response message.

- IEEE 802.11 Assigned WTP BSSID, see Section 6.3

- Vendor-Specific Payload, see [RFC5415]

4. CAPWAP Data Message Bindings

This section describes the CAPWAP data message bindings to support transport of IEEE 802.11 frames.

Payload encapsulation: The CAPWAP protocol defines the CAPWAP data message, which is used to encapsulate a wireless payload. For IEEE 802.11, the IEEE 802.11 header and payload are encapsulated (excluding the IEEE 802.11 FCS checksum). The IEEE 802.11 FCS checksum is handled by the WTP. This allows the WTP to validate an IEEE 802.11 frame prior to sending it to the AC. Similarly, when an AC wishes to transmit a frame to a station, the WTP computes and adds the FCS checksum.

Optional Wireless Specific Information: This optional CAPWAP header field (see Section 4.3 in [RFC5415]) is only used with CAPWAP data messages, and it serves two purposes, depending upon the direction of the message. For messages from the WTP to the AC, the field uses the format described in the "IEEE 802.11 Frame Info" field (see below). However, for messages sent by the AC to the WTP, the format used is described in the "Destination WLANs" field (also defined below).

Note that in both cases, the two optional headers fit in the "Data" field of the Wireless Specific Information header.

IEEE 802.11 Frame Info: When an IEEE 802.11 frame is received from a station over the air, it is encapsulated and this field is used to include radio and PHY-specific information associated with the frame.

The IEEE 802.11 Frame Info field has the following format:

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

RSSI: Received Signal Strength Indication (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.

Data Rate: The data rate field is a 16-bit unsigned value. The data rate field is a 16-bit unsigned value expressing the data rate of the packets received by the WTP in units of 0.1 Mbps. For instance, a packet received at 5.5 Mbps would be set to 55, while 11 Mbps would be set to 110.

Destination WLANs: The Destination WLANs field is used to specify the target WLANs for a given frame, and is only used with broadcast and multicast frames. This field allows the AC to transmit a single broadcast or multicast frame to the WTP and allows the WTP to perform the necessary frame replication. The field uses the following format:

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

WLAN ID bitmap: This bit field indicates the WLAN ID (see Section 6.1) on which the WTP will transmit the included frame. For instance, if a multicast packet is to be transmitted on WLANs 1 and 3, the bits for WLAN 1 and 3 of this field would be enabled. WLAN 1 is represented by bit 15 in the figure above, or the least significant bit, while WLAN 16 would be represented by bit zero (0), or the most significant bit, in the figure. This field is to be set to all zeroes for unicast packets and is unused if the WTP is not providing IEEE 802.11 encryption.

Reserved: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

5. CAPWAP Control Message Bindings

This section describes the IEEE 802.11-specific message elements included in CAPWAP Control Messages.

5.1. Discovery Request Message

The following IEEE 802.11-specific message element MUST be included in the CAPWAP Discovery Request Message.

- IEEE 802.11 WTP Radio Information, see Section 6.25. An IEEE 802.11 WTP Radio Information message element MUST be present for every radio in the WTP.

5.2. Discovery Response Message

The following IEEE 802.11-specific message element MUST be included in the CAPWAP Discovery Response Message.

- IEEE 802.11 WTP Radio Information, see Section 6.25. An IEEE 802.11 WTP Radio Information message element MUST be present for every radio in the WTP.

5.3. Primary Discovery Request Message

The following IEEE 802.11 specific message element MUST be included in the CAPWAP Primary Discovery Request message.

- IEEE 802.11 WTP Radio Information, see Section 6.25. An IEEE 802.11 WTP Radio Information message element MUST be present for every radio in the WTP.

5.4. Primary Discovery Response Message

The following IEEE 802.11-specific message element MUST be included in the CAPWAP Primary Discovery Response message.

- IEEE 802.11 WTP Radio Information, see Section 6.25. An IEEE 802.11 WTP Radio Information message element MUST be present for every radio in the WTP.

5.5. Join Request Message

The following IEEE 802.11-specific message element MUST be included in the CAPWAP Join Request message.

- IEEE 802.11 WTP Radio Information, see Section 6.25. An IEEE 802.11 WTP Radio Information message element MUST be present for every radio in the WTP.

5.6. Join Response Message

The following IEEE 802.11-specific message element MUST be included in the CAPWAP Join Response message.

- IEEE 802.11 WTP Radio Information, see Section 6.25. An IEEE 802.11 WTP Radio Information message element MUST be present for every radio in the WTP.

5.7. Configuration Status Request Message

The following IEEE 802.11-specific message elements MAY be included in the CAPWAP Configuration Status Request message. More than one of each message element listed MAY be included.

- IEEE 802.11 Antenna, see Section 6.2
- IEEE 802.11 Direct Sequence Control, see Section 6.5
- IEEE 802.11 MAC Operation, see Section 6.7
- IEEE 802.11 Multi-Domain Capability, see Section 6.9
- IEEE 802.11 Orthogonal Frequency Division Multiplexing (OFDM) Control, see Section 6.10
- IEEE 802.11 Supported Rates, see Section 6.17
- IEEE 802.11 Tx Power, see Section 6.18

- IEEE 802.11 TX Power Level, see Section 6.19
- IEEE 802.11 WTP Radio Configuration, see Section 6.23
- IEEE 802.11 WTP Radio Information, see Section 6.25. An IEEE 802.11 WTP Radio Information message element MUST be present for every radio in the WTP.

5.8. Configuration Status Response Message

The following IEEE 802.11 specific message elements MAY be included in the CAPWAP Configuration Status Response Message. More than one of each message element listed MAY be included.

- IEEE 802.11 Antenna, see Section 6.2
- IEEE 802.11 Direct Sequence Control, see Section 6.5
- IEEE 802.11 MAC Operation, see Section 6.7
- IEEE 802.11 Multi-Domain Capability, see Section 6.9
- IEEE 802.11 OFDM Control, see Section 6.10
- IEEE 802.11 Rate Set, see Section 6.11
- IEEE 802.11 Supported Rates, see Section 6.17
- IEEE 802.11 Tx Power, see Section 6.18
- IEEE 802.11 WTP Quality of Service, see Section 6.22
- IEEE 802.11 WTP Radio Configuration, see Section 6.23

5.9. Configuration Update Request Message

The following IEEE 802.11-specific message elements MAY be included in the CAPWAP Configuration Update Request message. More than one of each message element listed MAY be included.

- IEEE 802.11 Antenna, see Section 6.2
- IEEE 802.11 Direct Sequence Control, see Section 6.5
- IEEE 802.11 MAC Operation, see Section 6.7
- IEEE 802.11 Multi-Domain Capability, see Section 6.9

- IEEE 802.11 OFDM Control, see Section 6.10
- IEEE 802.11 Rate Set, see Section 6.11
- IEEE 802.11 RSNA Error Report from Station, see Section 6.12
- IEEE 802.11 Tx Power, see Section 6.18
- IEEE 802.11 WTP Quality of Service, see Section 6.22
- IEEE 802.11 WTP Radio Configuration, see Section 6.23

5.10. Station Configuration Request

The following IEEE 802.11-specific message elements MAY be included in the CAPWAP Station Configuration Request message. More than one of each message element listed MAY be included.

- IEEE 802.11 Station, see Section 6.13
- IEEE 802.11 Station Session Key, see Section 6.15
- IEEE 802.11 Station QoS Profile, see Section 6.14
- IEEE 802.11 Update Station Qos, see Section 6.20

5.11. Change State Event Request

The following IEEE 802.11-specific message element MAY be included in the CAPWAP Station Configuration Request message.

- IEEE 802.11 WTP Radio Fail Alarm Indication, see Section 6.24

5.12. WTP Event Request

The following IEEE 802.11-specific message elements MAY be included in the CAPWAP WTP Event Request message. More than one of each message element listed MAY be included.

- IEEE 802.11 MIC Countermeasures, see Section 6.8
- IEEE 802.11 RSNA Error Report from Station, see Section 6.12
- IEEE 802.11 Statistics, see Section 6.16

6. IEEE 802.11 Message Element Definitions

The following IEEE 802.11-specific message elements are defined in this section.

