Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 27, 2015

D. Liu
China Mobile
R. Zhang
China Telecom
L. Xue
J. Kaippallimalil
Huawei
R. Pazhyannur
S. Gundavelli
Cisco

October 24, 2014

Specification Alternate Tunnel Information for Data Frames in WLAN
draft-xue-opsawg-capwap-alt-tunnel-information-01

Abstract

In IEEE 802.11 Wireless Local Area Network (WLAN) architecture, in order to satisfy the scalability requirement, customer data frames are desired to be distributed to an endpoint as Access Router(AR) different from the Access Controller (AC). For tunneling the data frames, there are many known alternate tunnel technologies can be used, such as IP-GRE, IP-in-IP, CAPWAP, L2TP/L2TPv3, etc. To assist a WTP to set up the alternate tunnels for data plane, this document extends the CAPWAP message elements.

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 27, 2015.

Table of Contents

1. Introduction

Control and Provisioning of Wireless Access Points (CAPWAP) ([RFC5415], [RFC5416]) defines CAPWAP tunnel mode which can be used to encapsulate data frames and control/management frames of a station between the Wireless Transmission Point (WTP) and the Access Controller (AC). The customer data traffic on WTP can be either locally bridged or tunneled to the AC. In practice, operators who have deployed large numbers of WTPs desire to distribute the data traffic to a different entity (e.g., Access Router) rather than the AC for redundancy reasons. The architecture for tunneling WLAN user data frames to ARs is defined in [I-D.ietf-opsawg-capwap-alt-tunnel] and shown in Figure 1.

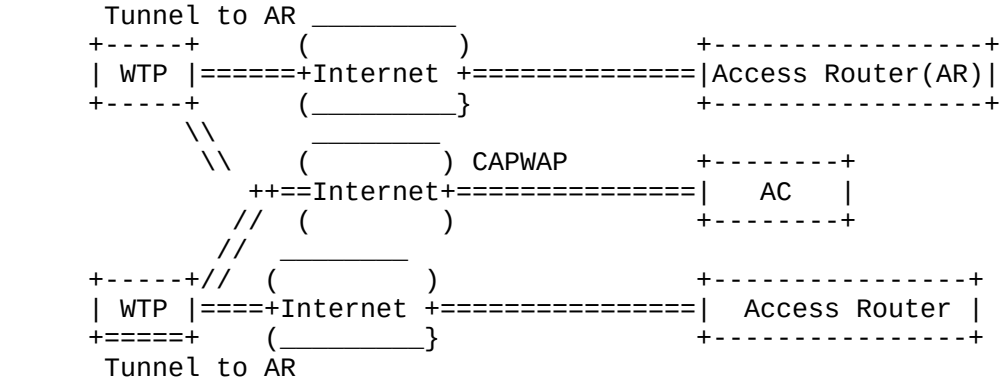


Figure 1: Centralized Control with Distributed Data

How the WTP can be configured with this alternate tunnel is already defined in [I-D.ietf-opsawg-capwap-alt-tunnel]. However, [I-D.ietf-opsawg-capwap-alt-tunnel] specifies only the generic container of the extension CAPWAP message elements used for this alternate tunnel (see Figure 2). The message elements information rely on a binding specification for a particular alternate tunnel protocol, such as GRE, IP-in-IP, CAPWAP, L2TP/L2TPv3 etc. This specification defines the binding specific CAPWAP message elements for using the different alternate tunnel protocols, one for each alternate tunnel protocol. Different Alternate Tunnel sub-message elements are defined.

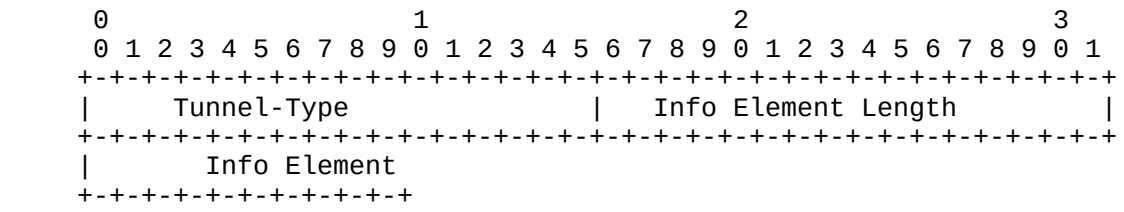


Figure 2: Alternate Tunnel Encapsulations Type

2. Data Frame Alternate Tunnel in WLAN

2.1. CAPWAP

When the WTP joins the AC, it should indicate its alternate tunnel encapsulation capability and the CAPWAP protocol should be one option. If the CAPWAP encapsulation is selected by the AC and configured by the AC to the WTP, the Info Element field of the generic encapsulation shown in Figure 2 should contain the following information:

- Access Router Information: IPv4 address or IPv6 address or Fully Qualified Domain Name (FQDN), which includes the Access Router information with which the WTP can associated for tunneling the user traffic.

