

Chapter 18

Interprovider and Carrier-of-Carriers VPNs Overview

This chapter describes in detail the operation of interprovider and carrier-of-carriers virtual private networks (VPNs) as described in RFC 2547bis, *BGP/MPLS VPNs*. As VPNs are deployed on the Internet, the customer of a VPN service provider might be another service provider rather than an end customer. The customer service provider depends on the VPN service provider to deliver a VPN transport service between the customer service provider's points of presence (POPs) or regional networks.

If the customer service provider's sites have different autonomous system (AS) numbers, then the VPN transit service provider supports carrier-of-carrier VPN service for the interprovider VPN service. If the customer service provider's sites have the same AS number, then the VPN transit service provider delivers a carrier-of-carriers VPN service.

This chapter discusses the following topics, which provide background information about carrier-of-carriers VPNs:

- Interprovider and Carrier-of-Carriers VPN Standards on page 425
- Traditional VPNs, Interprovider VPNs, and Carrier-of-Carriers VPNs on page 426
- Interprovider VPNs on page 428
- Carrier-of-Carriers VPNs on page 429

Interprovider and Carrier-of-Carriers VPN Standards

Interprovider and carrier-of-carriers VPNs are defined by the following documents:

- RFC 3107, *Carrying Label Information in BGP-4*.
- Internet draft draft-ietf-ppvpn-rfc2547bis-00.txt, *BGP/MPLS VPNs*.
- *RFC 2547bis: BGP/MPLS VPN Fundamentals*—a white paper located on the Juniper Networks Web site at <http://www.juniper.net/>.

To access Internet RFCs and drafts, go to the IETF Web site at <http://www.ietf.org/>.

Traditional VPNs, Interprovider VPNs, and Carrier-of-Carriers VPNs

The sections that follow provide an overview of traditional VPNs, interprovider and carrier-of-carriers VPNs, and the differences in how external and internal routes are handled in each of these environments.

In traditional IP routing architectures, there is a clear distinction between internal routes and external routes. From the perspective of an Internet service provider (ISP), internal routes include all the provider's internal links (including Border Gateway Protocol [BGP] next hops) and loopback interfaces. These internal routes are exchanged with other routing platforms in the ISP's network by means of an interior gateway protocol (IGP), such as Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS). All routes learned at Internet peering points or from customer sites are classified as external routes and are distributed by means of an exterior gateway protocol (EGP) such as BGP. In traditional IP routing architectures, the number of internal routes is typically much smaller than the number of external routes.

Standard VPNs

The traditional distinction between internal routes and external routes also applies to VPN routing architectures. As shown in Figure 1 on page 5, the provider (P) routers maintain only the service provider's internal routes (to provider edge [PE] routers and other P routers); they do not maintain VPN routes. PE routers are the only devices in the provider network that are required to maintain external routes.

The BGP next hop connects the external routes to the internal routes in traditional VPNs:

- The BGP next hop is advertised with each external route in BGP advertisements.
- The route to the BGP next hop is an internal route that is advertised by the IGP.
- Multiprotocol Label Switching (MPLS) provides packet forwarding from the ingress PE router to the BGP next-hop egress PE router.

Interprovider and Carrier-of-Carriers VPNs

All interprovider and carrier-of-carriers VPNs share the following characteristics:

- Each interprovider or carrier-of-carriers VPN customer must distinguish between internal and external customer routes.
- Internal customer routes must be maintained by the VPN service provider in its PE routers.
- External customer routes are carried only by the customer's routing platforms, not by the VPN service provider's routing platforms.

The key difference between interprovider and carrier-of-carriers VPNs is whether the customer sites belong to the same AS or to separate ASs:

- Interprovider VPNs—The customer sites belong to different ASs. You need to configure external Border Gateway Protocol (EBGP) to exchange the customer's external routes.
- Carrier-of-Carriers VPNs—The customer sites belong to the same AS. You need to configure internal Border Gateway Protocol (IBGP) to exchange the customer's external routes.

In general, each service provider in a VPN hierarchy is required to maintain its own internal routes in its P routers, and the internal routes of its customers in its PE routers. By recursively applying this rule, it is possible to create a hierarchy of VPNs.

