Lambda Net
on your wavelength

White Paper

Keep it Simple with BGP/MPLS Virtual Private Networks

Joël Repiquet

May 2002

www.lambdanet.net

info@lambdanet.fr

Contents

List of Figures

1. Introduction

BGP/MPLS VPNs are simple, scalable and as secure as ATM- or FR-based VPNs. They are fundamentally simple for the Customer because conventional IP routing is used, there is only one external routing peer per site, and they do not require any additional skills. Still, any choice regarding traffic flows and logical topology of the VPN is in the hand of the Customer.

BGP/MPLS VPNs are standardised in RFC2547bis ([1]) that is still a draft, but is fully adopted and implemented by major Vendors, especially Cisco and Juniper. This new VPN approach is based on two leading protocols – BGP and MPLS – that benefit from the most investigations in the IP World.

The purpose of this paper is to help the potential customers of IP VPNs grasp the essential aspects of this new approach. Therefore, it does not go deeply in the details but the fundamental characteristics are highlighted and illustrated accurately. The recommended reading for going further in the understanding of BGP/MPLS VPNs is the RFC2547bis itself which exposes clearly the concepts and which only drawback is to have no illustrations.

This paper is structured as follows:

- The Peer model, followed by BGP/MPLS VPNs, is briefly compared to various forms of Overlay model in Section 2.
- The various ways Customer sites can be defined are analysed at the beginning in Section 3; then the different phases of site-to-site route distribution across the backbone are examined in turn; the objective is here to illustrate it consistently through a global view of both the backbone and different VPNs; as a consequence of the routing tables building, VPN data forwarding is shown.
- Section 4 is dedicated to the Carrier of Carriers advanced feature, which enables another Service Provider to use the VPN services of a Carrier as a transport service. This SP can be another BGP/MPLS VPN SP or even an ISP.
- More than one Service Provider can offer BGP/MPLS VPN services to the same Customer. Inter-Provider backbone is discussed in Section 5.
- VPN users will generally be offered an Internet access; how this can be realised is explained in Section 6.
- Finally, besides a list of acronyms and references, a glossary will help you remind some key definitions.

2. VPN Models

The term “IP Virtual Private Network” (IP VPN) refers to IP connectivity between a set of sites, making use of a shared network infrastructure. At the edge of each site, the router acting as a gateway with the provider network is referred to as the **CE** (Customer Edge) and the SP (Service Provider) device at which a CE connects is known as a **PE** (Provider Edge).

2.1. Overlay vs. Peer VPNs

Depending on CE routers’ IP routing adjacency, one can distinguish two VPN models: Overlay and Peer. For comparing them, we will assume a full-mesh topology.

- With the **Overlay VPN model**, IP routing adjacency occurs directly between CEs (thus creating some form of virtual backbone over the SP backbone). However, a CE can be connected to the SP network (to some PE) via various forms of adjacency, ranging from layer 1 to layer 3. This form of VPN is also referred to as CE-based VPNs since the VPN logic is concentrated at the CEs.
- With the **Peer VPN model**, a CE is the routing peer of a PE and does NOT have any routing adjacency with other CEs. As a result, it gains IP connectivity with the other sites via this PE router. This form of VPN is also referred to as PE-based VPNs since the VPN logic is concentrated at the PEs. They are also known as Network-Based VPN (NBVPN).

Figure 1 shows a synoptic of the two approaches. The dotted lines are to be understood as direct routing adjacencies. Two typical topologies are illustrated: VPN Red is full-meshed while VPN Blue is of the form Hub-and-Spoke (where Spoke sites communicate with each other only via Hub sites). In case of Hub-and-Spoke topology, the Hub site will normally offer redundant accesses to the Spoke CEs. Partial-meshed topology could be considered as well. The figure shows immediately that there will be less requirements in terms of processing and interfaces for the CE router with the peer model.

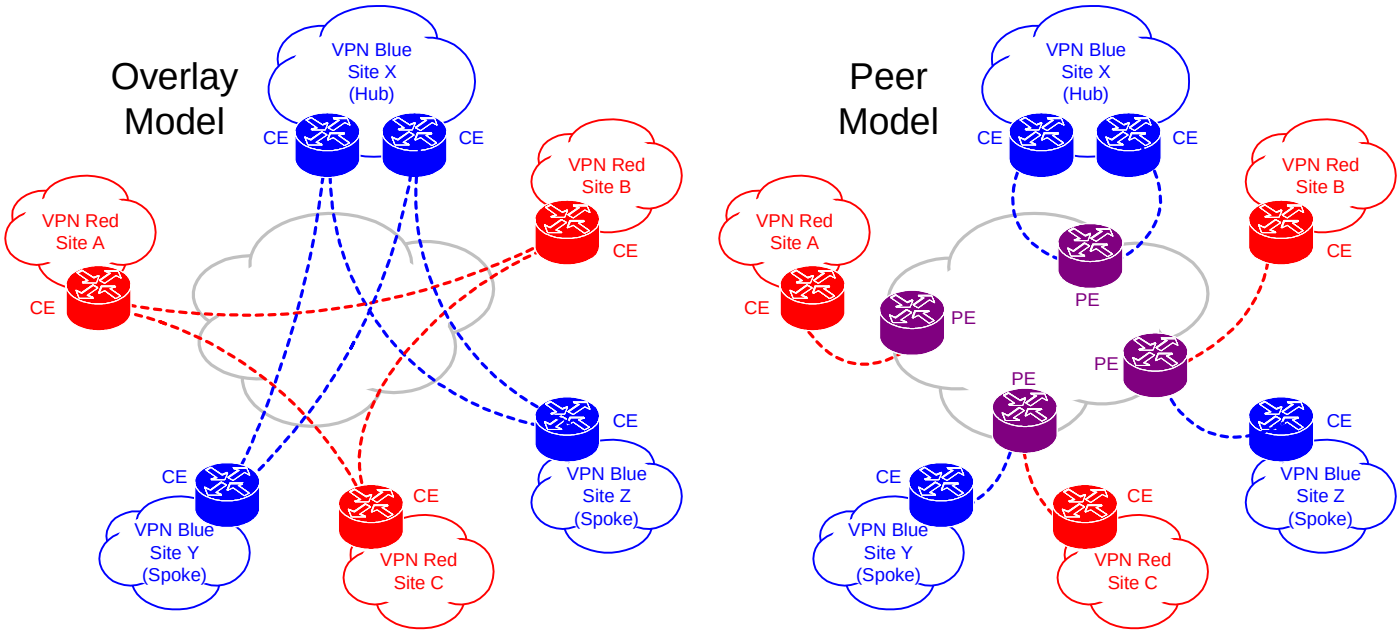


Figure 1: Overlay vs. Peer VPN Model

When the VPN Service Provider is responsible for the provisioning of the VPN, the VPN is referred to as PPVPN (Provider-Provisioned VPN). With CE-based PPVPN, the CE (as CPE: Customer Premises Equipment) must be part of the SP VPN offering. With PE-based PPVPN, there is no real CPE need since the CE acts as a normal router without any VPN-specific function; of course, the SP may offer the CPE option.

2.2. CE-to-CE Layering Chain

Prior to analysing the fundamental mechanisms of BGP/MPLS VPNs that apply to the Peer model, we illustrate briefly, under the form of protocol layering, inter-site communications with different approaches. An example of overlay model is considered for each level of CE-to-CE relationship (layer-1, layer-2 and layer-3). Finally the site-to-site communication is shown in case of BGP/MPLS VPNs.

Layer-1 CE-based VPNs

Here is the most basic CE-based VPN where CEs are directly connected at layer-1 level via PDH (E1, E3...) or SDH (STM-1, STM-4...) links. The access network and the backbone network may belong to different providers. The customer generally administers such a VPN since the Provider a priori has no specific involvement in IP services. It is simply mentioned here for comparison to the other types of VPN.

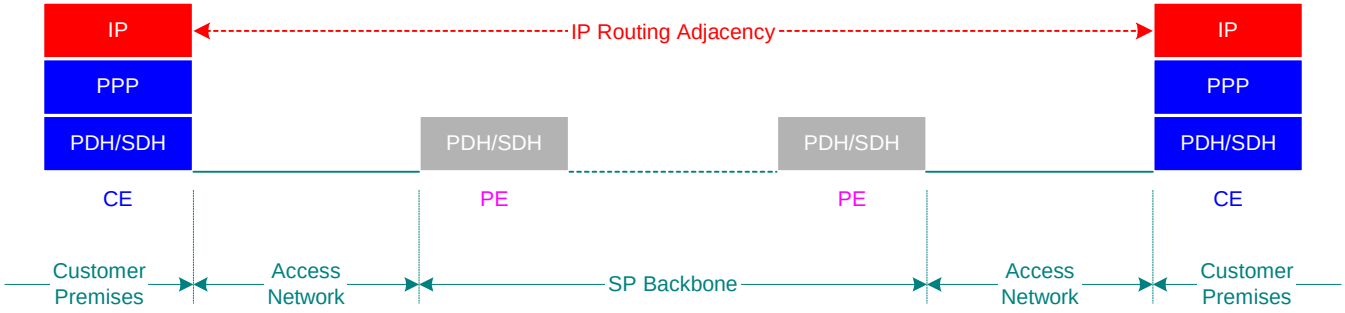
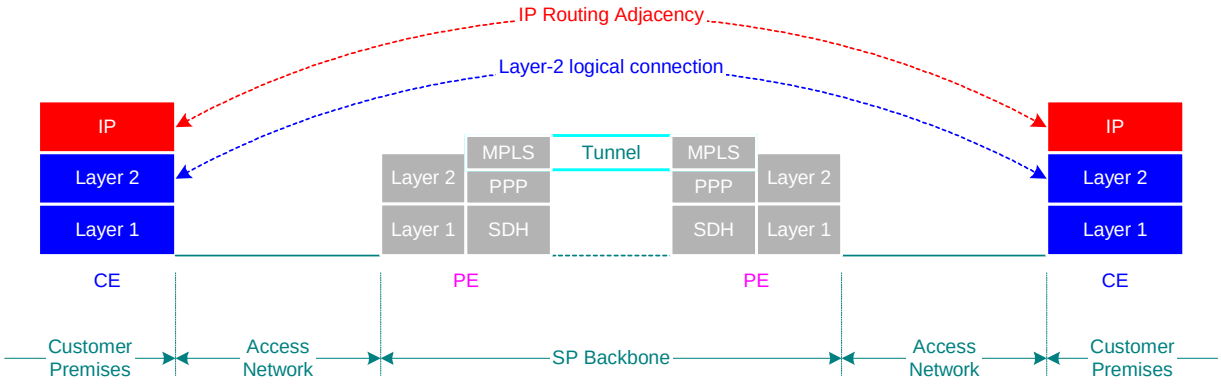


Figure 2: CE-to-CE layering chain with layer-1 CE-based VPNs

Layer-2 CE-based VPNs

Layer-2 CE-based VPNs have been introduced with ATM or Frame Relay provider backbones. The main advantage is that, conversely to layer-1 VPNs, several logical connections can be multiplexed over one physical access link. Nowadays, MPLS technology enables an SP to provide a data link service directly from its backbone router infrastructure. The figure hereafter illustrates such an MPLS-based data link service and it should be noted that the full set of interface types and capacities available on high-speed routers can be used on the access link between the CE and the PE. Besides ATM and FR interfaces, Ethernet with VLANs can be used. PPP or Cisco HDLC on PDH/SDH can also be used but in this case only one logical interface is possible within one physical interface; they are nevertheless mentioned because the advantage brought by MPLS is that the SP can offer (and price) only the required subrate of the physical interface bandwidth. Within the backbone, from PE to PE, the MPLS tunnels may be nested, thus improving the scalability of the solution.