- Tunnel DTLS Policy: The CAPWAP protocol allows optional protection of data packets using DTLS. Use of data packet protection on a WTP is determined by the associated AC policy. When the AC determines the DTLS is utilized, the D bit should be set. Otherwise, clear data packets will be encapsulated (see [RFC5415]).

- IEEE 802.11 Tagging Mode Policy: It is used to specify how the CAPWAP data channel packet are to be tagged for QoS purposes (see [RFC5416]).

- CAPWAP Transport Protocol: The CAPWAP protocol supports both UDP and UDP-Lite (see [RFC3828]). When run over IPv4, UDP is used for the CAPWAP data channels. When run over IPv6, the CAPWAP data channel may use either UDP or UDP-lite.

The message element structure for CAPWAP encapsulation is shown in Figure 3:

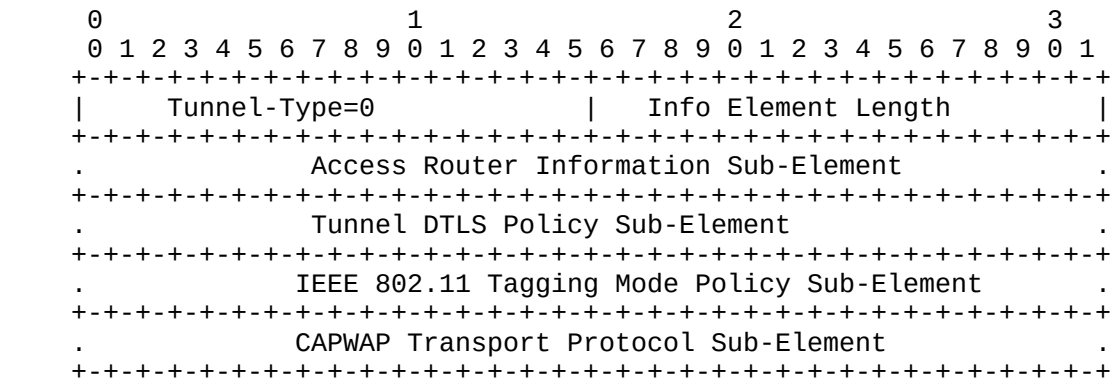


Figure 3: Alternate Tunnel Encapsulation - CAPWAP

2.2. L2TP

Layer Two Tunneling Protocol (L2TP) can pass PPP frames over an L2TP tunnel within a UDP datagram. When a AC selects the L2TP as the alternate tunnel encapsulation and reports the selection to the WTP, the WTP initiates the L2TP data tunnel establishment with the specific AR(s). The AR whose responsibility is to be a L2TP Network Server (LNS) (see [RFC2661]) should configure WTP during the calling request from hosts attaching to the WTP in IEEE 802.11 network. For L2TP, the Info Element field of the generic encapsulation shown in Figure 2 should contain the following information (not-exhaustive):

- Access Router (acts as LNS) Information: IPv4 address or IPv6 address or Fully Qualified Domain Name (FQDN), which includes the Access Router information with which the WTP can associate for tunneling the user traffic.

The message element structure for L2TP encapsulation is shown in Figure 4:

