Layer 3 VPN Working Group
Internet Draft
Document: draft-ietf-l3vpn-as-vr-02.txt
Expires: February 2007

Ananth Nagarajan
Juniper Networks

Junichi Sumimoto
Muneyoshi Suzuki
NTT Corporation

Paul Knight
Nortel Networks

Benson Schliesser
SAVVIS Communications

August 2006

Applicability Statement for Virtual Router-based Layer 3 PPVPN Approaches

Status of this Memo

Abstract

This document is an applicability statement for Layer 3 Provider Provisioned VPNs (L3 PPVPNs) that are based on Virtual Router (VR) approaches. This document describes how VR-based approaches meet the key requirements that are outlined in the PPVPN Applicability Statements Guideline document.

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

Table of Contents

1. Introduction

The virtual router concept for L3 PPVPNs is described in [PPVPNVR]. Based on the taxonomy of PPVPNs described in [FRAMEWORK], Virtual Router based approaches are classified as PE-based Layer 3 PPVPNs.

VR-based PPVPNs are used in the following situations:

- The customer wishes to outsource the maintenance and management of inter-site VPN connectivity to the Service Provider (SP).

- The SP desires to provide VPN service without upgrading its core network to support any specific technology (e.g., MPLS), i.e., the SP wants to provide a Layer 3 VPN service over a range of core network technologies, including existing IP routed or Layer 2 switched core networks, MPLS, or a combination of these technologies.

- The customer is not aware of the topology or mechanisms used in the SP core network and is responsible for routing between customer routers, which is independent of the routing used in the SP core. The customer-facing sides of the PE devices in the SP network are visible to the customer. The logical links between VRs are also visible to the customer, and optionally it is possible for the full private network topology (including the logical links) to be visible to routers within a site.

- The customer wishes to exercise control of routing functions at the CE routers at each of its VPN sites, while depending on the SP to provide transport for data traffic and for the customer's routing information across the SP core. From the viewpoint of any of the customer's routers, there will usually appear to be a single router hop to any other VPN site. The only routes exchanged between the CE routers and the PE devices are the customer's internal routes (with the possible addition of routes desired by the customer for Internet access via the SP, such as a default route).

- The customer sends IP traffic across the VPN, possibly including non-IP traffic encapsulated in IP by the customer.

- The VPN service provider does not own a backbone network but wishes to provide PPVPN services over a backbone obtained from some other provider.

- Several cooperating SPs desire to offer PPVPN service at points that span multiple administrative domains of the backbone, perhaps over the public Internet.

This document describes how Virtual Router based VPN approaches satisfy key requirements listed in the PPVPN Service Requirements document [REQTS] and the PPVPN Security Framework [SEC-FRMWK].

2. Service Provider Provisioning Model

Virtual Routers (VRs) can interact with other routers so as to be indistinguishable from an individual physical router. However, multiple instances of VRs can be configured within a single physical device. This provides a significant improvement in manageability and

provisioning flexibility. In addition, there is potential statistical multiplexing gain on "uplinks" from the PE router to P router, compared with use of multiple physical routers. Each VR can maintain its own separate routing tables, so if two virtual routers are in the same physical router, an interaction of one VR with one of its peers does not have any effect on the interaction of another VR with any of its own peers. In some implementations, VRs may share physical interface bandwidth.

VPNs are constructed via tunnels connecting VR pairs across the service provider backbone network. Per-VR routing protocol instantiations are run to distribute VPN reachability information. VPN membership information distribution is treated separately, and is achieved via sharing a VPN-ID, for example [RFC2685], between VRs that are members of a specific VPN. The detailed VR model is described in [PPVPNVR].

2.1 Auto-Discovery

In the VR-based PPVPNS, various auto discovery mechanisms are supported. VPN discovery can be achieved through directory servers [RADIUS-DIS], explicit configuration via a management platform, using multicast [COREVPN] or by piggybacking VPN membership and topology information via routing protocols such as BGP [VPN-BGP]. A combination of these mechanisms may also be used on a PE. For example, for some VPNs topology discovery is done only through a management platform. For others, dynamic topology discovery is achieved using existing routing protocol. BGP-based auto-discovery is described in [VPN-BGP], and may be used for membership and topology discovery.

It is important to note that, for the VR architecture, the auto-discovery mechanism is only used to automatically exchange control VPN information between VRs. It is not intended for interchange of the VPN routing information, which is accomplished by standard routing protocols running between the VRs, as discussed in [PPVPNVR].

3. Supported Topology and Traffic Types

VR-based PPVPNs can be constructed using either MPLS or IP tunnels (GRE, IP-in-IP, L2TP, IPSec) in the core network, or Layer 2 connections such as ATM or Frame Relay. The choice of the tunneling mechanism may impact other properties of the VPN itself, including scalability, manageability, QoS, security, etc. For example, the use of IPSec tunnels for encryption may impact forwarding performance on some devices, and therefore impact the number of sites or routes per VPN, the number of VPNs per PE, etc. The performance of IPSec tunnels may be improved through the use of dedicated hardware, which allows greater performance and scaling but potentially at increased cost.

Tunnels are created on a per-VPN basis. For transport across the network, a number of these tunnels may be aggregated and carried within a PE-PE tunnel. The SP has a high degree of flexibility in configuring the topology of a VPN interconnecting customer sites. The topology can be full-mesh, partial-mesh, or any arbitrary topology that has been agreed to by the customer and the SP.

4. Isolated Exchange of Routing and Data Information

By definition of a Virtual Private Network, the details of its addressing, topology, connectivity, and reachability as well as the data that it transports are implicitly considered to be private, and should therefore be isolated from other networks, including others that may be supported with the PPVPN infrastructure. [FRAMEWORK]

4.1 Isolation of Routing Information

In any PPVPN, the SP is responsible for maintaining isolation between networks except as explicitly intended by the VPN owner. In the VR model, a key mechanism for maintaining isolation is through isolating routing information, thereby constraining the distribution of reachability information.