	PDH	SDH	Ethernet
Layer 1	E1, E3, DS3	STM-1, STM-4...	10/100BT, GigE
Layer 2	ATM, FR, PPP, Cisco HDLC		VLAN 802.1Q

Figure 3: CE-to-CE layering chain with layer-2 CE-based VPNs (MPLS case)

Layer-3 CE-based VPNs

The logical connections between CEs can also be based on layer-3 IP tunnels, such as GRE (Generic Route Encapsulation, defined in RFCs 1701 and 1702) or IP-IP (IP encapsulation within IP, defined in RFC 2003). However, these solutions are prone to data spoofing and the overhead is at least 20 bytes per packet. IPsec-based solutions have therefore been preferred, the CE acting as a Security Gateway.

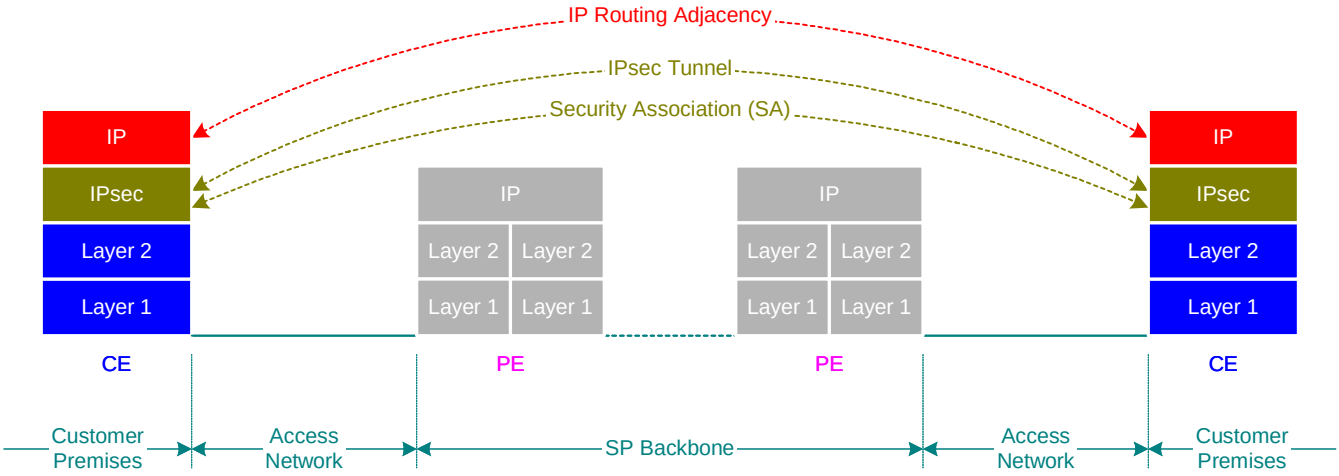


Figure 4: CE-to-CE layering chain with layer-3 CE-based VPNs using IPsec

The level of security that can be brought by IPsec in terms of authentication and confidentiality through the use of public key mechanisms is NOT questionable. However, here are some observations:

- Although IPsec in itself is well defined from end 1998 (in RFCs 2401 to 2412) there is no IPsec VPN standard defined yet. Surprisingly, the first standardisation effort (see [8]) is being carried out, at the IETF, within the frame of the PPVPN subgroup that defined BGP/MPLS VPN. Considering the so many options and combinations available with IPsec (tunnel vs. transport mode, AH vs. ESP headers, encryption algorithms, key exchange mechanisms...) the choice of an IPsec-based VPN SP entails some dependency between the Customer and the SP.
- IPsec adds a large overhead to each IP packet as well as significant processing time.
- It is not proved that strong security is required for the whole sites, and IPsec could advantageously be used at a finer grained level (e.g. subnet or host levels). Since IP connectivity is enabled between sites, IPsec can also be applied with any other form of VPN, including BGP/MPLS VPNs.

Layer-3 PE-based VPNs

Figure 5 illustrates the conventional IP peering between CE and PE, while PE-to-PE is based on both iBGP for VPN route distribution and hierarchical MPLS tunnelling for data forwarding. This is examined in more detail in the remainder of this paper.

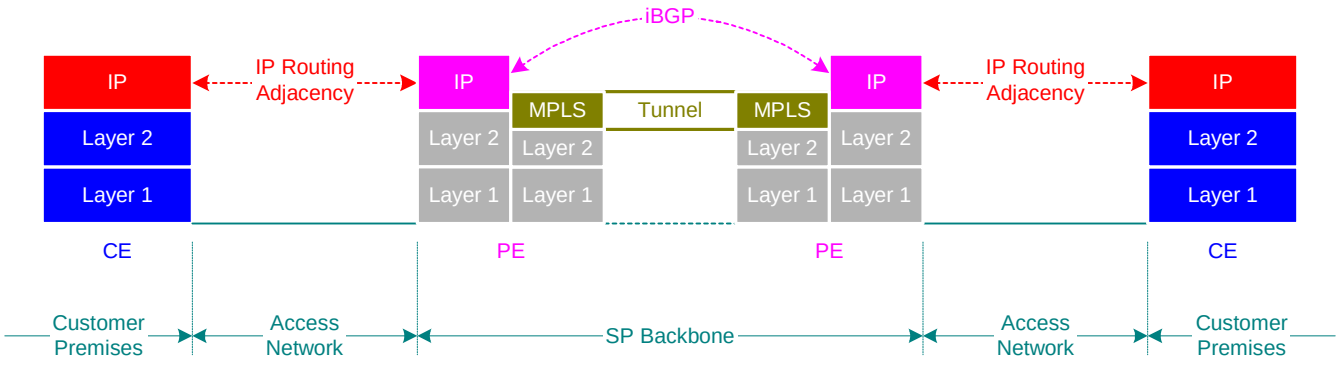


Figure 5: CE-to-CE layering chain with PE-based BGP/MPLS VPNs

3. BGP/MPLS VPNs Fundamentals

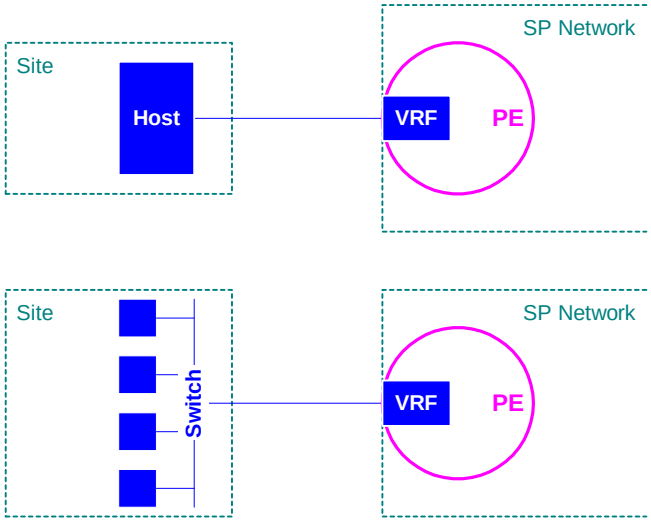
3.1. Sites and CEs

With BGP/MPLS VPNs, a set of sites is directly attached to an SP network. Those sites to which the SP provides IP connectivity by applying a routing policy constitute a VPN. From the perspective of the SP, a site represents a number of IP routes that it can learn over one or more sub-interfaces via a direct routing adjacency. The SP router to which a site can be attached is referred to as PE (Provider Edge). The customer equipment that is connected to the PE is known as a CE (Customer Edge).

The notion of Site and CE is worth refining because it extends the potential of BGP/MPLS VPNs.

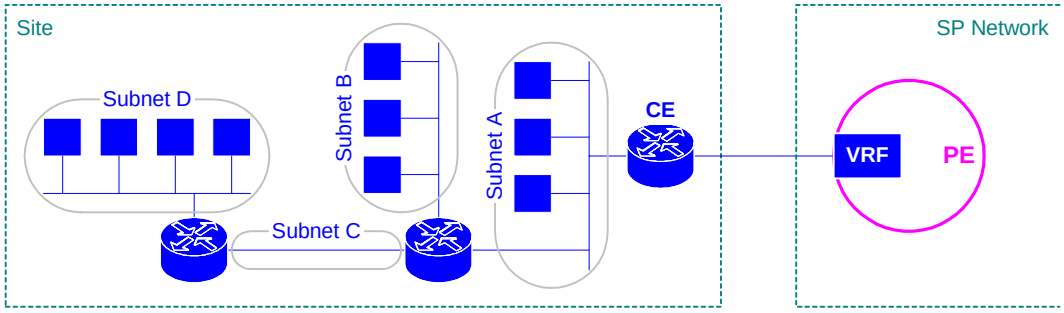
Host or Switch as CE

The CE may be a single host (for instance a server) or an Ethernet switch; it represents a single subnet and the SP directly declares it in the VPN routing instance (the VRF, as explained later on) at the PE. In this simple case, the Customer does not even need to install and manage a router at his site.



