Requirements for multicast in Provider Provisioned IP VPNs

<draft-morin-l3vpn-ppvnp-mcast-reqts-00.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 3 of RFC3667 [RFC3667]. By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she become aware will be disclosed, in accordance with RFC 3668.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

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

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

Abstract

This document presents a set of functional requirements for network solutions that allow the support of IP multicast within IP provider provided virtual private networks (PP VPNs). It specifies requirements both from the end user and service provider standpoints. It is intended that potential solutions, that specify the support of IP multicast within VPNs, use these requirements as a guideline. It is not the intent of this document to propose technical solutions, nor to detail solution specific issues.
1. Introduction

L3VPN services satisfying requirement defined in [VPN-REQ], are now being offered by many service providers worldwide. The success of those VPN services is certainly due to intrinsic characteristics of the solutions:

- customers are unaware of the deployed network technology and
do not need to activate specific mechanisms,
- P routers in the core are unaware of the numbers of VPN customers which allows a good scalability,
- the dynamic configuration of the VPNs which minimize configuration operation when adding new customers

In the meantime, there is a growing need for support of multicast services. Efforts to provide efficient IP multicast routing protocols and multicast group management have been done in standardization bodies which results in particular to the definition of PIM [PIM-SM] [PIM-SSM] and IGMP [IGMPv1] [IGMPv2] [IGMPv3].

However, multicast traffic is not supported natively within the solution defined in [RFC2547bis]. A simple solution to support multicast service in VPN networks consists in establishing unicast tunnels and replicating traffic on PEs. Such kind of techniques have obvious drawbacks such as scalability, operational cost, and bandwidth usage.

This document complements the generic L3 VPN requirement draft [VPN-REQ], by specifying additional requirements specific to multicast services. It clarifies the needs from both VPN client and provider standpoints and formulates the problems that should be addressed by technical solutions with as key objective to stay solution agnostic. There is no intent to either specify solution specific details in this document or application specific requirements.

It is intended that solutions that specify procedures and protocol extensions for multicast in VPN networks satisfy these requirements.

2. Conventions used in this document

2.1. Terminology

The reader is assumed to be familiar with the terminology in [VPN-REQ], [RFC2547bis], [PIM-SM], [PIM-SSM].

2.2. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

1. Problem Statement

1.1. Motivations
More and more L3 VPN customers use IP multicast services within their private infrastructures. Naturally, they want to extend these multicast services to remote sites that are connected via a VPN.
For instance, it could be a national TV channel with several geographical locations that wants to multicast a TV program from a central point to several regional locations within its VPN.

A solution to support multicast traffic would consist in using unicast PSN tunnels and letting PE routers (provider's routers) replicate traffic. This is obviously sub-optimal as it places the replication burden on the PE and hence has very poor scaling characteristics. It also wastes bandwidth and control plane resources in the provider network.

Thus, to provide multicast services for L3 VPN networks in an efficient manner (that is, with scalable impact on signaling and protocol state), in a large scale environment, new mechanisms are required. Existing L3 VPN mechanisms have to be enhanced to support multicast services.

1.2. Requirements Overview

This document targets provider provided IP VPN solutions designed to carry customer multicast traffic, with as main requirement the fact that a solution SHOULD first satisfy requirements documented in [VPN-REQ] : as much as possible, multicast service should have the same flavor as the unicast one, including same simplicity (technology unaware), the same quality of service (if any), the same management (e.g. monitoring of performances), etc.

Moreover, it is also obvious that a multicast VPN solution MUST interoperate seamlessly with current unicast solutions. Even if this is not a core requirement, it would also make sense that multicast VPN solutions define themselves as extensions to existing provider provided IP VPN solutions (such as for instance, [RFC2547bis] or [VR]) and privilege consistency with those.

Finally, this document identifies multicast specific issues - most notably from the service provider standpoint - and thus expresses additional requirements specific to multicast.

1.3. Scalability vs. optimality

An issue has been identified as intrinsic to the transport of multicast VPN traffic over a service provider network, whatever the technical solution chosen: in the general case, there is a tension between resource optimization and number of state maintained. Thus, some trade-off has to be made, and this document will express some requirements related to this trade-off.
2. Operational implementation examples

This section aims at presenting a few representative examples of multicast applications in a VPN context. The goal is to highlight
how different applications and network context may have a different
impact on how a trade-off is made.