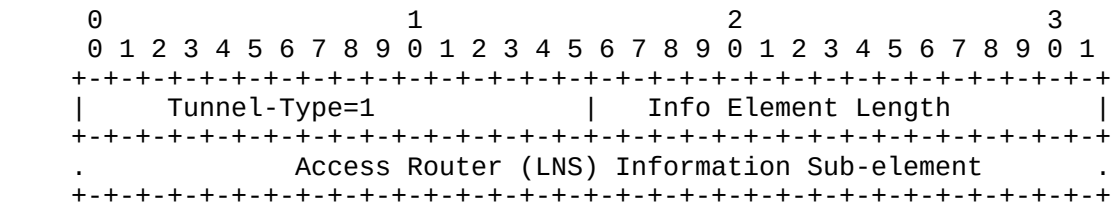


Figure 4: Alternate Tunnel Encapsulation - L2TP

2.3. L2TPv3

L2TPv3 (see [RFC3931]) borrows largely from L2TPv2. L2TPv3 tunnel can be used over multiple Packet-Switched Networks (PSN) such as IP, UDP, Frame Relay, ATM, MPLS, etc. L2TPv3 data tunnels may be utilized with or without the L2TP control channel, either via manual configuration or via other signaling methods to per-configure or distribute L2TP session information. In this document, L2TPv3 control channel is assumed to establish, manage and tear down the L2TPv3 data tunnels. For L2TPv3, the Info Element field of the generic encapsulation shown in Figure 2 should contain the following information:

- Access Router (acts as LNS) Information: IPv4 address or IPv6 address or Fully Qualified Domain Name (FQDN), which includes the Access Router information with which the WTP can associate for tunneling the user traffic.

The message element structure for L2TPv3 encapsulation is shown in Figure 5:

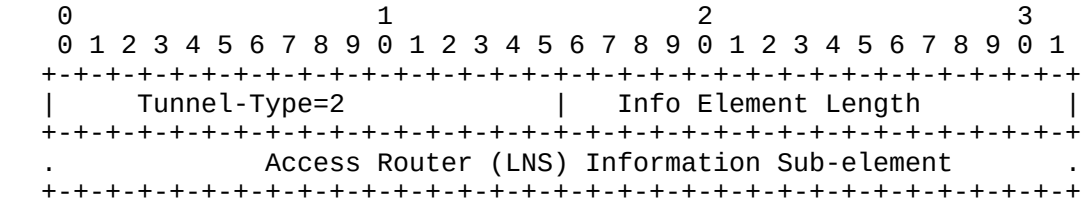


Figure 5: Alternate Tunnel Encapsulation - L2TPv3

2.4. IP-in-IP

If IP-in-IP encapsulation (see [RFC2003]) is selected by AC, the user traffic that arrives to a WTP is encapsulated within IP datagrams and delivered to an intermediate destination which is the Access Router. Once the encapsulated datagram arrives the AR, it is decapsulated. In the general case, the encapsulator WTP should obtain the AR as the decapsulator. If IP-in-IP encapsulation is selected by AC and configured by AC to WTP, the Info Element field of the generic encapsulation shown in Figure 2 should contain the following information:

- Access Router Information: IPv4 address or IPv6 address or Fully Qualified Domain Name (FQDN), which includes the Access Router information with which the WTP can associate for tunneling the user traffic.

The message element structure for IP-in-IP encapsulation is shown in Figure 6:

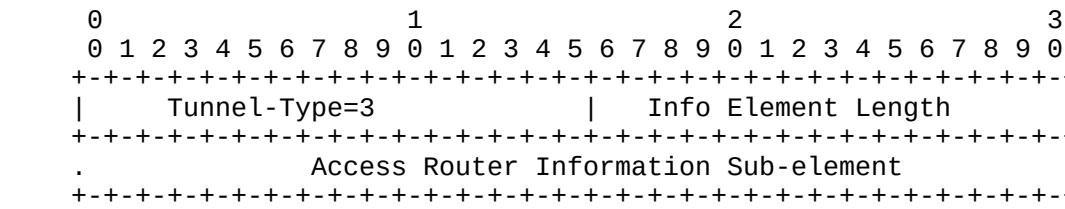


Figure 6: Alternate Tunnel Encapsulation - IP-in-IP

2.5. PMIPv6

Proxy Mobile IPv6 (PMIPv6, see [RFC5213]) is one option for alternate tunnel encapsulation between the WTP and the AR. In this scenario, a WTP should act as the Mobile Access Gateway (MAG) function that manages the mobility-related signaling for a station that is attached to the WTP IEEE 802.11 radio access. The Local Mobility Anchor (LMA) function should be located at the AR. In Proxy Mobile IPv6, the address of the LMA should be discovered by the MAG. If PMIPv6 encapsulation is selected by the AC and configured by the AC to a WTP, the Info Element field of the generic encapsulation shown in Figure 2 should contain the following information:

- Access Router (acts as LMA) Information: IPv6 address or Fully Qualified Domain Name (FQDN), which includes the Access Router information with which the WTP can associate for tunneling the user traffic.

