Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 26, 2015

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

July 25, 2014

Alternate Tunnel Encapsulation for Data Frames in CAPWAP
draft-ietf-opsawg-capwap-alt-tunnel-01

Abstract

CAPWAP defines a specification to encapsulate a station's data frames between the Wireless Transmission Point (WTP) and Access Controller (AC) using CAPWAP. Specifically, the station's IEEE 802.11 data frames can be either locally bridged or tunneled to the AC. When tunneled, a CAPWAP data channel is used for tunneling. In many deployments it is desirable to encapsulate date frames to an entity different from the AC for example to an Access Router (AR). Further, it may also be desirable to use different tunnel encapsulations to carry the stations' data frames. This document provides a specification for this and refers to it as Alternate tunnel encapsulation. The Alternate tunnel encapsulation allows 1) the WTP to tunnel non-management data frames to an endpoint different from the AC and 2) the WTP to tunnel using one of many known encapsulation types such as IP-IP, IP-GRE, CAPWAP. The WTP may advertise support for Alternate tunnel encapsulation during the discovery or join process and AC may select one of the supported Alternate Tunnel encapsulation types while configuring the WTP.

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 26, 2015.

Table of Contents

1. Introduction

Service Providers are deploying very large Wi-Fi deployments (ranging from hundreds of thousands of APs (referred to as WTPs in CAPWAP terminology) to millions of APs). These networks are designed to carry traffic generated from mobile users. The volume in mobile user traffic is already very large (in the order of petabytes per day) and expected to continue growing rapidly. As a result, operators are looking for solutions that can scale to meet the increasing demand.

One way to meet the scalability requirement is to split the control/ management plane from the data plane. This separation enables the data plane be scaled independently of the control/management plane. This document provides a description of a CAPWAP specification change that enables the separation of data plane from control plane.

CAPWAP ([RFC5415], [RFC5416]) defines a tunnel mode that specifies the frame tunneling type to be used for 802.11 data frames from stations associated with the WLAN. The following types are supported:

- Local Bridging: All user traffic is to be locally bridged.
- 802.3 Tunnel: All user traffic is to be tunneled to the AC in 802.3 format.
- 802.11 Tunnel: All user traffic is to be tunneled to the AC in 802.11 format.

There are two shortcomings with currently specified tunneled modes: 1) it does not allow the WTP to tunnel data frames to an endpoint different from the AC and 2) it does not allow the WTP to tunnel data frames using any encapsulation other than CAPWAP (as specified in Section 4.4.2 of [RFC5415]). Next, we describe what is driving the above mentioned two requirements.

Some operators deploying large number of Access Points prefer to centralize the management and control of Access Points while distributing the handling of data traffic to increase scaling. This motivates an architecture as shown in Figure 1 that has the AC in a centralized location and one or more tunnel gateways (or Access Routers) that terminate the data tunnels from the various WTPs. This split architecture has two benefits over an architecture where data traffic is aggregated at the AC: 1) reduces the scale requirement on data traffic handling capability of the AC and 2) leads to more efficient/optimal routing of data traffic.

