template
Internet-Draft
Intended status: Informational
Expires: October 4, 2017

D. Bird
W. Kumari
Google

April 2, 2017

Captive Portal ICMP Messages
draft-wkumari-capport-icmp-unreach-02

Abstract

This document defines a new ICMP Type for Captive Portal Messages. The ICMP Type will only be known to clients supporting this specification and provides both generic and flow 5-tuple specific notifications from the Captive Portal NAS.

Further, This document defines a multi-part ICMP extension to ICMP Destination Unreachable messages to signal, not only that the packet was dropped, but that it was dropped due to an Access Policy requiring Captive Portal interaction. Legacy clients will only be processing the ICMP Destination Unreachable.

[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/wlanmac/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.]

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 http://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 October 4, 2017.

Table of Contents

1. Introduction

Captive Portals work by blocking (or redirecting) communications outside of a "walled garden" until the user has either authenticated, acknowledged an Acceptable Use Policy (AUP), or otherwise satisfied the requirements of the Captive Portal. Depending on the captive portal implementation, connections other than HTTP will either timeout (silently packets dropped) or meet with a different,

inaccurate, error condition (like a TCP reset, for TCP connections, or ICMP Destination Unreachable with existing codes).

A current option for captive portal networks is to reject traffic not in the walled garden by 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 a new ICMP Type for Captive Portal. The Captive Portal ICMP Type can be used to send flow 5-tuple specific or general notifications to user devices. As a new ICMP type, it is expected to be ignored by legacy devices.

This document also defines an Extension Object that can be appended to selected multi-part ICMP messages to inform the user device that they are behind a captive portal, in addition to the underlying ICMP information. Devices able to understand the extension get extra information about the captive portal access policy, whereas legacy devices just understand the underlying ICMP message.

The Captive Portal and Destination Unreachable types provide the Captive Portal NAS options in terms of what notifications legacy devices can and should understand.

The Captive Portal ICMP Messages only provide notification. They do not provide any configuration. For that, we use [RFC7710] and the Captive Portal URI it provides.

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].

1.2. Terminology

Capport ICMP device Device or operating system compliant to this specification.

CP-NAS Network Access Server implementing Captive Portal enforcement.

Legacy device Device or operating system not compliant to this specification.

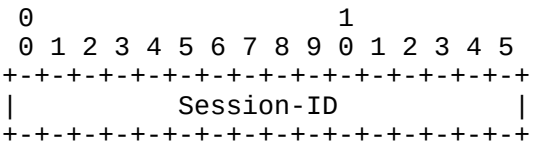
2. Captive Portal ICMP

Captive Portal ICMP messages come in two flavors. Messages can be sent using the Captive Portal ICMP Type or they can be sent as an ICMP Extension to an existing ICMP Type, such as Destination Unreachable. Data is encoded into the packet slightly differently in each case, however, the field formats remain consistent. All fields are in network byte order.

Capport ICMP devices MUST support [RFC7710].

2.1. Session-ID

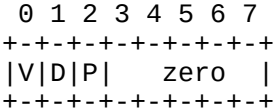
An unsigned short session identifier that groups ICMP messages. ICMP messages containing the same value MUST be assumed to be part of the same access policy. Any change in this value between ICMP messages from the same source IP address MUST be considered by the client to mean a change in access policy has occurred and previous notifications are no longer valid.



2.2. Flags

In Captive Portal ICMP Messages, a flags field contains bit flags for optional payload data fields. All data fields are unsigned 32bit integers.

Bit flags and their (optional) respective data fields:

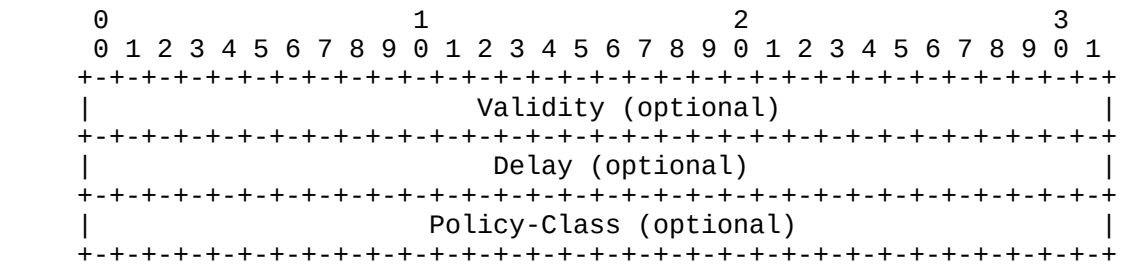


V - 1 bit Validity

D - 1 bit Delay

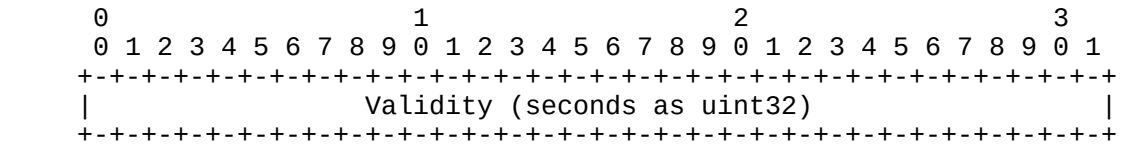
P - 1 bit Policy Class

Optional fields included in flags appear in the ICMP payload in the same order as the respective bits.



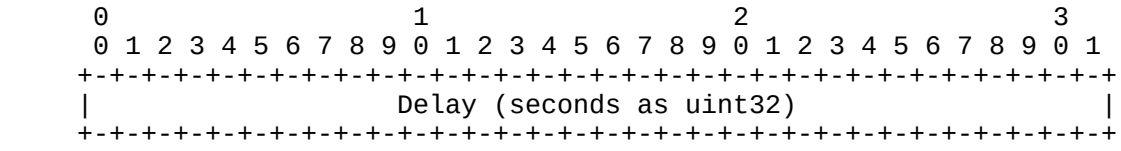
2.3. Validity

The Validity time, in seconds, that this result should be considered valid and the OS SHOULD not attempt to access the same resource in the meantime. During the Validity time, the NAS MAY chose to silently drop the packets of the same flow 5-tuple to selectively cause legacy clients to time-out connections.



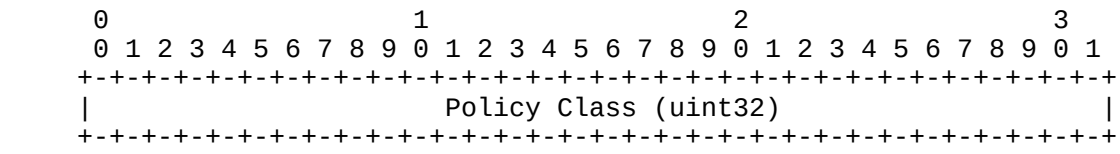
2.4. Delay

The Delay time, in seconds, is the time in future when this result should be considered valid. This is used to give advanced notice that a change in access policy is about to happen.



2.5. Policy Class

The Policy Class is an unsigned integer that provides a "hint" to the captive portal. When a client is specifically responding to a Captive Portal ICMP message and is launching a browser, the Policy Class is given to the portal as a reason for the visitor to visit the portal.



2.6. Message Code/C-Type

Captive Portal Message Code and C-Types:

0 General Change of Authorization (change in policy)

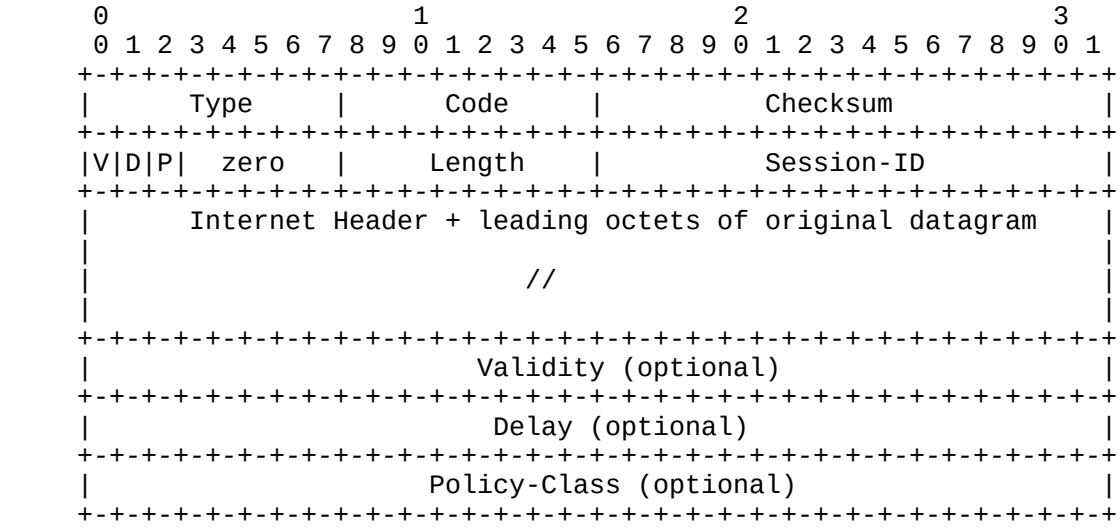
1 Packet/flow Error (dropped)