The message element structure for PMIPv6 encapsulation is shown in Figure 7:

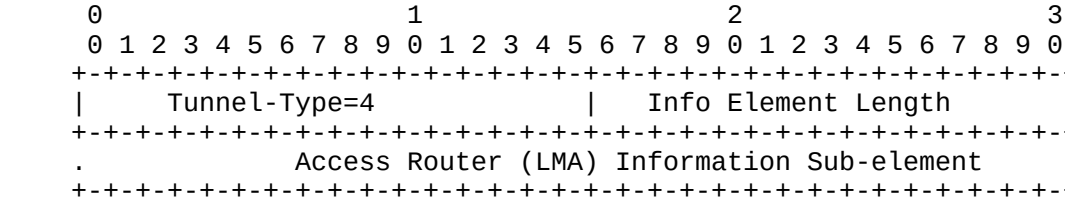


Figure 7: Alternate Tunnel Encapsulation - PMIPv6

2.6. GREv4/6

In order to encapsulate data traffic using GREv4/6 (see and [RFC1701][RFC2784]), the WTP needs to obtain the destination node IP address of a GRE tunnel (e.g., the AR address). Optionally, GRE Key Sub-element (see [RFC2784] and [RFC2890]) is needed for WTP to configure the complementary tunnel information. If WTP obtains the GRE Key Sub-element, the key MUST be inserted into the GRE encapsulation header. The Key is used for identifying extra context information about the received payload on AR. If the WTP obtains the Key information from the AC, the payload packets without the correspondent GRE Key or with an unmatched GRE Key will be silently dropped on the AR. For GRE, the Info Element field of the generic encapsulation shown in Figure 2 should contain the following information (not-exhaustive):

- Access Router Information: IPv4 address (for GREv4) or IPv6 address (for GREv6) or Fully Qualified Domain Name (FQDN) (For both GREv4 and GREv6), which includes the Access Router information with which the WTP can associate for tunneling the user traffic.

- GRE Key: The Key field contains a four octet number which is inserted by the WTP as defined in [RFC2890].

The message element structure for GREv4 encapsulation is shown in Figure 8:

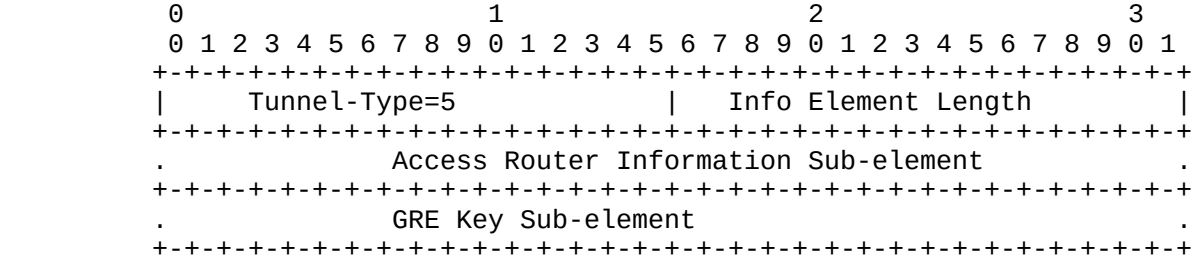


Figure 8: Alternate Tunnel Encapsulation - GREv4

The message element structure for GREv6 encapsulation is shown in Figure 9:

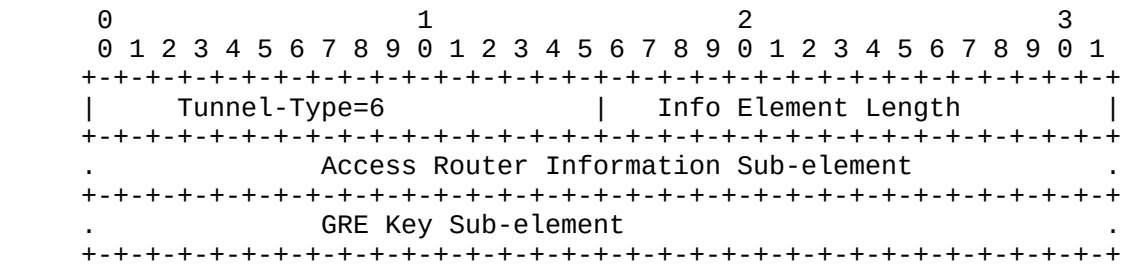


Figure 9: Alternate Tunnel Encapsulation - GREv6

3. Alternate Tunnel Information Elements

3.1. Access Router Information Sub-Elements

The Access Router Information Sub-Elements allow the AC to notify a WTP of which AR(s) are available for establishing a data tunnel. The AR information may be IPv4 address, IPv6 address, or AR domain name. If a WTP obtains the correct AR FQDN, the Name-to-IP address mapping is handled in the WTP (see [RFC2782]).