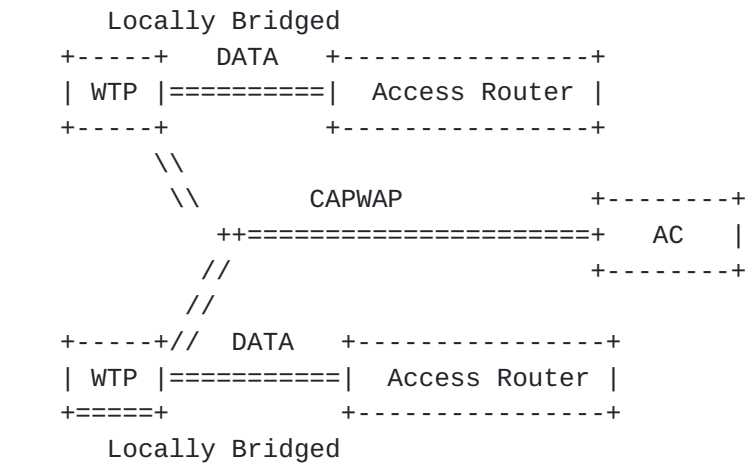

Figure 1: Centralized Control with Distributed Data

The above system (shown in Figure 1) could be achieved by setting the tunnel mode to Local bridging. In such a case the AC would handle control of WTPs as well as handle the management traffic to/from the stations. There is CAPWAP Control and Data Channel between the WTP and the AC. The CAPWAP Data channel carries the IEEE 802.11 management traffic (like IEEE 802.11 Action Frames). The station's data frames are locally bridged, i.e., not carried over the CAPWAP data channel. The station's data frames are handled by the Access Router. However, in many deployments the operator managing the WTPs/ AC may be different from the operator providing the internet connectivity to the WTPs. Further, the WTP operator may want (or be required by legal/regulatory requirements) to tunnel the traffic back to an Access Router in its network as shown in Figure 2. The tunneling requirement may be driven by the need to apply policy at the Access Router or a legal requirement to support lawful intercept of user traffic. What this means is that local bridging does not meet their requirements. Their requriements are met either by having the WTP tunnel the station's traffic to the AC or the WTP support an alternate tunnel, i.e., a tunnel to an alternate entity different from the AC. This is the motivation for Alternate Tunnel encapsulation support where the data tunnels from the WTP are terminated at an AR (and more specifically at an end point different from the AC).

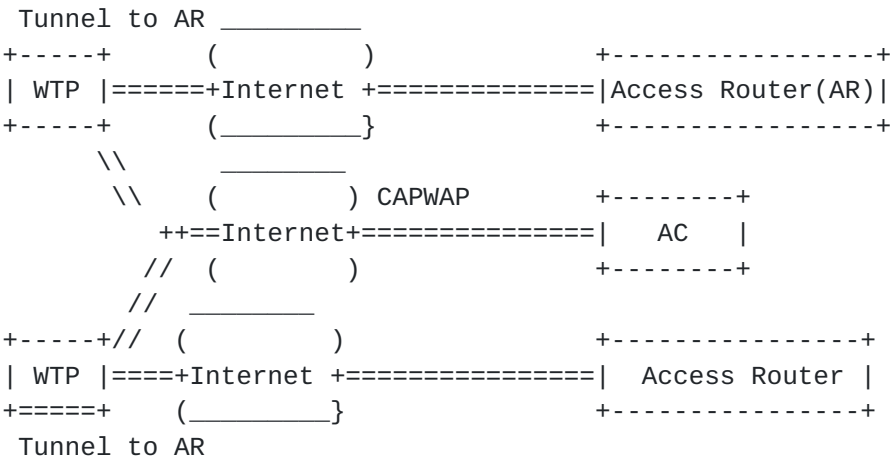

Figure 2: Centralized Control with Distributed Data

In the case where the WTP is tunneling data frames to an AR (and not the AC), the choice of tunnel encapsulation need not be restricted only to CAPWAP (as described in Section 4.4.2 of [RFC5415]). In fact, the WTP may additionally support other widely used encapsulation types such as L2TP, L2TPv3, IP-in-IP, IP/GRE, etc. The WTP may advertise the different alternate tunnel encapsulation types supported and the AC can select one of the supported encapsulation types. As shown in the figure there is still a CAPWAP control and data channel between the WTP and AC wherein the CAPWAP data channel carries the stations' management traffic. Thus the WTP will maintain three tunnels: CAPWAP Control, CAPWAP Data, and another (alternate) tunnel to the AR. The main reason to maintain a CAPWAP data channel is to minimize the changes on the WTP and AC required to transport stations' management frames (like EAP, IEEE 802.11 Action Frames). These management frames are transported over the CAPWAP data channel as they are done for case when the WTP's tunnel mode is configured as the local bridging. In this specification we describe how the WTP can be configured with this alternate tunnel.

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

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).

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.

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 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.

