Extranet in BGP Multicast VPN (MVPN)

draft-raggarwa-l3vpn-bgp-mvpn-extranet-06.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.
Abstract

This document describes clarifications and extensions to the procedures in [BGP-MVPN] for supporting extranets. The procedures specified in this document assume that BGP is used for transmission of MVPN customers’ multicast routing information within the service provider(s) infrastructure.
1. Specification of requirements

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].
2. Introduction

The extranet functionality that allows a MVPN site to receive/send multicast traffic from/to sites of other MVPNs is a requirement of RFC4834 [RFC4834] (section 5.1.6).

This document describes clarifications and extensions to the procedures in [BGP-MVPN] for supporting extranets. The procedures described in this document assume that BGP is used for transmission of MVPN customers' multicast routing information within the service provider(s) infrastructure [BGP-MVPN].

3. Extranet Service Model

In the context of MVPN the term "extranet" refers to the ability for multicast sources in one MVPN to send multicast traffic to multicast receivers in other MVPN(s), and likewise, the ability for multicast receivers in one MVPN to receive multicast traffic from multicast sources in other MVPN(s). Such multicast sources are referred to as "extranet sources". The multicast groups to which the extranet sources generate traffic are referred to as "extranet groups". The receivers that receive multicast traffic from extranet sources are referred to as "extranet receivers".

If a given VRF has (multicast) receivers behind attached CEs that can receive multicast traffic sourced in the configured set of extranet MVPNs, then the (unicast) addresses of these sources MUST be unambiguous both among these extranet MVPNs, as well as between any of these extranet MVPNs and the MVPN of the VRF.

Moreover, if a given VRF has (multicast) receivers behind attached CEs that can receive multicast traffic sourced in the configured set of extranet MVPNs, then the group addresses within the ASM range that these receivers can join MUST be unambiguous both among these extranet MVPNs, as well as between any of these extranet MVPNs and the MVPN of the VRF.
4. Routing Exchange in Support of Extranets

If a given VRF has (multicast) receivers behind attached CEs that can receive multicast traffic sourced in the configured set of extranet MVPNs, then this VRF MUST be able to import the "necessary" unicast and BGP MVPN auto-discovery routes advertised by other PEs for the MVPNs that contain the extranet sources.

The "necessary" routes are the routes required by the VRF to receive multicast traffic for the extranet sources and groups from other MVPNs. This includes unicast VPN-IP routes to the extranet sources, as well as BGP MVPN Source Active auto-discovery routes for the extranet sources and groups. It also includes Intra-AS, Inter-AS and S-PMSI auto-discovery routes that carry P-Tunnel attributes for the P-Tunnels used by the other MVPNs for sending multicast traffic for multicast sources and groups.

4.1. Exchange of Unicast Routes

Case 1: PIM-SM in SSM mode. To fit the SSM model, if a given (C-S, C-G) is in the extranet, then C-S should be in the extranet as well (or to be more precise, the VPN-IP route to C-S has to be advertised in the extranet).

Case 2: PIM-SM in ASM mode. To fit the ASM model, if a given C-G is in the extranet, then the C-RP for that C-G and all the C-Ss sending to that C-G should be in the extranet as well (or to be more precise, all the VPN-IP routes to C-RP and these C-Ss have to advertised in the extranet). Note that for a given C-G that is part of the extranet formed by several MVPNs, C-Ss for that C-G may be present in any of these MVPNs.

For both ASM and SSM modes, the VRFs connected to the sites that have extranet receivers for a given extranet source MUST be able to import a VPN-IP route to that source. In addition, for the ASM mode the VRFs connected to the sites that have extranet receivers for a given extranet group MUST be able to import a VPN-IP route to the C-RP of that extranet group.
4.2. Exchange of Source Active and S-PMSI auto-discovery routes

When all the VPN-IP routes originated by the same VRF carry the same set of RTs, then as long as the Source Active auto-discovery routes and S-PMSI auto-discovery routes use the default setting for their RTs (as specified in [BGP-MVPN]), setting up the appropriate RTs for the VPN-IP routes, would also result in the appropriate import of Source Active auto-discovery routes and S-PMSI auto-discovery routes.

When different VPN-IP routes originated by the same VRF carry different RTs, then the following rules result in the appropriate import of Source Active auto-discovery routes and S-PMSI auto-discovery routes:

+ By default a Source Active auto-discovery route for a given (C-S, C-G) MUST carry the same RT(s) as the VPN-IP route for C-S.

+ By default an S-PMSI auto-discovery route for a given (C-S, C-G) or (C-S, C-*) MUST carry the same RT(s) as the VPN-IP route for C-S.

+ By default an S-PMSI auto-discovery route for a given (C-*, C-G) MUST carry the same RT(s) as the VPN-IP route(s) for the multicast sources that are in the sites connected to that VRF and that originate (multicast) traffic for that C-G.

