L3VPN Working Group
Internet Draft
Intended Status: Standards Track
Expires: August 8, 2013
Updates: 6513,6514,6625

Yakov Rekhter (Editor)
Juniper Networks

Eric Rosen (Editor)
Cisco Systems

Rahul Aggarwal
Arktan

Yiqun Cai
Microsoft

Wim Henderickx
Alcatel-Lucent

Thomas Morin
France Telecom - Orange

Praveen Muley
Alcatel-Lucent

Ray Qiu
Juniper Networks

IJsbrand Wijnands
Cisco Systems

February 8, 2013

Extranet Multicast in BGP/IP MPLS VPNs

draft-ietf-l3vpn-mvpn-extranet-01.txt

Abstract

Previous RFCs specify the procedures necessary to allow IP multicast traffic to travel from one site to another within a BGP/MPLS IP VPN (Virtual Private Network). However, it is sometimes desirable to allow multicast traffic whose source is in one VPN to be received by systems that are in another VPN. This is known as a "Multicast VPN (MVPN) extranet". This document updates RFCs 6513, 6514, and 6625 by specifying the procedures that are necessary in order to provide MVPN extranet service.

Status of this Memo

Copyright and License Notice

Table of Contents

1. Introduction

Previous RFCs ([MVPN], [MVPN-BGP]) specify the procedures necessary to allow IP multicast traffic to travel from one site to another within a BGP/MPLS IP VPN (Virtual Private Network). However, it is sometimes desirable to allow multicast traffic whose source is in one VPN to be received by systems that are in another VPN. This is known as an "extranet MVPN". This document specifies the procedures that are necessary in order to provide Extranet MVPN functionality.

1.1. Terminology

This document uses terminology from [MVPN], and in particular uses the prefixes "C-" and "P-" as specified in Section 3.1 of [MVPN], and "A-D routes" for "auto-discovery routes".

The term "Upstream Multicast Hop" (UMH) is used as defined in [MVPN].

The term "UMH-eligible route" is used to mean "route eligible for UMH

determination", as defined in Section 5.1.1 of [MVPN]. We will say that a given UMH-eligible route or unicast route "matches" a given IP address, in the context of a given VRF, if the address prefix of the given route is the longest match in that VRF for the given IP address. We will sometimes say that a route "matches" a particular host if the route matches an IP address of the host.

We follow the terminology of section 3.2 of [MVPN-WILDCARDS] when talking of an S-PMSI A-D route being "installed". That is, we say that an S-PMSI A-D route is "installed" (in a given VRF) if it has been selected by the BGP decision process as the preferred route for its NLRI. We also follow the terminology of section 3.2 of [MVPN-WILDCARDS] when saying that an S-PMSI A-D route has been "originated by a given PE"; this means that the given PE's IP address is contained in the "Originating Router's IP Address" field in the NLRI of the route.

We use the following additional terminology and notation:

- Extranet C-source: a multicast source, in a given VPN, that is allowed by policy to send multicast traffic to receivers that are in other VPNs.

- Extranet C-receiver: a multicast receiver, in a given VPN, that is allowed by policy to receive multicast traffic from extranet C-sources that are in other VPNs.

- Extranet C-flow: a multicast flow (with a specified C-source address and C-group address) whose source is an extranet C-source, and which is allowed by policy to have extranet C-receivers.

- Extranet C-group: a multicast group address that is in the "Any Source Multicast" (ASM) group address range, and that is allowed by policy to have Extranet C-sources and Extranet C-receivers that are not all in the same VPN. Note that we will sometimes refer to "SSM C-group addresses" (i.e., to C-group addresses in the SSM group address range), but will never call them "extranet C-groups".

- Extranet C-RP: a multicast Rendezvous Point (RP) for an extranet C-group; it is allowed by policy to receive PIM register messages [PIM] from outside its VPN, and to send multicast data packets to extranet C-receivers outside its VPN.

- Host(C-S,A): the host (or if C-S is an "anycast address", the set of hosts) denoted by the address C-S in the context of VPN-A. For example, if a particular C-source in VPN A has address C-S, then Host(C-S,A) refers to that C-source.

- SAFI-n route: a BGP route whose AFI is either 1 (IPv4) or 2 (IPv6), and whose SAFI is "n".

Note that a given extranet C-source is not necessarily allowed to transmit to every extranet C-receiver; policy determines which extranet C-sources are allowed to transmit to which extranet C-receivers.

We say that a given VRF "contains" or "has" a multicast C-source (or that the C-source is "in" the VRF), if that C-source is in a site connected to that VRF, and the VRF originates a UMH-eligible route (see Section 3) that matches the address of the C-source.

We say that a given VRF "contains" or "has" a multicast C-receiver (or that the C-receiver is "in" the VRF), if that C-receiver is in a site connected to that VRF.

We say that a given VRF "contains" or "has" the C-RP for a given ASM group (or that the C-RP is "in" the VRF) if that C-RP is in a site connected to that VRF, and the VRF originates a unicast route and a (possibly different, possibly the same) UMH-eligible route (see Section 3) whose respective address prefixes match the C-RP address.

[MVPN] allows a set of "Provider tunnels" (P-tunnels) to be aggregated together and transported via an outer P-tunnel, i.e., it allows for the use of hierarchical Label Switched Paths (LSPs) as P-tunnels. A two-level hierarchical LSP, for example, can be thought of as a set of "inner tunnels" aggregated into an outer tunnel. In this document, when we speak of a P-tunnel, we are always speaking of the innermost P-tunnel, i.e., of a P-tunnel at the lowest level of hierarchy. P-tunnels are identified in the Provider Multicast Service Interface (PMSI) Tunnel Attributes (PTAs) [MVPN-BGP] of BGP Auto-Discovery (A-D) routes. Two PTAs that have the same Tunnel Type and Tunnel Identifier fields, but different MPLS label fields, are thus considered to identify two different P-tunnels. (I.e., for the purposes of this document, the MPLS label included in the PTA, if any, is considered to be part of the tunnel identifier.)

We say that the NLRI of a BGP S-PMSI A-D route or Source Active A-D route contains (C-S,C-G) if its "Multicast Source" field contains C-S and its "Multicast Group" field contains C-G. If either or both of these fields is encoded as a wildcard, we will say that the NLRI contains (C-*,C-*) (both fields encoded as wildcard), or (C-*,C-G)

(multicast source field encoded as wildcard) or (C-S,C-*) (multicast group field encoded as wildcard).

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL", when and only when appearing in all capital letters, are to be interpreted as described in [RFC2119].

1.2. Scope

1.2.1. Customer Multicast Control Protocols

This document presumes that the VPN customer is using "PIM Sparse Mode", operating in either "Source-Specific Mode" (SSM) or "Any Source Mode" (ASM), as the multicast control protocol at the customer sites. Support for other customer IP multicast control protocols (e.g., [BIDIR-PIM], PIM "Dense Mode") is outside the scope of this document. Support for the customer use of MPLS multicast control protocols (e.g., [mLDP], [RSVP-P2MP]) is also outside the scope of this document.

When a VPN customer uses ASM, the customer routers need to be able to map from a C-group address to a C-RP address. These mappings can be provisioned in each router, or can be discovered dynamically through protocols such as BSR [BSR]. However, it cannot be assumed that such protocols will automatically work in the context of an extranet. Discussion of the use of such protocols in an extranet is outside the scope of this document.

1.2.2. Provider Multicast Control Protocols

[MVPN] allows either PIM or BGP to be used as the protocol for distributing customer multicast routing information. Except where otherwise specified, such as in Sections 6 and 7, the procedures of this document cover both cases.

1.3. Overview

Consider two VPNs, VPN-S and VPN-R, each of which supports MVPN functionality as specified in [MVPN] and/or [MVPN-BGP]. In the simplest configuration, VPN-S is a collection of VRFs, each of which is configured with a particular Route Target (RT) value (call it "RT-S") as its import RT and as its export RT. Similarly, VPN-R is a collection of VRFs, each of which is configured with a particular RT value (call it "RT-R") as its import RT and as its export RT.

In this configuration, multicast C-receivers contained in a VPN-R VRF cannot receive multicast data traffic from multicast C-sources contained in a VPN-S VRF. If it is desired to allow this, one needs to create an MVPN "extranet". Creating an extranet requires procedures in addition to those specified in [MVPN], [MVPN-BGP], and [MVPN-WILDCARDS]; this document specifies these additional procedures.

In the example above, the additional procedures will allow a selected set of routes exported from the VPN-S VRFs (i.e., from the VRFs containing extranet C-sources) to be imported into the VPN-R VRFs (i.e., into the VRFs containing extranet C-receivers). These routes include the routes that are to be eligible for use as UMH routes (see Section 5.1 of [MVPN]) in the extranet, as well as a selected set of BGP A-D routes (Intra-AS I-PMSI A-D routes, S-PMSI A-D routes, Source Active A-D routes). Importing these routes into the VPN-R VRFs makes it possible to determine, in the context of a VPN-R VRF, that a particular C-multicast Join needs to be delivered to a particular VPN-S VRF. It also makes it possible to determine, in the context of a VPN-R VRF, the P-tunnel through which the aforementioned VPN-S VRF sends a particular C-flow.

Depending on the type of P-tunnel used, it may also be necessary for Leaf A-D routes to be exported by one or more VPN-R VRFs and imported into a VPN-S VRF.

There are no extranet-specific procedures governing the use and distribution of BGP C-Multicast routes.

If PIM is used as the PE-PE protocol for distributing C-multicast routing information, additional BGP A-D routes must be exported from the VPN-R VRFs and imported into the VPN-S VRFS, so that the VPN-S VRFs can join the P-tunnels that the VPN-R VRFs use for sending PIM control messages. Details can be found in Section 6.

The simple example above describes an extranet created from two MVPNs, one of which contains extranet C-sources and one of which contains extranet C-receivers. However, the procedures described in this document allow for much more complicated scenarios.

For instance, an extranet may contain extranet C-sources and/or extranet C-receivers from an arbitrary number of VPNs, not just from two VPNs. An extranet C-receiver in VPN-R may be allowed to receive multicast traffic from extranet C-sources in VPN-A, VPN-B, and VPN-C. Similarly, extranet C-sources in VPN-S may be allowed to send multicast traffic to multicast C-receivers that are in VPN-A, VPN-B, VPN-C, etc.

A given VPN customer may desire that only some of its multicast C-sources be treated as extranet C-sources. This can be accomplished by appropriate provisioning of the import and export RTs of that customer's VRFs (as well as the VRFs of other VPNs that contain extranet C-receivers for extranet C-flows of the given customer.)

A given VPN customer may desire that some of its extranet C-sources can transmit only to a certain set of VPNs, while other of its extranet C-sources can transmit only to a different set of VPNs. This can be accomplished by provisioning the VRFs to export different routes with different RTs.

In all these cases, the VPN customers set the policies, and the Service Provider (SP) implements the policies by the way it provisions the import and export RTs of the VRFs. It is assumed that the customer communicates to the SP the set of extranet C-source addresses, and the set of VPNs to which each C-source can transmit. This customer/SP communication is part of the service provisioning process, and outside the scope of this document.

It is possible that an extranet C-source will transmit both extranet C-flows and non-extranet C-flows. However, if extranet C-receiver C-R can receive extranet C-flows from extranet C-source C-S, the procedures of this document do not prevent C-R from requesting and receiving the non-extranet flows that are transmitted by C-S. Therefore it is NOT RECOMMENDED to allow an extranet C-source to transmit non-extranet C-flows. However, the Service Provider (SP) has no control over the set of C-flows transmitted by a given C-source, and can do no more than communicate this recommendation to its customers. (Alternatively, the customer and SP may coordinate on setting up filters to prevent unauthorized flows from being sent to a customer site; such a procedure is outside the scope of this document.) See the "Security Considerations" section for additional discussion of this issue.

2. Extranets and Overlapping Address Spaces

As specified in [L3VPN], the address space of one VPN may overlap with the address space of another. A given address may be "ambiguous", in that it denotes one system within VPN-A and a different system within VPN-B. In the notation of section 1.1, if an address C-S is ambiguous between VPNs A and B, then Host(C-S,A) != Host(C-S,B). However, any given address C-S must be unambiguous (i.e., denotes a single system) in the context of a given VPN.

When a set of VRFs belonging to different VPNs are combined into an extranet, it is no longer sufficient for an address to be unambiguous

only within the context of a single VPN:

1. Suppose C-S is the address of a given extranet C-source contained in VPN-A. Now consider the set of VPNs {VPN-B, VPN-C, ...} containing extranet C-receivers that are allowed by policy to receive extranet C-flows from VPN-A's C-S. The address C-S MUST be unambiguous among this entire set of VPNs (VPN-A, VPN-B, VPN-C, etc.); i.e., Host(C-S,A) == Host(C-S,B) == Host(C-S,C).

