Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: February 1, 2016

T. Tsou
Huawei Technologies
A. Clauberg
Deutsche Telekom
M. Boucadair
France Telecom
S. Venaas
Cisco Systems
Q. Sun
China Telecom
September 2, 2015

Address Acquisition For Multicast Content When Source and Receiver Support Differing IP Versions
draft-ietf-mboned-multrans-addr-acquisition-06

Abstract

Each IPTV operator has their own arrangements for pre-provisioning program information including addresses of the multicast groups corresponding to broadcast programs on the subscriber receiver. 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 what has to be done to allow the receiver to acquire multicast address information in the version it supports in such scenarios.

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 September 3, 2015.

Table of Contents

1. Introduction

In the case of broadcast delivery of program content, the operation of viewing a program follows a well-defined sequence. For the sake of reducing channel switching delay, the list of multicast addresses is generally pre-provisioned to the receiver as part of the program guide. Each operator has their own solution for achieving this delivery, despite the attempts at standardization recounted in Appendix A.

At some later time, after the program guide is delivered, the user chooses to view a program, possibly by selecting it from a displayed program listing, 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 guide.

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 addresses. Suppose now, as can occur in some scenarios, that the program guide contains only IPv4 addresses and the receiver supports IPv6 only, or vice versa. Then there will be a mismatch: the receivers will be unable to use the addresses that are provided in the program guide. This memo examines the possible strategies for remedying this mismatch, evaluating them in terms of their impact on receiver implementation and network operation.

Note that the simplest solution might be to avoid mismatches by making sure that new receivers are dual stack rather than IPv6- only.

The remarks in Section 4.1 of [ID.mboned-v4v6-mcast-ps] are relevant to the problem considered here, but are more restricted in scope.

2. Which Problem Are We Solving?

In some 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 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.mboned-v4v6-mcast-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, a receiver recognizes that it has received multicast group addresses, even when they are the wrong version. As one possibility, it invokes an external mapping function to convert them to the version it supports. The mapping function could be located in another node at the user site or at a node in the provider network.

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 can 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.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 a 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)", April 2012.

[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)", May 2012.

[ID.mboned-v4v6-mcast-ps]
Jacquenet, C., Boucadair, M., Lee, Y., Qin, J., Tsou, T., and Q. Sun, "IPv4-IPv6 Multicast: Problem Statement and Use Cases (Work in Progress)", May 2012.

[ID.softwire-multicast-prefix-option]
Qin, J., Boucadair, M., Tsou, T., and X. Deng, "DHCPv6 Options for IPv6 DS-Lite Multicast Prefix (Work in Progress)", March 2012.

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

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
Bantian, Longgang District
Shenzhen 518129
P.R. China

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

Email: mohamed.boucadair@orange.com

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

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

MBONED WG
Internet-Draft
Intended status: Standards Track
Expires: April 29, 2018

M. McBride
C. Perkins
Huawei

October 26, 2017

Multicast Wifi Problem Statement
draft-mcbride-mboned-wifi-mcast-problem-statement-01

Abstract

There have been known issues with multicast, in an 802.11 environment, which have prevented the deployment of multicast in these wifi environments. IETF multicast experts have been meeting together to discuss these issues and provide IEEE updates. The mboned working group is chartered to receive regular reports on the current state of the deployment of multicast technology, create "practice and experience" documents that capture the experience of those who have deployed and are deploying various multicast technologies, and provide feedback to other relevant working groups. As such, this document will gather the problems of wifi multicast into one problem statement document so as to offer the community guidance on current limitations.

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 https://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 29, 2018.

