OSPF as the PE/CE Protocol in BGP/MPLS VPNs

draft-rosen-vpns-ospf-bgp-mpls-06.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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

[VPN] describes a method of providing a VPN service. That method allows a variety of different protocols to be used as the routing protocol between the Customer Edge (CE) router and the Provider Edge (PE) router. However, it does not fully specify the procedures which must be implemented within the Provider’s network when OSPF is used as the PE/CE routing protocol. This document provides that specification.
1. Specification of Requirements

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

2. Introduction

[VPN] describes a method by which a Service Provider (SP) can use its IP backbone to provide a VPN service to customers. In that method, a customer's edge devices (CE devices) are connected to the provider's edge routers (PE routers). If the CE device is a router, then the PE router may become a routing peer of the CE router (in some routing protocol), and may as a result learn the routes which lead to the CE's site and which need to be distributed to other PE routers that attach to the same VPN.

The PE routers which attach to a common VPN use BGP to distribute the VPN's routes to each other. A CE router can then learn the routes to
other sites in the VPN by peering with its attached PE router in a routing protocol. CE routers at different sites do not, however, peer with each other.

It can be expected that many VPNs will use OSPF as their internal routing protocol. This does not necessarily mean that the PE routers need to use OSPF to peer with the CE routers. Each site in a VPN can use OSPF as its intra-site routing protocol, while using, e.g., BGP or RIP to distribute routes to a PE router. However, it is certainly convenient, when OSPF is being used intra-site, to use it on the PE-CE link as well, and [VPN] explicitly allows this.

Like anything else, the use of OSPF on the PE-CE link has advantages and disadvantages. The disadvantage to using OSPF on the PE-CE link is that it gets the PE router involved in a VPN site’s IGP, however peripherally. The advantages though are:

- The administrators of the CE router need not have any expertise in any routing protocol other than OSPF.
- The CE routers do not need to have support for any routing protocols other than OSPF.
- If a customer is transitioning his network from a traditional OSPF backbone to the VPN service described in [VPN], the use of OSPF on the PE-CE link eases the transitional issues.

It seems likely that some SPs and their customers will resolve these trade-offs in favor of the use of OSPF on the PE-CE link. Thus we need to specify the procedures which must be implemented by a PE router in order to make this possible. (No special procedures are needed in the CE router though; CE routers just run whatever OSPF implementations they may have.)

3. Requirements

Consider a set of VPN sites which are thought of as a common "OSPF domain". These will almost certainly be a set of sites which together constitute an "intranet", and each of which runs OSPF as its intra-site routing protocol.

Per [VPN], the VPN routes are distributed among the PE routers by BGP. If the PE uses OSPF to distribute routes to the CE router, the standard procedures governing BGP/OSPF interactions [OSPF] would cause routes from one site to be delivered to another as AS-external routes (in type 5 LSAs). This is undesirable; it would be much better to deliver such routes in type 3 LSAs (as inter-area routes),
so that they can be distinguished from any "real" AS-external routes that may be circulating in the VPN. (That is, so that they can be distinguished by OSPF from routes which really do not come from within the VPN.) Hence it is necessary for the PE routers to implement a modified version of the BGP/OSPF interaction procedures.

In fact, we would like to have a very general set of procedures which allows a customer to easily replace a legacy private OSPF backbone with the VPN service. We would like this procedure to meet the following set of requirements:

- The procedures should not make assumptions about the OSPF topology. In particular, it should not be assumed that customer sites are OSPF stub sites or NSSA sites. Nor should it be assumed that a customer site contains only one OSPF area, or that it has no area 0 routers.

However, in this document we do assume that any link between a PE router and a CE router is NOT an area 0 link. Optional procedures for handling the case where a PE-CE link is an area 0 link will be specified in a separate document.

- If VPN sites A and B are in the same OSPF domain, then routes from one should be presented to the other as OSPF intra-network routes. In general, this can be done by presenting such routes as inter-area routes, in type 3 LSAs.

Note that this allows two VPN sites to be connected via an "OSPF backdoor link". That is, one can have an OSPF link between the two sites which is used only when the VPN backbone is unavailable. (This would not be possible with the ordinary BGP/OSPF interaction procedures. The ordinary procedures would present routes via the VPN backbone as AS-external routes, and these could never be preferred to intra-network routes.) This may be very useful during a period of transition from a legacy OSPF backbone to a VPN backbone.

