Network based IP VPN Architecture
using Virtual Routers

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

This draft describes a network-based VPN architecture using virtual routers. The VPN service is built based on the virtual router (VR) concept, which has exactly the same mechanisms as a physical router, and therefore inherits all existing mechanisms and tools for configuration, operation, accounting, and maintenance. Within a VPN domain, an instance of routing is used to distribute VPN reachability information among VR routers. Any routing protocol can be used, and no VPN-related modifications or extensions are needed to the routing protocol for achieving VPN reachability. Virtual routers can be deployed in different VPN configurations, direct VR to VR connectivity through layer-2 or by aggregating multiple VRs into a single VR combined with IP or MPLS based tunnels. This architecture accommodates various backbone deployment scenarios, both where the VPN service provider owns the backbone, and where the VPN service provider obtains backbone service from one or more other service providers.

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.

Table of Contents

1  Introduction ........................................ 3
2  Virtual Router Architecture Requirements .......... 4
2.1 Membership ......................................... 4
2.2 Scalability ......................................... 4
2.3 Quality of Service .................................. 5
2.4 Auto-Discovery .................................... 5
2.5 Routing ............................................ 5
2.5.1 Routing between PE and CE ....................... 5
2.5.2 Routing in the Service Provider Network ....... 5
2.5.3 Routing between PEs............................... 5
2.6 Security ........................................... 5
2.7 Topology ........................................... 5
2.8 Tunneling .......................................... 6
2.9 Management ......................................... 6
2.10 General Requirements .............................. 6
3  Network Reference Model ............................ 6
3.1 Backbone ........................................... 7
4  Virtual Router Definition ........................... 7
5  How VPNs are built and deployed using VRs .......... 8
5.1 VR to VR Connectivity over layer-2 Connections... 8
5.2 VR to VR Connectivity through IP or MPLS Tunnels.. 9
5.3 Virtual Router Backbone Aggregation ............... 9
5.3.1 Tunneling ....................................... 10
5.3.1.1 MPLS Tunnels ................................ 10
1. Introduction

Several solutions have been put forward to achieve various levels of network privacy and traffic isolation when building VPNs across a shared IP backbone. Most of these solutions require separate per-VPN forwarding capabilities and make use of IP- or MPLS-based tunnels across the backbone [VPN-RFC2764], [RFC-2917], and [VPN-RFC2547bis].

This document describes a network-based VPN architecture using virtual routers. The architecture complies with the IP VPN framework described in [VPN-RFC2764]. The objective is to provide per-VPN routing, forwarding, quality of service, and service management capabilities. The VPN service is based on the virtual router concept, which has exactly the same mechanisms as a physical router, and therefore can inherit all existing mechanisms and tools for configuration, deployment, operation, troubleshooting, monitoring, and accounting. Virtual routers can be deployed in various VPN configurations. Direct VR to VR connectivity may be configured through layer-2 links or through a variety of tunnel mechanisms, using IP- or MPLS-based tunnels. Multiple VRs may be aggregated over a "backbone VR." This architecture accommodates various backbone deployment scenarios, including where the VPN service provider owns the backbone, and where the VPN service provider obtains backbone service from one or more other service providers.

Within a VPN domain, an instance of routing is used to distribute VPN reachability information among VR routers. Any routing protocol can be used, and no VPN-related modifications or extensions are needed to the routing protocol for achieving VPN reachability. VPN reachability information to and from customer sites can be dynamically learned from the CE using standard routing protocols, or...
it can be statically provisioned on the VR. The routing protocol between the virtual routers and CEs is independent of the routing used in the VPN backbone, between the VRs. That is, the routing protocol between the VRs may be the same or it might be different than the routing mechanism used between the CE and VR. Likewise, since the VR-to-VR connectivity can use tunnels, the inter-VR routing protocol can be independent of the routing used in the backbone network(s) over which the VR-based VPN runs.