Table of Contents

1. Introduction

Multicast over wifi has been used to low levels of success, usually to a point of being so negative that multicast over wifi is not allowed. In addition to protocol use of broadcast/multicast for control messages, more applications, such as push to talk in hospitals, video in enterprises and lectures in Universities, are streaming over wifi. And many end devices are increasingly using wifi for their connectivity. One of the primary problems multicast over wifi faces is that link local 802.11 doesn't necessarily support multicast, it supports broadcast. To make make multicast over wifi work successfully we often need to modify the multicast to instead be sent as unicast in order for it to successfully transmit with useable quality. Multicast over wifi experiences high packet error rates, no acknowledgements, and low data rate. This draft reviews these problems found with multicast over wifi. While this is not a solutions draft, common workarounds to some of the problems will be listed, along with the impact of the workarounds.

2. Multicast over WiFi Problems

802.11 is a wireless broadcast medium which works well for unicast and has become ubiquitous in its use. With multicast, however, problems arise over wifi. There are no ACKs for multicast packets,

for instance, so there can be a high level of packet error rate (PER) due to lack of retransmission and because the sender never backs off. It is not uncommon for there to be a packet loss rate of 5% which is particularly troublesome for video and other environments where high data rates and high reliability are required. Multicast, over wifi, is typically sent on a low date rate which makes video negatively impacted. Wifi loses many more packets then wired due to collisions and signal loss. There are also problems because clients are unable to stay in sleep mode due to the multicast control packets continuing to unnecessarily wake up those clients which subsequently reduces energy savings. Video is becoming the dominant content for end device applications, with multicast being the most natural method for applications to transmit video. Unfortunately, multicast, even though it is a very natural choice for video, incurs a large penalty over wifi.

One big difference between multicast over wired versus multicast over wired is that wired links are a fixed transmission rate. Wifi, on the other hand, has a transmission rate which varies over time depending upon the clients proximity to the AP. Throughput of video flows, and the capacity of the broader wifi network, will change and will impact the ability for QoS solutions to effectively reserve bandwidth and provide admission control.

The main problems associated with multicast over WiFi are as follows:

- Low Reliability
- Lower Data Rate
- High interference
- High Power Consumption

These points will be elaborated separately in the following subsections.

2.1. Low Reliability

Because of the lack of acknowledgement for packets from Access Point to the receivers, it is not possible for the Access Point to know whether or not a retransmission is needed. Even in the wired Internet, this characteristic commonly causes undesirably high error rates, contributing to the relatively slow uptake of multicast applications even though the protocols have been available for decades. The situation for wireless links is much worse, and is quite sensitive to the presence of background traffic.

2.2. Low Data Rate

For wireless stations associated with an Access Points, the necessary power for good reception can vary from station to station. For unicast, the goal is to minimize power requirements while maximizing the data rate to the destination. For multicast, the goal is simply to maximize the number of receivers that will correctly receive the multicast packet. For this purpose, generally the Access Point has to use a much lower data rate at a power level high enough for even the farthest station to receive the packet. Consequently, the data rate of a video stream, for instance, would be constrained by the environmental considerations of the least reliable receiver associated with the Access Point.

2.3. High Interference

As mentioned in the previous subsection, multicast transmission to the stations associated to an Access Point typically proceeds at a much higher power level than is required for unicat to many of the receivers. High power levels directly contribute to stronger interference. The interference due to multicast may extend to effects inhibiting packet reception at more distant stations that might even be associated with other Access Points. Moreover, the use of lower data rates implies that the physical medium will be occupied for a longer time to transmit a packet than would be required at high data rates. Thus, the level of interference due to multicast will be not only higher, but longer in duration.

Depending on the choice of 802.11 technology, and the configured choice for the base data rate for multicast transmission from the Access Point, the amount of additional interference can range from a factor of ten, to a factor thousands for 802.11ac.

2.4. High Power Consumption

One of the characteristics of multicast transmission is that every station has to be configured to wake up to receive the multicast, even though the received packet may ultimately be discarded. This process has a relatively large impact on the power consumption by the multicast receiver station.

