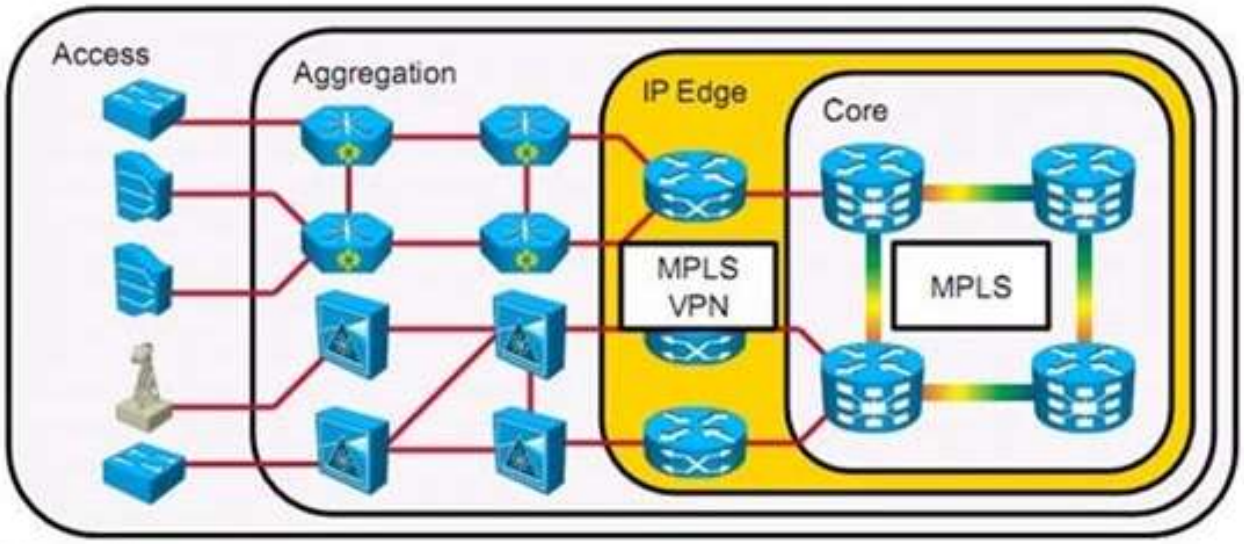
Introducing MPLS VPNs

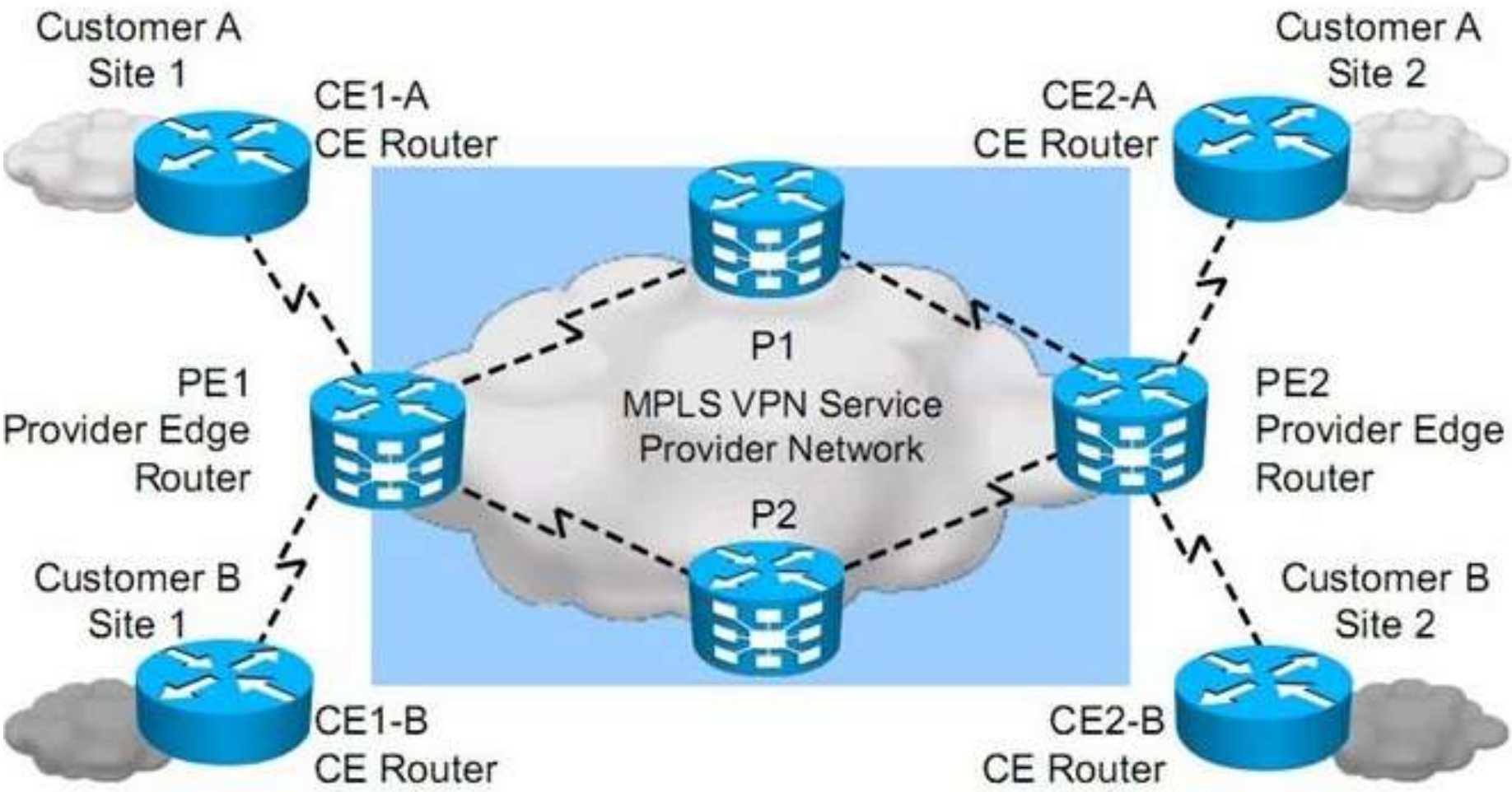
MPLS VPN Architechture

An MPLS VPN combines the best features of an