Extranet in BGP Multicast VPN

draft-raggarwa-l3vpn-bgp-mvpn-extranet-00.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 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

This document describes clarifications 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 [BGP-MVPN].

The extranet functionality is a requirement of RFC4834 [RFC4834] (section 5.1.6) and allows a VPN site to receive or send multicast traffic from sites (or to sites) of another VPN.
3. Extranet Service Model

In the context of MVPN the term "extranet" refers to the ability for multicast sources in one VPN to send multicast traffic to multicast receivers in other VPN(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".

The IP addresses used by extranet sources MUST NOT overlap with the IP addresses used by VPNs that receive multicast traffic from such sources. Moreover, in the case of PIM-SM in ASM mode addresses used by extranet groups MUST NOT overlap with the group addresses used by VPNs that have receivers for the extranet groups.

4. Routing Exchange in Support of Extranets

VRFs in the VPN that wish to access multicast extranet sources in other VPNs MUST be able to import the "necessary" unicast and BGP MVPN auto-discovery routes advertised by other PEs for VPNs that contain the extranet sources.

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

Case 1: PIM-SM in SSM mode. In this scenario a necessary condition for (C-S,C-G) traffic received on a particular VRF to be forwarded downstream is for the VRF to have a VPN-IP route to C-S. In other words the route to C-S must be advertised in the extranet. If this condition is not satisfied the traffic is discarded by the VRF when received from a CE.

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 VPNs, C-Ss for that C-G may be present in any of these VPNs.
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. This could be accomplished by either (a) setting the appropriate RTs that control import of VPN-IP routes on the VRFs connected to the receivers, or (b) setting the appropriate RTs that control export of VPN-IP routes on the VRF connected to the source.

Note that as long as the Source Active auto-discovery routes and S-PMSI auto-discovery routes use the default setting for their RTs, setting up the appropriate RTs for VPN-IP routes, as described above, would also result in the appropriate import of Source Active auto-discovery routes, and S-PMSI auto-discovery routes.

In addition, VRFs connected to the sites that have extranet receivers for a given extranet source MUST be able to import I-PMSI auto-discovery route originated by the VRF connected to the source. This could be accomplished by either (a) setting the appropriate RTs that control import of I-PMSI auto-discovery routes on the VRFs connected to the receivers, or (b) setting the appropriate RTs that control export of I-PMSI auto-discovery routes on the VRF connected to the source.

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 this VRF MUST also be able to import intra-AS I-PMSI auto-discovery routes originated by the VRFs connected to the sites that have extranet receivers for that source.

5. Multicast Extranet over Selective P-tunnels

Procedures in [BGP-MVPN] along with the routing exchange clarifications described in the previous section, are sufficient to support the scenario when the multicast extranet traffic is carried over selective P-tunnels (P-tunnels advertised by S-PMSI auto-discovery routes).

6. Multicast Extranet over Inclusive P-tunnels

There are (at least) three possible ways to support extranet multicast over inclusive P-tunnels.
6.1. Option 1

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 will be 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.

To carry (C-S, C-G) multicast traffic the PE by default should use the P-tunnel that has been advertised 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.

A special case of this option is the scenario where the set of extranet sources within a given VRF is the same as the set of multicast sources within that VRF. In this case there is no need to have two P-tunnels - one P-tunnel would suffice. As a result only one I-PMSI auto-discovery route would need to be originated by that VRF.

6.2. Option 2

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).

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) forwarding state for this non-extranet traffic. 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 VPN. 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 by 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 whose RTs form an empty intersection with the RTs carried in the VPN-IP route for the address carried in the Multicast Source field of MCAST-VPN NLRI. This check is in addition to the checks specified in section 9.1 of [MVPN-ARCH].

Note that for the above procedure to work, there should be a consistent choice with respect to handling import/export of VPN-IP routes and I-PMSI auto-discovery routes. That is, either (a) the import/export of both types of routes should be controlled by setting the appropriate RTs on the VRFs connected to the receivers, or (b) the import/export of both types of routes should be controlled by setting the appropriate RTs on the VRF connected to the source.

7. Option 3

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. IANA Considerations

This document does not impose any new IANA considerations.

9. Security Considerations

A VRF must be able to drop non-extranet traffic, if it receives such traffic from another PE. This is possible when an extranet VRF has both extranet and non-extranet sources and option 2 described in section 6 is used by that VRF to send traffic to other PEs. The procedures for dropping such traffic are described in section 6.
10. Acknowledgements

11. References

11.1. Normative References

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


11.2. Informative References


12. Author’s Address

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

Praveen Muley
Alcatel-Lucent
e-mail: Praveen.Muley@alcatel-lucent.com