Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 24, 2014

L. Xue
Z. Du
Huawei
D. Liu
China Mobile
R. Zhang
China Telecom
John. Kaippallimalil
Huawei

October 21, 2013

Capability Announcement and AR Discovery in CAPWAP Control and Data Channel Separation
draft-xue-opsawg-capwap-separation-capability-01

Abstract

In centralized IEEE 802.11 Wireless Local Area Network (WLAN) architecture, the Access Controller (AC) isn't intelligent enough actually to aggregate all the wireless frames, even the bandwidth requirement in the access point is increasing. Thus it is a general case in the existing operator's network that WTPs forward the wireless frames directly to Access Router (AR) to avoid overload on the AC. In this scenario, CAPWAP Control Channel and CAPWAP Data Channel are separated from each other. This document extends CAPWAP for applicability of CAPWAP Control and Data Channel separation.

Requirements Language

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].

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 24, 2014.

Table of Contents

1. Introduction 2
2. Split CAPWAP-CTL and CAPWAP-DATA Establishment 3
2.1. AR Discovery 3
2.2. Split Mode Capability Announcement 4
3. CAPWAP Message Elements for Split Mode 4
4. IANA Considerations 6
5. Security Considerations 6
6. References 6
6.1. Normative References 6
6.2. Informative References 7
Authors' Addresses 7

1. Introduction

In centralized IEEE 802.11 Wireless Local Area Network (WLAN) architecture, Control and Provisioning of Wireless Access Points (CAPWAP) protocol is defined to enable Access Controller (AC) to manage a collection of Wireless Termination Points (WTPs), specified in [RFC5415] and [RFC5416]. In the existing specifications, CAPWAP Control Channel and Data Channel are setup and managed as a converged procedure between a WTP and AC. CAPWAP Control messages are exchanged for management between a WTP and AC; meanwhile, CAPWAP data messages encapsulate forwarded wireless frames from/to WTP.

Actually, it is a general case in the existing operator's network that WTPs forward the wireless frames directly to Access Router (AR) to avoid overload on the AC. AC isn't intelligent enough to aggregate all the wireless frames, even the bandwidth requirement in the access point is increasing continually. In this scenario, CAPWAP

Control Channel and CAPWAP Data Channel should be separated from each other, shown in the following figure.

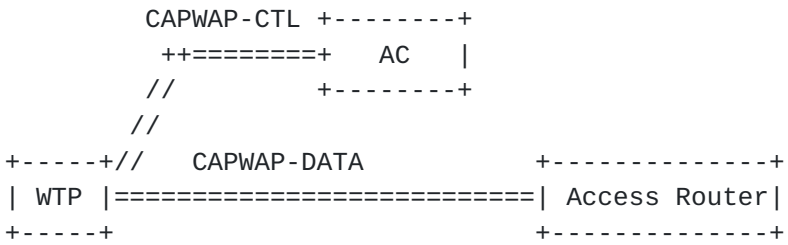


Figure 1: Split CAPWAP Control and CAPWAP DATA Channel

However, up to now, there is only one entire procedure for both CAPWAP Control Channel and CAPWAP Data Channel setup [RFC5415] between a WTP and AC. It is not suitable if CAPWAP Control Channel and CAPWAP Data Channel split. This document extends CAPWAP for applicability of CAPWAP Control Channel and CAPWAP Data Channel seperation.

2. Split CAPWAP-CTL and CAPWAP-DATA Establishment

This section describes the session establishment process for CAPWAP Control Channel and CAPWAP Data Channel seperation, named as CAPWAP Split Mode. In this architecture, the CAPWAP protocol should concern with not only interface between the WTP and the AC, but also the interface between the WTP and the AR.

On the bases of the existing CAPWAP procedure [RFC5415], additional phases should be considered, specified in following sub sections.

2.1. AR Discovery

In CAPWAP Split Mode, AR discovery should be the Preliminary phase for CAPWAP Data Channel. The WTPs MUST obtain the AR information, such as IP address which to establish the CAPWAP Data Channel. The AR information may be configured manually on the WTPs.