2. Alternate Tunnel Encapsulation

2.1. Description

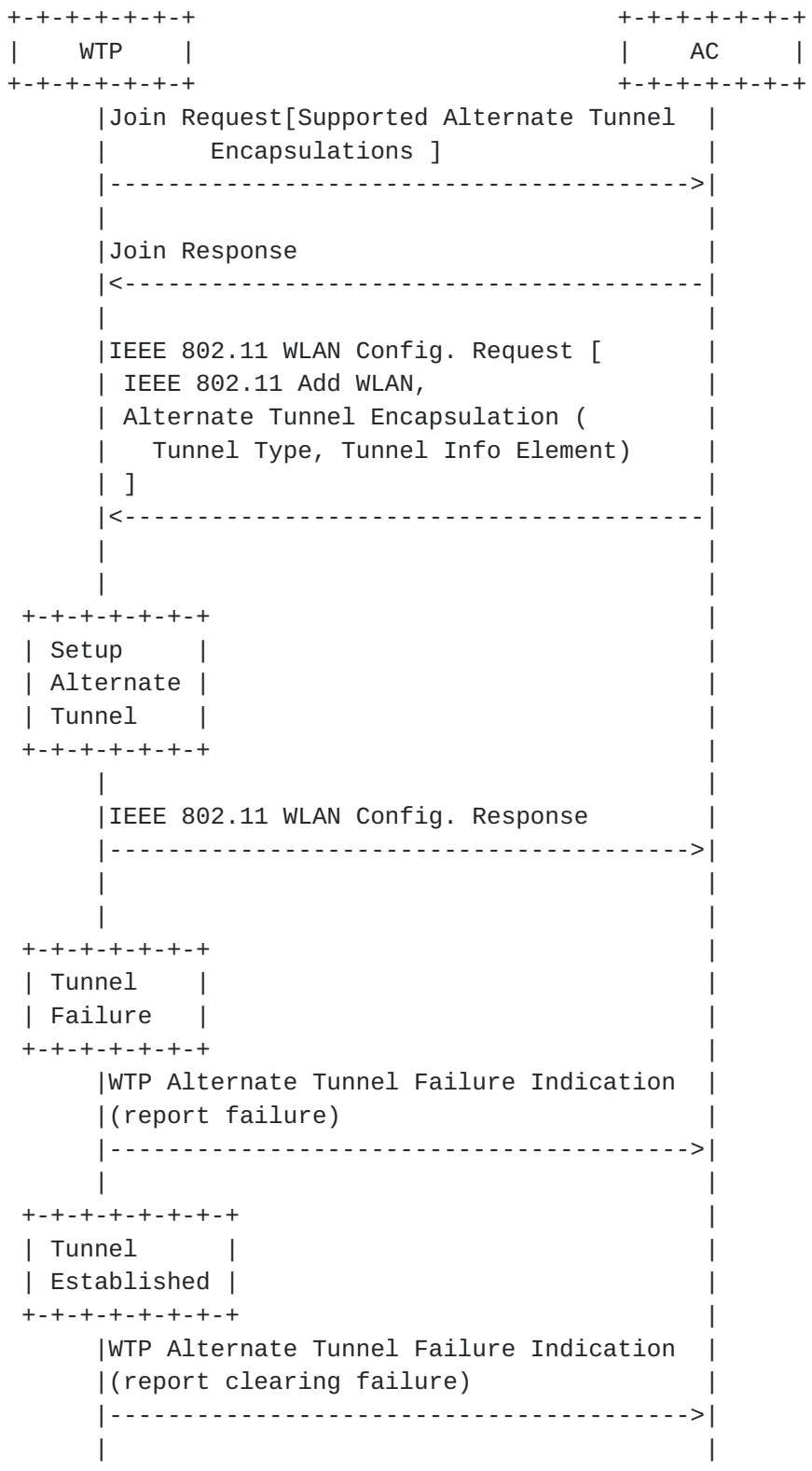

Figure 3: Setup of Alternate Tunnel

The above example describes how the alternate tunnel encapsulation may be established. When the WTP joins the AC, it should indicate its alternate tunnel encapsulation capability. The AC determines whether an alternate tunnel configuration is required. If an appropriate alternate tunnel type is selected, then the AC provides the alternate tunnel encapsulation message element containing the tunnel type and a tunnel-specific information element. (The tunnel-specific information element, for example, may contain information like the IP address of the tunnel termination point.) The WTP sets up the alternate tunnel using the alternate tunnel encapsulation message element.