There are two fundamental architectures for implementing network-based VPNs: virtual routers (VR) and piggybacking. The main difference between the two architectures resides in the model used to achieve VPN reachability and membership functions. In the VR model, each VR in the VPN domain is running an instance of routing protocol responsible for disseminating VPN reachability information between VRs. Therefore, VPN membership and VPN reachability are treated as separate functions, and separate mechanisms are used to implement these functions. VPN reachability is carried out by a per-VPN instance of routing, and a range of mechanisms is possible for determining membership (see section 6.0). In the piggyback model the VPN network layer is terminated at the edge of the backbone, and a backbone routing protocol (i.e., extended BGP-4) is responsible for disseminating the VPN membership and reachability information between provider edge routers (PE) for all the VPNs configured on the PE. [VPN-RFC2547bis] is an example of a piggyback VPN architecture.

2. Virtual Router Architecture Requirements

2.1 Membership

All virtual routers that are members of a specific VPN MUST share the same VPN identifier (VPN-ID). This should be the Globally Unique Identifier (GID) defined in [VPN-GID] or the VPN-ID format defined in [VPN-RFC2685].

2.2 Scalability

In this architecture, the backbone internal nodes (e.g., P devices) are not required to be VPN aware or VR aware, and therefore they don't keep any VPN state within the backbone. Thus the VR architecture is not a significant contributor to issues of backbone scalability.

The PE on which the VRs run (and the VRs themselves) should be able to accommodate rapid growth in the number of routes per VR, since this number can change suddenly as membership changes. The PE should be able to accommodate substantial growth in the number of VRs and CEs supported, to avoid reconfiguration that can disrupt existing connectivity. The use of the "backbone VR" (Section 5.3) improves the scalability of the PE, since many VRs on the PE may use the backbone VR for connectivity to other VPN sites.
2.3 Quality of Service

Existing quality of service mechanisms developed for physical routers should all be available to be used on a per-VR basis. Therefore, quality of service (policing, shaping, classification, and scheduling) SHOULD be configurable on a per-VPN basis.

2.4 Auto-discovery

It should be possible for the VRs to automatically discover each other, set up tunnels to each other, and exchange private routing information across the backbone. It is required that the auto-discovery mechanism take into consideration the case where the VPNs are implemented across administrative domains. We assume in this document that an auto-discovery mechanism which provides services similar to BGP (as described in [VPN-BGP]) is used as the mechanism to distribute membership, topology, and tunnel information among VRs which are members of the same VPN.

2.5 Routing

2.5.1 Routing between PE and CE

Any existing routing protocol can be used between PE and the CE. Typically, the routing protocol of the specific VPN site will be used. Static routes may be used. The routing protocol between the PE and the CE can be independent of the PE-to-PE routing.

2.5.2 Routing in the Service Provider Network (Backbone)

The choice of the backbone routing protocol should not be constrained by the VPNs.

2.5.3 Routing between PEs

Any existing routing protocol can be used between PEs. The routing protocol between the PEs can be independent of the CE-to-PE routing. As with any network design, care must be taken when multiple routing protocols are used, due to differences in metrics, detail of information, etc.

2.6 Security

The architecture MUST accommodate different levels of security for data, routing, and other control information. The architecture must provide authentication and encryption services for VPNs requiring strong security capabilities.

2.7 Topology
VPN topologies such as a hub and spoke, and full mesh MUST be supported. It should be possible to build arbitrary VPN topologies.

For example, in the case where the internal nodes (P devices) are also VR aware (NOTE this is not required - see section 2.2) then it is possible to have either tunnels from the PE or the CE connecting to these internal VRs. This type of VPN deployment can be useful when the internal nodes are geographically suitable to be a VPN hub.

2.8 Tunneling

The architecture should not be limited to a single tunneling mechanism. It should be possible to use IPSec, GRE [RFC-1701], IP in IP, and MPLS tunnels. It should also be possible to allow multiple VPNs to share a tunnel across a backbone. Therefore within a single VPN, different types of tunnels can be used.

2.9 Management

It should be easy to configure, deploy, operate and troubleshoot each VPN independently, using existing mechanisms and tools. Tools used for operating, managing and debugging IP networks can continue to be used without any modification. Most aspects of the management of the multiple VRs on the PE by the Service Provider are implementation-specific, and beyond the scope of this document.