The VR model of PPVPNs provides for isolation by instantiating multiple Virtual Routers (VR) on a single physical platform to support multiple VPNs. [PPVPNVR] Each VR has its own logical interfaces, routing tables, forwarding tables, and routing protocol instances. Note that a VR may share physical interfaces with other VRs, depending on the implementation and specific topology. This provides for isolated topology, addressing, and reachability for the VPN.

Addressing and Reachability includes the assignment, discovery, and distribution of source and/or destination information for the PPVPN. The isolation of this information implies that other networks, including other VPNs and the Internet, will have no visibility into the PPVPN except as explicitly configured.

Routing information carried between VRs is carried in through the same tunnels as data itself, and is therefore segregated from the underlying backbone infrastructure by the same mechanisms that segregate data between VPNs.

This model supports arbitrary routing architectures, including support for back-door links among customer VPN sites or other potentially unique routing architecture requirements. The support for arbitrary routing architectures, however, is accompanied by scalability and management issues. These issues are discussed later in this document.

In the VR approach, virtual routers are connected to the CEs through local links, and to each other across the backbone through tunneling services provided by the service provider across the backbone. All data traffic within the VR-based VPN is isolated from non-VPN traffic by these mechanisms.

Some VR implementations may provide the ability for customers to exercise limited management operations upon the VRs which are connected to the customer CEs. This may allow the customer to view routing tables, or traffic statistics, or to exercise some control over the customers routing. VRs MUST NOT allow any customer to circumvent the isolation of routing or data among VPNs.

4.2 Isolation of Data

Data for different VPNs in the VR model is segregated through the use of different link-layer connections or tunnels over a common SP backbone. [PPVPNVR] Examples of such tunnels include GRE, L2TP, IPSec, MPLS or Layer 2 connections such as ATM or Frame Relay. It should be noted that this isolation can be impacted by misconfiguration.

5. Access Control and Authentication

CE-PE authentication has not been specified for VR-based VPNs. PE/CE mutual authentication may be done via any mechanism supported by the routing protocol in which the CE and PE are peers (e.g., use of the TCP MD5 authentication when the CE/PE protocol is BGP), or by any other mechanism that may be desired by the customer.

In order for VR-based PPVPNs to support confidentiality, integrity, authentication, and replay attack prevention, mechanisms such as IPsec may be used as tunneling mechanism or used over VPN tunnels. Even with the use of IPsec, the security level offered is dependent on the scope of the IPsec security associations: encrypting on a CE-to-CE basis (as in CE-based VPNs) will offer a wider scope of protection than only encrypting on a PE-to-PE basis (as in PE-based VPNs), since the CE-PE link remains unencrypted in the latter case. However, PE-PE IPsec offers substantial advantages in efficiency, outsourcing, and integration with the dynamic membership and dynamic routing nature of the PPVPN. CE-PE IPsec can also be used to protect traffic on the CE-PE section of the network. In this case the traffic is only unprotected by IPsec within the PE device. Policy-based security and access control mechanisms or firewalls may be used between sites in the same VPN. These can be implemented on the PE router, or on the CE.

6. Security

6.1 Protection of User Data

As described above, end-to-end (CE-to-CE) IPSec may be used to protect user data. SPs may choose to provide CE-based IPSec as a value added service. If the SP core network is also part of the public Internet, the SP may choose to provide PE-to-PE IPSec as the tunneling mechanism between VRs.

If inter-SP VPNs are to be provided, IPSec tunnels may be used. The impact on QoS and SLAs in this case will have to be studied.

In general, user data is protected via the inherent isolation provided by the inter-VR tunnels. Varying levels of security of user data may be provided based on the type of tunnel that is used.

6.2 Service Provider Security Measures

In general, the SP should ensure that non-VPN traffic does not accidentally or maliciously enter a VPN. Since VRs can be configured very specifically for a customer, the SP can offer customers anti-spoofing or other traffic or route filtering services tailored for the customer's network. The SP's PE and P devices should be protected against intrusion or denial of service attacks. This is especially important because the SP core network may be used to provide general Internet services apart from VPN services. Therefore any Denial of Service attack or misconfiguration that impacts other VPN services and Internet services should be prevented. Since most of the traffic from CE to PE, apart from control (routing and network management) traffic, gets encapsulated to be carried across the SP network, the possibility of users sending traffic to other (non-PE) systems in the core network is minimized or eliminated. The inherent isolation of VR mechanisms helps provide this protection against attacks from customer sites, but additional specific measures are available:

- VR routing sessions can be authenticated between the PE and CE, and among PEs.

- If BGP is used as an auto-discovery mechanism between VRs, it should be further authenticated using mechanisms such as TCP MD5.

- Filtering of any management data entering the PE should be performed in order to prevent the acceptance of unauthorized packets from customers or other SPs into that PE.

Denial of Service attacks may occur via routing traffic or network management traffic, either intentionally or accidentally via routing instabilities or misconfigurations in the VPN. With Virtual router VPNs, in many cases a dynamic routing protocol will be run between CE routers and VRs within PE routers. Either the same or a different dynamic routing protocol may be run between VR instances in each PE associated with a VPN. If routing is unstable in the private network, it is possible for this instability to be propagated to the PE

routers. For example, in some cases a large number of routing updates could be sent from the CE router to a VR within a PE router, or between VR instances in different PE routers. This could potentially place a major or excessive processing load on the PE routers.