overlay VPN and a peer-to-peer VPN:

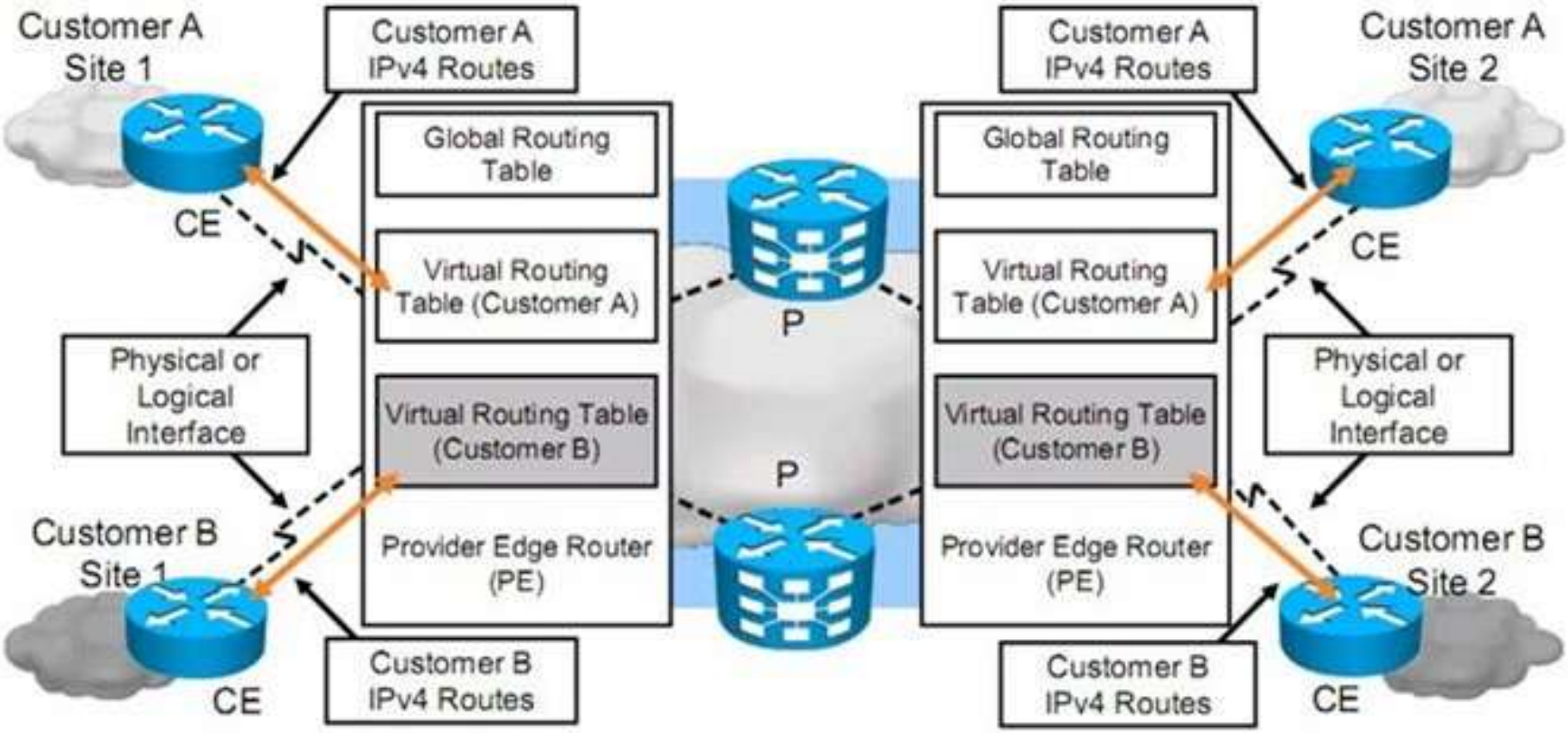
- PE routers participate in customer routing, guaranteeing optimum routing between sites and easy provisioning.
- PE routers carry a separate set of routes for each customer (similar to the dedicated PE router approach).
- Customers can use overlapping addresses.



