Internet Engineering Task Force (IETF)
Request for Comments: 8350
Category: Experimental
ISSN: 2070-1721

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

April 2018

Alternate Tunnel Encapsulation for Data Frames in Control and Provisioning of Wireless Access Points (CAPWAP)

Abstract

Control and Provisioning of Wireless Access Points (CAPWAP) is a protocol for encapsulating a station's data frames between the Wireless Transmission Point (WTP) and Access Controller (AC). 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, encapsulating data frames to an entity other than the AC (for example, to an Access Router (AR)) is desirable. Furthermore, it may also be desirable to use different tunnel encapsulation modes between the WTP and the Access Router. This document defines an extension to the CAPWAP protocol that supports this capability 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, or CAPWAP. The WTP may advertise support for alternate tunnel encapsulation during the discovery and join process, and the AC may select one of the supported alternate tunnel encapsulation types while configuring the WTP.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8350.

Copyright Notice

Table of Contents

1. Introduction

Service Providers are deploying very large Wi-Fi networks containing hundreds of thousands of Access Points (APs), which are referred to as Wireless Transmission Points (WTPs) in Control and Provisioning of Wireless Access Points (CAPWAP) terminology [RFC5415]. These networks are designed to carry traffic generated from mobile users. The volume in mobile user traffic is already very large and expected to continue growing rapidly. As a result, operators are looking for scalable solutions that can meet the increasing demand. The scalability requirement can be met by splitting the control/management plane from the data plane. This enables the data plane to scale independent of the control/management plane. This specification provides a way to enable such separation.

CAPWAP [RFC5415] [RFC5416] defines a tunnel mode that describes how the WTP handles the data plane (user traffic). The following types are defined:

- Local Bridging: All data frames are locally bridged.
- IEEE 802.3 Tunnel: All data frames are tunneled to the Access Controller (AC) in IEEE 802.3 format.
- IEEE 802.11 Tunnel: All data frames are tunneled to the AC in IEEE 802.11 format.

Figure 1 describes a system with Local Bridging. The AC is in a centralized location. The data plane is locally bridged by the WTPs; this leads to a system with a centralized control plane and a distributed data plane. This system has two benefits: 1) it reduces the scale requirement on the data traffic handling capability of the AC, and 2) it leads to more efficient/optimal routing of data traffic while maintaining centralized control/management.

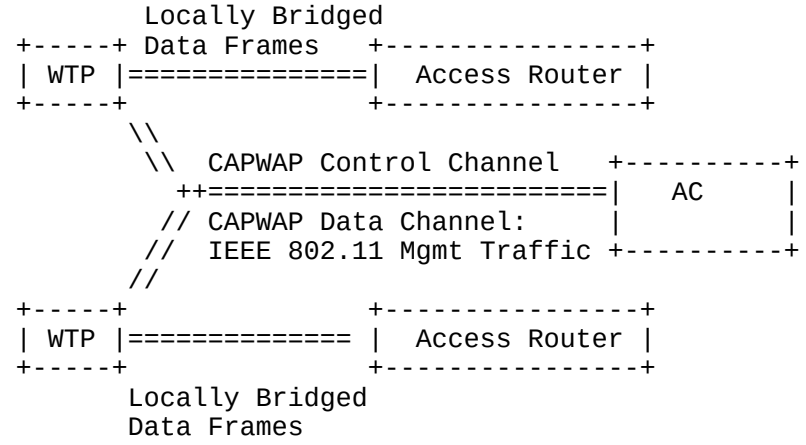

Figure 1: Centralized Control with Distributed Data

The AC handles control of WTPs. In addition, the AC also handles the IEEE 802.11 management traffic to/from the stations. There is a CAPWAP Control and Data Channel between the WTP and the AC. Note that even though there is no user traffic transported between the WTP and AC, there is still a CAPWAP Data Channel. The CAPWAP Data Channel carries the IEEE 802.11 management traffic (like IEEE 802.11 Action Frames).

Figure 2 shows a system where the tunnel mode is configured to tunnel data frames between the WTP and the AC using either the IEEE 802.3 Tunnel or 802.11 Tunnel configurations. Operators deploy this configuration when they need to tunnel the user traffic. The tunneling requirement may be driven by the need to apply policy at the AC. This requirement could be met in the locally bridged system (Figure 1) if the Access Router (AR) implemented the required policy. However, in many deployments, the operator managing the WTP is different than the operator managing the Access Router. When the operators are different, the policy has to be enforced in a tunnel termination point in the WTP operator's network.

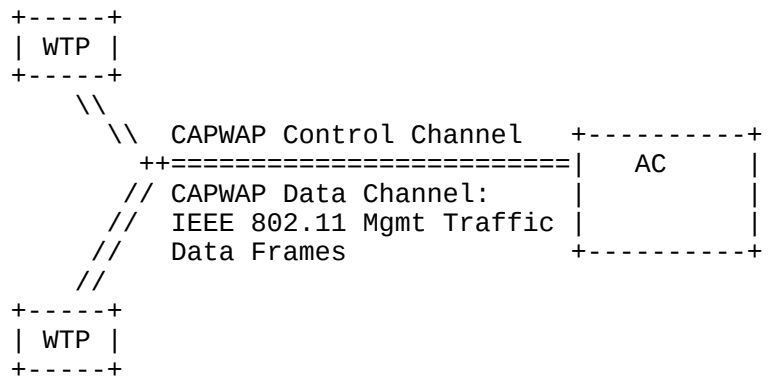

Figure 2: Centralized Control and Centralized Data

The key difference with the locally bridged system is that the data frames are tunneled to the AC instead of being locally bridged. There are two shortcomings with the system in Figure 2: 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]).

Figure 3 shows a system where the WTP tunnels data frames to an alternate entity different from the AC. The WTP also uses an alternate tunnel encapsulation such as Layer 2 Tunneling Protocol (L2TP), L2TPv3, IP-in-IP, IP/GRE, etc. This enables 1) independent scaling of data plane and 2) leveraging of commonly used tunnel encapsulations such as L2TP, GRE, etc.

