TRAM
Internet-Draft
Intended status: Experimental
Expires: April 24, 2017

P. Martinsen
S. Nandakumar
Cisco

October 21, 2016

DSCP mangle detection
draft-martinsen-tram-dscp-mangle-detection-00

Abstract

This document describes a mechanism for an endpoint to detect DSCP "mangling" by the network path.

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 April 24, 2017.

Table of Contents

1. Introduction

In some use-cases is useful to know if the network path changes the DSCP/TOS values in the IP header.

This document introduces a new STUN attribute that can carry the original DSCP/TOS values. This enables the remote receiver to compare the values in the IP header and the STUN attribute to detect mangling.

The information in the STUN attribute is probably of little interest for the remote receiver. The main use case is to collect metrics regarding how often DSCP values are mangled.

ICE could potentially also use this information to prefer paths with intact DSCP markings.

(Just assigning an attribute from IANA is possible, but we thought it was better to have a draft describing the attribute so everyone knows what it is)

2. Notational Conventions

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].

This specification uses terminology defined in ICE [RFC5245] And STUN [RFC5389].

3. Detecting DSCP mangling

Both ICE ICE [RFC5245] connectivity checks and TURN ICE [RFC5766] allocations can benefit from detecting if the DSCP bits survives the rough journey across the Internet ocean.

3.1. DSCP VALUE attribute

The IANA assigned STUN type for the new attribute is TBD-CA.

The format of the value in DSCP_VALUE attribute in the request is:

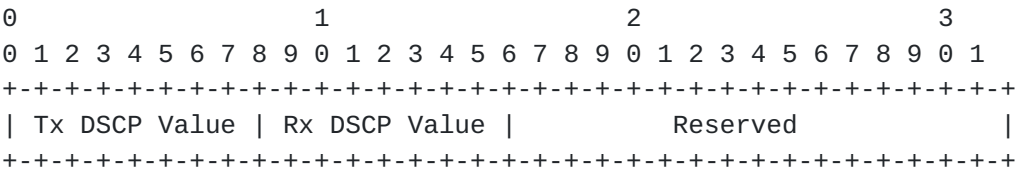

Figure 1: DSCP_VALUE attribute

The fields is described below:

Tx DSCP value: The DSCP/TOS field value if the IP header carrying the transmitted STUN packet.

Rx DSCP value: The DSCP/DOS field value if the IP header in received STUN packet on the same 5-tuple.

The padding is necessary to hit the 32-bit boundary needed for STUN attributes. The padding bits are ignored, but to allow for future reuse of these bits they MUST be set to 0.

3.2. Usage in Requests

When sending a STUN request in sets the Tx DSCP value field to the same value as the DSCP/TOS field in the IP header of the packet that is going to carry the STUN request. The Rx DSCP value MUST be set to 0.

3.3. Usage in Responses

This attribute MUST only be added to the response if it was present in the request.

The Tx DSCP value field is populated with the value of the DSCP/TOS field of the IP packet carrying the STUN response. the Rx DSCP value

is populated with the value from the DSCP/TOS field from the packet carrying the original receiving STUN request.

3.4. Example Operation

When a client receives the response it can compare the values of in the DSCP_VALUE attribute with values from the IP socket. The results could be used to detect and collect metrics regarding DSCP "survivability" on the Internet. It could potentially also influence ICE path decisions.

4. IANA Considerations

[Paragraphs in braces should be removed by the RFC Editor upon publication]

[The TRANSACTION_TRANSMIT_COUNTER attribute requires that IANA allocate a value in the "STUN attributes Registry" from the comprehension-optional range (0x8000-0xBFFF), to be replaced for TBD-CA throughout this document]

This document defines the DSCP_VALUE STUN attribute, described in Section 3. IANA has allocated the comprehension-optional code-point TBD-CA for this attribute.

5. Security Considerations

Security considerations discussed in [RFC5389] are to be taken into account. STUN requires the 96 bits transaction ID to be uniformly and randomly chosen from the interval 0 .. 2**96-1, and be cryptographically strong. This is good enough security against an off-path attacker. An on-path attacker can either inject a fake response or modify the values in DSCP_VALUE attribute to mislead the client and server. This attack can be mitigated using STUN authentication. As DSCP_VALUE is expected to be used between peers using ICE, and ICE uses STUN short-term credential mechanism the risk of on-path attack influencing the messages is minimal. If DSCP_VALUE is used with Allocate request then STUN long-term credential mechanism or STUN Extension for Third-Party Authorization [RFC7635] or (D)TLS connection can be used between the TURN client and the TURN server to prevent attackers from trying to impersonate a TURN server and sending bogus DSCP_VALUE attribute in the Allocate response.

The information sent in any STUN packet if not encrypted can potentially be observed passively and used for reconnaissance and later attacks.

6. Acknowledgements

Someone that provided feedback?

7. References

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

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, DOI 10.17487/RFC5245, April 2010, <http://www.rfc-editor.org/info/rfc5245>.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, DOI 10.17487/RFC5389, October 2008, <http://www.rfc-editor.org/info/rfc5389>.

[RFC5766] Mahy, R., Matthews, P., and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 5766, DOI 10.17487/RFC5766, April 2010, <http://www.rfc-editor.org/info/rfc5766>.

7.2. Informative References

[RFC7635] Reddy, T., Patil, P., Ravindranath, R., and J. Uberti, "Session Traversal Utilities for NAT (STUN) Extension for Third-Party Authorization", RFC 7635, DOI 10.17487/RFC7635, August 2015, <http://www.rfc-editor.org/info/rfc7635>.

Authors' Addresses

Paal-Erik Martinsen
Cisco Systems, Inc.
Philip Pedersens vei 22
Lysaker, Akershus 1325
Norway

Email: palmarti@cisco.com

Suhas Nandakumar
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134
USA

Email: snandaku@cisco.com