   The implication is that C-S in VPN-A is not necessarily an extranet C-source for all VPNs that contain extranet C-receivers; policy MUST be used to ensure that C-S is an extranet C-source for a given VPN, say VPN-B, only if C-S is unambiguous between VPN-A and VPN-B.

2. If a given VRF contains extranet C-receivers for a given extranet C-source, then the address of this C-source MUST be unambiguous among all the extranet C-sources for which there are C-receivers in the VRF. This is true whether or not C-sources are in VRFs that belong to the same or to different VPNs.

   The implication is that if C-S in VRF-X is ambiguous with C-S in VRF-Y, then there MUST NOT be any VRF, say VRF-Z, containing C-receivers that are allowed by policy to receive extranet C-flows from both C-S in VRF-X and C-S in VRF-Y.

Note: A VPN customer may be using "anycast" addresses. An anycast address is intentionally ambiguous, as it denotes a set of systems rather than a single system. In this document, we will consider an anycast address to be unambiguous in a given context as long as it denotes the same set of systems whenever it occurs in that context.

A multicast C-group address, say C-G, may also be ambiguous, in that it may be used for one multicast group in VPN-A and for an entirely different multicast group in VPN-B. If a set of MVPNs are combined into an extranet, and C-G is an extranet C-group, it is necessary to ensure that C-G is unambiguous among the entire set of VPNs whose VRFs contain extranet C-sources, C-RPs, and/or extranet C-receivers for that C-group. This may require, as part of the provisioning process, customer/SP communication that is outside the scope of this document.

Subject to these restrictions, the SP has complete control over the distribution of routes in an MVPN. This control is exerted either by provisioning the export RTs on the VRFs that originate the routes (i.e., on the VRFs that contain the extranet C-sources), or by

provisioning the the import RTs on the VRFs that receive the routes (i.e., on the VRFs that contain the extranet C-receivers), or both.

Some of the rules and restrictions on provisioning the RTs are applicable to all extranets; these are specified in Section 3. Sections 6 and 7 add additional rules and restrictions that are applicable only to particular extranet scenarios.

Sections 2.1 and 2.2 describe scenarios in which address ambiguity can arise within an extranet. The procedures specified in this document have been designed to ensure that the address ambiguity described in those sections does not result in misdelivery of traffic.

2.1. Ambiguity: P-tunnel with Extranet/Non-Extranet Flows

In the following, we will use the notation "VRF A-n" to mean "VRF n of VPN-A".

If VPN-A and VPN-B have overlapping address spaces, and are part of the same extranet, then the following problem may exist, as illustrated in Figure 1.

```
   C-S2(A)  C-S1                                      Join(C-S2(A),G)
     \     /                                              /
      \   /                                              /
    +-------+---+   P1: (C-S1,G), (C-S2(A),G)    +---+--------+
    |VRF A-1|   |---------------------------------|   |VRF A-2 |
    +-------+PE1|                                 |PE2+--------+
    |VRF B-1|   |---------------------------------|   |VRF B-2 |
    +-------+---+   P2: (C-S2(B),G)               +---+--------+
        /                                               /    \
       /                                               /      \
     C-S2(B)                             Join(C-S2(B),G)   Join(C-S1,G)
```

Figure 1 Ambiguity of Extranet and Non-Extranet Source Address

Suppose:

- VRF A-1, on PE1, contains an extranet C-source, whose IP address is C-S1, that is allowed to have receivers in VPN B. VRF A-1 thus exports to VPN B a UMH-eligible route matching C-S1.

- VRF A-1 also contains a non-extranet C-source, whose IP address is C-S2. VRF A-1 exports a UMH-eligible route matching C-S2 to other VPN A VRFs, but NOT to VPN B.

- VRF B-1, also on PE1, contains a non-extranet C-source whose IP address is C-S2. A UMH-eligible route matching C-S2 is thus exported from VRF B-1 to other VRFs in VPN B.

- Host(C-S2,A) != Host(C-S2,B). That is, C-S2 is an ambiguous address in any extranet that contains both VPN-A VRFs and VPN-B VRFs.

- VRF B-2, on some other PE, say PE2, requests to receive the multicast flow (C-S1,C-G). In the context of VRF B-2, C-S1 matches the route exported from VRF A-1. Thus B-2's request to receive the (C-S1,C-G) flow is transmitted to VRF A-1.

- VRF A-1 responds to VRF B-2's request for (C-S1,C-G) traffic by transmitting that traffic on P-tunnel P1.

- VRF B-2 joins P-tunnel P1, in order to receiver the (C-S1,C-G) traffic.

- VRF A-2, on PE2, requests to receive the (non-extranet) multicast flow (C-S2,C-G). In the context of VRF A-2, C-S2 matches the route exported from VRF A-1. Thus A-2's request to receive the (C-S2,C-G) traffic is transmitted to VRF A-1.

- VRF A-1 responds to VRF A-2's request for (C-S2,C-G) traffic by transmitting that traffic on P-tunnel P1.

- VRF A-2 joins P-tunnel P1, in order to receive the (C-S2,C-G) traffic.

- VRF B-2 requests to receive the (non-extranet) multicast flow (C-S2,C-G). In the context of VRF B-2, C-S2 matches the route exported from VRF B-1. Thus B-2's request to receive the (C-S2,C-G) flow is transmitted to VRF B-1.

- VRF B-1 responds to VRF B-2's request for (C-S2,C-G) traffic by transmitting that traffic on P-tunnel P2.

- VRF B-2 joins P-tunnel P2.

Since VRF B-2 has joined P-tunnel P1 and P-tunnel P2, it will receive (C-S2,C-G) traffic on both P-tunnels. But the (C-S2,C-G) traffic that VRF B-2 needs to receive is traveling on P-tunnel P2. The (C-S2,C-G) traffic arriving on P2 must be forwarded by B-2 to any

attached customer sites that have C-receivers for it. But B-2 MUST discard the (C-S2,C-G) traffic that it receives on P1, as this is not the traffic that it has requested. If the (C-S2,C-G) traffic arriving on P1 were forwarded to B-2's customer sites, the C-receivers would not be able to distinguish the two flows, and the result would be a corrupted data stream.

Note that the procedures of [MVPN] Section 9.1.1 ("Discarding Packets from the Wrong PE") will not cause VRF B-2 to discard the (C-S2,C-G) that arrives on tunnel P1, because P1 and P2 have the same upstream PE.

Therefore, it is necessary EITHER to prevent the above scenario from occurring, OR ELSE to ensure that multicast data packets will be discarded if they arrive on the wrong P-tunnel (even if they arrive from the expected PE).

Subsequent sections describe a set of procedures, which we call "extranet separation", that can be used to prevent extranet C-flows and non-extranet C-flows from being carried in the same P-tunnel, thereby preventing the above scenario from occurring.

Subsequent sections also describe a set of procedures that allows extranet and non-extranet C-flows to be carried in the same P-tunnel, but ensures that the packets of a given C-flow will be discarded if they arrive on the wrong P-tunnel (even if they arrive from the expected PE). In our example, VRF B-2 will be expecting the (C-S2,C-G) packets to arrive on P-tunnel P2. When VRF B-2 receives a multicast packet over a P-tunnel, and the multicast packet has source address C-S2 and destination address C-G, VRF B-2 will forward the packet only if it arrived over P-tunnel P2, but will discard it if it arrived over P-tunnel P1. Detailed procedures for associating a given C-flow with a given P-tunnel are provided in Sections 6 and 7.

2.2. Ambiguity: P-tunnel with Multiple Extranet Flows

Here is another example in which overlapping address spaces may cause a problem. This example is illustrated in Figure 2.

```
C-S2(A2D) C-S1(A2C)                               Join(C-S2(A2D),G)
    \     /                                              /
     \   /                                              /
   +-------+---+ P1: (C-S1(A2C),G), (C-S2(A2D),G)+---+--------+
   |VRF A-1|   |----------------------------------|   |VRF D-1 |
   +-------+PE1|                                  |PE2+--------+
   |VRF B-1|   |----------------------------------|   |VRF C-1 |
   +-------+---+ P2: (C-S2(B2C),G)                +---+--------+
       /                                              /  \
      /                                              /    \
    C-S2(B2C)                                       /      \
                                                  Join     Join
                                           (C-S2(B2C),G)  (C-S1(A2C),G)
```

Figure 2 Ambiguity of Extranet Source Addresses

Suppose:

- C-G is an SSM C-group address that is used in VPNs A, B, C, and D.

- VRF A-1, on PE1, contains an extranet C-source whose IP address is C-S1, and that is allowed by policy to have C-receivers in VPN C (but not in VPN D). VRF A-1 thus exports a UMH-eligible route matching C-S1 to VPN C.

- VRF A-1 also contains an extranet C-source whose IP address is C-S2, and that is allowed by policy to have C-receivers in VPN D (but not in VPN C). VRF A-1 thus exports a UMH-eligible route matching C-S2 to VPN D.

- VRF B-1, also on PE1, contains an extranet C-source whose IP address is C-S2, and that is allowed by policy to have C-receivers in VPN C (but not in VPN D). VRF B-1 thus exports a UMH-eligible route matching C-S2 to VPN C.

- Host(C-S2,A) != Host (C-S2,B). That is, C-S2 is an ambiguous address in any extranet that contains both VPN-A VRFs and VPN-B VRFs.

- VRF C-1, on some other PE, say PE2, requests to receive the extranet multicast flow (C-S1,C-G). In the context of VRF C-1, C-S1 matches the route exported from VRF A-1. Thus C-1's request to receive the (C-S1,C-G) flow is transmitted to VRF A-1.

  + VRF A-1 responds to VRF C-1's request for (C-S1,C-G) traffic by transmitting that traffic on P-tunnel P1,

- VRF C-1 joins P-tunnel P1, in order to receive the (C-S1,C-G) traffic.

- VRF C-1 requests to receive the extranet multicast flow (C-S2,C-G). In the context of VRF C-1, C-S2 matches the route exported from VRF B-1. Thus C-1's request to receive the (C-S2,C-G) flow is transmitted to VRF B-1.

- VRF B-1 responds by transmitting its (C-S2,C-G) traffic on P-tunnel P2.

- VRF C-1 joins P-tunnel P2 in order to receive the (C-S2,C-G) traffic.

- VRF D-1, on PE2, requests to receive the extranet multicast flow (C-S2,C-G). In the context of VRF D-1, C-S2 matches the route exported from VRF A-1. Thus D-1's request to receive the (C-S2,C-G) flow is transmitted to VRF A-1.

- VRF A-1 responds by transmitting its (C-S2,C-G) traffic on P-tunnel P1.

- VRF D-1 joins P-tunnel P1 in order to receive the (C-S2,C-G) traffic.

In this example, VRF A-1 has chosen to use the same P-tunnel, P1, to carry both its (C-S2,C-G) traffic and the (C-S1,C-G) traffic. VRF C-1 has joined tunnel P1 in order to receive the (C-S1,C-G) traffic from VRF A-1, which means that VRF C-1 will also receive the unwanted (C-S2,C-G) traffic from P1. VRF C-1 is also expecting (C-S2,C-G) traffic from VRF B-1; this traffic will be received from P2. Thus VRF C-1 is receiving (C-S2,C-G) traffic on both tunnels, and both C-flows arrive from the expected PE, PE1.

So again, a procedure is necessary that EITHER prevents this sort of ambiguity from occuring, OR ELSE that ensures that VRF C-1 discards any (C-S,C-G) traffic that arrives from "the wrong P-tunnel".

Note that extranet separation does not prevent this ambiguity from occuring, as the ambiguity is between two C-flows that are both extranet C-flows.

This ambiguity would not occur if C-G were an (ASM) extranet C-group, as the scenario would then violate the rule given in section 2 requiring that all sources sending to a particular ASM extranet

C-group must have addresses that are unambiguous over all the MVPNs receiving traffic for that C-group.

For P-tunnels that are advertised in S-PMSI A-D routes whose NLRI contains (C-S,C-G) or (C-S,C-*), the ambiguity described in this section can be prevented by provisioning a policy that assigns, to such P-tunnels, only flows from the same C-source.