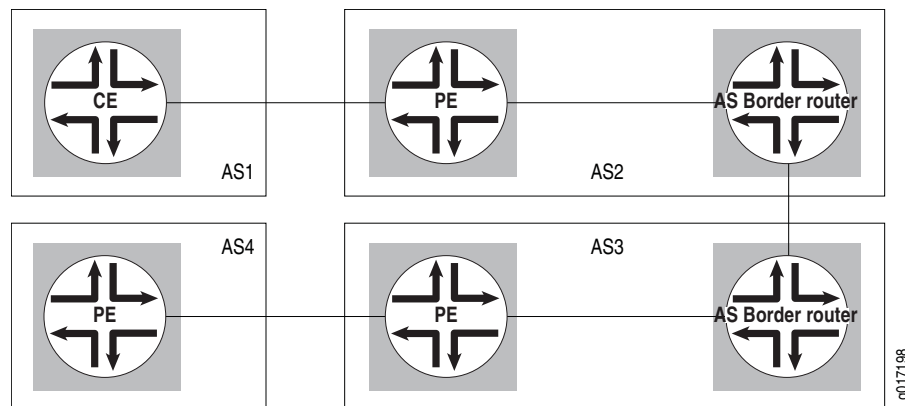
The following are definitions of the types of PE routers specific to interprovider and carrier-of-carriers VPNs:

- The AS border router is located at the AS border and handles traffic leaving and entering the AS.
- The end PE router is the PE router in the customer VPN; it is connected to the CE router at the end customer's site.

Interprovider VPNs

Interprovider VPNs provide connectivity between separate ASs. This functionality might be used by a VPN customer who has connections to several different ISPs, or different connections to the same ISP in different geographic regions, each of which has a different AS. Figure 46 illustrates the type of network topology used by an interprovider VPN.

Figure 46: Interprovider VPN Network Topology



The following sections describe the ways you can configure an interprovider VPN:

- Linking VRF Tables Between Autonomous Systems on page 428
- Configuring MP-EBGP Between AS Border Routers on page 428
- Configuring Multihop MP-EBGP Between AS Border Routers on page 429

Linking VRF Tables Between Autonomous Systems

You can connect two separate ASs by simply linking the VPN routing and forwarding (VRF) table in the AS border router of one AS to the VRF table in the AS border router in the other AS. Each AS border router must contain a VRF instance for every VPN configured in both service provider networks. You then configure an IP session between the two AS border routers. In effect, the AS border routers treat each other as customer edge (CE) routers.

Because of the complexity of the configuration, particularly with regard to scaling, this method is not recommended. The details of this configuration are not provided in this manual.

Configuring MP-EBGP Between AS Border Routers

In this approach, the PE routers within an AS use multiprotocol external BGP (MP-EBGP) to distribute labeled VPN-Internet Protocol version 4 (IPv4) routes to an AS border router or to a route reflector of which the AS border router is a client. The AS border router uses multiprotocol external BGP (MP-EBGP) to distribute the labeled VPN-IPv4 routes to its peer AS border router in the neighboring AS. The peer AS border router then uses MP-IBGP to distribute labeled VPN-IPv4 routes to PE routers, or to a route reflector of which the PE routers are a client.

This approach enhances the scalability of an EBGp VRF-to-VRF configuration because it eliminates the need to configure all the VPNs on every AS border router. However, it also introduces some complexity:

- All the VRF routes must be stored in the AS border router.
- An LSP must be established from ingress PE routers to egress PE routers.
- Secure connections must exist among the ASs along the path from the ingress PE router to the egress PE router.
- The ASs must be configured to know which AS border routers receive routes with specific route target attributes.

Configuring Multihop MP-EBGP Between AS Border Routers

In this type of interprovider VPN configuration, P routers do not need to know all the routes in all the VPNs. Only the PE routers must have all the VPN routes. The P routers simply forward traffic to the PE routers—they are not aware of the packets' destination. The connections between the AS border routers in separate ASs forward traffic between the ASs, much as a label-switched path (LSP) works.

The following are the basic steps you take to configure an interprovider VPN in this manner:

1. Configure multihop EBGp redistribution of labeled VPN-IPv4 routes between the source and destination ASs.
2. Configure EBGp to redistribute labeled IPv4 routes from its AS to neighboring ASs.
3. Configure MPLS on the end PE routers of the VPNs.