IEEE 802.11 Message Element	Type Value
IEEE 802.11 Add WLAN	1024
IEEE 802.11 Antenna	1025
IEEE 802.11 Assigned WTP BSSID	1026
IEEE 802.11 Delete WLAN	1027
IEEE 802.11 Direct Sequence Control	1028
IEEE 802.11 Information Element	1029
IEEE 802.11 MAC Operation	1030
IEEE 802.11 MIC Countermeasures	1031
IEEE 802.11 Multi-Domain Capability	1032
IEEE 802.11 OFDM Control	1033
IEEE 802.11 Rate Set	1034
IEEE 802.11 RSNA Error Report From Station	1035
IEEE 802.11 Station	1036
IEEE 802.11 Station QoS Profile	1037
IEEE 802.11 Station Session Key	1038
IEEE 802.11 Statistics	1039
IEEE 802.11 Supported Rates	1040
IEEE 802.11 Tx Power	1041
IEEE 802.11 Tx Power Level	1042
IEEE 802.11 Update Station QoS	1043
IEEE 802.11 Update WLAN	1044
IEEE 802.11 WTP Quality of Service	1045
IEEE 802.11 WTP Radio Configuration	1046
IEEE 802.11 WTP Radio Fail Alarm Indication	1047
IEEE 802.11 WTP Radio Information	1048

Figure 8: IEEE 802.11 Binding Message Elements

6.1. IEEE 802.11 Add WLAN

The IEEE 802.11 Add WLAN message element is used by the AC to define a WLAN on the WTP. The inclusion of this message element MUST also include IEEE 802.11 Information Element message elements, containing the following IEEE 802.11 IEs:

Power Constraint information element

EDCA Parameter Set information element

QoS Capability information element

WPA information element [WPA]

RSN information element

WMM information element [WMM]

These IEEE 802.11 Information Elements are stored by the WTP and included in any Probe Responses and Beacons generated, as specified in the IEEE 802.11 standard [IEEE.802-11.2007]. If present, the RSN Information Element is sent with the IEEE 802.11 Add WLAN message element to instruct the WTP on the usage of the Key field.

If cryptographic services are provided at the WTP, the WTP MUST observe the algorithm dictated in the Group Cipher Suite field of the RSN Information Element sent by the AC. The RSN Information Element is used to communicate any supported algorithm, including WEP, Temporal Key Integrity Protocol (TKIP) and AES-CCMP. In the case of static WEP keys, the RSN Information Element is still used to indicate the cryptographic algorithm even though no key exchange occurred.

An AC MAY include additional Information Elements as desired. The message element uses the following format:

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |    Radio ID   |    WLAN ID    |          Capability           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   Key Index   |   Key Status  |           Key Length          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                             Key...                            |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                           Group TSC                           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |           Group TSC           |      QoS      |   Auth Type   |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   MAC Mode    |  Tunnel Mode  | Suppress SSID |    SSID ...
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1024 for IEEE 802.11 Add WLAN

Length: >= 20

Radio ID: An 8-bit value representing the radio, whose value is between one (1) and 31.

WLAN ID: An 8-bit value specifying the WLAN Identifier. The value MUST be between one (1) and 16.

Capability: A 16-bit value containing the Capability information field to be advertised by the WTP in the Probe Request and Beacon frames. Each bit of the Capability field represents a different WTP capability, which are described in detail in [IEEE.802-11.2007]. The format of the field is:

```
  0                   1
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |E|I|C|F|P|S|B|A|M|Q|T|D|V|O|K|L|
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

E (ESS): The AC MUST set the Extended Service Set (ESS) subfield to 1.

I (IBSS): The AC MUST set the Independent Basic Service Set (IBSS) subfield to 0.

C (CF-Pollable): The AC sets the Contention Free Pollable (CF-Pollable) subfield based on the table found in [IEEE.802-11.2007].

F (CF-Poll Request): The AC sets the CF-Poll Request subfield based on the table found in [IEEE.802-11.2007].

P (Privacy): The AC sets the Privacy subfield based on the confidentiality requirements of the WLAN, as defined in [IEEE.802-11.2007].

S (Short Preamble): The AC sets the Short Preamble subfield based on whether the use of short preambles is permitted on the WLAN, as defined in [IEEE.802-11.2007].

B (PBCC): The AC sets the Packet Binary Convolutional Code (PBCC) modulation option subfield based on whether the use of PBCC is permitted on the WLAN, as defined in [IEEE.802-11.2007].

A (Channel Agility): The AC sets the Channel Agility subfield based on whether the WTP is capable of supporting the High Rate Direct Sequence Spread Spectrum (HR/DSSS), as defined in [IEEE.802-11.2007].

M (Spectrum Management): The AC sets the Spectrum Management subfield according to the value of the dot11SpectrumManagementRequired MIB variable, as defined in [IEEE.802-11.2007].

Q (QoS): The AC sets the Quality of Service (QoS) subfield based on the table found in [IEEE.802-11.2007].

T (Short Slot Time): The AC sets the Short Slot Time subfield according to the value of the WTP’s currently used slot time value, as defined in [IEEE.802-11.2007].

D (APSD): The AC sets the Automatic Power Save Delivery (APSD) subfield according to the value of the dot11APSDOptionImplemented Management Information Base (MIB) variable, as defined in [IEEE.802-11.2007].

V (Reserved): The AC sets the Reserved subfield to zero, as defined in [IEEE.802-11.2007].

O (DSSS-OFDM): The AC sets the DSSS-OFDM subfield to indicate the use of Direct Sequence Spread Spectrum with Orthogonal Frequency Division Multiplexing (DSSS-OFDM), as defined in [IEEE.802-11.2007].

K (Delayed Block ACK): The AC sets the Delayed Block ACK subfield according to the value of the dot11DelayedBlockAckOptionImplemented MIB variable, as defined in [IEEE.802-11.2007].

L (Immediate Block ACK): The AC sets the Delayed Block ACK subfield according to the value of the dot11ImmediateBlockAckOptionImplemented MIB variable, as defined in [IEEE.802-11.2007].

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

Key Status: A 1-byte value that specifies the state and usage of the key that has been included. Note this field is ignored if the Key Length field is set to zero (0). The following values describe the key usage and its status:

0 - A value of zero, with the inclusion of the RSN Information Element means that the WLAN uses per-station encryption keys, and therefore the key in the ’Key’ field is only used for multicast traffic.

1 - When set to one, the WLAN employs a shared Wired Equivalent Privacy (WEP) key, also known as a static WEP key, and uses the encryption key for both unicast and multicast traffic for all stations.

2 - The value of 2 indicates that the AC will begin rekeying the GTK with the STA's in the BSS. It is only valid when IEEE 802.11 is enabled as the security policy for the BSS.

3 - The value of 3 indicates that the AC has completed rekeying the GTK and broadcast packets no longer need to be duplicated and transmitted with both GTK's.

Key Length: A 16-bit value representing the length of the Key field.

Key: A Session Key, whose length is known via the Key Length field, used to provide data privacy. For encryption schemes that employ a separate encryption key for unicast and multicast traffic, the key included here only applies to multicast frames, and the cipher suite is specified in an accompanied RSN Information Element. In these scenarios, the key and cipher information is communicated via the Add Station message element, see Section 4.6.8 in [RFC5415] and the IEEE 802.11 Station Session Key message element, see Section 6.15. When used with WEP, the key field includes the broadcast key. When used with CCMP, the Key field includes the 128-bit Group Temporal Key. When used with TKIP, the Key field includes the 256-bit Group Temporal Key (which consists of a 128-bit key used as input for TKIP key mixing, and two 64-bit keys used for Michael).

Group TSC: A 48-bit value containing the Transmit Sequence Counter (TSC) for the updated group key. The WTP will set the TSC for broadcast/multicast frames to this value for the updated group key.

QoS: An 8-bit value specifying the default QoS policy for the WTP to apply to network traffic received for a non-WMM enabled STA.

The following enumerated values are supported:

0 - Best Effort

1 - Video

2 - Voice

3 - Background

Auth Type: An 8-bit value specifying the supported authentication type.

The following enumerated values are supported:

0 - Open System

1 - WEP Shared Key

MAC Mode: This field specifies whether the WTP should support the WLAN in Local or Split MAC mode. Note that the AC MUST NOT request a mode of operation that was not advertised by the WTP during the discovery process (see Section 4.6.43 in [RFC5415]). The following enumerated values are supported:

0 - Local MAC: Service for the WLAN is to be provided in Local MAC mode.

1 - Split MAC: Service for the WLAN is to be provided in Split MAC mode.

Tunnel Mode: This field specifies the frame tunneling type to be used for 802.11 data frames from all stations associated with the WLAN. The AC MUST NOT request a mode of operation that was not advertised by the WTP during the discovery process (see Section 4.6.42 in [RFC5415]). All IEEE 802.11 management frames MUST be tunneled using 802.11 Tunnel mode. The following enumerated values are supported:

0 - Local Bridging: All user traffic is to be locally bridged.

1 - 802.3 Tunnel: All user traffic is to be tunneled to the AC in 802.3 format (see Section 4.4.2 in [RFC5415]). Note that this option MUST NOT be selected with Split MAC mode.

2 - 802.11 Tunnel: All user traffic is to be tunneled to the AC in 802.11 format.

Suppress SSID: A boolean indicating whether the SSID is to be advertised by the WTP. A value of zero suppresses the SSID in the 802.11 Beacon and Probe Response frames, while a value of one will cause the WTP to populate the field.

SSID: The SSID attribute is the service set identifier that will be advertised by the WTP for this WLAN. The SSID field contains any ASCII character and MUST NOT exceed 32 octets in length, as defined in [IEEE.802-11.2007].

6.2. IEEE 802.11 Antenna

The IEEE 802.11 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 message element contains the following fields:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |   Diversity   |    Combiner   |  Antenna Cnt  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Antenna Selection...
+-+-+-+-+-+-+-+-+
```

Type: 1025 for IEEE 802.11 Antenna

Length: >= 5

Radio ID: An 8-bit value representing the radio to configure, whose value is between one (1) and 31.

