Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 18, 2014

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

February 14, 2014

IEEE 802.11 MAC Profile for CAPWAP
draft-ietf-opsawg-capwap-hybridmac-02

Abstract

CAPWAP defines two entities Wireless Transmission Point (WTP) and Access Controller (AC). CAPWAP also defines two MAC (Medium Access Control) modes for IEEE 802.11 WTPs: Split and Local MAC . For each MAC mode, CAPWAP describes how the MAC functionality is split between the WTP and AC. However, certain functions have not been clearly defined. For example for the Split MAC mode, the IEEE 802.11 encryption is specified as located in either the AC or the WTP with no clear way for the AC to inform the WTP where it should be. This lack of specification leads to interoperability especially when AC and WTP come from different vendors. To solve the problem, this specification defines a IEEE 802.11 MAC profile where each profile specifies an unambigous division of functionality between the WTP and AC. The IEEE 802.11 MAC profile is used as follows: The WTP informs the AC of the supported profiles during the discovery or join process and the AC configures the WTP with one of the supported profiles while configuring a WLAN.

time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 18, 2014.

Table of Contents

1. Introduction

The CAPWAP protocol supports two MAC modes of operation: Split and Local MAC, as described in [RFC5415], [RFC5416]. However, there are MAC functions that have not been clearly defined. For example IEEE 802.11 encryption is specified as located in either in the AC or the WTP with no clear way to negotiate where it should be located. Because different vendors have their own definition 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 difficulty in interoperating WTPs and ACs from different vendors.

Figure 1 quoted from [RFC5416], illustrates how the 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.

