Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 20, 2015

W. Kumari
Google
O. Gudmundsson
CloudFlare
P. Ebersman
Comcast
S. Sheng
ICANN

June 18, 2015

Captive-Portal Identification in DHCP / RA
draft-wkumari-dhc-capport-13

Abstract

In many environments offering short-term or temporary Internet access (such as coffee shops), it is common to start new connections in a captive portal mode. This highly restricts what the customer can do until the customer has authenticated.

This document describes a DHCP option (and a RA extension) to inform clients that they are behind some sort of captive portal device, and that they will need to authenticate to get Internet Access. It is not a full solution to address all of the issues that clients may have with captive portals; it is designed to be used in larger solutions.

[Ed note (remove): This document is being developed in github: https://github.com/wkumari/draft-wkumari-dhc-capport .]

Table of Contents

1. Introduction

In many environments, users need to connect to a captive portal device and agree to an acceptable use policy (AUP) and / or provide billing information before they can access the Internet. It is anticipated that the IETF will work on a more fully featured protocol at some point, to ease interaction with Captive Portals. Regardless of how that protocol operates, it is expected that this document will provide needed functionality because the client will need to know when it is behind a CP and how to contact it.

In order to present users with the payment or AUP pages, the captive portal device has to intercept the user's connections and redirect the user to the captive portal, using methods that are very similar to man-in-the-middle (MITM) attacks. As increasing focus is placed on security, and end nodes adopt a more secure stance, these interception techniques will become less effective and / or more intrusive.

This document describe a DHCP ([RFC2131]) option (Captive Portal) and an IPv6 Router Advertisement (RA) ([RFC4861]) extension that informs clients that they are behind a captive portal device and how to contact it.

1.1. Requirements notation

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].

2. The Captive-Portal Option

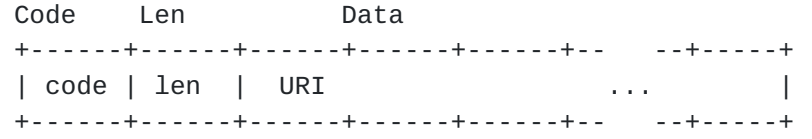
The Captive Portal DHCP / RA Option informs the client that it is behind a captive portal and provides the URI to access an authentication page. This is primarily intended to improve the user experience by getting them to the captive portal faster; for the foreseeable future, captive portals will still need to implement the interception techniques to serve legacy clients, and clients will need to perform probing to detect captive portals.

In order to support multiple "classes" of clients (e.g: IPv4 only, IPv6 only with DHCPv6([RFC3315]), IPv6 only with RA) the captive portal can provide the URI via multiple methods (IPv4 DHCP, IPv6 DHCP, IPv6 RA). The captive portal operator should ensure that the URIs handed out are equivalent to reduce the chance of operational problems.

In order to avoid having to perform DNS interception, the URI SHOULD contain an address literal, but MAY contain a DNS name if the captive portal allows the client to perform DNS requests to resolve the name.

2.1. IPv4 DHCP Option

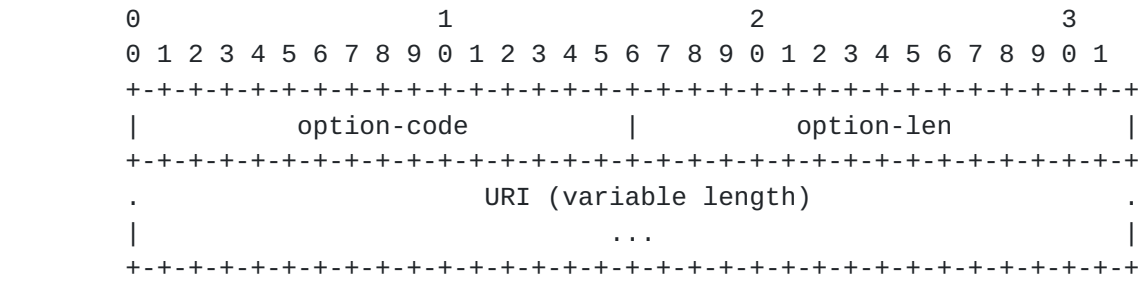
The format of the IPv4 Captive-Portal DHCP option is shown below.



