AVT
Internet-Draft
Updates: 3550 (if approved)
Intended status: Standards Track
Expires: February 27, 2011

A. Begen
Cisco
C. Perkins
University of Glasgow
D. Wing
Cisco

August 26, 2010

Guidelines for Choosing RTP Control Protocol (RTCP) Canonical Names (CNAMEs)

draft-ietf-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, its RTCP CNAME is meant to stay unchanged, so that RTP endpoints can be uniquely identified and associated with their RTP media streams. For proper functionality, RTCP CNAMEs should be unique within the participants of an RTP session. However, the existing guidelines for choosing the RTCP CNAME provided in the RTP standard are insufficient to achieve this uniqueness. This memo updates these guidelines to allow endpoints to choose unique RTCP CNAMEs.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

In Section 6.5.1 of the RTP specification, [RFC3550], there are a number of recommendations for choosing a unique RTCP CNAME for an RTP endpoint. However, in practice, some of these methods are not guaranteed to produce a unique RTCP CNAME. This memo updates guidelines for choosing RTCP CNAMEs, superceding those presented in Section 6.5.1 of [RFC3550].

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. Deficiencies with Earlier Guidelines for Choosing an RTCP CNAME

The recommendation in [RFC3550] is to generate an RTCP CNAME 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 (FQDN) of the host from which the real-time data originates. While this guidance was appropriate at the time [RFC3550] was written, FQDNs are no longer necessarily unique, and can sometimes be common across several endpoints in large service provider networks. Thus, the use of FQDN as the CNAME is strongly discouraged.

IPv4 addresses are also suggested for use in RTCP CNAMEs in [RFC3550], where the "host" part of the RTCP CNAME is the numeric representation of the IPv4 address of the interface from which the RTP data originates. As noted in [RFC3550], the use of private network address space [RFC1918] can result in hosts having network addresses that are not globally unique. Additionally, this shared use of the same IPv4 address can also occur with public IPv4 addresses if multiple hosts are assigned the same public IPv4 address and connected to a Network Address Translation (NAT) device [RFC3022]. When multiple hosts share the same IPv4 address, whether private or public, using the IPv4 address as the RTCP CNAME leads to RTCP CNAMEs that are not necessarily unique.

It is also noted in [RFC3550] 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 RTCP CNAMEs. The suggestion in [RFC3550] is that such applications provide a configuration option to allow the user to choose a unique RTCP CNAME, and puts the burden on the translator to translate RTCP 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.

4. Choosing an RTCP CNAME

It is difficult, and in some cases impossible, for a host to determine if there is a NAT between itself and its RTP peer. Furthermore, even some public IPv4 addresses can be shared by multiple hosts in the Internet. Thus, using the numeric representation of the IPv4 address as the "host" part of the RTCP CNAME is NOT RECOMMENDED.

4.1. Persistent RTCP CNAMEs vs. Per-Session RTCP CNAMEs

The RTCP CNAME can either be persistent across different RTP sessions for an RTP endpoint, or it can be unique per session, meaning that an RTP endpoint chooses a different RTCP CNAME for each RTP session.

An RTP endpoint that is emitting multiple related RTP streams that require synchronization at the other endpoint(s) MUST use the same RTCP CNAME for all streams that are to be synchronized. This requires a short-term persistent RTCP CNAME that is common across several RTP flows, and potentially across several related RTP sessions. A common example of such use occurs when lip-syncing audio and video streams in a multimedia session, where a single participant MUST use the same RTCP CNAME for its audio RTP session and for its video RTP session. Another example might be to synchronize the layers of a layered audio codec, where the same RTCP CNAME MUST be used for each layer.

A longer-term persistent RTCP CNAME is sometimes useful to facilitate third-party monitoring. One such use might be to allow network management tools to correlate the ongoing quality of service for a participant across multiple RTP sessions for fault diagnosis, and to understand long-term network performance statistics. Other, less benign, uses may also be envisaged. An implementation that wishes to discourage this type of third-party monitoring can generate a unique RTCP CNAME for each RTP session, or group of related RTP sessions, that it joins. Such a per-session RTCP CNAME cannot be used for traffic analysis, and so provides some limited form of privacy (note that there are non-RTP means that can be used by a third-party to correlate RTP sessions, so the use of per-session RTCP CNAMEs will not prevent a determined traffic analyst).

