template
Internet-Draft
Intended status: Informational
Expires: October 31, 2015

D. Bird
W. Kumari
Google

April 29, 2015

Captive Portal ICMP Destination Unreachable
draft-wkumari-capport-icmp-unreach-00

Abstract

This document defines a multi-part ICMP extension to signal that a user's device is behind a Captive Portal.

[Editor note: The IETF is currently discussing improvements in captive portal interactions and user experience improvements. See: https://www.ietf.org/mailman/listinfo/captive-portals]

[RFC Editor: Please remove this before publication. This document is being stored in github at https://github.com/wkumari/draft-wkumari-capport-icmp-unreach . Authors gratefully accept pull requests, and keep the latest (edit buffer) versions there, so commenters can follow along at home.]

Table of Contents

1. Introduction

Captive Portals work by blocking (or redirecting) communications outside of a "walled garden" until the user has authenticated and / or acknowledged an Acceptable Use Policy (AUP). Depending on the captive portal implementation, connections other than HTTP will either timeout (packets dropped) or meet with a different, inaccurate, error condition (like a TCP reset or ICMP Destination Unreachable with existing codes).

A current option for captive portal networks is to reject traffic not in the walled garden returning the Destination Unreachable either Host or Network Administratively Prohibited. However, these codes are typically permanent policies and do not specifically indicate a captive portal is in use.

This document defines an extension object that can be appended to selected multi-part ICMP messages to inform the user that they are behind a captive portal. This informs the user after they have attempted an initial connection and is generated by the Captive Portal NAS itself.

[Editor note: This is complementary, but solves a different problem to: https://tools.ietf.org/html/draft-wkumari-dhc-capport-12 - wkumari-dhc-capport provides information from a DHCP server (and so doesn't need any changes to deployed CPs, and provides information

before the client attempts a connection. It does not, however, have a way of noting that an existing connection has been interrupted.]

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. ICMP Dest Unreachable Captive Portal Object

This document defines an extension object that can be appended to selected multi-part ICMP messages ([RFC4884]). This extension permits Captive Portal (CP) NAS devices to inform user devices that their connection has been blocked by the Captive Portal NAS, and, optionally, how to contact the Captive Portal to satisfy it.

The Dest Unreachable Captive Portal Object can be appended to the ICMP Destination Unreachable messages. Figure 1 depicts the Dest Unreachable Captive Portal Object. It must be preceded by an ICMP Extension Structure Header and an ICMP Object Header. Both are defined in [RFC4884].

```
 0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |W|  Reserved   |         Validity (seconds)                    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                       Captive Portal URL                      ~
 ~                           (optional)                          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

W - 1 bit Warning. Indicates that the Validity refers to when the service will be interrupted. Note that the "offending" traffic was forwarded, not dropped.

Validity - 24 bits Time, in seconds, that this result should be considered valid (and the OS should not attempt to access the same resource in the meantime).

Captive Portal URL - Variable The optional URL of the Captive Portal. This allows Captive Portal detection software running on the user's device to locate and connect to the captive portal to improve the user experience. The length of the URL is calculated from the ICMP Extension Object header Length minue the ICMP

Extension Object and Captive Portal Object header lengths, which is zero when no URL is provided.

Editor note / questions. We are trying to get some feedback on A: this general idea and B: this implementation.

Some open questions.

W bit or C-Type We have currently specified a single bit (W) to indicate that the remaining lease time is running low, and the the connection will be interrupted sometime "soon". We could, instead, use a differnt C-Type. I think a bit is cleaner (and we have reserved 7 bits for future flags), but could be convinced (or, better yet, bribed) I'm wrong. Or that the whole "warning" idea is a bad one...

Legacy interaction If we *do* return e.g ICMP Destination Unreachable, Communication Administratively Prohibited to a "legacy" (non-Dest Unreachable Captive Portal Object aware) client with the 'W' bit set, what happens? In the testing I did, nothing bad seemed to happen, but I *could* see that some hosts may stop sending to that address, or...

General concept Is this idea useful?

3. IANA Considerations

The IANA is requested to assign a Class-Num identifier for the Dest Unreachable Captive Portal Object from the ICMP Extension Object Classes and Class Sub-types registry.

The IANA is also requested to form and administer the corresponding class sub-type (C-Type) space, as follows:

Dest Unreachable Captive Portal Sub-types:

0 Reserved.

1 This message format.

0x02-0xF6 Available for assignment

0xF7-0xFF Reserved for private use

C-Type values are assignable on a first-come-first-serve (FCFS) basis.

[Editor note: Currently we are not using the C-Type for anything, but I filled this in anyway. Probably we would overload it at a version identifier type thing, but it could also allow further extension, for example, a pointer to a status page.]

4. Security Considerations

The obvious security consideration is how to confirm that the received ICMP Message actually came from a Captive Portal, and was not generated from a passive observer on the network (to force the user to connect to a malicious device.).

5. Acknowledgements

The authors wish to thank the authors of RFC4950 (especially Ron Bonica) - I stole much of his text when writing the extension definition.

6. References

6.1. Normative References

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981.

[RFC1122] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

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

[RFC4884] Bonica, R., Gan, D., Tappan, D., and C. Pignataro, "Extended ICMP to Support Multi-Part Messages", RFC 4884, April 2007.

6.2. Informative References

[I-D.ietf-sidr-iana-objects] Manderson, T., Vegoda, L., and S. Kent, "RPKI Objects issued by IANA", draft-ietf-sidr-iana-objects-03 (work in progress), May 2011.

Appendix A. Changes / Author Notes.

[RFC Editor: Please remove this section before publication]

From -genesis to -00.

- o Initial text.

Authors' Addresses

David Bird
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: dbird@google.com

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

Email: warren@kumari.net