Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: August 20, 2012

T. Tsou
Huawei Technologies (USA)
A. Clauberg
Deutsche Telekom
M. Boucadair
France Telecom
S. Venaas
Cisco Systems
Q. Sun
China Telecom

February 17, 2012

Address Acquisition For Multicast Content When Source and Receiver Support Differing IP Versions
draft-tsou-mboned-multrans-addr-acquisition-00

Abstract

During the transition from IPv4 to IPv6, scenarios can occur where the IP version supported by the receiver differs from that supported by the source. This memo examines and evaluates alternative strategies for allowing the receiver to acquire multicast address information in such scenarios in the version it supports.

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 August 20, 2012.

Table of Contents

1. Introduction

Discussion of the multicast transition problem has focussed on the case of unidirectional delivery of multicast content. Within this scenario, the operation of viewing a program follows a well-defined sequence. For the sake of reducing the zapping delay, the list of multicast addresses is generally pre-provisioned to the receiver as part of the program guide prior to requesting access to the multicast content. At some subsequent time the user chooses to view a program, possibly by selecting it from a displayed program guide, or simply by selecting a channel. The receiver uses its pre-acquired information to signal to the network to receive the desired content. In particular, the receiver initiates reception of multicast content using the multicast group address and possibly a unicast source address supplied within the program information.

If the network, the source of the multicast content, and the receivers all use IPv4, it is evident that the program information will only include IPv4 multicast group addresses (and optionally, IPv4 unicast source addresses). Suppose now, as can occur in some transition scenarios, that IPv6-only receivers acquire program information containing these IPv4 addresses. Then there will be a mismatch: the IPv6-only receivers will be unable to use the addresses that are provided in the program information. This memo examines the possible strategies for remedying this mismatch, evaluating them in terms of their impact on receiver implementation and network operation.

This document makes reference to some of the scenarios described in Section 3 of [ID.jaclee-behave-v4v6-multicast-ps]. The remarks in Section 4.1 of [ID.jaclee-behave-v4v6-multicast-ps] are relevant to the problem considered here, but are more restricted in scope.

2. Which Problem Are We Solving?

In some transition scenarios, the source supports one IP version while the receiver and the provider network support the other (e.g., the source supports IPv4, the receiver and the network to which it is attached support IPv6). In this case, the problem stated above can be expressed as follows: how does the receiver acquire addresses of the IP version it supports, possibly with the help of the provider network?

In other transition scenarios, the source and provider network may support one IP version while the receiver supports another. In this case there are actually two problems: how the receiver acquires addresses that it supports (as already stated), and how to make those

addresses usable in a network supporting a different version? This second problem is the subject of a different memo and out of scope of the present one.

There is also a third class of scenarios, where the source and receiver support the same IP version but the intervening network supports a different one (e.g., the 4-6-4 scenario, Section 3.1 of [ID.jaclee-behave-v4v6-multicast-ps]). In those scenarios, delivering addresses of the right IP version to the receiver within the program guide is notionally a non-problem. The problem still can arise, if the intervening network intercepts and modifies the program guide to be consistent with the IP version it supports. In this case, the problem can be re-stated as: how can such modification be avoided when it is not needed?

3. Possible Solutions

This section explores three classes of solutions to the problem just described:

- reactive: the receiver recognizes that addresses it has received are in the wrong version and converts them through a request to a mapping function or using an in-built algorithm and accompanying configuration;

- dynamic modification: the network intercepts the access information and modifies it as necessary to meet the requirements of the receiver;

- administrative: the electronic program guide is modified in advance of its acquisition by the receiver to provide alternative address versions. Two variations on this strategy are identified.

3.1. The Reactive Strategy

According to this strategy, an IPv6 receiver receiving IPv4 addresses, for example, would recognize that they were the wrong version. As one possibility, it would package the addresses into one or two requests to a mapping function, which would return corresponding IPv6 addresses. In the 6-4-4 scenario (IPv6 receiver, IPv4 network and source), the mapping function could be located in another node at the user site or located in a dual-stack element at the provider edge. In the 6-6-4 case (IPv6 receiver and network, IPv4 source) it would have to be part of the provider network, although not necessarily at its edge.

