

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: April 25, 2013

CJ. Shao  
H. Deng  
China Mobile  
R. Zhang  
China Telecom  
F. Bari  
AT&T Services  
October 22, 2012

Enhancement of CAPWAP Problem Statement  
draft-shao-capwap-plus-ps-01

Abstract

In recent widescale deployments of large public Wi-Fi networks, and in their integration with cellular networks EAP based authentication has been considered as a good candidate to making Wi-Fi user experience seamless similar to what it has been for cellular users. A few new functions which could enhance CAPWAP protocol have been identified in such deployments that can help improve the large scale carrier grade Wi-Fi networks.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any 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 April 25, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

- 1. Introduction . . . . . 3
- 2. Conventions used in this document . . . . . 3
- 3. Supporting EAP authentication in Wi-Fi network . . . . . 3
  - 3.1. Scenario Description . . . . . 3
- 4. The Scope of Split and Local MAC mode . . . . . 4
- 5. 802.11n support . . . . . 4
- 6. Channel auto reconfiguration . . . . . 5
- 7. Power auto reconfiguration . . . . . 6
- 8. Security Considerations . . . . . 6
- 9. IANA Considerations . . . . . 6
- 10. Contributors . . . . . 6
- 11. Normative References . . . . . 6
- Authors' Addresses . . . . . 7

## 1. Introduction

Mobile devices such as smartphones and tablets continue to lead growth in internet traffic. It is predicted that such growth will continue even with the deployment of LTE network. Almost all mobile devices today are Wi-Fi enabled. Public Wi-Fi services have lately been paid more attention for that reason to help bring this growth of cellular data traffic to a sustainable level. Wi-Fi spectrum is free and globally available. Because of capacity and coverage issues, LTE networks will continue to need public Wi-Fi network as a complementary technology.

Recently industry efforts have been made to make Wi-Fi roaming as seamless as it is for cellular GSM networks by deploying EAP based authentication mechanism; Toward this end current CAPWAP protocol could be enhanced to help ease such deployments.

There have been a number of proprietary implementations of the interface between Access Point (AP) and Access Controller (AC) and some of them provide capabilities which could be used to improve the Wi-Fi performance. Once a standard interface is specified, the benefits for operators of standards based deployment will outweigh any benefits of past proprietary solutions.

## 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. Supporting EAP authentication in Wi-Fi network

Current EAP message is designed to be transmitted in CAPWAP data Plane. AC which is in the data path will act as the authenticator to transmit this EAP message to AAA server. An operator may however prefer to bypass the AC for the user plane in order to improve the performance of AC and allow it to manage more APs when the network is growing. In order to allow ACs to be bypassed for EAP messages, the CAPWAP control message could be extended to support EAP messages.

### 3.1. Scenario Description

The following figure shows where and how the problem arises. In many operators networks. The Access Controller is placed remotely at the central data center. In order to avoid the traffic aggregation at the AC, the data plane out of the AP is directed to the Access Router

(AR). In this scenario, the CAPWAP-CTL tunnel and CAPWAP-DATA tunnel are separated from each other.

Because there are no explicit message types to support the encapsulation of EAP packets in the CAPWAP-CTL tunnel, the EAP messages are tunneled via the CAPWAP-DATA plane to the AR. AR acts as authenticator in the EAP framework. After authentication, the AR receives the keying message for the session. But AC is supposed to deliver these keying messages to the AP, and AR has no standard interface to ship them to the AP or the AC. This is unacceptable in the scenario of EAP-based auto-authentication.

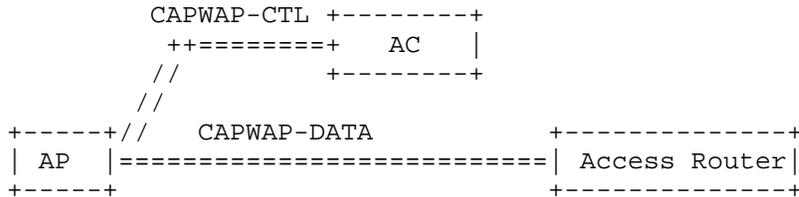


Figure 1: Split between CAPWAP-CTL and CAPWAP-DATA Plane

So it is desirable to encapsulate EAP messages in the CAPWAP-CTL plane, to avoid data aggregation and improve WLAN system scalability.