This issue can be mitigated via resource partitioning in the PE, in order to limit the amount of resources (e.g., CPU and memory) which any one VR is permitted to use in PE routers. Also, rate limits may be applied to the routing traffic sent from the CE to the PE. Alternately, when this problem is detected on the CE to PE link, the CE to PE interface may be shut down.

In order to prevent DoS attacks due to network management traffic, the functions available to the customer need to be strictly controlled. It may also be useful to limit the resource use of this capability. Resource partitioning may be appropriate internal to PE routers, and network management traffic from the CE to the PE may be rate limited (for example, to prevent network management traffic from CE to PE from being used in a DoS attack).

6.3 PPVPN Security Framework Template

As stated in the "PPVPN Security Framework" [SEC-FRMWK], "An evaluation of a given PPVPN approach using this template should

appear in the applicability statement for each PPVPN approach." Please refer to Appendix A for this detailed response.

7. Addressing

Virtual Routers may provide any or all of the services which are provided by a physical router, including Network Address Translation (NAT), packet filtering, etc. These VR capabilities can simplify the process of joining previously independent site networks, which may have overlapping address spaces. NAT can be used to satisfy intra-VPN non-unique addressing requirements. This facilitates the construction of short-term or ad-hoc VPNS. It should be noted, however, that NAT has accompanying scaling problems, and other mechanisms are needed to ensure proper routing updates, when two sites share the same routing domain.

Non-unique and private customer addresses may be supported by using encapsulation within the tunneling mechanisms employed between VR pairs (e.g., GRE, IP-in-IP etc.). As such, support for private addressing as specified in [RFC1918] allows for non-unique addresses between different VPNs.

8. Interoperability and Interworking

Interoperability and Interworking of VR-based VPNs with other L3 PPVPN mechanisms such as [RFC2547bis] is for further study. Since

VRs provide all IP router functionalities, various VR-based solutions interwork and interoperate to the extent that IP networks interoperate and interwork.

9. Network Access

9.1 Physical and Link Layer Topology

VR-based mechanisms do not affect the choice of physical and link layer technologies or topologies.

9.2

Temporary Access

Temporary access for a dial-up user to a VR can be provided via PPP and AAA, using a Remote Access Server. Other access mechanisms such as IPSec can also be used. Thus, it is possible provide login and password based access to a VR-based VPN from an authorized user connected to the Internet.

9.3 Access Connectivity

Multi-homing of CEs to multiple VRs (within the same or different PEs) is supported. The PEs (and consequently the VRs) may belong to different SPs.

Load sharing based on IGP or other traffic engineering mechanisms used in the SP core are naturally supported by VR-based VPNs.

10. Service Access

10.1 Internet Access

Simultaneous VPN and Internet Access can be supported via various mechanisms. A specific VR may be assigned as a default VR that is connected to the Internet. If a single VR is to be used to carry a customer's VPN as well as Internet traffic, Internet traffic can be distinguished from VPN traffic by associating a default VPN-ID with Internet traffic and pointing it to a default route to the Internet. This default route to the Internet need not be direct, but may instead point to a firewall or other security device which may use different interfaces for VPN access and Internet access.

10.2 Hosting, ASP, other services

All of the above "external" services can be supported by associating a separate address for every service that is not being used within the VPN. If a single server (for example, a web hosting server) is used to provide a particular service to all VPNs, NAT may be used to provide a unique address for clients to access that particular service. NAT can be performed either at the customer site or can be

integrated into the PE. The scaling impacts of adding NAT to the PE will have to be considered.

11. Service Provider Routing

VR-based PPVPNs do not impose any additional requirements on the IGP used in the service provider core network. However, if the customer VPN runs an IGP, the VRs (and consequently the PEs) must support that IGP. This customer IGP need not be the same as the IGP running in the Service Provider's core network.

From the customers viewpoint of its VPN IGP routing topology (if it uses one), the SPs network topology appears much simpler than it may actually be. Depending on the VR implementation, the SPs service offering, and the SPs physical topology, it may appear as either a single large router with interfaces for each VPN site, as a full mesh, with two routers between any two sites, as a hub-and spoke topology (when the customer wants all inter-site traffic to pass through one or more specific sites, for application of services such as security filtering), or other arbitrary topology. In general, the SP's actual core routing topology is invisible to the customer.

Fault handling is a specific problem when the timers used for the VR-to-VR routing peering are shorter than the timers used for the routing peering within the service provider(s) network. In this case a single failure within a service provider network may look like a collection of un-correlated failures in the VPN.

Moreover, since a VR doesn't really "know" what causes the failure, the VR may react to such a failure by re-routing along some other tunnel, while this other tunnel may be also affected by the same failure. As a result, this would slow down routing convergence within the VPN.

To avoid the problems mentioned above one may consider making the timers used for the VR-to-VR peering longer than the timers used for the routing peering within the service provider network (so that failures within the service provider network would be "invisible" to the VR-VR tunnels). But that has its own set of problems. While this may be possible to accomplish within a single routing domain (one needs to appropriately set the IGP timers within the domain), doing this in a network that includes more than one routing domain may be difficult (as timers include both IGP and BGP timers, and moreover, timers include IGP timers in several routing domains). Another consequence of making the timers used for the VR-to-VR peering over the tunnels longer than the timers used for the routing peering within the service provider network is that it would increase the amount of traffic that will be "black holed" in the case of VR

failures.

A key aspect of the issue here is that layer 3 problems in the SP network may appear as layer 2 problems in the VPN. Thus stability of the SP network, with an emphasis on quick recovery, is a key element in delivering satisfactory service.

Prevention of Denial of Service attacks caused by routing instabilities has been discussed in Section 6.2.