This approach involves a fair amount of work to implement. Not only

does the receiver need to recognize that addresses are the wrong version; it also has to implement a new protocol to the mapping function. It also has to discover that function.

As an alternative, the receiver could implement an algorithm to perform the mapping itself, for example, synthesizing an IPv6 address given the IPv4 address of the source using the approach described by [ID.mboned-64-multicast-address-format] for multicast group addresses or [RFC6052] for unicast source addresses. In this case, the receiver must be configured with the IPv6 prefixes allocated for that purpose in the network to which the receiver is attached (e.g., using [ID.qin-softwire-multicast-prefix-option]). When applicable, this approach clearly has advantages over an approach using an external mapping function. It still requires implementation effort in the receiver, but at more limited level.

3.2. Dynamic Modification

This strategy puts the entire burden of address adaptation on the provider network. It requires that an element in that network must intercept program guide information destined to the receiver, locate the access information, and map IP addresses to an alternate version as necessary to suit the receiver. If the problem identified in the last paragraph of Section 2 is to be avoided, the intercepting element has to be aware of the version supported by each receiver.

As noted in the description of the OMA architecture in Appendix A, it is possible that such an adaptive function is present, but not clear that its scope would extend to IP version changes. The need to include IP version along with other receiver-related information might or might not prove to be administratively demanding. With the dynamic modification strategy the workload on the adaptation function might be large enough to make it a bottleneck in the process of program acquisition. The mitigating factor is that program metadata will typically be retrieved rather less often than program content.

This strategy has the clear advantage that it requires no changes in the receiver.

3.3. Administrative Preparation

The basic idea with this strategy is that the access information in the program metadata is set up to provide the right address version in advance of acquisition by any receiver. There are two basic approaches:

- separate alternative versions of the access information are prepared. The correct version is served up to the receiver when

it requests it. Like the dynamic modification strategy, this approach assumes that it is administratively feasible for the program guide server to know the IP version of the requesting receiver. That may or may not be true in a given operator's context. Also as with the dynamic modification approach, no change is required in the receiver. The big advantage over dynamic modification is that there is no need for the complications of an intercepting adapting element.

- The same access information instance contains alternative IP address versions. Where SDP is used, we can think of ICE or ICE-lite [RFC5245] or the proposed 'altc' mechanism [ID.boucadair-altc]. This requires receiver modification to recognize the alternative syntax and (in the case of ICE and potentially in the case of ICE-Lite) to take part in STUN exchanges. However, it means that the same access information can be served up to all receivers in a backward-compatible manner.

The administrative strategy requires that the network provider have control over the translations used in the preparation of the alternative versions of the access information. The network has to be aware of the translations used, so it can reuse them at other stages of the multicast acquisition process. Note networks owned by different operators are likely to have different mappings between IPv4 and IPv6 addresses, so if multiple receiving networks are downstream of the same source network, each of them may have to prepare and make available its own IPv6 version of the electronic program guide.

4. Conclusions

To come.

5. Acknowledgements

TBD

6. IANA Considerations

This memo includes no request to IANA.

7. Security Considerations

To come.

8. Informative References

[ID.boucadair-altc]
Boucadair, M., Kaplan, H., Gilman, R., and S. Veikkolainen, "Session Description Protocol (SDP) Alternate Connectivity (ALTC) Attribute (Work in Progress)", November 2011.

[ID.jaclee-behave-v4v6-multicast-ps]
Jacquenet, C., Boucadair, M., Lee, Y., Qin, J., and T. Tsou, "IPv4-IPv6 Multicast: Problem Statement and Use Cases (Work in Progress)", November 2011.

[ID.mboned-64-multicast-address-format]
Boucadair, M., Qin, J., Lee, Y., Venaas, S., Li, X., and M. Xu, "IPv4-Embedded IPv6 Multicast Address Format (Work in Progress)", February 2012.

[ID.qin-softwire-multicast-prefix-option]
Qin, J., Boucadair, M., and T. Tsou, "DHCPv6 Options for IPv6 DS-Lite Multicast Prefix (Work in Progress)", October 2011.