2 Packet/flow Overflow (dropped)

3 Packet/flow Warning (not dropped)

2.7. Message Type

The Captive Portal ICMP Type message is specifically for Capport ICMP Compliant devices. It is expected that Legacy devices will ignore such messages.



As shown in the figure above, the Captive Portal Flags and Session-ID and part of the ICMP header. The optional fields are in the ICMP payload, past the (optional) original datagram headers of a length defined by Length.

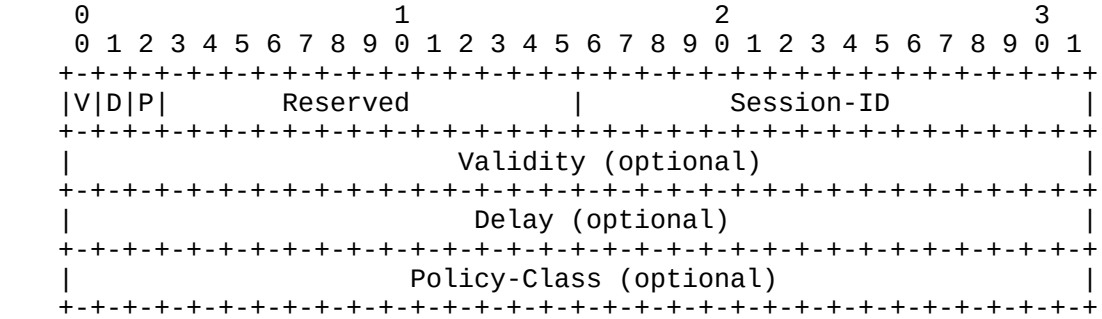
Length Number of 4 byte words of original datagram.

2.8. Extension Object

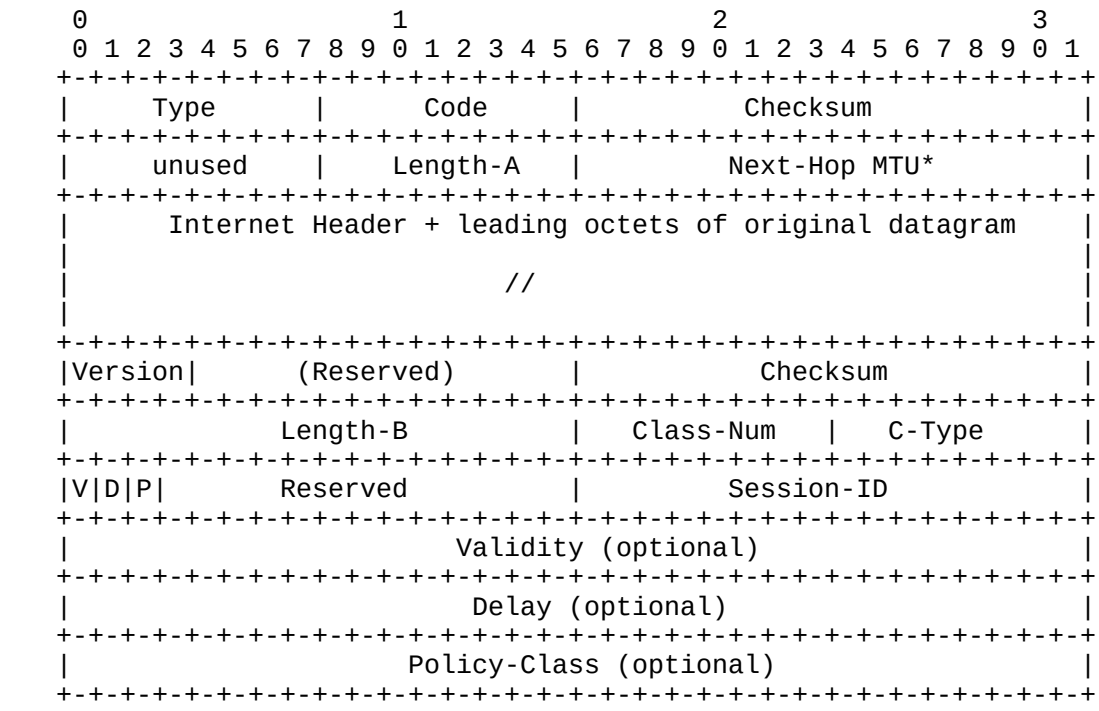
This document defines an extension object that can be appended to selected multi-part ICMP messages ([RFC4884]). This extension permits the CP-NAS to inform Capport ICMP Compliant devices that their connection has been blocked due to an Access Policy requiring interaction with the Captive Portal.