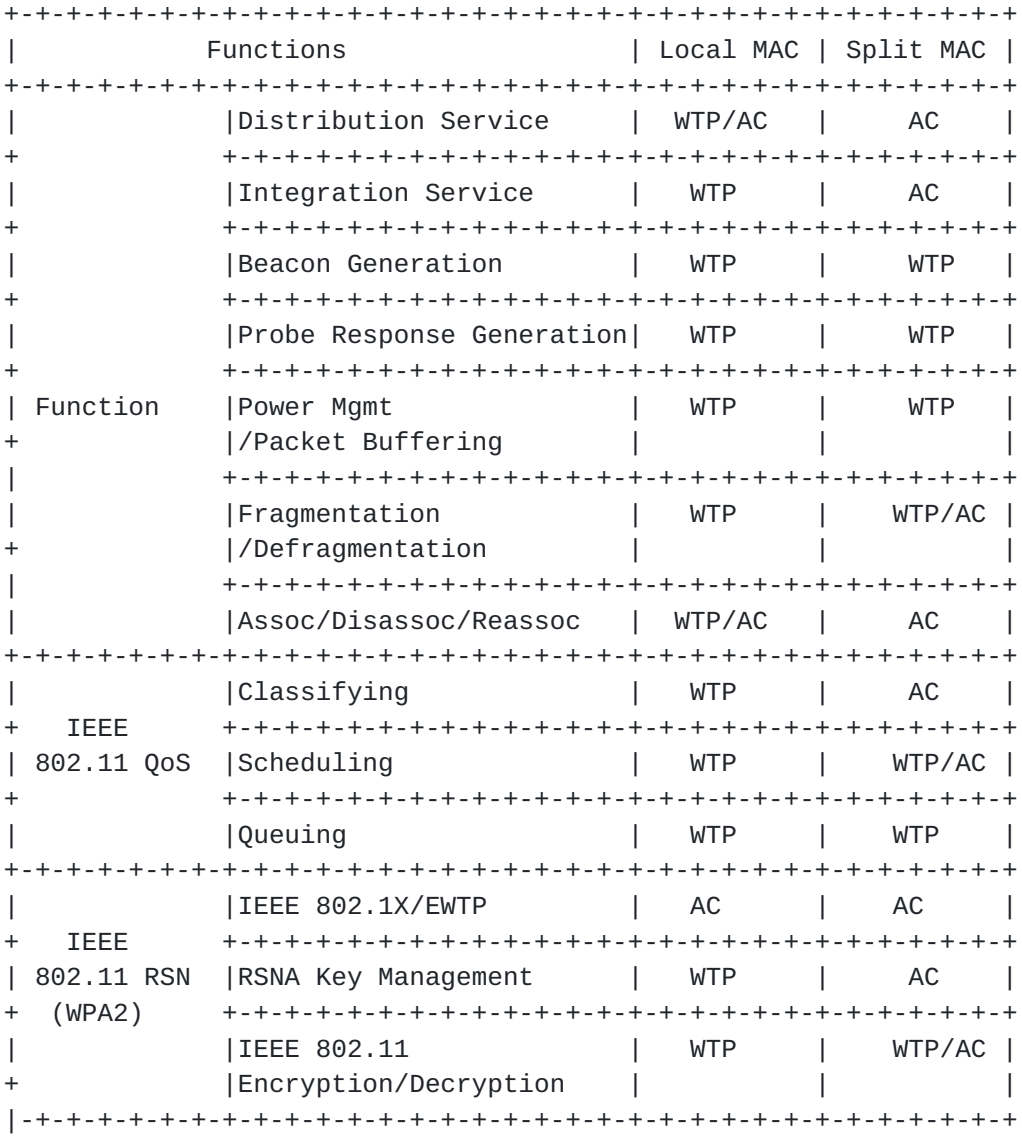

Figure 1: Functions in Local MAC and Split MAC

To solve this problem, this specification introduces IEEE 802.11 MAC profle. The MAC profile unamabigously specifies where the various MAC fucntionality should be located.

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 [RFC2119].

3. IEEE MAC Profile Descriptions

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

3.1. 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 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.

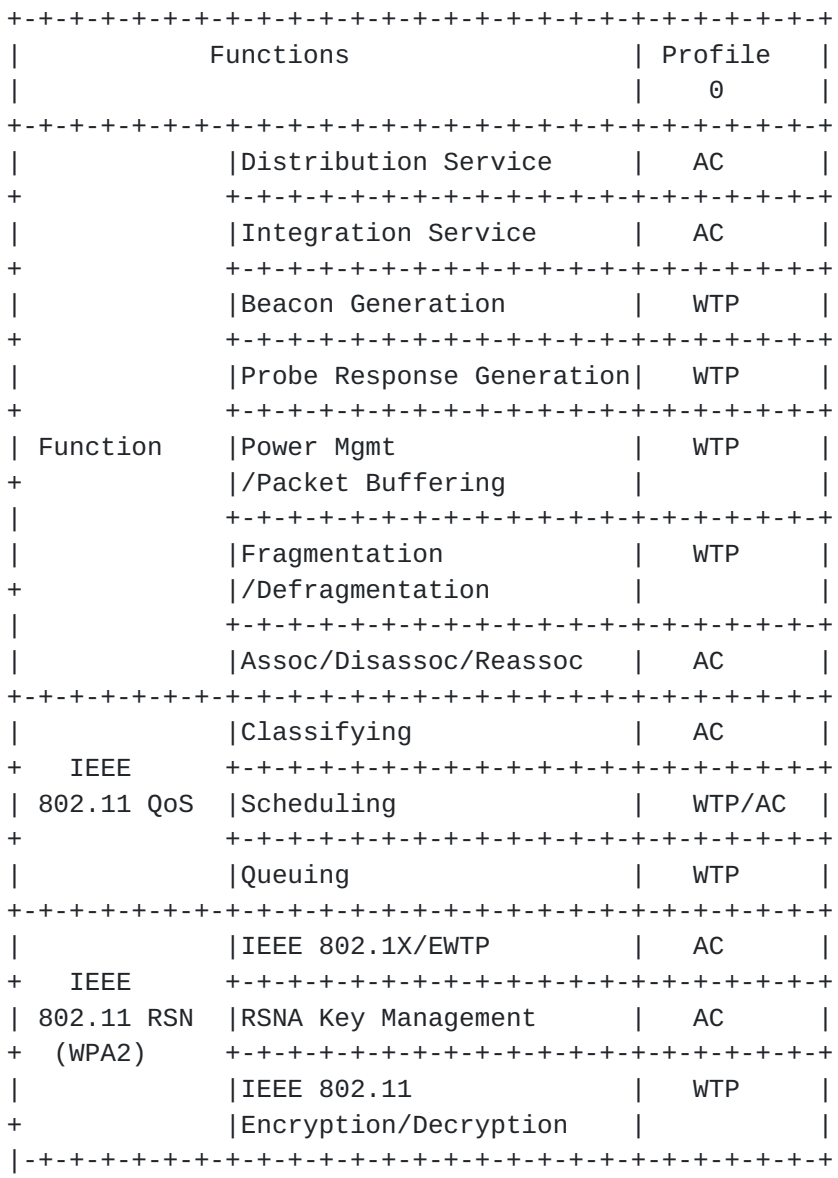

Figure 2: Functions in Split MAC with WTP Encryption

3.2. 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 except that IEEE 802.11 encryption/decryption is done only at the AC. Since fragmentation is always done at the same entity as the encryption, in this rofile, AC does fragmentation/defragmentation.