2.10 General Requirements

The followings are some general requirements for the VR architecture:
1) The architecture should accommodate different sizes of VPNs, and one VPN should not impact other VPNs on the PE.
2) The architecture MUST support overlapping VPN address spaces in separate VPNs.
3) The architecture should support direct paths between VPN sites that bypass the service provider backbone (backdoor links). Traffic can be directed to the backdoor link, or injected to the backbone with the flexibility of using both the backbone access, and the backdoor link as internal or external paths.
4) The architecture MUST work over different deployment scenarios, e.g. where the service provider owns its own backbone, and where the service provider obtains backbone service from one or more other service providers.

3. Network Reference Model

A VPN customer site is connected to the provider backbone by means of a connection between a Customer Edge (CE) device, (which can be a bridge or a router) and a virtual router (VR). CE devices are preconfigured to connect to one or more VRs. Multiple VRs may coexist on the same service provider edge device (PE).
CE devices can be attached to VRs over any type of access link (e.g. ATM, frame relay, ethernet, PPP or IP tunneling mechanism such as IPSec, L2TP or GRE tunnels).

CE sites can be statically connected to the provider network via dedicated circuits, or can use dial-up links. Routing tables associated with each virtual router define the site-to-site reachability for each VPN. The internal backbone provider routers (P) are not VPN aware and do not keep VPN state.

### 3.1 Backbone

In general the backbone is a shared network infrastructure, which represents either:
1) A layer-2 ATM or frame relay network.
2) An IP network.
3) An MPLS network.

Not all VPNs existing on the same PE are necessarily connected to the same backbone. A single VPN can be built from multiple transport technologies.

### 4. Virtual Router Definition

A virtual router (VR) is an emulation of a physical router at the software and/or hardware levels. Virtual routers have independent IP routing and forwarding tables and they are isolated from each other. This means that a VPN’s address space can overlap with another VPN’s address space. The addresses need only be unique within a VPN domain.

A virtual router has two main functions:
1) Constructing routing tables for the paths between VPN sites using any routing technologies (e.g., static, OSPF, RIP, or BGP).
2) Forwarding packets to the next hops within the VPN domain.

From the VPN user point of view, a virtual router provides the same functionality as a physical router. Separate routing, and forwarding
capabilities provide each VR with the appearance of a dedicated router that guarantees isolation from the traffic of other VPNs, while running on shared forwarding and transmission resources.

Virtual routers belonging to the same VPN domain must have the same Virtual Private Network Identifier (VPN-ID). Examples of VPN-ID formats are described in [VPN-RFC2685] and [VPN-GID]. To the CE access device, the virtual router appears as a neighbor router in the CE based network. The CE sends all traffic for non-local VPN destinations to the VR, unless the specific VPN topology provides alternate routes. Each CE access device must learn the set of destinations reachable through its connection to the virtual router; this may be as simple as a default route. Virtual routers participating in a single VPN domain are responsible for learning and disseminating VPN reachability information among themselves. A given VR holds the routes only for the specific VPN configured for that VR. Any routing protocol can be used between the VRs and the CEs.

5. How VPNs are built and deployed using VRs

Three main VR deployment scenarios can be used for building virtual private networks:
1) VR to VR connectivity over a layer 2 connection.
2) VR to VR connectivity tunneled over an IP or MPLS network.
3) Aggregating multiple virtual routers over a "backbone virtual router," which will provide connectivity over a layer 2, IP, or MPLS network.

The above VR deployment scenarios can coexist on a single PE and they are not mutually exclusive.

5.1 VR to VR Connectivity over Layer 2 Connections

As illustrated in figure 2, virtual routers can be deployed over direct layer-2 frame relay or ATM connections or other layer-2 transport technology.

```
+-----+ |               |            |               | +-----+
|VPN-A| | +----+        Layer-2 connections   +----+ | |VPN-A|
|sites|-|VR-A|<-------------------------------->|VR-A|--|sites|
+-----+ | +----+        |  --------  |        +----+ | +-----+
     |        |               |              |              |
     |{- Layer-2}-|        |{(Backbone)}|        +----+ | +-----+
+-----+ | +----+        |  --------  |        |VR-B|--|sites|
|VPN-B| |VR-B|                  |VR-B|--|VPN-B|
|sites| +-----+<-------------|--------|-------|+-----|
+-----+ |               |            |               | +-----+
```

Figure 2: VR to VR connectivity over a layer-2 backbone
This type of VR deployment allows direct quality of service engineering on a per-VPN connection basis. The connections can be statically configured or dynamically established.