- It should be possible to make use of an "OSPF backdoor link" between two sites, even if the two sites are in the same OSPF area, and neither of the routers attached to the inter-site backdoor link is an area 0 router. This can also be very useful during a transition period, and eliminates any need to reconfigure the sites’ routers to be ABRs.

Assuming that it is desired to have the route via the VPN backbone be preferred to the backdoor route, the VPN backbone itself must be presented to the CE routers at each site as a link between the two PE routers to which the CE routers are
respectively attached.

- The transition from the legacy private OSPF backbone to the VPN service must be simple and straightforward. The transition is likely to be phased, such that customer sites are migrated one by one from the legacy private OSPF backbone to the VPN service. During the transition, any given site might be connected to the VPN service, to the legacy OSPF backbone, or to both. Complete connectivity among all such sites must be maintained.

Since the VPN service is to replace the legacy backbone, it must be possible, by suitable adjustment of the OSPF metrics, to make OSPF prefer routes which traverse the SP’s VPN backbone to alternative routes which do not.

- The OSPF metric assigned to a given route should be carried transparently over the VPN backbone.

Routes from sites which are not in the same OSPF domain will appear as AS-external routes.

We presuppose familiarity with the contents of [OSPF], including the OSPF LSA types, and will refer without further exegesis to type 1, 2, 3, etc., LSAs. Familiarity with [VPN] is also presupposed.

4. BGP/OSPF Interaction Procedures for PE routers

4.1. Overview

[VPN] defines the notion of a Per-Site Routing and Forwarding Table, or VRF. A PE router must be capable of running multiple instances of OSPF, where each instance is associated with a particular VRF. (Whether these instances are realized as separate processes, or merely as separate contexts of a common process, is an implementation matter.)

BGP is used to distribute routes among the set of PE routers that attach to a single OSPF domain. Per [VPN], these routes are distributed as VPN-IP routes. Import/export to/from particular VRFs is governed via Route Targets. To meet the above requirements, a PE which imports a particular route into a particular VRF needs to know whether that route comes from the same OSPF domain and the same OSPF area as the CEs to which it is attached. Our procedure is to encode this information as BGP Extended Communities attributes [EXT], and have BGP distribute it along with the VPN-IP route. The OSPF metric of a route is also carried as a BGP attribute of the route.
If two PEs attach to different VPN sites that are in the same OSPF area (as indicated by the OSPF area number), the PE/CE links to those site MAY be treated as links within that area. In addition, each PE MAY flood, into that area, a type 1 LSA advertising a link to the other PE. If this procedure is followed, two VPN sites in the same OSPF area will see the VPN backbone as a link within that area, a link between the two PE routers. We refer to this link as a "sham link". This allows routes from one site to the other to be treated as intra-area routes. The procedures governing the use of sham links are specified in Section 4.2.3.

Every PE attached to a particular OSPF network MUST be an OSPF area 0 router. This allows it to distribute inter-area routes to the CE via Type 3 LSAs. In this document, we assume that the PE-CE link is NOT an area 0 link; optional procedures which allow the PE-CE link to be an area 0 link will be specified in a separate document.

When a PE router needs to distribute to a CE router a route which comes from a site outside the latter’s OSPF domain, the PE router presents itself as an ASBR, and distributes the route in a type 5 LSA. OSPF route tagging is used to ensure that a type 5 LSA generated by a PE router will be ignored by any other PE router that may receive it. A special OSPF route tag, which we will call the VPN Route Tag (see section 4.2.1), will be used for this purpose.

4.2. Details

4.2.1. General

If a PE and a CE are communicating via OSPF, the PE MUST create, and MUST flood to the CE, a type 1 LSA advertising its link to the CE. The PE MUST have an OSPF router id which is valid (i.e., unique) within the OSPF domain. The PE MUST also be configured to know which OSPF area the link is in. The case in which the PE-CE link is in area 0 is not covered in this document.

The PE MUST function as an OSPF area 0 router. That is, the link state topology from a site will NOT be passed along by the PE.

