June 2023

APPLICATION-AWARE DELIVERY OF MULTICAST TRAFFIC

Mankamana Prasad Mishra

Nitin Kumar

Rajiv Asati

Cullen Jennings

Giles Douglas Yorke Heron

APPLICATION-AWARE DELIVERY OF MULTICAST TRAFFIC

AUTHORS:
Mankamana Prasad Mishra
Nitin Kumar
Rajiv Asati
Cullen Jennings
Giles Douglas Yorke Heron

ABSTRACT

Techniques are presented herein that support application layer replication to optimally deliver multicast traffic over either the public Internet or a service provider network. The presented techniques encompass extensions to Border Gateway Protocol (BGP)-based signaling mechanisms that may be employed to notify network devices (such as endpoints) of the presence of an application-aware multicast capability. The presented techniques further encompass a replicator component that a controller may dynamically launch and program. Multicast traffic, that would normally travel along a conventional delivery path, may then take a unicast path to such a replicator at which point replication may be performed more efficiently within the network.

DETAILED DESCRIPTION

A traditional multicast network environment is transport-driven, where the transport protocol is responsible for creating a multicast distribution tree. Figure 1, below, presents elements of a typical multicast network which may be deployed across an industry.

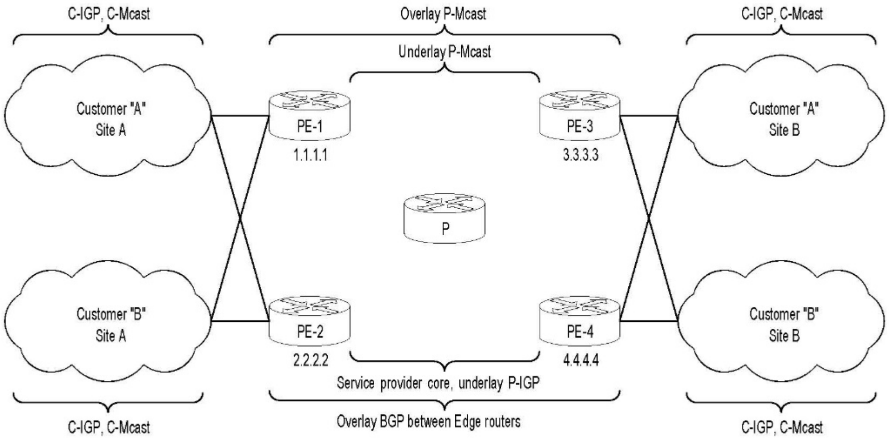

Figure 1: Exemplary Multicast Network

The exemplary multicast network that is shown in Figure 1, above, includes a number of different elements, various of which are identified in Table 1, below.

Table 1: Network Elements

Element	Description
C-IGP	An interior gateway protocol (IGP) instance running inside a customer network
C-Mcast	A multicast instance running inside a customer network
P-IGP	An IGP instance running inside of a provider network
P-Mcast	A multicast instance running inside of a provider network

Further, the exemplary network of Figure 1, above, encompasses two additional elements, an edge device which typically plays the role of a first hop router (FHR) for a multicast service (and to which, typically, sources are connected) and an edge device which typically plays the role of a last hop router (LHR) for a multicast service (and to which, typically, receivers are connected).

Currently, a customer may employ their own multicast network over which they may operate a Protocol-Independent Multicast (PIM) protocol or some other multicast protocol. Additionally, there is another layer of overlay and underlay signaling that is required in order to create the necessary trees in a service provider network. Since there can be a very large number of customer multicast flows, a service provider typically does not wish to create that many states and prefers, instead, to control the number of trees by aggregating together multiple customer flows.

However, such an approach raises a number of challenges. First, whenever a new transport migration takes place, there is a huge development cost associated with supporting multicast flows. For example, consider a transition from an Internet Protocol (IP) approach to a Multiprotocol Label Switching (MPLS) technique to a segment routing-based MPLS (SR-MPLS) approach to a segment routing paradigm that is applied to an IP version 6 underlay (SRv6). In each transition there are development efforts necessary to support multicast flows.

Second, additional skill sets are required to maintain and deploy multicast flows, which adds to the enterprise's operational costs. Third, visibility may be an issue for multicast flows due to flow aggregation. And fourth, with aggregation it is necessary to deliver traffic to sites where there are no active receivers.

Techniques are presented herein that move the above-described replication logic to an application layer instead of keeping it in a transport layer, achieving a multicast edge and unicast core orientation.

Recent market research validates the need for the presented techniques. Many vendors have begun looking into such an approach, as Internet-based high-interest live events reach new levels and bitrates increase to support the streaming of 4K resolution video, 8K resolution video, and augmented reality, all of which place unique stresses on a network. Additionally, enterprises have begun looking for alternate ways to deliver multicast traffic without using the existing procedures which are difficult to deploy and debug. While different entities are trying to solve the problem in different ways, the current Internet Engineering Task Force (IETF) trend (which encompasses a QUIC-based approach) demonstrates that this problem is real and requires a solution.