Diversity: An 8-bit value specifying whether the antenna is to provide receiver diversity. The value of this field is the same as the IEEE 802.11 dot11DiversitySelectionRx MIB element, see [IEEE.802-11.2007]. The following enumerated values are supported:

0 - Disabled

1 - Enabled (may only be true if the antenna can be used as a receiving antenna)

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

1 - Sectorized (Left)

2 - Sectorized (Right)

3 - Omni

4 - Multiple Input/Multiple Output (MIMO)

Antenna Count: An 8-bit value specifying the number of Antenna Selection fields. This value SHOULD be the same as the one found in the IEEE 802.11 dot11CurrentTxAntenna MIB element (see [IEEE.802-11.2007]).

Antenna Selection: One 8-bit antenna configuration value per antenna in the WTP, containing up to 255 antennas. The following enumerated values are supported:

1 - Internal Antenna

2 - External Antenna

6.3. IEEE 802.11 Assigned WTP BSSID

The IEEE 802.11 Assigned WTP BSSID is only included by the WTP when the IEEE 802.11 WLAN Configuration Request included the IEEE 802.11 Add WLAN message element. The BSSID value field of this message element contains the BSSID that has been assigned by the WTP, enabling the WTP to perform its own BSSID assignment.

The WTP is free to assign the BSSIDs the way it sees fit, but it is highly recommended that the WTP assign the BSSID using the following algorithm: BSSID = {base BSSID} + WLAN ID.

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

Type: 1026 for IEEE 802.11 Assigned WTP BSSID

Length: 8

Radio ID: An 8-bit value representing the radio, whose value is between one (1) and 31.

WLAN ID: An 8-bit value specifying the WLAN Identifier. The value MUST be between one (1) and 16.

BSSID: The BSSID assigned by the WTP for the WLAN created as a result of receiving an IEEE 802.11 Add WLAN.

6.4. IEEE 802.11 Delete WLAN

The IEEE 802.11 Delete WLAN message element is used to inform the WTP that a previously created WLAN is to be deleted, and contains the following fields:

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

Type: 1027 for IEEE 802.11 Delete WLAN

Length: 2

Radio ID: An 8-bit value representing the radio, whose value is between one (1) and 31.

WLAN ID: An 8-bit value specifying the WLAN Identifier. The value MUST be between one (1) and 16.

6.5. IEEE 802.11 Direct Sequence Control

The IEEE 802.11 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 provided. This element is only used for IEEE 802.11b radios. The message element has the following fields.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |    Reserved   | Current Chan  |  Current CCA  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Energy Detect Threshold                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1028 for IEEE 802.11 Direct Sequence Control

Length: 8

Radio ID: An 8-bit value representing the radio to configure, whose value is between one (1) and 31.

Reserved: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

Current Channel: This attribute contains the current operating frequency channel of the Direct Sequence Spread Spectrum (DSSS) PHY. This value comes from the IEEE 802.11 dot11CurrentChannel MIB element (see [IEEE.802-11.2007]).

Current CCA: The current Clear Channel Assessment (CCA) method in operation, whose value can be found in the IEEE 802.11 dot11CCAModeSupported MIB element (see [IEEE.802-11.2007]). 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. The value can be found in the IEEE 802.11 dot11EDThreshold MIB element (see [IEEE.802-11.2007]).

6.6. IEEE 802.11 Information Element

The IEEE 802.11 Information Element is used to communicate any IE defined in the IEEE 802.11 protocol. The data field contains the raw IE as it would be included within an IEEE 802.11 MAC management message.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Radio ID    |    WLAN ID    |B|P| Reserved  |Info Element...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1029 for IEEE 802.11 Information Element

Length: >= 4

Radio ID: An 8-bit value representing the radio, whose value is between one (1) and 31.

WLAN ID: An 8-bit value specifying the WLAN Identifier. The value MUST be between one (1) and 16.

B: When set, the WTP is to include the Information Element in IEEE 802.11 Beacons associated with the WLAN.

P: When set, the WTP is to include the Information Element in Probe Responses associated with the WLAN.

Reserved: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

Info Element: The IEEE 802.11 Information Element, which includes the type, length, and value field.

6.7. IEEE 802.11 MAC Operation

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

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |    Radio ID   |    Reserved   |         RTS Threshold         |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |  Short Retry  |  Long Retry   |    Fragmentation Threshold    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                       Tx MSDU Lifetime                        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                       Rx MSDU Lifetime                        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1030 for IEEE 802.11 MAC Operation

Length: 16

Radio ID: An 8-bit value representing the radio to configure, whose value is between one (1) and 31.

Reserved: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

RTS Threshold: This attribute indicates the number of octets in an MAC Protocol Data Unit (MPDU), below which a Request To Send/Clear To Send (RTS/CTS) handshake MUST NOT be performed. An RTS/CTS handshake MUST be performed at the beginning of any frame exchange sequence where the MPDU is of type Data or Management, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size MUST have the effect of turning off the RTS/CTS handshake for frames of Data or Management type transmitted by this STA. Setting this attribute to zero MUST have the effect of turning on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default value of this attribute MUST be 2347. The value of this field comes from the IEEE 802.11 dot11RTSThreshold MIB element, (see [IEEE.802-11.2007]).

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. The value of this field comes from the IEEE 802.11 dot11ShortRetryLimit MIB element, (see [IEEE.802-11.2007]).

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. The value of this field comes from the IEEE 802.11 dot11LongRetryLimit MIB element, (see [IEEE.802-11.2007]).

Fragmentation Threshold: This attribute specifies the current maximum size, in octets, of the MPDU that MAY be delivered to the PHY. A MAC Service Data Unit (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. The value of this field comes from the IEEE 802.11 dot11FragmentationThreshold MIB element, (see [IEEE.802-11.2007]).

Tx MSDU Lifetime: This attribute specifies the elapsed time in Time Units (TUs), 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. The value of this field comes from the IEEE 802.11 dot11MaxTransmitMSDULifetime MIB element, (see [IEEE.802-11.2007]).

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. The value of this field comes from the IEEE 802.11 dot11MaxReceiveLifetime MIB element, (see [IEEE.802-11.2007]).

6.8. IEEE 802.11 MIC Countermeasures

The IEEE 802.11 MIC Countermeasures message element is sent by the WTP to the AC to indicate the occurrence of a MIC failure. For more information on MIC failure events, see the dot11RSNATKIPCounterMeasuresInvoked MIB element definition in [IEEE.802-11.2007].

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

Type: 1031 for IEEE 802.11 MIC Countermeasures

Length: 8

Radio ID: The Radio Identifier, whose value is between one (1) and 31, 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. The value MUST be between one (1) and 16.

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

6.9. IEEE 802.11 Multi-Domain Capability

The IEEE 802.11 Multi-Domain Capability message element is used by the AC to inform the WTP of regulatory limits. The AC will transmit one message element per frequency band to indicate the regulatory constraints in that domain. The message element contains the following fields.

```
        0                   1                   2                   3
        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |    Radio ID   |    Reserved   |        First Channel #        |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |       Number of Channels      |       Max Tx Power Level      |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1032 for IEEE 802.11 Multi-Domain Capability

Length: 8

Radio ID: An 8-bit value representing the radio to configure, whose value is between one (1) and 31.

Reserved: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

First Channel #: This attribute indicates the value of the lowest channel number in the sub-band for the associated domain country string. The value of this field comes from the IEEE 802.11 dot11FirstChannelNumber MIB element (see [IEEE.802-11.2007]).

Number of Channels: This attribute indicates the value of the total number of channels allowed in the sub-band for the associated domain country string (see Section 6.23). The value of this field comes from the IEEE 802.11 dot11NumberofChannels MIB element (see [IEEE.802-11.2007]).

Max Tx Power Level: This attribute indicates the maximum transmit power, in dBm, allowed in the sub-band for the associated domain country string (see Section 6.23). The value of this field comes from the IEEE 802.11 dot11MaximumTransmitPowerLevel MIB element (see [IEEE.802-11.2007]).

6.10. IEEE 802.11 OFDM Control

The IEEE 802.11 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 received values. This message element is only used for 802.11a radios and contains the following fields:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |    Reserved   | Current Chan  |  Band Support |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         TI Threshold                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1033 for IEEE 802.11 OFDM Control

Length: 8

Radio ID: An 8-bit value representing the radio to configure, whose value is between one (1) and 31.

Reserved: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

Current Channel: This attribute contains the current operating frequency channel of the OFDM PHY. The value of this field comes from the IEEE 802.11 dot11CurrentFrequency MIB element (see [IEEE.802-11.2007]).

Band Supported: The capability of the OFDM PHY implementation to operate in the three Unlicensed National Information Infrastructure (U-NII) bands. The value of this field comes from the IEEE 802.11 dot11FrequencyBandsSupported MIB element (see [IEEE.802-11.2007]), coded as a bit field, whose values are:

Bit 0 - capable of operating in the 5.15-5.25 GHz band

Bit 1 - capable of operating in the 5.25-5.35 GHz band

Bit 2 - capable of operating in the 5.725-5.825 GHz band

Bit 3 - capable of operating in the 5.47-5.725 GHz band

Bit 4 - capable of operating in the lower Japanese 5.25 GHz band

Bit 5 - capable of operating in the 5.03-5.091 GHz band

Bit 6 - capable of operating in the 4.94-4.99 GHz band

For example, for an implementation capable of operating in the 5.15-5.35 GHz bands, this attribute would take the value 3.

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. The value of this field comes from the IEEE 802.11 dot11TIThreshold MIB element (see [IEEE.802-11.2007]).

6.11. 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.

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

Type: 1034 for IEEE 802.11 Rate Set

Length: >= 3

Radio ID: An 8-bit value representing the radio to configure, whose value is between one (1) and 31.

Rate Set: The AC generates the Rate Set that the WTP is to include in its Beacon and Probe messages. The length of this field is between 2 and 8 bytes. The value of this field comes from the IEEE 802.11 dot11OperationalRateSet MIB element (see [IEEE.802-11.2007]).

6.12. IEEE 802.11 RSNA Error Report From Station

The IEEE 802.11 RSN Error Report From Station message element is used by a WTP to send RSN error reports to the AC. The WTP does not need to transmit any reports that do not include any failures. The fields from this message element come from the IEEE 802.11 Dot11RSNAStatsEntry table, see [IEEE.802-11.2007].