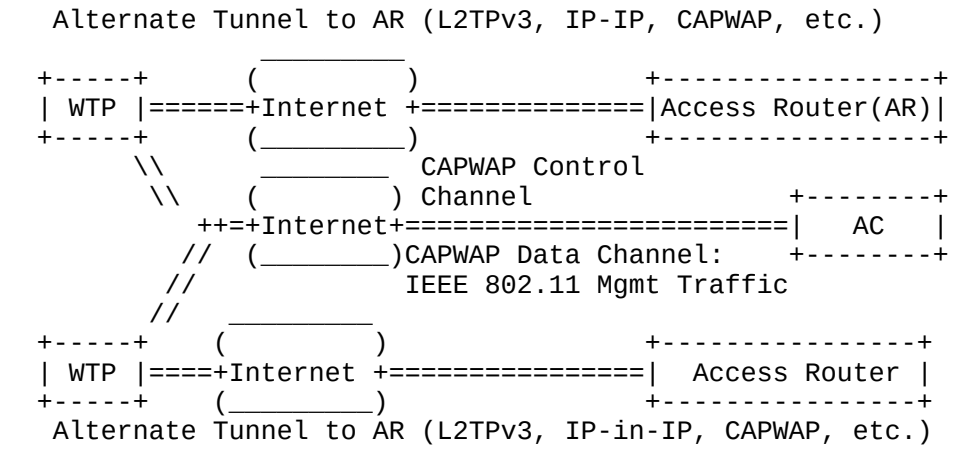

Figure 3: Centralized Control with an Alternate Tunnel for Data

The WTP may support widely used encapsulation types such as L2TP, L2TPv3, IP-in-IP, IP/GRE, etc. The WTP advertises the different alternate tunnel encapsulation types it can support. The AC configures one of the advertised types. As is shown in Figure 3, there is a CAPWAP Control and Data Channel between the WTP and AC. The CAPWAP Data Channel carries the stations' management traffic, as in the case of the locally bridged system. The main reason to maintain a CAPWAP Data Channel is to maintain similarity with the locally bridged system. The WTP maintains three tunnels: CAPWAP Control, CAPWAP Data, and another alternate tunnel for the data frames. The data frames are transported by an alternate tunnel between the WTP and a tunnel termination point, such as an Access Router. This specification describes how the alternate tunnel can be established. The specification defines message elements for the WTP to advertise support for alternate tunnel encapsulation, for the AC to configure alternate tunnel encapsulation, and for the WTP to report failure of the alternate tunnel.

The alternate tunnel encapsulation also supports the third-party WLAN service provider scenario (i.e., Virtual Network Operator (VNO)). Under this scenario, the WLAN provider owns the WTP and AC resources while the VNOs can rent the WTP resources from the WLAN provider for network access. The AC belonging to the WLAN service provider manages the WTPs in the centralized mode.

As shown in Figure 4, VNO 1 and VNO 2 don't possess the network access resources; however, they provide services by acquiring resources from the WLAN provider. Since 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, SSID1 is advertised by the WTP for VNO 1 while SSID2 is advertised by the WTP for VNO 2. Therefore, the data traffic from the user can be directly steered to the corresponding Access Router of the VNO who owns that user. As is shown in Figure 4, AC can notify multiple AR addresses for load balancing or redundancy.

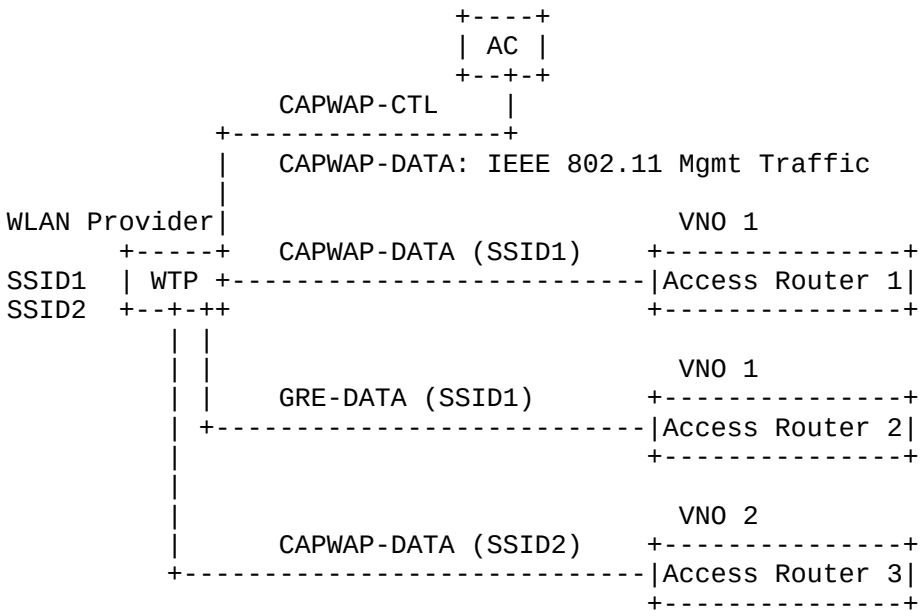

Figure 4: Third-Party WLAN Service Provider

1.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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.

Access Router (AR): A specialized router usually residing at the edge or boundary of a network. This router ensures the connectivity of its network with external networks, a wide area network, or the Internet.

Wireless Termination Point (WTP): The physical or network entity that contains a Radio Frequency (RF) antenna and wireless Physical layer (PHY) to transmit and receive station traffic for wireless access networks.

CAPWAP Control Channel: A bidirectional 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 bidirectional 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. In certain WTP modes, the CAPWAP Data Channel only transports IEEE 802.11 management frames and not the data plane (user traffic).

1.3. History of the Document

This document was started to accommodate Service Providers' need of a more flexible deployment mode with alternative tunnels [RFC7494]. Experiments and tests have been done for this alternate tunnel network infrastructure. However important, the deployment of relevant technology is yet to be completed. This Experimental document is intended to serve as an archival record for any future work on the operational and deployment requirements.