This memo defines several different ways by which an implementation can choose an RTCP CNAME. It is possible, and legitimate, for independent implementations to make different choices of RTCP CNAME when running on the same host. This may hinder third-party monitoring, unless some external means is provided to configure a persistent choice of RTCP CNAME for those implementations.

4.2. Requirements

An RTP endpoint that wishes to generate a persistent RTCP CNAME MUST use one of the following three methods:

- To produce a long-term persistent RTCP CNAME, and endpoint MUST generate and store a Universally Unique IDentifier (UUID) [RFC4122] for use as the "host" part of its RTCP CNAME. The string representation described in Section 3 of [RFC4122] MUST be used without "urn:uuid:", resulting in a 36 octet printable string representation.

- To produce a short-term persistent RTCP CNAME, an endpoint that has one or more IPv6 addresses MUST use one of those IPv6 address(es) as the "host" part of its RTCP CNAME, regardless of whether that IPv6 interface is being used for RTP communication or not. That address can be an IPv6 privacy address [RFC4941] or a unique local IPv6 unicast address [RFC4193]. The IPv6 address is converted to its textual representation [I-D.ietf-6man-text-addr-representation], resulting in a printable string representation as short as 3 octets and as long as 24 octets. Note: using IPv6 addresses as the "host" part of a CNAME was originally suggested in [RFC3550].

- To produce a short-term persistent RTCP CNAME, an endpoint that has only IPv4 addresses MUST use the numeric representation of the layer-2 (MAC) address of the interface that is used to initiate the RTP session as the "host" part of its RTCP 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" resulting in a 17 octet printable string representation. IPv4 addresses, whether public or private, SHOULD NOT be used as the RTCP CNAME host part, since they are not guaranteed to be unique.

In all three cases, the "user@" part of the RTCP CNAME MAY be omitted on single-user systems, and MAY be replaced by an opaque token on multiuser systems, to preserve privacy.

To generate a per-session RTCP CNAME, an endpoint MUST perform SHA1-HMAC [RFC2104] on the concatenated values of the RTP endpoint's initial SSRC, the source and destination IP addresses and ports, and a randomly-generated value [RFC4086], and then truncate the 160-bit output to 96 bits and finally convert the 96 bits to ASCII using Base64 encoding [RFC4648]. This results in a 16 octet printable string representation. Note that the RTCP CNAME MUST NOT change if an SSRC collision occurs, hence only the initial SSRC value chosen by the endpoint is used. The "user@" part of the RTCP CNAME is omitted when generating per-session RTCP CNAMEs.

5. Security Considerations

The security considerations of [RFC3550] apply to this memo.

In some environments, notably telephony, a fixed RTCP CNAME value allows separate RTP sessions to be correlated and eliminates the obfuscation provided by IPv6 privacy addresses [RFC4941] or IPv4 NAPT [RFC3022]. Secure RTP (SRTP) [RFC3711] can help prevent such correlation by encrypting Secure RTCP (SRTCP) but it should be noted that SRTP only mandates SRTCP integrity protection (not encryption). Thus, RTP applications used in such environments should consider encrypting their SRTCP or generate a per-session RTCP CNAME as discussed in Section 4.1.

6. IANA Considerations

No IANA actions are required.

7. Acknowledgments

Thanks to Marc Petit-Huguenin who suggested to use UUIDs in generating RTCP CNAMEs.

8. References

8.1. 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.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

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

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC4086] Eastlake, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

[I-D.ietf-6man-text-addr-representation] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", draft-ietf-6man-text-addr-representation-07 (work in progress), February 2010.

8.2. 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.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

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

Dan Wing
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA

Email: dwing@cisco.com