Opsawg Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 21, 2016

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

October 19, 2015

Alternate Tunnel Encapsulation for Data Frames in CAPWAP
draft-ietf-opsawg-capwap-alt-tunnel-06

Abstract

Control And Provisioning of Wireless Access Points (CAPWAP) defines a specification to encapsulate 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. 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.

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/.

Copyright Notice

Table of Contents

1. Introduction

Service Providers are deploying very large Wi-Fi deployments (ranging from hundreds of thousands of Access Points, 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 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.
- 802.3 Tunnel: All data frames are tunneled to the AC in 802.3 format.
- 802.11 Tunnel: All data frames are tunneled to the AC in 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 leading to a system with centralized control plane with distributed data plane. This system has two benefits: 1) reduces the scale requirement on data traffic handling capability of the AC and 2) leads to more efficient/optimal routing of data traffic while maintaining centralized control/management.

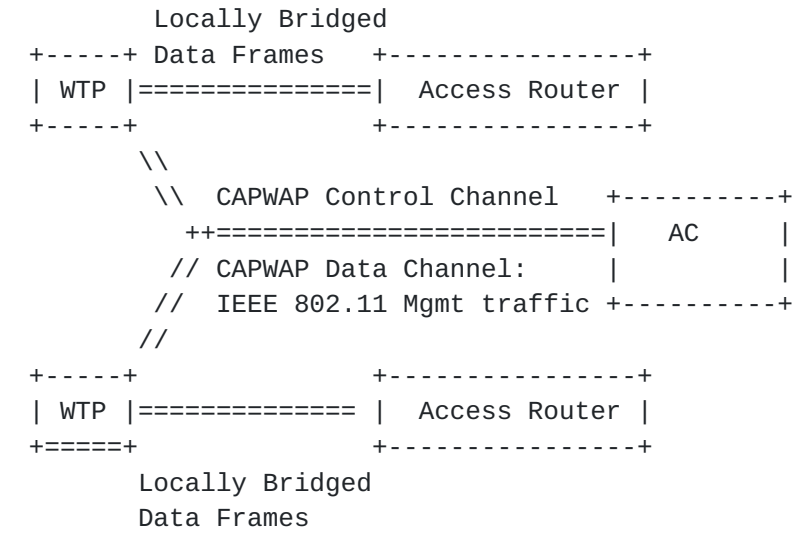

Figure 1: Centralized Control with Distributed Data

The AC handles control of WTPs. In addition, the AC also handles the IEEE 802.11 management traffic to/ from the stations. There is 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 either using 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 Access Router or a legal requirement to support lawful intercept of user traffic. This requirement could be met in the locally bridged system (Figure 1) if the access router 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.

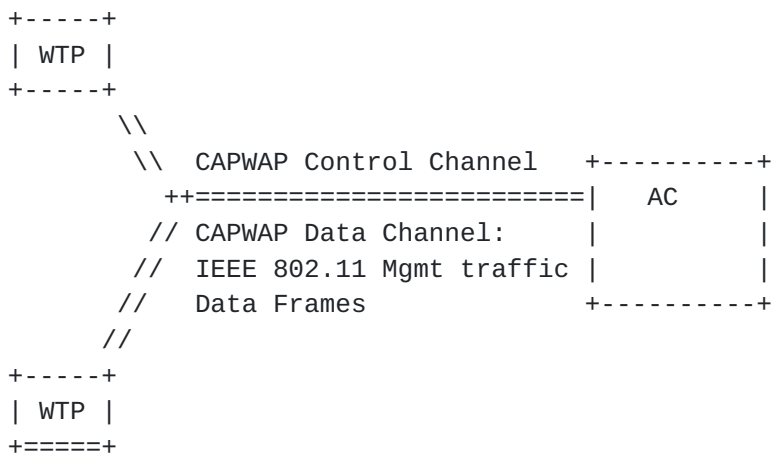

Figure 2: Centralized Control and Centralized Data

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 system in Figure 2. 1) They do not allow the WTP to tunnel data frames to an endpoint different from the AC and 2) They do 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 such as 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