5.2 VR to VR Connectivity through IP or MPLS tunnels

Virtual routers can connect over an IP or MPLS backbone. In a manner analogous to layer-2 transport, they can use the backbone to support tunneled connections among the VRs. The topology can be described similar to that for layer-2 transport, as in figure 2.

Although it is clearly possible to use a topology similar to the layer-2 model over an IP or MPLS backbone, the VR capability can support a different network deployment besides full mesh tunnels between VRs. This is the creation (on each PE) of another VR facing into the backbone network, which is used to build a kind of backbone VPN that may be shared among multiple customer VPNs. This is described below as the "backbone VR."

5.3 Virtual Router Backbone Aggregation

Another typical VPN configuration consists of connecting multiple virtual routers to the backbone through the use of a single virtual router (figure 3). For easy reference in the following sections we call this single virtual router "the backbone virtual router" or "the backbone VR."

The backbone virtual router is not functionally different than other virtual routers. It is only a virtual router that is configured and deployed in a special configuration.

```
      PE                    PE
+-----+                    +-----+
|VPN-A| +-----+  +-----+  +-----+
|sites| | VR-A | | VR-B | | sites|
|      | | VR-1 | | VR-2 |
+-----+ | (Backbones)  +-----+  +-----+
|VPN-B| | VR-B | | VPN-B|
|sites| | sites| | sites|
|      | |      | |      |
+-----+ | |      | |      |
      +-----+  +-----+

MPLS/IP based Tunnels

Figure 3: VR-1 and VR-2 used as backbone VRs
```

The backbone virtual router connects each PE to a shared backbone infrastructure. Backbone virtual routers can be deployed over ATM, FR, IP, or MPLS networks. Since the backbone VR allows the aggregation of VRs from multiple VPNs, backbone configuration can
remain unaffected as new VPNs or VPN sites are added. The relationship between the VRs and the backbone VR is an overlay relationship.

Note that although the concept is described above using a single backbone VR, there may be multiple backbone VRs per PE.

5.3.1 Tunneling

VPN data and routing information is tunneled through the use of IP or MPLS based tunnels (e.g., IPsec, GRE, IP in IP, MPLS). Depending on the tunnel technology used, the tunnels can be statically configured or dynamically established. The tunnel appears to VRs as a point-to-point link. Traffic sent through the tunnel, and forwarded by the backbone VR is opaque to the underlying backbone technology used.

A tunnel can be established per VPN or shared among many VPNs (VRs). The tunnel can originate from the backbone virtual router or from the VRs. This can provide an opportunity for service differentiation, in which a service provider can offer a higher level of service (at a higher price point) for individually mapped VPN connections among a customer’s VRs.

The backbone VR makes it appear as if each VR within a VPN is directly connected (full and partial mesh configurations supported). Each VR within the VPN exchanges routing information directly with the other VRs in the VPN.

VPNs may use different type of tunnels for inter-VR connectivity. Some sites may use MPLS as their tunnel technology of choice. Other sites (which transit through non-secure domains) may choose to use IPsec to encrypt their data.

The scalability and security of dynamic tunnel establishment between VRs will be enhanced by the ability to exchange a VPN-ID. [VPN-BGP] supports auto-discovery of the VPN-ID within BGP-based networks. Further work is needed to determine the requirements and usage of the VPN-ID exchange within IPsec-based tunneling scenarios.

5.3.1.1 MPLS Tunnels

MPLS tunneling can be used in different forwarding scenarios. A hierarchy of two labels can be used. One simple forwarding scenario is where the inner label identifies the VR intended to receive the private packet (to be forwarded to the CE). Another forwarding scenario is to distribute the inner label on a per-VPN basis across the tunnel. In this case the label distribution process can be achieved using BGP or an existing label distribution protocol on a per-VPN basis. The inner label relates to the private VPN prefix. The label and reachability distribution is done through the tunnels.
On the egress side traffic will be directed to the egress interface by looking up the inner label.