```
        0                   1                   2                   3
        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                       Client MAC Address                      |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |      Client MAC Address       |             BSSID             |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                             BSSID                             |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |   Radio ID    |    WLAN ID    |           Reserved            |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                        TKIP ICV Errors                        |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                    TKIP Local MIC Failures                    |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                   TKIP Remote MIC Failures                    |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                          CCMP Replays                         |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                       CCMP Decrypt Errors                     |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                          TKIP Replays                         |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1035 for IEEE 802.11 RSNA Error Report From Station

Length: 40

Client MAC Address: The Client MAC Address of the station.

BSSID: The BSSID on which the failures are being reported.

Radio ID: The Radio Identifier, whose value is between one (1) and 31, typically refers to some interface index on the WTP.

WLAN ID: The WLAN ID on which the RSNA failures are being reported. The value MUST be between one (1) and 16.

Reserved: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

TKIP ICV Errors: A 32-bit value representing the number of Temporal Key Integrity Protocol (TKIP) (as defined in [IEEE.802-11.2007]) ICV errors encountered when decrypting packets from the station. The value of this field comes from the IEEE 802.11 dot11RSNAStatsTKIPICVErrors MIB element (see [IEEE.802-11.2007]).

TKIP Local MIC Failures: A 32-bit value representing the number of MIC failures encountered when checking the integrity of packets received from the station. The value of this field comes from the IEEE 802.11 dot11RSNAStatsTKIPLocalMICFailures MIB element (see [IEEE.802-11.2007]).

TKIP Remote MIC Failures: A 32-bit value representing the number of MIC failures reported by the station encountered (possibly via the EAPOL-Key frame). The value of this field comes from the IEEE 802.11 dot11RSNAStatsTKIPRemoteMICFailures MIB element (see [IEEE.802-11.2007]).

CCMP Replays: A 32-bit value representing the number of CCMP MPDUs discarded by the replay detection mechanism. The value of this field comes from the IEEE 802.11 dot11RSNACCMPReplays MIB element (see [IEEE.802-11.2007]).

CCMP Decrypt Errors: A 32-bit value representing the number of CCMP MDPUs discarded by the decryption algorithm. The value of this field comes from the IEEE 802.11 dot11RSNACCMPDecryptErrors MIB element (see [IEEE.802-11.2007]).

TKIP Replays: A 32-bit value representing the number of TKIP Replays detected in frames received from the station. The value of this field comes from the IEEE 802.11 dot11RSNAStatsTKIPReplays MIB element (see [IEEE.802-11.2007]).

6.13. IEEE 802.11 Station

The IEEE 802.11 Station message element accompanies the Add Station message element, and is used to deliver IEEE 802.11 station policy from the AC to the WTP.

The latest IEEE 802.11 Station message element overrides any previously received message elements.

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.

```
      0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |    Radio ID   |        Association ID         |     Flags     |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                          MAC Address                          |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |          MAC Address          |         Capabilities          |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |   WLAN ID     |Supported Rates|
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1036 for IEEE 802.11 Station

Length: >= 14

Radio ID: An 8-bit value representing the radio, whose value is between one (1) and 31.

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

Flags: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

MAC Address: The station’s MAC Address

Capabilities: A 16-bit field containing the IEEE 802.11 Capabilities Information Field to use with the station.

WLAN ID: An 8-bit value specifying the WLAN Identifier. The value MUST be between one (1) and 16.

Supported Rates: The variable-length field containing the supported rates to be used with the station, as found in the IEEE 802.11 dot11OperationalRateSet MIB element (see [IEEE.802-11.2007]). This field MUST NOT exceed 126 octets and specifies the set of data rates at which the station may transmit data, where each octet represents a data rate.

6.14. IEEE 802.11 Station QoS Profile

The IEEE 802.11 Station QoS Profile message element contains the maximum IEEE 802.11e priority tag that may be used by the station. Any packet received that exceeds the value encoded in this message element MUST be tagged using the maximum value permitted by to the user. The priority tag MUST be between zero (0) and seven (7). This message element MUST NOT be present without the IEEE 802.11 Station (see Section 6.13) message element.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                           MAC Address                         |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |          MAC Address          |         Reserved      |8021p|
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1037 for IEEE 802.11 Station QoS Profile

Length: 8

MAC Address: The station’s MAC Address

Reserved: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

8021p: The maximum 802.1p priority value that the WTP will allow in the Traffic Identifier (TID) field in the extended 802.11e QoS Data header.

6.15. IEEE 802.11 Station Session Key

The IEEE 802.11 Station Session Key message element is sent by the AC to provision encryption keys, or to configure an access policy, on the WTP. This message element MUST NOT be present without the IEEE 802.11 Station (see Section 6.13) message element, and MUST NOT be sent if the WTP had not specifically advertised support for the requested encryption scheme, through the WTP Descriptor Message Element’s Encryption Capabilities field (see Section 8.1).

When the Key field is non-zero in length, the RSN Information Element MUST be sent along with the IEEE 802.11 Station Session Key in order to instruct the WTP on the usage of the Key field. The WTP MUST observe the Authentication and Key Management (AKM) field of the RSN Information Element in order to identify the authentication protocol to be enforced with the station.

If cryptographic services are provided at the WTP, the WTP MUST observe the algorithm dictated in the Pairwise Cipher Suite field of the RSN Information Element sent by the AC. The RSN Information Element included here is the one sent by the AC in the third message of the 4-Way Key Handshake, which specifies which cipher is to be applied to provide encryption and decryption services with the station. The RSN Information Element is used to communicate any supported algorithm, including WEP, TKIP, and AES-CCMP. In the case of static WEP keys, the RSN Information Element is still used to indicate the cryptographic algorithm even though no key exchange occurred.

If the IEEE 802.11 Station Session Key message element's 'AKM-Only' bit is set, the WTP MUST drop all IEEE 802.11 packets that are not part of the Authentication and Key Management (AKM), such as EAP. Note that AKM-Only MAY be set while an encryption key is in force, requiring that the AKM packets be encrypted. Once the station has successfully completed authentication via the AKM, the AC MUST send a new Add Station message element to remove the AKM-Only restriction, and optionally push the session key down to the WTP.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                          MAC Address                          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |          MAC Address          |A|C|           Flags           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                         Pairwise TSC                          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |         Pairwise TSC          |         Pairwise RSC          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                         Pairwise RSC                          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |    Key...
    +-+-+-+-+-+-+-+-
```

Type: 1038 for IEEE 802.11 Station Session Key

Length: >= 25

MAC Address: The station's MAC Address

Flags: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support. The following bits are defined:

A: The 1-bit AKM-Only field is set by the AC to inform the WTP that is MUST NOT accept any 802.11 Data Frames other than AKM frames. This is the equivalent of the WTP's IEEE 802.1X port for the station to be in the closed state. When set, the WTP MUST drop any non-IEEE 802.1X packets it receives from the 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 are properly encrypted as specified in the RSN Information Element, 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. Since packets received by the WTP will be encrypted, the WTP cannot modify the contents of the packets, including modifying the DSCP markings of the encapsulated packet. In this case, this function would be the responsibility of the AC.

Pairwise TSC: The 6-byte Transmit Sequence Counter (TSC) field to use for unicast packets transmitted to the station.