11.1 Core Router Awareness of Mechanisms Used

Since tunnels are established between VR pairs, the core router (P router) does not have any information of the mechanisms used to construct the VPN. If MPLS is the tunneling mechanism that is used between the VRs, the core routers may have to be MPLS enabled in order to leverage the benefits of MPLS tunnels (e.g., traffic engineering). As such, while the core routers are not aware of VPN-specific information, they should support requirements to meet relevant SLAs. (e.g., for guaranteed QoS, the core routers may need to support appropriate QoS mechanisms).

12. Migration Impacts

Similar to other Layer 3 PPVPN architectures, any CE using services provided using the VR approach can access a PE similar to the way it would access another CE router in a private network using leased lines. As the VR approach makes use of standard routing protocols without any extensions, there is no requirement for additional capabilities on the part of CEs in order to interoperate with a VR-based PPVPN.

Key design considerations include:

- The PEs will introduce extra router hops

- If the VR-VR backbone routing protocol differs from the sites, then IGP metric implications should be carefully evaluated. This would be particularly true for multihomed VPN sites.

In general, a VR-based PPVPN offers the customer a greatly simplified network topology compared to a customer-managed private network, since each CE router sees a single link as the next-hop route to all other VPN sites. There is no need to configure multiple physical or logical interfaces on the CE routers.

Multi-homed VPN sites or sites with back-door connections will involve design decisions as to whether each of the multiple links should operate as a backup link or as a load-sharing link.

Also, since the VR approach does not depend on the backbone architecture in terms of routing protocols, a VR-based L3 PPVPN can be offered on a service provider core network without the need for

specific core technologies. For example, the core network does not need specific mechanisms like MPLS to be implemented on the P routers. Similarly, if the core network is a Layer 2 network based on ATM or Frame Relay, VR-based VPNs can still be constructed.

It should be noted, however, that core network mechanisms would determine the overall properties and services that may be provided over the VPN. For example, in order to support customer QoS SLAs, the core network should be robustly engineered or should support QoS mechanisms, in addition to SLA marking at the PE.

Thus, while migration impacts in the case of basic VPN functionality using VR are minimal from the customers' or providers' point of view, appropriate core mechanisms may be necessary for certain services.

13. Scalability

VR is a technology for implementing logical routing instances in a PE device. A PE device may contain more than one VR and a VR supports one VPN. Therefore, scalability of a VR and conventional physical router are basically the same, e.g., if different routing protocols are used for customer and network sides of a VR or physical router, the load is increased compared with the case when the same protocols are used.

The major factor contributing to scalability constraint in the VR approach is the number of VRs which can be supported by a PE. This is

because, the number of VRs in a PE device is equal to the number of VPNs which are supported by the PE.

Resources used by a VR instance include memory and processor resources, used to support VPN tunnel mechanisms, routing protocol instances, route tables, interface management, etc. The extent to which these resources are utilized impact scalability.

Much of the resource utilization for a given VPN will be affected by the topology of the VPN. For instance, a VPN with a full-mesh topology will require that VRs have more peers for the VPN tunneling mechanism, for routing protocol adjacencies, for security protocols, etc., while a hub-and-spoke model will constrain the resources required for 'spoke' PE routers.

From a VR perspective, scalability also depends on whether the same routing protocols are used between VRs as in the backbone network. If the inter-VR routing protocols are different from the backbone IGP, the scaling and management impacts for configuring routing protocols on a per-VR basis may be significant. For example, it may be necessary to maintain OSPF databases for the entire customer VPN topology, as opposed to maintaining information for only directly connected customer sites. Additionally, the customer IGP may need to maintain information about the entire VR topology, for the VRs which

are connected to the customer's CEs. Other concerns include routing loop avoidance, route redistribution, etc. Thus, while the VR model allows the routing protocols between customers and VRs to be different than the backbone IGP, this flexibility can be accompanied by scalability concerns. Mechanisms such as OSPF areas may be used to circumvent such scaling issues.

It is normal in many cases for a VR located in a PE router to run a routing instance with each other VR which is part of the same VPN. In some cases this could result in a large number of routing adjacencies. The number of routing adjacencies could aggravate the impact of instability in routing in the private network, or aggravate the impact of routing protocol DOS attack described in Section 6.2.

As mentioned in Section 6.2, this can be mitigated by appropriate resource partitioning in the PE, and by rate limiting of routing packets, including packets from CE to PE and well as packets from PE to PE. Also, while this consideration may limit the number of VRs

which may potentially be supported from a single PE device, it does not have any significant effect on the overall scaling of a network implementing the VR approach.

14. QoS/SLA

VR-based PPVPNs support any kind of QoS that the core network and the tunneling mechanism used support.

VR-based VPNs can utilize different quality of service mechanisms. QoS mechanisms developed for physical routers can be used with VRs, on a per-VR basis. e.g. classification, policing, drop policies, traffic shaping and scheduling/bandwidth reservation. The architecture allows separate quality of service engineering of the VPNs and the backbone. However, the tunneling mechanisms themselves should support relevant QoS mechanisms.

15. SLA Monitoring

VR-based VPNs can implement a variety of methods to monitor compliance with Service Level Agreements. Since the links between VRs make use of tunnels across the underlying backbone network, the SLA monitoring capabilities of the backbone network can be used to monitor the performance of the inter-VR links. Because the inter-VR links are tunnels, and the SLA monitoring capabilities of the backbone network may not include per-tunnel monitoring capabilities, some VR implementations support additional SLA monitoring mechanisms. Performance to SLA requirements within the PEs hosting the VRs is typically monitored via internal processes to ensure compliance from end to end. In addition, either the service provider or the VPN customer can use all existing SLA tracking tools (round trip time measurement, traceroute mapping, etc.) within the VR-based VPN.

