Internet Engineering Task Force (IETF)
Request for Comments: 8910
Obsoletes: 7710
Updates: 3679
Category: Standards Track
ISSN: 2070-1721

W. Kumari
Google
E. Kline
Loon

September 2020

Captive-Portal Identification in DHCP and 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 user can do until the user has satisfied the captive portal conditions.

This document describes a DHCPv4 and DHCPv6 option and a Router Advertisement (RA) option to inform clients that they are behind some sort of captive portal enforcement device, and that they will need to satisfy the Captive Portal conditions 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 one component of a standardized approach for hosts to interact with such portals. While this document defines how the network operator may convey the captive portal API endpoint to hosts, the specific methods of satisfying and interacting with the captive portal are out of scope of this document.

This document replaces RFC 7710, which used DHCP code point 160. Due to a conflict, this document specifies 114. Consequently, this document also updates RFC 3679.

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 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/rfc8910.

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. Regardless of how that mechanism operates, this document provides functionality to allow the client 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, a captive portal enforcement device presently has to intercept the user's connections and redirect the user to a captive portal server, 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 DHCPv4 [RFC2131] and DHCPv6 [RFC8415] option (Captive-Portal) and an IPv6 Router Advertisement (RA) [RFC4861] option that informs clients that they are behind a captive portal enforcement device and the API endpoint that the host can contact for more information.

This document replaces RFC 7710 [RFC7710], which used DHCP code point 160. Due to a conflict, this document specifies 114. Consequently, this document also updates [RFC3679].

1.1. Requirements Notation

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.

2. The Captive-Portal Option

The Captive-Portal DHCP/RA Option informs the client that it may be behind a captive portal and provides the URI to access an API as defined by [RFC8908]. This is primarily intended to improve the user experience by showing the user the captive portal information faster and more reliably. Note that, for the foreseeable future, captive portals will still need to implement interception techniques to serve legacy clients, and clients will need to perform probing to detect

captive portals; nonetheless, the mechanism provided by this document provides a more reliable and performant way to do so, and is therefore the preferred mechanism for captive portal detection.

Clients that support the Captive Portal DHCP option SHOULD include the option in the Parameter Request List in DHCPREQUEST messages. DHCP servers MAY send the Captive Portal option without any explicit request.

In order to support multiple "classes" of clients (e.g., IPv4 only, IPv6 only with DHCPv6 ([RFC8415]), and IPv6 only with RA), the captive network can provision the client with the URI via multiple methods (IPv4 DHCP, IPv6 DHCP, and IPv6 RA). The captive portal operator SHOULD ensure that the URIs provisioned by each method are identical to reduce the chance of operational problems. 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 by any of the IPv6 options described in this document. In IPv6-only environments, this restriction can be relaxed.

In all variants of this option, the URI MUST be that of the captive portal API endpoint ([RFC8908]).

A captive portal MAY do content negotiation (Section 3.4 of [RFC7231]) and attempt to redirect clients querying without an explicit indication of support for the captive portal API content type (i.e., without application/capport+json listed explicitly anywhere within an Accept header field as described in Section 5.3 of [RFC7231]). In so doing, the captive portal SHOULD redirect the client to the value associated with the "user-portal-url" API key. When performing such content negotiation (Section 3.4 of [RFC7231]), implementors of captive portals need to keep in mind that such responses might be cached, and therefore SHOULD include an appropriate Vary header field (Section 7.1.4 of [RFC7231]) or set the Cache-Control header field in any responses to "private" or a more restrictive value such as "no-store" (Section 5.2.2.3 of [RFC7234]).

The URI SHOULD NOT contain an IP address literal. Exceptions to this might include networks with only one operational IP address family where DNS is either not available or not fully functional until the captive portal has been satisfied. Use of IP Address certificates ([RFC3779]) adds considerations that are out of scope for this document.

Networks with no captive portals may explicitly indicate this condition by using this option with the IANA-assigned URI for this purpose. Clients observing the URI value "urn:ietf:params:capport:unrestricted" may forego time-consuming forms of captive portal detection.

2.1. IPv4 DHCP Option

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

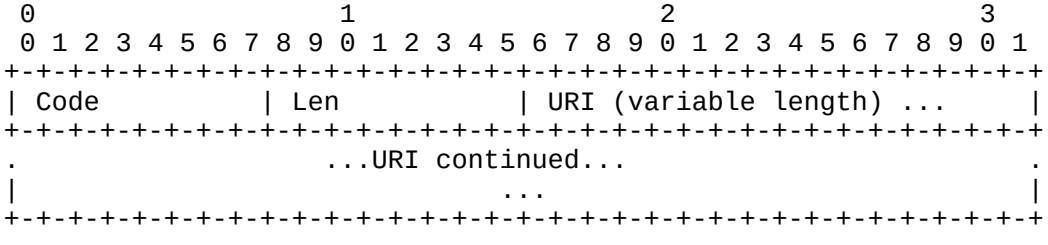

Figure 1: Captive-Portal DHCPv4 Option Format

Code: The Captive-Portal DHCPv4 Option (114) (one octet).

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

URI: The URI for the captive portal API endpoint to which the user should connect (encoded following the rules in [RFC3986]).