Pairwise RSC: The 6-byte Receive Sequence Counter (RSC) to use for unicast packets received from the station.

Key: The pairwise key the WTP is to use when encrypting traffic to/from the station. The format of the keys differs based on the crypto algorithm used. For unicast WEP keys, the Key field consists of the actual unicast encryption key (note, this is used when WEP is used in conjunction with 802.1X, and therefore a unicast encryption key exists). When used with CCMP, the Key field includes the 128-bit Temporal Key. When used with TKIP, the Key field includes the 256-bit Temporal Key (which consists of a 128-bit key used as input for TKIP key mixing, and two 64-bit keys used for Michael).

6.16. IEEE 802.11 Statistics

The IEEE 802.11 Statistics message element is sent by the WTP to transmit its current statistics, and it contains the following fields. All of the fields in this message element are set to zero upon WTP initialization. The fields will roll over when they reach their maximum value of 4294967295. Due to the nature of each counter representing different data points, the rollover event will vary greatly across each field. Applications or human operators using these counters need to be aware of the minimal possible times between rollover events in order to make sure that no consecutive rollover events are missed.

```
        0                   1                   2                   3
        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |    Radio ID   |                   Reserved                    |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                       Tx Fragment Count                       |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                       Multicast Tx Count                      |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                          Failed Count                         |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                          Retry Count                          |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                      Multiple Retry Count                     |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                     Frame Duplicate Count                     |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                       RTS Success Count                       |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                       RTS Failure Count                       |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                       ACK Failure Count                       |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                       Rx Fragment Count                       |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                       Multicast RX Count                      |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                        FCS Error  Count                       |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                        Tx Frame Count                         |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                       Decryption Errors                       |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                  Discarded QoS Fragment Count                 |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                    Associated Station Count                   |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                  QoS CF Polls Received Count                  |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                   QoS CF Polls Unused Count                   |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                  QoS CF Polls Unusable Count                  |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1039 for IEEE 802.11 Statistics

Length: 80

Radio ID: An 8-bit value representing the radio, whose value is between one (1) and 31.

Reserved: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

Tx Fragment Count: A 32-bit value representing the number of fragmented frames transmitted. The value of this field comes from the IEEE 802.11 dot11TransmittedFragmentCount MIB element (see [IEEE.802-11.2007]).

Multicast Tx Count: A 32-bit value representing the number of multicast frames transmitted. The value of this field comes from the IEEE 802.11 dot11MulticastTransmittedFrameCount MIB element (see [IEEE.802-11.2007]).

Failed Count: A 32-bit value representing the transmit excessive retries. The value of this field comes from the IEEE 802.11 dot11FailedCount MIB element (see [IEEE.802-11.2007]).

Retry Count: A 32-bit value representing the number of transmit retries. The value of this field comes from the IEEE 802.11 dot11RetryCount MIB element (see [IEEE.802-11.2007]).

Multiple Retry Count: A 32-bit value representing the number of transmits that required more than one retry. The value of this field comes from the IEEE 802.11 dot11MultipleRetryCount MIB element (see [IEEE.802-11.2007]).

Frame Duplicate Count: A 32-bit value representing the duplicate frames received. The value of this field comes from the IEEE 802.11 dot11FrameDuplicateCount MIB element (see [IEEE.802-11.2007]).

RTS Success Count: A 32-bit value representing the number of successfully transmitted Ready To Send (RTS). The value of this field comes from the IEEE 802.11 dot11RTSSuccessCount MIB element (see [IEEE.802-11.2007]).

RTS Failure Count: A 32-bit value representing the failed transmitted RTS. The value of this field comes from the IEEE 802.11 dot11RTSFailureCount MIB element (see [IEEE.802-11.2007]).

ACK Failure Count: A 32-bit value representing the number of failed acknowledgements. The value of this field comes from the IEEE 802.11 dot11ACKFailureCount MIB element (see [IEEE.802-11.2007]).

Rx Fragment Count: A 32-bit value representing the number of fragmented frames received. The value of this field comes from the IEEE 802.11 dot11ReceivedFragmentCount MIB element (see [IEEE.802-11.2007]).

Multicast RX Count: A 32-bit value representing the number of multicast frames received. The value of this field comes from the IEEE 802.11 dot11MulticastReceivedFrameCount MIB element (see [IEEE.802-11.2007]).

FCS Error Count: A 32-bit value representing the number of FCS failures. The value of this field comes from the IEEE 802.11 dot11FCSErrorCount MIB element (see [IEEE.802-11.2007]).

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. The value of this field comes from the IEEE 802.11 dot11WEPUndecryptableCount MIB element (see [IEEE.802-11.2007]).

Discarded QoS Fragment Count: A 32-bit value representing the number of discarded QoS fragments received. The value of this field comes from the IEEE 802.11 dot11QoSDiscardedFragmentCount MIB element (see [IEEE.802-11.2007]).

Associated Station Count: A 32-bit value representing the number of number of associated stations. The value of this field comes from the IEEE 802.11 dot11AssociatedStationCount MIB element (see [IEEE.802-11.2007]).

QoS CF Polls Received Count: A 32-bit value representing the number of (+)CF-Polls received. The value of this field comes from the IEEE 802.11 dot11QosCFPollsReceivedCount MIB element (see [IEEE.802-11.2007]).

QoS CF Polls Unused Count: A 32-bit value representing the number of (+)CF-Polls that have been received, but not used. The value of this field comes from the IEEE 802.11 dot11QosCFPollsUnusedCount MIB element (see [IEEE.802-11.2007]).

QoS CF Polls Unusable Count: A 32-bit value representing the number of (+)CF-Polls that have been received, but could not be used due to the Transmission Opportunity (TXOP) size being smaller than the time that is required for one frame exchange sequence. The value of this field comes from the IEEE 802.11 dot11QosCFPollsUnusableCount MIB element (see [IEEE.802-11.2007]).

6.17. IEEE 802.11 Supported Rates

The IEEE 802.11 Supported Rates message element is sent by the WTP to indicate the rates that it supports, and contains the following fields.

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

Type: 1040 for IEEE 802.11 Supported Rates

Length: >= 3

Radio ID: An 8-bit value representing the radio, whose value is between one (1) and 31.

Supported Rates: The WTP includes the Supported Rates that its hardware supports. The format is identical to the Rate Set message element and is between 2 and 8 bytes in length.

6.18. IEEE 802.11 Tx Power

The IEEE 802.11 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.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |    Radio ID   |    Reserved   |        Current Tx Power       |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1041 for IEEE 802.11 Tx Power

Length: 4

Radio ID: An 8-bit value representing the radio to configure, whose value is between one (1) and 31.

Reserved: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

Current Tx Power: This attribute contains the current transmit output power in mW, as described in the dot11CurrentTxPowerLevel MIB variable, see [IEEE.802-11.2007].

6.19. IEEE 802.11 Tx Power Level

The IEEE 802.11 Tx Power Level message element is sent by the WTP and contains the different power levels supported. The values found in this message element are found in the IEEE 802.11 Dot11PhyTxPowerEntry MIB table, see [IEEE.802-11.2007].

The value field contains the following:

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |    Radio ID   |   Num Levels  |        Power Level [n]        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1042 for IEEE 802.11 Tx Power Level

Length: >= 4

Radio ID: An 8-bit value representing the radio to configure, whose value is between one (1) and 31.

Num Levels: The number of power level attributes. The value of this field comes from the IEEE 802.11 dot11NumberSupportedPowerLevels MIB element (see [IEEE.802-11.2007]).

Power Level: Each power level field contains a supported power level, in mW. The value of this field comes from the corresponding IEEE 802.11 dot11TxPowerLevel[n] MIB element, see [IEEE.802-11.2007].

6.20. IEEE 802.11 Update Station QoS

The IEEE 802.11 Update Station QoS message element is used to change the Quality of Service policy on the WTP for a given station. The QoS tags included in this message element are to be applied to packets received at the WTP from the station indicated through the MAC Address field. This message element overrides the default values provided through the IEEE 802.11 WTP Quality of Service message element (see Section 6.22). Any tagging performed by the WTP MUST be directly applied to the packets received from the station, as well as the CAPWAP tunnel, if the packets are tunneled to the AC. See Section 2.6 for more information.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   Radio ID    |                  MAC Address                  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          MAC Address          |       QoS Sub-Element...      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1043 for IEEE 802.11 Update Station QoS

Length: 8

Radio ID: The Radio Identifier, whose value is between one (1) and 31, typically refers to some interface index on the WTP.

MAC Address: The station’s MAC Address.

QoS Sub-Element: The IEEE 802.11 WTP Quality of Service message element contains four QoS sub-elements, one for every QoS profile. The order of the QoS profiles are Voice, Video, Best Effort, and Background.

```
    0                   1
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Reserved|8021p|RSV| DSCP Tag  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Reserved: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

8021p: The 3-bit 802.1p priority value to use if packets are to be IEEE 802.1p tagged. This field is used only if the ’P’ bit in the WTP Quality of Service message element was set; otherwise, its contents MUST be ignored.