5.3.1.2 IPSec Tunnels

IPSec is needed when there is a requirement for strong encryption or strong authentication. It also supports multiplexing and a signalling protocol - IKE. IPSec tunnels can be established between two VPN sites across the backbone (originating from the backbone VRs).

5.3.2 Routing

The backbone VR exchanges backbone routing information with other backbone entities (P routers and possibly other backbone VRs). The backbone routing is separated from the customer VPN routing.

Virtual routers can run any routing protocol on their local VPN domain. Both static routes and dynamic routing protocols such as RIP, OSPF, and BGP-4 can be used. VPN sites exchange routing information through the tunnels over the backbone.

If a backdoor link is used between VPN sites running any IGP, then by adjusting the backdoor link costs appropriately, the backbone link can be favored for forwarding VPN traffic. By lowering the weight, the backdoor link can be used as a backup link in case the backbone path fails.

5.3.3 Relationship between the VRs and the Backbone VR

The routing domain of a set of VRs participating in a single VPN has no relation to the routing domain of the backbone VR. The backbone VR is not necessarily aware of the routing instances running on each private virtual router. However, because the backbone VR is also a virtual router, it can build routing relationships with other VRs if needed.

5.3.4 Multiple Backbones connected to a single PE

Figure 4 illustrates an example where multiple backbones are connected to the same PE. This type of configuration can be used when the PE is connected to multiple service provider backbones, or when the service provider offers different VPN services for different types of backbones.
6. VPN Auto-Discovery

The virtual router approach explicitly separates the mechanisms used for distributing reachability information from mechanisms used for distributing VPN topology and membership information. VPN membership information refers to the set of PEs that have customers in a particular VPN. VPN topology represents the set of PEs and their interconnectivity within the VPN. The topology can be a full-mesh of PEs, a hub and spoke, or anything in between. Dynamic topology can also be handled due to on-demand VPN customers.

VPN discovery can be achieved through different mechanisms, for example:

- Directory server approach, in which VRs query a server to determine their neighbors.
- Explicit configuration via a management platform.
- Piggybacking VPN membership and topology information using existing routing protocols (e.g., BGP) [VPN-BGP].
- Other VPN membership and topology auto-discovery approaches.

The above mechanisms can be combined on a single PE. As an example, for some VPNs topology discovery is done only through a management platform. For others, dynamic topology discovery is achieved using existing routing protocols.
In this document it is assumed that a mechanism that provides services similar to BGP is used to achieve auto-discovery of VPN members. As described in [VPN-BGP], VR addresses are exchanged, along with the information needed to enable the PEs to determine which VRs are in the same VPN ("membership"), and which of those VRs are to have VPN connectivity ("topology"). Once the VRs are reachable through the tunnels, routes ("reachability") are then exchanged by running existing routing protocols on a per-VPN basis across the tunnels.

It is important to note that, for the VR architecture, the auto-discovery mechanism is only used to automatically exchange VPN control information between VRs. It is not intended for piggybacking VPN private reachability information onto the backbone routing instance, as is done in [VPN-RFC2547bis], for example.

7. VRs and Extranets

Extranets are commonly used to refer to a scenario whereby two or more companies have network access to a limited amount of each other’s corporate data. An important feature of extranets is the control of who can access what data, and this is essentially a policy decision. Policy decisions are enforced at the interconnection points between different domains [VPN-RFC2764]. The enforcement may be done via a firewall, a router with access list functionality, or any device capable of applying policy decisions to transit traffic.

In the VR architecture, policy can be enforced between two VPNs, or between a VPN and the Internet, in exactly the same manner as is done today without VPNs. For example, two VRs (VPNs) could be interconnected, with each VR locally imposing its own policy controls, via a firewall or other enforcement mechanism, on all traffic that enters its VPN from the outside (whether from another VR or from the Internet). Combining firewalls and exchanging private routes between VRs (members of different VPNs) provide a flexible mechanism to build different flavors of extranets.