MPLS VPN Network Architechture Component

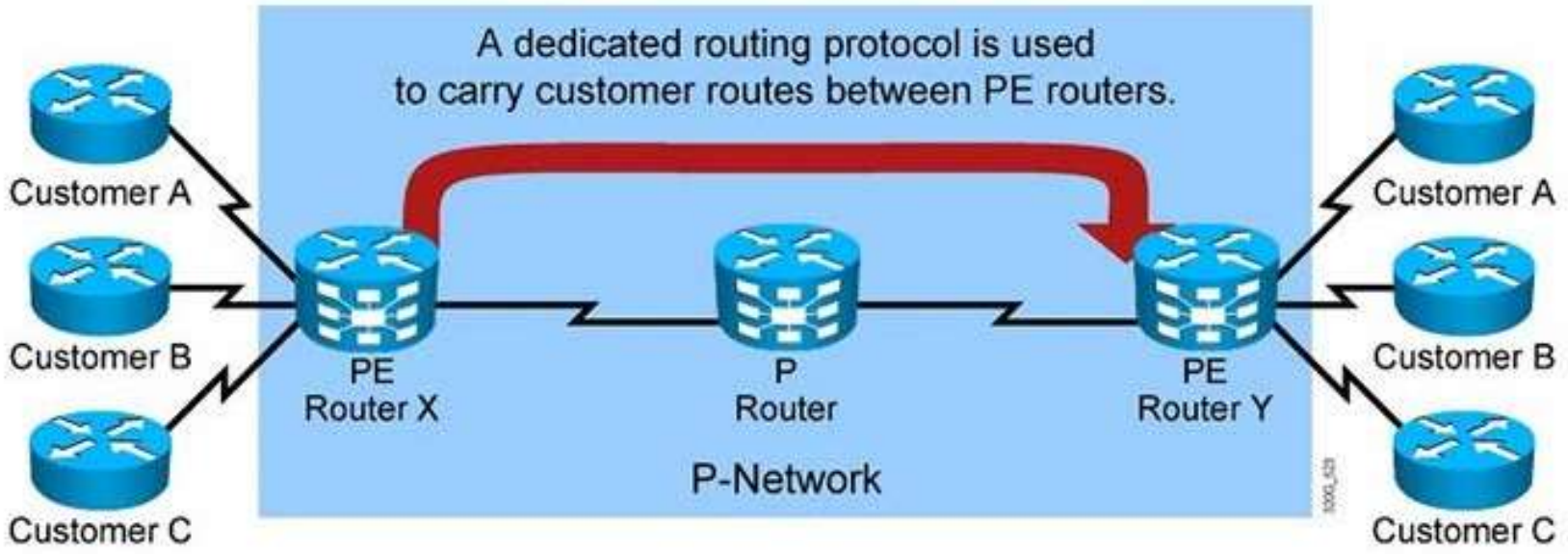


PE Router Architecture



A PE router in an MPLS VPN uses virtual routing tables to implement the functionality of customer-dedicated PE routers.

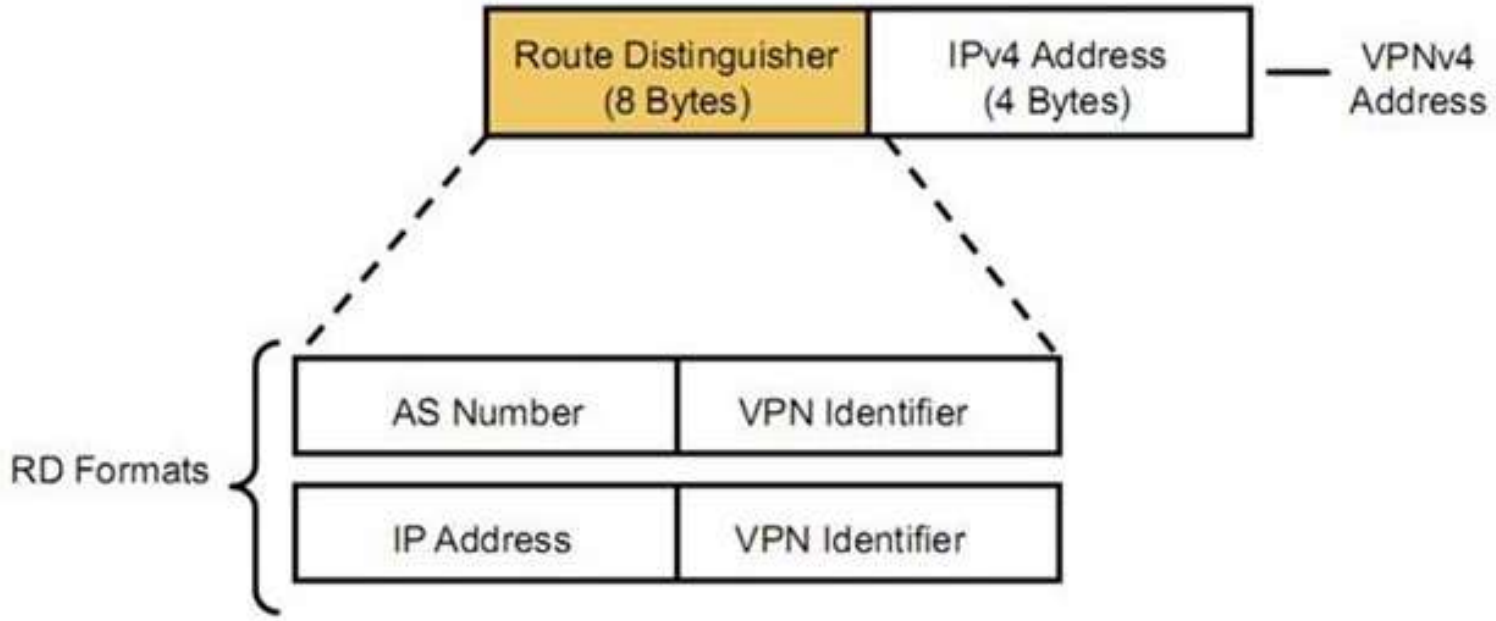
Propagation of Routing Information Across the P-Network