Physical Router as CE

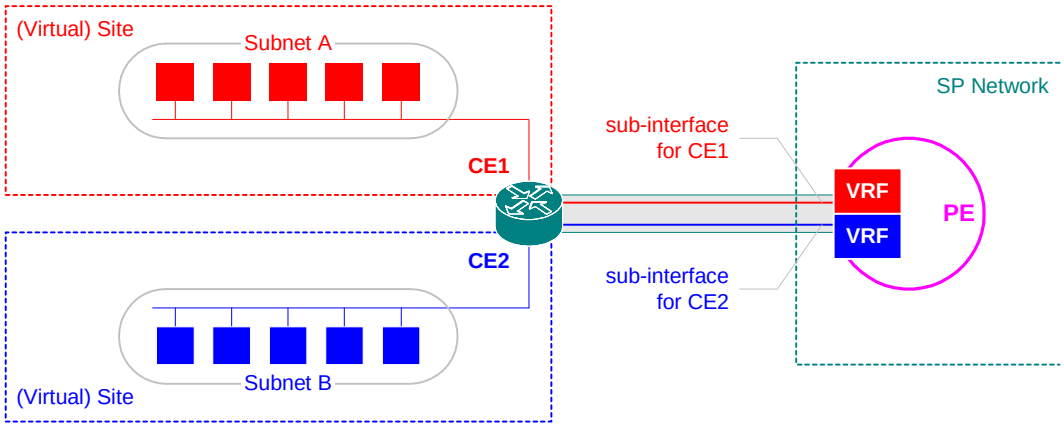
In most of the cases the CE will be a physical router that represents a number of subnets (or routes) as illustrated below. This gateway router will learn the site's internal routes via its IGP and will then advertise dynamically these routes to the PE to which it is attached.



It is likely that the systems in a site will be in the same geographical area. However, one could imagine Subnet D in the figure here above to be at a remote location. It will be part of the site since the VPN SP backbone is not involved.

Virtual Site

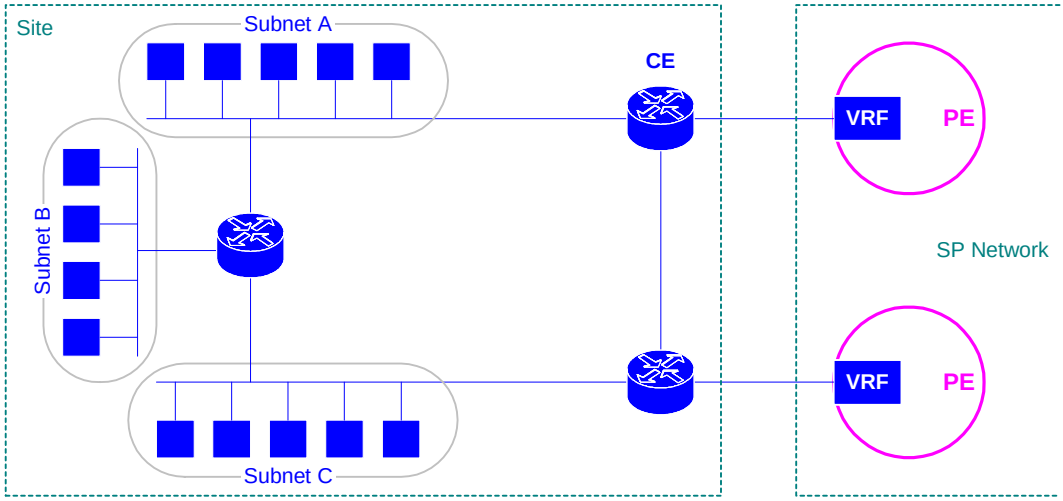
The interface at the PE (and the CE) for a CE-PE link is better to be seen as a sub-interface (or logical interface). There can be (with FR, ATM and VLAN layer-2 encapsulation modes) several sub-interfaces for the same physical interface. As a result, a physical CE router, through its physical connection to the PE, can represent several virtual sites (and be viewed therefore as several CEs) by splitting route subsets between separate sub-interfaces.



Some alternatives are possible: (1) use several physical interfaces instead of sub-interfaces within a single physical interface (it would be the only possibility anyway with PPP or Cisco HDLC encapsulation modes); (2) instead of a router, this could be realised with an Ethernet switch, via VLANs; (3) in some cases, instead of having the physical site split into several virtual sites, it can be up to a host to have its traffic dynamically routed towards the appropriate VPN sub-interface.

Resiliency in CE-PE Connections

For resilience, a site can be attached via more than one CE to one or more PEs (moreover, as this will be discussed at the end of this paper, to the same or different VPN service providers).



3.2. VPN Routing & Forwarding tables (VRFs)

Figure 6 shows a Service Provider network attached to a number of sites that represent 3 VPNs (Red, Blue and Green). Those routers within the SP network that are not attached to CEs are referred to as P (for Provider core) routers. We will base our explanations of BGP/MPLS VPNs mechanisms on this same global view; this model is inspired by a case study presented in reference [4] and will enable you to understand the various phases.

The customer administers its VPN and therefore assigns IP addresses throughout the sites. It is likely that these addresses will be within the private ranges defined in RFC 1918 (it could be non-globally unique public IP addresses as well). As a result, the same addresses could be assigned for different VPNs. This overlapping is enabled by BGP/MPLS VPNs.

As illustrated, Site 5 is part of two VPNs: there is an overlapping between VPN Blue and VPN Green. This is why the corresponding CE and VRF are shown in brown.

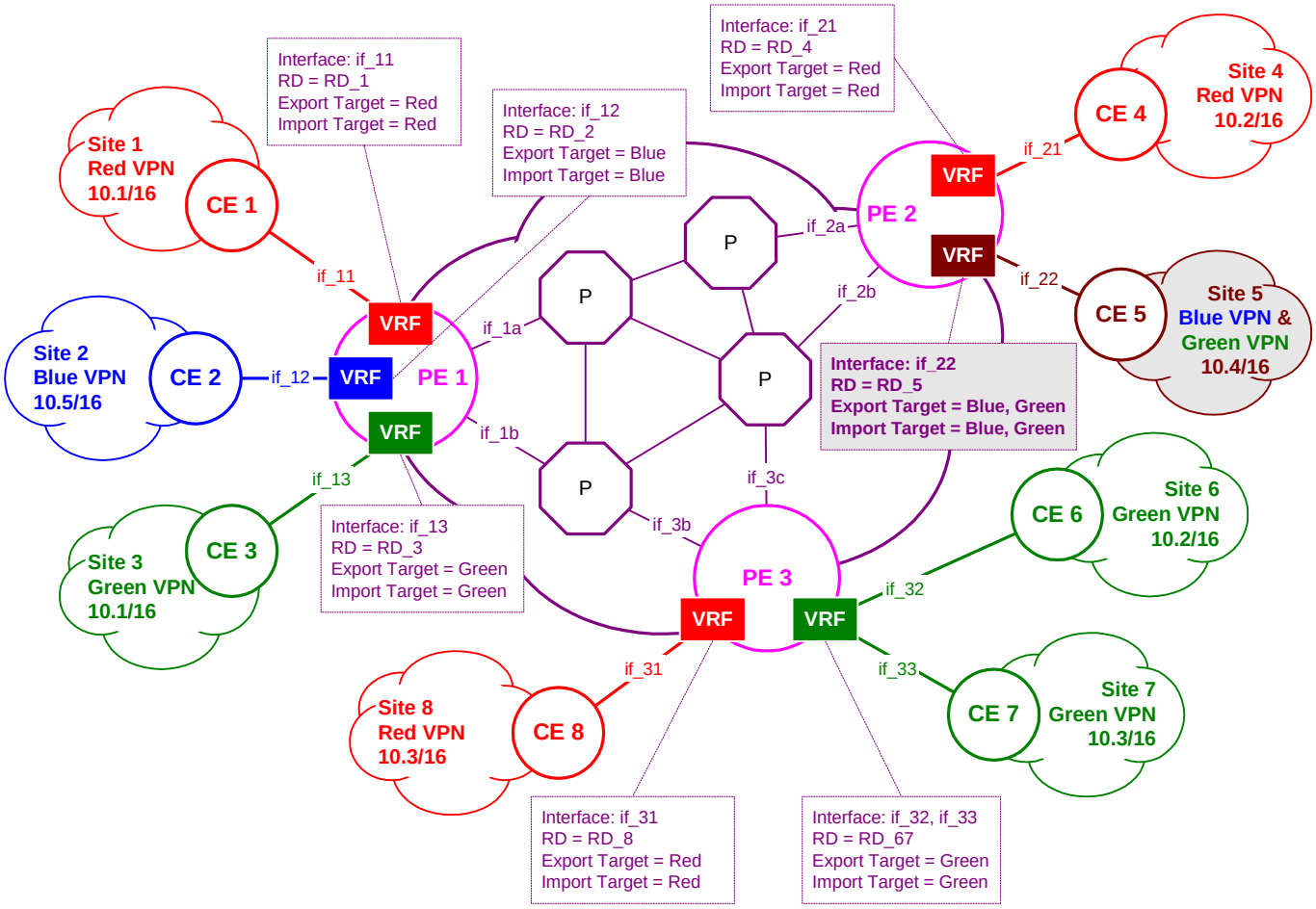


Figure 6: BGP/MPLS VPN – VPN Routing & Forwarding tables (VRFs)

At a PE, a VRF represents the context that is specific to an attached VPN; a VRF is primarily associated to (is identified by) the one or more sub-interfaces through which the sites belonging to this VPN are connected. In Figure 6 study case, all the VRFs have only one sub-interface but VRF Green at PE3 that has 2 sub-interfaces (those of Site 6 and 7). The other parameters that must be defined at VRF creation time are (1) the route distinguisher (RD) and (2) the route targets (RT) for the Import and Export policies; these parameters are used when the VPN private routes are distributed via the backbone to the other sites. The RDs enable the overlapping of addresses between VPNs while the RTs enable the distribution of VPN routes to the relevant remote sites.

3.3. Pre-established iBGP sessions and LSPs

For VPN sites to be attached and be operational, there are two prerequisites to be performed at SP network configuration time: (1) the establishment of internal BGP (iBGP) sessions between PEs and (2) the set-up of MPLS label switch paths between PEs. These two conditions summarize the fundamental mechanisms used by BGP/MPLS VPNs:

- On the Control plane: the use of BGP for the distribution of VPN routes through the SP backbone
- On the Data plane: the use of MPLS for the IP traffic forwarding itself, more exactly the transfer of VPN data through the SP backbone.