The Captive Portal Extension Object can be appended to the ICMP Destination Unreachable messages. When Legacy devices receive such messages, they will only understand the Destination Unreachable, ignoring the extensions.

When used in an Extension Object, the Captive Portal ICMP data fields are packed into an extension structure as shown below.



The following figure depicts the Destination Unreachable message with Captive Portal Extension. It must be preceded by an ICMP Extension Structure Header and an ICMP Object Header. Both are defined in [RFC4884].



Type Set to 3 for Destination Unreachable.

Code Can be any value Code value for Type.

Length-A Length, in 4 byte words, of original datagram.

Version Set to version 2, per RFC 4884.

Length-B Length of extension.

Class-Num Set to Captive Portal Class-Num.

C-Type See section 2.6.

3. Captive Portal URL Formatting

The Session-ID and Policy Class is used along with the RFC 7710 URI received from DHCP or IPv6 RA to send the user to the captive portal.

```
RFC_7710_URI . SEP .
      'icmp_session=' . SESSION_ID . '&' .
      'policy_class=' . [POLICY_CLASS[,POLICY_CLASS]]
```

RFC_7710_URI The URI received from DHCP or IPv6 RA per RFC 7710.

SEP If the RFC_7710_URI contains a '?', then SEP equals ampersand, otherwise a question mark.

SESSION_ID The Session-ID value in integer format.

POLICY_CLASS Zero or more Policy Class values gathers for the same Session-ID leading to the user notification..

Examples:

https://wifi.domain.com/portal?icmp_session=10&policy_class=100
https://my.domain.com/?do=login&icmp_session=10&policy_class=100,20

4. IANA Considerations

The IANA is requested to assign a Captive Portal ICMP Message Type, as well as Code values defined in section 2.6..

The IANA is also requested to assign a Class-Num identifier for the Captive Portal Extension 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 per section 2.6.

5. Security Considerations

This method simply annotates existing ICMP Destination Unreachable messages to inform users why their connection was blocked. This technique can be used to inform captive portal detection probe software that there is a captive portal present (and potentially to connect to the URL handed out using draft-wkumari-dhc-capport. We anticipate that there will be a new solution devised (such as a well known URL / URI on captive portals) to allow the user / captive portal probe to do something more useful with this information.

6. Acknowledgements

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

7. References

7.1. Normative References

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, DOI 10.17487/RFC0792, September 1981, <http://www.rfc-editor.org/info/rfc792>.

[RFC1122] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <http://www.rfc-editor.org/info/rfc1122>.

[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>.

[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>.

[RFC4884] Bonica, R., Gan, D., Tappan, D., and C. Pignataro, "Extended ICMP to Support Multi-Part Messages", RFC 4884, DOI 10.17487/RFC4884, April 2007, <http://www.rfc-editor.org/info/rfc4884>.

[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, <http://www.rfc-editor.org/info/rfc7710>.

7.2. 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 -01 to 02.

- Added a new ICMP Type, redefined message payload and flags, and introduces Codes/C-Types.

From -00 to 01.

- Changed the Captive Portal URL to a URI, and specificed that this can ONLY contain a path element, which is appended to http://<gateway_ip>. This is to prevent hijacking connections to other addresses.

- Then removed the entire URL / URI scheme entirely.

From -genesis to -00.

- 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