4.3. Exchange of I-PMSI auto-discovery routes

A VRF connected to the site(s) that have extranet receivers for a given extranet source MUST be able to import the I-PMSI auto-discovery route originated by the VRF connected to the source. Note that as long as the I-PMSI auto-discovery routes use the default setting for their RTs (as specified in [BGP-MVPN]), setting up the appropriate RTs for the VPN-IP routes, would also result in the appropriate import of I-PMSI auto-discovery routes.

If a given VRF connected to a given extranet source uses P2MP RSVP-TE as an inclusive P-tunnel to carry (multicast) traffic from that source, then the RT(s) carried by the I-PMSI auto-discovery routes originated by the VRFs connected to the sites that have the extranet receivers for that source, and the import RT(s) of the VRF connected to the (extranet) source MUST be such that these routes will be imported into that VRF.
5. Originating C-multicast routes

Procedures specified in section "Constructing the rest of the C-multicast route" of [BGP-MVPN] are modified as follows. If the local and the upstream PEs are in different ASes, then the local PE has to find in its VRF not just an Inter-AS I-PMSI A-D route whose Source AS field carries the autonomous system number of the upstream PE (as specified in section 11.1.3 of [BGP-MVPN]), but an Inter-AS I-PMSI A-D route whose Source AS field carries the autonomous system number of the upstream PE, and whose RTs form a non-empty intersection with the RTs carried in the VPN-IP route imported into that VRF for the address carried in the Multicast Source field of MCAST-VPN NLRI.

6. Multicast Extranet over Selective P-tunnels

In the following we consider only the S-PMSI auto-discovery routes used for the extranets.

6.1. Non-aggregated S-PMSIs

When each S-PMSI auto-discovery routes originated from a VRF on a given PE advertises a distinct P-tunnel in the PMSI Tunnel attribute, the procedures in [BGP-MVPN], along with the routing exchange clarifications described above, are sufficient to support the scenario when the multicast extranet traffic is carried over selective P-tunnels (P-tunnels advertised by the S-PMSI auto-discovery routes).

An implementation MUST support multicast extranets with non-aggregated S-PMSIs.

6.2. Aggregated S-PMSIs

When multiple S-PMSI auto-discovery routes originated from a VRF on a given PE advertise the same P-tunnel in the PMSI Tunnel attribute, and each such route also advertises a distinct (upstream assigned) label in the attribute, then the procedures in [BGP-MVPN], along with the routing exchange clarifications described above, are sufficient.

When multiple S-PMSI auto-discovery routes originated from a VRF on a given PE advertise the same P-tunnel in the PMSI Tunnel attribute, and the PMSI Tunnel attribute of each of these routes does not carry a distinct (upstream assigned) label per route, then in addition to the procedures in [BGP-MVPN] and the routing exchange clarifications described above, the following is required.
When the local PE receives from some other PE (C-S, C-G) traffic on a P-tunnel that the other PE advertised in an S-PMSI auto-discovery route that has been imported into a VRF on the local PE, the local PE performs procedures specified in section 12.3 of [BGP-MVPN] only if: (1) the VRF does contain an S-PMSI auto-discovery route for (C-S, C-G), and (2) the (C-S, C-G) traffic is received on the P-tunnel advertised in the PMSI Tunnel attribute of that route, and (3) RTs of that route form a non-empty intersection with the RTs carried in the VPN-IP route for C-S imported into that VRF. Otherwise, if at least one of the above conditions is false, the local PE MUST discard (and not forward) this traffic.

An implementation SHOULD support multicast extranets with aggregated S-PMSI.

7. Multicast Extranet over Inclusive P-tunnels

There are (at least) four possible ways to support extranet multicast over inclusive P-tunnels.

7.1. Option 1

This option assumes that the set of the extranet sources within a given VRF is the same as the set of the multicast sources within that VRF.

Procedures in [BGP-MVPN], along with the routing exchange clarifications described above, are sufficient to support this option.

An implementation MUST support this option.

7.2. Option 2

Each VRF that has set of extranet sources being part of that VRF uses not one, but two inclusive P-tunnels for sending multicast traffic. The first one is used for sending multicast traffic from the non-extranet sources; the second is used for sending multicast traffic from the extranet sources.

Each of these P-tunnels is advertised by its own I-PMSI auto-discovery route. Therefore, these two routes MUST NOT use the same RD. The distribution scope of the second route SHOULD include all the VRFs that are within the scope of the first route, plus all the other VRFs that have the extranet receivers for the extranet sources of the
VRF that originates the route. Thus the P-tunnel advertised by the second route spans all the VRFs spanned by the P-tunnel advertised by the first route, plus all the VRFs that have the extranet receivers for the extranet sources of the VRF that originates the route.

The set of RTs carried by the first I-PMSI auto-discovery route follows the rules specified in [BGP-MVPN]. The set of RTs carried by the second I-PMSI auto-discovery route MUST form a non-empty intersection with the RTs carried by the VPN-IP routes for the extranet multicast sources in the VRF that originates the route.

To carry (C-S, C-G) multicast traffic the PE by default should use the P-tunnel that the PE advertises in the I-PMSI auto-discovery route that has the same set of RTs as the VPN-IP route to C-S advertised by the PE.