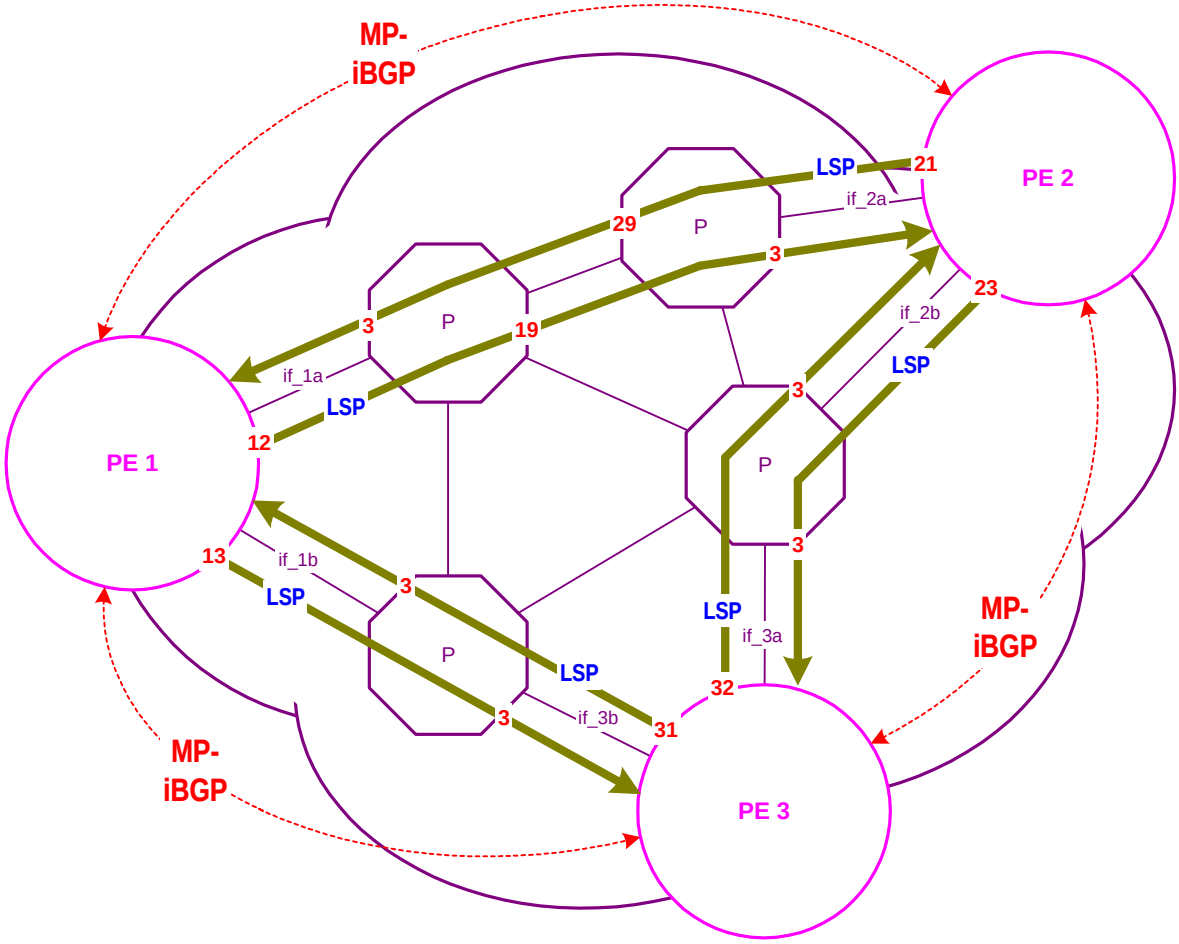


Figure 7: BGP/MPLS VPN – PE-to-PE pre-established iBGP sessions and LSPs

Multi-protocol BGP must be used for the sessions between PEs. However, this is no more a new feature and this functionality is integrated in the software of backbone routers. MP-BGP is required because it enables routers to convey other routes than the classical 4-byte IPv4 routes. As we will see later on, VPN routes are not distributed within the backbone as IPv4 routes; they are prefixed with the route distinguisher and are therefore 12-bytes long. Instead of a full-mesh of PE-to-PE iBGP sessions, route reflectors can be used for scalability. This point is not discussed further since it does not impact the logic of VPN routes distribution.

MPLS LSPs are unidirectional and therefore a pair of LSPs must be established between PEs (for QoS purposes, several pairs could be set-up with different queuing priorities). It should be noticed, in the perspective of the data transfer phase discussed later on, that the number shown at the ingress side of the LSP, represents the “outer” label. The labels shown at the egress side of a P router represents the “swap” labels (e.g. 19 and 29 between PE1 and PE2). The labels numbered “3” represent a special label value indicating that this P router is the penultimate hop in the path.

LSPs are established using either LDP or RSVP.

3.4. Control Plane – VPN Route Distribution

Distribution of VPN routes is shown in several phases: (1) from CE to PE (2) from PE to PE and (3) from PE to CE. It should be noted that, although the representation suggests some simultaneity for all sites, this process occurs either when a site is attached or detached (join and prune operations), or when some routes are added, modified or removed at a site.

CE to PE

From the customer perspective, routing occurs normally. Once agreed with the SP which sites are parts of which VPN and what is the logical topology – a full-meshed topology is enabled by default but the customer may want to restrict it to some partial-meshed topology – the CE peers with its PE and advertises its routes. The routing protocols may be interior routing protocols (RIP, OSPF) or BGP. It is also possible not to use any routing protocol and instead have static routing configured at each site. For clarification, we will assume in the remainder of this paper that dynamic routing is used.

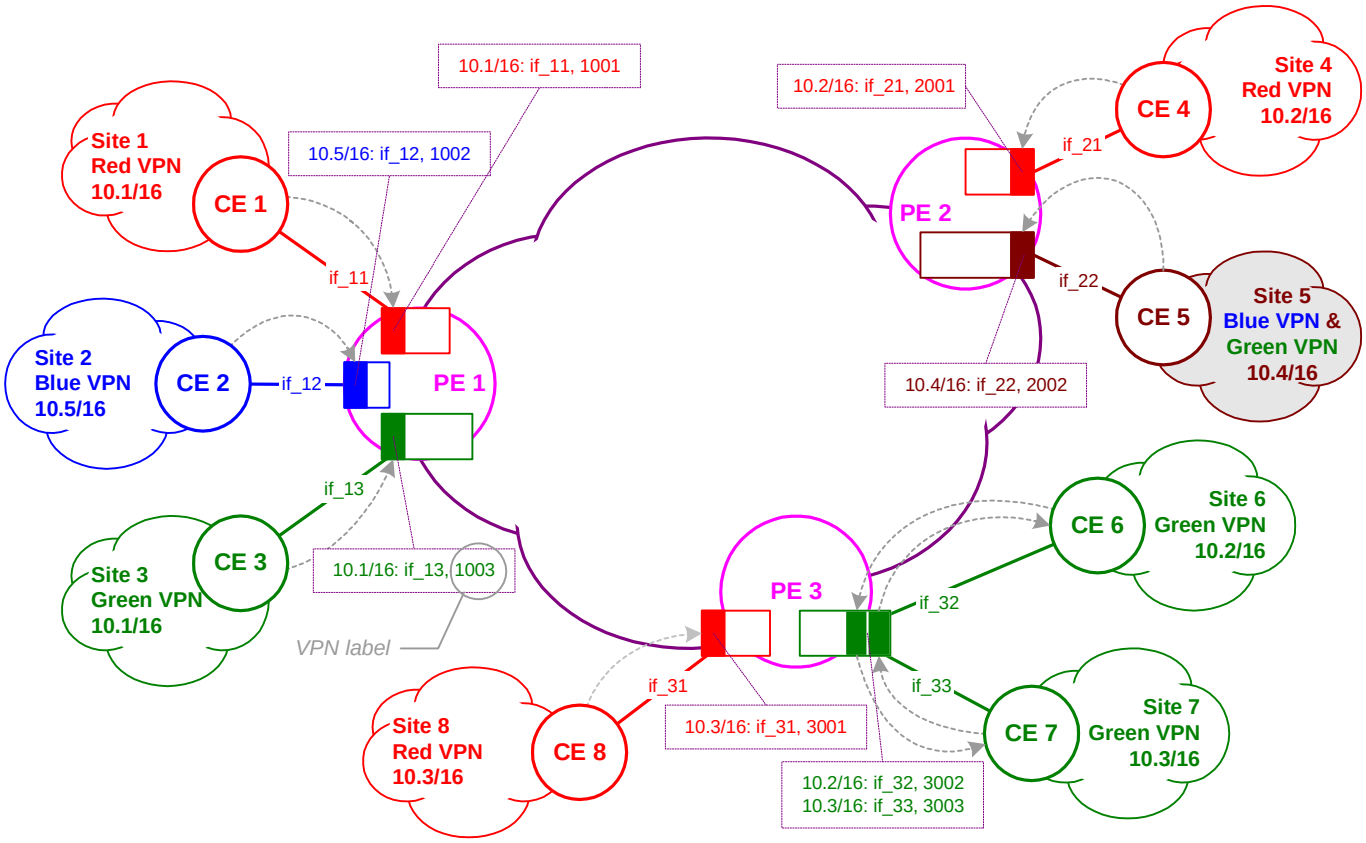


Figure 8: BGP/MPLS VPN – CE to PE Route Distribution

When the PE receives routes over a VRF sub-interface, it stores them in the associated VRF. These local routes are at the classical IP format (and are stored as such in the VRF). In the VRF, they are associated to the VRF sub-interface and are assigned a label value. This label is known as the "**VPN label**" (also known as "inner label" or "bottom label" in regards to its conveyance within the LSP). The VPN label value is a PE's local matter. It identifies the VRF sub-interface by which this route is learned. Hence, routes learned over the same VRF sub-interface will have the same label value. This will enable the PE when receiving traffic towards one of these routes to choose the suitable sub-interface.

When two sites (or more) attached to one PE are in the same VPN, they gain connectivity directly via the VRF that they share. This is illustrated on Figure 8 with Sites 6 and 7. In this figure, the VRF are "dimensioned" according to the number of routes they will eventually contain. At this stage, the local routes in the VRF are represented in plain colour. It should be noticed that for an overall understanding of the illustration, labels and VRF interfaces have been numbered consistently with the first digit corresponding to the PE number (e.g. if_31 and VPN label 3001 for CE8 connected to PE3).