16. Management

16.1 Service Provider Management of Customer Site

The SP may choose to manage the customer site (i.e., the CE devices)

for added revenue. If the SP uses a centralized customer management system, care should be taken to uniquely identify various CEs belonging to different VPNs, so that CE devices from different VPNs do not reach each other.

The customer may desire to have access to the PE device for monitoring purposes (e.g., ping, traceroute). Providing such access is at the discretion of the SP.

Traffic statistics in order to prove SLAs to customers may be provided on a periodic basis. Other statistics that can show enhanced SP capabilities, including protection against Denial of Service attacks, failure etc., can be provided to the customer.

16.2 Customer Management of VR

Some VR implementations may provide the ability for customers to exercise limited management operations upon the VRs which are connected to the customer CEs. This may allow the customer to view routing tables, or traffic statistics, or to exercise some control over the customers routing.
Customer network management and troubleshooting systems will generally have less ability to gather information from the VRs than from the customers own routers, and will also have little or no ability to directly change VR configurations. The customers systems should be planned so as to accommodate the restricted capabilities of the VRs to respond to customer network management processes.

Prevention of Denial of Service attacks due to network management traffic originating from customer management of the VR has been discussed in Section 6.2.

16.3 Service Provider Network Management

When an SP provides VR-based VPN services, it is highly likely that the PE devices used are complex because of the number of VRs supported, the number of routing adjacencies between VR pairs, maintenance of tunnel and VPN-specific information and possibly other information such as QoS. Thus the management of the PE is extremely critical for the SP. If the SP core is also used to provide Internet services, adequate mechanisms should be in place in order to not allow misconfigurations or instabilities in the PE control plane to affect the general Internet operations or impact other VPN customers. In addition to normal SP network management, prevention of Denial of Service attacks must be in place in the PEs. Resource partitioning

and rate limiting, as described in Section 6.2 are examples of such mechanisms.

17. Security considerations

There are no additional security considerations besides those already addressed in this document in Section 6, and in Appendix A. VR-based VPNs are expected to meet the security framework described in [SEC-FRMWK].

Appendix A: Responses to Security Evaluation Template

This Appendix presents an evaluation of how the Virtual Router model measures up against the Security Evaluation Template developed in the PPVPN Security Framework [SEC-FRMWK]. As stated in that document, "An evaluation of a given PPVPN approach using this template should appear in the applicability statement for each PPVPN approach."

NOTE: For ease of reference to the PPVPN Security Framework [SEC-FRMWK], the assertion numbering scheme from the Security Template of that document is retained in this Appendix.

1. The approach provides complete IP address space separation for each L3 VPN.

The VR approach completely addresses the requirement by instantiating a separate VR for each VPN that is configured on any specific PE. Each VR maintains separate routing tables, so each L3 VPN has complete IP address separation from other VPNs. Connections between VRs in the same VPN are tunneled across the Service Provider's network, providing separation between the IP address space of the SP and each VPN.

2. The approach provides complete L2 address space separation for each L2 VPN.

The requirement is not applicable to the VR approach because VR is a L3 VPN.

3. The approach provides complete VLAN ID space separation for each L2 VPN.

The requirement is not applicable to the VR approach because VR is a L3 VPN.

4. The approach provides complete IP route separation for each L3 VPN.

The VR approach completely addresses the requirement by instantiating a separate VR for each VPN that is configured on any specific PE. Each VR maintains separate routing tables, so each L3 VPN has complete IP route separation from other VPNs. Routes for each VPN are distributed by tunneling across the Service Provider's network between VRs of the same VPN, providing separation between the various VPN routes, and between the routes of the SP and each VPN.

5. The approach provides complete L2 forwarding separation for each L2 VPN.

The requirement is not applicable to the VR approach because VR is a L3 VPN.

6. The approach provides a means to prevent improper cross-connection of sites in separate VPNs.

The VR approach completely addresses the requirement by using a VPN-ID to positively identify the VPN membership of each VR. The VPN ID is used when BGP is used for auto-discovery. It might also be used when a management system is used for discovery, in which case the VPN-ID is used by the appropriate MIB, for example [VR-MIB]. VRs of different VPNs will not form routing adjacencies or exchange VPN data. Alternatively, CE to CE authentication [L3-VERIF], could also be used to protect against the threat of improper cross-connection.

7. The approach provides a means to detect improper cross-connection of sites in separate VPNs.

The VR approach partially addresses the requirement by using a VPN-ID to positively identify the VPN membership of each VR. VRs connected to the wrong VPN (for instance, through an ATM or MPLS configuration error) would not establish routing adjacencies or exchange VPN data. However, there is not a requirement in [L3VPNVR] to specifically detect improper cross-connection. The improper cross-connection would simply result in a non-working VPN link, which would need to be detected and corrected by normal troubleshooting techniques.

In the case of misconfiguration of a VR with the wrong VPN-ID and other VPN attributes, the VR approach does not specify a method of detecting the improper cross-connection. However, a method of detecting PE misconfiguration is described in [L3-VERIF], based on tokens exchanged between CEs and PEs. The VR approach is compatible with either the BGP-based or UDP-based token exchange models that are described in that document, to address the case of misconfiguration of VPN membership on the PE.

8. The approach protects against the introduction of unauthorized packets into each VPN.

    a. In the CE-PE link

The VR approach completely addresses the requirement by supporting the optional use of IPsec protection for the CE-PE link. The VR approach allows a choice of CE-PE link configurations, thereby allowing the PPVPN customer and the PPVPN Service Provider to select the link type which will provide the desired degree of protection against this threat. However, the VR approach by itself does not provide specific packet-by-packet protection against this threat.

    b. In a single- or multi- provider PPVPN backbone

The VR approach partially addresses the requirement by specifying the use of tunnels between VRs across the backbone. Thus it provides protection against the introduction of unauthorized packets to the full extent of the underlying tunnel technologies. However, the VR model by itself does not completely address the requirement, because it allows the use of tunneling technologies such as GRE or IP-in-IP which may not provide protection against this threat.