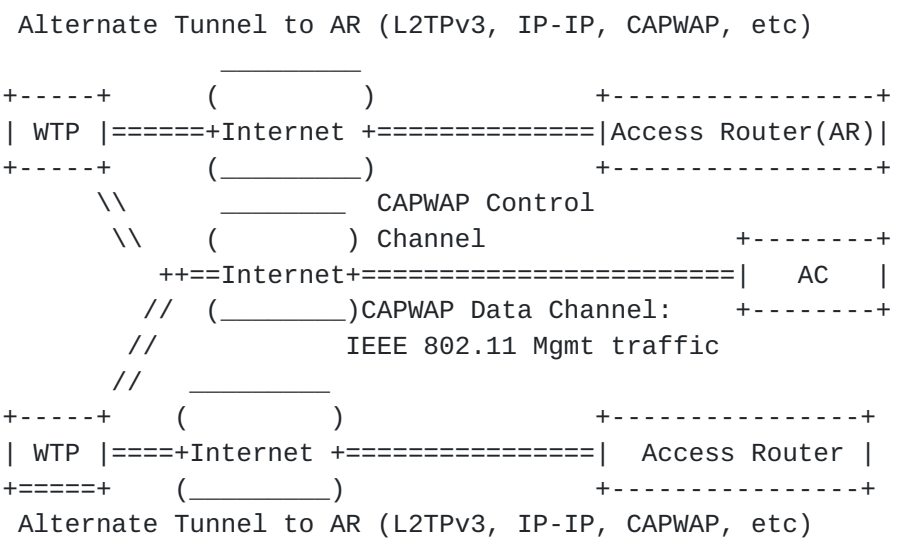

Figure 3: Centralized Control with Alternate Tunnel for Data

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 shown in the figure 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 frame. 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, 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&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 VNO1; while SSID2 is advertised by the WTP for VNO2. Therefore the data traffic from the user can be directly steered to the corresponding access router of the VNO who owns that user.

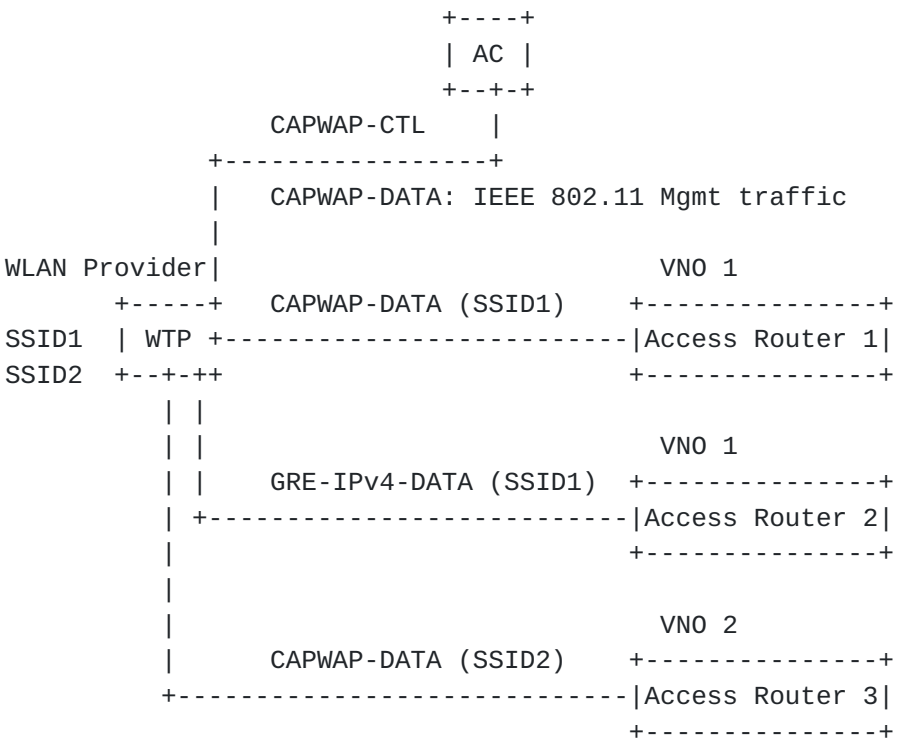

Figure 4: Third-party WLAN Service Provider

1.1. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "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.