2. Alternate Tunnel Encapsulation Overview

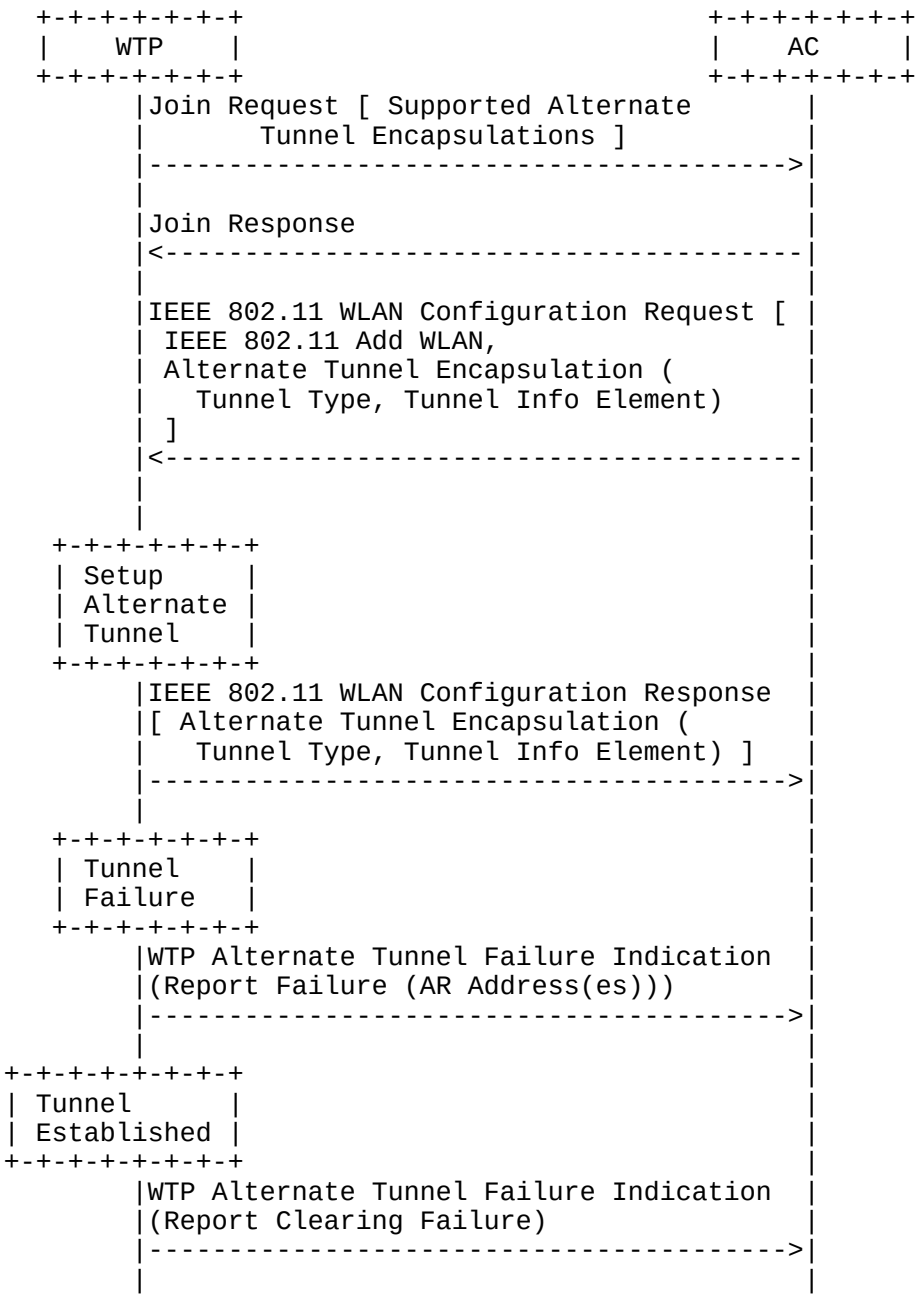

Figure 5: Setup of an Alternate Tunnel

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 Encapsulations Type 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 Encapsulations Type message element.

Since an AC can configure a WTP with more than one AR available for the WTP to establish the data tunnel(s) for user traffic, it may be useful for the WTP to communicate the selected AR. To enable this, the IEEE 802.11 WLAN Configuration Response may carry the Alternate Tunnel Encapsulations Type message element containing the AR list element corresponding to the selected AR as shown in Figure 5.

On detecting a tunnel failure, the WTP SHALL forward data frames to the AC and discard the frames. In addition, the WTP may dissociate existing clients and refuse association requests from new clients. Depending on the implementation and deployment scenario, the AC may choose to reconfigure the WLAN (on the WTP) to a Local Bridging mode or to tunnel frames to the AC. When the WTP detects an alternate tunnel failure, the WTP informs the AC using a message element, IEEE 802.11 WTP Alternate Tunnel Failure Indication (defined in Section 3.3). It MAY be carried in the WTP Event Request message, which is defined in [RFC5415].

The WTP also needs to notify the AC of which AR(s) are unavailable. Particularly, in the VNO scenario, the AC of the WLAN service provider needs to maintain the association of the AR addresses of the VNOs and SSIDs and provide this information to the WTP for the purpose of load balancing or master-slave mode.

The message element has a Status field that indicates whether the message is reporting a failure or clearing the previously reported failure.

For the case where an AC is unreachable but the tunnel endpoint is still reachable, the WTP behavior is up to the implementation. For example, the WTP could choose to either tear down the alternate tunnel or let the existing user’s traffic continue to be tunneled.

3. Extensions for CAPWAP Protocol Message Elements

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:

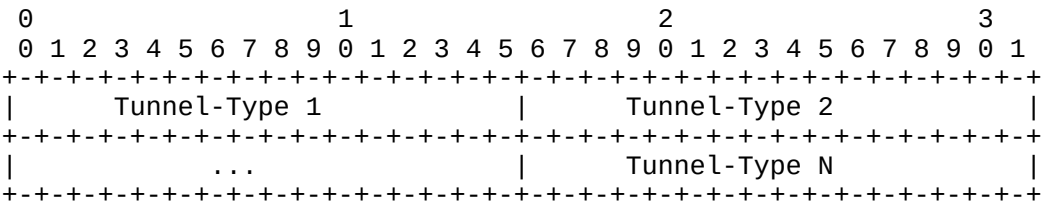

Figure 6: Supported Alternate Tunnel Encapsulations

- Type: 54 for Supported Alternate Tunnel Encapsulations Type
- Length: The length in bytes; two bytes for each Alternative Tunnel-Type that is included
- Tunnel-Type: This is identified by the value defined in Section 3.2. There may be one or more Tunnel-Types, as is shown in Figure 6.

3.2. Alternate Tunnel Encapsulations Type

This message element can be sent by the AC, allows the AC to select the alternate tunnel encapsulation, and 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). Besides, the message element can also be sent by the WTP to communicate the selected AR(s).

The message element contains the following fields:

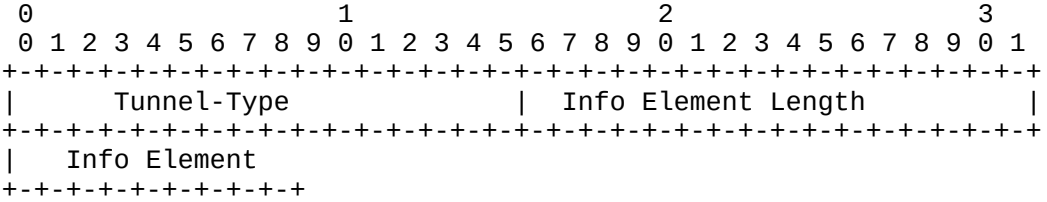

Figure 7: Alternate Tunnel Encapsulations Type

- Type: 55 for Alternate Tunnel Encapsulations Type

- Length: > 4

- Tunnel-Type: The Tunnel-Type is specified by a 2-byte value. This specification defines the values from 0 to 6 as given below. The remaining values are reserved for future use.