When the WTP detects an alternate tunnel failure, the WTP informs the AC using a message element (defined in this specification), WTP Alternate Tunnel Fail Indication. The message element has a status field that indicates whether the message denotes reporting a failure or the clearing of the previously reported failure.

3. Protocol Considerations

3.1. Supported Alternate Tunnel Encapsulations

This message element is sent by a WTP to communicate its capability to support alternate tunnel encapsulations. The message element contains the following fields:

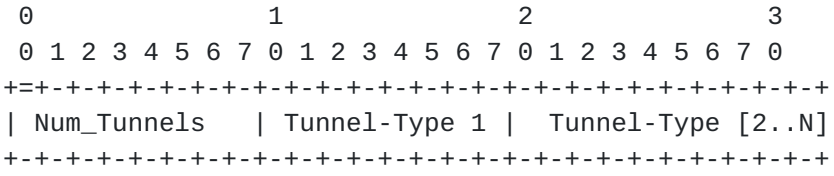

Figure 4: Supported Alternate Tunnel Encapsulations

- Type: <IANA-1> for Supported Alternate Tunnel Encapsulations
- Length: The length in bytes is 1 + Num_Tunnels
- Num_Tunnels: This refers to number of tunnel types present in the message element. At least one tunnel type must be present.
- Tunnel-Type: This is identified by value defined in Section 3.2

3.2. Alternate Tunnel Encapsulations Type

This message element is sent by the AC. This message element allows the AC to select the alternate tunnel encapsulation. This message element may be provided along with the IEEE 802.11 Add WLAN message element. When the message element is present the following fields of the IEEE 802.11 Add WLAN element shall be set as follows: MAC mode is

set to 0 (Local MAC) and Tunnel Mode is set to 0 (Local Bridging). The message element contains the following fields

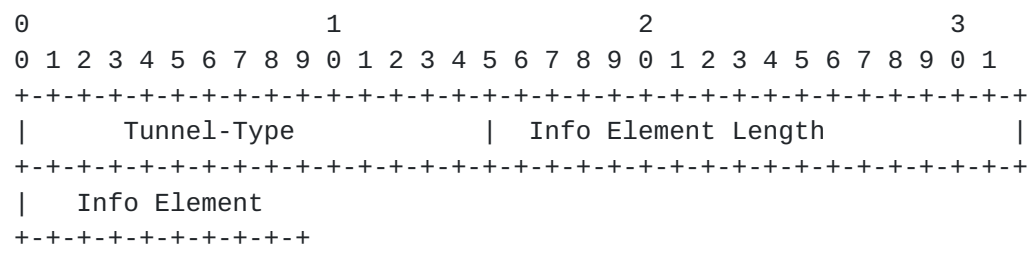

Figure 5: Alternate Tunnel Encapsulations Type

- Type: <IANA-2> for Alternate Tunnel Encapsulation Type
- Length: > 4
- Tunnel-Type: The tunnel type is specified by a 2 byte value. This specification defines the values from zero (0) to five (5) as given below. The remaining values are reserved for future use.

  * 0: CAPWAP. This refers to a CAPWAP data channel described in [RFC5415][RFC5416]. Additional decscription in [I-D.xue-opsawg-capwap-alt-tunnel-information].
  * 1: L2TP. This refers to tunnel encapsulation described in [RFC2661].
  * 2: L2TPv3. This refers to tunnel encapsulation described in [RFC3931].
  * 3: IP-in-IP. This refers to tunnel encapsulation described in [RFC2003].
  * 4: PMIPv6. This refers to the tunneling encapsulation described in [RFC5213]
- Info Element: This field contains tunnel specific configuration parameters to enable the WTP to setup the alternate tunnel. For example if the tunnel type is CAPWAP then this field may contain the following (non-exhaustive) list of parameters

  * Access Router IPv4 address
  * Access Router IPv6 address
  * Tunnel DTLS Policy
  * IEEE 802.11 Tagging Policy

  This specification only defines a generic container for such message elements. We anticipate that these message elements (for the different protocols) will be defined in separate documents, potentially one for each tunneling protocols. See

[I-D.xue-opsawg-capwap-alt-tunnel-information] for example of such a specification.