PE to PE

Once the PE has learned local routes from its CEs, it will advertise them – **via BGP** – to the other PEs, according to the Route Distinguisher and Export Route Target(s) that were defined at VRF creation time (see Figure 6). First, the VPN routes could not be conveyed as such via BGP (since IP address overlapping can normally occur between VPNs) otherwise only one route would be kept, thus making the others unreachable. Routes are therefore prefixed with an 8-byte Route Distinguisher that typically consists of the SP's AS number plus the VPN identifier. Besides, the VPN label that was allocated to each local route must also be conveyed with this route. This is why we refer to the format of VPN routes when advertised through the backbone as **labelled VPN-IPv4 routes**. The VPN routes will also be flagged – **as extended BGP community attributes** – with their one or more Route Targets. Finally, the Next Hop BGP attribute value is the (advertising) PE loopback address itself.

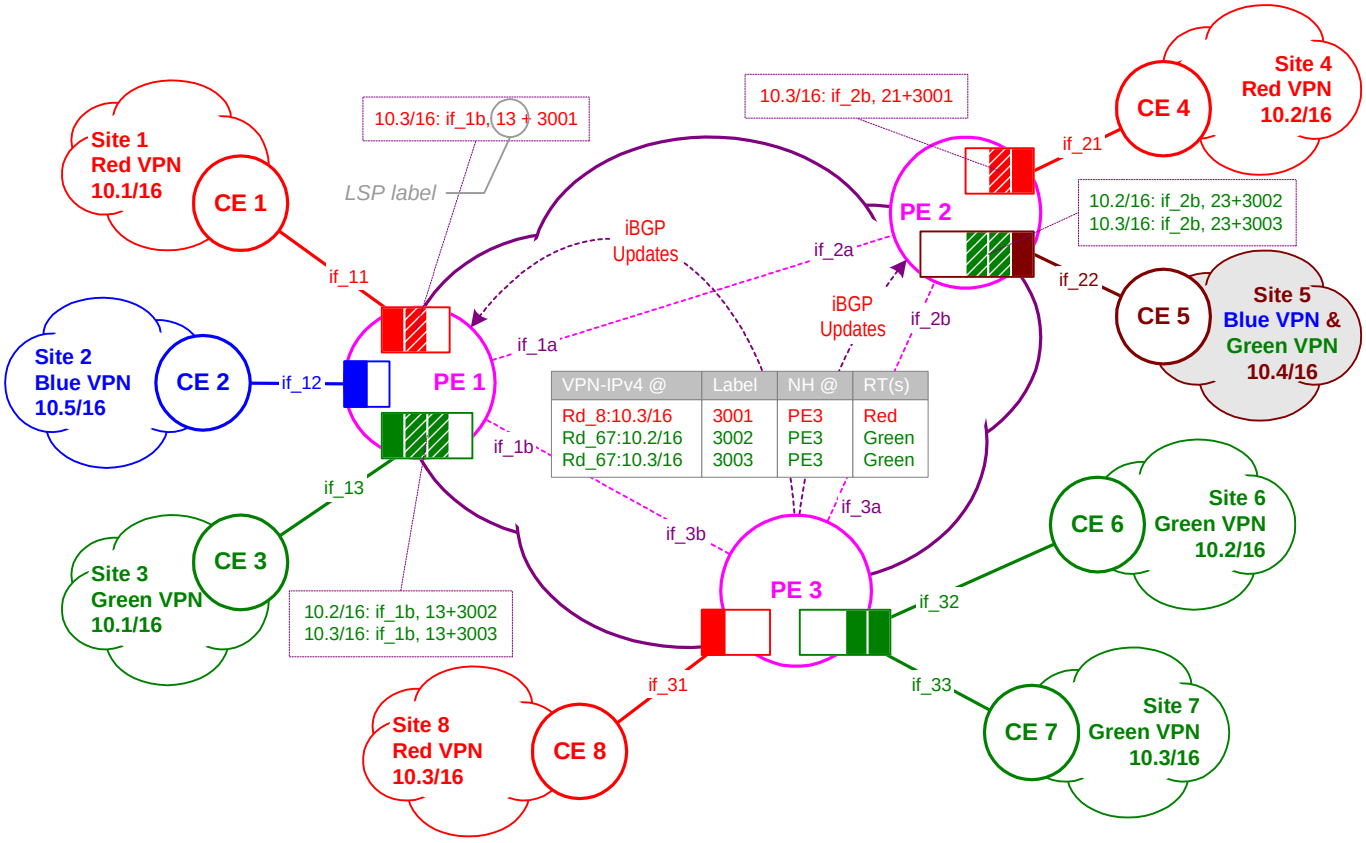


Figure 9: BGP/MPLS VPN – PE-to-PE Route Distribution

An example of the VPN route distribution from PE3 to other PEs is shown in Figure 9. PE3 exports the local routes of its two VRFs according to the RD and Export RT of each VRF. When PE1 and PE2 receive these BGP updates, they will filter the labelled VPN routes according to the Import Policy of each of their VRFs, before completing these VRFs with the relevant VPN routes.

In Figure 9, the remote routes in VRFs "Red" and "Blue" at PE1, as well as in VRFs "Red" and "Brown" at PE2, are shown with a different pattern (with transversal lines). They are stored in the VRF as IPv4 routes (the RD has been removed) along with the suitable interface and label stack (where the outmost label represents the LSP ingress label enabling this PE to reach the egress PE – as mentioned in the BGP Next Hop parameter – while the inner label is the VPN label just received with this VPN route).

Once all the VPN routes have been distributed through the SP backbone, all the VRFs of all the PEs contain both their local routes as well as the remote routes, as shown in Figure 10.

PE to CE

When a VRF at a PE is updated with a remote route, it advertises this route to the attached CEs that are associated to this VRF. As shown in Figure 10, there is then full IP connectivity between the sites belonging to the same VPN. For example Site 1 has learned via its peer PE (PE1) the routes from Sites 4 and 8. Similarly, Site 5, which is shared between VPN Blue and VPN Green, has learned routes from remote site 2 (Blue) as well as remote sites 3, 6 and 7 (Green).

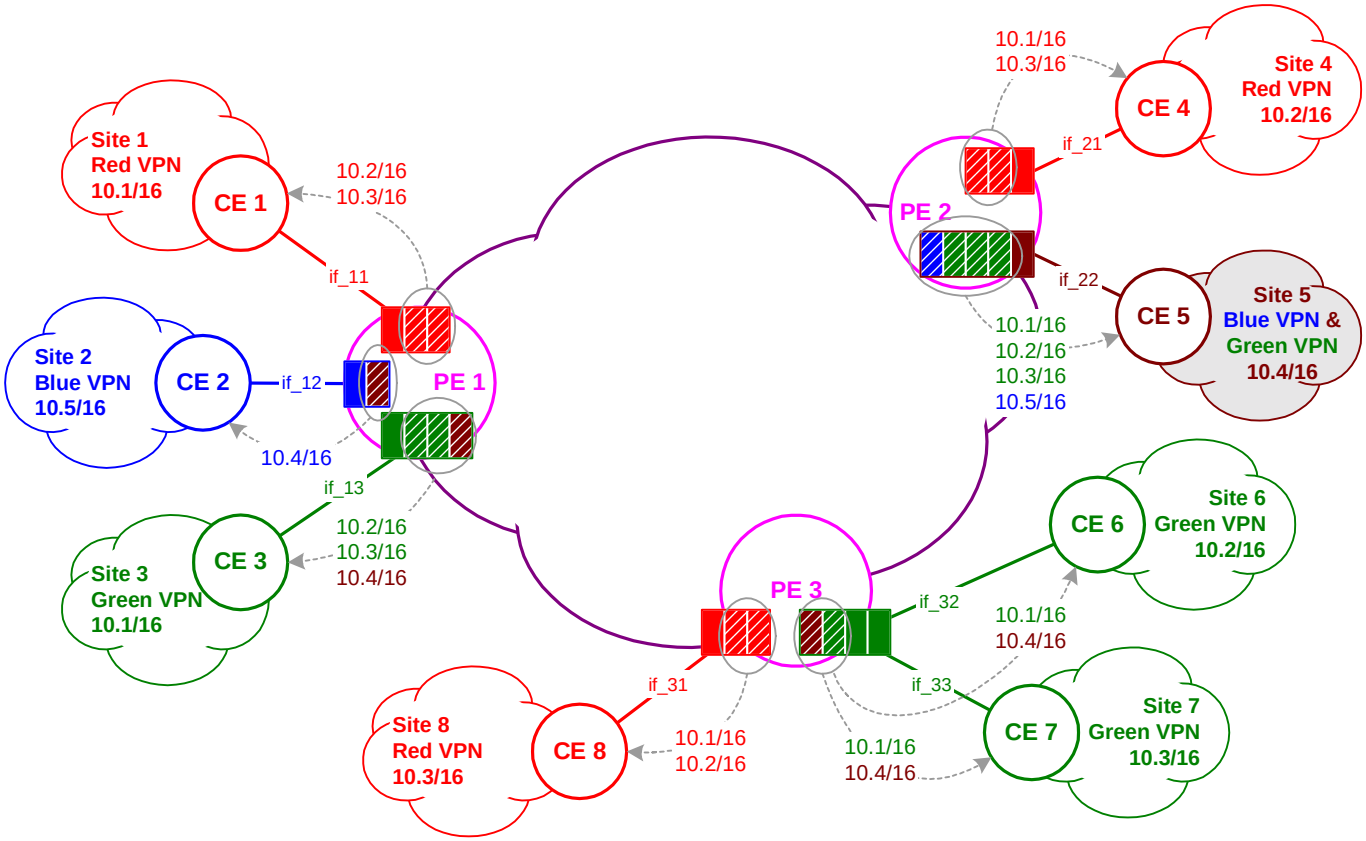


Figure 10: BGP/MPLS VPN – PE-to-CE Route Distribution

Here is a summary of the (logical) tables finally available at each VRF:

- Remote routes are shown in bold and shaded in grey
- There is no outer label for the local routes

PE1	Route	Output Interface	Outer Label	Inner Label
VRF Red	10.1/16	if_11		1001
	10.2/16	**if_1a**	**12**	**2001**
	10.3/16	**if_1b**	**13**	**3001**
VRF Blue	10.5/16	if_12		1002
	10.4/16	**if_1a**	**12**	**2002**
VRF Green	10.1/16	if_13		1003
	10.2/16	**if_1b**	**13**	**3002**
	10.3/16	**if_1b**	**13**	**3003**
	10.4/16	**if_1a**	**12**	**2002**

PE2	Route	Output Interface	Outer Label	Inner Label
VRF Red	10.2/16	if_21		2001
	10.1/16	**if_2a**	**21**	**1001**
	10.3/16	**if_2b**	**23**	**3001**
VRF Brown	10.4/16	if_22		2002
	10.1/16	**if_2a**	**21**	**1003**
	10.2/16	**if_2b**	**23**	**3002**
	10.3/16	**if_2b**	**23**	**3003**
	10.5/16	**if_2a**	**21**	**1002**

PE3	Route	Output Interface	Outer Label	Inner Label
VRF Red	10.3/16	if_31		3001
	10.1/16	**if_3b**	**31**	**1001**
	10.2/16	**if_3a**	**32**	**2001**
VRF Green	10.2/16	if_32		3002
	10.3/16	if_33		3003
	10.1/16	**if_3b**	**31**	**1003**
	10.4/16	**if_3a**	**32**	**2002**

3.5. Data Plane – Forwarding across the Backbone

Route distribution on the control plane has enabled the building of the VRFs and thus prepared the transfer of IP traffic between sites. Figure 11 illustrates two simultaneous data transfers: (1) from a host at Site 1 to, for example, some server at Site 4 (with IP address 10.2.4.2); and (2) from a host at Site 3 to some other server at Site 5 (with IP address 10.4.1.8).

