Network Working Group
Internet Draft
Category: Informational

Expires: March 17, 2011

S. Yasukawa
NTT
A. Farrel
Old Dog Consulting

September 17, 2010

PCC-PCE Communication Requirements for VPNs

draft-ietf-pce-vpn-req-02.txt

Abstract

The Path Computation Element (PCE) provides path computation functions in support of traffic engineering in Multiprotocol Label Switching (MPLS) and Generalized MPLS (GMPLS) networks.

An important application of MPLS and GMPLS networks is Virtual Private Networks (VPNs) that may be constructed using Label Switched Paths (LSPs) in the MPLS and GMPLS networks as VPN tunnels. PCE may be applied as a tool to compute the paths of such tunnels in order to achieve better use of the network resources and to provide better levels of service to the VPN customers.

Generic requirements for a communication protocol between Path Computation Clients (PCCs) and PCEs are presented in "Path Computation Element (PCE) Communication Protocol Generic Requirements". This document complements the generic requirements and presents a detailed set of PCC-PCE communication protocol requirements that are specific to the application of PCE to VPNs.

Contents

1. Introduction

The Virtual Private Network (VPN) is an important service offered by network providers to their customers. A lot of different VPN technologies such as IP-VPN and VPLS [RFC2764], [RFC4761], [RFC4762] have been developed and are deployed into many service providers' networks to enhance their service capabilities. VPN technologies have also has been extended to support multicast services [RFC4834] and layer 1 servics [RFC4847].

Multiprotocol Label Switching (MPLS) [RFC3031] and Generalized MPLS (GMPLS) [RFC3945] are often used to provide VPN solutions within provider core networks because Label Switched Paths (LSPs) provide traffic trunks that can be used to connect customers' VPN sites. These LSPs can be traffic engineered to help meet service level agreements (SLAs) and to enhance the manageability of providers' networks.

To meet customer demands and to realize competitive VPN network infrastructures, one promising possibility for service providers (SPs) is to deploy a common IP/MPLS network infrastructure for several VPN services. To realize this, the core network operator faces the following challenges.

- The SP must accommodate multiple VPN services which might have different network policies within a common IP/MPLS core network. This may require sophisticated traffic engineering (TE) mechanisms for the TE-LSPs that support more than one VPN.

- The SP must introduce automatic VPN establishment/addition/deletion mechanisms on top of an IP/MPLS core network to reduce their Operational Expenditure (OPEX). This requires some automatic path calculation and setup mechanisms during the VPN establishment/ addition/deletion processes.

- The SP must introduce VPN interworking functions that enable interworking between multiple domains of the same VPN service (e.g., Inter-AS operation), and interworking between multiple VPN service networks.

Designing TE-LSPs is a key technical component to meet these challenges. The Path Computation Element (PCE) defined in [RFC4655] is an entity that is capable of computing network paths and routes based on a network graph, and applying computational constraints. PCE is applicable of computating traffic engineered paths for MPLS and GMPLS LSPs, and so it is natural to seek to apply the same technology to support VPNs.

In the PCE architecture, the Path Computation Element Communication Protocol (PCECP) is used to exchange path computation requests and responses between Path Computation Clients (PCCs) and PCEs, and also between PCEs. Generic requirements for PCECP are presented in [RFC4657]. PCECP is described in [RFC5440].

This document presents a set of requirements for the Path Computation Element Communication Protocol (PCECP) when PCE is used in support of VPNs.

Specific requirements for PCECP in support of point-to-multipoint path computation such as might be used in support of multicast VPNs are described in [RFC5862].

2. Terminology

2.1. Conventions used in this document

For clarity of 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 [RFC2119].

2.2. Specific Terminology

PCE terminology is defined in [RFC4655].

Applicable MPLS terminology may be found in [RFC3031] and [RFC2702].

GMPLS terminology is defined in [RFC3945]

VPN terminology can be found in [RFC4026] with additional terms in [RFC4834] and [RFC4847].

The reader is assumed to be familiar with this terminology.

3. Core Network Requirements in Support of VPNs

This section is not intended to describe the function of VPNs, nor to provide a full description of how core networks support VPNs. Its purpose is to enumerate the principal features and functions that are used to support VPNs within a core network and with which PCE might be able to assist. This material is only present to give context to Section 4 that lists the specific PCECP requirements in support of VPNs.

3.1. VPN-Specific Behavior

3.1.1. Per-VPN Policy

A core network may apply different policies to the VPN connections established on behalf of different VPNs. Some policy decisions may be made at the time of path computation and could, therefore, be implemented through PCE provided that PCE has access to the correct policy information (perhaps through a policy server [RFC5394]), and is aware of the associated VPN ID.