- Code: The Captive-Portal DHCPv4 Option (TBA1) (one octet)
- Len: The length, in octets of the URI.
- URI: The URI of the authentication page that the user should connect to.

2.2. IPv6 DHCP Option

The format of the IPv6 Captive-Portal DHCP option is shown below.



- option-code: The Captive-Portal DHCPv6Option (TBA2) (two octets)

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

- URI: The URI of the authentication page that the user should connect to.

See [RFC7227], Section 5.7 for more examples of DHCP Options with URIs.

3. The Captive-Portal IPv6 RA Option

This section describes the Captive-Portal Router Advertisement option.

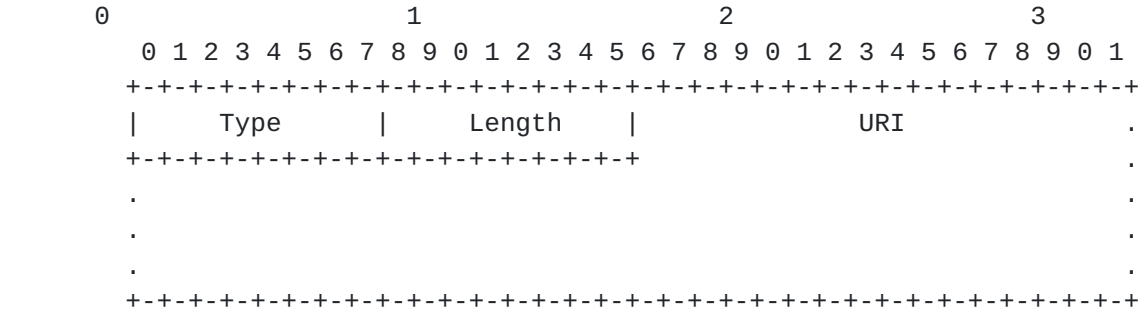


Figure 2: Captive-Portal RA Option Format

Type TBA3

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

URI The URI of the authentication page that the user should connect to. For the reasons described above, the implementer might want to use an IP address literal instead of a DNS name. This should

be padded with NULL (0x0) to make the total option length (including the Type and Length fields) a multiple of 8 bytes.

4. IANA Considerations

This document defines two DHCP Captive-Portal options, one for IPv6 and one for IPv6. It requires assignment of an option code (TBA1) to be assigned from "Bootp and DHCP options" registry (http://www.iana.org/assignments/ bootp-dhcp-parameters/bootp-dhcp-parameters.xml), as specified in [RFC2939]. It also requires assignment of an option code (TBA2) from the "DHCPv6 and DHCPv6 options" registry (http://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xml).

IANA is also requested to assign an IPv6 RA Option Type code (TBA3) from the "IPv6 Neighbor Discovery Option Formats" registry. Thanks IANA!

5. Security Considerations

An attacker with the ability to inject DHCP messages could include this option and so force users to contact an address of his choosing. As an attacker with this capability could simply list himself as the default gateway (and so intercept all the victim's traffic); this does not provide them with significantly more capabilities. Fake DHCP servers / fake RAs are currently a security concern - this doesn't make them any better or worse.

Devices and systems that automatically connect to an open network could potentially be tracked using the techniques described in this document (forcing the user to continually authenticate, or exposing their browser fingerprint). However, similar tracking can already be performed with the standard captive portal mechanisms, so this technique does not give the attackers more capabilities.

By simplifying the interaction with the captive portal systems, and doing away with the need for interception, we think that users will be less likely to disable useful security safeguards like DNSSEC validation, VPNs, etc. In addition, because the system knows that it is behind a captive portal, it can know not to send cookies, credentials, etc. Redirection to a portal where TLS can be used without hijacking can ameliorate some of the implications of connecting to a potentially malicious captive portal.