However, it is not always possible to determine, through inspection of the control messages, whether this policy has been deployed. For instance, suppose a given VRF has imported a set of S-PMSI A-D routes, that each route in the set has bound only a single (C-S1,C-G1) to a single P-tunnel, and that each route in the set identifies a different P-tunnel in its PTA than is identified by the PTA of any other route in the set. One cannot infer from this that there is no ambiguity, as the same P-tunnel may also have been advertised in an S-PMSI A-D route that is not imported by the given VRF, and that S-PMSI A-D route may have bound (C-S2,C-G2) to the P-tunnel, where C-S1 != C-S2.

Therefore, in order to determine that a given P-tunnel (advertised in a (C-S,C-G) or (C-S,C-*) S-PMSI A-D route) carries only C-flows from a single C-source, one must have a priori knowledge (through provisioning) that this policy has been deployed. In the remainder of this document, we will refer to this policy as the "Single C-source per (C-S,C-G) or (C-S,C-*) P-tunnel" policy. Note that this policy is only applicable to P-tunnels that are advertised only in (C-S,C-G) or (C-S,C-*) S-PMSI A-D routes.

Of course, if a P-tunnel is advertised in (a) an I-PMSI A-D route, or (b) an S-PMSI A-D route whose NLRI contains (C-*,C-*), or (c) an S-PMSI A-D route whose NLRI contains (C-*,C-G), then it is always possible for the P-tunnel to contain traffic from multiple C-sources; there is no policy that can prevent that.

However, if a P-tunnel advertised in a (C-*,C-G) S-PMSI A-D route contains only traffic addressed to a single C-G, the address uniqueness rules of section 2 prevent the C-source addresses from being ambiguous; the set of C-sources transmitting to a particular extranet C-group address must be unambiguous over the set of MVPNs that have receivers for that C-group. So for P-tunnels that are advertised in (C-*,C-G) S-PMSI A-D routes, the ambiguity described in this section can be prevented by provisioning a policy that assigns, to such P-tunnels, only flows to the same extranet C-group. We will refer to this policy as the "Single C-group per (C-*,C-G) P-tunnel" policy.

Sections 6 and 7 describe procedures that cause a VRF with

C-receivers to discard any (C-S,C-G) traffic that arrives on "the wrong P-tunnel". These procedures are needed unless all of the following conditions hold:

- the "Single C-source per (C-S,C-G) or (C-S,C-*) P-tunnel" policy is provisioned, and

- either no (C-*,C-G) S-PMSI A-D routes are advertised, or else the "Single C-group per (C-*,C-G) P-tunnel" policy is provisioned, and

- no P-tunnels are advertised in I-PMSI A-D routes, and

- no (C-*,C-*) S-PMSI A-D routes are advertised.

This means that if any PE that contains a VRF of the extranet is not capable of discarding traffic that arrives on the wrong P-tunnel, all VRFs of the extranet MUST be provisioned such that the above conditions hold.

Note that the "Single C-source per (C-S,C-G) or (C-S,C-*) P-tunnel" policy and the "Single C-group per (C-*,C-G) P-tunnel" policy both imply extranet separation for tunnels advertised in the S-PMSI A-D routes to which the policies apply.

3. Distribution of Routes that Match C-S/C-RP Addresses

3.1. UMH-Eligible Routes

As described in Section 5.1 of [MVPN], in order for a C-flow (C-S,C-G) to be carried across the SP backbone, a VRF that has multicast receivers for that C-flow MUST import a route that matches C-S, and this route must be "eligible for UMH selection". In this document, we will refer to these routes as "UMH-eligible extranet C-source routes".

The UMH-eligible extranet C-source routes do not necessarily have to be unicast routes. If one wants, e.g., a VPN-R C-receiver to be able to receive extranet C-flows from C-sources in VPN-S, but one does not want any VPN-R system to be able to send unicast traffic to those C-sources, then the UMH-eligible routes exported from VPN-S and imported by VPN-R MAY be SAFI-129 routes (see Section 5.1.1 of [MVPN]). The SAFI-129 routes are used only for UMH determination, but not for unicast routing.

If a customer is using PIM-SM in ASM mode, and one or more customer sites have C-receivers that are allowed by policy to join a (C-*,C-G)

tree, where C-G is an extranet C-group, then any VRF with C-receivers for that group MUST import a UMH-eligible route that matches C-RP, where C-RP is the Rendezvous Point (RP) address for C-G.

The UMH-eligible extranet C-source and C-RP routes do not have to be "host routes." That is, they can be routes whose IPv4 address prefixes are not 32 bits in length, or whose IPv6 address prefixes are not 128 bits in length. So it is possible for a UMH-eligible extranet C-source route to match the address of an extranet C-source and to also match the address of a non-extranet C-source. However, if such a route is exported from a VPN-S VRF and imported by a VPN-R VRF, VPN-R receivers will be able to receive C-flows from any non-extranet C-sources whose addresses match that route. To prevent this, the VPN-S VRF SHOULD be provisioned such that it will NOT export a UMH-eligible route that matches (in the context of the VPN-R VRF) both extranet C-sources and non-extranet C-sources. Failure to follow this rule may result in a VPN security violation. (See Section 10.)

In general, one does not want ALL the routes from the VPN-S VRFs to be exported to all the VPN-R VRFs, as only a subset of the routes in the VPN-S VRFs will be UMH-eligible extranet C-source routes. Route distribution is, as always in a BGP/MPLS IP VPN [L3VPN], controlled by Route Targets (RTs). A variety of route distribution policies can be created by appropriately provisioning the import and export RTs of the various VRFs.

For example, the VPN-S VRFs that contain extranet C-sources could be configured to apply an export RT whose value is "RT-A-extranet" to the routes that match the extranet C-sources. The VPN-R VRFs that contain extranet C-receivers allowed to receive extranet C-flows from VPN-S extranet C-sources could then be configured with "RT-A-extranet" as an import RT.

Arbitrarily complex policies can be created by suitable manipulation of the import and export RTs.

3.2. When Unicast Routes to C-RPs Must be Distributed

Suppose a VRF contains a C-source, C-S, that may transmit to a particular extranet C-group C-G. Then the VRF must import a unicast route matching that C-RP of that group. This allows the C-S's Designated Router to unicast Register messages to the C-RP when C-S begins to send traffic to C-G. The unicast route matching the C-RP is needed whether or not the VRF has also imported a SAFI-129 route matching the C-RP. If the VRF contains both transmitters and receivers for a particular extranet C-group, and if the PEs are doing

UMH determination by means of SAFI-129 route, both a SAFI-129 route and a unicast route matching the C-RP are needed.

If the customer is using "anycast-RP"([RFC3446], [RFC4610]), then all the C-RPs that serve a particular extranet C-group need to send unicast messages to each other. Thus any VRF that contains a C-RP for a particular extranet C-group needs to import unicast routes matching ALL the other C-RPs that serve that extranet C-group.

A sufficient condition for meeting these requirements of this sub-section is that the C-sources and C-RPs for a given extranet C-group are all in the same MVPN. While this is not a necessary condition, it may be impractical to provision the MVPN properly if this condition doesn't hold.

3.3. Other Unicast Routes that Must be Distributed

A C-RP for an extranet multicast C-group must be able to send PIM Register-Stop messages to the "first hop Designated Router" of each of that C-group's C-sources. This means that any VRF containing a C-RP must import unicast routes to all of C-G's C-sources and to all of the first hop Designated Routers of those C-sources. Unless the C-RP and all the C-sources are in the same VPN, this may be impractical.

3.4. Route Targets and Ambiguous UMH-Eligible Routes

This section imposes constraints on the way RTs are assigned to (a) UMH-eligible routes and to (b) the BGP A-D routes that advertise P-tunnels (i.e., to BGP A-D routes that contain a PTA). The constraints specified here apply to any extranet for which the ambiguity of Section 2.2 is possible. (The conditions under which such ambiguity is possible are described in Section 2.2.)

We want to ensure that, in any given VRF, the UMH-eligible route matching a given extranet C-source has an RT in common with every BGP A-D route that advertises a P-tunnel that may be used to carry extranet multicast traffic from that C-source. We also want to ensure that the UMH-eligible route matching a given extranet C-source does not have any RT in common with any BGP A-D route that advertises a P-tunnel that may be used to carry any multicast traffic from a different C-source that has the same IP address. This enables us to determine whether traffic that appears to be from the given C-source is really arriving on the "wrong tunnel", and hence is really from a different C-source with the same IP address.

Suppose an IP address C-S is used in VPN-A as the address of one system, and is used in VPN-B as the address of a different system. In this case, one or more VPN-A VRFs may export a VPN-IP route whose NLRI is <RD1,S>, and one or more VPN-B VRFs may export a VPN-IP route whose NLRI is <RD2,S>, where RD1 != RD2. Consider two routes, R1 and R2, for which the following conditions all hold:

- R1 and R2 are UMH-eligible extranet C-source or C-RP routes, or are unicast routes matching a C-RP

- R1 is exported from a VRF of VPN-A, while R2 is exported from a VRF of a different VPN, say VPN-B

- R1's NLRI specifies IP address prefix S/n

- R2's NLRI specifies IP address prefix S/m

- m >= n, (S/m is either the same as or more specific than S/n)

- There is some host address H such that:

    * H denotes a different system in VPN-A than in VPN-B,

    * H/m == S/m (so either S/m or S/n might be a longest match for H in some VRF).

We impose the following constraint: RTs MUST be assigned in such a way that R1 and R2 do not have any RT in common.

(This constraint is not as onerous at it may seem. Typically R1 and R2 would not have an RT in common, as that might result in their being imported into the same VRF, making the address H ambiguous in that VRF.)

Sections 6 and 7 specify procedures for determining if a received C-flow has been received over the wrong P-tunnel. Those procedures will not work if this constraint is violated. (The constraint described in this section is necessary but not sufficient for the procedures of those sections to work; additional constraints, covering the assignment of RTs to BGP A-D routes, are given in subsequent sections.)

3.5. Dynamically Marking Extranet Routes

3.5.1. The Extranet Source Extended Community

Sections 3.1-3.4 place specific requirements on the way in which certain VPN-IP routes are distributed. In order to ensure that these requirements are met, a VPN customer must tell its SP which routes are the matching routes for extranet C-sources and C-RPs. This may be done as part of the provisioning process. Note that this does not necessarily require customer/provider interaction every time the customer adds a new extranet C-source or C-RP, but only when the IP address of the new C-source or C-RP does not match an existing route that is already being distributed as a VPN-IP extranet route. Nevertheless, it seems worthwhile to support an OPTIONAL mechanism that allows a customer to dynamically mark certain routes as being extranet routes.

To facilitate this, we define a new transitive opaque extended community, the "Extranet Source" extended community. When a CE router advertises (via BGP) a route to a PE router, and the AFI/SAFI of the route is 1/1, 1/2, 1/4, 2/1, 2/2, or 2/4, the Extranet Source extended community MAY be attached to the route. The value field of the extended community MUST be set to zero. By placing this extended community on a particular route, a CE router indicates to a PE router that the procedures of sections 3.1-3.4 are to be applied to that route. That is, the CE router may use this extended community to indicate to the PE router that a particular route is to be treated as a route that matches the address of an extranet source, and exported accordingly to other VPNs.

If a CE is advertising SAFI-2 routes to the PE as the UMH-eligible extranet C-source and C-RP routes, and if the CE is using the Extranet Source extended community, it is important that the CE attach that extended community to the SAFI-2 routes, rather than just to the corresponding SAFI-1 routes. Otherwise extranet receivers may not be able to join the (C-S,C-G) or (C-*,C-G) multicast trees.

However, if the C-sources and the C-RPs for a given extranet C-group are not all in the same VPN, the extended community would also have to be attached to the SAFI-1 routes that match the C-RP addresses and to the SAFI-1 routes that match the addresses of the first hop designated routers for all the C-sources. Otherwise, the first hop routers might not be able to send PIM Register messages to the C-RPs, and the C-RPs might not be able to send PIM Register-Stop messages to the first hop routers.

While this extended community allows a customer to inform the SP dynamically that certain routes are "extranet routes", it does not

allow a customer to control the set of RTs that the route will carry when it is redistributed as a VPN-IP route. Thus it is only useful when all the extranet routes from a given VRF are exported with exactly the same set of RTs. (Cf. section 4.3.1 of [L3VPN], which does provide a mechanism that, if properly supported by the SP, allows the customer to determine the set of RTs carried by a VPN-IP route.)

Note that misconfiguration on the CE router can result in the Extranet Source extended community being mistakenly attached to a route that is not intended to be exported as an extranet route. This could result in a VPN security violation.

3.5.2. Distribution of the Extranet Source EC

A CE or PE router that supports the Extranet Source extended community MUST support a configuration item, "Extranet_Source", that can be configured per BGP session. This configuration item has four possible values: "disabled", "send_only", "receive_only", and "send_and_receive". The default value of this configuration item MUST be "disabled".