The PE MUST support at least one OSPF instance for each OSPF domain to which it attaches. Each instance of OSPF MUST be associated with a single VRF. If n CEs associated with that VRF are running OSPF on their respective PE/CE links, then those n CEs are OSPF adjacencies of the PE in the corresponding instance of OSPF. Generally, though not necessarily, if the PE attaches to several CEs in the same OSPF domain, it will associate the interfaces to those PEs with a single VRF.
Each OSPF domain MUST be associated with a Domain Identifier. This MUST be configurable, and the default value (if none is configured) SHOULD be NULL. More precisely, each VRF associated with an OSPF instance will either be configured with one or more Domain Identifiers, or else will use NULL as its Domain Identifier.

A VRF MAY be configured with several Domain Identifier values. In this case, one of these is considered to be the "primary" Domain Identifier; this MUST be determinable by configuration. If a VRF has exactly one Domain Identifier configured, this is of course its primary Domain Identifier. If a VRF is configured with more than one Domain Identifiers, the NULL Domain Identifier MUST NOT be one of them.

With respect to the set of VRFs in a given OSPF domain, one of the following two conditions MUST hold:

1. They all have the NULL Domain Identifier, OR
2. Each VRF is configured with a set of Domain Identifiers, and in this set is the primary Domain Identifier of every other VRF in the domain.

A Domain Identifier is an eight-byte quantity which is a valid BGP Extended Communities attribute, as specified in section 4.2.2. If a particular VRF has a single non-NUL Domain Identifier, when routes from that VRF are distributed as by BGP as VPN-IPv4 routes, the routes MUST carry the corresponding Domain Identifier Extended Communities attribute. If the VRF has more than one Domain Identifier, the routes MUST carry the the Domain Identifier Extended Communities attribute corresponding to the VRF’s primary Domain Identifier. If the VRF’s Domain Identifier is NULL, the Domain Identifier Extended Communities attribute MAY be omitted when routes from that VRF are distributed; alternatively, a value of the Domain Identifier Extended Communities attribute which represents NULL (see section 4.2.2) MAY be carried with the route.

If a particular OSPF domain has the NULL Domain Identifier, care must be taken to avoid having routes from that OSPF domain and routes from another OSPF domain imported into the same VRF.

If a particular VRF in a PE is associated with an instance of OSPF, then it will be configured with a special OSPF route tag value, which we call the VPN Route Tag. This route tag MUST be included in the Type 5 LSAs which the PE originates (as the result of receiving a BGP-distributed VPN-IP route, see section 4.2.4) and sends to any of the attached CEIs. Its value is arbitrary, but must be distinct from any OSPF Route Tag being used within the OSPF domain. Its value MUST
therefore be configurable. If the Autonomous System number is two bytes long, the default value SHOULD be an automatically computed tag based on the Autonomous System number of the VPN backbone:

\[
\text{Tag} = \langle \text{Automatic} = 1, \text{Complete} = 1, \text{PathLength} = 01 \rangle
\]

If the Autonomous System number is four bytes long, then a Route Tag value MUST be configured, and it MUST be distinct from any Route Tag used within the VPN itself.

If a PE router needs to use OSPF to distribute to a CE router a route which comes from a site outside the CE router’s OSPF domain, the PE router SHOULD present itself to the CE router as an Autonomous System Border Router (ASBR), and SHOULD report such routes as AS-external routes. That is, these PE routers originate Type 5 LSAs reporting the extra-domain routes as AS-external routes. Each such Type 5 LSA MUST contain an OSPF route tag whose value is that of the VPN Route Tag. This tag identifies the route as having come from a PE router. The VPN Route Tag MUST be used to ensure that a Type 5 LSA originated by a PE router is not redistributed through the OSPF area to another PE router.

4.2.2. Handling LSAs from the CE

This section specifies the way in which a PE router handles the OSPF LSAs it receives from a CE router.

If a Type 5 LSA is received from the CE, and if it does NOT have an OSPF route tag value equal to the VPN Route Tag (see section 4.2.1), it is processed normally, for the relevant instance of OSPF in the PE.

If a Type 5 LSA is received from the CE, and if it has an OSPF route tag value equal to the VPN Route Tag (see section 4.2.1), then the information from that LSA is not used by the SPF computation. (This will prevent the VRF from containing routes based on that...
information.) Otherwise the LSA is handled normally.