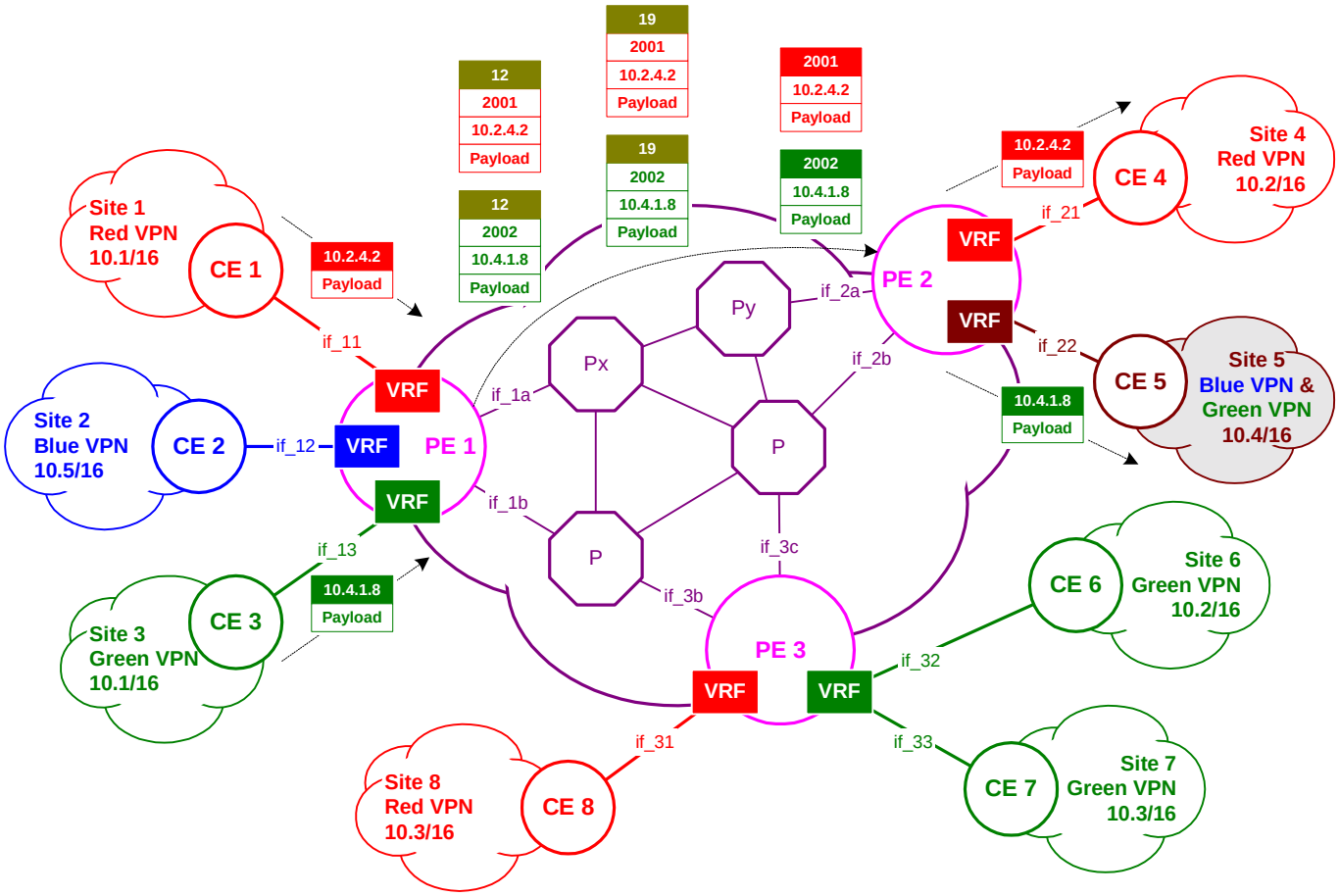


Figure 11: BGP/MPLS VPN – Forwarding across the Backbone

When the IP packet with destination address **10.2.4.2** is received by PE1 from CE1, the Red VRF is interrogated and the entry corresponding to **10.2/16** route indicates **if_1a** as output interface, **12+2001** as label stack, as well as (not shown) a data link header. The label stack is inserted in front of the IP packet, the data link header is inserted in front of the label stack and the resulting frame is queued on the output interface. Similarly, when the IP packet with destination address **10.4.1.8** is received by PE1 from CE3, the Green VRF is interrogated and the entry corresponding to **10.4/16** route indicates **if_1a** as output interface, **12+2002** as label stack, as well as (not shown) a data link header. The label stack is inserted in front of the IP packet, the data link header is inserted in front of the label stack and the resulting frame is queued on the output interface.

The two frames are sent on the LSP egress path (PE1's output interface: if_1a); at Px router, the top labels are swapped (19 replaces 12) and the labelled packets forwarded towards Py, which is the penultimate hop in the LSP. As a result, the outer labels are popped and the packets sent towards PE2 with only the inner label in front. At egress PE2, the relevant VRF sub-interface is retrieved from the VPN label and the original IPv4 packet is finally forwarded to the CE enabling you to reach the server within the site.

4. Carrier of Carriers

A BGP/MPLS VPN service provider is referred to as a **Carrier of Carriers** when its role is to deliver VPN services to another SP of which sites (typically POPs, but possibly regional networks) are geographically dispersed. This SP can be another **BGP/MPLS VPN SP** or an **Internet Service Provider (ISP)**. All the sites of the customer SP have the **same AS number**.

Figure 12 shows (in gold colour) a BGP/MPLS VPN SP as a customer (the SP). In this example, the sites are single POPs with only one router acting (1) as a CE vis-à-vis the Carrier's PE, and (2) as a PE in regards to its own customers. The SP's routers could be simply co-located at the Carrier's POPs.

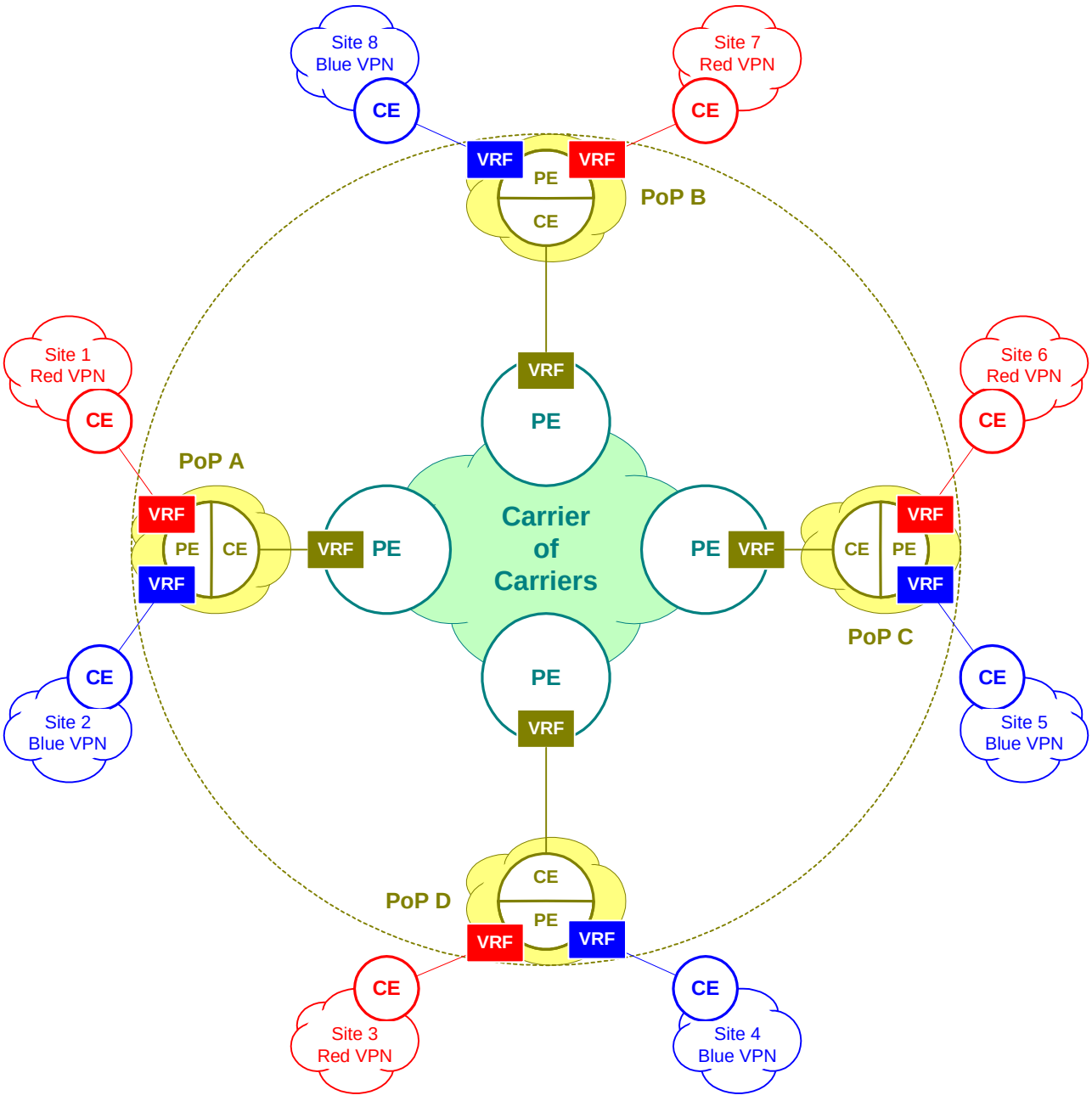


Figure 12: Carrier of Carriers – BGP/MPLS VPN SP as a Customer

With this method: (1) the SP needs only advertise – from CE to PE – its (few) **internal routes** to the Carrier; (2) MPLS is at least required between the Carrier and the SP at the CE-PE boundary; and (3) the SP establishes MP-iBGP sessions between its PEs for distributing its own **external routes**, i.e. labelled VPN IPV4 routes in case of a BGP/MPLS VPN SP, or the so-called "100,000" Internet routes in case of an ISP.