However, it is difficult to operate when there are large numbers of WTPs in the network. Auto-configuration method is required to enable AR discovery. Several dynamic methods such as DHCP or DNS could be useful, but this document does not discuss these methods in detail. Actually, AR Discovery can be completed in the process of CAPWAP Control Channel procedure defined in [RFC5415].

It's known that AC and AR are deployed centralized in operators' network. Always, AC can acquire AR information in the network via manual configuration. After the Discovery Response messages

received[RFC5415], a WTP can select an AC with which to establish a secure DTLS session for CAPWAP Control Channel. Then AC configures the WTP with AR address appropriately via Configuration Status Response. When a WTP receives the Configuration Status Response message carrying AR address, it checks and restores the AR address for CAPWAP Data Channel.

In order to support AR discovery on a WTP, a new CAPWAP message element, the AR Information Element is defined in section 3.

Additionally, the AR discovery process may also support load-sharing and recovery from a single AR point of failure.

2.2. Split Mode Capability Announcement

In order to support CAPWAP Split Mode, the split mode capability MUST be announced with agreement between a WTP and AC. Otherwise, the CAPWAP Data messages will be sent to AC instead of AR, which violates the split mode .

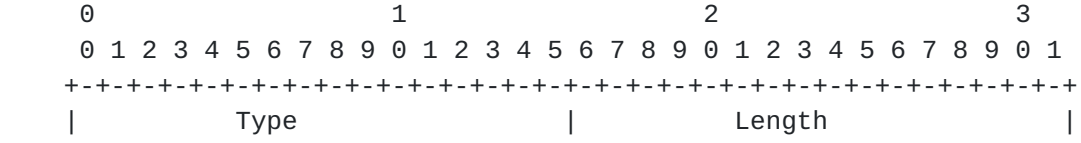
The CAPWAP Split Capability announcement can be achieved during Join Operations [RFC5415]between a WTP and AC. A new CAPWAP message element, the CAPWAP Mode Element is included in the Join Request message and Join Response message between WTP and AC in order to negotiate about the CAPWAP Mode. The element format is defined in Section 3.

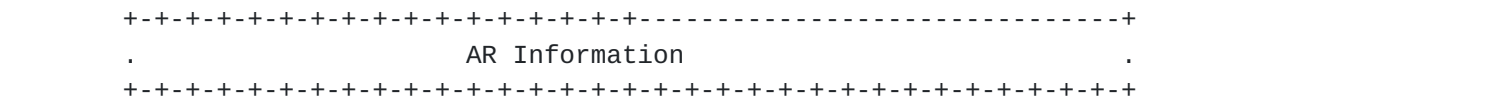
Besides, the decision about the CAPWAP mode between a WTP and AC can be made based on operator's requirements. For example, if the CAPWAP Mode Element included in either Join Request message or Join Response message, or both is set as Split Mode value, the CAPWAP will work in Split mode. Or, the agreement is consistent the value of CAPWAP Mode element carried in Join Request messages send by WTP. In this document, the methods to arrive decision agreement about the CAPWAP mode between a WTP and AC are not mandatory.

3. CAPWAP Message Elements for Split Mode

As aforementioned, two new CAPWAP message elements are defined in this section for CAPWAP Split Mode.

The AR Information Element is used by the AC to configure the AR information to WTP. The format is shown as follows.



