Opsawg Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 26, 2015

J. You
H. Song
Huawei
R. Zhang
China Telecom

May 25, 2015

CAPWAP Control and Data Channel Separation for Multi-provider Scenario
draft-you-opsawg-capwap-separation-for-mp-01

Abstract

The CAPWAP control channel and data channel split architecture has some benefits, such as relieving the capacity pressure of the AC. However, the current documents are not specific to the multi-provider scenario. This document discusses the third-party WLAN service provider scenario (i.e. Virtual Network Operator, VNO), and proposes to extend CAPWAP for supporting this use case.

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 November 26, 2015.

Copyright Notice

Table of Contents

1. Introduction

The CAPWAP control channel and data channel split architecture has some benefits, such as relieving the capacity pressure of the AC, which has been discussed in [I-D.ietf-opsawg-capwap-alt-tunnel] etc.

In this document, we introduce a third-party WLAN service provider scenario (i.e. VNO), as shown in Figure 1, and also verify the benefits of having this split architecture. In this scenario, the WLAN provider owns the WTP and AC resources. Other VNOs can rent the WTP resources from the WLAN provider for network access. The AC belonging to the WLAN service provider controls the WTP in a centralized location.

Given that VNOs 1/2 don't have their own network access resources, they rent the WTP resources from the WLAN provider. VNO 1/2 provide the services to their customers by renting the network access resources. The users of VNO 1/2 are authenticated by VNO 1/2 themselves respectively. As the WLAN service provider isn't aware of the users' data traffic of VNO 1/2, the data traffic from the users can be directly routed to the corresponding Access Router (AR) of the provider who owns the users. The data traffic directly to the AR can significantly avoid overload on the AC.

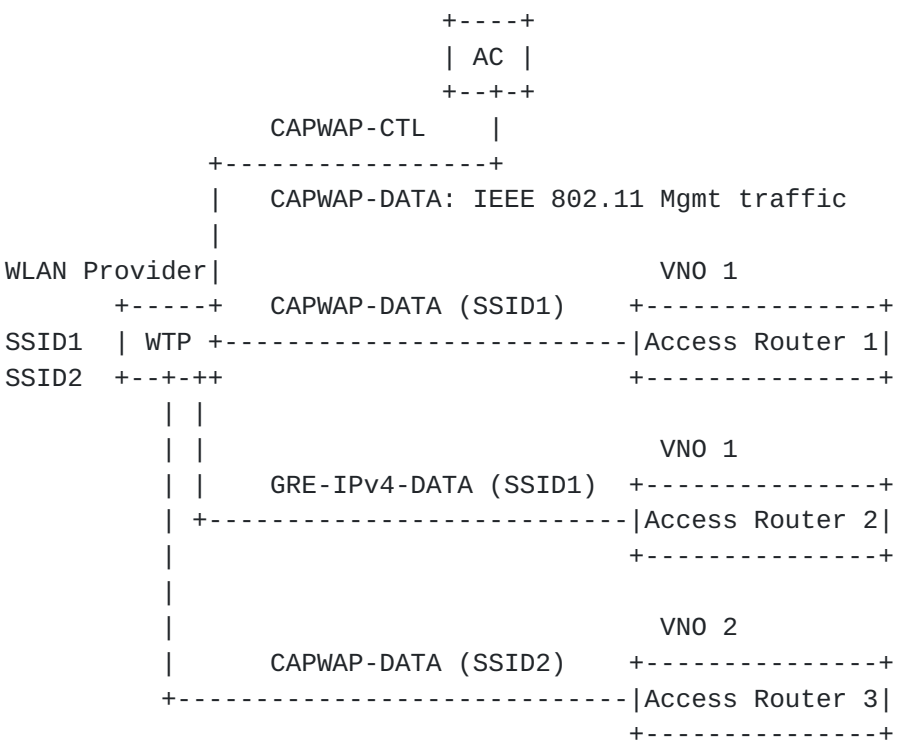

Figure 1: Third-party WLAN Service Provider

This document discusses the third-party WLAN service provider scenario, and proposes to extend CAPWAP for supporting this use case. [I-D.ietf-opsawg-capwap-alt-tunnel] describes CAPWAP Control Channel and CAPWAP Data Channel separation (i.e. CAPWAP Split Mode), but it is not specific to multi-provider scenario. The following section will discuss the extension in order to support multi-provider scenario.

2. Terminology

This section contains definitions for terms used frequently throughout this document. However, many additional definitions can be found in [RFC5415] and [RFC5416].

Station (STA): A device that contains an IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).

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.

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 Router (AR): The access server of the provider.

CAPWAP Control Channel: A bi-directional flow defined by the AC IP Address, WTP IP Address, AC control port, WTP control port, and the transport-layer protocol (UDP or UDP-Lite) over which CAPWAP Control packets are sent and received.

CAPWAP Data Channel: A bi-directional flow defined by the AC IP Address, WTP IP Address, AC data port, WTP data port, and the transport-layer protocol (UDP or UDP-Lite) over which CAPWAP Data packets are sent and received.