3. Common remedies to multicast over wifi problems

One common solution to the multicast over wifi problem is to convert the multicast traffic into unicast. This is often referred to as multicast to unicast (MC2UC). Converting the packets to unicast is beneficial because unicast packets are acknowledged and retransmitted as needed to prevent as much loss. The Access Points (AP) is also

able to provide rate limiting as needed. The drawback with this approach is that the benefit of using multicast is defeated.

Using 802.11n helps provide a more reliable and higher level of signal-to-noise ratio in a wifi environment over which multicast (broadcast) packets can be sent. This can provide higher throughput and reliability but the broadcast limitations remain.

4. State of the Union

In discussing these issues over email and, most recently, in a side meeting at IETF 99, it is generally agreed that these problems will not be fixed anytime soon primarily because it's expensive to do so and multicast is unreliable. The problem of v6 neighbor discovery saturating the wifi link is only part of the problem. A big problem is that the 802.11 multicast channel is an afterthought and only given 100th of the bandwidth. Multicast is basically a second class citizen, to unicast, over wifi. Unicast may have allocated 10mb while Multicast will be allocated 1mb. There are many protocols using multicast and there needs to be something provided in order to make them more reliable. Wifi traffic classes may help. We need to determine what problem should be solved by the IETF and what problem should be solved by the IEEE.

Apple's Bonjour protocol, for instance, provides service discovery (for printing) that utilizes multicast. It's the first thing operators drop. Even if multicast snooping is utilized, everyone registers at once using Bonjour and the network has serious degradation. There is also a lot of work being developed to help save battery life such as the devices not waking up when receiving a multicast packet. If an AP, for instance, expresses a DTIM of 3 then it will send a multicast packet every 3 packets. But the reality is that most AP's will send a multicast every 30 packets. For unicast there's a TIM. But because multicast is going to everyone, the AP sends a broadcast to everyone. DTIM does power management but clients can choose to wake up or not and whether to drop the packet or not. Then they don't know why their bonjour doesn't work. The IETF may just need to decide that broadcast is more expensive so multicast needs to be sent wired. 802.1ak works on ethernet and wifi. 802.1ak has been pulled into 802.1Q as of 802.1Q-2011. 802.1Q-2014 can be looked at here: http://www.ieee802.org/1/pages/802.1Q-2014.html . If we don't find a generic solution we need to establish guidelines for multicast over wifi within the mboned wg. A multicast over wifi IETF mailing list is formed (mcast-wifi@ietf.org) and more discussion to be had there. This draft will serve as the current state of affairs.

This is not a solutions draft, but to provide an idea going forward, a reliable registration to Layer-2 multicast groups and a reliable multicast operation at Layer-2 could provide a generic solution. There is no need to support 2^24 groups to get solicited node multicast working: it is possible to simply select a number of trailing bits that make sense for a given network size to limit the amount of unwanted deliveries to reasonable levels. We need to encourage IEEE 802.1 and 802.11 to revisit L2 multicast issues. In particular, Wi-Fi provides a broadcast service, not a multicast one. In fact all frames are broadcast at the PHY level unless we beamform. What comes with unicast is the property of being much faster (2 orders of magnitude) and much more reliable (L2 ARQ).

5. IANA Considerations

None

6. Security Considerations

None

7. Acknowledgments

The following people have contributed information and discussion in the meetings and on the list which proved helpful for the development of the latest version this Internet Draft:

Dave Taht, Donald Eastlake, Pascal Thubert, Juan Carlos Zuniga, Mikael Abrahamsson, Diego Dujovne, David Schinazi, Stig Venaas, Stuart Cheshire, Lorenzo, Greg Shephard, Mark Hamilton

8. 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, <https://www.rfc-editor.org/info/rfc2119>.

Authors' Addresses

Mike McBride
Huawei
2330 Central Expressway
Santa Clara CA 95055
USA

Email: michael.mcbride@huawei.com

Charlie Perkins
Huawei
2330 Central Expressway
Santa Clara CA 95055
USA

Email: charlie.perkins@huawei.com