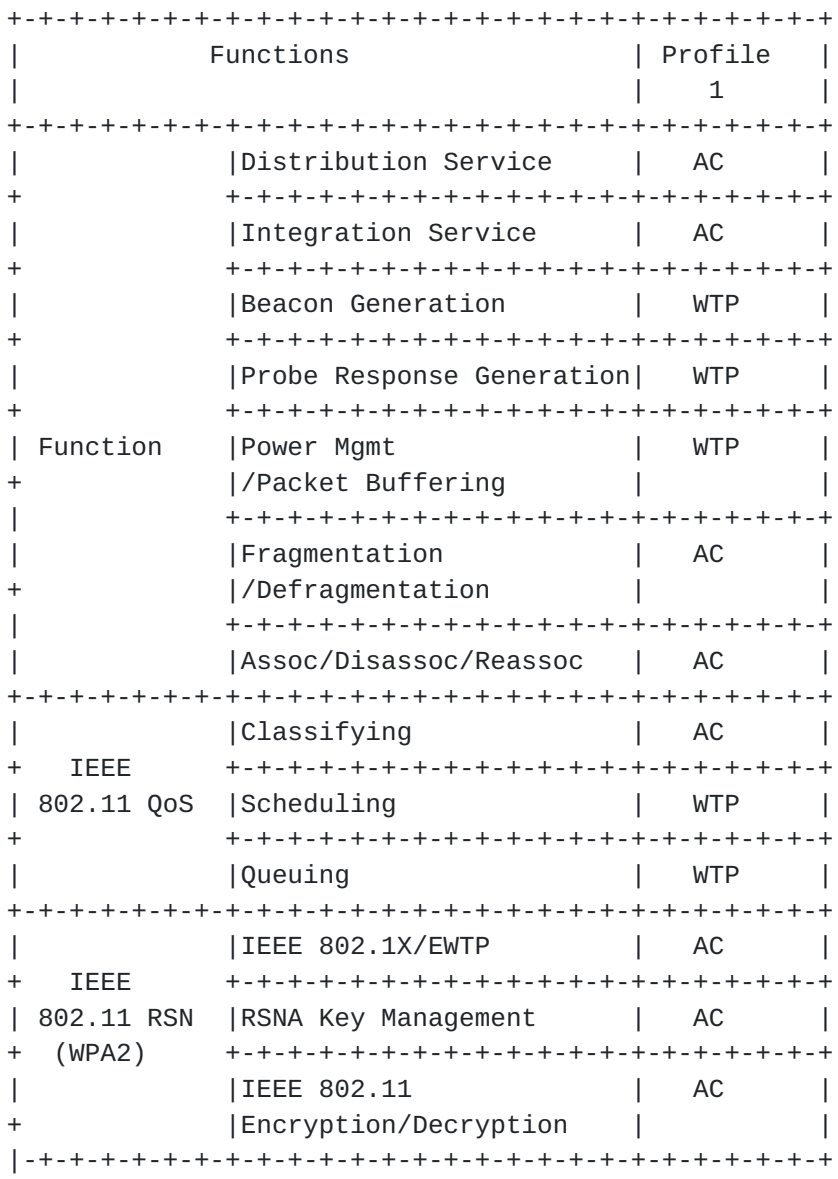

Figure 3: Functions in Split MAC with AC encryption

3.3. IEEE 802.11 MAC Profile Frame Exchange

An example of message exchange using the 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 either in a Discovery Request message or the Join Request message. The AC determines the appropriate profile and the configures the WTP with the profile while configuring the WLAN.