With the optional use of IPsec, the VR approach completely supports the requirement.

    c. In the Internet used as PPVPN backbone

The VR approach partially addresses the requirement by specifying the use of tunnels between VRs across the backbone, including across the Internet. IPsec tunnels provide reliable protection against the introduction of unauthorized packets in this case, and the VR model completely addresses the requirement when IPsec is used. However,

the VR model by itself does not completely address the requirement, because it allows the use of tunneling technologies such as GRE or IP-in-IP which may not provide protection against this threat.

9. The approach provides confidentiality (secrecy) protection for PPVPN user data.

    a. In the CE-PE link

The VR approach completely addresses the requirement by supporting the optional use of IPsec protection for the CE-PE link. However, the VR approach by itself does not provide specific confidentiality protection.

    b. In a single- or multi- provider PPVPN backbone

The VR approach completely addresses the requirement by supporting the optional use of IPsec protection for the backbone links. Other tunnel types offer varying degrees of confidentiality.

    c. In the Internet used as PPVPN backbone

The VR approach completely addresses the requirement by supporting the optional use of IPsec protection for the backbone links, including links over the Internet. Other tunnel types offer varying degrees of confidentiality, and may not be reliably supported over an arbitrary Internet path.

10. The approach provides sender authentication for PPVPN user data.

    a. In the CE-PE link

The VR approach completely addresses the requirement by supporting the optional use of IPsec authentication on the CE-PE link. When the IPsec Security Association is established, the use of authentication can be specified. Authentication will be applied to each packet. When IPsec is not used, the VR approach does not inherently provide sender authentication on the CE-PE link.

    b. In a single- or multi- provider PPVPN backbone

The VR approach partially addresses the requirement of sender authentication across the backbone, through the use of the VPN-ID. The VPN-ID acts to authenticate the VRs configured on the PEs to each other as senders across the backbone, although it does not authenticate the CE senders, since the VPN-ID is only used between the VRs. This is a cryptographically weak authentication, but since the PE configurations are managed by the Service Provider(s) and should not be subject to manipulation by attackers, it is of significant value against accidental misconfiguration.

In addition, IPsec authentication can be configured between the VRs, and between the CEs and VRs, so that a chain of authentication can be established between CE senders across the PPVPN. With the use of IPsec, the VR approach completely addresses the requirement across the backbone in either a single- or multi-provider case.

c. In the Internet used as PPVPN backbone

The VR approach partially addresses the requirement of sender authentication across the Internet through the use of IPsec and the VPN-ID, as discussed in the previous response (10.b).

11. The approach provides integrity protection for PPVPN user data.

a. In the CE-PE link
b. In a single- or multi- provider PPVPN backbone
c. In the Internet used as PPVPN backbone

In each situation (11.a-c), the VR approach completely addresses the requirement of integrity protection, through the optional use of IPsec. Integrity checking is typically performed along with the authentication protection discussed in item 10 above. The VR approach does not provide additional integrity checking in its basic form.

12. The approach provides protection against replay attacks for PPVPN user data.

a. In the CE-PE link
b. In a single- or multi- provider PPVPN backbone
c. In the Internet used as PPVPN backbone

In each situation (12.a-c), the VR approach completely addresses the requirement of protection against replay attacks, through the optional use of IPsec with replay protection enabled. Replay attack protection is accomplished by checking the sequence number in the IPsec AH or ESP packet header, and is typically performed along with the authentication protection discussed in item 10 above. The VR approach does not provide additional replay attack protection in its basic form.

13. The approach provides protection against unauthorized traffic pattern analysis for PPVPN user data.

a. In the CE-PE link

The VR approach partially addresses the requirement of protection against traffic pattern analysis through the optional use of IPsec on the CE-PE link. Since IPsec-protected traffic on the CE-PE link only reveals the amount of traffic between the CE and PE, and not the ultimate destination of that traffic within the VPN, only limited information on traffic patterns could be gained by analyzing any particular CE-PE link. If an attacker is able to measure the traffic on all CE-PE links of a VPN, then a fairly detailed traffic pattern analysis could be performed. Where the CE-PE traffic is not protected by IPsec in the VR approach, the traffic would be visible to an attacker with access to the data stream, and the attacker could derive a significant amount of traffic pattern analysis information. However, note that it is unusual for an attacker to have access to the data stream on any CE-PE link, unless the user taps the line or compromises the CE or PE devices. In this case, traffic pattern analysis may be a relatively minor concern compared to other concerns of direct data interception.

b. In a single- or multi- provider PPVPN backbone

The VR approach partially addresses the requirement of protection against traffic pattern analysis through the optional use of IPsec on the backbone. This obscures the actual source and destination of traffic, along with the traffic contents. Only the fact that data is being transmitted between PEs or VRs can be detected through traffic interception. If multiple CEs of a single VPN are connected to a single VR, then an attacker analyzing the backbone traffic would not be able to distinguish between traffic to or from the various CEs. In addition, an attacker would need to obtain detailed information on the internal configurations of the Service Provider's PE devices in order to correlate captured backbone traffic with any particular VPN.

An optional extension to the VR approach completely addresses the requirement of protection against traffic pattern analysis by using a backbone virtual router in addition to using IPsec on the backbone. Since the backbone VR links act to multiplex data of multiple VPNs, and the IPsec obscures other information which could identify the VPN

source or destination, an attacker would face an almost insurmountable obstacle to reliable traffic pattern analysis based on capturing backbone traffic.

c. In the Internet used as PPVPN backbone

Similar to (13.c.) above for a provider-managed backbone, the VR approach provides either partial or complete protection, using IPsec and the backbone VR, over the Internet. Traffic interception may be a somewhat more likely problem on the Internet than on a SP backbone, but the VR approach provides a means of addressing the threat in either case.

