Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: January 15, 2014

R. Zhang
China Telecom
Z. Cao
H. Deng
China Mobile
R. Pazhyannur
S. Gundavelli
Cisco

July 14, 2013

Separation of CAPWAP Control and Data Plane: Scenarios, Requirements and Solutions

draft-zhang-opsawg-capwap-cds-00

Abstract

This document describes the scenarios and requirements of separating CAPWAP Data and Control plane. This specification provides a CAPWAP extension to allow two distinct AC component: AC-DP (AC-Data Plane) and AC-CP (AC-Control Plane). AC-DP handles all user payload with the exception of layer 2 management frames between the AC and user such as IEEE 802.11 association, authentication, probe, Action Frame. AC-CP handles all control messages between the WTP and AC. In addition, the AC-CP wil handle user payload related to layer-2 management frames such as those mentioned above.

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 January 15, 2014.

Copyright Notice

Table of Contents

1. Introduction

Control and Provisioning of Wireless Access Points (CAPWAP) was designed as an interoperable protocol between the wireless access point and the access controller. This architecture makes it possible for the access controller to manage a huge number of wireless access points. With the goals and requirements established in[RFC4564] , CAPWAP protocols were specified in [RFC5415] , [RFC5416]and [RFC5417].

The specificaitons mentioned above mainly design the different control message types used by the AC to control multiple WTPs. CAPWAP specifies that all user payload is transported on the CAPWAP-DATA channel. As an example, EAP messages, as key protocol exchange elements in the WLAN architecture also need to be encapsulated in the CAPWAP-DATA. The CAPWAP protocol does not specify how to encapsulate EAP message in its control plane. As a result, the protocol does not allow for splitting the CAPWAP control and data plane where control messages

There are multiple ways of meeting the above requirements. This document first analyzes the capability of current CAPWAP solutions

and proposes ways to working around the problem without changing existing specifications.

1.1. 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]

1.2. Terminology

Access Controller (AC): The network entity that provides WTP access to the network infrastructure in the data plane, control plane, management plane, or a combination therein.

Access Point (AP): the same with Wireless Termination Point (WTP), The physical or network entity that contains an RF antenna and wireless Physical Layer (PHY) to transmit and receive station traffic for wireless access networks.

CAPWAP Control Plane: A bi-directional flow over which CAPWAP Control packets are sent and received.

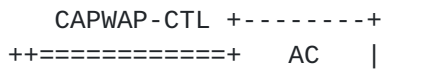
CAPWAP Data Plane: A bi-directional flow over which CAPWAP Data packets are sent and received.

EAP: Extensible Authentication Protocol, the EAP framework is specified in [RFC3748].

2. Scenario and Analysis

The following figure shows where and how the problem arises. In many operators' network, the Access Controller is placed remotely at the central data center. In order to avoid the traffic aggregation at the AC, the data traffic from the AP is directed to the Access Router (AR). In this scenario, the CAPWAP-CTL plane and CAPWAP-DATA plane are separated from each other.

Note: a powerful AC that aggregates the data flows is not a long-term solution to the problem. Because operators always plan the network capacity at a certain level, but with the air interface bandwidth increasing (e.g., from 11g to 11n and 11ac), and the increasing number of access requests on each WTP, the AC may not scale to meet the requirements.



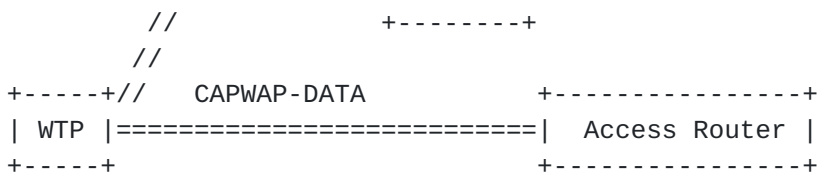


Figure 1: Split between CAPWAP-CTL and CAPWAP-DATA Plane

Because there are no explict message types to support the encapsulation of EAP packets (and more generally layer 2 management frames) in the CAPWAP-CTL plane, the EAP messages are tunneled via the CAPWAP-DATA plane to the AR. AR would act as the authenticator in the EAP framework. After authentication, the AR receives the EAP keying message for the session. However, this mode of operation would undermine the main benefit of having the AC .as the centralized entity for authentication and policy.

Another scenario is the third-party WLAN deployment scenario, in which the access network is a rental property from an broadband operator different from the one who provides authentication services. As shown in Figure 2, The AP is broadcasting a SSID of the Operator #1, say "Operator-1-WLAN", but broadband access network is provided by another Operator #2. To authenticate the users of operator one, the users should be authenticated by the AC in operator one. The data traffic can be routed locally with the access router of operator #2. In this case, there is also a need of separation between CAPWAP-CTL and CAPWAP-DATA traffics.