If a CE or PE router receives a route with the Extranet Source extended community attached, and the route was received over a BGP session that has the Extranet_Source configuration item set to "disabled" or to "send_only", then the router MUST remove the Extranet Source extended community from that route, and in all respects MUST treat that route is if the Extranet Source extended community had not been present.

A CE or PE router MUST NOT attach the Extranet Source extended community to any route it distributes over a BGP session for which the Extranet_Source configuration item is set to "disabled" or "receive_only". Similarly, it MUST remove the Extranet Source extended community from any route that it distributes over a BGP session for which the Extranet_Source configuration item is set to "disabled" or "receive_only".

This means that the CE router's use of the Extranet Source extended community will have no effect unless its use has been explicitly enabled by the SP.

In a typical deployment, if a SP wants to allow a particular CE to use the Extranet_Source extended community, the PE should configure the BGP session to that CE such that the Extranet_Source configuration item is set to "receive_only". At the CE, the configuration item for that session should be set to "send_only".

This will ensure that the Extranet Source extended community functions only as a signal between a CE router and the PE router to which it is attached, and that the extended community does not travel any farther.

Whatever the settings of the Extranet_Source configuration item, the Extranet Source extended community MUST NOT be attached to any route whose SAFI is 5 (MCAST-VPN routes). If a PE receives a route whose SAFI is 5, and if that route has an Extranet Source extended community, the PE MUST ignore that community. If the PE redistributes the route, it MUST first strip off the Extranet Source extended community.

If a route of AFI/SAFI 1/1, 1/2, 1/4, 1/128, 1/129, 2/1, 2/2, 2/4, 2/128 or 2/129 is received on one BGP session and redistributed on another, where the Extranet_Source configuration item of the first session is set to "enabled" or "receive_only", and the Extranet_Source configuration item of the second session is set to "enabled" or "send_only", then if the route was received with the Extranet_Source extended community attached, that community should remain attached (with its value field unchanged) when the route is redistributed. If a route with SAFI 1 or 2 is "translated" into a route with SAFI 128 or 129 respectively, and if the former route has the Extranet Source extended community attached to it, the latter route SHOULD have the same extended community attached to it (with its value field unchanged).

These settings can be used if it is desirable for the Extranet Source extended community to be carried across the network. This might be useful, for example, if a particular VPN has an "option A interconnect" (see [L3VPN], section 10) somewhere in the network, and it is desirable for the Extranet Source extended community to be carried over that interconnect.

The rules determining whether the Extranet Source extended community can be carried on a particular BGP session will of course only be applied at a given router if that router understands that extended community and implements the procedures of this section. Care must be take not to set the Extended_Source configuration item for a given BGP session to any value other than "disabled" unless it is known that the router at the other send of the BGP session implements these procedures.

3.6. The 'Extranet Separation' Extended Community

We define a new transitive opaque extended community, the "Extranet Separation" extended community. This extended community is used only when extranet separation is being used. Its value field MUST be set to zero upon origination, MUST be ignored upon reception, and MUST be passed unchanged by intermediate routers.

If a VRF has been provisioned to use extranet separation, and if that VRF has been provisioned to transmit any extranet C-flows on a P-tunnel that it advertises in an I-PMSI A-D route or a (C-*,C-*) S-PMSI A-D route, then any UMH-eligible routes and/or unicast routes that are exported from that VRF following the procedures of sections 3.1-3.4 MUST carry the Extranet Separation extended community. In addition, if an I-PMSI A-D route and/or (C-*,C-*) S-PMSI A-D route, exported from that VRF, is used to carry extranet traffic, that A-D route MUST also carry the Extranet Separation extended community. Further details may be found in sections 7.3, 7.4.4, and 7.4.5.

4. Extranet Transmission Models

This document specifies several "extranet transmission models". A given VRF, containing extranet C-sources or C-receivers, MUST use only one of these models. Further if VRF S contains extranet C-sources, VRF R contains extranet C-receivers, and it is allowed by policy for an extranet C-receiver in VRF R to receive a C-flow from an extranet C-source in VRF S, then VRFs S and R MUST use the same extranet transmission model. The model used by a given VRF is determined by provisioning.

4.1. Transmitting an Extranet C-flow on a Single PMSI

In one extranet transmission model, which we call the "transmitting an extranet C-flow on a single PMSI" model, or more simply, the "single PMSI per C-flow model", a PE transmitting a packet of an extranet C-flow transmits it on only a single PMSI. If the PMSI is instantiated by a multicast P-tunnel, this means that the PE transmits the packet on a single P-tunnel. Of course, if the PE is a replication point for that multicast P-tunnel, the packet is transmitted more than once by the PE. Similarly, if the PMSI is instantiated by a set of unicast tunnels (i.e., via Ingress Replication), each packet may be transmitted multiple times. It is still the case though that the packet is transmitted only on one PMSI.

This document provides procedures for supporting this transmission

model using either BGP or PIM as the PE-PE C-multicast control protocol.

There are two variants of this transmission model: "without extranet separation" and "with extranet separation".

4.1.1. Without Extranet Separation

In this variant, multicast data traffic from extranet C-sources and from non-extranet C-sources may be carried in the same P-tunnel.

This document provides procedures for supporting this variant using either BGP or PIM as the PE-PE C-multicast control protocol.

4.1.2. With Extranet Separation

In this variant, multicast data traffic from extranet C-sources and from non-extranet C-sources are never carried in the same P-tunnel. Under certain circumstances, this can reduce the amount of multicast data traffic that is delivered unnecessarily to certain PE routers. It also eliminates the ambiguity discussed in Section 2.1.1.

By definition, when extranet separation is used, the following rule MUST be applied:

> Traffic from extranet C-sources MUST NOT be carried in the same P-tunnel as traffic from non-extranet C-sources.

If VRF-S does not contain both extranet C-sources and non-extranet C-sources, this condition holds automatically. Otherwise it is necessary to advertise P-tunnels that are specifically used for carrying only extranet C-flows.

This document provides procedures for supporting extranet separation when BGP is used as the PE-PE C-multicast control protocol. Support for extranet separation using PIM as the PE-PE C-multicast control protocol is outside the scope of this document.

4.2. Transmitting an Extranet C-flow over Multiple PMSIs

The second extranet transmission model is called the "transmitting an extranet C-flow over multiple PMSIs" model, or more simply, the "multiple PMSIs per C-flow model". In this model, a PE may transmit the packets of an extranet C-flow on several different PMSIs.

Support for extranet separation with this model is outside the scope of this document.

This document provides procedures for supporting this transmission model when PIM as the PE-PE C-multicast control protocol. Support for this transmission model when BGP is used as the PE-PE C-multicast control protocol is outside the scope of this document.

5. Origination and Distribution of BGP A-D Routes

Except where otherwise specified, this section describes procedures and restrictions that are independent of the PE-PE C-multicast control protocol.

5.1. Route Targets of UMH-eligible Routes and A-D Routes

Suppose there is an extranet C-flow such that:

- The extranet C-source of that C-flow is in VRF A-1.

- One or more extranet C-receivers of that C-flow are in VRF B-1.

In this case VRF A-1 must export a UMH-eligible route that matches the extranet C-source address, and VRF B-1 must import that route. In addition, VRF A-1 must export an Intra-AS I-PMSI A-D route or an S-PMSI A-D route specifying the P-tunnel through which it will send the data traffic of the given extranet C-flow, and VRF B-1 must import that route. If BGP is the PE-PE C-multicast control protocol, then under certain conditions (as specified in [MVPN-BGP]), VRF A-1 may also need to export a Source Active A-D route specifying that it contains a source of the given C-flow, and VRF B-1 must import that Source Active A-D route. That is, in order for VRF B-1 to receive a C-flow from, a given extranet C-source contained in VRF A-1, VRF A-1 must export a set of A-D routes that are "about" that source, and VRF B-1 must import them.

One way to ensure this is to provision an RT that is carried by all the routes exported from VRF A-1 that are "about" a given extranet C-source, and to provision this RT as an import RT at any VRF (such

as VRF B-1) that is allowed to receive extranet flows from source.

If the "single PMSI per C-flow" transmission model is being used (with or without extranet separation), there is a an additional requirement, stated below, on the way RTs are provisioned, as the RTs carried by a UMH-eligible route that matches a given extranet C-source may need to be used to identify the A-D routes that are "about" that source.

Consider the following scenario:

- IP address S is the address of one system in VPN-A, and of a different system in VPN-B.

- VRF A-1 on PE1 exports UMH-eligible route R1, which is a matching route for S.

- VRF A-1 on PE1 exports an A-D route P1 whose PTA identifies a P-tunnel through which VRF A-1 may send traffic whose C-source is S, where one of the following conditions holds:

  * P1 is an I-PMSI A-D route, OR

  * P1 is an S-PMSI A-D route whose NLRI contains (C-*,C-*) or (C-*,C-G), OR

  * P1 is an S-PMSI A-D route whose NLRI contains (C-S,C-G) or (C-S,C-*), BUT the "single C-source per (C-S,C-G) or (C-S,C-*) P-tunnel" policy is not provisioned.

  * P1 is a Source Active A-D route whose NLRI contains (C-S,C-G)

- VRF B-1 on PE1 exports a UMH-eligible route R2, which is a matching route for S.

- VRF B-1 on PE1 exports an A-D route P2 whose PTA identifies a P-tunnel on which VRF B-1 may send traffic whose C-source is S, where one of the following conditions holds:

  * P2 is an I-PMSI A-D route, OR

  * P2 is an S-PMSI A-D route whose NLRI specifies (C-*,C-*) or (C-*,C-G), OR

  * P2 is an S-PMSI A-D whose NLRI specifies (C-S,C-G) or (C-S,C-*), BUT the "single C-source per (C-S,C-G) or (C-S,C-*) P-tunnel" policy is not provisioned.

* P2 is a Source Active A-D route whose NLRI contains (C-S,C-G)

As already specified in section 3.1, there MUST NOT be any RT that is common to both R1 and R2. In addition, the following set of rules for RT assignment MUST be followed when extranets are supported. This set of rules supports all the extranet transmission models described in this specification:

- There MUST NOT be any RT that is carried by both P1 and P2.

- The intersection of the set of RTs carried by P1 and the set of RTs carried by R1 MUST be non-null, and any VRF that imports both P1 and R1 MUST be configured with an import RT from this intersection.

- The intersection of the set of RTs carried by P2 and the set of RTs carried by R2 MUST be non-null, and any VRF that imports both P2 and R2 MUST be configured with an import RT from this intersection.

Suppose VRF C-1 on PE2 imports P1 and R1 from VRF A-1, while also importing P2 from VRF B-1. Since:

- R1 is VRF C-1's route to S, and

- R1 has an RT in common with P1, and

- R1 has no RT in common with P2

it can be concluded that VRF C-1 should expect that multicast traffic from S will arrive on the P-tunnel specified in P1. See Sections 6 and 7 for more details on determining the expected P-tunnel for a given extranet C-flow.

While the assignment of import and export RTs to routes is a deployment and provisioning issue rather than a protocol issue, it should be understood that failure to follow these rules is likely to result in VPN security violations.

5.2. Considerations for Particular Inclusive Tunnel Types

5.2.1. RSVP-TE P2MP

Suppose a VRF, VRF-S, contains a given extranet C-source C-S, and that VRF-S advertises in its Intra-AS I-PMSI A-D route a P2MP RSVP-TE as the P-tunnel to carry (extranet multicast) traffic. Suppose VRF-R contains an extranet C-receiver that is allowed by policy to receive extranet flows from C-S. Then the RT(s) carried by the Intra-AS I-PMSI A-D routes originated by VRF-R must be such that those Intra-AS I-PMSI A-D routes will be imported into VRF-S. (I.e., In order for VRF-S to set up the P2MP RSVP-TE P-tunnel, it must know all the PEs that are leaf nodes of the P-tunnel, and to learn this it MUST import an Intra-AS I-PMSI A-D route from every VRF that needs to receive data through that tunnel.)

5.2.2. Unicast LSP Tunnels

[MVPN] and [MVPN-BGP] specify procedures that allow I-PMSIs to be instantiated by "ingress replication". In effect, the Inclusive P-Tunnel that instantiates the I-PMSI is really a set of unicast tunnels. Suppose the PEs of a given VPN are PE1, PE2, ..., PEn. If PE1 has a multicast data packet to send on the I-PMSI, it unicasts a copy of the packet to PE1, a copy to PE2, ..., a copy to PEn. Each unicast is sent through a unicast tunnel terminating at the receiving PE.