4. The Scope of Split and Local MAC mode

There are 3 major categories has been specified by CAPWAP, the first is about Functions: such as "Distribution Service", "Integration Service", "Beacon Generation", "Probe Response Generation" "Power Mgmt/Packet Buffering", "Fragmentation/Defragmentation", and "Assoc/Disassoc/Reassoc"; the second is about QoS, such as, "Classifying", "Scheduling", and "Queuing"; the third is about RSN (WPA2) such as "IEEE 802.1X/EAP", "RSNA Key Management", and "IEEE 802.11 Encryption/Decryption". Even Split and Local MAC model has optional implementation, either at AP or AC, this lead to serious issue about Interoperation

Proposing a specific mode about all this implementation will help interoperation among different vendors.

5. 802.11n support

There are a couple of capabilities of 802.11n that need to be supported by CAPWAP control message such as radio capability, radio configuration and station information.

IEEE 802.11n standard was published in 2009 and it is an amendment to the IEEE 802.11-2007 standard to improve network throughput. The maximum data rate increases to 600Mbit/s physical throughput rate. In the physical layer, 802.11n use OFDM and MIMO to achieve the high throughput. 802.11n use multiple antennas to form antenna array which can be dynamically adjusted to improve the signal strength and extend the coverage.

802.11n support two modes of channel usage: 20MHz mode and 40MHz mode. 802.11n has a new feature called channel binding. It can bind two adjacent 20MHz channel to one 40MHz channel to improve the throughput. If using 40MHz channel configuration there will be only one non-overlapping channel in 2.4GHz. In the large scale deployment scenario, operator need to use 20MHz channel configuration in 2.4GHz to allow more non-overlapping channels.

In MAC layer, a new feature of 802.11n is Short Guard Interval(GI). 802.11a/g use 800ns guard interval between the adjacent information symbols. In 802.11n, the GI can be configured to 400nm under good wireless condition.

Another feature in 802.11 MAC layer is Block ACK. 802.11n can use one ACK frame to acknowledge several MPDU receiving event.

CAPWAP need to be extended to support the above new 802.11n features. For example, CAPWAP should allow the access controller to know the supported 802.11n features and the access controller should be able to configure the different channel binding modes. One possible solution is to extend the CAPWAP information element for 802.11n.

## 6. Channel auto reconfiguration

Channel auto reconfiguration could improve the Wi-Fi performance, CAPWAP message could be extended to support this function.

Each channel may provide different quality of service, when WTP works. WTP can be active or passive scanning and monitoring each channel, form the report of measurement results to the Access Controller. WTP can periodically send configure status request to the AC. According to the current channel quality and other channel quality scanning report, ACs decide whether modify the channel to be used, send the configure status response packet to set up a new channel for the WTP.

## 7. Power auto reconfiguration

Power auto reconfiguration could improve the Wi-Fi performance. CAPWAP message could be extended to achieve following outcome.

- o Maximize Spectrum Usage: Real-world Wi-Fi deployments are depending on the features of shared media. Three channels available in the 2.4GHz band and 23 channels in the 5GHz band. Power auto reconfiguration could help these channels be fully utilized. As the results, clients could be distributed across all available channels.
- o Reduce Interference: when multiple devices attempt to simultaneously access the same channel at the same time, a co-channel interference likely happned. It reduces overall performance of the channel. The reconfiguration via CAPWAP could efficiently mitigate the interference. That is essential to proper network operation
- o Optimize Coverage: Simply increasing AP power may not help to maximize converage because it creates an unbalanced condition in which more distantly located clients may perform poorly due to their lower transmit output power. The power reconfiguration could achieve a balanced environment, where configuration could ensure that coverage is uniform and adequate throughout the service area.

## 8. Security Considerations

BD

## 9. IANA Considerations

None

## 10. Contributors

Yifan Chen cheniyifan@chinamobile.com

Bocun Deng 13316090701@189.cn

Satoru Matsushima satoru.matsushima@tm.softbank.co.jp

## 11. 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.

#### Authors' Addresses

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

Email: [shaochunju@chinamobile.com](mailto:shaochunju@chinamobile.com)

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

Email: [denghui@chinamobile.com](mailto:denghui@chinamobile.com)

Rong Zhang  
China Telecom  
No.109 Zhongshandadao avenue  
Tianhe District,  
Guangzhou 510630  
China

Email: [zhangr@gsta.com](mailto:zhangr@gsta.com)

Farooq Bari  
AT&T Services  
7277 164th Avenue NE  
Redmond  
US

Email: farooq.bari@att.com

