AVT
Internet-Draft
Updates: 3550 (if approved)
Intended status: Standards Track
Expires: November 6, 2010

A. Begen
Cisco
C. Perkins
University of Glasgow

May 5, 2010

Guidelines for Choosing RTP Control Protocol (RTCP) Canonical Names (CNAMEs)
draft-begen-avt-rtp-cnames-01

Abstract

The RTP Control Protocol (RTCP) Canonical Name (CNAME) is a persistent transport-level identifier for an RTP endpoint. While the Synchronization Source (SSRC) identifier of an RTP endpoint may change if a collision is detected, or when the RTP application is restarted, the CNAME is meant to stay unchanged, so that RTP endpoints can be uniquely identified and associated with their RTP media streams. For proper functionality, CNAMEs should be unique within the participants of an RTP session. However, the recommendations for choice of the RTCP CNAME provided in RFC 3550 are insufficient to achieve this uniqueness. This memo updates the guidelines in RFC 3550 to allow endpoints to choose unique CNAMEs.

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 November 6, 2010.

Copyright Notice

Table of Contents

1. Introduction

In Section 6.5.1 of [RFC3550], there are a number of recommendations for choosing the RTCP CNAME for an RTP endpoint. These recommend that the CNAME is of the form "user@host" for multiuser systems, or "host" if the username is not available. The "host" part is specified to be the fully qualified domain name of the host from which the real-time data originates, or the numeric representation of the IP address of the interface from which the RTP data originates for hosts that do not have a domain name.

As noted in [RFC3550], the use of private network address space [RFC1918] can result in hosts having network addresses that are not globally unique. However, this problem is not solely with private network addresses, but may also occur with public IP addresses, where multiple hosts are assigned the same public IP address and connected to a Network Address Translation (NAT) device [I-D.miles-behave-l2nat]. When multiple hosts share the same IP address, using the IP address as the CNAME can lead to non-unique CNAMEs.

[RFC3550] also notes that if hosts with private addresses and no direct IP connectivity to the public Internet have their RTP packets forwarded to the public Internet through an RTP-level translator, they may end up having non-unique CNAMEs. [RFC3550] suggests that such applications provide a configuration option to allow the user to choose a unique CNAME, and puts the burden on the translator to translate CNAMEs from private addresses to public addresses if necessary to keep private addresses from being exposed. Experience has shown that this does not work well in practice.

For all these reasons, this memo proposes alternative algorithms for choosing CNAMEs.

2. 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].

3. Choice of RTCP CNAME in Private Networks

It is a difficult task for a host to determine whether it resides behind a NAT without the help of an external mechanism such as STUN [RFC5389]. Furthermore, even some public IP addresses can be shared by multiple hosts in the Internet. Thus, using the numeric

representation of the IP address as the RTCP CNAME is NOT RECOMMENDED.

In order to meet the SHOULD requirement of Section 6.5.1 of [RFC3550], RTP endpoints SHOULD practice one of the following guidelines:

- Given that IPv6 addresses are naturally unique, a host MAY use its IPv6 address as the CNAME when using an IPv6 interface for RTP communication. If the RTP endpoint is associated with a unique local IPv6 unicast address [RFC4193], that address MAY be used as the CNAME as well. Using IPv6 addresses as CNAMEs was originally suggested in [RFC3550].

- A host that does not know its fully qualified domain name, and is configured with a private IP address on the interface it is using for RTP communication, MAY use the numeric representation of the layer-2 (MAC) address of the interface it is using for RTP communication as the "host" part of its CNAME. For IEEE 802 MAC addresses, such as Ethernet, the standard colon-separated hexadecimal format is to be used, e.g., "00:23:32:af:9b:aa".

- A host MAY use its Universally Unique IDentifier (UUID) [RFC4122] as the CNAME.

This memo does not mandate a specific order in which these methods should be practiced. A specific order would be only needed if an RTP endpoint was expected to be comprised of multiple programs that independently needed to choose the same CNAME. Since this is not a common implementation technique, a specific order is not needed.

4. Security Considerations

The security considerations of [RFC3550] apply to this document as well.

5. IANA Considerations

There are no IANA considerations in this document.

6. Acknowledgments

Thanks to Dan Wing who pointed out the concerns about cases where two hosts could share the same public IP address. Also, thanks to Marc Petit-Huguenin who suggested to use UUIDs as CNAMEs.

7. References

7.1. Normative References

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

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

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, July 2005.

7.2. Informative References

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, October 2008.

[I-D.miles-behave-l2nat] Miles, D. and M. Townsley, "Layer2-Aware NAT", draft-miles-behave-l2nat-00 (work in progress), March 2009.

Authors' Addresses

Ali Begen
Cisco
181 Bay Street
Toronto, ON M5J 2T3
CANADA

Email: abegen@cisco.com

Colin Perkins
University of Glasgow
Department of Computing Science
Glasgow, G12 8QQ
UK

Email: csp@csperkins.org