3.1.2. Per-VPN Constraints and Algorithms

It is conceivable that different path computation behavior might be applied for the VPN connections belonging to different VPNs. This might, for example, reflect the different SLAs made for the different VPN services/customers. PCE can implement such differences in computational characteristics through specific requests or by being configured to provide different default behaviors according to the VPN ID.

3.1.3. Per-VPN Resources

In order to make it simpler to guarantee service levels core network resources may be assigned as reserved for use in support of a specific VPN or to be shared amongst only a subset of the total number of VPNs. This division of resources has an obvious impact on path computation and, provided the information can be made available to PCE in its traffic engineering database (TED) and that the VPN ID is supplied along with the path computation request, PCE can provide a path that conforms to the per-VPN resource allocation configuration.

3.1.4. LSP Protection Schemes and Resource Sharing

The SLA negotiated between network provider and VPN customer will dictate the level of LSP protection required within the network. A PCE can be used to compute protected (i.e., resource disjoint) paths.

Some protection schemes (1:n, extra traffic, etc.) allow resources used for protection paths to be shared. It may be a condition of the SLA that protection resources used to support one VPN are not shared outside that VPN, or are shared only with a subset of other VPNs. This might be a condition imposed for security or to improve protection guarantees. PCE can compute protection paths limited to a subset of the network resources. Full support of this function would, however, either require that PCE keep track of the VPNs that use shareable resources by updating its TED, or that PCE is fully stateful.

3.2. Customer Control of The Core Network

The customer network may wish to exert some control over the path of the VPN connection in the core network using techniques such as those in [RFC4206] and [RFC4208]. Such control may be expressed as inclusion constraints to the computation of the path of the VPN connection LSP, and PCE can compute paths with such constraints.

3.3. Private Address Spaces

VPNs may operate private address spaces. This has only two consequences for the core network.

- In order that a PE-to-PE LSP can be set up across the core network it is necessary to convert the tuple {VPN ID, destination CE address} to the target destination PE address. and this may require access to "reachablity information". That is, it may be necessary to know through which PEs a given CE can be reached in order to perform this mapping.

  Provided that the PCE is configured with or learns the appropriate mapping tables and knows the VPN ID, it can provide this translation as part of path computation. The target address would need to be flagged as a CE address and not as the destination of the core LSP.

- The customer network may exert some control over the path of the VPN connection in the core network as described in Section 3.2. In this case, the core addresses supplied by the customer network to the source PE in an explicit route may be expressed using the customer VPN's private address space. Again, the PCE is capable of providing the required translation as part of the path computation operation.

3.4. CE-CE Service Protection Schemes

The LSP protection described in Section 3.1.4 applies to PE-PE connections. It is also possible that the VPN will wish to operate CE-CE protection by forming separate CE-CE connections over the core network, usually by connecting each CE to more than one PE. Such CE-CE connections need to use disjoint paths within the core network, but unless the VPN exerts control over these paths (see Section 3.2) the responsibility for ensuring diversity is delegated to the core network. Since the CE-CE connections are established separately, the core network cannot compute a pair of mutually disjoint paths. Instead, the second path must be computed to avoid the resources of the first path. PCE can perform such a computation using the details of the first path as exclusions in the second computation.

3.5. Aggregation Schemes

Support of VPNs with very many access points may cause significant scaling issues for a core network. Similarly, the support of a large number of VPNs may cause problems.

Aggregation solutions may be applied to improve scaling within the core network, for example, by utilizing one PE-PE tunnel to carry the traffic for multiple VPNs.

These aggregation schemes require careful analysis of traffic loads to ensure that the VPNs each meet their service requirements and this may necesitate special computations based on aggregate demands. A PCE can perform such computations.

3.5.1. Sharing Core Tunnels

Where a pair of PEs both provide access to a set of VPNs, there is no requirement for multiple LSP tunnels across the core between the PEs. Traffic between the VPN sites can share a tunnel.

A stateful PCE that is requested to compute the path of a new PE-PE LSP might be able to indicate that an existing LSP would be suitable. This function, however, might be more appropriately implemented in a descint "VPN Manager" component.

3.5.2. Handling Core Scalability

Core network scalability may become an issue when mesh connectivity is required between very many PEs since this may result in exceptionally many LSPs crossing the middle of the network. One mechanism to handle this is to build a mesh of hierarchical LSP tunnels within the core of the core network, and to use these to

provide forwarding adjacencies [RFC4206] or to operate a layered (client/server) network [RFC5212].