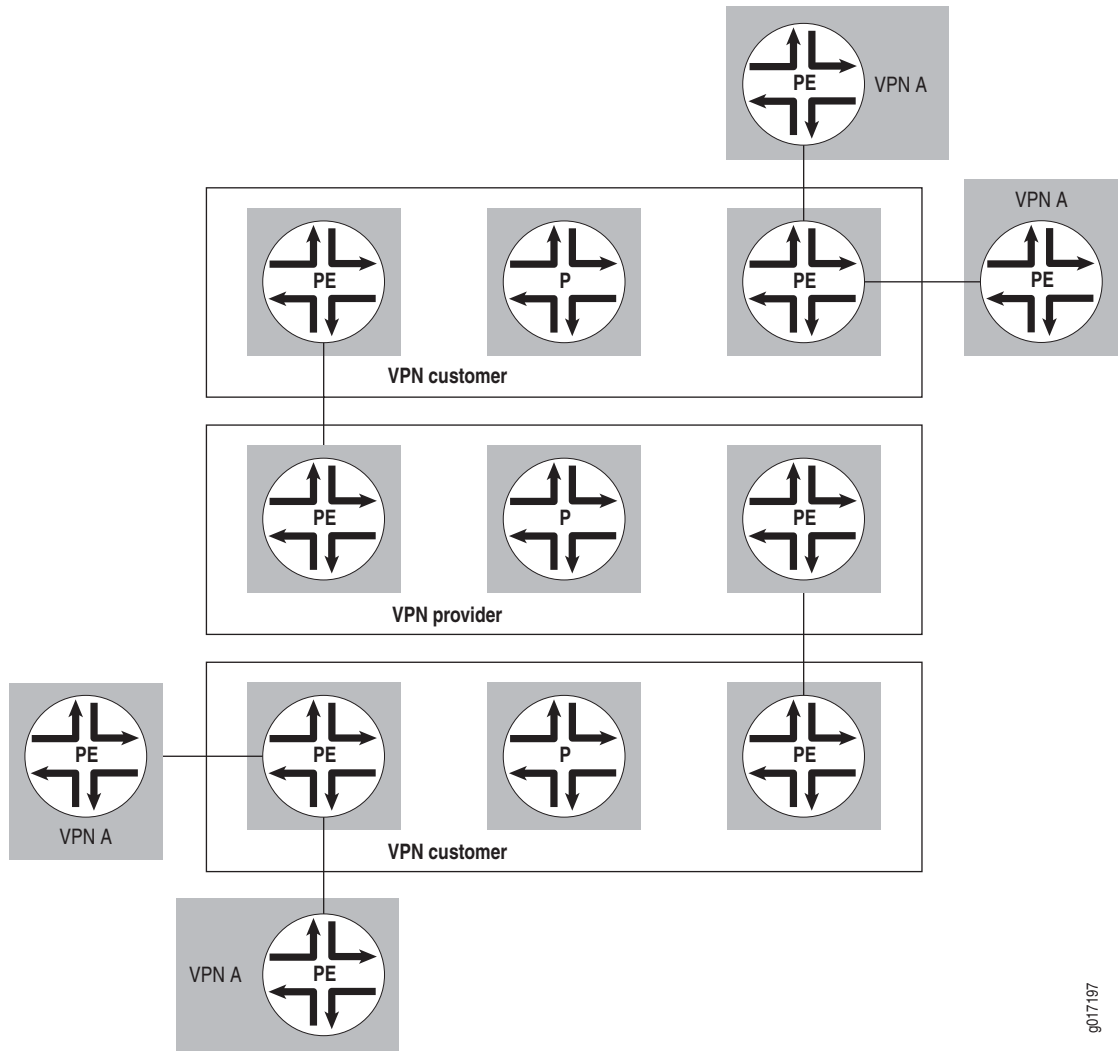
Carrier-of-Carriers VPNs

The customer of a VPN service provider might be a service provider for the end customer. The following are the two main types of carrier-of-carriers VPNs (as described in *BGP/MPLS VPNs*):

- Internet Service Provider as the Customer on page 431—The VPN customer is an ISP that uses the VPN service provider's network to connect its geographically disparate regional networks. The customer does not have to configure MPLS within its regional networks.
- VPN Service Provider as the Customer on page 431—The VPN customer is itself a VPN service provider offering VPN service to its customers. The carrier-of-carriers VPN service customer relies on the backbone VPN service provider for intersite connectivity. The customer VPN service provider is required to run MPLS within its regional networks.

Figure 47 on page 430 illustrates the network architecture used for a carrier-of-carriers VPN service.

Figure 47: Carrier-of-Carriers VPN Architecture



g017197

Internet Service Provider as the Customer

In this type of carrier-of-carriers VPN configuration, ISP A configures its network to provide Internet service to ISP B. ISP B provides the connection to the customer wanting Internet service, but the actual Internet service is provided by ISP A.

This type of carrier-of-carriers VPN configuration has the following characteristics:

- The carrier-of-carriers VPN service customer (ISP B) does not need to configure MPLS on its network.
- The carrier-of-carriers VPN service provider (ISP A) must configure MPLS on its network.
- MPLS must also be configured on the CE routers and PE routers connected together in the carrier-of-carriers VPN service customer's and carrier-of-carriers VPN service provider's networks.

VPN Service Provider as the Customer

A VPN service provider can have customers that are themselves VPN service providers. In this type of configuration, also called a hierarchical or recursive VPN, the customer VPN service provider's VPN-IPv4 routes are considered external routes, and the backbone VPN service provider does not import them into its VRF table. The backbone VPN service provider imports only the customer VPN service provider's internal routes into its VRF table.

This type of configuration is similar to the configuration described in the "Internet Service Provider as the Customer" section. The similarities and differences are shown in Table 12.

Table 12: Comparison of Interprovider and Carrier-of-Carriers VPNs

Feature	ISP Customer	VPN Service Provider Customer
Customer edge device	AS border router	PE router
IBGP sessions	Carry IPv4 routes	Carry external VPN-IPv4 routes with associated labels
Forwarding within the customer network	MPLS is optional	MPLS is required