3.3. IEEE 802.11 WTP Alternate Tunnel Failure Indication

The Alternate Tunnel Encapsulation message element is sent by the WTP to inform the AC about the status of the Alternate Tunnel. The message element contains the following fields

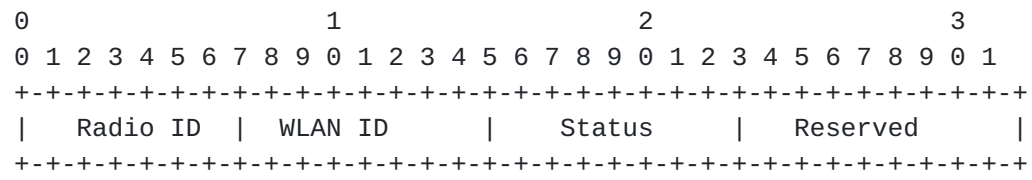

Figure 6: IEEE 802.11 WTP Alternate Tunnel Failure Indication

- Type: <IANA-3> for IEEE 802.11 WTP Alternate Tunnel Failure Indication
- 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.

4. IANA Considerations

This document requires the following IANA considerations.

- <IANA-1>. This specification defines the Supported Alternate Tunnel Encapsulations Type message element in Section 3.1. This elements needs to be registered in the existing CAPWAP Message Element Type registry, defined in [RFC5415]. The Type value for this element needs to be between 1 and 1023 (see Section 15.7 in [RFC5415]).
- <IANA-2>. This specification defines the Alternate Tunnel Encapsulations Type message element in Section 3.2. This element needs to be registered in the existing CAPWAP Message Element Type registry, defined in [RFC5415]. The Type value for this element needs to be between 1 and 1023.
- <IANA-3>. This specification defines the IEEE 802.11 WTP Alternate Tunnel Failure Indication message element in

Section 3.3. This element needs to be registered in the existing CAPWAP Message Element Type registry, defined in [RFC5415]. The Type value for this element needs to be between 1024 and 2047.

- Tunnel-Type: This specification defines the Alternate Tunnel Encapsulations Type message element. This element contains a field Tunnel-Type. The namespace for the field is 16 bits (0-65535)). This specification defines values, zero (0) through five (5) and can be found in Section 3.2. The remaining values (6-65535) are controlled and maintained by IANA and require an Expert Review. IANA needs to create a Tunnel-Type registry whose format is given below.

Tunnel-Type	Type Value	Reference
CAPWAP	0	
L2TP	1	
L2TPv3	2	
IP-IP	3	
PMIPv6	4	

5. Security Considerations

This document introduces three new CAPWAP WTPssage elements. These elements are transported within CAPWAP Control messages as the existing message elements. Therefore, this document does not introduce any new security risks compared to [RFC5415] and [RFC5416]. The security considerations described in [RFC5415] and [RFC5416] apply here as well.

6. Contributors

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

7. References

7.1. Normative References

[RFC2003] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

[RFC2661] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[RFC3931] Lau, J., Townsley, M., and I. Goyret, "Layer Two Tunneling Protocol - Version 3 (L2TPv3)", RFC 3931, March 2005.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[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.

7.2. Informative References

[I-D.xue-opsawg-capwap-alt-tunnel-information]
Liu, D., Zhang, R., Xue, L., Kaippallimalil, J., Pazhyannur, R., and S. Gundavelli, "Specification Alternate Tunnel Information for Data Frames in WLAN", draft-xue-opsawg-capwap-alt-tunnel-information-00 (work in progress), July 2014.

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

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
No.32 Xuanwumen West Street
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

Li Xue
Huawei
No.156 Beiqing Rd. Z-park, HaiDian District
Beijing
China

Email: xueli@huawei.com