  * 0: CAPWAP. This refers to a CAPWAP Data Channel described in [RFC5415] and [RFC5416].

  * 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-UDP. This refers to the UDP encapsulation mode for Proxy Mobile IPv6 (PMIPv6) described in [RFC5844]. This encapsulation mode is the basic encapsulation mode and does not include the TLV header specified in Section 7.2 of [RFC5845].

  * 5: GRE. This refers to GRE tunnel encapsulation as described in [RFC2784].

  * 6: GTPv1-U. This refers to the GPRS Tunnelling Protocol (GTP) User Plane mode as described in [TS.3GPP.29.281].

- Info Element: This field contains tunnel-specific configuration parameters to enable the WTP to set up the alternate tunnel. This specification provides details for this element for CAPWAP, PMIPv6, and GRE. This specification reserves the tunnel type values for the key tunnel types and defines the most common message elements. It is anticipated that message elements for the other protocols (like L2TPv3) will be defined in other specifications in the future.

3.3. IEEE 802.11 WTP Alternate Tunnel Failure Indication

The WTP MAY include the Alternate Tunnel Failure Indication message in a WTP Event Request message to inform the AC about the status of the alternate tunnel. For the case where the WTP establishes data tunnels with multiple ARs (e.g., under a VNO scenario), the WTP needs to notify the AC of which AR(s) are unavailable. The message element contains the following fields:

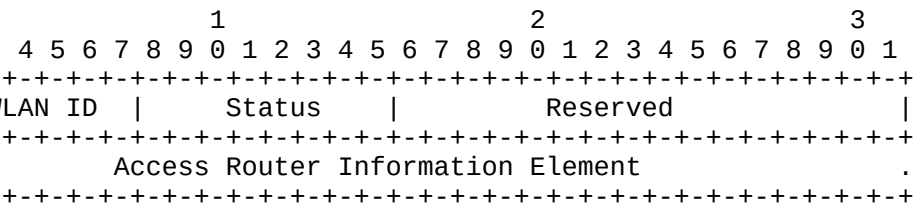

Figure 8: IEEE 802.11 WTP Alternate Tunnel Failure Indication

- Type: 1062 for IEEE 802.11 WTP Alternate Tunnel Failure Indication

- Length: > 4

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

- Status: An 8-bit boolean indicating whether the radio failure is being reported or cleared. A value of 0 is used to clear the event, while a value of 1 is used to report the event.

- Reserved: MUST be set to a value of 0 and MUST be ignored by the receiver.

- Access Router Information Element: The IPv4 or IPv6 address of the Access Router that terminates the alternate tunnel. The Access Router Information Elements allow the WTP to notify the AC of which AR(s) are unavailable.

4. Alternate Tunnel Types

4.1. CAPWAP-Based Alternate Tunnel

If the CAPWAP encapsulation is selected by the AC and configured by the AC to the WTP, the Info Element field defined in Section 3.2 SHOULD contain the following information:

- Access Router Information: The IPv4 or IPv6 address of the Access Router for the alternate tunnel.

- Tunnel DTLS Policy: The CAPWAP protocol allows optional protection of data packets using DTLS. Use of data packet protection on a WTP is not mandatory but is determined by the associated AC policy. (This is consistent with the WTP behavior described in [RFC5415].)

- IEEE 802.11 Tagging Mode Policy: It is used to specify how the CAPWAP Data Channel packets are to be tagged for QoS purposes (see [RFC5416] for more details).

- 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 9:

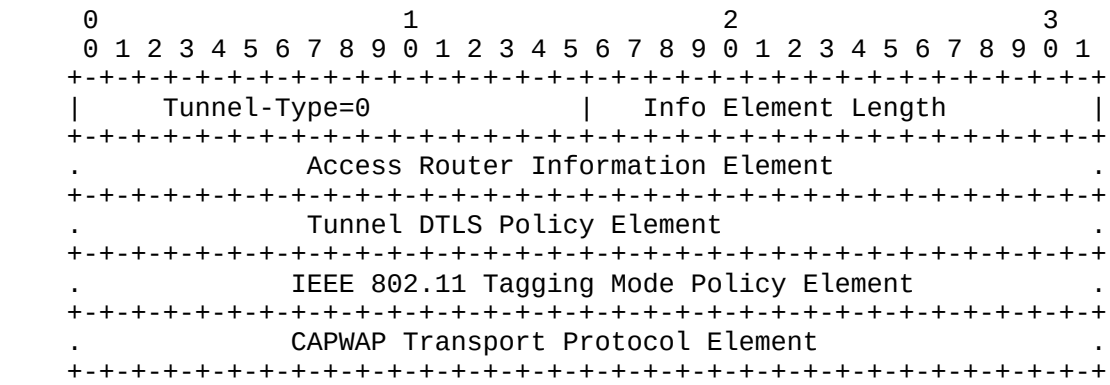

Figure 9: Alternate Tunnel Encapsulation - CAPWAP

4.2. PMIPv6-Based Alternate Tunnel

A user plane based on PMIPv6 (defined in [RFC5213]) can also be used as an alternate tunnel encapsulation between the WTP and the AR. In this scenario, a WTP acts 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 is at the AR. If PMIPv6 UDP encapsulation is selected by the AC and configured by the AC to a WTP, the Info Element field defined in Section 3.2 SHOULD contain the following information:

- Access Router (acting as LMA) Information: IPv4 or IPv6 address for the alternate tunnel endpoint.

The message element structure for PMIPv6 encapsulation is shown in Figure 10:

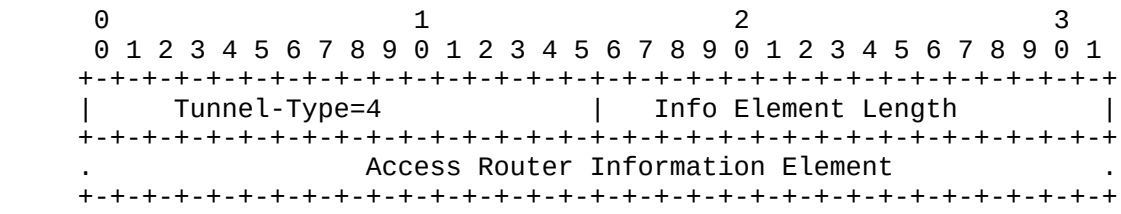

Figure 10: Alternate Tunnel Encapsulation - PMIPv6

4.3. GRE-Based Alternate Tunnel

A user plane based on Generic Routing Encapsulation (defined in [RFC2784]) can also be used as an alternate tunnel encapsulation between the WTP and the AR. In this scenario, a WTP and the Access Router represent the two endpoints of the GRE tunnel. If GRE is selected by the AC and configured by the AC to a WTP, the Info Element field defined in Section 3.2 SHOULD contain the following information:

- Access Router Information: The IPv4 or IPv6 address for the alternate tunnel endpoint.
- GRE Key Information: The Key field is intended to be used for identifying an individual traffic flow within a tunnel [RFC2890].