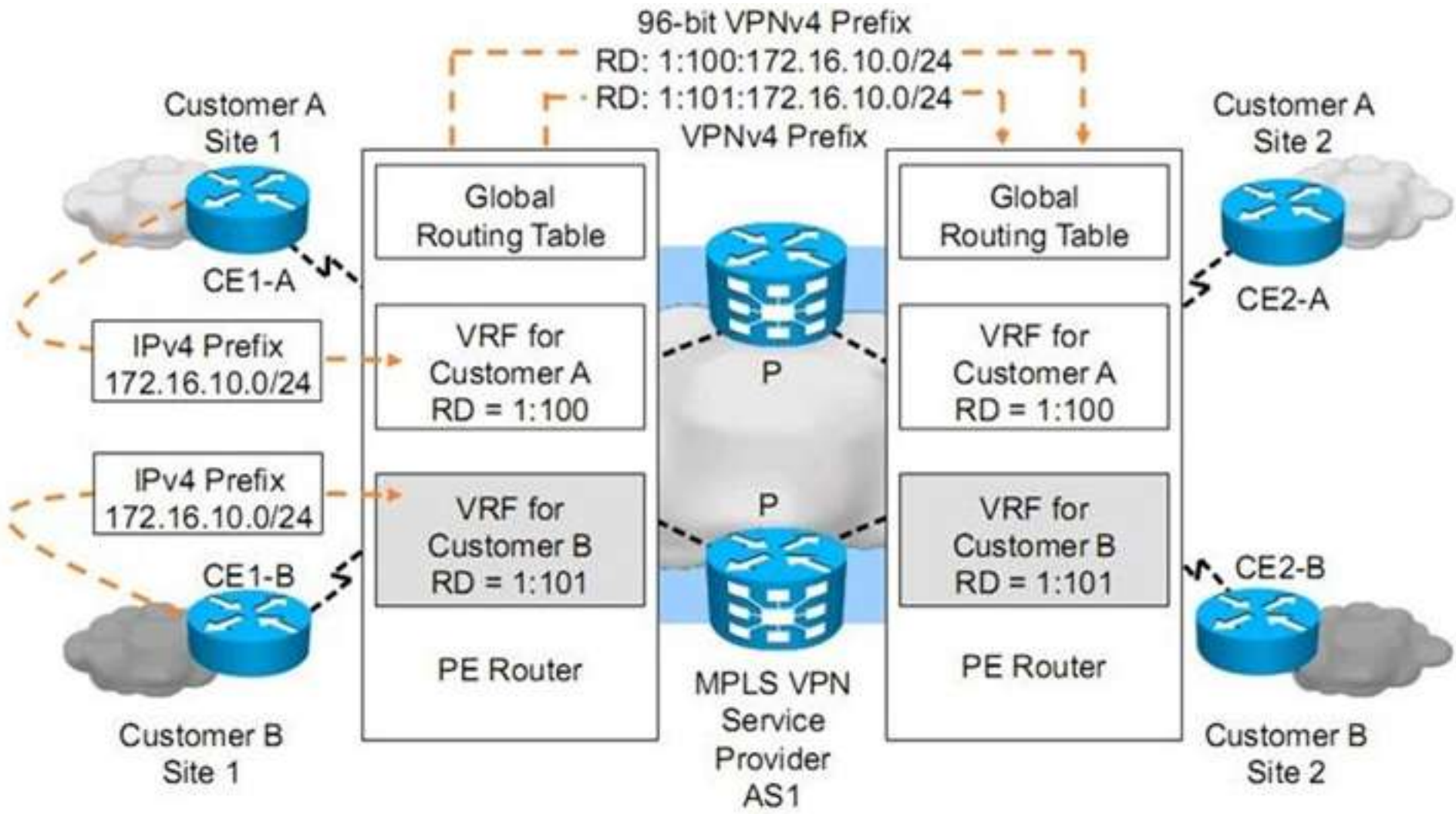
- Run a single routing protocol that will carry all customer routes between PE routers. Use MPLS labels to exchange packets between PE routers.
- P routers do not carry customer routes; the solution is scalable.
- The number of customer routes can be very large. BGP4 is the only routing protocol that can scale to a very large number of routes.
- BGP is used to exchange customer routes directly between PE routers.
- Extend the customer addresses to make them unique.