PCE can compute the paths of PE-PE LSPs that use these core tunnels as forwarding adjacencies. Alternatively, when a multi-layered approach is taken, PCE may be an ideal computation tool where inter-layer or separate layer TE visibility is available [PCE-INTER-LAYER].

3.6. Multicast Considerations

VPNs may be required to support multicast traffic [RFC4834]. Various solutions have been proposed including some that use traffic engineered MPLS LSPs within the core network.

3.6.1. Unicast or Multicast LSPs

VPN connectivity for multicast VPNs may be provided by unicast or multicast LSPs. Data sourced through a CE and passed to a PE must be distributed across the network and delivered through multiple PEs to many CEs that participate in the same VPN. There are three models as follows.

a. PE Replication.

In this model multicast traffic is replicated by the ingress PE and distributed on unicast (point-to-point) LSPs to the egress PEs. The egress PEs may, themselves, be responsible for further replication if there are multiple attached CEs.

This model does not place any different requirements on the traffic engineering model from unicast VPNs, and a PCE can be used to compute the paths of the PE-PE TE-LSPs.

b. Rendezvous Point Replication

Replication can be placed within the network through the use of a rendezvous point. A unicast LSP carries data from the ingress PE to the rendezvous point where it is replicated and distributed to egress PEs along other unicast LSPs.

Rendezvous points may also be used to support multicast VPNs with multiple data sources. Further, a hierarchy of such points of replication could be constructed to achieve better network utilization.

Again, the point-to-point LSPs are no different from the TE-LSPs described before, and a PCE can be used to compute their paths. A

PCE might also be used to select an appropriate rendezvous point for a traffic flow in a VPN, and where a hierarchy of replication points is used, PCE could coordinate them so that no egress PCE receives duplicate data. These latter functions, however, are more suited to a VPN Manager component leaving PCE to perform path computation operations consistent with its specification in [RFC4655].

c. Multicast LSPs

Most efficient use of the core network can be made by establishing multicast LSPs, otherwise known as point-to-multipoint (P2MP) LSPs. These provide a distribution tree from the ingress PE to the egress PEs. Data replication happens within the forwarding plane at branch nodes (see Section 3.6.2).

It is possible to combine these three models in any mix. A PCE may be particularly helpful in identifying existing shareable LSPs that can determine what mixture of models to use.

3.6.2. P2MP Traffic Engineering

The computation of the routes for P2MP trees is non-trivial as suitable branch nodes must be located within the core network. The computation is made more complex by various factors including different replication capabilities of the core network nodes and different objective optimization criteria (such as least sum cost paths known as Steiner trees, and shortest paths to each destination).

The complexity of the P2MP computation makes it particularly suitable to offload to a dedicated PCE [RFC5862].

3.6.3. Aggregation onto P2MP LSPs

Aggregation of traffic from multicast VPNs onto core P2MP LSPs is more complicated than for unicast traffic. In the unicast case (see Section 3.5.1) it is possible for all traffic between a pair of PEs to share the same tunnel, but in the multicast case, sharing a tunnel requires that there is a common set of egress PEs or that receiving PEs can discard unwanted traffic. Various solutions to this problem are possible: each requires that the paths of P2MP LSPs are computed and that is something with which PCE can assist. But the fundamental problem of determining how many tunnels to use and how to multiplex traffic onto the tunnels is a function best performed by a distinct VPN Manager component.

3.7. VPN Establishment/Addition/Deletion

BGP-based auto-discovery mechanisms are widely deployed in VPNs for membership discovery. The auto-discovery mechanism is used not only to automatically detect VPN membership, but also to automatically establish PE-to-PE tunnels after detecting VPN membership. Combining this auto-discovery mechanism and the LSP establishment mechanism, one can establish the VPN's PE-to-PE LSPs automatically. But one challenge of this approach is that when multiple independent PEs set up PE-to-PE LSPs independently, it is impossible to set up the LSPs to be optimal considering network-wide constraints. To accomplish this network-wide optimization, some centralized path computation element is necessary to coordinate the computation of the paths of the LSPs, and PCE can perform this function.

3.8. Interworking Between Multiple VPN Domains

To enable interworking between multiple VPN domains (such as Inter-AS procedures for IP-VPNs, or multi-hop pseudowire procedures for VPLS) some smart, end-to-end-based path calculation is necessary. A PCE can perform this kind of path calculation, for example, through cooperation with other PCEs.