RSV: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

DSCP Tag: The 6-bit DSCP label to use if packets are eligible to be DSCP tagged, specifically an IPv4 or IPv6 packet (see [RFC2474]). This field is used only if the ’D’ bit in the WTP Quality of Service message element was set; otherwise, its contents MUST be ignored.

6.21. IEEE 802.11 Update WLAN

The IEEE 802.11 Update WLAN message element is used by the AC to define a wireless LAN on the WTP. The inclusion of this message element MUST also include the IEEE 802.11 Information Element message element, containing the following 802.11 IEs:

Power Constraint information element

WPA information element [WPA]

RSN information element

Enhanced Distributed Channel Access (EDCA) Parameter Set information element

QoS Capability information element

WMM information element [WMM]

These IEEE 802.11 Information Elements are stored by the WTP and included in any Probe Responses and Beacons generated, as specified in the IEEE 802.11 standard [IEEE.802-11.2007].

If cryptographic services are provided at the WTP, the WTP MUST observe the algorithm dictated in the Group Cipher Suite field of the RSN Information Element sent by the AC. The RSN Information Element is used to communicate any supported algorithm, including WEP, TKIP, and AES-CCMP. In the case of static WEP keys, the RSN Information Element is still used to indicate the cryptographic algorithm even though no key exchange occurred.

The message element uses the following format:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |     WLAN ID   |           Capability          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Key Index   |  Key Status   |           Key Length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              Key...                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1044 for IEEE 802.11 Update WLAN

Length: >= 8

Radio ID: An 8-bit value representing the radio, whose value is between one (1) and 31.

WLAN ID: An 8-bit value specifying the WLAN Identifier. The value MUST be between one (1) and 16.

Capability: A 16-bit value containing the Capability information field to be advertised by the WTP in the Probe Request and Beacon frames. Each bit of the Capability field represents a different WTP capability, which are described in detail in [IEEE.802-11.2007]. The format of the field is:

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|E|I|C|F|P|S|B|A|M|Q|T|D|V|O|K|L|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

E (ESS):   The AC MUST set the Extended Service Set (ESS) subfield to 1.

I (IBSS):   The AC MUST set the Independent Basic Service Set (IBSS) subfield to 0.

C (CF-Pollable):   The AC sets the Contention Free Pollable (CF-Pollable) subfield based on the table found in [IEEE.802-11.2007].

F (CF-Poll Request):   The AC sets the CF-Poll Request subfield based on the table found in [IEEE.802-11.2007].

P (Privacy): The AC sets the Privacy subfield based on the confidentiality requirements of the WLAN, as defined in [IEEE.802-11.2007].

S (Short Preamble): The AC sets the Short Preamble subfield based on whether the use of short preambles are permitted on the WLAN, as defined in [IEEE.802-11.2007].

B (PBCC): The AC sets the Packet Binary Convolutional Code (PBCC) modulation option subfield based on whether the use of PBCC is permitted on the WLAN, as defined in [IEEE.802-11.2007].

A (Channel Agility): The AC sets the Channel Agility subfield based on whether the WTP is capable of supporting the High Rate Direct Sequence Spread Spectrum (HR/DSSS), as defined in [IEEE.802-11.2007].

M (Spectrum Management): The AC sets the Spectrum Management subfield according to the value of the dot11SpectrumManagementRequired MIB variable, as defined in [IEEE.802-11.2007].

Q (QoS): The AC sets the Quality of Service (QoS) subfield based on the table found in [IEEE.802-11.2007].

T (Short Slot Time): The AC sets the Short Slot Time subfield according to the value of the WTP’s currently used slot time value, as defined in [IEEE.802-11.2007].

D (APSD): The AC sets the APSD subfield according to the value of the dot11APSDOptionImplemented Management Information Base (MIB) variable, as defined in [IEEE.802-11.2007].

V (Reserved): The AC sets the Reserved subfield to zero, as defined in [IEEE.802-11.2007].

O (DSSS-OFDM): The AC sets the DSSS-OFDM subfield to indicate the use of Direct Sequence Spread Spectrum with Orthogonal Frequency Division Multiplexing (DSSS-OFDM), as defined in [IEEE.802-11.2007].

K (Delayed Block ACK): The AC sets the Delayed Block ACK subfield according to the value of the dot11DelayedBlockAckOptionImplemented MIB variable, as defined in [IEEE.802-11.2007].

L (Immediate Block ACK): The AC sets the Delayed Block ACK subfield according to the value of the dot11ImmediateBlockAckOptionImplemented MIB variable, as defined in [IEEE.802-11.2007].

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

Key Status: A 1-byte value that specifies the state and usage of the key that has been included. The following values describe the key usage and its status:

0 - A value of zero, with the inclusion of the RSN Information Element means that the WLAN uses per-station encryption keys, and therefore the key in the 'Key' field is only used for multicast traffic.

1 - When set to one, the WLAN employs a shared WEP key, also known as a static WEP key, and uses the encryption key for both unicast and multicast traffic for all stations.

2 - The value of 2 indicates that the AC will begin rekeying the GTK with the STA's in the BSS. It is only valid when IEEE 802.11 is enabled as the security policy for the BSS.

3 - The value of 3 indicates that the AC has completed rekeying the GTK and broadcast packets no longer need to be duplicated and transmitted with both GTK's.

Key Length: A 16-bit value representing the length of the Key field.

Key: A Session Key, whose length is known via the Key Length field, used to provide data privacy. For static WEP keys, which is true when the 'Key Status' bit is set to one, this key is used for both unicast and multicast traffic. For encryption schemes that employ a separate encryption key for unicast and multicast traffic, the key included here only applies to multicast data, and the cipher suite is specified in an accompanied RSN Information Element. In these scenarios, the key, and cipher information, is communicated via the Add Station message element, see Section 4.6.8 in [RFC5415]. When used with WEP, the Key field includes the broadcast key. When used with CCMP, the Key field includes the 128-bit Group Temporal Key. When used with TKIP, the Key field includes the 256-bit Group Temporal Key (which consists of a 128-bit key used as input for TKIP key mixing, and two 64-bit keys used for Michael).

6.22. IEEE 802.11 WTP Quality of Service

The IEEE 802.11 WTP Quality of Service message element value is sent by the AC to the WTP to communicate Quality of Service configuration information. The QoS tags included in this message element are the default QoS values to be applied to packets received by the WTP from stations on a particular radio. Any tagging performed by the WTP MUST be directly applied to the packets received from the station, as well as the CAPWAP tunnel, if the packets are tunneled to the AC. See Section 2.6 for more information.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   Radio ID    |Tagging Policy |       QoS Sub-Element ...
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1045 for IEEE 802.11 WTP Quality of Service

Length: 34

Radio ID: The Radio Identifier, whose value is between one (1) and 31, typically refers to some interface index on the WTP.

Tagging Policy: A bit field indicating how the WTP is to mark packets for QoS purposes. The required WTP behavior is defined in Section 2.6.1. The field has the following format:

```
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|Rsvd |P|Q|D|O|I|
+-+-+-+-+-+-+-+-+
```

Rsvd: A set of reserved bits for future use. All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

P: When set, the WTP is to employ the 802.1p QoS mechanism (see Section 2.6.1.1), and the WTP is to use the ’Q’ bit.

Q: When the ’P’ bit is set, the ’Q’ bit is used by the AC to communicate to the WTP how 802.1p QoS is to be enforced. Details on the behavior of the ’Q’ bit are specified in Section 2.6.1.1.

D: When set, the WTP is to employ the DSCP QoS mechanism (see Section 2.6.1.2), and the WTP is to use the ’O’ and ’I’ bits.

O: When the ’D’ bit is set, the ’O’ bit is used by the AC to communicate to the WTP how DSCP QoS is to be enforced on the outer (tunneled) header. Details on the behavior of the ’O’ bit are specified in Section 2.6.1.2.

I: When the ’D’ bit is set, the ’I’ bit is used by the AC to communicate to the WTP how DSCP QoS is to be enforced on the station’s packet (inner) header. Details on the behavior of the ’I’ bit are specified in Section 2.6.1.2.

QoS Sub-Element: The IEEE 802.11 WTP Quality of Service message element contains four QoS sub-elements, one for every QoS profile. The order of the QoS profiles are Voice, Video, Best Effort, and Background.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Queue Depth  |             CWMin             |     CWMax     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     CWMax     |     AIFS      | Reserved|8021p|RSV| DSCP Tag  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

CWMin: The Contention Window minimum (CWmin) value for the QoS transmit queue. The value of this field comes from the IEEE 802.11 dot11EDCATableCWMin MIB element (see [IEEE.802-11.2007]).

CWMax: The Contention Window maximum (CWmax) value for the QoS transmit queue. The value of this field comes from the IEEE 802.11 dot11EDCATableCWMax MIB element (see [IEEE.802-11.2007]).

