Internet Engineering Task Force (IETF)
Request for Comments: 7494
Category: Standards Track
ISSN: 2070-1721

C. Shao
H. Deng
China Mobile
R. Pazhyannur
Cisco Systems
F. Bari
AT&T
R. Zhang
China Telecom
S. Matsushima
SoftBank Telecom

April 2015

IEEE 802.11 Medium Access Control (MAC) Profile for Control and Provisioning of Wireless Access Points (CAPWAP)

Abstract

The Control and Provisioning of Wireless Access Points (CAPWAP) protocol binding for IEEE 802.11 defines two Medium Access Control (MAC) modes for IEEE 802.11 Wireless Transmission Points (WTPs): Split and Local MAC. In the Split MAC mode, the partitioning of encryption/decryption functions is not clearly defined. In the Split MAC mode description, IEEE 802.11 encryption is specified as located in either the Access Controller (AC) or the WTP, with no clear way for the AC to inform the WTP of where the encryption functionality should be located. This leads to interoperability issues, especially when the AC and WTP come from different vendors. To prevent interoperability issues, this specification defines an IEEE 802.11 MAC Profile message element in which each profile specifies an unambiguous division of encryption functionality between the WTP and AC.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

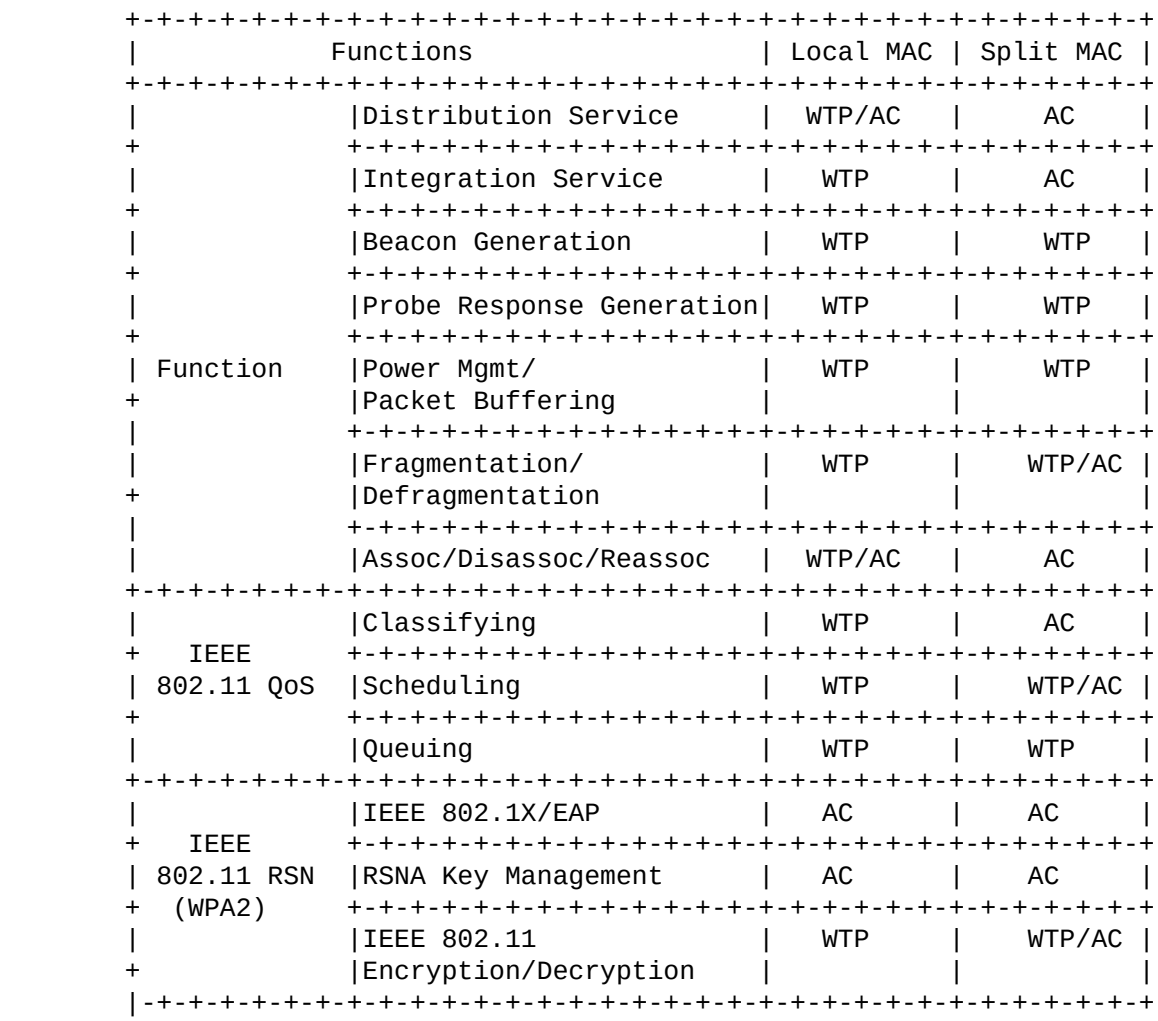
Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7494.