The scope of the presented techniques ranges from one provider edge device to another provider edge device. This is the area where a Border Gateway Protocol (BGP)-based Layer 3 virtual private network (L3VPN) for unicast traffic and a multicast virtual private network (mVPN) for multicast traffic may be deployed.

At a high level, the presented techniques encompass extensions to BGP-based signaling mechanisms that may be employed to notify devices of the presence of an application-aware multicast capability. Under aspects of the presented techniques a headend device may perform a handoff procedure by passing a multicast flow to a QUIC-based application and BGP extensions may be employed to provide all of the endpoints with application information where multicast traffic is expected. Under further aspects of the presented techniques a controller may dynamically program replication points within a network and endpoints may decode back a multicast flow.

The techniques presented herein may be further understood through the illustrative arrangement that is presented in Figure 2, below.

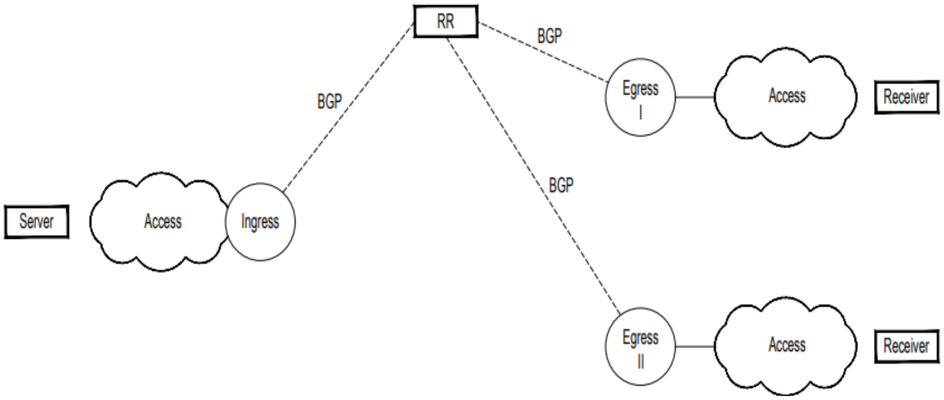

Figure 2: Illustrative Arrangement

The topology that is depicted in Figure 2, above, expresses a simple network comprising two sites to which the same video content needs to be delivered. Using BGP's auto discovery mode, additional information may be exchanged to notify all of the end devices that support exists for application-aware multicasting. Figure 3, below, illustrates elements of such activity.

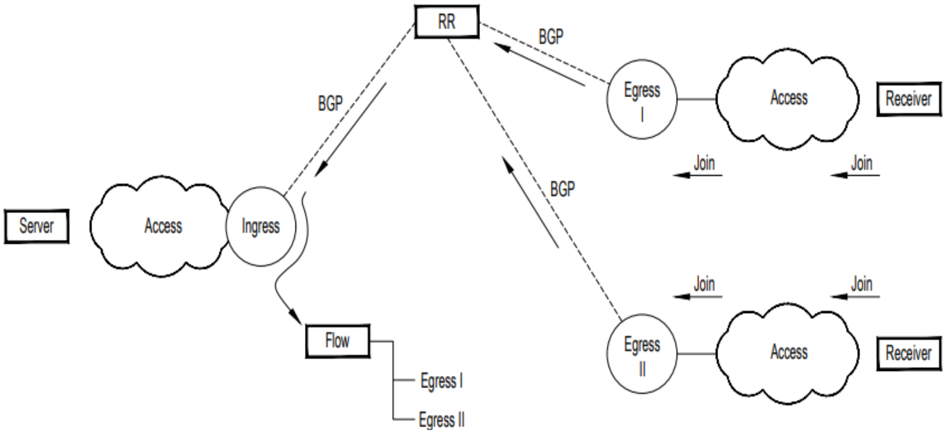

Figure 3: Exchange of Additional Information

As shown in Figure 3, above, when a membership (e.g., a join) request is received from an access network, the signaling of the same to an ingress edge device may be conveyed through BGP using an overlay mechanism. Figure 4, below, illustrates elements of such activity.