Route Distinguishers

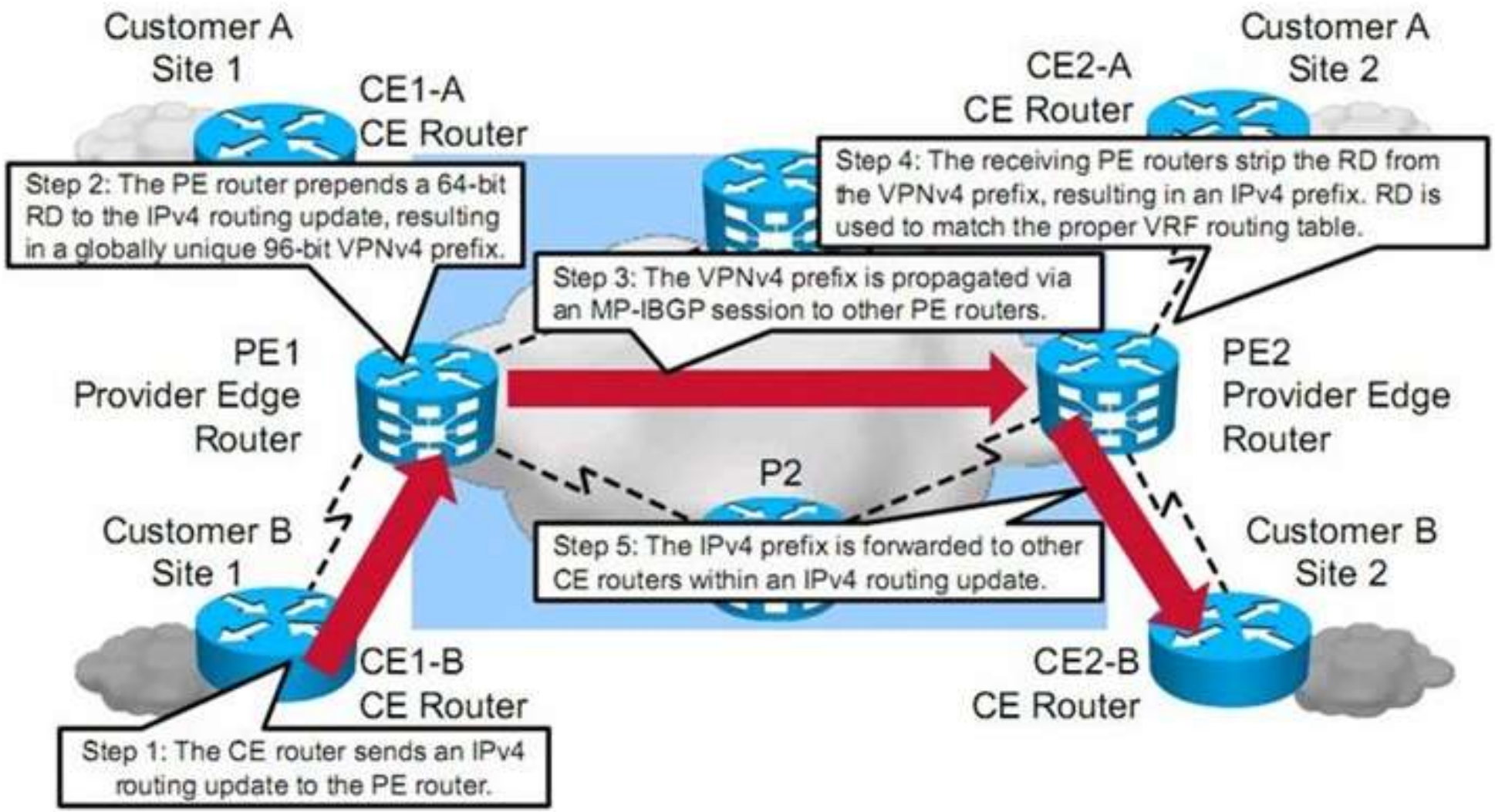
- In the MPLS VPN backbone, the PE router needs to implement processes that enable overlapping address spaces in connected customer networks.
- The 64-bit route distinguisher is prepended to an IPv4 address to make it globally unique.
- The resulting address is a VPNv4 address.
- VPNv4 addresses are exchanged between PE routers via BGP4.