The message element structure for GRE is shown in Figure 11:

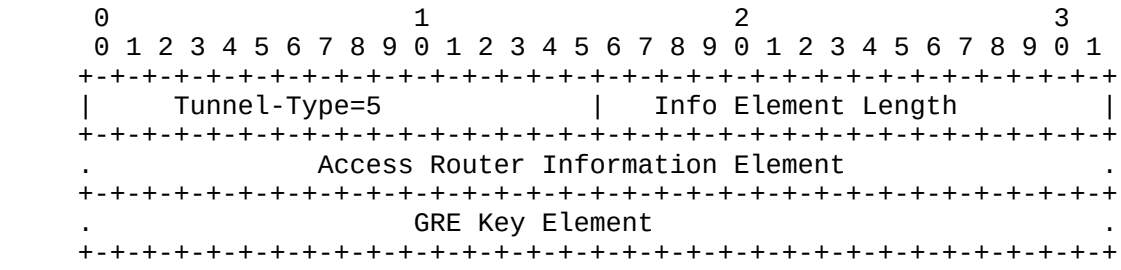

Figure 11: Alternate Tunnel Encapsulation - GRE

5. Alternate Tunnel Information Elements

This section defines the various elements described in Sections 4.1, 4.2, and 4.3.

These information elements can only be included in the Alternate Tunnel Encapsulations Type message element and the IEEE 802.11 WTP Alternate Tunnel Failure Indication message element as their sub-elements.

5.1. Access Router Information Elements

The Access Router Information Elements allow the AC to notify a WTP of which AR(s) are available for establishing a data tunnel. The AR information may be an IPv4 or IPv6 address. For any Tunnel-Type, this information element SHOULD be included in the Alternate Tunnel Encapsulations Type message element.

If the Alternate Tunnel Encapsulations Type message element is sent by the WTP to communicate the selected AR(s), this Access Router Information Element SHOULD be included in it.

The following are the Access Router Information Elements defined in this specification. The AC can use one of them to notify the WTP about the destination information of the data tunnel. The Elements containing the AR IPv4 address MUST NOT be used if an IPv6 Data Channel with IPv6 transport is used.

5.1.1. AR IPv4 List Element

This element (see Figure 12) 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.

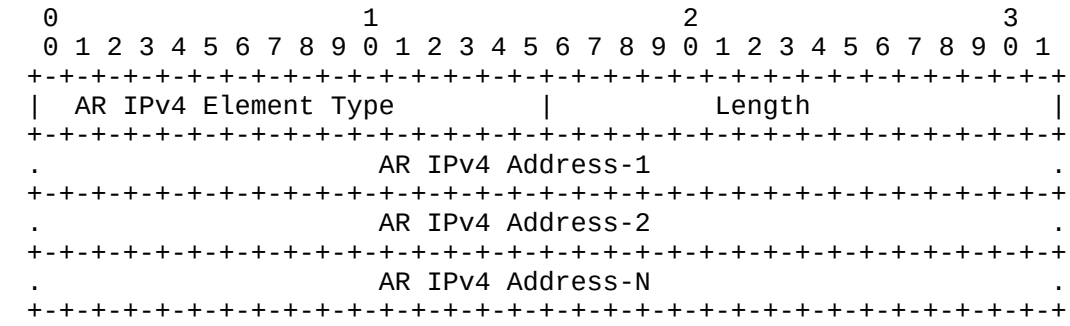

Figure 12: AR IPv4 List Element

Type: 0

Length: This refers to the total length in octets of the element, excluding the Type and Length fields.

AR IPv4 Address: The IPv4 address of the AR. At least one IPv4 address SHALL be present. Multiple addresses may be provided for load balancing or redundancy.

5.1.2. AR IPv6 List Element

This element (see Figure 13) 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.

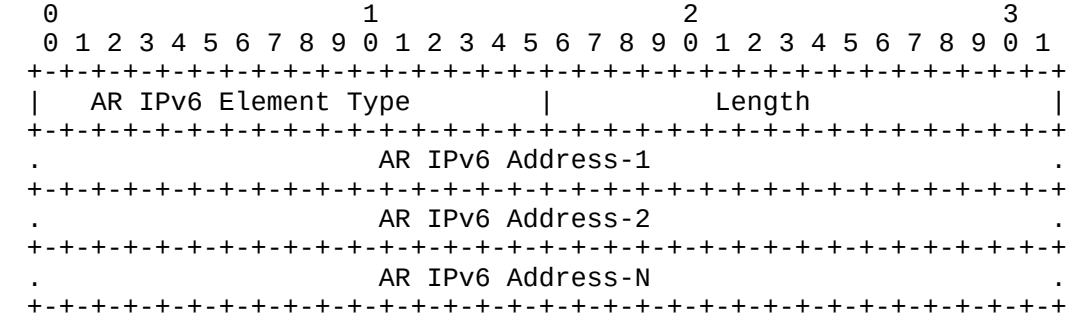

Figure 13: AR IPv6 List Element

Type: 1

Length: This refers to the total length in octets of the element excluding the Type and Length fields.

AR IPv6 Address: The IPv6 address of the AR. At least one IPv6 address SHALL be present. Multiple addresses may be provided for load balancing or redundancy.

5.2. Tunnel DTLS Policy Element

The AC distributes its Datagram Transport Layer Security (DTLS) usage policy for the CAPWAP data tunnel between a WTP and the AR. There are multiple supported options, which are represented by the bit fields 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 Element obeys the definition in [RFC5415]. If, for reliability reasons, the AC has provided more than one AR address in the Access Router Information Element, the same Tunnel

DTLS Policy (the last one in Figure 14) is generally applied for all tunnels associated with those ARs. Otherwise, Tunnel DTLS Policy MUST be bonded together with each of the Access Router Information Elements, and the WTP will enforce the independent tunnel DTLS policy for each tunnel with a specific AR.