8. VPNs across Domains

It is possible that a VPN may cross multiple domains administered by different service providers. In the VR model, tunnels are used to provide intra-VPN connectivity across the backbones. The main requirement on the service provider in order to achieve end-to-end cross-domain VPN connectivity is the ability for both domains to support a common tunnel technology. Once the tunnel is established, private data (e.g., routing information, and private customer data) can flow from one domain to the other with the same level of security as is provided in a single service provider network. Another possible scenario is to use two virtual routers configured on each PE at the interconnection point. Each VR will use policy
decisions and firewalling to control VPN traffic transiting from one domain to the other.

The ability to use a standard VPN-ID format also allows unambiguous VPN identification across domains.

9. Internet Access

The same link attaching the CE to the VR can be used to provide Internet access to the VPN sites. The VR operations are decoupled from the mechanisms used by the customer sites to access the Internet.

There are a number of ways to provide Internet access to a VPN using the VR model. One way of providing VPN Internet access is to configure the backbone VR to steer private traffic to the VPN VR, and Internet traffic to the normal backbone/Internet forwarding table. The backbone VR can hold the Internet routes (so it will not be necessary for the VPN VRs to handle them). Firewalls should be used to secure the access (with the ability to use NAT).

Other options are also valid. One may want to have a particular VR handling Internet access only (rather than going to the backbone VR), or a default route to an Internet gateway can be used.

10. Carrier’s Carrier Case

It is possible that a VPN service is also a network of a service provider offering VPN services. Different options can be used to implement the VPN hierarchy.

In one approach, tunnels are built from the VPN edges to the CEs, and the VRs transparently provide VPN service to the remote CEs. This can be useful in the case where the CEs are themselves VRs and the service provider is also outsourcing the management of his customer VPN services.

Another case is where the remote VPN services are completely transparent to the VRs (on the PEs). This is the default case. It is up to the VPN network to distribute VPN reachability across the CEs.

Another option is for the VPN service to implement the VR architecture. In this option, the VPN Backbone VRs appear as CEs to the VRs configured on the PEs.

11. Operations and Management

Each VR operates independently, and can be individually reconfigured without affecting other VRs on the same PE. In some implementations, it may be possible for a VR to be "rebooted" by a customer without affecting other VRs. In case of PE failure (e.g., migration, upgrades, etc.), the service provider may want to control
and decide what VPN services get reestablished first. This particular point is important when a large number of VPNs is supported on the PE where each VPN service has different service availability requirements.

Since each VR operates as an independent router, it is possible for the management of the VRs to be outsourced. VPN customers may choose to configure (or perhaps only to monitor) the VRs that make up their VPN. It is also possible that the backbone VRs could be managed by a separate entity.

11.1 Backbone Migration

One benefit in using multiple backbone virtual routers is the ability for the backbone network administrator to migrate its backbone from one core technology to another with minimal disruption to VPN services. Conversely, a VPN configuration change or a VPN-software upgrade is totally transparent to the backbone protocol and policies (this is due to decoupling the VPN routing protocol from the provider backbone routing protocol).

11.2 Troubleshooting

The service provider or the VPN customer can use all existing troubleshooting tools on a per-VPN basis (e.g. ping and traceroute). As an example, a VPN customer may be able to telnet to its own VR and perform some troubleshooting operations. In this particular case, the service provider can configure for each VPN customer restricted privileges over the virtual router associated with the customer VPN network. This access may provide only the privilege to monitor (with no privilege to change) the layer 3 status of the customer’s VPN. The service provider may be able to offer VPN customers an SNMP-based method for read-only access to information about their own VPN. However, backbone topology information is completely hidden to the VPN VR, and therefore to the service provider’s customer.

12. Quality of Service

This architecture can utilize a variety of Quality of Service mechanisms. QoS mechanisms developed for physical routers can be used with VRs, on a per-VR basis, including classification, policing, drop policies, traffic shaping and scheduling/bandwidth reservation. The architecture allows separate quality of service engineering of the VPNs and the backbone.