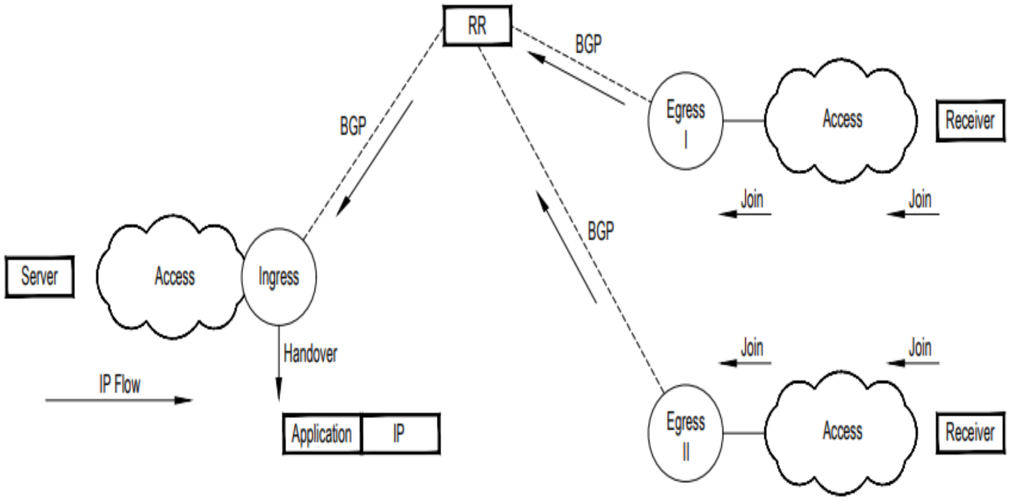

Figure 4: Exemplary Signaling

As depicted in Figure 4, above, after a server begins sending multicast traffic, that traffic may be handed over to an application for delivery. Then, a controller may examine the locations of the ingress and egress devices, dynamically launch a replicator, and program information about the instant flow. Figure 5, below, illustrates elements of such activity.

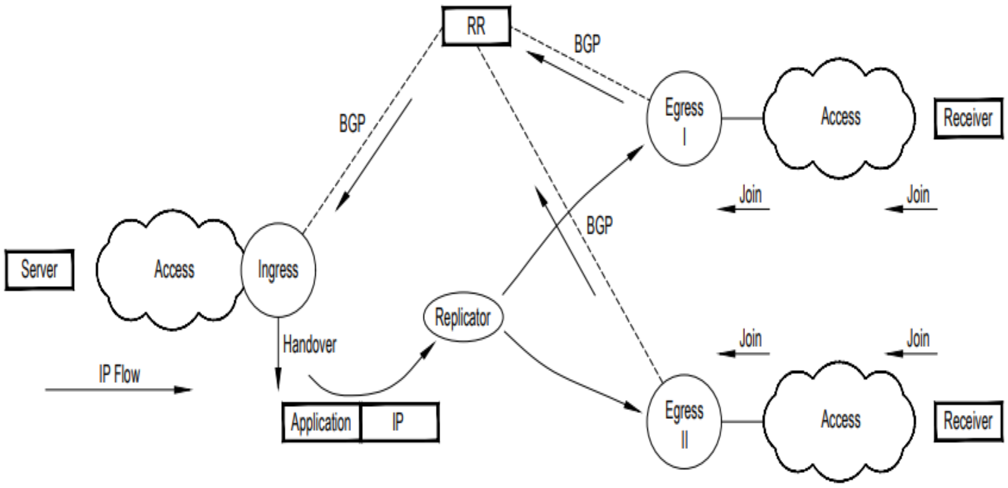

Figure 5: Illustrative Replicator

As shown in Figure 5, above, the traffic may take a unicast path to a replicator and replication may then be performed within the network. According to the presented techniques, a number of different options may be employed for such replication.

A first option encompasses the use of User Datagram Protocol (UDP)-based proxy replication, wherein replication may occur within a proxy towards multiple endpoints of a next set of proxies. Under such an approach, a Real-time Transport Protocol (RTP) or Real-Time Transport Control Protocol (RTCP) layer would be aware of the traffic that is being multicast.

A second option encompasses the use of RTP-based proxy replication, wherein replication may occur within a proxy (as with the first option that was described above) but such a proxy may also implement various supporting capabilities like forward error correction (FEC), acknowledgement (ACK) and negative-acknowledgement (NACK), etc. Such an approach may be too complex for a router's application-specific integrated circuits (ASICs) so the necessary functionality may be implemented in either cloud-native RTP proxies or application containers on a router. Further, such an approach may be combined with an SRv6 layer in a network so that an RTP-based proxy may impose the binding segment identifier (SID) with a controller programing the RTP-based proxies and the SRv6 routers.

It is important to note that the presented techniques also provide an opportunity for the deployment of proxy devices throughout the public Internet in support of accomplishing replication.

The use of the techniques presented herein offers a number of benefits. Compared to an existing mVPN mechanism or other multicast procedure, the most significant benefit encompasses visibility and the ability to reuse a unicast traffic engineered path. Since replication happens under the presented techniques at an application layer, for the balance of a network that traffic may be delivered as unicast traffic which is easier to account for compared to multicast traffic. An additional benefit encompasses the fact that there is currently no way to accomplish a multicast flow in the public Internet. Through the presented techniques, a replicator may be introduced into the public Internet in support of replication through the same.

In summary, techniques have been presented herein that support application layer replication to optimally deliver multicast traffic over either the public Internet or a service provider network. The presented techniques encompass extensions to BGP-based signaling mechanisms that may be employed to notify network devices (such as endpoints) of the presence of an application-aware multicast capability. The presented techniques further encompass a replicator component that a controller may dynamically launch and program. Multicast traffic, that would normally travel along a conventional delivery path, may then take a unicast path to such a replicator at which point replication may be performed more efficiently within the network.