Internet Engineering Task Force (IETF)
Request for Comments: 7710
Category: Standards Track
ISSN: 2070-1721

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

December 2015

Captive-Portal Identification Using DHCP or Router Advertisements (RAs)

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 Router Advertisement (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. The method of authenticating to and interacting with the captive portal is out of scope for this document.

Status of This Memo

This is an Internet Standards Track document.

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). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7710.

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 captive portal 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 describes a DHCP ([RFC2131]) option (Captive-Portal) and an IPv6 Router Advertisement (RA) ([RFC4861]) extension that inform 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

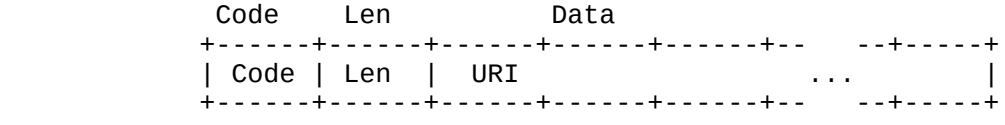
The Captive-Portal DHCP/RA option informs the client that it is behind a captive portal and provides the URI to access an authentication page. This is primarily intended to improve the user experience by getting them to the captive portal faster; for the foreseeable future, captive portals will still 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. The maximum length of the URI that can be carried in IPv4 DHCP is 255 bytes, so URIs longer than 255 bytes should not be used in IPv6 DHCP or IPv6 RA.

In order to avoid having to perform DNS interception, the URI SHOULD contain an address literal. If the captive portal allows the client to perform DNS requests to resolve the name, it is then acceptable for the URI to contain a DNS name. The URI parameter is not null terminated.

2.1. IPv4 DHCP Option

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

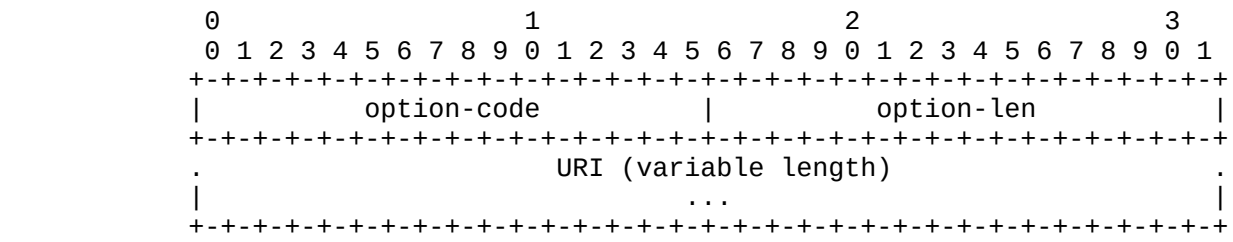


- Code: The Captive-Portal DHCPv4 option (160) (one octet).
- Len: The length, in octets of the URI.

- URI: The contact URI for the captive portal that the user should connect to (encoded following the rules in [RFC3986]).

2.2. IPv6 DHCP Option

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

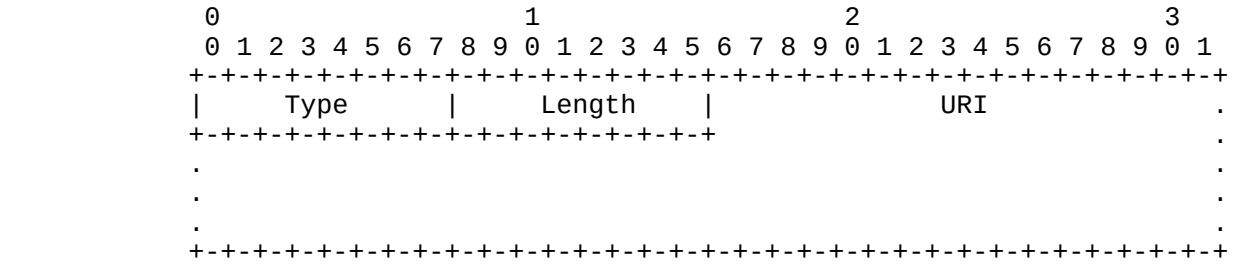


- option-code: The Captive-Portal DHCPv6 option (103) (two octets).
- option-len: The length, in octets of the URI.
- URI: The contact URI for the captive portal that the user should connect to (encoded following the rules in [RFC3986]).

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

2.3. The Captive-Portal IPv6 RA Option

The format of the Captive-Portal Router Advertisement option is shown below.



- Type: 37
- Length: 8-bit unsigned integer. The length of the option (including the Type and Length fields) in units of 8 bytes.

- URI: The contact URI for the captive portal 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.

3. IANA Considerations

This document defines two DHCP Captive-Portal options, one for IPv4 and one for IPv6. An option code (160) has been assigned from the "BOOTP Vendor Extensions and DHCP Options" registry (http://www.iana.org/assignments/bootp-dhcp-parameters), as specified in [RFC2939]. Also, an option code (103) has been assigned from the "Option Codes" registry under DHCPv6 parameters (http://www.iana.org/assignments/dhcpv6-parameters).

IANA also has assigned an IPv6 RA Option Type code (37) from the "IPv6 Neighbor Discovery Option Formats" registry under ICMPv6 parameters (http://www.iana.org/assignments/icmpv6-parameters). Thanks, IANA!

4. 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 the attacker with significantly more capabilities, but because this document removes the need for interception, the attacker may have an easier time performing the attack. As the operating systems and application that make use of this information know that they are connecting to a captive-portal device (as opposed to intercepted connections), they can render the page in a sandboxed environment and take other precautions, such as clearly labeling the page as untrusted. The means of sandboxing and how the user interface presents this information are not covered in this document -- by their nature, those are implementation specific and best left to the application and user-interface designers.

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.

Captive portals are increasingly hijacking TLS connections to force browsers to talk to the portal. Providing the portal's URI via a DHCP or RA option is a cleaner technique and reduces user expectations of being hijacked; this may improve security by making users more reluctant to accept TLS hijacking, which can be performed from beyond the network associated with the captive portal.

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. By handing out a URI that is protected with TLS, the captive-portal operator can attempt to reassure the user that the captive portal is not malicious.

5. 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, <http://www.rfc-editor.org/info/rfc2119>.

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

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <http://www.rfc-editor.org/info/rfc3315>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>.

[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, <http://www.rfc-editor.org/info/rfc4861>.

[RFC7227] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", BCP 187, RFC 7227, DOI 10.17487/RFC7227, May 2014, <http://www.rfc-editor.org/info/rfc7227>.

6. Informative References

[RFC2939] Droms, R., "Procedures and IANA Guidelines for Definition of New DHCP Options and Message Types", BCP 43, RFC 2939, DOI 10.17487/RFC2939, September 2000, <http://www.rfc-editor.org/info/rfc2939>.

Acknowledgements

Thanks to Vint Cerf for asking for this document to be written. 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, Barry Leiba, Ted Lemon, Martin Nilsson, Ole Troan, and Asbjorn Tonnesen for detailed reviews and comments. Thanks for David Black for review and providing text for the security considerations. Also, great thanks to Joel Jaeggli for providing feedback and text.

Authors' Addresses

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
United States

Email: warren@kumari.net

Olafur Gudmundsson
CloudFlare
San Francisco, CA 94107
United States

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, CA 90094
United States
Phone: +1.310.301.5800

Email: steve.sheng@icann.org