When the local PE receives from other PEs (multicast) traffic corresponding to the (multicast) state advertised in the C-multicast route originated from given VRF on the local PE, the PE MUST discard (and not forward) this traffic if it was received on a P-tunnel that is advertised by an I-PMSI auto-discovery route that has been imported into the VRF, and whose RTs form an empty intersection with the RTs carried in the VPN-IP route imported into that VRF for the address carried in the Multicast Source field of MCAST-VPN NLRI. Note that this check is in addition to the checks specified in section 9.1 of [MVPN-ARCH].

An implementation SHOULD support this option.

7.3. Option 3

Each VRF has just one inclusive P-tunnel that is used to send data originated by the sites connected to that VRF. In this case if the set of extranet multicast sources are part of that VRF, then all other VRFs that are part of the extranet must be able to receive data on that P-tunnel (all these VRFs must be able import the I-PMSI auto-discovery route that advertises this P-tunnel).

In addition to the rules specified in [BGP-MVPN], the set of RTs carried by the I-PMSI auto-discovery route that advertises this P-tunnel MUST form a non-empty intersection with the RTs carried by the VPN-IP routes for the extranet multicast sources in that VRF.

Moreover, with this option the set of RTs of the I-PMSI auto-discovery routes originated by the VRFs that contain extranet multicast sources MUST be the same as in the absence of the extranet. The route import policy for both intra-AS and inter-AS I-PMSI auto-
discovery routes on the VRFs that have receivers for the (multicast) traffic originated by these sources MUST be such that these VRF MUST be able to import these routes.

A VRF that is receiving traffic on an inclusive P-tunnel from the extranet sources connected to another VRF may also receive on that P-tunnel the non-extranet traffic from that VRF. Such traffic will be dropped by the receiving VRF anyway if it doesn’t have (C-S, C-G) or (C-*, C-G) forwarding state for this non-extranet traffic. However, the receiving VRF may have forwarding state for such traffic if the address space for the non-extranet sources connected to the sending VRF overlaps with the address space of the sources in the receiving VRF’s MVPN. To take care of this case the receiving VRF MUST be able to drop the non-extranet traffic if it arrives on the unexpected P-Tunnel. The following describes how the unexpected P-Tunnel is determined.

When the local PE receives from other PEs (multicast) traffic corresponding to the (multicast) state advertised in the C-multicast route originated from given VRF on the local PE, the PE MUST discard (and not forward) this traffic if it was received on a P-tunnel that is advertised by an I-PMSI auto-discovery route that has been imported into the VRF, and whose RTs form an empty intersection with the RTs carried in the VPN-IP route imported into that VRF for the address carried in the Multicast Source field of MCAST-VPN NLRI. Note that this check is in addition to the checks specified in section 9.1 of [MVPN-ARCH].

An implementation SHOULD support this option.

7.4. Option 4

Each VRF that has set of extranet multicast sources being part of that VRF is a root of as many inclusive P-tunnels as the number of MVPNs in the extranet. A given (C-S, C-G) multicast traffic has to be sent over each of these P-tunnels. From the point of view of the number of P-tunnels, and the amount of replication required this is the least desirable option, and is included here just for the sake of completeness.
8. Multiple Extranet VRFs on the same PE

When multiple VRFs that contain extranet receivers for a given extranet source are present on the same PE, this PE becomes a single leaf of the P-tunnel used for sending (multicast) traffic from that source to these extranet receivers. Specific procedures for replicating this traffic on that PE to these multiple VRFs are a purely local to the PE matter, and thus are out of the scope of this document.

For a given extranet the site(s) that contain the extranet source(s) and the site(s) that contain the extranet receiver(s) may be connected to the same PE. In this scenario the procedures by which (multicast) traffic from these sources is delivered to these receivers is purely local matter to the PE matter, and thus are outside the scope of this document.

An implementation MUST support multiple extranet VRFs on a PE.

9. IANA Considerations

This document does not impose any new IANA considerations.

10. Security Considerations

A VRF must be able to drop non-extranet traffic, if it receives such traffic from another PE. The procedures for dropping such traffic are described in this document.

11. Acknowledgements

The authors would like to thank Eric Rosen for his comments.
12. References

12.1. Normative References

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels.", Bradner, March 1997


[BGP-MVPN], R. Aggarwal, E. Rosen, T. Morin, Y. Rekhter, "BGP Encodings for Multicast in MPLS/BGP IP VPNs", draft-ietf-l3vpn-2547bis-mcast-bgp, work in progress

12.2. Informative References


13. Authors’ Addresses

Rahul Aggarwal
Juniper Networks
1194 North Mathilda Ave.
Sunnyvale, CA 94089
Email: rahul@juniper.net

Yakov Rekhter
Juniper Networks
1194 North Mathilda Ave.
Sunnyvale, CA 94089
Email: yakov@juniper.net

Thomas Morin
France Telecom - Orange Labs
2, avenue Pierre-Marzin
22307 Lannion Cedex
France
Email: thomas.morin@orange-ftgroup.com

Wim Henderickx
Alcatel-Lucent
e-mail: wim.henderickx@alcatel-lucent.be