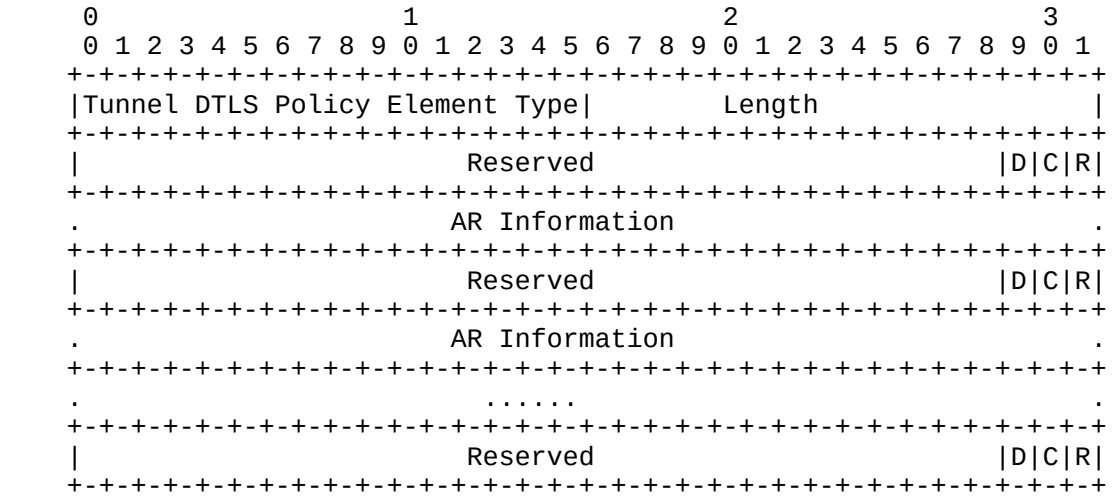

Figure 14: Tunnel DTLS Policy Element

Type: 2

Length: This refers to the total length in octets of the element excluding the Type and Length fields.

Reserved: A set of reserved bits for future use. All implementations complying with this protocol MUST set to 0 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.

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

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

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

AR Information: This means Access Router Information Element. In this context, each address in AR Information MUST be one of previously specified AR addresses.

In Figure 14, the last element that has no AR Information is the default tunnel DTLS policy, which provides options for any address not previously mentioned. Therefore, the AR Information field here is optional. In this element, if all ARs share the same tunnel DTLS policy, there won't be an AR Information field or its specific tunnel DTLS policy.

5.3. IEEE 802.11 Tagging Mode Policy Element

In IEEE 802.11 networks, the IEEE 802.11 Tagging Mode Policy Element is used to specify how the WTP applies 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 by the IEEE 802.11 WTP Quality of Service defined in Section 6.22 of [RFC5416].

If, for reliability reasons, the AC has provided more than one AR address in the Access Router Information Element, the same IEEE 802.11 Tagging Mode Policy (the last one in Figure 15) is generally applied for all tunnels associated with those ARs. Otherwise, IEEE 802.11 Tagging Mode Policy MUST be bonded together with each of the Access Router Information Elements, and the WTP will enforce the independent IEEE 802.11 Tagging Mode Policy for each tunnel with a specific AR.

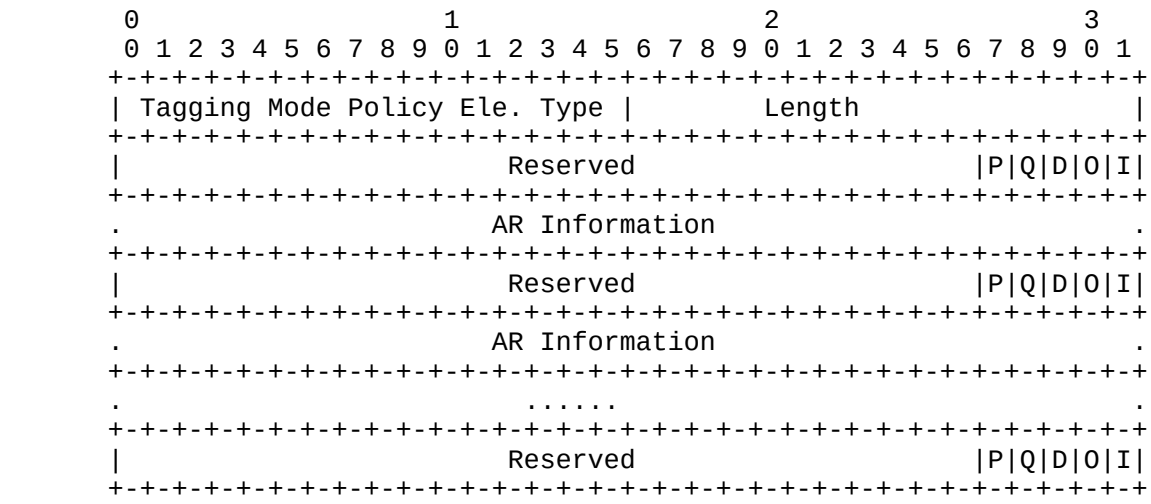

Figure 15: IEEE 802.11 Tagging Mode Policy Element

Type: 3

Length: This refers to the total length in octets of the element excluding the Type and Length fields.

Reserved: A set of reserved bits for future use.

P: When set, the WTP is to employ the IEEE 802.1p QoS mechanism (see [RFC5416]).

Q: When the 'P' bit is set, the 'Q' bit is used by the AC to communicate to the WTP how IEEE 802.1p QoS is to be enforced (see [RFC5416]).

D: When set, the WTP is to employ the DSCP QoS mechanism (see [RFC5416]).

O: When the 'D' bit is set, the 'O' bit is used by the AC to communicate to the WTP how Differentiated Services Code Point (DSCP) QoS is to be enforced on the outer (tunneled) header (see [RFC5416]).

I: When the 'D' bit is set, the 'I' bit is used by the AC to communicate to the WTP how DSCP QoS is to be enforced on the station's packet (inner) header (see [RFC5416]).

AR Information: This means Access Router Information Element. In this context, each address in AR information MUST be one of the previously specified AR addresses.

In Figure 15, the last element that has no AR information is the default IEEE 802.11 Tagging Mode Policy, which provides options for any address not previously mentioned. Therefore, the AR Information field here is optional. If all ARs share the same IEEE 802.11 Tagging Mode Policy, in this element, there will not be an AR Information field and its specific IEEE 802.11 Tagging Mode Policy.

5.4. CAPWAP Transport Protocol 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 configures the WTP for which the transport protocol is to be used for the CAPWAP data tunnel.

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

If, for reliability reasons, the AC has provided more than one AR address in the Access Router Information Element, the same CAPWAP Transport Protocol (the last one in Figure 16) is generally applied for all tunnels associated with those ARs. Otherwise, CAPWAP Transport Protocol MUST be bonded together with each of the Access Router Information Elements, and the WTP will enforce the independent CAPWAP Transport Protocol for each tunnel with a specific AR.