6. Acknowledgements

Thanks to Vint Cerf for the initial idea / asking me to write this. Thanks to Wes George for supplying the IPv6 text. Thanks to Lorenzo and Erik for the V6 RA kick in the pants.

Thanks to Fred Baker, Paul Hoffman, Ted Lemon, Martin Nilsson, Ole Troan and Asbjorn Tonnesen for detailed review and comments. Also great thanks to Joel Jaeggli for providing feedback and text.

7. Normative References

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

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC7227] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", BCP 187, RFC 7227, May 2014.

Appendix A. Changes / Author Notes.

[RFC Editor: Please remove this section before publication]

From 13.2 to 13(posted):

- Shortened the document by removing most of the [Editors notes], Section 2, Section 5 and Appendix A. They were mainly background and have served their purpose. This change suggested by Paul Hoffman.

From 13.1 to 13.2:

- Moved all of the "what an OS could do with this info" to an Appendix, to make it even clearer that this is simply an example.

From -12 to -13.1:

There was a Captive Portal Bar BoF held at the Dallas IETF meeting. See https://github.com/httpwg/wiki/wiki/Captive-Portals for some details. This document was discussed, and I got a fair bit of feedback. Incorporating some of this in -13.

- "In the text discussing why a captive portal notification might be useful (section 2.2 maybe?), perhaps you should say something about HSTS and HTTP2.0, since they will further erode the ability to use common captive portal redirection techniques." - Wes George.

- Integrated a bunch of useful comments from Martin Nilsson

From -11 to -12:

- Integrated a whole bunch of comments from Ted Lemon, including missing references, track, missing size of DHCP option,

From 10 to 11:

- Updated Olafur's affiliation.

From 09 to 10:

- Ted Lemon and Joel Jaeggli: there's no benefit to insisting on an ordering. I think you should just say that the ordering is indeterminate, and if different mechanisms give non-equivalent answers, this is likely to cause operational problems in practice.

From 08 to 09:

- Put back the DHCPv6 option, and made the fact that is separate from the DHCPv4 option clearer (Ted Lemon)

From 07 to 08:

- Incorporated comments from Ted Lemon. Made the document much shorter.

- Some cleanup.

From 06 to 07:

- Incoroprated a bunch of comments from Asbjorn Tonnesen

- Clarified that this document is only for the DHCP bits, not everything.

- CP's *can* do HTTP redirects to DNS names, as long as they allow access to all needed services.

From 05 to 06:

- Integrated comments from Joel, as below
- Better introduction text, around the "kludgy hacks" section.
- Better "neither condones nor condemns" text
- Fingerprint text.
- Some discussions on the v4 literal stuff.
- More Security Consideration text.

From 04 to 05:

- Integrated comments, primarily from Fred Baker.

From 03 to 04:

- Some text cleanup for readability.
- Some disclaimers about it working better on initial connection versus CP timeout.
- Some more text explaining that CP interception is indistinguishable from an attack.
- Connectivity Check test.
- Posting just before the draft cutoff - "I love deadlines. I love the whooshing noise they make as they go by." -- Douglas Adams, The Salmon of Doubt

From -02 to 03:

- Removed the DHCPv6 stuff (as suggested / requested by Erik Kline)
- Simplified / cleaned up text (I'm inclined to waffle on, then trim the fluff)
- This was written on a United flight with in-flight WiFi - unfortunately I couldn't use it because their CP was borked. :-P

From -01 to 02:

- Added the IPv6 RA stuff.

From -00 to -01:

- Many nits and editorial changes.
- Whole bunch of extra text and review from Wes George on v6.

From initial to -00.

- Nothing changed in the template!

Authors' Addresses

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: warren@kumari.net

Olafur Gudmundsson
CloudFlare
San Francisco, CA 94107
USA

Email: olafur@cloudflare.com

Paul Ebersman
Comcast

Email: ebersman-ietf@dragon.net

Steve Sheng
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles 90094
United States of America

Phone: +1.310.301.5800
Email: steve.sheng@icann.org