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

2. Alternate Tunnel Encapsulation

2.1. Description

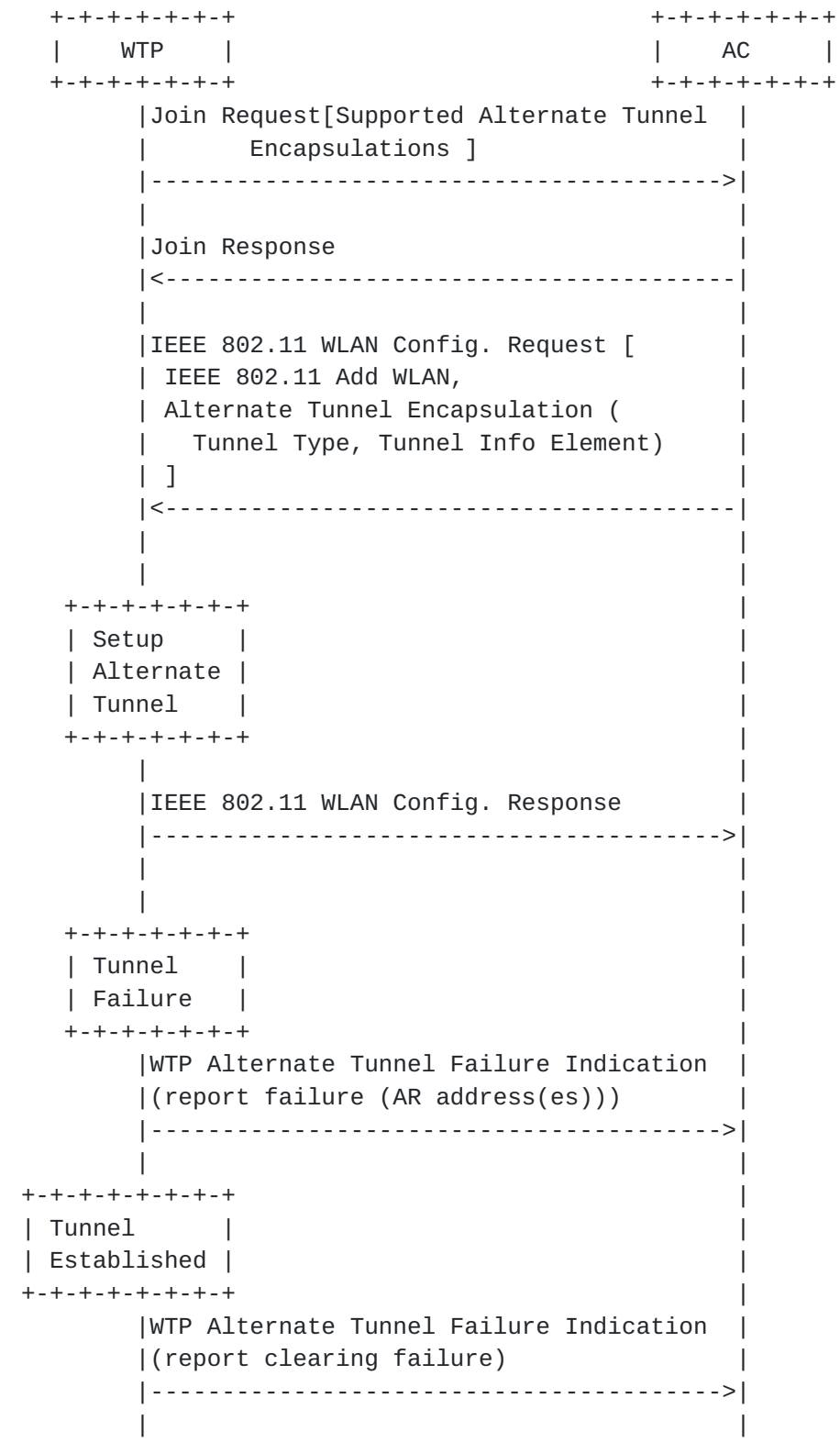

Figure 5: Setup of Alternate Tunnel

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.

On detecting a tunnel failure, WTP shall forward data frames to the AC and discard the frames. In addition, 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, WTP Alternate Tunnel Fail Indication (defined in this specification).

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 denotes reporting a failure or the clearing of the previously reported failure.