4. PCECP Requirements for PCE Support of VPNs

This section sets out requirements that must be met by the PCE Communications Protocol (PCECP) when PCE is used to support path computation for VPNs. These requirements supplement those common requirements described in [RFC4657], and are complementary to additional requirements present in other requirements documents such as [RFC4927], [RFC5376], and [PCE-INTER-LAYER].

4.1. Identification of VPN

Since computations may be specific to the VPN that will use the core LSP, it MUST be possible to specify the VPN ID on a path computation request.

4.2. Identification of Related VPNs

Certain computations of paths for VPN connections may need to exclude or include core resource sharing or traffic aggregation by identifying specific other VPNs. Thus is MUST be possible to specify a list of related VPN IDs on a path computation request.

This list SHOULD be accompanied by a context so that it is possible to provide lists of related VPNs for different purposes on the same path computation request. Contexts identified at this time are as

follows:

- Allowed to share network resources with LSPs for the listed VPNs.
- Prohibited from sharing network resources with LSPs for the listed VPNs.
- Allowed to carry traffic for the other listed VPNs.
- Prohibited from carrying traffic for the other listed VPNs.

Further contexts may be defined in the future and the protocol field that defines context SHOULD be reasonably extensible.

4.3. Scoping of Addresses

If the addresses used in any part of a path computation request or response are not within the scope of the network for which the computation is to be performed (for example, they are customer VPN addresses for core network nodes) this needs to be identified to the PCE. A path computation request MUST allow the PCC to indicate that certain addresses are in the scope of the customer VPN.

4.4. Cooperation between Customer PCE and Core PCE

In order for cooperation between customer and core PCEs to be most efficient, it SHOULD be possible for an initial path computation request sent from a PCC to the first PCE to identify the other PCEs with which the first PCE should cooperate.

It SHOULD also be possible for a path computation response to identify other PCEs for use at further stages in the LSP establishment process. This information would need to be carried in signaling messages to be available at downstream nodes (such as the PEs), but how this information is conveyed in signaling messages is beyond the scope of this document.

4.5. Path Diversity

Path protection schemes require that path computation requests MUST be able to indicate diversity requirements.

PE-PE protection requires that a single path computation request MUST be able to request multiple paths meeting specified diversity requirements. This requirement is already covered in [RFC4657].

CE-CE protection requires that a path computation request MUST be able to request specific diversity from another, previously computed path by specifying the links and nodes of that path. This requirement for exclusions is already covered in [RFC4657].

4.6. Point-to-Multipoint

The requirements for PCECP to support path computation for P2MP LSPs are presented in [RFC5862].

4.7. Incorporating Path Calculation During VPN Membership Discovery

In order for a PE (PCC) to request a PCE to calculate PE-to-PE VPN paths, and in order for the PE to set up these LSPs during the VPN establishment/addition/deletion process, the PCE MUST monitor VPN membership discovery. In this context, "monitor" means that the PCE's network map MUST be updated to include VPN membership information. For further discussion of how the PCE network map may be constructed refer to [RFC4655].

5. Manageability Considerations

The use of PCECP to compute paths in support of VPNs extends the manageability considerations for PCECP.

5.1 Control of Function and Policy

No additional controls of function or policy are required over and above those that are required for basic operation of PCECP. However, it should be noted that separate controls may be required for each VPN that is supported. Further, the customer may require access to some or all of the controls for their VPN.

5.2 Information and Data Models

The PCECP may be modeled and controlled through MIB modules. It may be desirable to divide such modeling and control per VPN. In particular, where access to, or control of MIB data is provided to customers so that they can gather statistics or manage the behavior of PCEs for their VPN, clear separation must be enforced so that customers have no control over or visibility into each other's VPN operation.

5.3 Liveness Detection and Monitoring

No additional liveness detection and monitoring facilities are required to be added to PCECP because of VPN support.

5.4 Verifying Correct Operation

There are no additional requirements for verifying the correct operation of the PCECP.

If information is made available to allow an operator to verify the correct computation of a path, care must be taken over precisely what information is exposed to customers so as to preserve customer confidentiality. This topic, however, falls outside the scope of manageability considerations for the PCECP.

5.5 Requirements on Other Protocols and Functional Components

The manageability of PCECP places certain requirements on the manageability of other protocols, in particular on the underlying transport protocol. The application of PCE to VPNs does not extend PCECP's requirements to be able to manage other protocols or functional components.

It should be noted that the applicability of PCE to VPNs has significant impact on the management and operation of other protocols used for PCE discovery, VPN membership discovery and advertisement, and LSP signaling. These topics are out of scope for this document.

5.6 Impact on Network Operation

As described in [RFC4655], the use of PCE may impact the operation of a network. Additionally, there are consequences of applying PCE to VPNs.