The following are the Access Router Information Sub-Elements defined in this specification. The AC can use one of them to notify the destination information of the data tunnel to the WTP. The Sub-Elements containing the AR IPv4 address MUST NOT be used if an IPv6 data channel such as PMIPv6 or GREv6 is used.

3.1.1. AR IPv4 Address Sub-Element

This Sub-Element (see Figure 10) is used by the AC to configure a WTP with the AR IPv4 address available for the WTP to establish the data tunnel for user traffic.

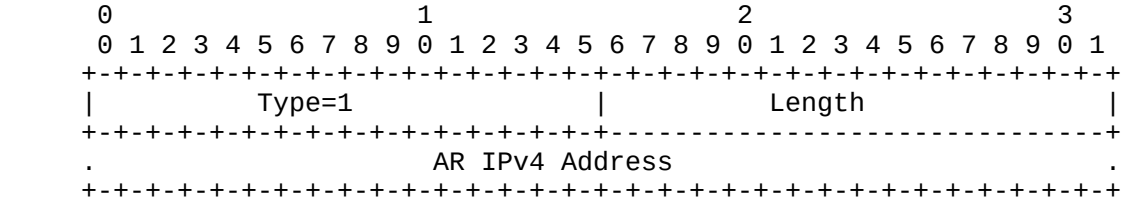


Figure 10: AR IPv4 Address Sub-Element

Type: 1 for AR IPv4 Address

Length: 4

AR IPv4 Address: 32-bit integer containing AR IPv4 Address.

3.1.2. AR IPv4 Address for Load-balance Sub-Element

This Sub-Element (see Figure 11) is used to satisfy load-balance and reliability requirements. There may be multiple AR addresses available for a WTP and provided by an AC. The WTP can use the AR information to send user traffic.

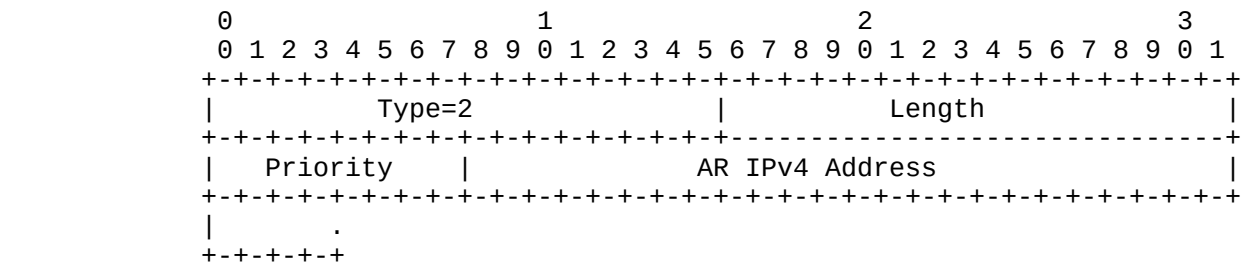


Figure 11: AR IPv4 Address for Load-balance Sub-Element

Type: 2 for AR IPv4 Address for Load-balance

Length:>=5

Priority: A value between 1 and 255 specifying the priority order for the preferred AR. For instance, the value of one (1) is used to set the primary AR, the value of two (2) is used to set the secondary; two instances with the same value are used for load-balance, etc.

AR IPv4 Address: 32-bit integer containing AR IPv4 Address binding with the specific priority. There may be an array of pairs binding priority and AR IPv4 address.

3.1.3. AR IPv6 Address Sub-Element

This Sub-Element (see Figure 12) is used by the AC to configure a WTP with the AR IPv6 address available for the WTP to establish the data tunnel for user traffic.

