Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: June 21, 2015

C. Shao
H. Deng
China Mobile
R. Pazhyannur
Cisco Systems
F. Bari
AT&T
R. Zhang
China Telecom
S. Matsushima
SoftBank Telecom
December 18, 2014

IEEE 802.11 MAC Profile for CAPWAP
draft-ietf-opsawg-capwap-hybridmac-08

Abstract

The CAPWAP protocol binding for IEEE 802.11 defines two MAC (Medium Access Control) modes for IEEE 802.11 WTP (Wireless Transmission Point): Split and Local MAC. In the Split MAC mode, the partitioning of encryption/decryption functions are not clearly defined. In the Split MAC mode description, IEEE 802.11 encryption is specified as located in either the AC (Access Controller) 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 Internet-Draft will expire on June 21, 2015.

Copyright Notice

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 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.

Functions		Local MAC	Split MAC
Function	Distribution Service	WTP/AC	AC
	Integration Service	WTP	AC
	Beacon Generation	WTP	WTP
	Probe Response Generation	WTP	WTP
	Power Mgmt /Packet Buffering	WTP	WTP
	Fragmentation /Defragmentation	WTP	WTP/AC
	Assoc/Disassoc/Reassoc	WTP/AC	AC
IEEE 802.11 QoS	Classifying	WTP	AC
	Scheduling	WTP	WTP/AC
	Queuing	WTP	WTP
IEEE 802.11 RSN (WPA2)	IEEE 802.1X/EAP	AC	AC
	RSNA Key Management	AC	AC
	IEEE 802.11 Encryption/Decryption	WTP	WTP/AC

Figure 1: Functions in Local MAC and Split MAC

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

2. 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.

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.

Functions		Profile 0
Function	Distribution Service	AC
	Integration Service	AC
	Beacon Generation	WTP
	Probe Response Generation	WTP
	Power Mgmt /Packet Buffering	WTP
	Fragmentation /Defragmentation	WTP
	Assoc/Disassoc/Reassoc	AC
IEEE 802.11 QoS	Classifying	AC
	Scheduling	WTP/AC
	Queuing	WTP
IEEE 802.11 RSN (WPA2)	IEEE 802.1X/EAP	AC
	RSNA Key Management	AC
	IEEE 802.11 Encryption/Decryption	WTP

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.

```
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |            Functions                 | Profile   |
   |                                      |    1      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             |Distribution Service    |   AC      |
   +             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             |Integration Service     |   AC      |
   +             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             |Beacon Generation       |   WTP     |
   +             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             |Probe Response Generation|  WTP     |
   +             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Function    |Power Mgmt              |   WTP     |
   +             |/Packet Buffering       |           |
   |             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             |Fragmentation           |   AC      |
   +             |/Defragmentation        |           |
   |             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             |Assoc/Disassoc/Reassoc  |   AC      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             |Classifying             |   AC      |
   +   IEEE      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | 802.11 QoS  |Scheduling              |   WTP     |
   +             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             |Queuing                 |   WTP     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             |IEEE 802.1X/EAP        |   AC      |
   +   IEEE      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | 802.11 RSN  |RSNA Key Management     |   AC      |
   +  (WPA2)     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             |IEEE 802.11             |   AC      |
   +             |Encryption/Decryption   |           |
   |-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 either in 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.

```
       +-+-+-+-+-+-+                             +-+-+-+-+-+-+
       |    WTP    |                             |    AC     |
       +-+-+-+-+-+-+                             +-+-+-+-+-+-+
             |Join Request[Supported IEEE 802.11       |
             |       MAC Profiles   ]                  |
             |---------------------------------------->|
             |                                         |
             |Join Response                            |
             |<----------------------------------------|
             |                                         |
             |IEEE 802.11 WLAN Config. Request [       |
             | IEEE 802.11 Add WLAN,                   |
             | IEEE 802.11 MAC Profile                 |
             |   ]                                     |
             |<----------------------------------------|
             |                                         |
             |IEEE 802.11 WLAN Config. Response        |
             |---------------------------------------->|
```

Figure 4: Message Exchange For Negotiating MAC Profile

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.

```
           0               1               2               3
           0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0
          +=+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
          | Num_Profiles  |  Profile_1    |   Profile_[2..N]..
          +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Figure 5: IEEE 802.11 Supported MAC Profiles

- o Type: TBD for IEEE 802.11 Supported MAC Profiles
- o Num_Profiles >=1: This refers to number of profiles present in this message element. There must be at least one profile.
- o 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.

```
 0 1 2 3 4 5 6 7
+=+-+-+-+-+-+-+-+
|  Profile      |
+-+-+-+-+-+-+-+-+
```

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

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

This document requires the following IANA actions:

- This specification defines two new message elements, IEEE 802.11 Supported MAC Profiles (described in Section 3.1) and IEEE 802.11 MAC Profile (described in Section 3.2). These elements needs to be registered in the existing CAPWAP Message Element Type registry, defined in [RFC5415]. The values for these elements needs to be between 1024 and 2047 (see Section 15.7 in [RFC5415]).

CAPWAP Protocol Message Element	Type Value
IEEE 802.11 Supported MAC Profiles	TBD1
IEEE 802.11 MAC Profile	TBD2

- 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 MAC profile denotes 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 require an Expert Review. IANA needs to create a new sub-registry called IEEE 802.11 Split MAC Profile and add the new sub-registry to 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	
Split MAC with AC encryption	1	

6. Contributors

Yifan Chen chenyifan@chinamobile.com

Naibao Zhou zhounaibao@chinamobile.com

7. 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.

8. Normative References

[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 Systems
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