See Section 2 of [RFC2132] for more on the format of IPv4 DHCP options.

Note that the URI parameter is not null terminated.

2.2. IPv6 DHCP Option

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

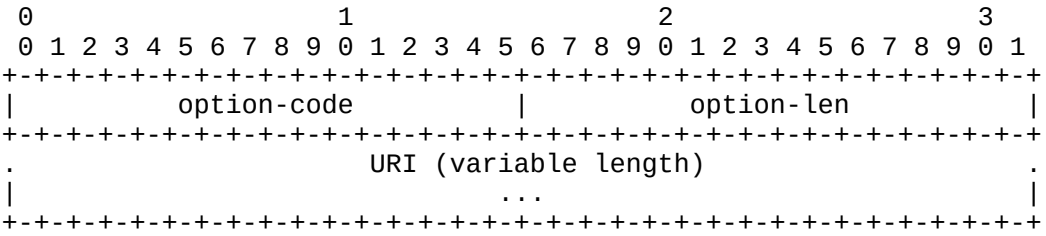

Figure 2: Captive-Portal DHCPv6 Option Format

option-code: The Captive-Portal DHCPv6 Option (103) (two octets).

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

URI: The URI for the captive portal API endpoint to which the user should connect (encoded following the rules in [RFC3986]).

See Section 5.7 of [RFC7227] for more examples of DHCP Options with URIs. See Section 21.1 of [RFC8415] for more on the format of IPv6 DHCP options.

Note that the URI parameter is not 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 DHCP options.

2.3. The Captive-Portal IPv6 RA Option

This section describes the Captive-Portal Router Advertisement option.

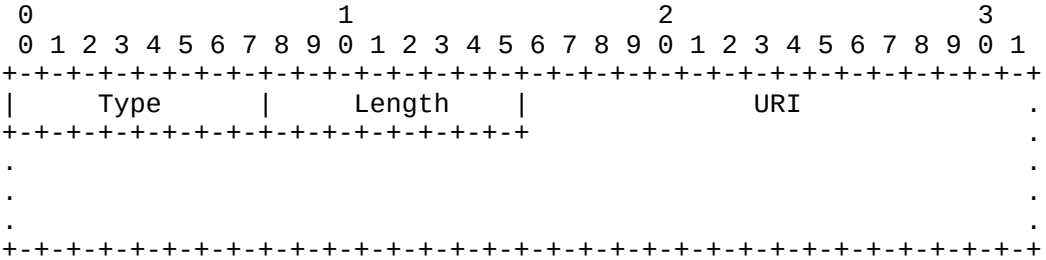

Figure 3: Captive-Portal RA Option Format

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 URI for the captive portal 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.

3. Precedence of API URIs

A device may learn about Captive Portal API URIs through more than one of (or indeed all of) the above options. Implementations can select their own precedence order (e.g., prefer one of the IPv6 options before the DHCPv4 option, or vice versa, et cetera).

If the URIs learned via more than one option described in Section 2 are not all identical, this condition should be logged for the device owner or administrator; it is a network configuration error if the learned URIs are not all identical.

4. IANA Considerations

IANA has registered a new IETF URN protocol parameter ([RFC3553]). IANA has also reallocated two DHCPv4 option codes (see Appendix B for background) and updated the references for previously registered DHCPv6 and IPv6 ND options.

4.1. Captive Portal Unrestricted Identifier

IANA has registered a new entry in the "IETF URN Sub-namespace for Registered Protocol Parameter Identifiers" registry defined in [RFC3553]:

Registered Parameter Identifier: capport:unrestricted
Reference: RFC 8910
IANA Registry Reference: RFC 8910

Only one value is defined (see URN above). No hierarchy is defined and, therefore, no sub-namespace registrations are possible.

4.2. BOOTP Vendor Extensions and DHCP Options Code Change

IANA has updated the "BOOTP Vendor Extensions and DHCP Options" registry (https://www.iana.org/assignments/bootp-dhcp-parameters) as follows.

Tag: 114
Name: DHCP Captive-Portal
Data Length: N
Meaning: DHCP Captive-Portal
Reference: RFC 8910

Tag: 160
Name: Unassigned
Data Length:
Meaning: Previously assigned by [RFC7710]; known to also be used by Polycom.
Reference: [RFC7710] RFC 8910

4.3. Update DHCPv6 and IPv6 ND Options Registries

IANA has updated the DHCPv6 (103 - DHCP Captive-Portal) and IPv6 ND (37 - DHCP Captive-Portal) options previously registered in [RFC7710] to reference this document.

5. Security Considerations

By removing or reducing the need for captive portals to perform MITM hijacking, this mechanism improves security by making the portal and its actions visible, rather than hidden, and reduces the likelihood that users will disable useful security safeguards like DNSSEC validation, VPNs, etc. in order to interact with the captive portal. 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.

Clients processing these options SHOULD validate that the option's contents conform to the validation requirements for URIs, including those described in [RFC3986].