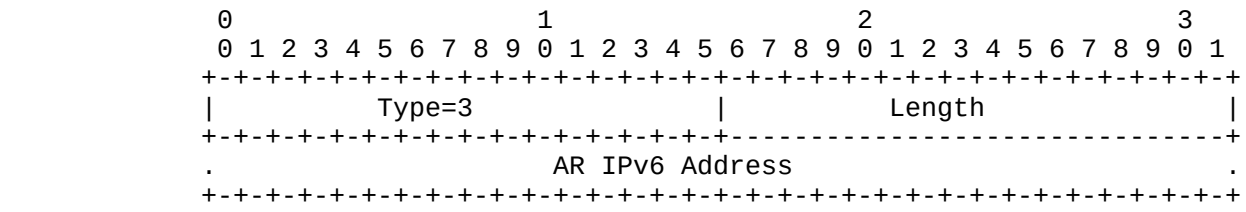


Figure 12: AR IPv6 Address Sub-Element

Type: 3 for AR IPv6 Address

Length: 16

AR IPv6 Address: 128-bit integer containing AR IPv6 Address

3.1.4. AR IPv6 Address for Load-balance Sub-Element

This Sub-Element (see Figure 13) is used to satisfy load-balance and reliability requirements. There may be multiple AR addresses available for a WTP and provided by an AC. A WTP can use the AR information to send user traffic.

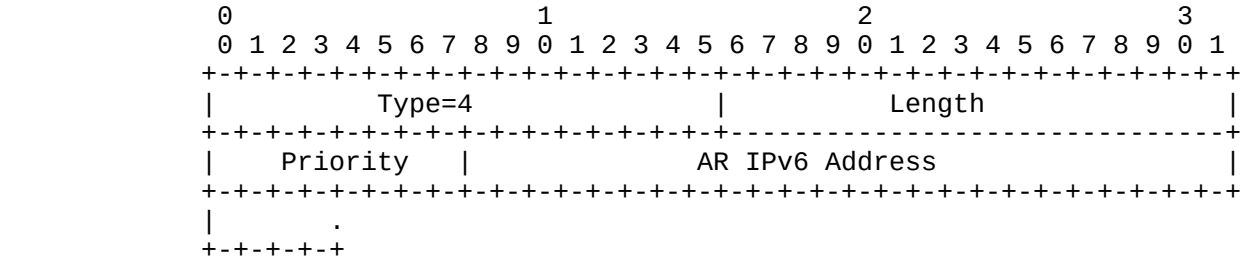


Figure 13: AR IPv6 Address for Load-balance Sub-Element

Type: 4 for AR IPv6 Address for Load-balance

Length:>= 17

Priority: A value between 1 and 255 specifying the priority order of the preferred AR. For instance, the value of one (1) is used to set the primary AR, the value of two (2) is used to set the secondary; two instances with the same value are used for load-balance, etc.

AR IPv6 Address: 128-bit integer containing AR IPv6 Address binding with the specific priority. There may be an array of pairs binding priority and AR IPv6 address.

3.1.5. AR FQDN Sub-Element

This Sub-Element (see Figure 14) is used by the AC to configure a WTP with AR FQDN available to establish the data tunnel for user traffic. Based on the FQDN, a WTP can acquire the AR IP address via DNS.

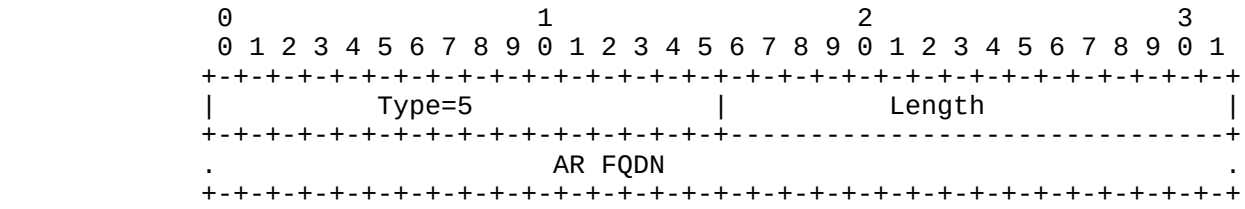


Figure 14: AR FQDN Sub-Element

Type: 5 for AR FQDN

Length:>=1

AR FQDN: A variable-length string containing the AR FQDN.

3.1.6. AR FQDN for Load-balance Sub-Element

This Sub-Element (see Figure 15) is used to satisfy load-balance and reliability requirements. There may be multiple AR FQDNs available for a WTP and provided by an AC. A WTP can use the AR information to send user traffic.