14. The control protocol(s) used for each of the following functions provide for message integrity and peer authentication:

a. VPN membership discovery

The VR approach can use several types of membership discovery, including BGP-based auto-discovery and configuration. When BGP-based auto-discovery is used, the VR approach completely addresses the requirement of providing control message integrity and peer authentication using the MD5 option. The protection of configuration mechanisms for VR approaches is outside the scope of the VR mechanism. VPN membership discovery using the VR approach provides integrated peer authentication through the use of the VPN-ID, which is common to all VRs within a single VPN.

b. Tunnel establishment

The VR approach does not specify a control protocol for tunnel establishment, but when IPsec tunnels are used, the VR approach completely addresses the requirement of providing message integrity and peer authentication. In addition, the use of the VPN-ID provides an integrated method of peer authentication among VRs within a single VPN.

c. VPN topology and reachability advertisement
   i. PE-PE

In the VR approach, VPN topology and reachability advertisement uses standard routing protocols between the VRs, carried within tunnels.

These routing protocols can provide message integrity and peer authentication when the protocol supports it, as in MD5 options. In addition, when IPsec is used for the tunnels, it provides complete support for security for any routing protocol running between the VRs (between the PEs).

ii. PE-CE

The VR approach uses standard routing protocols between the VR (PE) and CE to provide VPN topology and reachability advertisement. The security features of routing protocols, such as MD5 options, can be applied, with or without IPsec. In addition, the VR-CE link can be protected with IPsec to provide complete support for securing the routing protocols. In the VR approach, some aspects of topology and reachability in the PE-CE relationship will be configured rather than exchanged dynamically. The security of configuration mechanisms is beyond the scope of the VR specification.

d. VPN provisioning and management

The VPN provisioning and management requirement is addressed in a way that is beyond the scope of the VR approach. Most parts of the VPN provisioning and management will be performed via configuration within the VR model, and thus there are no specific protocols defined within the VR VPN scheme for these functions.

e. VPN monitoring and attack detection and reporting

VPN monitoring and attack detection and reporting requirements are addressed in a way that is beyond the scope of the VR approach. Most parts of these functions will be performed via a variety of network management tools within the VR model, and thus there are no specific protocols defined within the VR VPN scheme for these functions. Since the VR approach is based on standard router functionality, the management technologies which have been developed in the industry for router security will be widely applicable for VR-based VPNs.

f. Other VPN-specific control protocols, if any.

Since the VR approach is based on standard router operations, there are no VPN-specific control protocols defined for the VR model.

The following questions solicit free-form answers.

15. Describe the protection, if any, the approach provides against PPVPN-specific DOS attacks (i.e. Inter-trusted-zone DOS attacks):

    a. Protection of the service provider infrastructure against Data Plane or Control Plane DOS attacks originated in a private (PPVPN user) network and aimed at PPVPN mechanisms.

In the VR approach, the service provider-managed VRs typically appear to the PPVPN users to be a single router connecting all of the VPN sites.

The VRs should be configured to allow only three types of traffic from the user VPN sites:
- routing protocols

- data packets destined for another site within the same VPN as the originating site
- data packets with non-VPN destinations, if permitted by the Service Provider.

This configuration serves to prevent most types of control plane attacks, since any type of direct connection from a VPN site to the VR's management functions using protocols such as SNMP, ftp, tftp, rlogin, rsh, etc., should be disallowed. The VR allows the same types of configurations as are common on physical routers to enforce this kind of configuration.

A control plane attack might still be able to attempt to use the first type of traffic, while a data plane attack might use the latter two. These cases are discussed below.

A control plane attack might consist of the CE device sending improper routing information to the VR. This could consist of unauthorized or malformed routes, rapid announcement and/or withdrawal of proper routes, or some combination of these. Since the VR has the same mechanisms as a physical router, the VR can use well-known routing security features to provide protection against this kind of attack, including route filters and route flap damping, or it could be configured with the allowable routes for the specific VPN

site, and not accept routing updates from the site. The VPN mechanisms in the VR do not make it more susceptible to control plane attacks such as those based on routing protocols.

A data plane attack on the VR would consist of a CE transmitting a large amount of traffic to the VR. Since the VR has all of the mechanisms of a physical router, it can be configured to handle the traffic using the same techniques as any Service Provider router. The VPN mechanisms in the VR do not make it more susceptible to DoS attacks based on traffic flooding.

The VR architecture used in the PE devices provides for isolation of the operation of the VRs configured on it. Thus measures taken to defend against excessive traffic from one VPN site should not be able to affect the operation of other VRs in that PE, or elsewhere in the network.

b. Protection of the service provider infrastructure against Data Plane or Control Plane DOS attacks originated in the Internet and aimed at PPVPN mechanisms.

Both data plane and control plane DoS attacks which originate in the Internet can be prevented by overall design of Service Provider network, for instance by the use of filtering to block any packets destined to internal SP devices such as VRs. Internal SP devices may also be configured with private or non-routable addresses to help prevent access from the Internet. The VPN mechanisms in the VR do

not make it more susceptible to DoS attacks from the Internet. Since VRs have the capabilities of physical routers, they can use the techniques available to Service Provider routers to provide various protective measures.

c. Protection of PPVPN users against Data Plane or Control Plane DOS attacks originated from the Internet or from other PPVPN users and aimed at PPVPN mechanisms.

The VR model completely supports protection of PPVPN users from either data plane or control plane DoS attacks directly from the Internet, unless Internet connectivity is specifically configured for an individual VPN. Since inter-VR links are tunneled, there is no opportunity for non-VPN traffic, such as Internet traffic, to be introduced into the VPN.