If PE1 sends a multicast data packet to PE2 via ingress replication, the procedures of [MVPN] and [MVPN-BGP] ensure that PE2 will be able to identify the VRF to which the packet is directed, and to recognize that the packet arrived on an inclusive tunnel. But the procedures of [MVPN] and [MVPN-BGP] do not ensure that PE2 will be able to determine that PE1 transmitted the packet. If the unicast tunnel from PE1 to PE2 is a MP2P LSP, or if it is a P2P LSP for which penultimate hop popping (PHP) ([MPLS-ARCH]) is used, PE2 will not be able to determine, for a packet transmitted on an I-PMSI, which of the other PEs transmitted the packet. This would make it impossible to apply the procedures of [MVPN] section 9.1.1, "Discarding Packets from the Wrong PE".

Due to this restriction, this document does not support extranet functionality in an MVPN that uses I-PMSIs instantiated by ingress replication using unicast tunnels that are MP2P LSPs or P2P LSPs that use PHP. For MVPNs that use I-PMSIs instantiated by ingress replication, extranet functionality is supported only if the encapsulation of the unicast tunneling technology allows the receiving PE to infer the identity of the transmitting PE.

If it is desired to instantiate the PMSIs via ingress replication, and the desired tunnel type is an MP2P LSP or an LSP that uses PHP, an alternative is to use (C-*,C-*) S-PMSIs instead of I-PMSIs. (See [MVPN-WILDCARDS] and Sections 7.2.2, 7.3.2, and 7.4.4 of this document.) This has much the same effect in the data plane, and there are no restrictions on the type of unicast tunnel that can be used for instantiating S-PMSIs.

6. When PIM is the PE-PE C-multicast Control Plane

As specified in [MVPN], when PIM is used as the PE-PE C-multicast control plane for a particular MVPN, there is an MI-PMSI for that MVPN, and all the PEs of that MVPN must be able to send and receive on that MI-PMSI. Associated with each VRF of the MVPN is a PIM C-instance, and the PIM C-instance treats the MI-PMSI as if it were a LAN interface. That is, the "ordinary" PIM procedures run over the MI-PMSI just as they would over a real LAN interface, except that the data plane and control plane "RPF checks" need to be modified. Section 5.2 of [MVPN] specifies the RPF check modifications for non-extranet MVPN service.

For example, suppose that there are two VPNs, VPN-S and VPN-R. In the absence of extranet support, all the VRFs of VPN-S are connected via one MI-PMSI (call it "the VPN-S MI-PMSI"), and all the VRFs of VPN-R are connected via another ("the VPN-R MI-PMSI"). If we want to provide extranet service in which the extranet C-sources are attached to some set of VPN-S VRFs, while the extranet C-receivers are attached to some set of VPN-R VRFs, then we have two choices:

1. either the VPN-R VRFs need to join the VPN-S MI-PMSI, or

2. the VPN-S VRFs need to join the VPN-R MI-PMSI.

The first choice is used to support the "single PMSI per C-flow" transmission model. The second choice is used to support the "multiple PMSIs per C-flow" transmission model.

Procedures for both models are described below.

To support these models, it must be possible to determine which I-PMSI A-D routes are associated with the VPN-S I-PMSI, and which are associated with the VPN-R I-PMSI. Procedures are given for assigning RTs to these routes in a way that makes this determination possible.

Both models allow the use of S-PMSIs to carry multicast data traffic. If a VRF containing receivers can receive from multiple MI-PMSIs,

each S-PMSI must be uniquely associated with a particular MI-PMSI. Procedures are given for assigning RTs to these routes in a way that makes this determination possible.

All the procedures specified in Sections 3-5 still apply.

Note that there are no special extranet procedures for Inter-AS I-PMSI A-D routes or for Leaf A-D routes. Source Active A-D routes are not used when PIM is the PE-PE C-multicast protocol.

6.1. Provisioning VRFs with RTs

6.1.1. Incoming and Outgoing Extranet RTs

In the absence of extranet service, suppose that each VRF of a given VPN, call it VPN-S, is configured with RT-S as its import and export RT, and that each VRF of a second VPN, call it VPN-R, is configured with RT-R as its import and export RT. We will refer to RT-S and RT-R as "non-extranet RTs".

Now suppose that VPN-S contains some extranet C-sources, and VPN-R contains some extranet C-receivers that are allowed by policy to receive extranet C-flows from the VPN-S extranet C-sources.

To set up this S-to-R extranet, it is necessary to provision an additional RT, call it RT-S-to-R, whose value is, in general, distinct from RT-S and RT-R.

A VPN-S VRF that contains extranet C-sources allowed to transmit to VPN-R must be configured with RT-S-to-R as an "Outgoing Extranet RT".

A VPN-R VRF that contains extranet C-receivers allowed to received from VPN-S must be configured with RT-S-to-R as an "Incoming Extranet RT".

Note that the terms "Incoming" and "Outgoing" in this context refer to the direction of multicast data packets relative to the VRF.

The Incoming Extranet RTs and Outgoing Extranet RTs that are configured for a given VRF serve as import RTs for that VRF. They also serve as export RTs, but only for specific routes as specified in section 6.1.2 below.

Note that any VRF that contains both extranet C-sources and extranet C-receivers MUST be configured with both Outgoing and Incoming Extranet RTs.

A VRF may be configured with more than one Incoming and/or Outgoing Extranet RT.

If it happens to be the case that all C-sources in VPN-S are extranet C-sources allowed to transmit to VPN-R, then VPN-S VRFs may be configured such that RT-S is both a non-extranet RT and an Outgoing Extranet RT, and VPN-R VRFs may be configured such that RT-S is an Incoming Extranet RT.

6.1.2. UMH-eligible Routes and RTs

Suppose R1 is a route, exported from a VPN-S VRF, matching an extranet C-source that is allowed by policy to transmit to VPN-R. Then R1 MUST carry the Outgoing Extranet RT used for the S-to-R extranet. This will cause the route to be imported into the VPN-R VRFs that have extranet C-receivers that are allowed by policy to receive from VPN-S.

The rules of Section 3 regarding route targets and ambiguous addresses still apply.

6.1.3. PIM C-Instance Reverse Path Forwarding Determination

Suppose a PIM control message, call it M, is received by a given VRF V, from a particular P-tunnel T. In order to process control message M, the PIM C-instance associated with VRF V may need to do an "RPF determination" (see section 5.2.2 of RFC 6513) for a particular IP prefix S. RPF determination is based upon the rules for UMH selection as specified in section 5.1 of RFC 6513.

This document adds an additional constraint on the UMH selection procedure. When doing RPF determination for a PIM control message received over a P-tunnel, a route matching prefix S is not considered to be eligible for UMH selection unless there is an RT, call it RT1, configured as one of V's Outgoing Extranet RTs, such that the following two conditions both hold:

1. The route matching S is exported from VRF V carrying RT1, and

2. An I-PMSI A-D route advertising P-tunnel T (in its PTA) has been imported into VRF V, and that I-PMSI A-D route carries RT1.

6.2. Single PMSI per C-flow Model

In this model, if a VPN-S VRF has extranet multicast C-sources, and a VPN-R VRF has extranet multicast C-receivers allowed by policy to receive from the C-sources in the VPN-S VRF, then the VPN-R VRF joins the MI-PMSI that VPN-S uses for its non-extranet traffic.

6.2.1. Forming the MI-PMSIs

Consider a VPN-S VRF that has extranet C-sources. Per [MVPN], each VPN-S VRF must originate an Intra-AS I-PMSI A-D route containing a PMSI Tunnel Attribute (PTA) specifying the P-tunnel to be used as part of the VPN-S MI-PMSI. In the absence of extranet service, this route carries the VRF's non-extranet RT, RT-S. When extranet service is provided (using the "single PMSI per C-flow" model), this route MUST also carry EACH of the VRF's Outgoing Extranet RTs.

Consider a VPN-R VRF that has extranet C-receivers. Per [MVPN], each VPN-R VRF must originate an Intra-AS I-PMSI A-D route containing a PTA specifying the P-tunnel to be used as part of the VPN-R MI-PMSI. This route carries the VRF's non-extranet RT RT-R. When extranet service is provided (using the "single PMSI per C-flow" model), the VPN-R VRF MUST also originate one or more additional Intra-AS I-PMSI A-D routes. It MUST originate one additional Intra-AS I-PMSI A-D route for each Incoming Extranet RT with which it has been configured; each such route will carry exactly one of the configured Incoming Extranet RTs.

Note that when a VRF originates more than one Intra-AS I-PMSI A-D route, each of them MUST contain a different RD in its NLRI. In addition, we add the requirement that any pair of such routes MUST NOT contain an RT in common.

A VRF with extranet C-sources MUST join the P-tunnels advertised in the imported I-PMSI A-D routes that carry its non-extranet RT or any of its Outgoing Extranet RTs. This set of P-tunnels will be treated as instantiating a single MI-PMSI, and the associated PIM C-instance will treat that MI-PMSI as a single LAN, and will run PIM procedures on that LAN, as specified in [MVPN]. The fact that the MI-PMSI attaches to VRFs of different VPNs is not known to the PIM C-instance of the VRF containing the sources.

A VRF with extranet C-receivers MUST join the P-tunnels advertised in all the imported I-PMSI A-D routes. The set of P-tunnels advertised in the I-PMSI A-D routes that carry a particular Incoming Extranet RT are treated as instantiating a particular MI-PMSI. So a VRF with C-receivers will "see" several MI-PMSIs, one corresponding to the

non-extranet, and as many as one for each configured Incoming Extranet RT. The PIM C-instance associated with the VRF will treat each of these MI-PMSIs as a separate LAN interface.

As an example, suppose:

- All VPN-R VRFs are configured with RT-R as a non-extranet import and export RT,
- VPN-R VRFs with extranet receivers are configured with RT-S-to-R as an Incoming Extranet RT,
- VPN-S VRFs with extranet transmitters are configured:
    - with RT-S as a non-extranet import and export RT
    - with a list of IP addresses that are the addresses of the extranet sources
    - with RT-S-to-R as an Outgoing Extranet RT

Then VPN-S VRFs will export UMH-eligible routes matching extranet C-sources, and these routes will carry both RT-S and RT-S-to-R. Each VPN-S VRF will also export an Intra-AS I-PMSI A-D route that carries both RT-S and RT-S-to-R.

VPN-R VRFs will originate and export two Intra-AS I-PMSI A-D routes: one carrying RT-R, and one carrying RT-S-to-R. The Intra-AS I-PMSI A-D route with RT-S-to-R will be imported into the VPN-S VRFs.

VPN-R will regard all the I-PMSI A-D routes it has exported or imported with RT-S-to-R as part of a single MI-PMSI. VPN-R will regard all the I-PMSI A-D routes it has exported or imported with RT-R as part of a second MI-PMSI. The PIM C-instance associated with a VPN-R VRF will treat the two MI-PMSIs as two separate LAN interfaces. However, the VPN-S VRFs will regard all the I-PMSI A-D routes imported with RT-S or RT-S-to-R as establishing only a single MI-PMSI. One can think of this as follows: the VPN-R VRFs have joined the VPN-S MI-PMSI, as well as the VPN-R MI-PMSI.

Extranets consisting of more than two VPNs are easily supported as follows. Suppose there are three VPNs, VPN-A, VPN-B, and VPN-C. VPN-A and VPN-B have extranet C-sources, and VPN-C contains receivers for both VPN-A extranet C-sources and VPN-B extranet C-sources. In this case, the VPN-C VRFs that have receivers for both VPN-A and VPN-B sources may be provisioned as follows. These VPN-C VRFs may be provisioned with RT-C as a non-extranet RT, and with RT-A-to-C and RT-B-to-C as Incoming Extranet RTs. In this case, the VPN-C VRFs

that are so provisioned will originate three Intra-AS I-PMSI A-D routes (each with a different RD in its NLRI), each of which carries exactly one of the three RTs just mentioned. The VPN-B VRFs with extranet C-sources will be provisioned with RT-B-to-C as an Outgoing Extranet RT, and the VPN-A VRFs are provisioned with RT-A-to-C as an Outgoing Extranet RT. The result will be that the PIM C-instance associated with a VPN-C VRF will see three LAN interfaces: one for the non-extranet, one for each of the two extranets. This generalizes easily to the case where there are VPN-C receivers in n different extranets (i.e., receiving extranet flows whose sources are in n different VPNs).