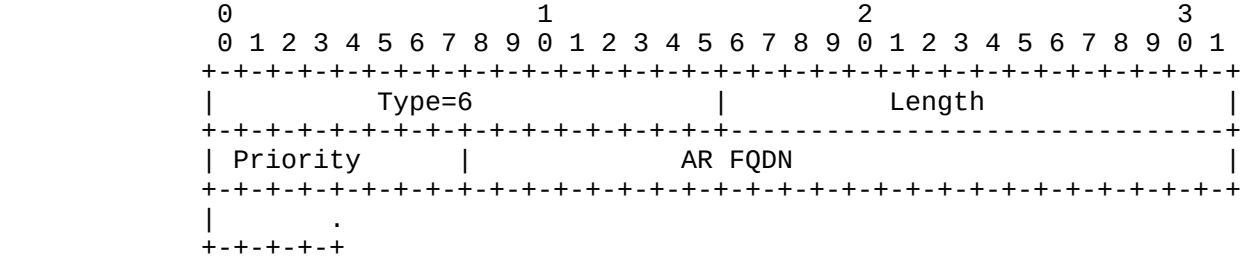


Figure 15: AR FQDN for Load-balance Sub-Element

Type: 6 for AR FQDN for Load-balance

Prefer: A value between 1 and 255 specifying the priority order of the preferred AR. For instance, the value of one (1) is used to set the primary AR, the value of two (2) is used to set the secondary; two instances with the same value are used for load-balance, etc.

AR FQDN: Variable-length string containing AR FQDN binding with the specific priority. There may be an array of pairs binding priority and AR FQDN.

3.2. Tunnel DTLS Policy Sub-Element

The AC distributes its DTLS usage policy for the CAPWAP data tunnel between a WTP and the AR. There are multiple supported options, represented by the bit field below as defined in AC Descriptor message elements. The WTP MUST abide by one of the options for tunneling user traffic with AR. The Tunnel DTLS Policy Sub-Element obey the definition in [RFC5415]. If there are more than one ARs information provided by the AC for reliability reasons, the same Tunnel DTLS Policy (see Figure 16) is generally applied for all tunnels associated with the ARs. Otherwise, Tunnel DTLS Policy MUST be bonding together with each of the ARs, then WTP will enforce the independent tunnel DTLS policy for each tunnel with a specific AR.

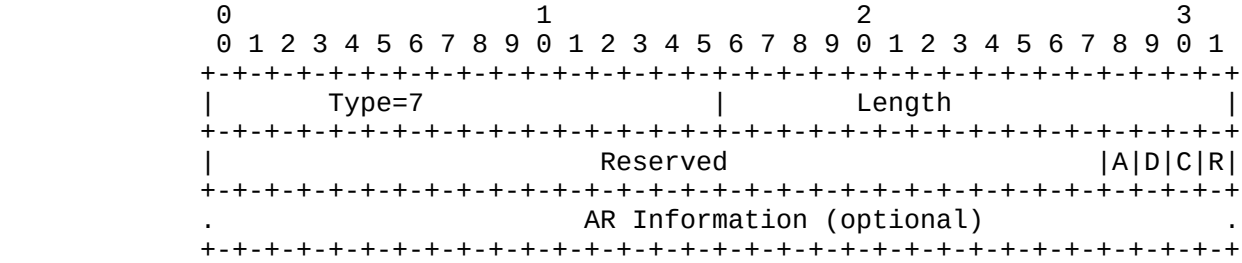


Figure 16: Tunnel DTLS Policy Sub-Element

Type: 7 for Tunnel DTLS Policy

Length: >=6

Reserved: A set of reserved bits for future use. All implementations complying with this protocol MUST set to zero any bits that are reserved in the version of the protocol supported by that implementation. Receivers MUST ignore all bits not defined for the version of the protocol they support.

A: If A bit is set, there is an AR information associated with the DTLS policy. There may be an array of pairs binding DTLS policy information and AR information contained in the Tunnel DTLS Policy Sub-Element. Otherwise, the same Tunnel DTLS Policy (see Figure 16) is generally applied for all tunnels associated with the ARs configured by the AC.

D: DTLS-Enabled Data Channel Supported (see [RFC5415]).

C: Clear Text Data Channel Supported (see [RFC5415]).

R: A reserved bit for future use abide (see [RFC5415]).