13. Scalability

Only the PEs are handling the VPN type information. The internal backbone routers (the P routers) are usually not VPN aware. Furthermore, virtual routers allow multiple private CE-based networks to connect to a single PE.
One advantage of the ability to contain the VPN address space and VPN routing and forwarding capabilities within the virtual router entity is the possibility to distribute PE system resources on a per-VPN basis. Indeed, as an example, different scheduling mechanisms can be used for processing each VPN activity within the PE. This type of per-VPN resource management contributes to establishing a wide range of priority schemes among the VPNs within the PE.

### 14. Security Considerations

Various levels of data, routing and configuration security can be implemented. Any existing security-related mechanisms supported by existing routing protocols (e.g. authentication) can be used unmodified in the VR architecture. If IPSec tunneling is used as the tunneling protocol, then both the control and data traffic that travels over the tunnel can be secured; so that routing specific security enhancements are not needed. Any private routing, forwarding and addressing manipulation is done within the virtual router context. Direct layer-2 connections (ATM, FR), or specific tunneling mechanisms can also provide various levels of data security.

### 15. Document Change History

Version -03:
Document change history section added.
References updated.
Author information updated.
Section 5.3.1 - Paragraph on VPN-ID exchange added.
Version -04:
Separated Normative and Informative references.
16. Normative References


17. Informative References


18. Acknowledgments

The authors would like to acknowledge the following individuals for their helpful comments and suggestions: Bilel Jamoussi, David Hudson, David Drynan, Ru Wadasinghe, Scott Larrigan, Peter Ashwood-Smith, Martin Pepin, Ahmad Khalid, Don Fedyk, Keerti Melkote, Ron Bonica, Jerry Sydir, Mark Duffy, and Benson Schliesser.
19. Author’s Addresses

Document Editor  (Please send comments to editor.)
Paul Knight
Nortel Networks
600 Technology Park Drive
Billerica, MA 01821 USA
Email: paknight@nortelnetworks.com
Phone: +1 (978) 288 6414

Hamid Ould-Brahim
Nortel Networks
P O Box 3511 Station C
Ottawa, ON K1Y 4H7
Canada
Phone: +1 (613) 765 3418
Email: hbrahim@nortelnetworks.com

Gregory Wright
Nortel Networks
P O Box 3511 Station C
Ottawa, ON K1Y 4H7
Canada
Phone: +1 (613) 765 7912
Email: gwright@nortelnetworks.com

Rainer Bach
T-Data
Hans-Guenther-Sohl-Strasse7
40235, Duesseldorf
Germany
Phone: +49 211 694 2420
Email: Rainer.Bach@telekom.de

Abraham Young
Huawei Technologies Co., Ltd.
Kefa Road
Science-Based Industrial Park
Nanshan District, Shenzhen 518057
China
Phone: +86-755-6540808
Email: abyoungh@huawei.com

Chandru Sargor
Cosine Communications
1200 Bridge Parkway
Redwood City, CA 94065
USA
Phone: +1 (650) 637-2416
Email: Chandramouli.Sargor@cosinecom.com

Internet-Draft  draft-ietf-ppvpn-vpn-vr-04.txt  May 2003

Luyuan Fang                           Dr. Christian Weber
AT&T                                  Arcor AG & Co.
200 Laurel Avenue                     Koelner Strasse 5
Middletown, NJ 07748                  65760 Eschborn
USA                                   Germany
Phone: +1 (732) 420-1921              Phone: +49(0)69-2169-3973
Email: Luyuanfang@att.com             Christian-Weber@arcor.net

Full Copyright Statement

"Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to
others, and derivative works that comment on or otherwise explain it
or assist in its implementation may be prepared, copied, published
and distributed, in whole or in part, without restriction of any
kind, provided that the above copyright notice and this paragraph
are included on all such copies and derivative works. However, this
removing the copyright notice or references to the Internet Society
or other Internet organizations, except as needed for the purpose of
developing Internet standards in which case the procedures for
copyrights defined in the Internet Standards process must be
followed, or as required to translate it into languages other than
English.

The limited permissions granted above are perpetual and will not be
revoked by the Internet Society or its successors or assigns.
This document and the information contained herein is provided on an
"AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING
TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING
BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION
HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.