[MPEG-7_DDL]
ISO/IEC, "ISO/IEC 15938-2 (2002): "Information technology - Multimedia content description interface - Part 2: Description definition language".", 2002.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC4078] Earnshaw, N., Aoki, S., Ashley, A., and W. Kameyama, "The TV-Anytime Content Reference Identifier (CRID)", RFC 4078, May 2005.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, April 2010.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.

Appendix A. Some Background On Program Guides

Numerous organizations have been involved in the development of specifications for IPTV. Those specifications and the requirements of individual providers have influenced the development of existing receivers. Any solution to the multicast transition problem described in Section 1 has to take account of the effort involved not only in the direct development of a new generation of receivers, but also in evolving the specifications on which those receivers are based. It is thus worthwhile to review the current situation as it affects multicast transition.

The TV-Anytime forum (http://www.tv-anytime.org/) did early work in the area, formally terminating in 2005. Their work focussed on the description of program content, to facilitate the creation of such descriptions and their navigation by the user. The results are documented in the ETSI TS 102 822 series of technical specifications.

The content reference identifier (CRID) is a fundamental concept in the TV-Anytime data model. It refers to a specific piece of content or to other CRIDs, the latter thereby providing a method for grouping related pieces of content. TV-Anytime registered the CRID: URL schema in [RFC4078]. Quoting from the abstract of that document:

> The Uniform Resource Locator (URL) scheme "CRID:" has been devised to allow references to current or future scheduled publications of broadcast media content over television distribution platforms and the Internet.
>
> The initial intended application is as an embedded link within scheduled programme description metadata that can be used by the home user or agent to associate a programme selection with the corresponding programme location information for subsequent automatic acquisition.

The process of location resolution for the CRID: URL for an individual piece of content locates the content itself so that the user can access it. TV-Anywhere left the details of that process unspecified.

The Open IPTV Forum (http://www.oipf.tv) has focussed on defining the user-to-network interface, particularly for fixed broadband access. The architecture is based on the ETSI NGN (Next Generation Networks) model. The receiver obtains the actual access information for a given program, including the multicast group address and possibly a unicast source address, from XML-encoded program information following the Open IPTV Forum schema. The receiver uses SIP (Session Initiation Protocol [RFC3261]) signalling to obtain authorization and

resources for a session, before signalling at the multicast level to acquire the program. The SIP signalling conveys the multicast group address and the unicast source address, if available, in the form of an SDP (Session Description Protocol [RFC4566]) session description.

Finally, the Open Mobile Alliance (OMA, http://www.openmobilealliance.org/) has defined a series of specifications relating to broadcast services over wireless networks. The source and multicast group addresses used to acquire a given program instance are provided in SDP fragments either directly embedded in the primary electronic program guide or pointed to by it. The OMA architecture provides functionality to adapt access information within the program guide to the requirements of the transport network to which the user is attached, but this functionality appears to be primarily directed toward overcoming differences in technology rather than a general capability for modification.

In conclusion, it appears that there are at least two extant sources of specifications for the receiver interface, each providing its own data model, XML data schema, and detailed architecture. In the OMA case, the access information including the source and multicast group addresses is embedded as an SDP fragment within a larger set of XML-encoded program metadata. The OMA metadata can be supplied to the receiver in multiple segments, through multiple channels. This complicates the task of intercepting that metadata and modifying it in a particular transport network.

Authors' Addresses

Tina Tsou
Huawei Technologies (USA)
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4424
Email: Tina.Tsou.Zouting@huawei.com

Axel Clauberg
Deutsche Telekom
Deutsche Telekom AG, GTN-FM4
Landgrabenweg 151
Bonn, 53227
Germany

Phone: +4922893618546
Email: axel.clauberg@telekom.de

Mohamed Boucadair
France Telecom
Rennes, 35000
France

Phone:
Email: mohamed.boucadair@orange.com

Stig Venaas
Cisco Systems
Tasman Drive
San Jose, CA 95134
USA

Phone:
Email: stig@cisco.com

Qiong Sun
China Telecom
Room 708, No.118, Xizhimennei Street
Beijing, 100035
P.R.China

Phone: +86-10-58552936
Email: sunqiong@ctbri.com.cn