[to be completed]

3. Requirements for supporting IP multicast within IP PP VPNs

Again, the aim of this draft is not to specify solutions but to give
requirements for supporting IP multicast within IP PP VPNs.

In order to list these requirements we have taken two different
standpoints of two different important entities: the end user (the
customer using the VPN) and the service provider.

In the rest of the document, we mean by a "solution", a solution that
allows to perform multicast into a provider provisioned IP VPN.

3.1. End user/customer standpoint

3.1.1. Service definition

As for unicast, the multicast service should be provider provisioned
and shall not need some extra features on the customer equipments
(CE).

3.1.2. CE-PE routing protocols

Between the CEs and the PEs the multicast protocols that SHOULD be
implemented in the solution are PIM-SM [PIM-SM] (including PIM-SSM
[PIM-SSM], and bidirectional PIM [BIDIR-PIM]), and IGMP (v1, v2 and
v3 [IGMPv1] [IGMPv2] [IGMPv3]).

3.1.3. Quality of Service (QoS)

First, general considerations about QoS in L3VPNs as developed in
section 5.5 of [VPN-REQ] are also relevant to this section.

The QoS includes various parameters such as delay, jitter, packet
loss, and service availability expressed in percentage of time.
These parameters are defined in the unicast current provider provided
VPN services, are sold by the service provider to the customers and
defined in the SLA (Service Level Agreements).
The level of availability of multicast traffic should be on par with what exists for unicast traffic. For instance traffic protection mechanisms SHOULD be available for customer multicast traffic when it is carried over the service provider network.

The multicast in the VPN solution shall allow to define at least the same level of quality of service. As multicast is often used to deliver high quality services such as video broadcast, the solution
should have additional features to support high QoS such as bandwidth reservation and call admission control.

Moreover, a multicast VPN solution should as much as possible ensure that client multicast traffic packets are not lost nor duplicated, even if the means used to carry a client multicast data stream over the provider network changes.

3.1.4. SLA parameters measurement

As SLA parameters are part of the sold service, they are often monitored. The monitoring is used for technical reasons by the service provider and is often sold to the customer for e2e service purposes.

The solution shall allow to monitor SLA parameters and may allow to use similar techniques (as those used by the unicast services) to monitor them.

Multicast specific characteristics that may be monitored are, for instance, multicast statistics per stream and latency time to receive a multicast group traffic across the VPN.

3.1.5. Data transmission security

Security is a key point for customer who uses a VPN solution. The RFC2547 model offers some guarantees concerning the security level of data transmission within the VPN.

The solution shall provide an architecture that has the same level of security both for the unicast and multicast traffic.

A VPN multicast solution may choose to make the optimality/scalability trade-off stated in section 1.3 by distributing multicast traffic of a client group to a set of PE routers that may include PEs which are not part of the VPN. From a security standpoint, this may be a problem for some VPN customers, thus a multicast VPN solution using such a scheme should offer ways to avoid this for specific customers (and/or specific customer multicast streams).

3.1.6. Monitoring and Troubleshooting

Apart from obvious statistics on multicast traffic, customers of a
multicast VPN will need information concerning the status of their multicast resource usage.

Indeed, as mentioned in section 3.2.3, for scalability purpose service provider may limit the number (and/or throughput) of multicast streams that are received and produced at a client site, and obviously customers will need to be able to know their current
resource usage (state and throughput) and will need to receive some kind of alert if rejects are happening.

3.1.7. Extranet

In current PP L3VPN models, a customer site may be setup to be part of multiple VPNs. The need for a corresponding multicast feature will need to be assessed in further revisions of this draft, but a multicast solution should at least specify how it handles multicast traffic of a such site.

3.1.8. Multi-homing, load balancing and resiliency

A multicast VPN solution should be compatible with current solutions aimed at improving the service robustness for customers such as multi-homing, CE-PE link load balancing and failover. A multicast VPN solution should also be able to offer those same features for multicast traffic.

3.1.9. Addressing

A multicast provider provided L3VPN should not impose restrictions on multicast group addresses used by VPN customers.

In particular, as for unicast traffic, overlap of multicast group address sets used by different customers MUST be supported.

3.2. Service provider standpoint

3.2.1. Scalability

Some currently standardized and deployed L3VPN solution have the major advantage of being scalable in the core regarding the number of customers and number of customer routes. For instance, in the [RFC2547bis] model, a P router sees a number of MPLS tunnels that is only linked to the number of PEs and not at all to the number of customers.