Next, the PE must examine the corresponding VRF. For every address prefix which appears there, the PE must create a VPN-IPv4 route in BGP. Each such route will have some of the following Extended Community attributes:

- **The OSPF Domain Identifier Extended Communities attribute.** This MUST be present, UNLESS the VRF has a NULL Domain Identifier, in which case it MAY be omitted. This attribute is encoded with a two-byte type field, and its type is either 0005, 0105, or 0205. For backwards compatibility, the type 8005 MAY be used as well, and is treated as if it were 0005. If the VRF has a NULL Domain Identifier, and the OSPF Domain Identifier Extended Communities attribute is NOT omitted, then the attribute’s value field must be all zeroes, and its type field may be any of 0005, 0105, 0205, or 8005.

- **OSPF Route Type Extended Communities Attribute.** This attribute MUST be present. It is encoded with a two-byte type field, and its type is 0306. The type 8000 SHOULD be accepted as well, to ensure backwards compatibility. The remaining six bytes of the Attribute are encoded as follows:

  * **Area Number:** 4 bytes, encoding a 32-bit area number. For AS-external routes, the value is 0. A non-zero value identifies the route as being internal to the OSPF domain, and as being within the identified area. Area numbers are relative to a particular OSPF domain.

  * **OSPF Route Type:** 1 byte, encoded as follows:

    **1 or 2** for intra-area routes (depending on whether the route came from a type 1 or a type 2 LSA -- however this difference is not significant to the procedures specified herein)

    **3** for summary routes

    **5** for external routes (area number must be 0)

    **7** for NSSA routes.

    **129** for Sham Link Endpoint Addresses. See section 4.2.3.2 for the specification of when this value must be used.
* Options: 1 byte. Currently this is only used if the route
type is 5 or 7. Setting the least significant bit in the
field indicates that the route carries a type 2 metric.

- OSPF Router Id Extended Communities Attribute. This OPTIONAL
attribute specifies the OSPF Router Id of the system that is
identified in the BGP Next Hop attribute. More precisely, it
specifies the Router Id of the particular VRF from which this
route was exported. This attribute is encoded with a two-byte
type field, and its type is 0107, with the router id itself
carried in the first 4 bytes of the value field. The type 8001
SHOULD be accepted as well, to ensure backwards compatibility,
and should be treated as if it were 0107.

- MED. By default, this SHOULD be set to the value of the OSPF
distance associated with the route, plus 1.

The intention of all this is the following. OSPF Routes from one site
are converted to BGP, distributed across the VPN backbone, and
possibly converted back to OSPF routes before being distributed into
another site. With these attributes, BGP carries enough information
about the route to enable the route to be converted back into OSPF
"transparently", just as if BGP had not been involved.

Routes which a PE receives in type 4 LSAs MUST be ignored.

The attributes specified above are in addition to any other
attributes which routes must carry in accord with the [VPN].

The Site of Origin attribute, which is usually required by [VPN], is
OPTIONAL for routes which a PE learns from a CE via OSPF.

Use of the Site of Origin attribute would, in the case of a multiply
homed site (i.e., a site attached to several PE routers), prevent an
intra-site route from being reinjected into a site from the VPN
backbone. Such a reinjection would not harm the routing, because the
route via the VPN backbone would be advertised in a type 3 LSA, and
hence would appear to be an inter-area route; the real intra-area
route would be preferred. But unnecessary overhead would be
introduced. On the other hand, if the Site of Origin attribute is not
used, a partitioned site will find itself automatically repaired,
since traffic from one partition to the other will automatically
travel via the VPN backbone. Therefore the use of a Site of Origin
attribute is optional, so that a trade-off can be made between the
cost of the increased overhead and the value of automatic partition
repair.
4.2.3. Sham Links

4.2.3.1. Intra-Area Routes

Suppose there are two sites in the same OSPF area. Each site is attached to a different PE router, and there is also an intra-area OSPF link connecting the two sites.

It is possible to treat these two sites as a single VPN site which just happens to be multihomed to the backbone. This is in fact the simplest thing to do, and is perfectly adequate, providing that the preferred route between the two sites is via the intra-area OSPF link (a "backdoor link"), rather than via the VPN backbone. There will be routes between sites that go through the PE routers, but these routes will appear to be inter-area routes, and OSPF will consider them to be less preferable than the intra-area routes through the backdoor link.

If it is desired to have OSPF prefer the routes through the backbone over the routes through the backdoor link, then the routes through the backbone must be appear to be intra-area routes. To make a route through the backbone appear to be an intra-area route, it is necessary to make it appear as if there is an intra-area link connecting the two PE routers. This is what we refer to as a "sham link". (If the two sites attach to the same PE router, this of course is not necessary.)

