Dynamic Host Configuration
Internet-Draft
Intended status: Standards Track
Expires: 9 May 2024

S. Muthusamy
Y. Lee
R. Kothari
Comcast

6 November 2023

Mobile Subscription Info in DHCP and Router Advertisement
draft-muthusamy-dhc-mobile-sub-info-01

Abstract

In some environments where a mobile client joins a network via simple DHCP process and/or IPv6 Router Advertisement, the serving network may want to know the mobile client's mobile subscription information. This is particularly useful when a mobile client switches to a private Wi-Fi network such as home network which uses simple SSID/ Pre-Shared-Key combination. The network can use the mobile subscription information to identify the client's serving mobile network and provide service continuity.

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 https://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 9 May 2024.

Copyright Notice

Table of Contents

1. Introduction

When a mobile client roams in the range of a known Wi-Fi network, it is common for the mobile client to switch from the mobile network to the Wi-Fi network. The Wi-Fi network may be setup to use simple SSID/Pre-Shared-Key combination (e.g., home private network) and does not require EAP-AKA authentication [RFC4187] for the client to join the network. As such the network will not be able to identify the client's mobile subscription. In an environment where the mobile network and the Wi-Fi network are of the same service provider, the service provider may want to retrieve the mobile subscription information from the client and offer service continuity (e.g., Parental Control) while the client is on the private Wi-Fi network.

In this draft, we define a DHCPv4 [RFC2131] and DHCPv6 [RFC8415] option (Mobile-Sub-Info) and an IPv6 Router Advertisement (RA) [RFC4861] that inform mobile clients to exchange Mobile Subscription Information with the network.

1.1. Requirements Language

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 RFC 2119 [RFC2119] RFC 8174 [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. The Mobile-Subscription Information Option

The Mobile Subscription Information DHCP/RA Option (Mobile-Sub-Info) signals the client that the network wants to obtain the Mobile subscription Information from the client. The option contains a URL the client may use it to securely exchange mobile subscription information with the network. The mechanism is similar to Captive-

Portal Identification in DHCP and Router Advertisements (RAs) defined in [RFC8910]. The Mobile-Sub-Info Option contains a URL that provides a web address to the client to initiate a secure connection to trigger the EAP-AKA process [RFC4187] with the network. The process is outside of the DHCP and RA protocol process that gives flexibility to the client and network to use standard web technology to securely exchange messages. As such, it relaxes the 255-byte length restriction imposed by DHCPv4 option. Upon successful information exchange, the network MAY continue to provide similar mobile network services (e.g., Parental Control) after the client switching from the mobile network to the Wi-Fi network using SSID/PSK combination.

2.1. Client Behavior

Clients that support Mobile-Sub-Info DHCP option SHOULD include the option in the Parameter Request List in DHCPREQUEST message. DHCP server MAY send the Mobile-Sub-Info option without explicit request. Client receives the URL in the option MAY initiate a request to the network to exchange Mobile Subscription Information. Client MAY safely ignore the option either it doesn't support it or its local policy chooses not to respond to the request.

2.2. Server Behavior

To support different types of clients (e.g., IPv4-only, IPv6-only with DHCPv6 and IPv6-only with RA), the network must provide different methods to inform the client of supporting the Mobile-Sub-Info option. The network SHOULD provision identical Mobile-Subscription-URI in each method to avoid ambiguity. As of the maximum length of the URI that can be carried in DHCPv4 is 255 bytes, URIs SHOULD not be longer than 255 bytes. If the network supports only DHCPv6, the restriction can be relaxed. The URL MUST not contain any explicit IP address information.

2.3. The Mobile-Sub-Info IPv4 DHCP Option

The format of the Mobile-Sub-Info DHCP option is shown below.

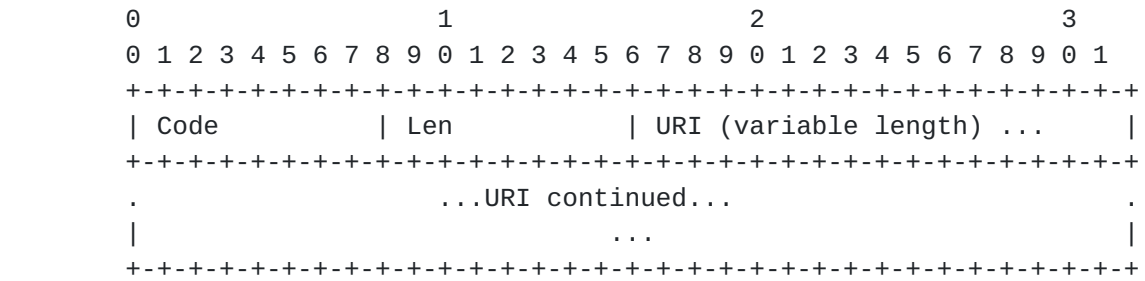

Figure 1: Mobile-Sub-Info DHCPv4 Option Format

Code: The Mobile Subscription Inormation DHCPv4 Option (TBD) (one

octet).

Len: The length (one octet), in octets, of the URI.

URI: The URI for the mobile subscription API endpoint to which the user should connect.

2.4. The Mobile-Sub-Info IPv6 DHCP Option

The format of the Mobile-Sub-Info DHCP option is shown below.