Suppose again that there are there are three VPNs, VPN-A, VPN-B, and VPN-C. But in this example, VPN-A is the only one with extranet sources, while VPN-B and VPN-C both have receivers for the VPN-A extranet sources. This can be provisioned as either one extranet or as two.

To provision it as one extranet, the VPN-A VRFs are configured with one Outgoing Extranet RT, call it "RT-A-extranet". The VPN-B and VPN-C VRFs with extranet receivers will be provisioned with RT-A-extranet as Incoming Extranet RT. Thus the VPN-B and VPN-C VRFs will each originate two Intra-AS I-PMSI A-D routes, one for non-extranet, and one for the extranet. The Intra-AS I-PMSI A-D route, from a given VRF, for the extranet will carry RT-A-extranet, but will not share any RT with the non-extranet A-D routes exported from the same VRF.

The result is that the VPN-B and VPN-C VRFs each belong to two MI-PMSIs, one for the extranet and one for the intranet. The MI-PMSI for the extranet attaches VPN-A VRFs, VPN-B VRFs, and VPN-C VRFs.

Alternatively, one could provision the VPN-A VRFs so that some UMH-eligible extranet source routes carry an RT which we will call "RT-A-to-B", and some carry an RT which we will call "RT-A-to-C". The VPN-A VRFs would be configured with both of these as Outgoing Extranet RTs. To allow an extranet flow from a VPN-A source to have both VPN-B and VPN-C receivers, the UMH-eligible route for that source would carry both RTs. VPN-B VRFs (but not VPN-C VRFs) would be provisioned with RT-A-to-B as an Incoming Extranet RT. VPN-C VRFs (but not VPN-B VRFs) would be provisioned with RT-A-to-C as an an Incoming Extranet RT.

Following the rules above, if any VPN-A extranet source is to have both VPN-B and VPN-C receivers, the VPN-B and VPN-C VRFs will each originate two I-PMSI A-D routes, one for extranet and one for non-extranet. The single Intra-AS I-PMSI A-D route originated by the VPN-A VRFs will have both RT-A-to-B and RT-A-to-C among its RTs (as

well as VPN-A's non-extranet RT). The extranet I-PMSI A-D route originated from a VPN-B VRF would have RT-A-to-B, and the extranet I-PMSI A-D route originated from a VPN-C VRF would have RT-A-to-C.

If a given VRF contains both extranet C-receivers and extranet C-sources, the procedures described above still work, as the VRF will be configured with both Incoming Extranet RTs and Outgoing Extranet RTs; the VRF functions both as a VPN-S VRF and as a VPN-R VRF.

6.2.2. S-PMSIs

When PIM is used as the PE-PE C-multicast control plane, every S-PMSI is considered to be part of the "emulated LAN" that "corresponds" to a particular MI-PMSI.

When the bindings of C-flows to particular S-PMSIs are announced via S-PMSI Join Messages ([MVPN], Section 7) sent on the MI-PMSI, the S-PMSI is considered to be part of the same LAN interface as the corresponding MI-PMSI.

When the bindings of C-flows to particular S-PMSIs are announced via S-PMSI A-D routes, then any S-PMSI A-D route exported from that VRF MUST have an RT in common with exactly one of the Intra-AS A-D routes exported from that VRF, and this MUST be one of the VRF's Outgoing Extranet RTs. Further, the S-PMSI A-D route MUST NOT have an RT in common with any other Intra-AS A-D route exported from a VRF on the same PE. A given S-PMSI A-D route will be considered to "correspond" to the MI-PMSI of the Intra-AS I-PMSI A-D route (originated from the same PE) with which it shares an RT.

The MI-PMSI that corresponds to a given S-PMSI is determined as follows:

- If there is an Intra-AS I-PMSI A-D route originated by the same PE that originated the S-PMSI A-D route, and if the those two routes have an RT in common, and if that RT is one of the VRF's Incoming Extranet RTs, then the S-PMSI corresponds to the I-PMSI associated with that Intra-AS I-PMSI A-D route.

- Otherwise, if there is an Inter-AS I-PMSI A-D route originated in the same AS as the S-PMSI A-D route, and if the those two routes have an RT in common, and if that RT is one of the VRF's Incoming Extranet RTs, then the S-PMSI corresponds to the I-PMSI associated with that Inter-AS I-PMSI A-D route.

- Otherwise, there must be a configuration error (a violation of the requirements of Sections 3-5 of this document).

When wildcard S-PMSIs are used, the rules given in [MVPN-WILDCARDS] for determining whether a given S-PMSI A-D route is a "match for reception" to a given (C-S,C-G) or (C-*,C-G) are modified as follows:

> A given S-PMSI A-D route MUST NOT be considered to be a "match for reception" for a given (C-S,C-G) or (C-*,C-G) state UNLESS that S-PMSI A-D route "corresponds" (as defined above) to the MI-PMSI that is the incoming interface for the given state.

The rules given in [MVPN-WILDCARDS] for determining whether a given S-PMSI A-D route is a "match for transmission" are unchanged.

6.2.3. Sending PIM Control Packets

Suppose a PE, say PE1, receives a PIM Join(S,G) from a CE, over a VRF interface that is associated with a VPN-R VRF. The PE does the RPF check for S by looking up S in the VPN-R VRF. The PIM C-instance associated with that VRF must determine the correct P-tunnel over which to send a PIM Join(S,G) to other PEs.

To do this, PE1 finds, in the VRF associated with the interface over which the Join was received, the selected UMH route for S, following the procedures of section 5.1 of [MVPN]. PE1 determines the set of RTs carried by that route. PE1 then checks to see if there is an Intra-AS I-PMSI A-D route, currently originated by PE1, that has an RT in common with the selected UMH route for S.

If the rules of Sections 3-5 have been followed, each of PE1's selected UMH routes will share an RT with a single one of PE1's currently originated Intra-AS I-PMSI A-D routes. If this is so, the Join is sent on the P-tunnel advertised in the PTA of that route. Otherwise, the Join MUST NOT be sent.

In essence, this procedure makes the RPF check for C-S resolve to the MI-PMSI that is serving as the next hop "interface" to C-S.

If a PE receives a PIM Join(*,G) from a CE, the procedure for doing the RPF check is the same, except that the selected UMH route will be a route to the C-RP associated with the C-G group.

6.2.4. Receiving PIM Control Packets

When a PIM C-instance receives a PIM control message from a P-tunnel, it needs to identify the message's "incoming interface". This incoming interface is the MI-PMSI of which the P-tunnel is a part.

6.2.5. Sending and Receiving Data Packets

The rules for choosing the PMSI on which to send a multicast data packet are as specified in [MVPN] and [MVPN-WILDCARDS], with one new restriction: a VPN-S VRF always transmits a multicast data packet either on the VPN-S MI-PMSI or on an S-PMSI that corresponds to the VPN-S MI-PMSI. From the perspective of the PIM C-instance, there is only one outgoing interface.

When a PIM C-instance receives a multicast data packet from a given P-tunnel, and that P-tunnel is being used to instantiate an MI-PMSI, the MI-PMSI of which the P-tunnel is a part (see Sections 6.2.1 and 6.2.2) is considered to be the packet's "incoming interface". If the packet is received on a P-tunnel that was advertised in an S-PMSI A-D route, the packet's "incoming interface" is the MI-PMSI to which that S-PMSI route corresponds, as defined in Section 6.2.2. Ordinary PIM rules for data plane RPF check apply.

Following ordinary PIM procedures, packets arriving from an unexpected incoming interface are discarded. This eliminates any problems due to the ambiguities described in Sections 2.1 and 2.2.

6.3. Multiple PMSIs per C-flow Model

In this model, if a VPN-S VRF has extranet multicast C-sources, and a VPN-R VRF has extranet multicast C-receivers allowed by policy to receive from the C-sources in the VPN-S VRF, then the VPN-S VRF joins the MI-PMSI that VPN-R uses for its non-extranet traffic.

In the "single PMSI per C-flow" transmission model (as described in Section 6.2), a PE that needs to transmit a multicast data packet to a set of other PEs transmits the packet on a single PMSI. This means that if a packet needs to be transmitted from a VPN-A VRF and received at a VPN-B VRF and a VPN-C VRF, there must be some P-tunnel from which the VPN-B and VPN-C VRFs can both receive packets.

In the "multiple PMSIs per C-flow" transmission model, a PE that needs to transmit a multicast data packet to a set of other PEs may transmit the packet on several different PMSIs. (Of course, any given packet is transmitted only once on a given P-tunnel.) For

example, if a C-flow (C-S,C-G) has a VPN-A C-source, a VPN-B receiver, and a VPN-C receiver, there could be one PMSI that the VPN-A VRF uses to transmit the packet to the VPN-B VRFs, and another PMSI that the VPN-A VRF uses to transmit the packet to the VPN-C VRFs.

6.3.1. Forming the MI-PMSIs

Consider a VPN-R VRF that has extranet C-receivers. Per [MVPN], each VPN-R VRF must originate an Intra-AS I-PMSI A-D route containing a PMSI Tunnel Attribute (PTA) specifying the P-tunnel to be used as part of the VPN-R MI-PMSI. In the absence of extranet service, this route carries the VRF's non-extranet RT, RT-R. When extranet service is provided (using the "single PMSI per C-flow" model), this route MUST also carry each of the VRF's Incoming Extranet RTs.

Consider a VPN-S VRF that has extranet C-sources. Per [MVPN], each VPN-S VRF must originate an Intra-AS I-PMSI A-D route containing a PTA specifying the P-tunnel to be used as part of the VPN-S MI-PMSI. This route carries the VRF's non-extranet RT RT-S. When extranet service is provided using the "multiple PMSI per C-flow" model, the VPN-S VRF MUST also originate one or more additional Intra-AS I-PMSI A-D routes. It MUST originate one additional Intra-AS I-PMSI A-D route for each outgiong extranet RT with which it has been configured; each such route will have a distinct RD, and will carry exactly one of the configured Outgoing Extranet RTs.

As with the "single PMSI per C-flow" transmission model, VRFs containing extranet C-receivers need to import UMH-eligible extranet C-source routes from VRFs containing C-sources. This is ensured by the rules of Sections 3-5.

However, in the "multiple PMSIs per C-flow model", a VRF containing only C-receivers originates only a single Intra-AS I-PMSI A-D route, carrying the non-extranet RT and all the Incoming Extranet RTs.

When a VRF containing C-receivers imports Intra-AS I-PMSI A-D routes that carry the non-extranet RT or one of the Incoming Extranet RTs, the P-tunnels specified in the PTA of all such routes are considered to be part of the same MI-PMSI. I.e., the associated PIM C-instance will treat them as part of a single interface.

In this model, it is the VRF containing extranet C-sources that must originate multiple Intra-AS I-PMSI A-D routes. Each such route must have a distinct RD, and the set of RTs carried by any one of these routes must be disjoint from the set carried by any other. There

must be one such route for each of the VRF's Outgoing Extranet RTs, and Each such route must carry exactly one of the VRF's Outgoing Extranet RTs. The VRFs containing extranet C-sources MUST also import all the A-D routes originated by the VRFs containing extranet C-receivers. If a set of originated and/or imported Intra-AS I-PMSI A-D routes have an RT in common, and that RT is one of the VRF's Outgoing Export RTs, then those routes are considered to be "about" the same MI-PMSI. The PIM C-instance of the VRF treats each MI-PMSI as a LAN Interface.

In effect, if VPN-S has only extranet C-sources and VPN-R has only extranet C-receivers, this model has the VPN-S VRFs join the VPN-R MI-PMSI. The VPN-S VRFs will thus be attached to multiple MI-PMSIs, while the VPN-R VRFs are attached to only one. The fact that the VPN-R MI-PMSI is attached to VPN-S VRFs is not known to the PIM C-instance at the VPN-R VRFs.

If a VPN-A VRF has extranet C-sources allowed to send to C-receivers in a VPN-B VRF, and the VPN-B VRF has C-sources allowed to send to C-receivers in the VPN-A VRF, the above procedures still work as specified.

Following normal PIM procedures, when the PIM C-instance at a VRF with extranet C-sources receives a Join(C-S,C-G) or a Join(C-*,C-G) over an MI-PMSI, it may create (C-S,C-G) or (C-*,C-G) state, and the MI-PMSI over which the Join was received may be added to the set of outgoing interfaces for that multicast state. If n MI-PMSIs are added to the outgoing interface list for a particular multicast state, a multicast data packet may need to be replicated n times, and transmitted once on each of the n MI-PMSIs.

Since the all multicast data packets received from another PE are received over a single emulated LAN, it is not necessary to have any special procedures to determine a packet's "incoming interface". The ambiguities described in Section 2.1 and 2.2 do not occur, because a VPN-R VRF can only receive multicast data traffic that has been requested by a VPN-R VRF.

