Reporting of Happy Eyeballs Failures
draft-palet-v6ops-he-reporting-00

Abstract

   This document describes an extension to Happy Eyeballs in order to
   report IPv6 failures that force the fall-back to IPv4 and
   consequently, facilitate the troubleshooting of IPv6 networks.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   Happy Eyeballs ([RFC6555]) provides a way for improving user-visible
   delay when IPv6 connectivity is performing worse than the IPv4 one.

   However, this hides the possible IPv6 connectivity issues to the
   operator because users don't notice anything broken, so they aren't
   reporting it to their providers.

   The goal of this document is to specify an extension of HE, in order
   to use existing protocols for providing a reporting to the operator,
   which can be used to setup alarms and trigger further investigation
   so to improve network reliability, facilitating the detection of
   failures as soon as they appear, without the need of external
   monitoring.

2. Using Syslog

   In order to simplify the reporting of the HE failures, syslog
   ([RFC5424]) over UDP ([RFC5426]), MUST be used, by means of the
   default port (514) with IPv6-only.

   The intend is to make this reporting very simple, so no choice of
   alternative ports or transport protocols is offered.

   Operators willing to use this reporting MUST configure at least one
   syslog collector at the IPv6 prefix formed as:

   Network-Specific Prefix::192.88.99.1

   The Network-Specific Prefix (NSP) MUST be chosen by the operator from
   its RIR allocated IPv6 addressing space.

   Additional collectors can be made available by using anycast at the
   NSP + 192.88.99.0/24 prefix

3. **Discovery of the syslog collector NSP**

   The same mechanism described by RFC7050 ([RFC7050]) should be used to
   define the address of the syslog collector(s).

   Because the collectors will be using an IPv6 address with the 32 low
   order bits from the reserved range 192.88.99.0/24, this will not be
   in conflict with any public addresses used in Internet, so this
   mechanism is compatible with the expected usage of the NSP for NAT64.

4. **HE behaviour on failure detection**

   This section will specify the exact behaviour of HE in order to
   initiate the reporting and the specific format/parameters of the HE
   failure message to be sent to the syslog collector.

   A preliminary consideration is to include, in addition to the syslog
   required parameters, the timeouts detected, the failed destination
   address and the source prefix from where the destination has failed.

   TBD.

5. **Privacy Considerations**

   The goal is to provide the operator information about the failures
   detected by HE, without requiring specific users traffic information.
   Towards this, it will be sufficient to provide to the syslog
   collector details about the failed destination address and source
   prefix. So privacy issues regarding identification of a specific
   device or users are avoided.

   Nowadays, operators already log this information in order to comply
   with lawful interception regulations, and in general, data protection
   regulations allow this logging when technically required. Data
   protection regulations explicitly say that the data can't be
   disclosed, and there is no need to do so.

   In general, vendors also collect telemetry data from devices, in
   order to improve OSs and in some situations, there are regulations
   that enforce offering the user to enable/disable that feature. So we
   could consider offering the same feature for this mechanism.

   When the mechanism described in this document detects a failure, the
   operator will need to find if the problem is related to:

   o A specific user (inside the customer local networks, or even at
      their WAN router).

o   A group of users (e.g., one or several part of the access or
    distribution networks).

o   The entire operator network (e.g., core network or transit router/
    s).

o   The destination network.

o   Somewhere else in the path to the destination (e.g., transit
    providers).

Those cases, in terms of privacy considerations, will fall into one
of the following categories:

a. Failure cause is internal to a specific customer (LANs or router/
    s): The operator may decide, depending on their country
    regulations and services offered to that customer, to inform the
    customer (and decide what information is provided), or ignore the
    failure and include it in a "while list" (i.e., list of "don't
    care" failures), so the monitoring system doesn't keep providing
    alerts on it.

b. Failure cause is due to the operator network: The operator will
    need to find the cause and fix the failure, without disclosing
    any personal data.

c. Failure cause is due to third parties: The operator don't need to
    disclose any specific user source address/prefix, because in this
    case, the shorter prefix (typically the RIR allocated prefix or
    part of it, when is being announced split among different BGP
    peers), from which the failure has been verified.

In the most extreme case, a more restrictive usage of this procedure,
not involving logging any user source address/prefix, will be to log
only the failed destination address. In a big percentage of the
cases, it will be enough for the operator to detect the failure, as
experience shows that HE fall-back occurs mainly because path or
destination misconfiguration or issues. So, the ISP could replicate
the failure from any other source address in its network to the same
failed destination. If we take this approach, failures internal to a
specific customer, could not be reported by the operator to the
customer (as there is no source data logging), and together with
partial failures of the operator network will require extra work from
operator's staff to research the cause of the failure (i.e., it is in
my network, part of it, a specific customer or external).

So, there is no distinction between the privacy issues from this
protocol compared to regular network operation, abuse reporting, etc.

[6](). Security Considerations

This document does not have any specific security considerations.

[7](). IANA Considerations

IANA is requested to reserve 192.88.99.0/24 for this RFC, which was previously released by ([[RFC7526]()]).

[8](). Acknowledgements

The author would like to acknowledge the inputs of TBD ...

[9](). Normative References

[RFC5424]   Gerhards, R., "The Syslog Protocol", [RFC 5424](),
            DOI 10.17487/RFC5424, March 2009,
            <[https://www.rfc-editor.org/info/rfc5424]()>.

[RFC5426]   Okmianski, A., "Transmission of Syslog Messages over UDP",
            [RFC 5426](), DOI 10.17487/RFC5426, March 2009,
            <[https://www.rfc-editor.org/info/rfc5426]()>.

[RFC6555]   Wing, D. and A. Yourtchenko, "Happy Eyeballs: Success with
            Dual-Stack Hosts", [RFC 6555](), DOI 10.17487/RFC6555, April
            2012, <[https://www.rfc-editor.org/info/rfc6555]()>.

[RFC7050]   Savolainen, T., Korhonen, J., and D. Wing, "Discovery of
            the IPv6 Prefix Used for IPv6 Address Synthesis",
            [RFC 7050](), DOI 10.17487/RFC7050, November 2013,
            <[https://www.rfc-editor.org/info/rfc7050]()>.

[RFC7526]   Troan, O. and B. Carpenter, Ed., "Deprecating the Anycast
            Prefix for 6to4 Relay Routers", [BCP 196](), [RFC 7526](),
            DOI 10.17487/RFC7526, May 2015,
            <[https://www.rfc-editor.org/info/rfc7526]()>.

Authors' Addresses

   Jordi Palet Martinez
   The IPv6 Company
   Molino de la Navata, 75
   La Navata - Galapagar, Madrid 28420
   Spain

   Email: jordi.palet@theipv6company.com
   URI: [http://www.theipv6company.com/]()

   Carlos Martinez
   LACNIC
   Rambla Republica de Mexico, 6125
   Montevideo 11400
   Uruguay

   Email: carlos@lacnic.net
   URI: http://www.lacnic.net/