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

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:

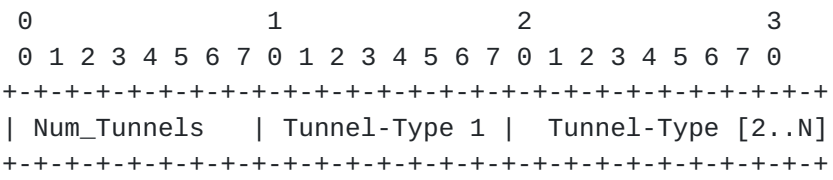

Figure 6: Supported Alternate Tunnel Encapsulations

- 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

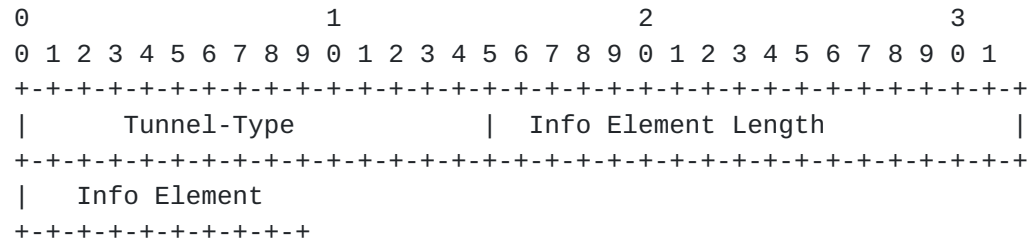

Figure 7: Alternate Tunnel Encapsulations Type

- 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].
  * 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]
  * 5: GRE-IPv4. This refers to GRE encapsulation with IPv4 as the delivery protocol as described in RFC2874.
  * 6: GRE-IPv6. This refers to GRE encapsulation with IPv6 as the delivery protocol as described in RFC2874.

- Info Element: This field contains tunnel specific configuration parameters to enable the WTP to setup the alternate tunnel. This specification provides details for this elements for CAPWAP and PMIPv6. We anticipate that message elements for the other protocols (like L2TPv3, etc) will be defined in other specifications in the future.

3.3. IEEE 802.11 WTP Alternate Tunnel Failure Indication

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

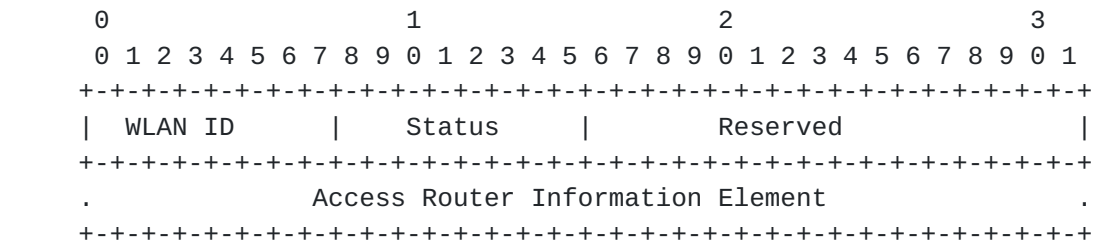

Figure 8: IEEE 802.11 WTP Alternate Tunnel Failure Indication

- Type: <IANA-3> 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 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 Element: IPv4 address or IPv6 address or Fully Qualified Domain Name (FQDN), of the Access Router for the alternate tunnel. The Access Router Information Elements allow the WTP to notify the AC of which AR(s) are unavailable.

3.4. 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: IPv4 address or IPv6 address or Fully Qualified Domain Name (FQDN), 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 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 packet 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:

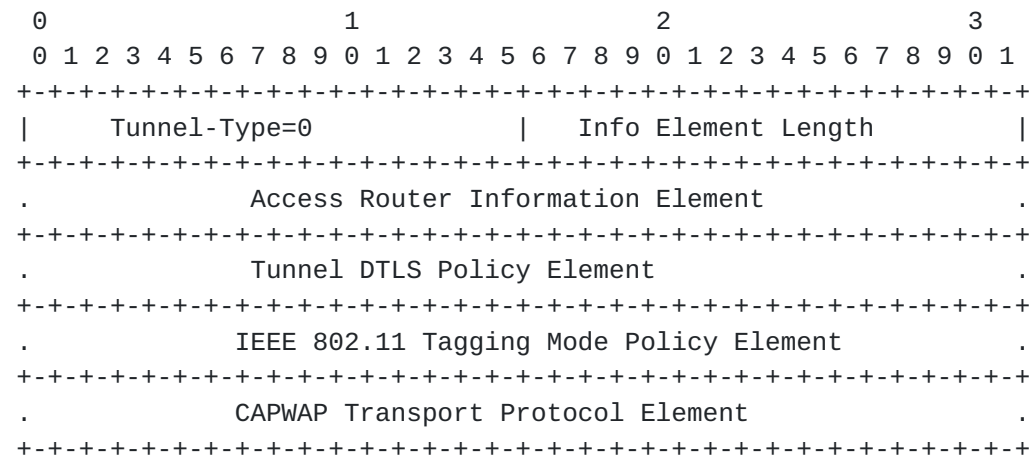

Figure 9: Alternate Tunnel Encapsulation - CAPWAP

3.5. PMIPv6 based Alternate Tunnel

Proxy Mobile IPv6 (PMIPv6) (defined in [RFC5213]) can also be used for 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 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:

o Access Router (acts as LMA) Information: IPv6 address or Fully Qualified Domain Name (FQDN) for the alternate tunnel endpoint.

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

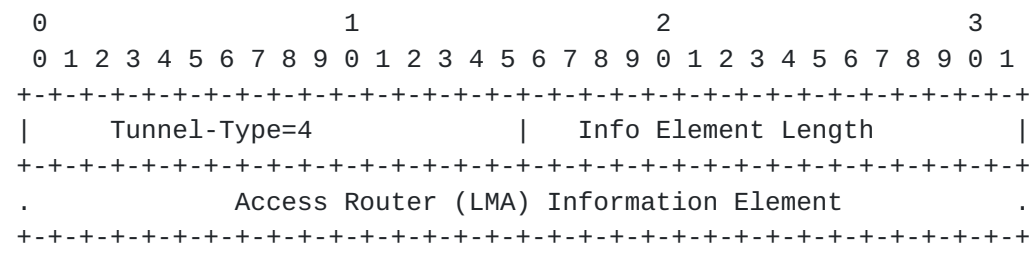

Figure 10: Alternate Tunnel Encapsulation - PMIPv6

3.6. Alternate Tunnel Information Elements

This section defines the various elements described in Section 3.4 and Section 3.5

3.6.1. 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 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 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 Elements containing the AR IPv4 address MUST NOT be used if an IPv6 data channel such as PMIPv6 or GREv6 is used.

3.6.1.1. AR IPv4 List Element

This Element (see Figure 11) 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.

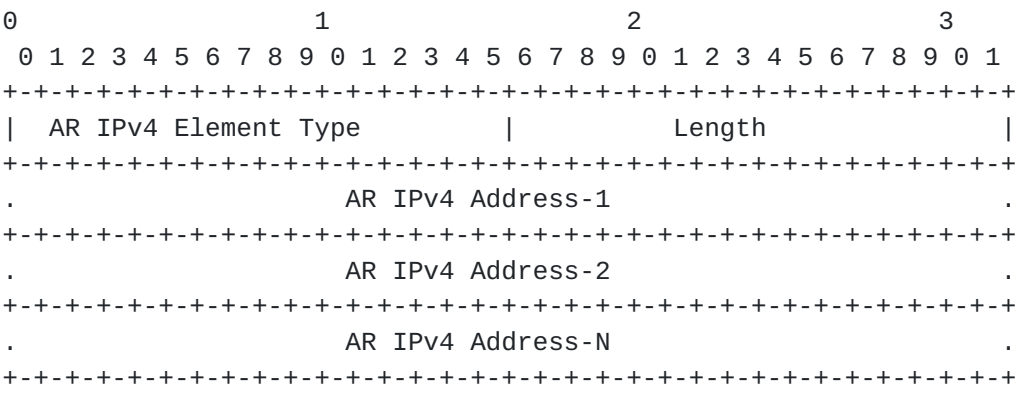

Figure 11: AR IPv4 List Element

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

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

3.6.1.2. AR IPv6 List Element

This 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.