Table of Contents

1. Introduction

The CAPWAP protocol supports two MAC modes of operation: Split and Local MAC, as described in [RFC5415] and [RFC5416]. However, there are MAC functions that have not been clearly defined. For example, IEEE 802.11 [IEEE.802.11] encryption is specified as located in either the AC or the WTP with no clear way to negotiate where it should be located. Because different vendors have different definitions of the MAC mode, many MAC-layer functions are mapped differently to either the WTP or the AC by different vendors. Therefore, depending upon the vendor, the operators in their deployments have to perform different configurations based on implementation of the two modes by their vendor. If there is no clear specification, then operators will experience interoperability issues with WTPs and ACs from different vendors.

Figure 1 from [RFC5416] illustrates how some functions are processed in different places in the Local MAC and Split MAC mode. Specifically, note that in the Split MAC mode, the IEEE 802.11 encryption/decryption is specified as WTP/AC, implying that it could be at either location. This is not an issue with Local MAC because encryption is always at the WTP.



Note:
RSN - Robust Security Network
RSNA - Robust Security Network Association
WPA2 - Wi-Fi Protected Access 2

Figure 1: Functions in Local MAC and Split MAC

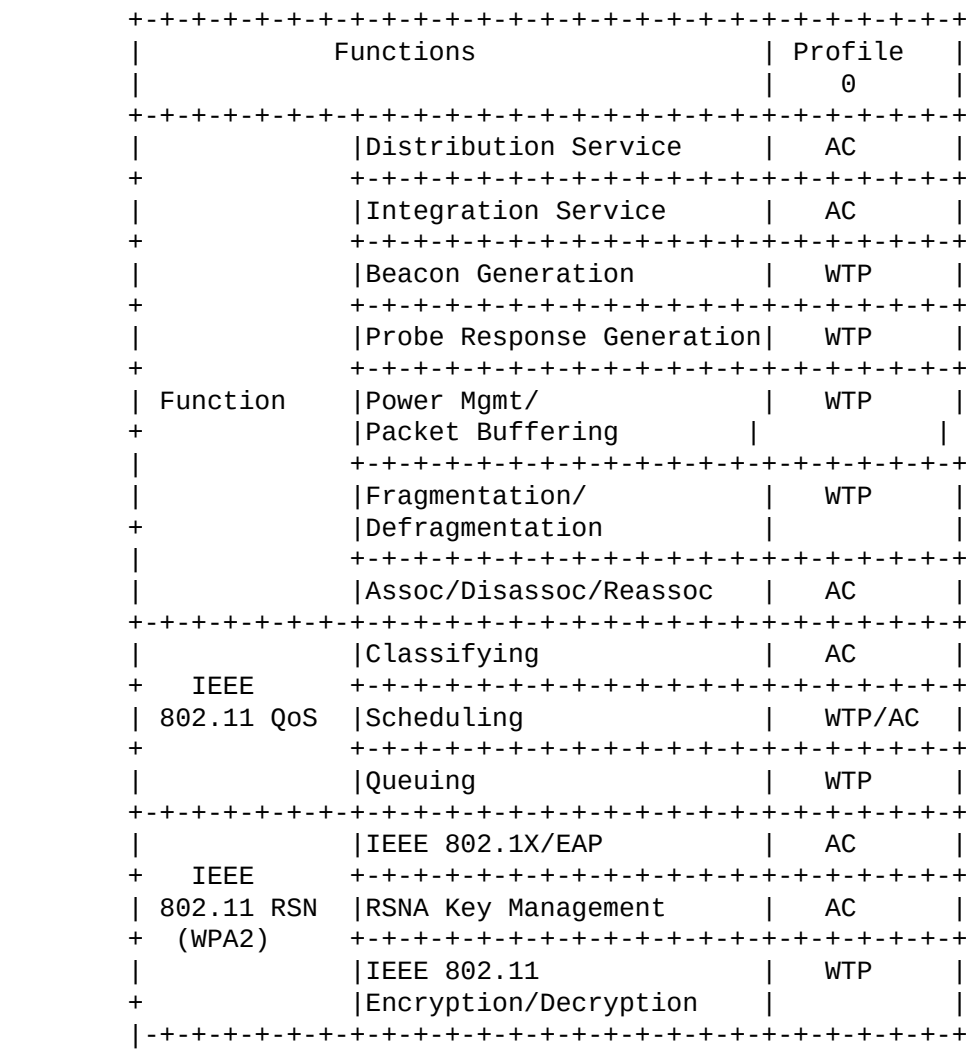
To solve this problem, this specification introduces the IEEE 802.11 MAC Profile. The IEEE 802.11 MAC Profile unambiguously specifies where the various MAC functionalities should be located.