As far as possible, this independence in the core, with respect to the number of customers and to customer activity, is recommended. Yet, it is identified that in our context the scalability and resource usage optimality goals are competing, so this requirement may be reduced to having the possibility of bounding the quantity of states that the service provider needs to maintain in the core, the bound being independent of the multicast activity of VPN customers.
It is expected that multicast VPN solutions will use some kind of point to multipoint technology to efficiently carry VPN multicast traffic, and that such technologies require maintaining state information, and will use resources in the control plane (memory and processing, and possibly address space).
Scalability is a key requirement for multicast VPN solutions. Solutions MUST be designed to scale well with an increase in the number of any of the following:
- the number of PEs
- the number of customers VPNs (total and per PE)
- the number of PEs and sites in any VPN
- the number of client multicast channels (groups or source-groups)

Both scalability of performance and operation MUST be considered.

Key considerations SHOULD include:
- the processing resources needed on the control plan (neighborhood or session maintenance messages, keep-alives, timers, etc.)
- the memory resources needed for the control plane
- the amount of protocol information transmitted to manage a multicast VPN (message size)
- the amount of potential routing extensions
- the amount of control plane processing required on PE and P to add remove a customer site (or a customer from a multicast session)
- the number of multicast IP addresses used (if IP multicast distribution trees are used to carry customer multicast traffic)

It is expected that the applicability of each solution will be evaluated with regards to the aforementioned scalability criteria.

These considerations naturally lead us to believe that proposed solutions SHOULD offer the possibility of sharing such resources between different VPN multicast streams (between different VPNs, between different VPN multicast streams of the same or of different VPNs). This means, for instance, being able to share IP multicast trees between several customers.

Those scalability issues are expected to be more pregnant on P routers, but a multicast in VPNs solution should address both P and PE routers as far as scalability is concerned.

3.2.2. Resource optimization

3.2.2.1. General goals

One of the aims of the use of multicast instead of unicast is resource optimization in the network.
The two obvious things that a multicast VPN solution would want to avoid are useless duplication — when same data travels twice or more on a same link (e.g. when doing ingress PE replication) — and data sent uselessly (e.g. PE receiving traffic they don’t need).
3.2.2.2. Trade-off and tuning

But as previously stated in this document, a scalable resource optimal solution is probably not possible. Thus what is expected from a multicast VPN solution is that it addresses the resource optimization issue taking into account the fact that some trade-off has to be made.

Moreover, we think that a "one size fits all" trade-off probably does not exist either, and that the most sensible approach would be a versatile solution offering the providers appropriate configurable settings letting them tune the trade-off according to their peculiar constraints (network topology, platforms, customer applications, level of service offered etc.).

3.2.2.3. Traffic engineering

In addition, if traffic engineering features are provided by the connection mode that is used between PEs for unicast traffic in the VPN service, the solution SHOULD provide the same for multicast traffic.

The solution should offer mean to support key multicast TE objectives as defined in [RFC 3272].

3.2.3. Control mechanisms

The solution must provide some mechanisms to control the source emission within a VPN. This control includes the number of sources and/or the total bit rate of all the sources.

At the reception level, the solution must also provide mechanisms to control the number of channels (group or source/group) to which a VPN site has subscribed and/or the total bit rate.

All these mechanisms must be configurable by the service provider in order to control the amount of multicast traffic within a VPN.

Moreover it may be desirable to be able to impose some global bound on the quantity of state used by a VPN in the core network for its multicast traffic.

3.2.4. Infrastructure security
Concerning the infrastructure, the solution shall provide the same level of security for the service provider. For instance, that means that the intrinsic protection against DOS and DDOS attacks of the BGP/MPLS solution must be the same in the multicast solution.

Moreover, since multicast traffic and routing are intrinsically dynamic, some mechanism must be proposed so that the frequency of changes in the way client traffic is carried over the core is bounded.
and not tightly coupled to dynamic changes of multicast traffic in
the customer network.

Last, control mechanisms described in previous section are also to be
considered from this infrastructure security point of view.

3.2.5. Robustness

Resiliency is also crucial to infrastructure security, thus a
multicast VPN solution shall whether avoid single points of failures
or propose some technical solution making possible to implement a
failover mechanism.