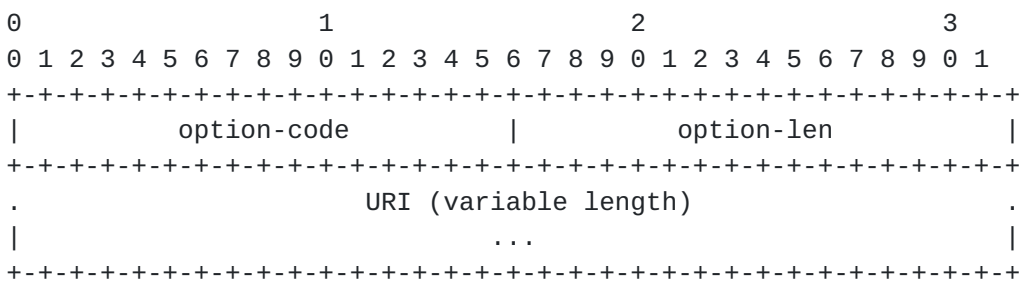

Figure 2: Mobile-Sub-Info DHCPv6 Option Format

option-code: The Mobile Subscription DHCPv6 Option (TBD) (two octet).

option-len: The unsigned 16-bit length, in octets, of the URI.

URI: The URI for the mobile subscription API endpoint to which the user should connect (encoded following the rules in).

2.5. The Mobile-Sub-Info IPv6 RA Option

The format of the Mobile-Sub-Info RA option is shown below.

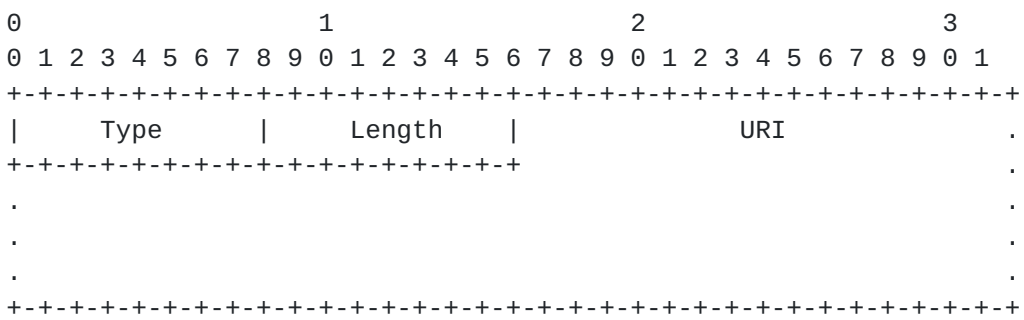

Figure 3: Mobile Subscription RA Option Format

Type: TBD

Length: 8-bit unsigned integer. The length of the option (including the Type and Length fields) in units of 8 bytes.

URI: The URI for the mobile subscription API endpoint to which

the user should connect. This MUST be padded with NUL (0x00) to make the total option length (including the Type and Length fields) a multiple of 8 bytes.

Note that the URI parameter is not guaranteed to be null terminated.

As the maximum length of the URI that can be carried in IPv4 DHCP is 255 bytes, URIs longer than this SHOULD NOT be provisioned via IPv6 RA options.

2.6. Precedence of API URIs

When client receives the Mobile-Subscription option and supports this option, it SHOULD retrieve the URL from the option and initiate a GET request [RFC2616] with the URL over HTTPS [RFC2818] . When the network receives the request, it SHOULD start the EAP-AKA process over HTTPS [RFC4187] by sending EAP-Request/AKA-Identity to exchange mobile subscription information with the client. Note that this precedence is independent to the DHCP and RA protocol. Should a client choose not to use this option or the EAP-AKA process fails, it does not impact the DHCP and RA process.

In this draft, we present EAP-AKA as the mobile information exchange method. However, other methods could also be considered. This is out-of-scope of this draft.

2.7. IANA Considerations

Option TBA

2.8. Security Considerations

The Option contains a URL that is transmitted in unencrypted plain text. An attacker on the same LAN segment may setup a rogue DHCP server or send out rogue RA to mis-guide the victim to connect to an attacker's server. The EAP-AKA transaction is protected by the EAP-AKA security framework. That being said, the client MUST initiate the request over HTTPS [RFC2818] and disgard any non HTTPS protocol (i.e., HTTP) proposed in the option.

3. Normative References

[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>.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <https://www.rfc-editor.org/info/rfc2131>.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H.,

Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, DOI 10.17487/RFC2616, June 1999, <https://www.rfc-editor.org/info/rfc2616>.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <https://www.rfc-editor.org/info/rfc2818>.

[RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, DOI 10.17487/RFC4187, January 2006, <https://www.rfc-editor.org/info/rfc4187>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

4. Informative References

[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>.

[RFC8910] Kumari, W. and E. Kline, "Captive-Portal Identification in DHCP and Router Advertisements (RAs)", RFC 8910, DOI 10.17487/RFC8910, September 2020, <https://www.rfc-editor.org/info/rfc8910>.

Authors' Addresses

Saravanan Muthusamy
Comcast
1800 Arch Street
Philadelphia, PA 19103
United States of America
Email: Saravanan_Muthusamy@comcast.com

Yiu L. Lee
Comcast
1800 Arch Street
Philadelphia, PA 19103
United States of America
Email: yiu_lee@comcast.com

Ruchi Kothari
Comcast
1800 Arch Street
Philadelphia, PA 19103
United States of America
Email: Ruchi_Kothari@comcast.com