3. Split CAPWAP-CTL and CAPWAP-DATA for Multi-provider

A WTP is capable of supporting up to 16 Service Set Identifiers (SSIDs). The WLAN provider may provide network access service for different providers with different SSIDs. For example, in Figure 1, SSID1 is advertised by the WTP for VNO1; and SSID2 is advertised by the WTP for VNO2. Give that a user attaches to the network by SSID1, the WTP needs to send the user's data traffic to AR1/AR2 of VNO1 via CAPWAP/GRE-IPv4 data channel. So WTP needs to obtain the AR addresses of different providers first. The AC of the WLAN service provider needs to maintain the association of the AR addresses of the tenant providers and SSIDs, and provide this information to the WTP.

For the above example (Figure 1), the following steps describe how the alternate tunnels are established using the alternate tunnel encapsulation message element [I-D.ietf-opsawg-capwap-alt-tunnel].

1. The AC provides an alternate tunnel encapsulation message element containing the tunnel type and a tunnel-specific information element, as shown in Figure 2. Specifically,

IEEE 802.11 WLAN Config. Request [IEEE 802.11 Add WLAN (WLAN ID 1 (mapping to SSID1)), Alternate Tunnel Encapsulation (Tunnel Type=CAPWAP, Tunnel Info Element (AR1))];

The WTP sets up the alternate tunnel with AR1.

2. The AC provides an alternate tunnel encapsulation message element containing the tunnel type and a tunnel-specific information element, as shown in Figure 2. Specifically,

IEEE 802.11 WLAN Config. Request [IEEE 802.11 Add WLAN (WLAN ID 1 (mapping to SSID1)), Alternate Tunnel Encapsulation (Tunnel Type= GRE-IPv4, Tunnel Info Element (AR2))];

The WTP sets up the alternate tunnel with AR2. Multiple ARs may be provided for load balancing for VNO1.

3. The AC provides an alternate tunnel encapsulation message element containing the tunnel type and a tunnel-specific information element, as shown in Figure 2. Specifically,

IEEE 802.11 WLAN Config. Request [IEEE 802.11 Add WLAN (WLAN ID 2 (mapping to SSID2)), Alternate Tunnel Encapsulation (Tunnel Type= CAPWAP, Tunnel Info Element (AR3))];

The WTP sets up the alternate tunnel with AR3.

4. When the WTP detects an alternate tunnel failure, the WTP informs the AC using a message element, WTP Alternate Tunnel Fail Indication defined in [I-D.ietf-opsawg-capwap-alt-tunnel]. The WTP needs to notify the AC of which AR(s) are unavailable.