7. When BGP is the PE-PE C-multicast Control Plane

This document assumes that if BGP is used as the PE-PE C-multicast control plane, the "Single PMSI per C-flow" model is used. Procedures for providing the "Multiple PMSIs per C-flow" model with BGP C-multicast are outside the scope of this document.

When BGP is used as the C-multicast control plane, the Single PMSI per C-flow model may be used either with or without "extranet

separation". (Recall that "extranet separation" means that no P-tunnel can carry both traffic from extranet sources and traffic from non-extranet sources.) In either case, the data traffic may be carried on inclusive tunnels only, or on selective tunnels only (known as the "S-PMSI only" model), or on a combination of inclusive and selective tunnels. This is determined by provisioning. The procedures specified below support all three choices.

Note that there are no special extranet procedures for Inter-AS I-PMSI A-D routes or for Leaf A-D routes.

7.1. Originating C-multicast Routes

This section applies whether extranet separation is used or not.

Procedures specified in Section 11.1.3 ("Constructing the rest of the C-multicast route") of [MVPN-BGP] 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 [MVPN-BGP]), 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 by the selected UMH route for the address carried in the Multicast Source field of MCAST-VPN NLRI.

7.2. Originating A-D Routes Without Extranet Separation

7.2.1. Intra-AS I-PMSI A-D Routes

Consider a VRF, call it VRF-S, that contains extranet C-sources, and that exports UMH-eligible routes matching those C-sources. The VRF may also originate and export an Intra-AS I-PMSI A-D route.

As specified in [MVPN-BGP], if exactly one Intra-AS I-PMSI A-D route is originated by and exported from VRF-S, the RTs carried by that route MUST be chosen such that every VRF that imports a UMH-eligible route from VRF-S also imports this Intra-AS I-PMSI A-D route.

If inclusive P-tunnels are being used to carry extranet C-flows, there are additional requirements on the way the RTs carried by the Intra-AS I-PMSI A-D routes must be chosen, as specified in the following paragraph.

If VRF-S is using Inclusive P-tunnels, but is not using extranet separation, there is one inclusive P-tunnel rooted at VRF-S, and this

tunnel carries both extranet and non-extranet C-flows. This inclusive tunnel is identified in the PMSI Tunnel Attribute (PTA) of the Intra-AS I-PMSI A-D route originated from VRF-S. The set of RTs carried by this Intra-AS I-PMSI A-D route MUST be chosen so as to ensure that every VRF that imports a UMH-eligible route from this VRF-S also imports this Intra-AS I-PMSI A-D route. Further, the set of RTs carried by this Intra-AS I-PMSI A-D route MUST be chosen such that it has at least one RT in common with every UMH-eligible route that is exported from the VRF.

7.2.2. S-PMSI A-D Routes

Suppose that a given S-PMSI A-D route, exported from VRF-S, is used to bind some or all of the extranet C-flows from a given extranet C-source to a given selective P-tunnel. (This includes S-PMSI A-D routes that use wildcards [MVPN-WILDCARDS]). That S-PMSI A-D route MUST have at least one RT in common with each of the UMH-eligible routes that is exported from VRF-S and that matches the given extranet C-source. Further, the RTs MUST be such that every VRF that imports one of these UMH-eligible routes also imports the S-PMSI A-D route.

An implementation MUST allow the set of RTs carried by the S-PMSI A-D routes to be specified by configuration. In the absence of such configuration, an S-PMSI A-D route originated by a given VRF X MUST carry a default set of RTs, as specified by the following rules:

1. By default an S-PMSI A-D route originated by VRF X for a given (C-S,C-G) or (C-S,C-*) carries the same RT(s) as the UMH-eligible route originated by VRF X that matches C-S.

2. By default an S-PMSI A-D route originated by VRF X for a given (C-*,C-G) carries as its RTs a set union of all RT(s) of the UMH-eligible route(s) matching the multicast C-sources contained in VRF X that could originate traffic for that C-G. Moreover, if the VRF contains (as defined in section 1.1) the C-RP of C-G, then this set union also includes the RT(s) of the UMH-eligible route matching C-RP, and of the unicast VPN-IP route matching C-RP.

3. By default, if a (C-*,C-*) S-PMSI A-D route originated by VRF X is to be used for both extranet and non-extranet traffic, it carries the same RTs that would be carried (as specified in section 7.2.1) by an I-PMSI A-D route originated by VRF X if that I-PMSI A-D route were advertising an inclusive P-tunnel for carrying both extranet and non-extranet traffic. In general, a given VRF would not originate both (a) an S-PMSI A-D

route advertising a (C-*,C-*) selective P-tunnel for both extranet and non-extranet traffic and (b) an I-PMSI A-D route advertising an inclusive P-tunnel for both extranet and non-extranet traffic, as the inclusive P-tunnel would not get used in that case.

7.2.3. Source Active A-D Routes

If VRF-S exports a Source Active A-D route that contains C-S in the Multicast Source field of its NLRI, and if that VRF also exports a UMH-eligible route matching C-S, the Source Active A-D route MUST carry at least one RT in common with the UMH-eligible route. The RT must be chosen such that the following condition holds: if VRF-R contains an extranet C-receiver allowed by policy to receive extranet traffic from C-S, then VRF-R imports both the UMH-eligible route and the Source Active A-D route.

By default, a Source Active A-D route for a given (C,S,C-G), exported by a given VRF, carries the same set of RTs as the UMH-eligible route matching C-S that is exported from that VRF.

7.3. Originating A-D Routes With Extranet Separation

7.3.1. Intra-AS I-PMSI A-D Routes

This section applies when VRF-S is using extranet separation, AND when VRF-S is using an Inclusive P-tunnel to carry some or all of the extranet C-flows that it needs to transmit to other VRFs.

If VRF-S contains both extranet C-sources and non-extranet C-sources, and if inclusive P-tunnels are used to carry both extranet C-flows and non-extranet C-flows, then there MUST be two inclusive tunnels from VRF-S, one of which is to be used only to carry extranet C-flows (the "extranet inclusive P-tunnel"), and one of which is to be used only to carry non-extranet C-flows (the "non-extranet inclusive P-tunnel"). In this case, the VRF MUST originate two Intra-AS I-PMSI A-D routes. Their respective NLRIs must of course have different RDs. One of the Intra-AS I-PMSI A-D routes identifies the extranet inclusive P-tunnel in its PTA, the other identifiers the non-extranet Inclusive P-tunnel in its PTA.

If VRF-S uses an Inclusive P-tunnel for carrying extranet traffic, but does not use an Inclusive P-tunnel for carrying non-extranet traffic, then of course only a single Intra-AS I-PMSI A-D route need be originated. The PTA of this route identifies the "extranet inclusive P-tunnel".

An Intra-AS I-PMSI A-D route whose PTA identifies an extranet inclusive P-tunnel MUST carry the Extranet Separation extended community defined in section 3.6.

The RTs carried by an Intra-AS I-PMSI A-D route whose PTA identifies the "extranet inclusive P-tunnel" MUST be chosen such that the following condition holds: if a VRF (call it VRF-R) imports a UMH-eligible route from VRF-S, and if that route matches an extranet C-source, then VRF-R also imports that Intra-AS I-PMSI A-D route.

These procedures generalize easily to the case where there are n inclusive P-tunnels from VRF-S. One such P-tunnel is used to carry flows from non-extranet C-sources. The other n-1 inclusive P-tunnels are used as follows. The set of extranet C-sources is partitioned into n-1 non-intersecting sets. Each such set is associated (by provisioning) to one such P-tunnel. A particular inclusive P-tunnel is then used to carry only those extranet C-flows whose C-sources (or C-RPs) are in the corresponding set.

Note that when extranet separation is used, it is possible to use an inclusive P-tunnel for non-extranet traffic while using only selective P-tunnels for extranet traffic. It is also possible to use an inclusive P-tunnel for extranet traffic while using only selective P-tunnels for non-extranet traffic.

7.3.2. S-PMSI A-D Routes

Suppose that a given S-PMSI A-D route, exported from VRF-S, is used to bind some or all of the extranet C-flows from a given extranet C-source to a given selective P-tunnel. (This includes S-PMSI A-D routes that use wildcards [MVPN-WILDCARDS]). That S-PMSI A-D route MUST have at least one RT in common with each of the UMH-eligible routes, exported from VRF-S, that matches the given extranet C-source. Further, the RTs MUST be such that every VRF that imports one of these UMH-eligible routes also imports the S-PMSI A-D route.

The following rules, specific to the use of extranet separation, apply:

- A selective P-tunnel MUST NOT carry C-flows from both extranet and non-extranet C-sources,

- If it is desired to use a (C-*,C-*) S-PMSI to carry extranet traffic and also to use a (C-*,C-*) S-PMSI to carry non-extranet traffic, then two (C-*,C-*) S-PMSI A-D routes MUST be originated. These two routes MUST have different RDs in their respective NLRI fields, and their respective PTAs MUST identify different

P-tunnels.

- A (C-*,C-*) S-PMSI A-D route advertising a P-tunnel that is used to carry extranet traffic MUST carry the Extranet Separation extended community defined in section 3.6.

An implementation MUST allow the set of RTs carried by the S-PMSI A-D routes to be specified by configuration. In the absence of such configuration, an S-PMSI A-D route originated by a given VRF X MUST carry a default set of RTs, as specified by the following rules:

1. Rule 1 of section 7.2.2 applies.

2. By default, if C-G is an extranet C-group, rule 2 of section 7.2.2 applies.

3. By default, if a (C-*,C-*) S-PMSI A-D route originated by VRF X is to be used for extranet traffic, it carries the same RTs that would be carried (as specified in section 7.3.1) by an I-PMSI A-D route originated by VRF X if that I-PMSI A-D route were advertising an inclusive P-tunnel for carrying extranet traffic. In general, a given VRF would not originate both an S-PMSI A-D route advertising a (C-*,C-*) selective P-tunnel for extranet traffic and an I-PMSI A-D route advertising an inclusive P-tunnel for extranet traffic, as the inclusive P-tunnel would not get used in that case.

7.3.3. Source Active A-D Routes

The procedures of Section 7.2.3 apply.

7.4. Determining the Expected P-tunnel for a C-flow

This section applies whether extranet separation is used or not.

In the context of a VRF with receivers for a particular C-flow, a PE must determine the P-tunnel over which packets of that C-flow are expected to arrive. This is done by finding an I-PMSI or S-PMSI A-D route that "matches" the flow. The matching A-D route will contain a PTA that specifies the P-tunnel being used to carry the traffic of that C-flow. We will refer to this P-tunnel as the "expected P-tunnel" for the C-flow.

A PE that needs to receive a given (C-S,C-G) or (C-*,C-G) C-flow MUST join the expected P-tunnel for that C-flow, and the PE MUST remain joined to the P-tunnel as long as the PE continues to need to receive

the given C-flow, and the P-tunnel continues to remain the expected P-tunnel for that C-flow.

If a PTA specifies a non-zero MPLS label, then the PE originating the A-D route containing that PTA is advertising an aggregate P-tunnel. The aggregate P-tunnel can be thought of as an outer P-tunnel multiplexing some number of inner P-tunnels. The inner P-tunnels are demultiplexed by means of the MPLS label in the PTA. In this document, when we talk of the "expected P-tunnel" in the context of an aggregate P-tunnel, we refer to a particular inner P-tunnel, not to the outer P-tunnel. It is this "inner P-tunnel" that is the expected P-tunnel for a given C-flow.

In order to find the expected P-tunnel for a given C-flow, the upstream PE of the C-flow is first determined. Then the S-PMSI A-D routes originated by that PE are examined, and their NLRIs compared to the (C-S/C-RP,C-G) of the flow, to see if there is a "match for reception". (If there is no S-PMSI A-D route that matches a given C-flow, the expected P-tunnel for that C-flow may have been advertised in an I-PMSI A-D route; see section 7.4.5.)

The rules for determining, in non-extranet cases, whether a given C-flow is a "match for reception" for a given S-PMSI A-D route are given in [MVPN-WILDCARDS] Section 3.2. Note that we use the terms "installed" and "originated" as they are defined in [MVPN-WILDCARDS] Section 3.2. (See also Section 1.1 of this document.)

This specification adds additional rules for determining whether a given S-PMSI A-D route is a "match for reception" for a given (C-S/C-RP,C-G). Note that these rules all assume the context of a particular VRF into which the A-D route has been imported.