RD Operation



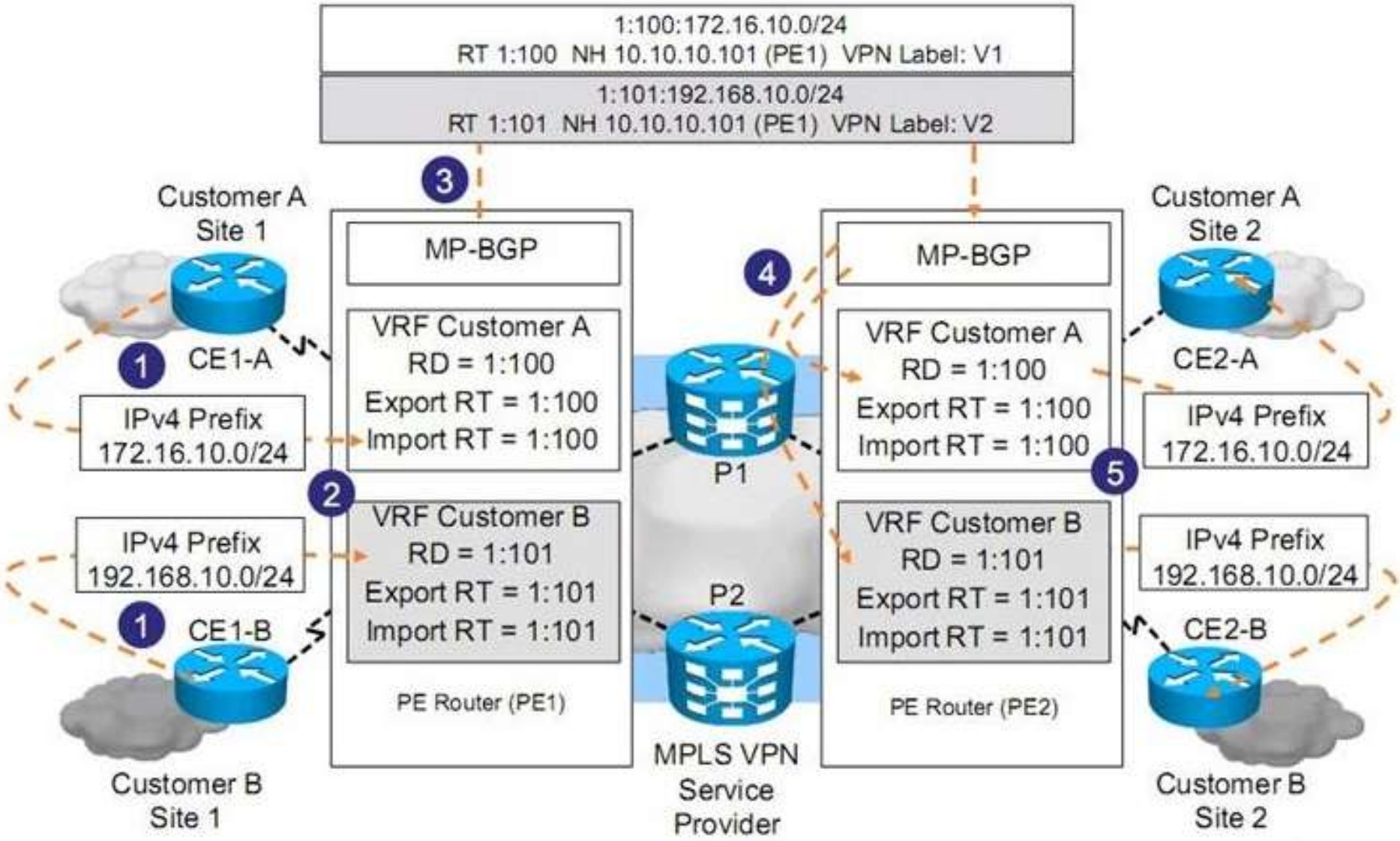
RD Process Flow



Route Targets

- The RD cannot identify participation in more than one VPN.
- RTs were introduced in the MPLS VPN architecture to support complex VPN topologies.
- RTs are additional attributes attached to VPNv4 BGP routes to indicate VPN membership.
- Extended BGP communities are used to encode these attributes.
- Export RTs:
  - Identifying VPN membership
  - Appended to the customer route when it is converted into a VPNv4 route
- Import RTs:
  - Associated with each virtual routing table
  - Select routes to be inserted into the virtual routing table