Figure 13 shows, in contrast to the previous case, an ISP as a customer. In this example, the sites are single POPs with only one router acting (1) as a CE vis-à-vis the Carrier's PE, and (2) as an ASBR (AS Border Router) in regards to its own customers, peering partners, or upstream transit providers.

Note: *This figure purposely does not represent a realistic localisation of the different types of AS peers. Instead, it reflects the logical organisation of Internet connectivity: upstream providers at the top, peering partners laterally, and customers at the bottom...*

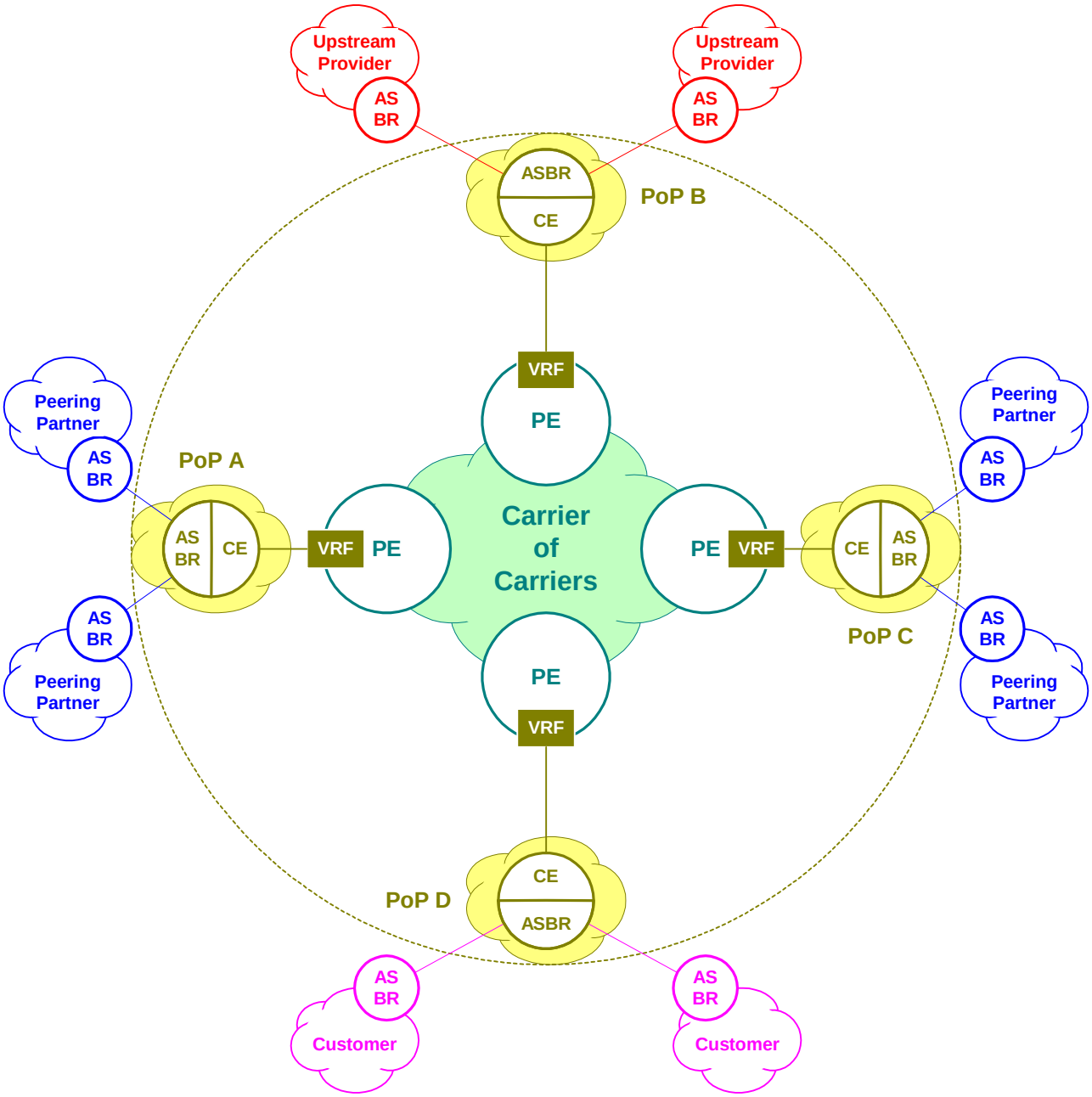


Figure 13: Carrier of Carriers – ISP as a Customer

5. Multi-Provider BGP/MPLS VPNs

A same BGP/MPLS VPN can be split over two (or more) service providers. These SP networks, which have different AS numbers, must therefore be interconnected, either directly (as shown in Figure 14) or via some transit service provider. Assuming that each SP has globally unique addresses, the preferred solution is (1) to use EBGP between border routers for the redistribution of labelled IPv4 internal routes; and (2) to establish multi-hop eBGP sessions for inter-provider PE-to-PE redistribution of labelled VPN IPv4 routes.

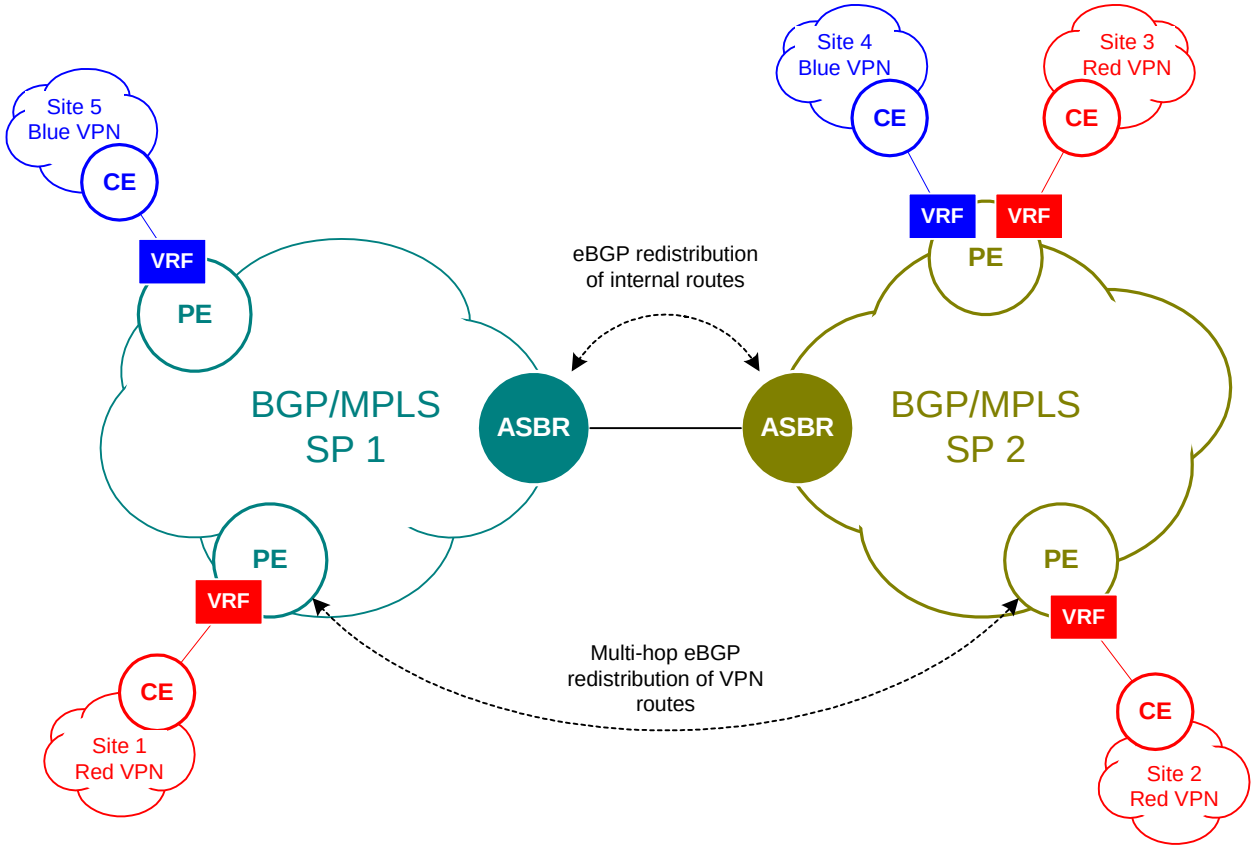


Figure 14: Multi-Provider BGP/MPLS VPNs – Direct Interconnection

In case a transit provider is used between the two BGP/MPLS VPN SPs, this transit provider can be either itself a BGP/MPLS VPN SP, or simply an MPLS-capable SP.

It should be noted that the eBGP solutions used for multi-AS operations (between different SPs) could be applied as well in the case of a single SP that has several AS numbers.

6. Accessing Internet from a BGP/MPLS VPN

6.1. Non-VRF Internet Access

A centralised Customer site with an Internet access via another interface to the same SP enables all VPN users, via a Firewall with NAT function, to access the Internet.