AIFS: The Arbitration Inter Frame Spacing (AIFS) to use for the QoS transmit queue. The value of this field comes from the IEEE 802.11 dot11EDCATableAIFSN MIB element (see [IEEE.802-11.2007]).

Reserved: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

8021p: The 3-bit 802.1p priority value to use if packets are to be IEEE 802.1p tagged. This field is used only if the 'P' bit is set; otherwise, its contents MUST be ignored.

RSV: All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

DSCP Tag: The 6-bit DSCP label to use if packets are eligible to be DSCP tagged, specifically an IPv4 or IPv6 packet (see [RFC2474]). This field is used only if the 'D' bit is set; otherwise, its contents MUST be ignored.

6.23. IEEE 802.11 WTP Radio Configuration

The IEEE 802.11 WTP WLAN Radio Configuration message element is used by the AC to configure a Radio on the WTP, and by the WTP to deliver its radio configuration to the AC. The message element value contains the following fields:

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |   Radio ID    |Short Preamble| Num of BSSIDs |  DTIM Period  |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                            BSSID                              |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |          BSSID                |      Beacon Period            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                        Country String                         |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 1046 for IEEE 802.11 WTP WLAN Radio Configuration

Length: 16

Radio ID: An 8-bit value representing the radio to configure, whose value is between one (1) and 31.

Short Preamble: An 8-bit value indicating whether short preamble is supported. The following enumerated values are currently supported:

0 - Short preamble not supported.

1 - Short preamble is supported.

BSSID: The WLAN Radio’s base MAC Address.

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, and is between 1 and 16.

DTIM Period: This attribute specifies the number of Beacon intervals that elapse between transmission of Beacons frames containing a Traffic Indication Map (TIM) element whose Delivery Traffic Indication Message (DTIM) Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames. The value of this field comes from the IEEE 802.11 dot11DTIMPeriod MIB element (see [IEEE.802-11.2007]).

Beacon Period: This attribute specifies the number of Time Unit (TU) that a station uses for scheduling Beacon transmissions. This value is transmitted in Beacon and Probe Response frames. The value of this field comes from the IEEE 802.11 dot11BeaconPeriod MIB element (see [IEEE.802-11.2007]).

Country String: This attribute identifies the country in which the station is operating. The value of this field comes from the IEEE 802.11 dot11CountryString MIB element (see [IEEE.802-11.2007]). Some regulatory domains do not allow WTPs to have user configurable country string, and require that it be a fixed value during the manufacturing process. Therefore, WTP vendors that wish to allow for the configuration of this field will need to validate this behavior during its radio certification process. Other WTP vendors may simply wish to treat this WTP configuration parameter as read-only. The country strings can be found in [ISO.3166-1].

The WTP and AC MAY ignore the value of this field, depending upon regulatory requirements, for example to avoid classification as a Software-Defined Radio. When this field is used, the first two octets of this string is the two-character country string as described in [ISO.3166-1], and the third octet MUST either be a space, ’O’, ’I’, or X’ as defined below. When the value of the third octet is 255 (HEX 0xff), the country string field is not used, and MUST be ignored. The following are the possible values for the third octet:

1. an ASCII space character, if the regulations under which the station is operating encompass all environments in the country,

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

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

4. an ASCII ’X’ character, if the station is operating under a non-country entity. The first two octets of the non-country entity shall be two ASCII ’XX’ characters,

5. a HEX 0xff character means that the country string field is not used and MUST be ignored.

Note that the last byte of the Country String MUST be set to NULL.

6.24. IEEE 802.11 WTP Radio Fail Alarm Indication

The IEEE 802.11 WTP Radio Fail Alarm Indication message element is sent by the WTP to the AC when it detects a radio failure.

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

Type: 1047 for IEEE 802.11 WTP Radio Fail Alarm Indication

Length: 4

Radio ID: The Radio Identifier, whose value is between one (1) and 31, typically refers to some interface index on the WTP.

Type: The type of radio failure detected. The following enumerated 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: All implementations complying with version zero of this protocol MUST set these bits to zero. Receivers MUST ignore all bits not defined for the version of the protocol they support.

6.25. IEEE 802.11 WTP Radio Information

The IEEE 802.11 WTP Radio Information message element is used to communicate the radio information for each IEEE 802.11 radio in the WTP. The Discovery Request message, Primary Discovery Request message, and Join Request message 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 IEEE 802.11 technology specific binding is to be used with the WTP.

The message element contains two fields, as shown below.

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

Type: 1048 for IEEE 802.11 WTP Radio Information

Length: 5

Radio ID: The Radio Identifier, whose value is between one (1) and 31, which typically refers to an interface index on the WTP.

Radio Type: The type of radio present. Note this is a bit field that is used to specify support for more than a single type of PHY/MAC. The field has the following format:

```
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|Reservd|N|G|A|B|
+-+-+-+-+-+-+-+-+
```

Reservd: A set of reserved bits for future use. All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

N: An IEEE 802.11n radio.

G: An IEEE 802.11g radio.

A: An IEEE 802.11a radio.

B: An IEEE 802.11b radio.

7. IEEE 802.11 Binding WTP Saved Variables

This section contains the IEEE 802.11 binding specific variables that SHOULD be saved in non-volatile memory on the WTP.

7.1. IEEE80211AntennaInfo

The WTP-per-radio antenna configuration, defined in Section 6.2.

7.2. IEEE80211DSControl

The WTP-per-radio Direct Sequence Control configuration, defined in Section 6.5.

7.3. IEEE80211MACOperation

The WTP-per-radio MAC Operation configuration, defined in Section 6.7.

7.4. IEEE80211OFDMControl

The WTP-per-radio OFDM MAC Operation configuration, defined in Section 6.10.

7.5. IEEE80211Rateset

The WTP-per-radio Basic Rate Set configuration, defined in Section 6.11.

7.6. IEEE80211TxPower

The WTP-per-radio Transmit Power configuration, defined in Section 6.18.

7.7. IEEE80211QoS

The WTP-per-radio Quality of Service configuration, defined in Section 6.22.

7.8. IEEE80211RadioConfig

The WTP-per-radio Radio Configuration, defined in Section 6.23.

8. Technology Specific Message Element Values

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

8.1. WTP Descriptor Message Element, Encryption Capabilities Field

This specification defines two new bits for the WTP Descriptor's Encryption Capabilities field, as defined in [RFC5415]. Note that only the bits defined in this specification are described below. WEP is not explicitly advertised as a WTP capability since all WTPs are expected to support the encryption cipher. The format of the Encryption Capabilities field is:

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

A: WTP supports AES-CCMP, as defined in [IEEE.802-11.2007].

T: WTP supports TKIP and Michael, as defined in [IEEE.802-11.2007] and [WPA], respectively.

9. Security Considerations

This section describes security considerations for using IEEE 802.11 with the CAPWAP protocol. A complete threat analysis of the CAPWAP protocol can also be found in [RFC5418].

9.1. IEEE 802.11 Security

When used with an IEEE 802.11 infrastructure with WEP encryption, the CAPWAP protocol does not add any new vulnerabilities. Derived Session Keys between the STA and WTP can be compromised, resulting in many well-documented attacks. Implementers SHOULD discourage the use of WEP and encourage the use of technically-sound cryptographic solutions such as those in an IEEE 802.11 RSN.

STA authentication is performed using IEEE 802.lX, and consequently EAP. Implementers SHOULD use EAP methods meeting the requirements specified [RFC4017].

When used with IEEE 802.11 RSN security, the CAPWAP protocol may introduce new vulnerabilities, depending on whether the link security (packet encryption and integrity verification) is provided by the WTP or the AC. When the link security function is provided by the AC, no new security concerns are introduced.

However, when the WTP provides link security, a new vulnerability will exist when the following conditions are true:

- The client is not the first to associate to the WTP/ESSID (i.e., other clients are associated), a GTK already exists, and

- traffic has been broadcast under the existing GTK.

Under these circumstances, the receive sequence counter (KeyRSC) associated with the GTK is non-zero, but because the AC anchors the 4-way handshake with the client, the exact value of the KeyRSC is not known when the AC constructs the message containing the GTK. The client will update its Key RSC value to the current valid KeyRSC upon receipt of a valid multicast/broadcast message, but prior to this, previous multicast/broadcast traffic that was secured with the existing GTK may be replayed, and the client will accept this traffic as valid.

Typically, busy networks will produce numerous multicast or broadcast frames per second, so the window of opportunity with respect to such replay is expected to be very small. In most conditions, it is expected that replayed frames could be detected (and logged) by the WTP.

The only way to completely close this window is to provide the exact KeyRSC value in message 3 of the 4-way handshake; any other approach simply narrows the window to varying degrees. Given the low relative threat level this presents, the additional complexity introduced by providing the exact KeyRSC value is not warranted. That is, this specification provides for a calculated risk in this regard.

The AC SHOULD use an RSC of 0 when computing message-3 of the 4-way 802.11i handshake, unless the AC has knowledge of a more optimal RSC value to use. Mechanisms for determining a more optimal RSC value are outside the scope of this specification.