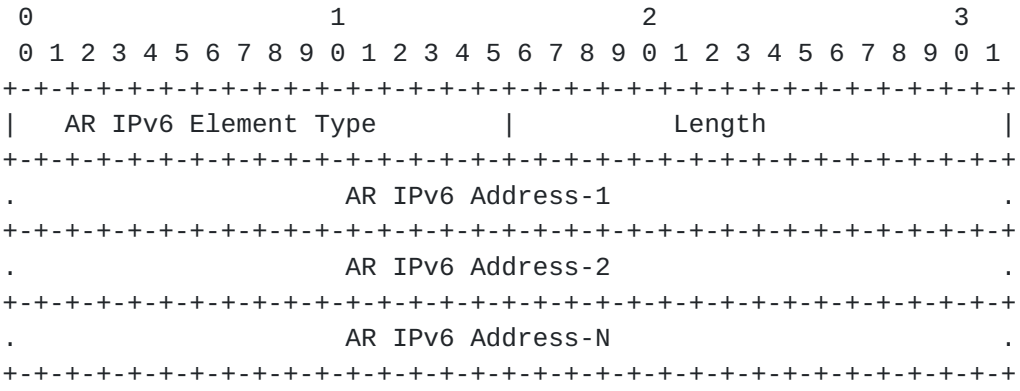

Figure 12: AR IPv6 List Element

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

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

3.6.1.3. AR FQDN List Element

This Element (see Figure 13) 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.

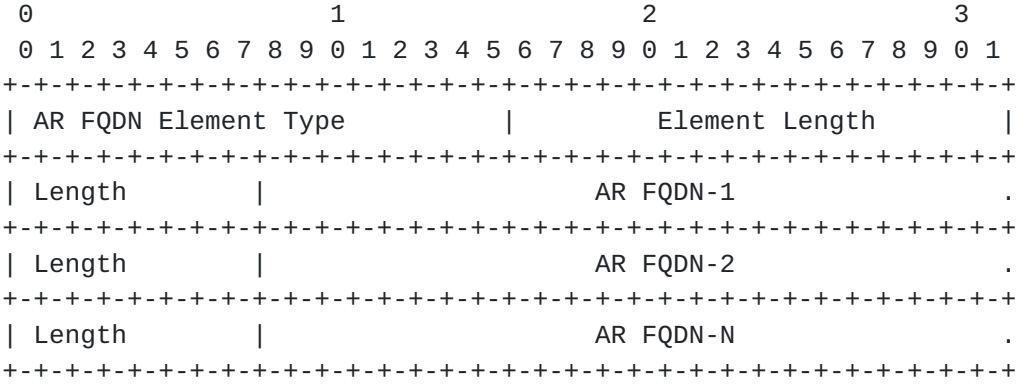

Figure 13: AR FQDN List Element

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

Length: The length of each AR FQDN.

AR FQDN: An array of variable-length string containing AR FQDN. This can be used to satisfy load-balance and reliability requirements.

3.6.2. IEEE 802.11 WLAN Configuration Response

Since 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 contain the AR list element containing the selected AR.

3.6.3. Tunnel DTLS Policy 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 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 14) 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.

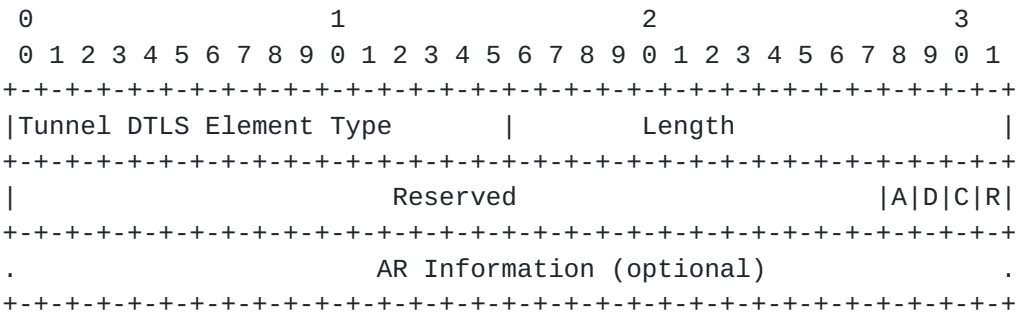

Figure 14: Tunnel DTLS Policy Element

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 Element. Otherwise, the same Tunnel DTLS Policy (see Figure 14) 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]).

3.6.4. IEEE 802.11 Tagging Mode Policy Element

In 802.11 networks, IEEE 802.11 Tagging Mode Policy 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].