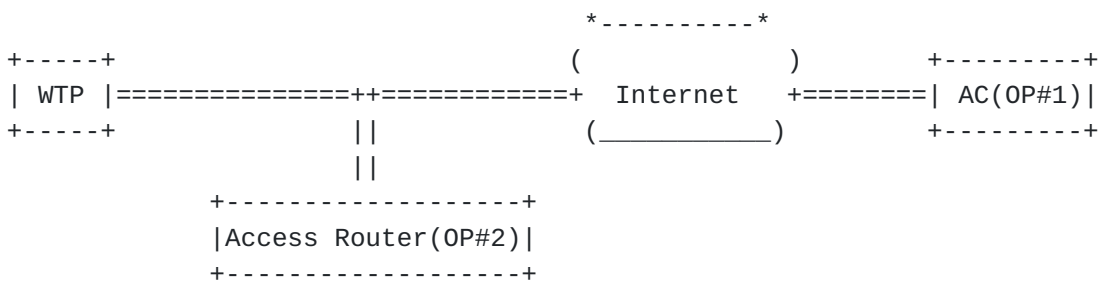


Figure 2: Access Service and Authentication Service Provided by different Operators

3. Analysis of Local Bridging Model

In the Local-MAC model defined in [RFC5416] Section 2.2.2, it says that:

"The WTP MAY locally bridge client data frames (and provide the necessary encryption and decryption services). The WTP MAY also tunnel client data frames to the AC, using 802.3 frame tunnel mode or 802.11 frame tunnel mode."

Some have rightly suggested that the Local-MAC model provides a way to separate Data and Control Plane. In this case where the WTP can locally bridge the user traffic (wihtout any CAPWAP encapsulation). EAP and other management traffic can still be carried over the CAPWAP-DATA tunnel between the WTP and AC. The limitation of this behavior is two fold: This requries the Access Router (that will apply policy, etc) to be on the same Layer-2 network as the WTP. In many deployments, the traffic would need to be tunneled between the WTP and the Access Router that applies the policy. Second, without outer layer CAPWAP Data header, charging and controlling policies could not be applied to the data plane.

The Figure 3 shows this case where WTP encapsulates EAP messages into CAPWAP-DATA plane but locally bridges data frames.

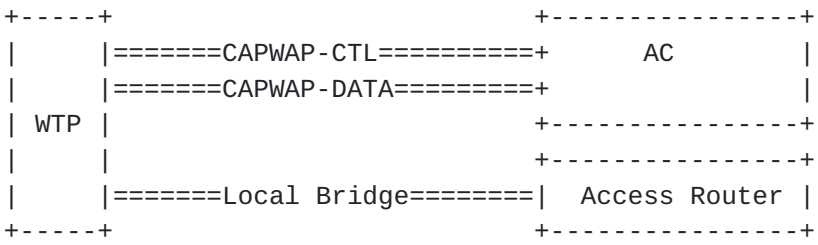


Figure 3: Local Bridging Model

4. Multiple CAPWAP Data Tunnels

A proposed solution is to create multiple CAPWAP-DATA tunnels. As shown in Figure 4, the WTP encapsulates all control messages between the WTP and AC in teh CAPWAP-Control tunnel. In addition, all Layer 2 management frames (EAP, etc) are also transported in the CAPWAP-DATA tunnel between WTP and AC-CP. In addition, WTP encapsulates all non-management user payload into a secondary CAPWAP-DATA tunnel between WTP and AC-DP.

This brings up issues related to setting up of the secondary data tunnel, such as how does the WTP discover the IP address of AC-DP,

and what security creedentials are used to setup the tunnel. We plan to address this in the next version of this draft.

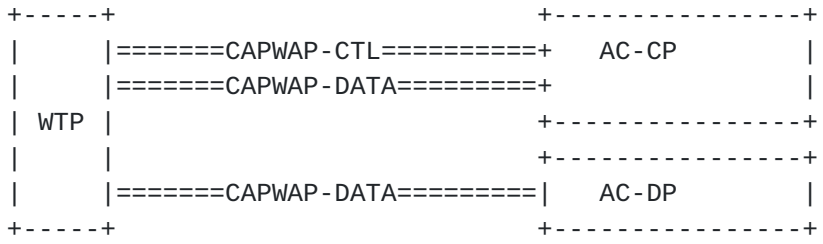


Figure 4: Multiple DATA tunnels Model

5. IANA Considerations

This document has no requests to the IANA.

6. Security Considerations

Security considerations for the CAPWAP protocol has been analyzed in Section 12 of [RFC5415]. This document does not introduce other security issues besides what has been analyzed in RFC5415.

7. Contributors

This document stems from the joint work of Hong Liu, Yifan Chen, Chunju Shao from China Mobile Research.

Thank Dorothy Stanley for reviewing the document and recommending ways to move forward with both technology and editorial parts of the document.

Thank all the contributors of this document.

8. References

8.1. Normative References

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

8.2. Informative References

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

[RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[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.

[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.

[RFC5417] Calhoun, P., "Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option", RFC 5417, March 2009.

Authors' Addresses

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

Email: zhangr@gsta.com

Zhen Cao
China Mobile
Xuanwumenxi Ave. No. 32
Beijing 100871
China

Phone: +86-10-52686688
Email: zehn.cao@gmail.com, caozhen@chinamobile.com

Hui Deng
China Mobile
Xuanwumenxi Ave. No. 32
Beijing 100053
China

Email: denghui@chinamobile.com

Rajesh S. Pazhyannur
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: rpazhyan@cisco.com

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com