A sham link can be thought of as a relation between two VRFs. If two VRFs are to be connected by a sham link, each VRF must be associated with a "Sham Link Endpoint Address", a /32 address which is treated as an address of the PE router containing that VRF. The Sham Link Endpoint Address associated with a VRF MUST be configurable, and it MAY default to the VRF’s router id. The Sham Link Endpoint Address is an address in the VPN’s address space, not the SP’s address space.

A VRF needs only a single Sham Link Endpoint Address, no matter how many sham links it has. It MUST be distributed by BGP as a VPN-IPv4 address, and it MAY be distributed by OSPF.

4.2.3.2. Creating Sham Links

Sham links may be manually configured, or they may be auto-configured.

Each VRF that is associated with a PE-CE link on which OSPF is running MUST be configurable as to whether auto-configuration of sham links to/from that VRF is allowed. The default MUST be "manual"
configuration".

If a VRF is configured for manual configuration of the sham links, it will never initiate auto-configuration of a sham link, nor will it ever create a sham link as the result of a remotely initiated auto-configuration procedure. If a VRF is configured for auto-configuration of sham links, manual configuration of particular sham links is still allowed. In any event, no more than one sham link with the same pair of sham link endpoint addresses will ever be created.

To manually configure a sham link between two VRFs, each VRF has to be configured to create a sham link to the other, where the "other" is identified by its sham link endpoint address. Procedures for single-ended manual configuration of the sham link are for further study.

If a VRF is configured for auto-configuration of sham links, it MUST distribute, via BGP, a VPN-IP route corresponding to the Sham Link Endpoint Address. This route MUST have the OSPF Route Type Extended Community attribute, with the OSPF Route Type field set to "Sham Link Endpoint Address".

When a PE receives such a route, with a RT value that allows the route to be imported into a particular VRF, then if

- that route has an OSPF Domain Identifier Extended Communities attribute which is identical to one of the VRF’s Domain Identifiers, or the route has no OSPF Domain Identifier Extended Communities attribute and the VRF has a NULL Domain Identifier, and

- that route has an OSPF area number which matches that of the VRF,

then a sham link may be created from the local VRF to the VRF identified by the sham link endpoint address.

When comparing two OSPF Domain Identifier Extended Communities attributes for equality, all eight bytes of the Extended Communities attribute must be compared. The two attributes are regarded as equal only if they are identical in all eight bytes, or if the lower order six bytes are identical, and one attribute has two high order bytes of 0005 and the other has two high order bytes of 8005.

If all VRFs are configured for auto-configuration of sham links, a full mesh of sham links will be created among all the sites which are in the same OSPF area. This may not be what is desired. To obtain more control over the set of sham links which are created, some of
all of the VRFs can be configured to disable auto-configuration of the sham links.

Note that sham links may be created for any area.

4.2.3.3. Treatment of Sham Links

Sham links SHOULD be treated by OSPF as OSPF Demand Circuits. This means that LSAs will be flooded over them, but periodic refresh traffic is avoided. Note that, as long as the backdoor link is up, flooding the LSAs over the sham link serves no purpose. However, if the backdoor link goes down, OSPF does not have mechanisms enabling the routers in one site to rapidly flush the LSAs from the other site. Therefore it is still necessary to maintain synchronization among the LSA databases at the two sites, hence the flooding over the sham link.

The sham link is an unnumbered point-to-point intra-area link, and is advertised by means of a type 1 LSA.

The OSPF metric associated with a sham link must be configurable (and there must be a configurable default). Whether traffic between the sites flows via a backdoor link or via the VPN backbone (i.e., via the sham link) depends on the settings of the OSPF link metrics. The metrics can be set so that the backdoor link is not used unless connectivity via the VPN backbone fails, for example.

The default Hello Interval for sham links is 10 seconds, and the default Router Dead Interval for sham links is 40 seconds.

If a PE determines that a particular route traverses the sham link, then the PE SHOULD NOT redistribute that route into BGP as a VPN-IPv4 route.

4.2.4. VPN-IP routes received via BGP

This section describes how the PE router handles VPN-IP routes received via BGP.