3.3. IEEE 802.11 Tagging Mode Policy Sub-Element

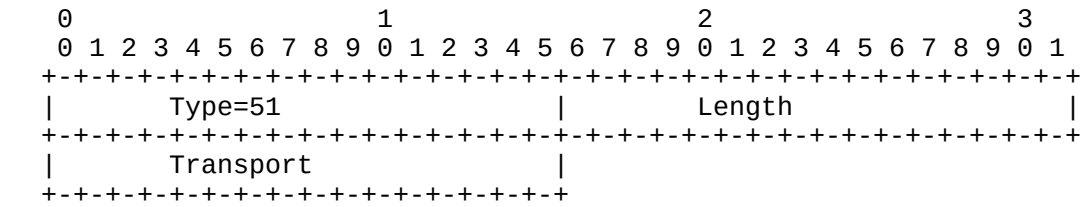
In 802.11 networks, IEEE 802.11 Tagging Mode Policy Sub-Element is used to specify how the WTP apply the QoS tagging policy when receiving the packets from stations on a particular radio. When the WTP sends out the packet to data channel to the AR(s), the packets have to be tagged for QoS purposes (see [RFC5416]).

The IEEE 802.11 Tagging Mode Policy abides the IEEE 802.11 WTP Quality of Service defined in Section 6.22 of [RFC5416].

3.4. CAPWAP Transport Protocol Sub-Element

The CAPWAP data tunnel supports both UDP and UDP-Lite (see [RFC3828]). When run over IPv4, UDP is used for the CAPWAP data channels. When run over IPv6, the CAPWAP data channel may use either UDP or UDP-lite. The AC specifies and configure the WTP for which transport protocol is to be used for the CAPWAP data tunnel.

The CAPWAP Transport Protocol Sub-Element abides the definition in Section 4.6.14 of [RFC5415].



CAPWAP Transport Protocol Sub-Element

Type: 51 for CAPWAP Transport Protocol [RFC5415].

Length: 1

Transport: The transport to use for the CAPWAP Data channel. The following enumerated values are supported:

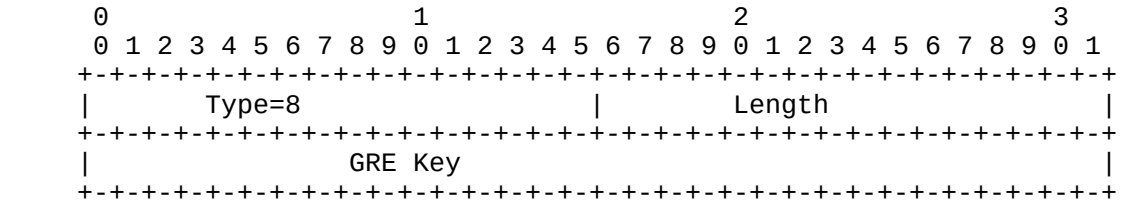
1 - UDP-Lite: The UDP-Lite transport protocol is to be used for the CAPWAP Data channel. Note that this option MUST NOT be used if the CAPWAP Control channel is being used over IPv4 and AR address is IPv4 contained in the AR Information Sub-Element.

2 - UDP: The UDP transport protocol is to be used for the CAPWAP Data channel.

3.5. GRE Key Sub-Element

If a WTP receives the GRE Key Sub-Element in the Alternate Tunnel Encapsulation message element for GREv4 or GREv6 selection, the WTP must insert the GRE Key to the encapsulation packet (see [RFC2890]). An AR acting as decapsulating tunnel endpoint identifies packets belonging to a traffic flow based on the Key value.

The GRE Key Sub-Element field contains a four octet number defined in [RFC2890].



GRE Key Sub-Element

Type: 8 for GRE Key Sub-Element

Length: 4

GRE Key: The Key field contains a four octet number which is inserted by the WTP according to [RFC2890].

4. IANA Considerations

To be specified in later versions.

5. Security Considerations

To be specified in later versions.

6. References

6.1. Normative References

[RFC1701] Hanks, S., Li, T., Farinacci, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 1701, October 1994.

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

[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.

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

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

[RFC2890] Dommety, G., "Key and Sequence Number Extensions to GRE", RFC 2890, September 2000.

[RFC3828] Larzon, L-A., Degermark, M., Pink, S., Jonsson, L-E., and G. Fairhurst, "The Lightweight User Datagram Protocol (UDP-Lite)", RFC 3828, July 2004.

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

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[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.

6.2. 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-03 (work in progress), September 2014.

Authors' Addresses

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

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

Email: xueli@huawei.com

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

Email: john.kaippallimalil@huawei.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