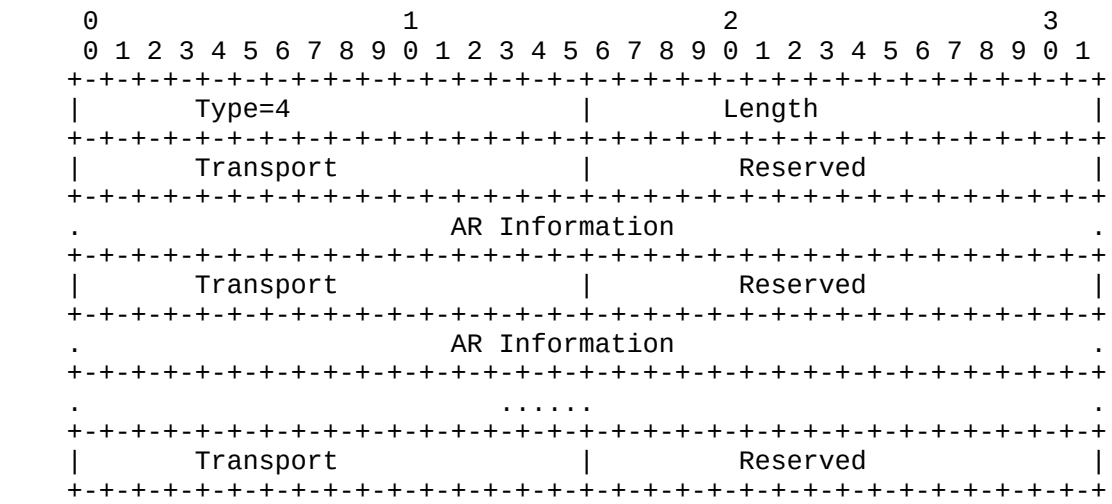

Figure 16: CAPWAP Transport Protocol Element

Type: 4

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 if the AR address contained in the AR Information Element is an IPv4 address.

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

AR Information: This means Access Router Information Element. In this context, each address in AR information MUST be one of the previously specified AR addresses.

In Figure 16, the last element that has no AR information is the default CAPWAP Transport Protocol, which provides options for any address not previously mentioned. Therefore, the AR Information field here is optional. If all ARs share the same CAPWAP Transport Protocol, in this element, there will not be an AR Information field and its specific CAPWAP Transport Protocol.

5.5. GRE Key Element

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

The GRE Key Element field contains a 4-octet number defined in [RFC2890].

If, for reliability reasons, the AC has provided more than one AR address in the Access Router Information Element, a GRE Key Element MAY be bonded together with each of the Access Router Information Elements, and the WTP will enforce the independent GRE Key for each tunnel with a specific AR.

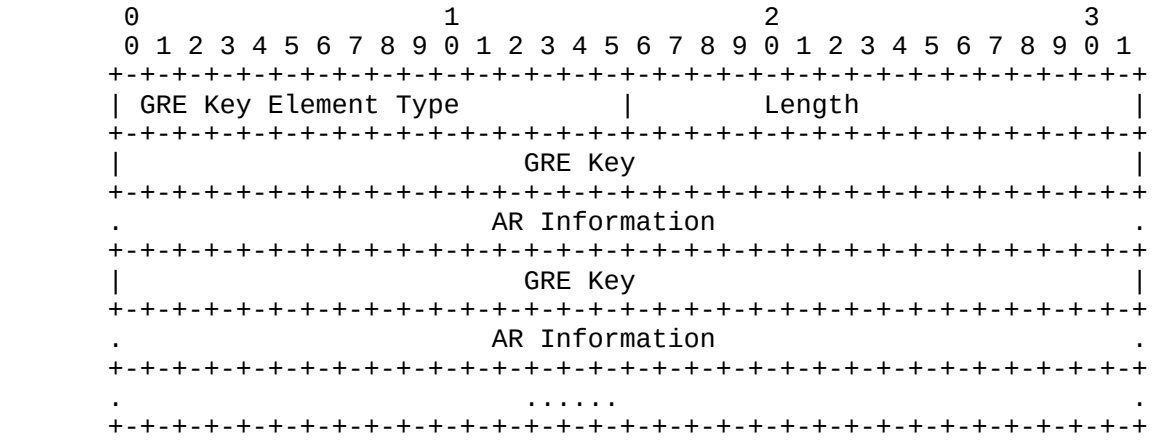

Figure 17: GRE Key Element

Type: 5

Length: This refers to the total length in octets of the element excluding the Type and Length fields.

GRE Key: The Key field contains a 4-octet number that is inserted by the WTP according to [RFC2890].

AR Information: This means Access Router Information Element. In this context, it SHOULD be restricted to a single address and MUST be the address of one of previously specified AR addresses.

Any address not explicitly mentioned here does not have a GRE key.

5.6. IPv6 MTU Element

If AC has chosen a tunneling mechanism based on IPv6, it SHOULD support the minimum IPv6 MTU requirements [RFC8200]. This issue is described in [ARCH-TUNNELS]. AC SHOULD inform the WTP about the IPv6 MTU information in the Tunnel Info Element field.

If, for reliability reasons, the AC has provided more than one AR address in the Access Router Information Element, an IPv6 MTU Element MAY be bonded together with each of the Access Router Information Elements, and the WTP will enforce the independent IPv6 MTU for each tunnel with a specific AR.

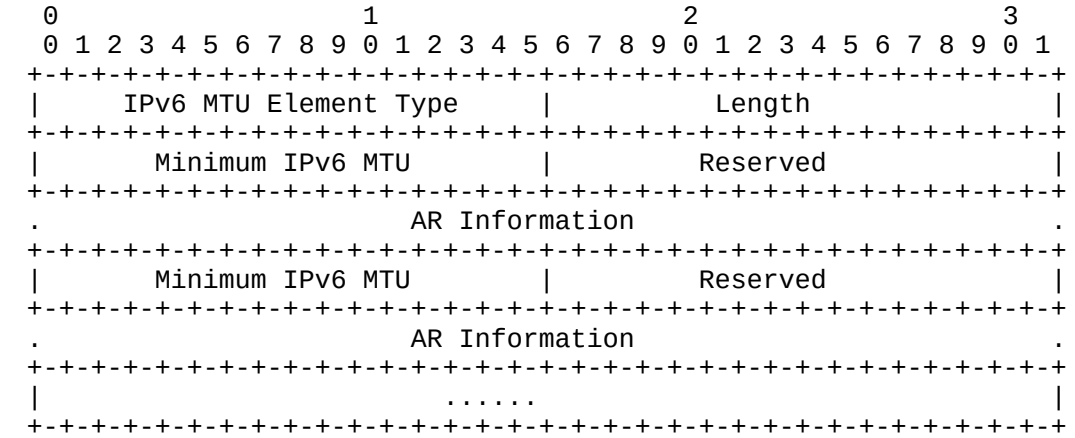

Figure 18: IPv6 MTU Element

Type: 6

Length: This refers to the total length in octets of the element excluding the Type and Length fields.