2. IEEE MAC Profile Descriptions

A IEEE 802.11 MAC Profile refers to a description of how the MAC functionality is split between the WTP and AC shown in Figure 1.

2.1. Split MAC with WTP Encryption

The functional split for the Split MAC with WTP encryption is provided in Figure 2. This profile is similar to the Split MAC description in [RFC5416], except that IEEE 802.11 encryption/decryption is at the WTP. Note that fragmentation is always done at the same entity as the encryption. Consequently, in this profile fragmentation/defragmentation is also done only at the WTP. Note that scheduling functionality is denoted as WTP/AC. As explained in [RFC5416], this means that the admission control component of IEEE 802.11 resides on the AC; the real-time scheduling and queuing functions are on the WTP.



Note:
EAP - Extensible Authentication Protocol

Figure 2: Functions in Split MAC with WTP Encryption

2.2. Split MAC with AC Encryption

The functional split for the Split MAC with AC encryption is provided in Figure 3. This profile is similar to the Split MAC in [RFC5416], except that IEEE 802.11 encryption/decryption is at the AC. Since fragmentation is always done at the same entity as the encryption, in this profile, AC does fragmentation/defragmentation.

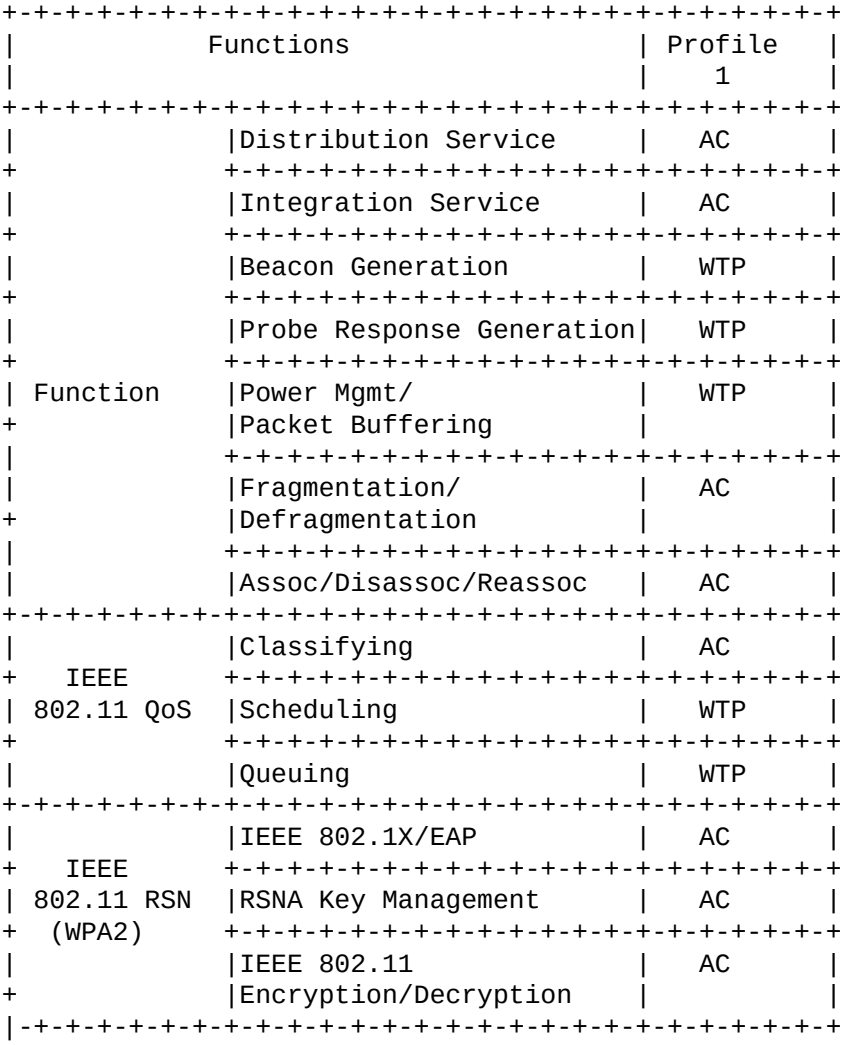


Figure 3: Functions in Split MAC with AC encryption

2.3. IEEE 802.11 MAC Profile Frame Exchange

An example of message exchange using the IEEE 802.11 MAC Profile message element is shown in Figure 4. The WTP informs the AC of the various MAC Profiles it supports. This happens in either a Discovery Request message or the Join Request message. The AC determines the appropriate profile and configures the WTP with the profile while configuring the WLAN.

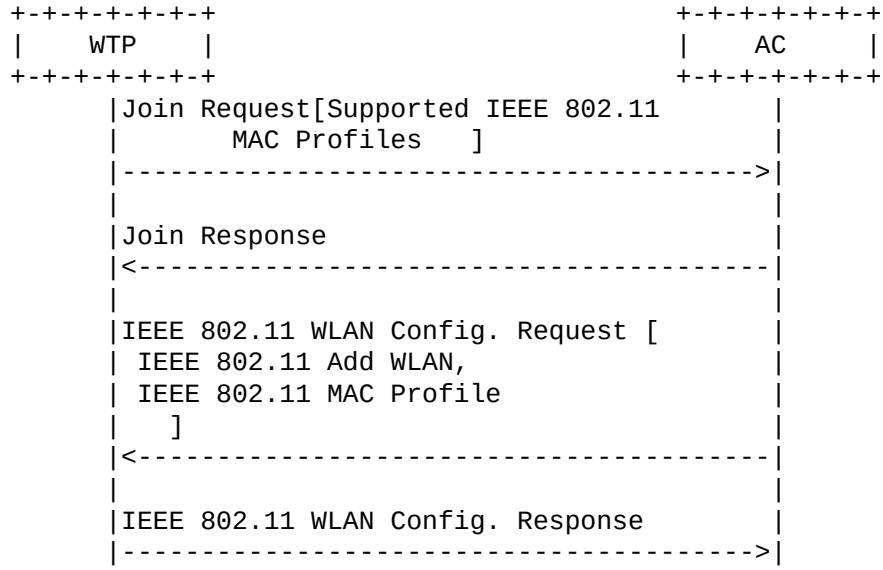


Figure 4: Message Exchange for Negotiating MAC Profiles

3. MAC Profile Message Element Definitions

3.1. IEEE 802.11 Supported MAC Profiles

The IEEE 802.11 Supported MAC Profile message element allows the WTP to communicate the profiles it supports. The Discovery Request message, Primary Discovery Request message, and Join Request message may include one such message element.

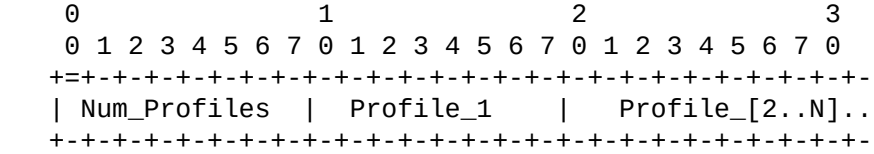


Figure 5: IEEE 802.11 Supported MAC Profiles

- Type: 1060 for IEEE 802.11 Supported MAC Profiles

- Num_Profiles >=1: This refers to the number of profiles present in this message element. There must be at least one profile.