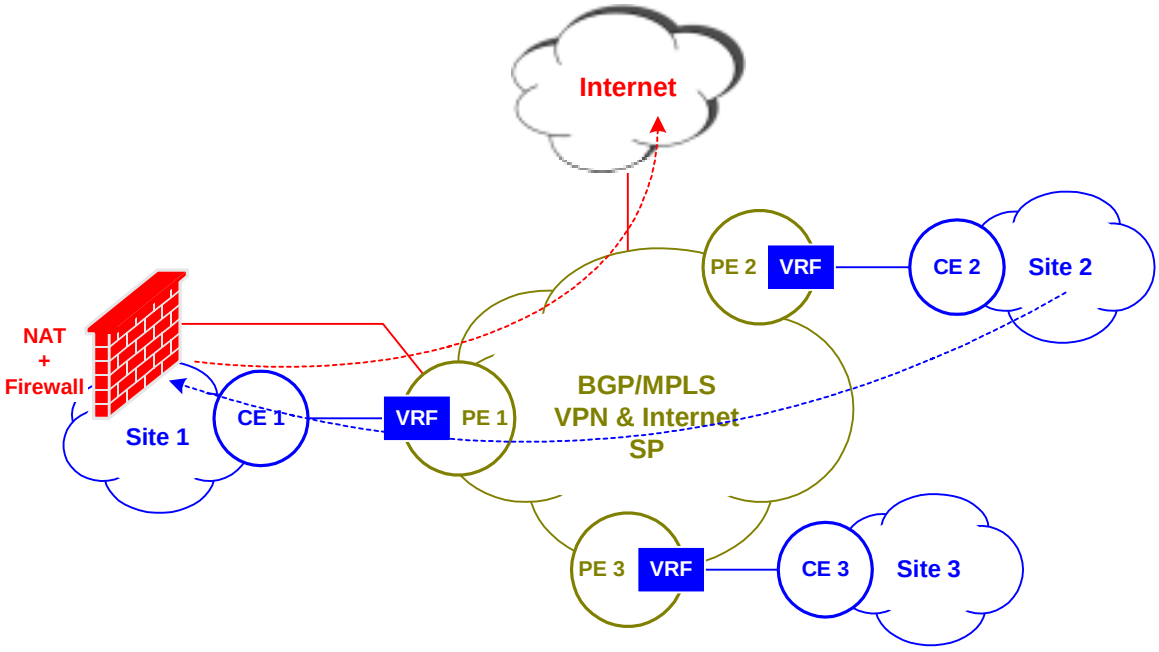


Figure 15: Non-VRF Internet Access

6.2. VRF Internet Access

The VRF sub-interface can be used as well for accessing the Internet. However, unless this service is offered by the SP, the NAT and Firewalls are required, generally at one or more centralised sites.

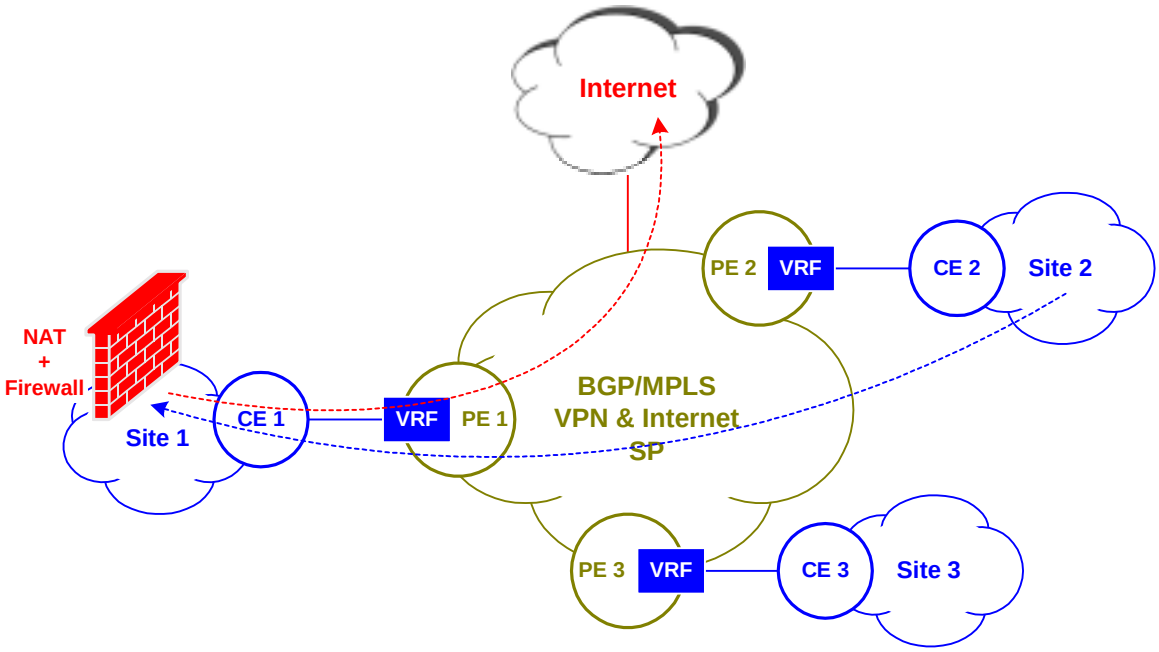


Figure 16: VRF Internet Access

List of Abbreviations

AS	Autonomous System
ASBR	Autonomous System Border Router
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CE	Customer Edge
CPE	Customer Premises Equipment
EBGP	External BGP (also eBGP)
EGP	Exterior Gateway Protocol
FR	Frame Relay
GRE	Generic Routing Encapsulation
IBGP	Internal BGP (also iBGP)
IGP	Interior Gateway Protocol (e.g., RIP, IS-IS and OSPF)
IKE	Internet Key Exchange
IPSec	Internet Protocol Security protocol
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
LAN	Local Area Network
LDP	Label Distribution Protocol
LSP	Label Switched Path
LSR	Label Switching Router
MP-BGP	Multi Protocol BGP (accordingly MP-iBGP and MP-eBGP)
MPLS	Multi Protocol Label Switching
NAT	Network Address Translation
NBVPN	Network-Based VPN
OSPF	Open Shortest Path First routing protocol
P	Provider equipment
PDH	Plesiochronous Digital Hierarchy (E1, E3, DS3)
PE	Provider Edge
POP	Point Of Presence
PPP	Point-to-Point Protocol
PPVPN	Provider Provisioned VPN
RD	Route Distinguisher
RIP	Routing Information Protocol
RR	Route Reflector
RSVP	Resource Reservation Protocol
RT	Route Target
SA	Security Association
SDH	Synchronous Digital Hierarchy (STM-1, STM-4, STM-16...)
SP	Service Provider
VPN	Virtual Private Network
VRF	VPN Routing and Forwarding table

References

[1] "BGP/MPLS VPNs", Rosen, E. et al., draft-ietf-ppvpn-rfc2547bis-01.txt, January 2002.

[2] "Use of PE-PE IPsec in RFC2547 VPNs", Rosen, E. et al., draft-ietf-ppvpn-ipsec-2547-01.txt, February 2002.

[3] "Use of PE-PE GRE or IP in RFC2547 VPNs", Y. Rekhter & E. Rosen, draft-ietf-ppvpn-gre-ip-2547-01.txt, February 2002.

[4] "RFC2547bis: BGP/MPLS VPN Fundamentals" White Paper; Chuck Semeria; 03/01 Juniper Networks

[5] "RFC2547bis: BGP/MPLS VPN Hierarchical and Recursive Applications" White Paper; Chuck Semeria; 07/01 Juniper Networks

[6] "Service requirements for Layer 3 Provider Provisioned Virtual Private Networks", Carugi, M. et al., draft-ietf-ppvpn-requirements-04.txt, March 2002.

[7] "A Framework for Layer 3 Provider Provisioned Virtual Private Networks", Callon, R. et al., draft-ietf-ppvpn-framework-04.txt, February 2002.

[8] "A Framework for Provider Provisioned CE-based Virtual Private Networks using IPsec", De Clercq et. al., draft-ietf-ppvpn-ce-based-01.txt, November 2001.

[9] "MPLS and VPN Architectures", Ivan Pepelnjak & Jim Guichard; Cisco Press

Glossary

VPN – communication between a set of sites, making use of a shared network infrastructure.

PPVPN – VPN for which the service provider participates in management and provisioning of the VPN.

User – A user is an entity (e.g., a human being using a host, a server, or a system) that has been authorized to use a VPN service

Site – A site is a set of users that have mutual IP reachability without use of a specific service provider network. A site may consist of a set of users that are in geographic proximity. However, two geographic locations connected via another provider's network would also constitute a single site since communication between the two locations does not involve the use of the service provider offering the VPN service.

Customer – A single organization, corporation, or enterprise that administratively controls a set of sites.

Intranet – An intranet restricts communication to a set of sites that belong to one customer. An example is branch offices at different sites that require communication to a headquarters site.

Extranet – An extranet allows the specification of communication between a set of sites that belong to different customers. In other words, two or more organizations have access to a specified set of each other's sites. Examples of an extranet scenario include multiple companies cooperating in joint software development, a service provider having access to information from the vendors' corporate sites, different companies, or universities participating in a consortium.

Access connection – An access connection provides connectivity between a CE and a PE. This includes PPP over dedicated physical circuits, as well as logical circuits, such as Ethernet, frame Relay or ATM, or IP tunnels (e.g., IPsec, L2TP).

Access network – An access network provides access connections between CE and PE devices. It may be a TDM network, L2 network (e.g. FR, ATM, and Ethernet), or an IP network over which access is tunnelled

Tunnel – A tunnel between two entities is formed by encapsulating packets within another encapsulating header for purpose of transmission between those two entities in support of a VPN application. Examples of protocols commonly used for tunnelling are: MPLS, GRE, IPsec, and IP-in-IP tunnels.

Hierarchical Tunnel – Encapsulating one tunnel within another forms a hierarchical tunnel. Note that the tunnelling protocols need not be the same in a hierarchical tunnel. In the context of VPNs, a hierarchical tunnel is a logical association between two entities (e.g., a CE or PE switching-router or router) defined by the innermost tunnel protocol header in a hierarchical tunnel For reasons of efficiency, some VPN solutions use hierarchical tunnels between PE routers to reduce the number of tunnels seen by P routers in the backbone.

CE-based VPN – A CE-based VPN is one in which knowledge of L3 aspects of the customer network is limited to CE devices. Customer sites are interconnected via tunnels or nested tunnels. The SP backbone is unaware of the existence of the VPN.

PE-based VPN – A PE-based VPN is one in which the SP backbone is aware of (i.e., maintains state information for) the VPN, and provides a layer 3 service that routes packets between customer sites using the customer network's address space.