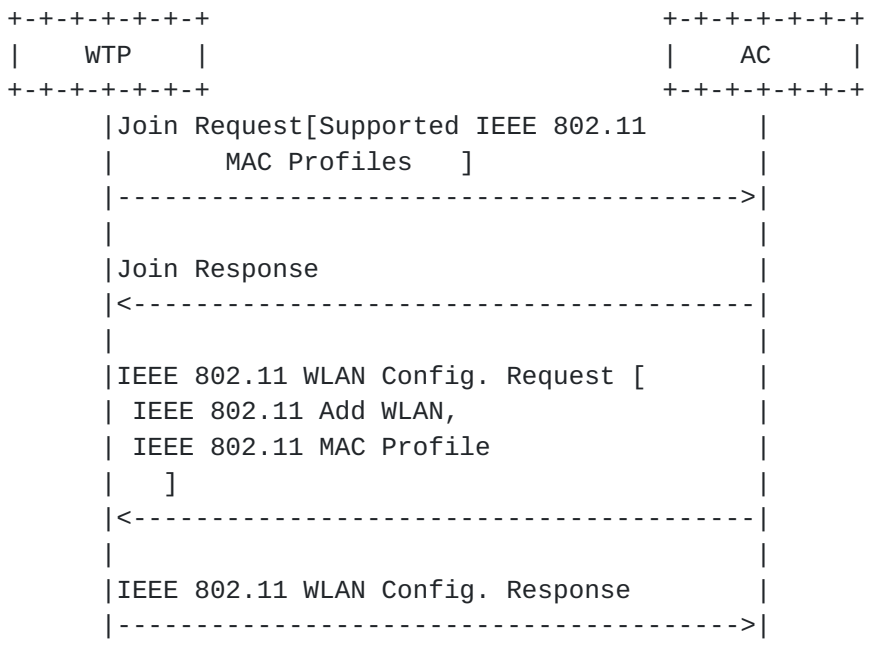

Figure 4: Message Exchange For Negotiating MAC Profile

4. MAC Profile Message Element Definitions

4.1. 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.

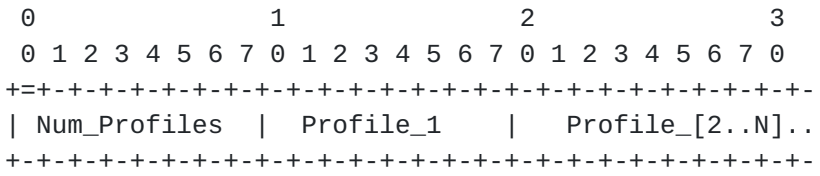

Figure 5: IEEE 802.11 Supported MAC Profiles

- Type: TBD for IEEE 802.11 Supported MAC Profiles
- Num_Profiles >=1: This refers to number of profiles present in this messaage element. There must be at least one profile.
- Profile: Each profile is idnentified by a value specified in Section 4.2.

4.2. IEEE 802.11 MAC Profile

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

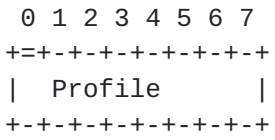

Figure 6: IEEE 802.11 MAC Profile

- Type: TBD for IEEE 802.11 MAC Profile
- Profile: The profile is identified by a value as given below

  - 0: This refers to the Split MAC Profile with WTP encryption
  - 1: This refers to the Split MAC Profile with AC encryption

5. Security Considerations

This document doesn't specify security risk difference from [RFC5416]. Please refer to the Security section of [RFC5416]

6. IANA Considerations

This document requires the following IANA actions.

- This specification defines a new message element, IEEE 802.11 Supported MAC Profiles. The format of this option is described in Section 4.1. This value needs to be regsitered in the existing CAPWAP Message Element Type registry, defined in [RFC5415].
- This specification defines a new message element, IEEE 802.11 MAC Profile. The format of this option is described in Section 4.2. This value needs to be regsitered in the existing CAPWAP Message Element Type registry, defined in [RFC5415].
- The Profile field in the IEEE 802.11 Supported MAC Profiles message element and IEEE 802.11 MAC Profile message element (see Section 4.2) is used to denote the MAC profile. This document defines two values, zero (0) and one (1), and the remaining values (2-255) are controlled and maintained by IANA and require an Expert Review.

7. Contributors

Yifan Chen chenyifan@chinamobile.com

Naibao Zhou zhounaibao@chinamobile.com

8. Acknowledgments

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

Guidance from management team: Melinda Shore, Scott Bradner, Chris Liljenstolpe, Benoit Claise, Joel Jaeggli, Dan Romascanu are highly appreciated.

9. Normative References

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

[RFC4564] Govindan, S., Cheng, H., Yao, ZH., Zhou, WH., and L. Yang, "Objectives for Control and Provisioning of Wireless Access Points (CAPWAP)", RFC 4564, July 2006.

[RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, March 2009.

[RFC5416] Calhoun, P., Montemurro, M., and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11", RFC 5416, March 2009.

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
170 West Tasman Drive
San Jose, CA 95134
USA

Email: rpazhyan@cisco.com

Farooq Bari
AT&T
7277 164th Ave NE
Redmond WA 98052
USA

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