10. IANA Considerations

This section details the actions IANA has taken per this specification. There are numerous registries that have been be created, and the contents, document action (see [RFC5226], and registry format are all included below. Note that in cases where bit fields are referred to, the bit numbering is left to right, where the leftmost bit is labeled as bit zero (0).

10.1. CAPWAP Wireless Binding Identifier

This specification requires a value assigned from the Wireless Binding Identifier namespace, defined in [RFC5415]. (1) has been assigned (see Section 2.1, as it is used in implementations.

10.2. CAPWAP IEEE 802.11 Message Types

IANA created a new sub-registry in the existing CAPWAP Message Type registry, which is defined in [RFC5415].

IANA created and maintains the CAPWAP IEEE 802.11 Message Types sub-registry for all message types whose Enterprise Number is set to 13277. The namespace is 8 bits (3398912-3399167), where the value 3398912 is reserved and must not be assigned. The values 3398913 and 3398914 are allocated in this specification, and can be found in Section 3. Any new assignments of a CAPWAP IEEE 802.11 Message Type (whose Enterprise Number is set to 13277) require an Expert Review. The format of the registry maintained by IANA is as follows:

CAPWAP IEEE 802.11 Control Message	Message Type Value	Reference

10.3. CAPWAP Message Element Type

This specification defines new values to be registered to the existing CAPWAP Message Element Type registry, defined in [RFC5415]. The values used in this document, 1024 through 1048, as listed in Figure 8 are recommended as implementations already exist that make use of these values.

10.4. IEEE 802.11 Key Status

The Key Status field in the IEEE 802.11 Add WLAN message element (see Section 6.1) and IEEE 802.11 Update WLAN message element (see Section 6.21) is used to provide information about the status of the keying exchange. This document defines four values, zero (0) through three (3), and the remaining values (4-255) are controlled and maintained by IANA and requires an Expert Review.

10.5. IEEE 802.11 QoS

The QoS field in the IEEE 802.11 Add WLAN message element (see Section 6.1) is used to configure a QoS policy for the WLAN. The namespace is 8 bits (0-255), where the values zero (0) through three (3) are allocated in this specification, and can be found in Section 6.1. This namespace is managed by IANA and assignments require an Expert Review. IANA created the IEEE 802.11 QoS registry, whose format is:

IEEE 802.11 QoS	Type Value	Reference

10.6. IEEE 802.11 Auth Type

The Auth Type field in the IEEE 802.11 Add WLAN message element (see Section 6.1) is 8 bits and is used to configure the IEEE 802.11 authentication policy for the WLAN. The namespace is 8 bits (0-255), where the values zero (0) and one (1) are allocated in this specification, and can be found in Section 6.1. This namespace is managed by IANA and assignments require an Expert Review. IANA created the IEEE 802.11 Auth Type registry, whose format is:

IEEE 802.11 Auth Type	Type Value	Reference

10.7. IEEE 802.11 Antenna Combiner

The Combiner field in the IEEE 802.11 Antenna message element (see Section 6.2) is used to provide information about the WTP’s antennas. The namespace is 8 bits (0-255), where the values one (1) through four (4) are allocated in this specification, and can be found in Section 6.2. This namespace is managed by IANA and assignments require an Expert Review. IANA created the IEEE 802.11 Antenna Combiner registry, whose format is:

IEEE 802.11 Antenna Combiner	Type Value	Reference

10.8. IEEE 802.11 Antenna Selection

The Antenna Selection field in the IEEE 802.11 Antenna message element (see Section 6.2) is used to provide information about the WTP’s antennas. The namespace is 8 bits (0-255), where the values zero (0) is reserved and used and the values one (1) through two (2) are allocated in this specification, and can be found in Section 6.2. This namespace is managed by IANA and assignments require an Expert Review. IANA created the IEEE 802.11 Antenna Selection registry, whose format is:

IEEE 802.11 Antenna Selection	Type Value	Reference

10.9. IEEE 802.11 Session Key Flags

The flags field in the IEEE 802.11 Station Session Key message element (see Section 6.15) is 16 bits and is used to configure the session key association with the mobile device. This specification defines bits zero (0) and one (1), while bits two (2) through fifteen are reserved. The reserved bits are managed by IANA and assignment requires an Expert Review. IANA created the IEEE 802.11 Session Key Flags registry, whose format is:

IEEE 802.11 Station Session Key	Bit Position	Reference

10.10. IEEE 802.11 Tagging Policy

The Tagging Policy field in the IEEE 802.11 WTP Quality of Service message element (see Section 6.22) is 8 bits and is used to specify how the CAPWAP Data Channel packets are to be tagged. This specification defines bits three (3) through seven (7). The remaining bits are managed by IANA and assignment requires an Expert Review. IANA created the IEEE 802.11 Tagging Policy registry, whose format is:

IEEE 802.11 Tagging Policy	Bit Position	Reference

10.11. IEEE 802.11 WTP Radio Fail

The Type field in the IEEE 802.11 WTP Radio Fail Alarm Indication message element (see Section 6.24) is used to provide information on why a WTP’s radio has failed. The namespace is 8 bits (0-255), where the value zero (0) is reserved and unused, while the values one (1) and two (2) are allocated in this specification, and can be found in Section 6.24. This namespace is managed by IANA and assignments require an Expert Review. IANA created the IEEE 802.11 WTP Radio Fail registry, whose format is:

IEEE 802.11 WTP Radio Fail	Type Value	Reference

10.12. IEEE 802.11 WTP Radio Type

The Radio Type field in the IEEE 802.11 WTP Radio Information message element (see Section 6.25) is 8 bits and is used to provide information about the WTP's radio type. This specification defines bits four (4) through seven (7). The remaining bits are managed by IANA and assignment requires an Expert Review. IANA created the IEEE 802.11 WTP Radio Type registry, whose format is:

IEEE 802.11 WTP Radio Type	Bit Position	Reference

10.13. WTP Encryption Capabilities

The WTP Encryption Capabilities field in the WTP Descriptor message element (see Section 8.1) is 16 bits and is used by the WTP to indicate its IEEE 802.11 encryption capabilities. This specification defines bits 12 and 13. The reserved bits are managed by IANA and assignment requires an Expert Review. IANA created the IEEE 802.11 Encryption Capabilities registry, whose format is:

IEEE 802.11 Encryption Capabilities	Bit Position	Reference

11. Acknowledgments

The following individuals are acknowledged for their contributions to this binding specification: Puneet Agarwal, Charles Clancy, Pasi Eronen, Saravanan Govindan, Scott Kelly, Peter Nilsson, Bob O'Hara, David Perkins, Margaret Wasserman, and Yong Zhang.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[RFC3246] Davie, B., Charny, A., Bennet, J., Benson, K., Le Boudec, J., Courtney, W., Davari, S., Firoiu, V., and D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)", RFC 3246, March 2002.

[RFC3168]	Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.
[RFC3748]	Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.
[RFC5226]	Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.
[FIPS.197.2001]	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>.
[ISO.3166-1]	ISO Standard, "International Organization for Standardization, Codes for the representation of names of countries and their subdivisions - Part 1: Country codes", ISO Standard 3166-1:1997, 1997.
[IEEE.802-11.2007]	"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>.
[RFC5415]	Montemurro, M., Stanley, D., and P. Calhoun, "CAPWAP Protocol Specification", RFC 5415, March 2009.
[IEEE.802-1X.2004]	"Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Port-Based Network Access Control", IEEE Standard 802.1X, 2004, <http://standards.ieee.org/getieee802/download/802.1X-2004.pdf>.

[IEEE.802-1Q.2005]	"Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Virtual Bridged Local Area Networks", IEEE Standard 802.1Q, 2005, <http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf>.

12.2. Informative References

[RFC4017]	Stanley, D., Walker, J., and B. Aboba, "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs", RFC 4017, March 2005.
[RFC4118]	Yang, L., Zerfos, P., and E. Sadot, "Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)", RFC 4118, June 2005.
[RFC5418]	Kelly, S. and C. Clancy, "Control And Provisioning for Wireless Access Points (CAPWAP) Threat Analysis for IEEE 802.11 Deployments", RFC 5418, March 2009.
[WPA]	"Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise", March 2005, <www.wi-fi.org>.
[WMM]	"Support for Multimedia Applications with Quality of Service in WiFi Networks)", September 2004, <www.wi-fi.org>.

Editors’ Addresses

Pat R. Calhoun (editor)
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134

Phone: +1 408-902-3240
EMail: pcalhoun@cisco.com

Michael P. Montemurro (editor)
Research In Motion
5090 Commerce Blvd
Mississauga, ON L4W 5M4
Canada

Phone: +1 905-629-4746 x4999
EMail: mmontemurro@rim.com

Dorothy Stanley (editor)
Aruba Networks
1322 Crossman Ave
Sunnyvale, CA 94089

Phone: +1 630-363-1389
EMail: dstanley@arubanetworks.com