Minimum IPv6 MTU: The field contains a 2-octet number indicating the minimum IPv6 MTU in the tunnel.

AR Information: This means Access Router Information Element. In this context, each address in AR information MUST be one of previously specified AR addresses.

6. IANA Considerations

Per this document, IANA has registered the following values in the existing "CAPWAP Message Element Type" registry, defined in [RFC5415].

- 54: Supported Alternate Tunnel Encapsulations Type as defined in Section 3.1.
- 55: Alternate Tunnel Encapsulations Type as defined in Section 3.2.
- 1062: IEEE 802.11 WTP Alternate Tunnel Failure Indication as defined in Section 3.3.

Per this document, IANA has created a registry called "Alternate Tunnel-Types" under "CAPWAP Parameters". 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 0 through 6 and can be found in Section 3.2. Future allocations of values in this namespace are to be assigned by IANA using the "Specification Required" policy [RFC8126]. The registry format is given below.

Description	Value	Reference
CAPWAP	0	[RFC5415] [RFC5416]
L2TP	1	[RFC2661]
L2TPv3	2	[RFC3931]
IP-IP	3	[RFC2003]
PMIPv6-UDP	4	[RFC5844]
GRE	5	[RFC2784]
GTPv1-U	6	[TS.3GPP.29.281]

Per this document, IANA has created a registry called "Alternate Tunnel Sub-elements" under "CAPWAP Parameters". This specification defines the Alternate Tunnel Sub-elements. Currently, these information elements can only be included in the Alternate Tunnel Encapsulations Type message element with the IEEE 802.11 WTP Alternate Tunnel Failure Indication message element as its sub-elements. These information elements contain a Type field. The namespace for the field is 16 bits (0-65535). This specification defines values 0 through 6 in Section 5. This namespace is managed by IANA, and assignments require an Expert Review [RFC8126].

Description	Value
AR IPv4 List	0
AR IPv6 List	1
Tunnel DTLS Policy	2
IEEE 802.11 Tagging Mode Policy	3
CAPWAP Transport Protocol	4
GRE Key	5
IPv6 MTU	6

7. Security Considerations

This document introduces three new CAPWAP WTP message elements. These elements are transported within CAPWAP Control messages as the existing message elements. Therefore, this document does not introduce any new security risks to the control plane compared to [RFC5415] and [RFC5416]. In the data plane, if the encapsulation type selected itself is not secured, it is suggested to protect the tunnel by using known secure methods, such as IPsec.

8. References

8.1. Normative References

[RFC2003] Perkins, C., "IP Encapsulation within IP", RFC 2003, DOI 10.17487/RFC2003, October 1996, <https://www.rfc-editor.org/info/rfc2003>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2661] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, DOI 10.17487/RFC2661, August 1999, <https://www.rfc-editor.org/info/rfc2661>.

[RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, DOI 10.17487/RFC2784, March 2000, <https://www.rfc-editor.org/info/rfc2784>.

[RFC2890] Dommety, G., "Key and Sequence Number Extensions to GRE", RFC 2890, DOI 10.17487/RFC2890, September 2000, <https://www.rfc-editor.org/info/rfc2890>.

[RFC3828] Larzon, L-A., Degermark, M., Pink, S., Jonsson, L-E., Ed., and G. Fairhurst, Ed., "The Lightweight User Datagram Protocol (UDP-Lite)", RFC 3828, DOI 10.17487/RFC3828, July 2004, <https://www.rfc-editor.org/info/rfc3828>.

[RFC3931] Lau, J., Ed., Townsley, M., Ed., and I. Goyret, Ed., "Layer Two Tunneling Protocol - Version 3 (L2TPv3)", RFC 3931, DOI 10.17487/RFC3931, March 2005, <https://www.rfc-editor.org/info/rfc3931>.

[RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, DOI 10.17487/RFC5415, March 2009, <https://www.rfc-editor.org/info/rfc5415>.

[RFC5416] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11", RFC 5416, DOI 10.17487/RFC5416, March 2009, <https://www.rfc-editor.org/info/rfc5416>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

8.2. Informative References

[ARCH-TUNNELS]
Touch, J. and M. Townsley, "IP Tunnels in the Internet Architecture", Work in Progress, draft-ietf-intarea-tunnels-08, January 2018.

[RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <https://www.rfc-editor.org/info/rfc5213>.

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, DOI 10.17487/RFC5844, May 2010, <https://www.rfc-editor.org/info/rfc5844>.

[RFC5845] Muhanna, A., Khalil, M., Gundavelli, S., and K. Leung, "Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6", RFC 5845, DOI 10.17487/RFC5845, June 2010, <https://www.rfc-editor.org/info/rfc5845>.

[RFC7494] Shao, C., Deng, H., Pazhyannur, R., Bari, F., Zhang, R., and S. Matsushima, "IEEE 802.11 Medium Access Control (MAC) Profile for Control and Provisioning of Wireless Access Points (CAPWAP)", RFC 7494, DOI 10.17487/RFC7494, April 2015, <https://www.rfc-editor.org/info/rfc7494>.

[TS.3GPP.29.281]
3GPP, "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)", 3GPP TS 29.281, V13.1.0, March 2016.

Contributors

The authors would like to thank Andreas Schultz, Hong Liu, Yifan Chen, Chunju Shao, Li Xue, Jianjie You, Jin Li, Joe Touch, Alexey Melnikov, Kathleen Moriarty, Mirja Kuehlewind, Catherine Meadows, and Paul Kyzivat for their valuable comments.

Authors' Addresses

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

Email: zhangr@gsta.com

Rajesh S. Pazhyannur
Cisco
170 West Tasman Drive
San Jose, CA 95134
United States of America

Email: rpazhyan@cisco.com

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
United States of America

Email: sgundave@cisco.com

Zhen Cao
Huawei
Xinxi Rd. 3
Beijing 100085
China

Email: zhencao.ietf@gmail.com

Hui Deng
Huawei
Xinxi Rd. 3
Beijing 100085
China

Email: denghui02@gmail.com

Zongpeng Du
Huawei
No.156 Beiqing Rd. Z-park, HaiDian District
Beijing 100095
China

Email: duzongpeng@huawei.com