The rules given in [MVPN-WILDCARDS] for determining whether a given S-PMSI A-D route is a "match for transmission" remain unchanged.

Under certain conditions, the upstream PE for a given (C-S,C-G) flow is determined by examining the Source Active A-D routes that have (C-S,C-G) encoded in their NLRI fields. When extranet functionality is being provided, an SA A-D route is considered to "match" a (C-S,C-G) flow, in the context of a given VRF with receivers for that flow, only if the selected UMH route to C-S has at least one RT in common with the SA A-D route, and at least one of the RTs in common is an import RT of the VRF. Once the upstream PE is selected, the P-tunnel over which the flow is expected is determined according to the procedures described in this section.

7.4.1. (C-S,C-G) S-PMSI A-D Routes

When extranet functionality is being provided, an S-PMSI A-D route whose NLRI contains (C-S,C-G) is NOT considered to be a "match for reception" for a given C-flow (C-S,C-G) unless one of the following conditions holds (in addition to the conditions specified in [MVPN-WILDCARDS]):

- the "single C-source per (C-S,C-G) or (C-S,C-*) P-tunnel" is provisioned, or

- the selected UMH route for C-S has at least one RT in common with the S-PMSI A-D route, and at least one of the common RTs is an import RT of the VRF.

7.4.2. (C-S,C-*) S-PMSI A-D Routes

When extranet functionality is being provided, an S-PMSI A-D route whose NLRI contains (C-S,C-*) is NOT considered to be a "match for reception" for a given C-flow (C-S,C-G) unless one of the following conditions holds, in addition to the conditions specified in [MVPN-WILDCARDS]:

- the "single C-source per (C-S,C-G) or (C-S,C-*) P-tunnel" is provisioned, or

- the selected UMH route for C-S has at least one RT in common with the S-PMSI A-D route, and at least one of the common RTs is an import RT of the VRF.

7.4.3. (C-*,C-G) S-PMSI A-D Routes

When extranet functionality is being provided, an S-PMSI A-D route whose NLRI contains (C-*,C-G) is NOT considered to be a "match for reception" for a given C-flow (C-S,C-G) in a given VRF unless either condition 1 or condition 2 below holds, in addition to the conditions specified in [MVPN-WILDCARDS]:

1. The given VRF has currently originated a C-multicast Shared Tree Join route for (C-*,C-G), and

   a) (C-*,C-G) matches an installed (C-*,C-G) S-PMSI A-D route (according to [MVPN-WILDCARDS]) in the given VRF, and

b) either

i) the "Single C-group per (C-*,C-G) P-tunnel" policy has been provisioned, or

ii) the RTs of that S-PMSI A-D route form a non-empty intersection with the RTs carried in the VRF's selected UMH route for C-RP of that C-G, or

iii) there are one or more Source Active A-D routes for (C-S,C-G) installed in the VRF, where these routes have been originated by the same PE as the (C-*,C-G) S-PMSI A-D route, and the RTs of the (C-*,C-G) S-PMSI A-D route form a non-empty intersection with the RTs of one or more of the selected UMH-eligible routes for C-S.

2. The given VRF does not have a currently originated C-multicast Shared Tree Join for (C-*,C-G), but

a) there are one or more values for C-S for which the VRF has a currently originated Source Tree Join C-multicast route for (C-S,C-G), and

b) the (C-* C-G) S-PMSI A-D route matches (according to [MVPN-WILDCARDS]) each such (C-S,C-G), and

c) either

i) the "Single C-group per (C-*,C-G) P-tunnel" policy has been provisioned, or

ii) the RTs of that S-PMSI A-D route form a non-empty intersection with the RTs carried in the VRF's selected UMH routes for each such C-S

If a VRF has an installed (C-*,C-G) S-PMSI A-D route, but does not have a (C-S,C-G) or (C-*,C-G) multicast state that matches that route for reception, the procedures of section 12.3 ("Receiving S-PMSI A-D Routes by PEs") of [MVPN-BGP] are not invoked for that route. If those multicast states are created at some later time when the route is still installed, the procedures of section 12.3 of [MVPN-BGP] are invoked at that time.

7.4.4. (C-*,C-*) S-PMSI A-D Routes

A (C-*,C-*) S-PMSI A-D Route (call it "R-AD") is NOT considered to be a match for reception for a given C-flow (C-S,C-G) or (C-*,C-G) unless the following conditions hold (in addition to the conditions specified in [MVPN-WILDCARDS)]:

- the selected UMH route (call it "R-UMH") for C-S or for C-G's C-RP respectively has at least one RT in common with R-AD, and at least one of the common RTs is an import RT of the VRF.

- either R-AD and R-UMH both carry the Extranet Separation extended community, or neither carries the Extranet Separation extended community.

7.4.5. I-PMSI A-D Routes

If the VRF contains no matching S-PMSI A-D routes for a C-flow, then the C-flow is expected to arrive on an Inclusive P-tunnel.

Let R-UMH be the selected UMH route for the given C-flow. That is, if the C-flow is (C-S,C-G), R-UMH is the selected UMH route for C-S, while if the C-flow is (C-*,C-G), R-UMH is the selected UMH route for C-RP. The selected upstream PE for the flow is determined from the VRF Route Import RT of R-UMH. The "selected upstream AS" for the flow is determined from the Source AS Extended Community of R-UMH.

The inclusive P-tunnel that is expected to be carrying a particular C-flow is found as follows:

- If the selected upstream AS is the local AS, then look in the VRF for an installed Intra-AS I-PMSI A-D route, R-AD, such that (a) R-AD originated by the selected upstream PE, (b) R-AD has at least one an RT in common with R-UMH, (c) at least one of the common RTs is an import RT of the local VRF, and (d) either R-AD and R-UMH both carry the Extranet Separation extended community, or neither carries the Extranet Separation extended community.

  The PTA of R-AD specifies the P-tunnel over which traffic of the given C-flow is expected.

- If the selected upstream AS is not the local AS, then look in the VRF for an installed Inter-AS I-PMSI A-D route, R-AD, such that (a) the Source AS field of R-AD's NLRI contains the AS number of the selected upstream AS, (b) R-AD has at least one RT in common with R-UMH, (c) at least one of the common RTs is an import RT of the local VRF, and (d) either R-AD and R-UMH both carry the Extranet Separation extended community, or neither carries the

Extranet Separation extended community.

The PTA of R-AD specifies the P-tunnel over which traffic of the given C-flow is expected.

7.5. Packets Arriving from the Wrong P-tunnel

Any packets that arrive on P-tunnel other than the expected P-tunnel (as defined in Section 7.4) MUST be discarded. Note that packets arriving on the wrong P-tunnel are to be discarded even if they are arriving from the expected PE.

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. The PE MUST be able to replicate this traffic to the multiple VRFs. Specific procedures for doing so are local to the PE, and outside 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 a local matter to the PE, and outside the scope of this document.

An implementation MUST support multiple extranet VRFs on a PE.

9. IANA Considerations

IANA is requested to allocate a new BGP Extended Community, the "Extranet Source" extended community. This is to be allocated from the range of transitive communities in the "opaque extended community" registry.

IANA is requested to allocate a new BGP Extended Community, the "Extranet Separation" extended community. This is to be allocated from the range of transitive communities in the "opaque extended community" registry.

10. Security Considerations

The security considerations of [MVPN] and [MVPN-BGP] are applicable.

In general, different VPNs are allowed to have overlapping IP address spaces, i.e., a host in one VPN may have the same IP address as a host in another. This is safe because the customer routes from a given VPN do not pass into other VPNs. Even if there is overlapping address space among VPNs, the routes that are known at any given VPN site are unambiguous, as long as the address space of that VPN is unambiguous. However, this is not necessarily true when extranet service is provided. If an extranet C-receiver in VPN-R is to be able to receive multicast traffic from an extranet C-source in VPN-S, then the address of the VPN-S extranet C-source must be imported into one or more VPN-R VRFs. If that address is also the address of a VPN-R non-extranet C-source, then a system attempting to receive an extranet C-flow from the VPN-R extranet C-source may instead receive a non-extranet C-flow from the VPN-S C-source. This would result in a VPN security violation.

To avoid this, this document specifies that if a route is imported into a given VRF, all addresses that are match that route must be unambiguous in the context of that VRF. Improper provisioning of the RTs may cause this rule to be violated, and hence result in a VPN security violation.

It is possible that a given multicast C-source is the source of multiple flows, some of which are intended to be extranet C-flows, and some of which are intended to be non-extranet flows. However, the procedures of this document will allow any C-receiver that is able to receive the extranet C-flows from a given C-source to also receive the non-extranet C-flows from that source. As a result, VPN security violations may result if any system is a C-source for both extranet and non-extranet C-flows. However, the set of C-flows transmitted by a given C-source is not under the control of the SP. SPs who offer the extranet MVPN service must make sure that this potential for VPN security violations is clearly understood by the customers who administer the C-sources.

This specification does not require that UMH-eligible routes be "host routes"; they may be less specific routes. So it is possible for the NLRI of a UMH-eligible route to contain an address prefix that matches the address of both an extranet C-source and a non-extranet C-source. If such a route is exported from a VPN-S VRF and imported by a VPN-R VRF, C-receivers contained in VPN-R will be able to receive C-flows from the non-extranet C-sources whose addresses match that route. This may result in VPN security violations. Service providers who offer the extranet MVPN service must make sure that

this is clearly understood by the customers who administer the distribution of routes from CE to PE routers.

If the address ambiguities described in Sections 2.1 and 2.2 are not prohibited by policy, VRFs MUST be able to discard traffic that arrives on the wrong P-tunnel; otherwise VPN security violations may occur.

Section 3.5 specifies the OPTIONAL use of a new extended community, the Extranet Source extended community. Security considerations regarding the use and distribution of that extended community are discussed in that section.

11. Acknowledgments

The authors wish to thank DP Ayyadevara, Robert Kebler, Padmini Misra, Rayen Mohanty, Maria Napierala, Karthik Subramanian, and Kurt Windisch. Special thanks to Jeffrey (Zhaohui) Zhang for his careful review and for providing the ascii art for section 5.

12. Authors' Addresses

Rahul Aggarwal
Juniper Networks
1194 North Mathilda Ave.
Sunnyvale, CA 94089
Email: raggarwa_1@yahoo.com

Yiqun Cai
Microsoft
1065 La Avenida
Mountain View, CA 94043
Email: yiqunc@microsoft.com

Wim Henderickx
Alcatel-Lucent
Email: wim.henderickx@alcatel-lucent.com

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

Praveen Muley
Alcatel-Lucent
Email: Praveen.Muley@alcatel-lucent.com

Ray Qiu
1194 North Mathilda Avenue
Sunnyvale, California 94089
Email: rqiu@juniper.net

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

Eric C. Rosen
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA, 01719
Email: erosen@cisco.com

IJsbrand Wijnands
Cisco Systems, Inc.
De kleetlaan 6a Diegem 1831
Belgium
Email: ice@cisco.com

13. References

13.1. Normative References

[L3VPN] "BGP/MPLS IP VPNs", E. Rosen, Y. Rekhter, et. al., RFC 4364, February 2006

[MPLS-ARCH] "MPLS Architecture", E. Rosen, A. Viswanathan, R. Callon, RFC 3031, January 2001

[MVPN] "Multicast in MPLS/BGP IP VPNs", E. Rosen, R. Aggarwal, et. al., RFC 6513, February 2012

[MVPN-BGP] "BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs", R. Aggarwal, E. Rosen, T. Morin, Y. Rekhter, RFC 6514, February 2012

[MVPN-WILDCARDS] "Wildcards in Multicast VPN Auto-Discovery Routes", Rosen, Rekhter, Henderickx, Qiu, RFC 6625, May 2012

[PIM] "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", Fenner, Handley, Holbrook, Kouvelas, RFC 4601, August 2006

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

13.2. Informative References

[BIDIR-PIM] "Bidirectional Protocol Independent Multicast", Handley, Kouvelas, Speakman, Vicisano, RFC 5015, October 2007

[BSR] "Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)", N. Bhaskar, A. Gall, J. Lingard, S. Venaas, RFC 5059, January 2008

[mLDP] "Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths", IJ. Wijnands, I. Minei, K. Kompella, B. Thomas, RFC 6388, November 2011.

[RFC3446] "Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)", D. Kim, D. Meyer, H. Kilmer, D. Farinacci, January 2003

[RFC4610] "Anycast-RP Using Protocol Independent Multicast (PIM)", D. Farinacci, Y. Cai, August 2006

[RSVP-P2MP] "Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)", R. Aggarwal, D. Papadimitriou, S. Yasukawa, RFC 4875, May 2007