3.6.5. 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 configure the WTP for which transport protocol is to be used for the CAPWAP data tunnel.

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

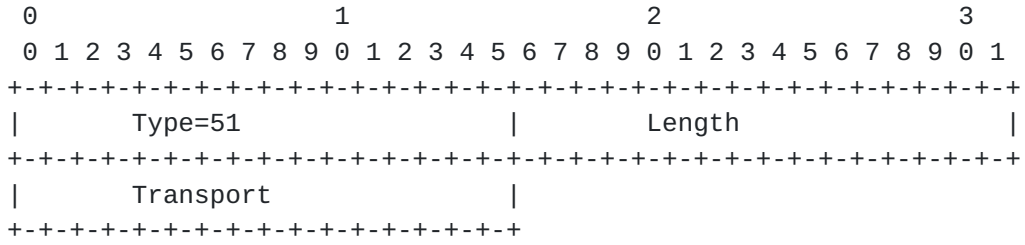

Figure 15: CAPWAP Transport Protocol Element

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 Element.

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

3.6.6. GRE Key Element

If a WTP receives the GRE Key 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 Element field contains a four octet number defined in [RFC2890].

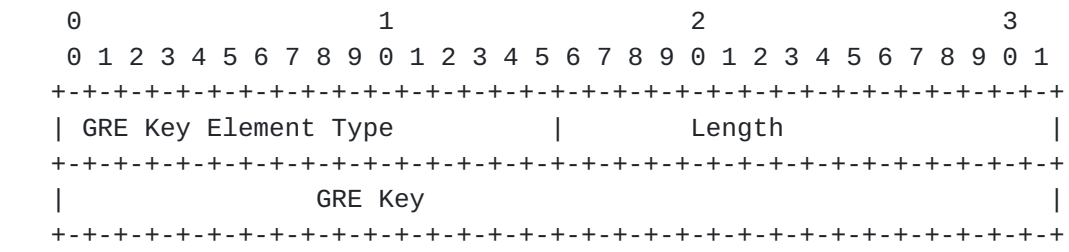

Figure 16: GRE Key Element

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

4. IANA Considerations

This document requires the following IANA considerations.

- o <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]).
- o <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.
- o <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.
- o 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 six (6) and can be found in Section 3.2. Future allocations of values in this name space are to be assigned by IANA using the "Specification Required" policy. IANA needs to create a registry called CAPWAP Alternate Tunnel-Types. The registry format is given below.
- o AR IPv4 Element Type: AR IPv4 List Element (see Figure 11) 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.
- o AR IPv6 Element Type: AR IPv6 List 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.

- o AR FQDN Element Type: AR FQDN Element (see Figure 13) is used by the AC to configure a WTP with AR FQDN available to establish the data tunnel for user traffic.
- o Tunnel DTLS Element Type: The Tunnel DTLS Policy Element obey the definition in [RFC5415].
- o GRE Key Element Type: If a WTP receives the GRE Key Element in the Alternate Tunnel Encapsulation message element for GREv4 or GREv6 selection, the WTP must insert the GRE Key to the encapsulation packet

Tunnel-Type	Type Value	Reference
CAPWAP	0	[RFC5415],[RFC5416]
L2TP	1	[RFC2661]
L2TPv3	2	[RFC3931]
IP-IP	3	[RFC2003]
PMIPv6	4	[RFC5213]
GRE-IPv4	5	[RFC2784]
GRE-IPv6	6	[RFC2784]

5. 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 compared to [RFC5415] and [RFC5416]. In CAPWAP, security for CAPWAP Data Channel is optional and security policy is determined by AC. Similarly, the AC determines the security for the Alternate Tunnel between WTP and Alternate Tunnel Encapsulation Gateway. 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. The authors would like to thank Zongpeng Du and Jin Li for their valuable comments.

7. References

7.1. Normative References

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

[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, <http://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, <http://www.rfc-editor.org/info/rfc2784>.

[RFC2890] Dommety, G., "Key and Sequence Number Extensions to GRE", RFC 2890, DOI 10.17487/RFC2890, September 2000, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc3931>.

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

[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, <http://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, <http://www.rfc-editor.org/info/rfc5416>.

7.2. Informative References

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

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: zhen.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

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

Email: youjianjie@huawei.com