3.2.6. Management tools, OAM

The operation of a multicast VPN solution shall be as light as
possible and automatic configuration and discovery should be
privileged. Particularly the operational cost of setting up
multicast on a PE should be as low as possible.

Moreover, monitoring of multicast specific parameters and statistics
should be offered to the service provider.

Most notably the provider should have access to:
- multicast traffic statistics
- information about client multicast resource usage (state and
  throughput)
- alarms when limits are reached on such resources
- statistics on decisions related to how client traffic is carried
  on transport trees (e.g. traffic switched onto a stream specific
  multicast tree)
- statistics on parameters that could help the provider to
evaluate its optimality/state trade-off

3.2.7. Trouble shooting

A multicast VPN solution that would dynamically adapt the way some
client multicast traffic is carried over the provider network may
incur the disadvantage of being hard to troubleshoot.

In such a case, to help diagnose multicast network issues a multicast
VPN solution should provide monitoring information describing how
client traffic is carried over the network (e.g. which provider
multicast group is used for such and such client multicast stream).
Moreover a solution may also provide configuration options to avoid
any dynamic changes, for multicast traffic of a particular VPN or a
specific multicast stream (client group or source-group).

3.2.8. Inter-AS, inter provider
A multicast VPN solution shall support inter area, inter-AS and inter provider multicast VPNs. Options A, B and C (as described in section 10 of [RFC2547bis]) SHOULD be supported.

Moreover such support should be possible without compromising other requirements of this draft, and should not incur penalty on scalability and bandwidth resource usage.

3.2.9. Tunneling Requirements

Connectivity between PE devices in the backbone SHOULD be able to use a range of tunneling technologies, including point-to-point and point-to-multipoint, such as L2TP [L2TP-MCAST], IPSEC [IPSEC], GRE [GRE], IP-in-IP, MPLS [P2MP], etc.

In a multicast VPN solution extending a unicast IP PP VPN solution, consistency in the tunneling technology has to be privileged: such a solution SHOULD allow the use of the same tunneling technology for multicast as for unicast.

3.2.10. Architecture consideration

As far as possible, the solution shall minimize the number of protocols that have to be activated within the core network, i.e. in the P and PE routers.

It is desirable to maximize the re-use of existing L3 VPN techniques and protocols. For instance, the same routing protocol (or an extension) shall be used both for unicast and multicast solution.

Moreover, introducing new protocol specific to this issue should be avoided when possible (on both PE and P routers), and extensions to existing protocols should be preferred when relevant.

The motivations behind those requirements are good interworking and troubleshooting.

3.2.11. Compatibility

First, it is a requirement that unicast and multicast services MUST be able to co-exist within the same VPN.

A multicast VPN solution SHOULD prevent compatibility and migration issues, for instance by privileging mechanisms facilitating forward
compatibility. Most notably a solution supporting only a subset of those requirements SHOULD be designed to be compatible with future enhanced revisions.

It SHOULD be an aim of any multicast into VPN solution to offer as much backward compatibility as possible. An ideal which is probably impossible to achieve would be to offer multicast VPN services across legacy routers without any change to any router in the network.
4. Security Considerations

This document does not by itself raise particular security issues.

5. Acknowledgments

The authors would like to thank Vincent Parfait (Equant), Elodie Hemon Larreur and Sebastien Loye (France Telecom) and for their review and suggestion of an earlier draft of this document.

The authors would also like to thank Zubair Ahmad (Equant) for his valuable input.

6. References

6.1. Normative references


[VPN-REQ] M. Carugi, et. al., "Service requirements for Layer 3 PPVPNs", draft-ietf-l3vpn-requirements-02 (work in progress)


[IGMPv1] S. Deering, "Host extensions for IP multicasting", RFC 1112

[IGMPv2] W. Fenner, "Internet Group Management Protocol, IGMP


6.2. Informative references

7. Author’s Addresses

Thomas Morin
France Telecom R & D
2, avenue Pierre-Marzin
22307 Lannion Cedex
France
Email: thomas.morin@francetelecom.com

Renaud Moignard
France Telecom R & D
2, avenue Pierre-Marzin
22307 Lannion Cedex
France
Email: renaud.moignard@francetelecom.com

Jean-Louis Le Roux
8. Intellectual Property Notice

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

8.1. IPR Disclosure Acknowledgement

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

Full Copyright Statement

"Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be
followed, or as required to translate it into languages other than English.
The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.