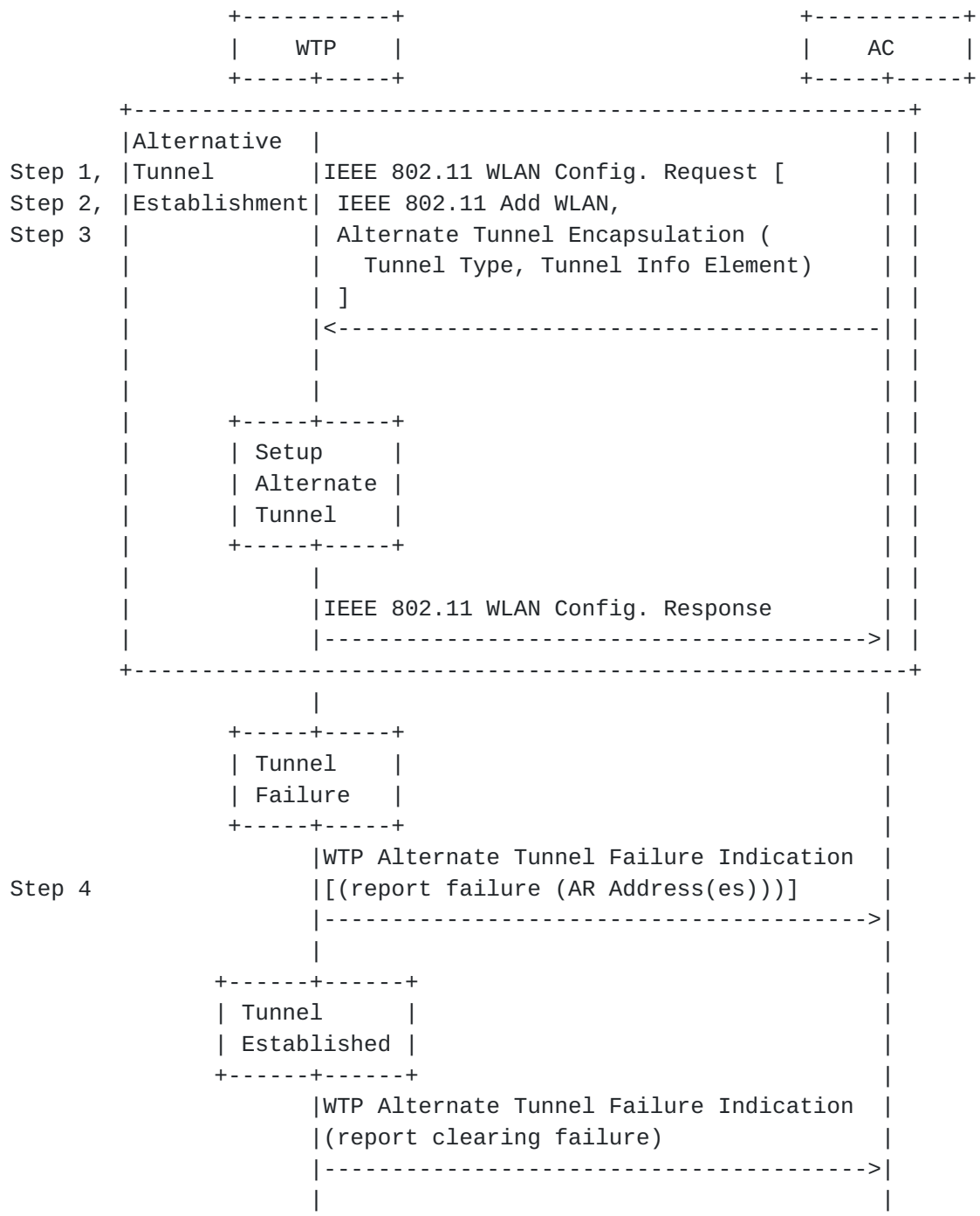

Figure 2: Setup of Alternate Tunnels

4. IEEE 802.11 WTP Alternate Tunnel Failure Indication

When the WTP detects an alternate tunnel failure, the WTP informs the AC using a message element, WTP Alternate Tunnel Fail Indication defined in [I-D.ietf-opsawg-capwap-alt-tunnel]. For the case where WTP establishes data tunnels with multiple ARs under VNO scenarios,

the WTP needs to notify the AC of which AR(s) are unavailable, as shown in Figure 2.

The Alternate Tunnel Failure Indication message element is extended to contain the AR information, as follows:

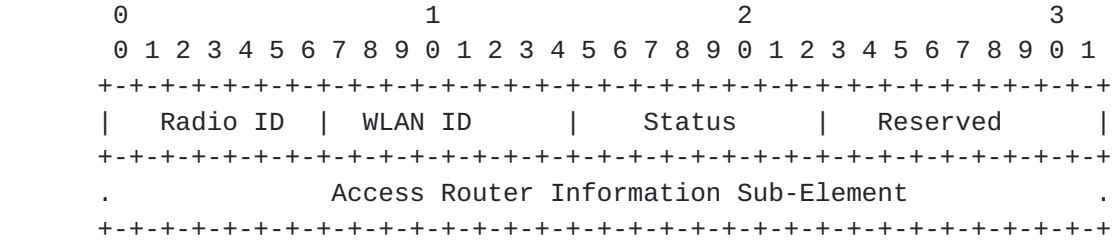

Figure 3: IEEE 802.11 WTP Alternate Tunnel Failure Indication

Type: IEEE 802.11 WTP Alternate Tunnel Failure Indication defined in [I-D.ietf-opsawg-capwap-alt-tunnel].

Length: > 4

Radio ID: The Radio Identifier, whose value is between one (1) and 31, typically refers to some interface index on the WTP.

WLAN ID: An 8-bit value specifying the WLAN Identifier. The value MUST be between one (1) and 16.

Status: An 8-bit boolean indicating whether the radio failure is being reported or cleared. A value of zero is used to clear the event, while a value of one is used to report the event.

Access Router Information Sub-Element [I-D.ietf-opsawg-capwap-alt-tunnel]: IPv4 address or IPv6 address or Fully Qualified Domain Name (FQDN), of the Access Router for the alternate tunnel. The Access Router Information Sub-Elements allow the WTP to notify the AC of which AR(s) are unavailable.

5. IANA Considerations

This document has no IANA actions.

6. 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.

7. Acknowledgement

The authors would like to thank Zongpeng Du and Jin Li for their valuable comments.

8. References

8.1. 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.

8.2. Informative References

[I-D.ietf-opsawg-capwap-alt-tunnel] Zhang, R., Cao, Z., Deng, H., Pazhyannur, R., Gundavelli, S., and L. Xue, "Alternate Tunnel Encapsulation for Data Frames in CAPWAP", draft-ietf-opsawg-capwap-alt-tunnel-05 (work in progress), April 2015.

Authors' Addresses

Jianjie You
Huawei
101 Software Avenue, Yuhuatai District
Nanjing 210012
China

Email: youjianjie@huawei.com

Haibin Song
Huawei
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012
China

Email: haibin.song@huawei.com

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

Email: zhangr@gsta.com