- Profile: Each profile is identified by a value specified in Section 3.2.

3.2. IEEE 802.11 MAC Profile

The IEEE 802.11 MAC Profile message element allows the AC to select a profile. This message element may be provided along with the IEEE 802.11 ADD WLAN message element while configuring a WLAN on the WTP.

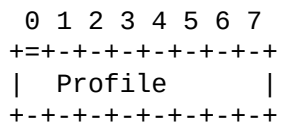


Figure 6: IEEE 802.11 MAC Profile

- Type: 1061 for IEEE 802.11 MAC Profile

- Profile: The profile is identified by a value as given below

  * 0: This refers to the IEEE 802.11 Split MAC Profile with WTP encryption

  * 1: This refers to the IEEE 802.11 Split MAC Profile with AC encryption

4. Security Considerations

This document does not introduce any new security risks compared to [RFC5416]. The negotiation messages between the WTP and AC have origin authentication and data integrity. As a result, an attacker cannot interfere with the messages to force a less-secure mode choice. The security considerations described in [RFC5416] apply here as well.

5. IANA Considerations

The following IANA actions have been completed.

- This specification defines two new message elements: IEEE 802.11 Supported MAC Profiles (described in Section 3.1) and the IEEE 802.11 MAC Profile (described in Section 3.2). These elements have been registered in the existing "CAPWAP Message Element Type" registry, defined in [RFC5415].

CAPWAP Protocol Message Element	Type Value
IEEE 802.11 Supported MAC Profiles	1060
IEEE 802.11 MAC Profile	1061

- The IEEE 802.11 Supported MAC Profiles message element and IEEE 802.11 MAC Profile message element include a Profile field (as defined in Section 3.2). The Profile field in the IEEE 802.11 Supported MAC Profiles denotes the MAC Profiles supported by the WTP. The Profile field in the IEEE 802.11 MAC Profile denotes the MAC Profile assigned to the WTP. The namespace for the field is 8 bits (0-255). This specification defines two values: zero (0) and one (1) as described below. The remaining values (2-255) are controlled and maintained by IANA, and the registration procedure is Expert Review [RFC5226]. IANA has created a new subregistry called "IEEE 802.11 Split MAC Profile" under the existing registry "Control And Provisioning of Wireless Access Points (CAPWAP) Parameters". The registry format is given below.

Profile	Type Value	Reference
Split MAC with WTP encryption	0	RFC 7494
Split MAC with AC encryption	1	RFC 7494

6. References

6.1. Normative References

[IEEE.802.11] IEEE, "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2012, March 2012, <http://standards.ieee.org/about/get/802/802.11.html>.

[RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, March 2009, <http://www.rfc-editor.org/info/rfc5415>.

[RFC5416] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11", RFC 5416, March 2009, <http://www.rfc-editor.org/info/rfc5416>.

6.2. Informative References

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

Acknowledgments

The authors are grateful for extremely valuable suggestions from Dorothy Stanley in developing this specification.

Guidance from the management team -- Melinda Shore, Scott Bradner, Chris Liljenstolpe, Benoit Claise, Joel Jaeggli, and Dan Romascanu -- is highly appreciated.

Contributors

Yifan Chen <chenyifan@chinamobile.com>

Naibao Zhou <zhounaibao@chinamobile.com>

Authors' Addresses

Chunju Shao
China Mobile
No.32 Xuanwumen West Street
Beijing 100053
China

EMail: shaochunju@chinamobile.com

Hui Deng
China Mobile
No.32 Xuanwumen West Street
Beijing 100053
China

EMail: denghui@chinamobile.com

Rajesh S. Pazhyannur
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134
United States

EMail: rpazhyan@cisco.com

Farooq Bari
AT&T
7277 164th Ave NE
Redmond, WA 98052
United States

EMail: farooq.bari@att.com

Rong Zhang
China Telecom
No.109 Zhongshandadao avenue
Guangzhou 510630
China

EMail: zhangr@gsta.com

Satoru Matsushima
SoftBank Telecom
1-9-1 Higashi-Shinbashi, Munato-ku
Tokyo
Japan

EMail: satoru.matsushima@g.softbank.co.jp