If a received BGP VPN-IP route is not installed in the VRF, nothing is reported to the CE. A received route will not be installed into the VRF if some other route is preferable. (Note that a route which is not installed in the VRF may still cause the PE to create an OSPF link to another PE as specified in the previous section.)
Note that according to the usual OSPF route preference rules, intra-area routes, as computed by the OSPF, will be installed in the VRF in preference to any other routes received over BGP. This means that the CE will simply not hear about inter-area or external routes to address prefixes for which there is an intra-area route.

In the following, we specify what is reported, in OSPF LSAs, by the PE to the CE, assuming that the PE is not configured to do any further summarization or filtering of the routing information before reporting it to the CE.

4.2.4.1. Routes from Different Domains

To determine how to process an a received VPN-IP route, it is necessary to compare the OSPF Domain Identifier Extended Communities attribute carried by the route (if any) with the OSPF Domain Identifier Extended Communities attribute(s) with which the VRF has been configured (if any). In general, when two such attributes are compared, all eight bytes must be compared. Thus two OSPF Domain Identifier Extended Communities attributes are regarded as equal if and only if one of the following three conditions holds:

1. They are identical in all eight bytes.

2. They are identical in their lower order six bytes (value field), but one attribute has two high order bytes (type field) of 0005 and the other has two high order bytes (type field) of 8005. (This condition is for backwards compatibility.)

3. The lower order six bytes (value field) of both attributes consist entirely of zeroes. In this case, the two attributes are considered to be identical irrespective of their type fields, and they are regarded as representing the NULL Domain Identifier.

If one of the following three conditions holds, a VPN-IP route received via BGP is regarded as being from a different domain than the VRF into which the route is being installed.

1. The VRF has a non-NULL OSPF Domain Identifier, but either

   a) the route has no OSPF Domain Identifier Extended Communities attribute, or
b) the route has an OSPF Domain Identifier Extended Communities attribute whose value field consists of all zeroes

2. the route has an OSPF Domain Identifier Extended Communities attribute whose value field does not consist of all zeroes, and the VRF is configured with the NULL Domain Identifier (or with any encoding of the NULL Domain Identifier as specified above)

3. the router has an OSPF Domain Identifier Extended Communities attribute which is not identical to any of the OSPF Domain Identifiers associated with the VRF.

If any of these three conditions holds, the route is distributed to the CE in a type 5 LSA. The VPN Route Tag (see section 4.2.1) MUST be placed in the LSA. By default, a type 2 metric value is included in the LSA, and by default, its value is taken from the MED attribute of the VPN-IP route. If the MED is not present, a default metric value is used.

4.2.4.2. Other External Routes

If the route has an OSPF route type of external route, it MUST be advertised to the CE in a type 5 LSA. The VPN Route Tag (see section 4.2.1) MUST be placed in the LSA. By default, the MED, if present, is converted to a type 1 or type 2 metric, as determined by the external route property of the VPN-IPv4 route. If no MED is present, a default type 2 metric value is used.

Note that this way of handling AS-external routes makes every PE appear to be an ASBR attached to all the AS-external routes. In a multihomed site, this can result in a number of type 5 LSAs containing the same information.

4.2.4.3. Summary Routes

If the conditions of the previous two sections do not hold, then the route should be treated as if it had been received in an OSPF type 3 LSA. This means that the PE will report the route in a type 3 LSA to the CE. (Note that this case is possible even if the VPN-IP route carries an area number identical to that of the CE router. This means that if an area is "partitioned" such that the two pieces are connected only via the VPN backbone, it appears to be two areas, with inter-area routes between them.)
5. Acknowledgments

Significant contributions to this work have been made by Derek Yeung and Yakov Rekhter.

Thanks to Ross Callon and Ajay Singhal for their comments.

6. Authors’ Address

Eric C. Rosen
Cisco Systems, Inc.
250 Apollo Drive
Chelmsford, MA, 01824

E-mail: erosen@cisco.com

Peter Psenak
Parc Pegasus,
De Kleetlaan 6A
1831 Diegem
Belgium

E-mail: ppsenak@cisco.com

Padma Pillay-Esnault
Juniper Networks
1194 N. Mathilda Avenue
Sunnyvale, CA 94089

E-mail: padma@juniper.net

7. Normative References


[VPN] "BGP/MPLS VPNs", draft-ietf-ppvpn-rfc2547bis-03.txt, Rosen, E., et. al., October, 2002

Rosen, et al. [Page 16]