Each of the options described in this document is presented to a node using the same protocols used to provision other information critical to the node's successful configuration on a network. The security considerations applicable to each of these provisioning mechanisms also apply when the node is attempting to learn the information conveyed in these options. In the absence of security measures like RA-Guard ([RFC6105], [RFC7113]) or DHCPv6-Shield [RFC7610], an attacker could inject, modify, or block DHCP messages or RAs.

An attacker with the ability to inject DHCP messages or RAs could include an option from this document to force users to contact an address of the attacker's choosing. An attacker with this capability could simply list themselves as the default gateway (and so intercept all the victim's traffic); this does not provide them with significantly more capabilities, but because this document removes the need for interception, the attacker may have an easier time performing the attack.

However, as the operating systems and application(s) that make use of this information know that they are connecting to a captive portal device (as opposed to intercepted connections where the OS/ application may not know that they are connecting to a captive portal or hostile device), 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 a user interface presenting this information is not covered in this document; by its nature, it is 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 resatisfy the Captive Portal conditions or exposing their browser fingerprint). However, similar tracking can already be performed with the presently common 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.

6. References

6.1. 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>.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, DOI 10.17487/RFC2132, March 1997, <https://www.rfc-editor.org/info/rfc2132>.

[RFC3553] Mealling, M., Masinter, L., Hardie, T., and G. Klyne, "An IETF URN Sub-namespace for Registered Protocol Parameters", BCP 73, RFC 3553, DOI 10.17487/RFC3553, June 2003, <https://www.rfc-editor.org/info/rfc3553>.

[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, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc7227>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <https://www.rfc-editor.org/info/rfc7231>.

[RFC7234] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Caching", RFC 7234, DOI 10.17487/RFC7234, June 2014, <https://www.rfc-editor.org/info/rfc7234>.

[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>.

[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>.

6.2. Informative References

[RFC3679] Droms, R., "Unused Dynamic Host Configuration Protocol (DHCP) Option Codes", RFC 3679, DOI 10.17487/RFC3679, January 2004, <https://www.rfc-editor.org/info/rfc3679>.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, DOI 10.17487/RFC3779, June 2004, <https://www.rfc-editor.org/info/rfc3779>.

[RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105,

DOI 10.17487/RFC6105, February 2011,
<https://www.rfc-editor.org/info/rfc6105>.

[RFC7113] Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", RFC 7113, DOI 10.17487/RFC7113, February 2014, <https://www.rfc-editor.org/info/rfc7113>.

[RFC7610] Gont, F., Liu, W., and G. Van de Velde, "DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers", BCP 199, RFC 7610, DOI 10.17487/RFC7610, August 2015, <https://www.rfc-editor.org/info/rfc7610>.

[RFC7710] Kumari, W., Gudmundsson, O., Ebersman, P., and S. Sheng, "Captive-Portal Identification Using DHCP or Router Advertisements (RAs)", RFC 7710, DOI 10.17487/RFC7710, December 2015, <https://www.rfc-editor.org/info/rfc7710>.

[RFC8908] Pauly, T., Ed. and D. Thakore, Ed., "Captive Portal API", RFC 8908, DOI 10.17487/RFC8908, September 2020, <https://www.rfc-editor.org/info/rfc8908>.

Appendix A. Changes from RFC 7710

This document incorporates the following changes from [RFC7710].

1. Clarified that IP string literals are NOT RECOMMENDED.

2. Clarified that the option URI MUST be that of the captive portal API endpoint.

3. Clarified that captive portals MAY do content negotiation.

4. Added text about Captive Portal API URI precedence in the event of a network configuration error.

5. Added urn:ietf:params:capport:unrestricted URN.

6. Noted that the DHCPv4 Option Code changed from 160 to 114.

Appendix B. Observations from IETF 106 Network Experiment

During IETF 106 in Singapore, an experiment (https://tickets.meeting.ietf.org/wiki/IETF106network#Experiments) enabling clients compatible with the Captive Portal API to discover a venue-info-url (see experiment description (https://tickets.meeting.ietf.org/wiki/CAPPORT) for more detail) revealed that some Polycom devices on the same network made use of DHCPv4 option code 160 for other purposes (https://community.polycom.com/t5/VoIP-SIP-Phones/DHCP-Standardization-160-vs-66/td-p/72577).

The presence of DHCPv4 Option code 160 holding a value indicating the Captive Portal API URL caused these devices to not function as desired. For this reason, IANA has deprecated option code 160 and allocated a different value to be used for the Captive Portal API URL.

Acknowledgements

This document is a -bis of RFC 7710. Thanks to all of the original authors (Warren Kumari, Olafur Gudmundsson, Paul Ebersman, and Steve Sheng) and original contributors.

Also thanks to the CAPPORT WG for all of the discussion and improvements, including contributions and review from Joe Clarke,

Lorenzo Colitti, Dave Dolson, Hans Kuhn, Kyle Larose, Clemens Schimpe, Martin Thomson, Michael Richardson, Remi Nguyen Van, Subash Tirupachur Comerica, Bernie Volz, and Tommy Pauly.

Authors' Addresses

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

Email: warren@kumari.net

Erik Kline
Loon
1600 Amphitheatre Parkway
Mountain View, CA 94043
United States of America

Email: ek@loon.com