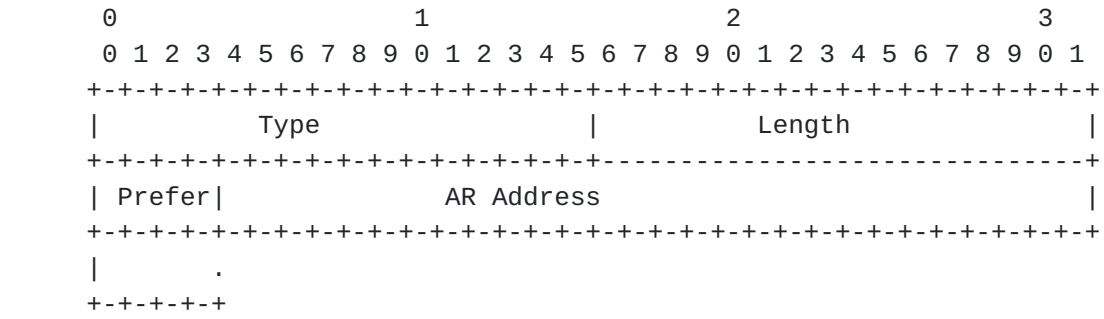


AR Information Element

Type: TBD

Length: >=8

AR Information: The IP address of AR served for WTP in the network. In order to support load-sharing and recovery from a single AR point of failure. The AR information can be formatted via TLV for sub-elements, the sub-element format is:



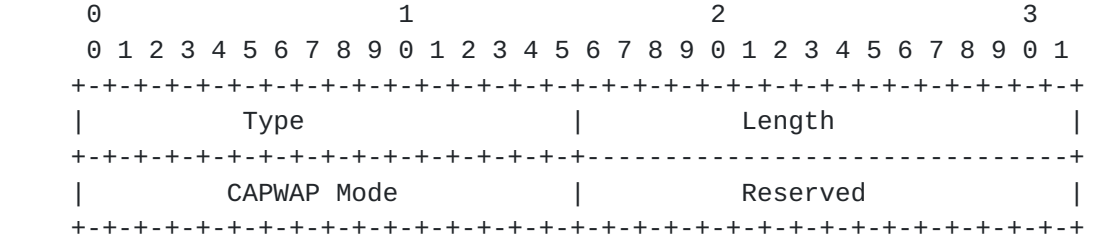
Load-sharing AR Information sub-element

Type: 1

Length; >= 9

AR Address: the IP address of AR served for WTP in the network.

The CAPWAP Mode element is used for the split mode capability which MUST be announced with agreement between a WTP and AC. The format is shown as follows.



CAPWAP Mode Element

Type: TBD

Length: 8

CAPWAP Mode: If the value is 0, the CAPWAP mode is converged defined in [RFC5415]. If the value is 1, the CAPWAP mode is split mode, defined in this document.

Reserved: It can be used by operators to define the rule for making CAPWAP mode decision.

4. IANA Considerations

This document defines two CAPWAP elements used in CAPWAP Split Mode. IANA is requested to allocate the following type.

- The type for AR Information Element
- The type for CAPWAP Mode Element

5. Security Considerations

This document does not constrain the use of encryption mechanisms to protect the data channel. If there is security requirement for CAPWAP Data Channel, Datagram Transport Layer Security (DTLS) [RFC4347] and the IPSec mechanism [RFC2401] can be used to guarantee the security of the CAPWAP Data Channel.

If DTLS is used for CAPWAP Data Channel in CAPWAP Split Mode, the DTLS procedure is required between a WTP and AR.

6. References

6.1. Normative References

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

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 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.

6.2. Informative References

[I-D.cao-capwap-eap]
Zhang, R., Cao, Z., and H. Luo, "Encapsulation of EAP Messages in CAPWAP Control Plane", draft-cao-capwap-eap-00 (work in progress), October 2012.

Authors' Addresses

Li Xue
Huawei
No.156 Beiqing Rd. Z-park, Shi-Chuang-Ke-Ji-Shi-Fan-Yuan, HaiDian District
Beijing 100095
China

Email: xueli@huawei.com

Zongpeng Du
Huawei
No.156 Beiqing Rd. Z-park, Shi-Chuang-Ke-Ji-Shi-Fan-Yuan, HaiDian District
Beijing 100095
China

Email: duzongpeng@huawei.com

Dapeng Liu
China Mobile
Unit 2, 28 Xuanwumenxi Ave, Xuanwu District
Beijing 100053
China

Email: liudapeng@chinamobile.com

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

Email: zhangr@gsta.com

John Kaippallimalil
Huawei
5430 Legacy Drive, Suite 175
Plano, TX 75024

Email: john.kaippallimalil@huawei.com