The PCECP is required to handle issues of congestion that are caused by significant numbers of computation requests issued in a small period of time. In practice, separate PCEs might be used to service the requirements of different VPNs with the result that this problem might not be so significant.

Otherwise, the extensions to PCECP to cover the use of PCE for VPNs do not have additional impact on the operation of the core network.

5.7 Other Considerations

No other management considerations arise.

6. Security Considerations

Security is an important feature for VPNs. VPN customers expect and require that their data and service information is kept secure from interception or interference by other users of the provider network.

Since the provider network will possibly support multiple VPNs as well as other services, the traffic of an individual VPN and the computation information that applies to that VPN are vulnerable within the provider network. It is important that the PCECP exchanges

are protected so that there is no visibility of computation information and so that VPN traffic cannot be diverted, for example by the spoofing or manipulation of a computed path.

These requirements do not place any additional security requirements on the PCECP above those described in [RFC4657], but the application of PCE in support of VPNs does require that those security requirements be correctly implemented and applied.

7. IANA Considerations

This document makes no requests for IANA action.

8. Acknowledgments

TBD

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to indicate requirements levels", RFC 2119, March 1997.

[RFC2702] Awduche, D., Malcolm, J., Agogbua, J., O'Dell, M., and McManus, J., "Requirements for Traffic Engineering Over MPLS", RFC 2702, September 1999.

[RFC3031] Rosen, E., Viswanathan, A., and Callon, R., "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[RFC3945] Mannie, E., "Generalized Multi-Protocol Label Switching Architecture", RFC 3945, October 2004.

[RFC4026] Andersson, L., and Madsen, T., "Provider Provisioned Virtual Private Network (VPN) Terminology", RFC 4026, March 2005.

[RFC4655] Farrel, A., Vasseur, J.P., and Ash, G., "A Path Computation Element (PCE)-Based Architecture", RFC 4655, August 2006.

[RFC4657] Ash, J., and Le Roux, J-L., "Path Computation Element (PCE) Communication Protocol Generic Requirements", RFC 4657, September 2006.

9.2. Informative References

[RFC2764] Gleeson, B., Lin, A., Heinanen, J., Armitage, G., and Malis, A., "A Framework for IP Based Virtual Private Networks", RFC 2764, February 2000

[RFC4206] Kompella, K., and Rekhter, Y., "Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)", RFC 4206, October 2005.

[RFC4208] G. Swallow et al., "Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model", RFC 4208, October 2005.

[RFC4761] Kompella, K., and Rekhter, Y., "Virtual Private LAN Service (VPLS) Using BGP for Auto-discovery and Signaling", RFC 4761, January 2007.

[RFC4762] Lasserre, M., and Kompella, K., "Virtual Private LAN Services over MPLS", RFC 4762, January 2007.

[RFC4847] Takeda, T., "Framework and Requirements for Layer 1 Virtual Private Networks", RFC 4847, April 2007.

[RFC4834] Morin, T., "Requirements for Multicast in Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs)", RFC 4834, April 2007.

[RFC4927] Le Roux, J-L, Ed., "Path Computation Element Communication Protocol (PCECP) Specific Requirements for Inter-Area MPLS and GMPLS Traffic Engineering", RFC 4927, June 2007.

[RFC5212] K. Shiomoto et al., "Requirements for GMPLS-Based Multi-Region and Multi-Layer Networks (MRN/MLN)", RFC 5212, July 2008.

[RFC5376] Bitar, N., et al., "Inter-AS Requirements for the Path Computation Element Communication Protocol (PCECP)", RFC 5376, November 2008.

[RFC5394] Bryskin, I., Papadimitriou, D., and Berger, L., "Policy-Enabled Path Computation Framework", RFC 5394, December 2008.

[RFC5440] Vasseur, JP., et al., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, March 2009.

[RFC5862] Yasukawa, S. and Farrel, A., "Path Computation Clients (PCC) - Path Computation Element (PCE) Requirements for Point-to-Multipoint MPLS-TE", RFC 5862, June 2010.

[PCE-INTER-LAYER] Oki, E., "PCC-PCE Communication Requirements for Inter-Layer Traffic Engineering", draft-ietf-pce-inter-layer-req, work in progress.

10. Authors' Addresses

Seisho Yasukawa
NTT Corporation
9-11, Midori-Cho 3-Chome
Musashino-Shi, Tokyo 180-8585,
Japan
Email: yasukawa.seisho@lab.ntt.co.jp

Adrian Farrel
Old Dog Consulting
EMail: adrian@olddog.co.uk