If an individual VPN includes PPVPN-mediated Internet connectivity as a configured option, then the VR(s) providing the Internet access should be configured with appropriate firewall policies to protect against Dos (and other) attacks.

The mechanisms discussed above in (15.a) and (15.b) for protection of the Service Provider infrastructure from VPN-based and Internet-based DoS attacks also serve to protect other VPNs from attacks from these sources. The VPN mechanisms used in the VR approach do not make it more susceptible to propagating DoS attacks among VPNs, since the basic VR architecture defines effective separation of all PE resources among the VRs.

Attacks from one VPN site toward another VPN site in the same VPN are outside the scope of the VR approach, although the VR model makes it possible to configure firewall protections including internal attack protection at each VR if this service is desired.

16. Describe the protection, if any, the approach provides against unstable or malicious operation of a PPVPN user network:

    a. Protection against high levels of, or malicious design of, routing traffic from PPVPN user networks to the service provider network.

This is discussed in the response to (15.a) above. Since the VR has the same mechanisms as a physical router, the VR can use well-known routing security features to provide protection against this kind of attack, including route filters and route flap damping, or it could be configured with the allowable routes for the specific VPN site, and not accept routing updates from the site.

    b. Protection against high levels of, or malicious design of, network management traffic from PPVPN user networks to the service provider network.

Since the VR approach imbues each VR with the capabilities of physical routers, including filtering and firewall functionality, the VRs should be configured by the Service Provider with appropriate filters to block network management traffic directed at any Service Provider system. Network management traffic from PPVPN users does

not have any privileged access to the Service Provider network outside of the VR-VR tunnels, so they will be blocked by the same mechanisms which prevent this kind of attack from anywhere in the Internet.

c. Protection against worms and probes originated in the PPVPN user networks, sent towards the service provider network.

Similar to the filtering capabilities which the VR and use to block network management traffic, the VR can be configured to block any kind of traffic directed at any component of the service provider network. Since the traffic originating in PPVPN user networks is contained in tunnels after it is received at the VR serving any particular VPN site, the VR approach makes it fairly simple to prevent traffic originating in PPVPN user networks from being able to reach any Service Provider device. Worms or probes from PPVPN users do not have any privileged access to the Service Provider network outside of the VR-VR tunnels, so they will be blocked by the same mechanisms which prevent this kind of attack from anywhere in the Internet.

17. Is the approach subject to any approach-specific vulnerabilities not specifically addressed by this template? If so describe the defense or mitigation, if any, the approach provides for each.

The authors are not aware of any VR-specific vulnerabilities not addressed by this template.

References

Informative References

[PPVPNVR] Ould-Brahim, H., et al., "Network based IP VPN Architecture using Virtual Routers", work in progress.
[FRAMEWORK] R. Callon, et al., "A Framework for Layer 3 Provider Provisioned Virtual Private Networks," RFC 4410.
[REQTS] McDysan, D., et al., "Service requirements for Layer 3 Provider Provisioned Virtual Private Networks", RFC 4031.
[SEC-FRMWK] Fang, L., et al., "Security Framework for Provider Provisioned Virtual Private Networks", RFC 4111.
[RFC2685] Fox B., et al, "Virtual Private Networks Identifier", RFC 2685, September 1999.
[RADIUS-DIS] Heinanen J., "Using Radius for PE-Based VPN Discovery", work in progress.
[VPN-BGP] Ould-Brahim, H., et al, "Using BGP as an Auto-Discovery Mechanism for Network-based VPNs", work in progress.
[RFC1918] Rekhter, Y. et al., "Address Allocation for Private Internets," RFC 1918, February 1996.
[RFC2547bis] Rosen E., et al, "BGP/MPLS VPNs", RFC 4364.
[RFC2764] Gleeson, B., et al., "A Framework for IP Based Virtual Private Networks", RFC 2764, February 2000.
[L3-VERIF] Bonica, R. et al., "CE-to-CE Member Verification for Layer 3 VPNs",work in progress.
[VR-MIB] Seltzer, E et al., Virtual Router Management Information Base Using SMIv2, work in progress

Acknowledgments

The authors of this draft would like to acknowledge the suggestions and comments received from the entire Layer 3 Applicability Statement Design Team formed in the PPVPN working group. Besides the authors, the members of the design team include Marco Carugi, Eric Rosen, Jeremy De Clercq, Luyuan Fang, Dave McDysan, Cliff Wang, Olivier Paridaens, Tom Nadeau, Yakov Rekhter and Rick Wilder. Thanks are also due to the authors of [PPVPNVR], especially Hamid Ould-Brahim. Many thanks are due to the constructive comments made by Ross Callon and Mark Duffy.

Author's Addresses

Ananth Nagarajan
Juniper Networks
E-mail: ananth@juniper.net

Muneyoshi Suzuki
NTT Information Sharing Platform Labs.
3-9-11, Midori-cho,
Musashino-shi, Tokyo 180-8585, Japan
Email: suzuki.muneyoshi@lab.ntt.co.jp

Junichi Sumimoto
NTT Communications Corporation
3-20-2 Nishi-Shinjuku,
Shinjuku-ku, Tokyo 163-1421, Japan
E-mail: j.sumimoto@ntt.com

Paul Knight
Nortel Networks
600 Technology Park Drive
Billerica, MA 01821
+1-978-288-6414
E-mail: paul.knight@nortel.com

Benson Schliesser
SAVVIS Communications
1 Savvis Parkway
St. Louis, MO 63017 USA
+1-877-203-1097
Email: bensons@savvis.net

Acknowledgement:

Funding for the RFC Editor function is currently provided by the Internet Society.