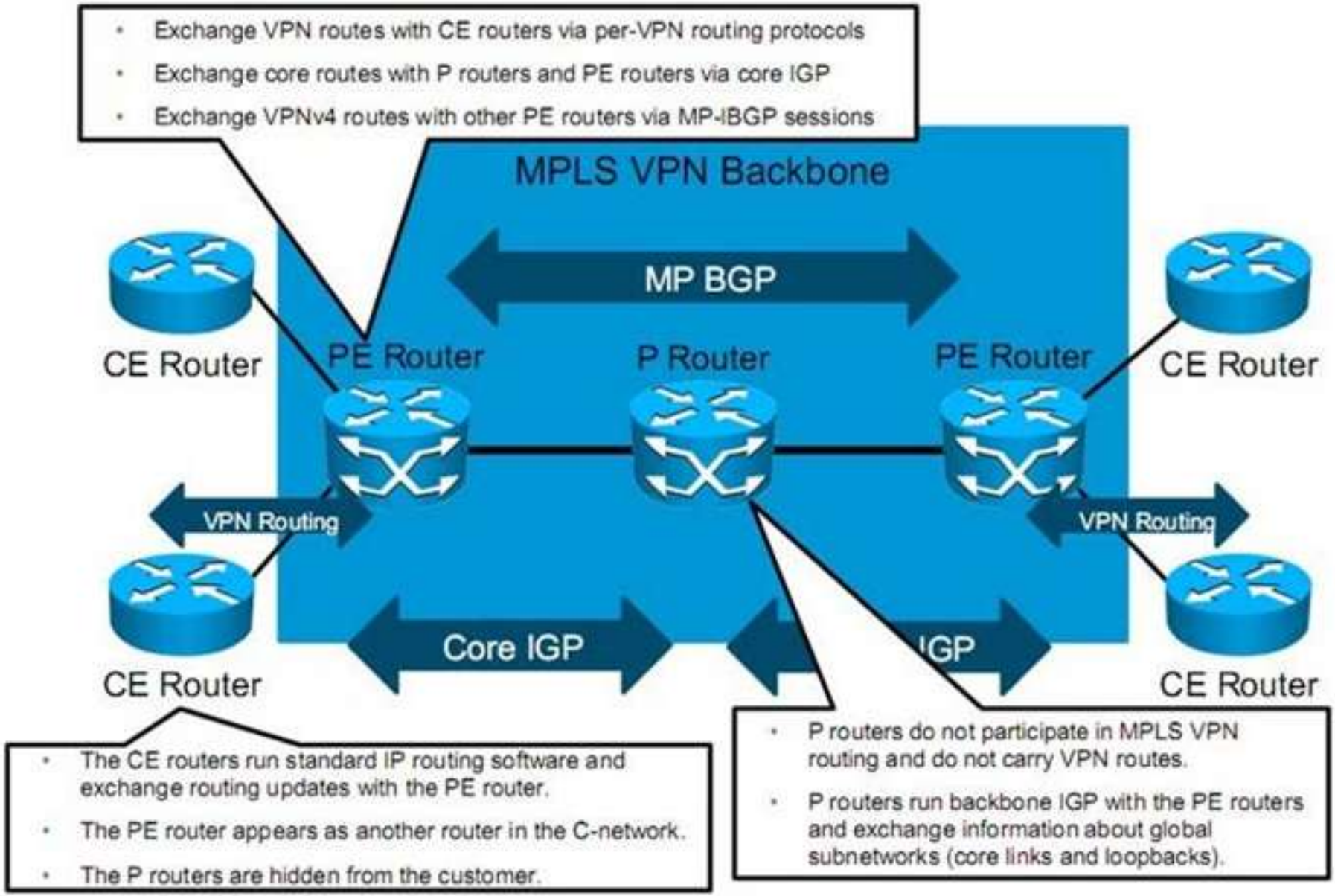
RT and RD Operation



MPLS VPN Routing Requirements

- CE Routers must run standard IP Routing software
- PE Routers must support MPLS VPN Services and IP Routing
- P Router must not participate in customer VPN Routing

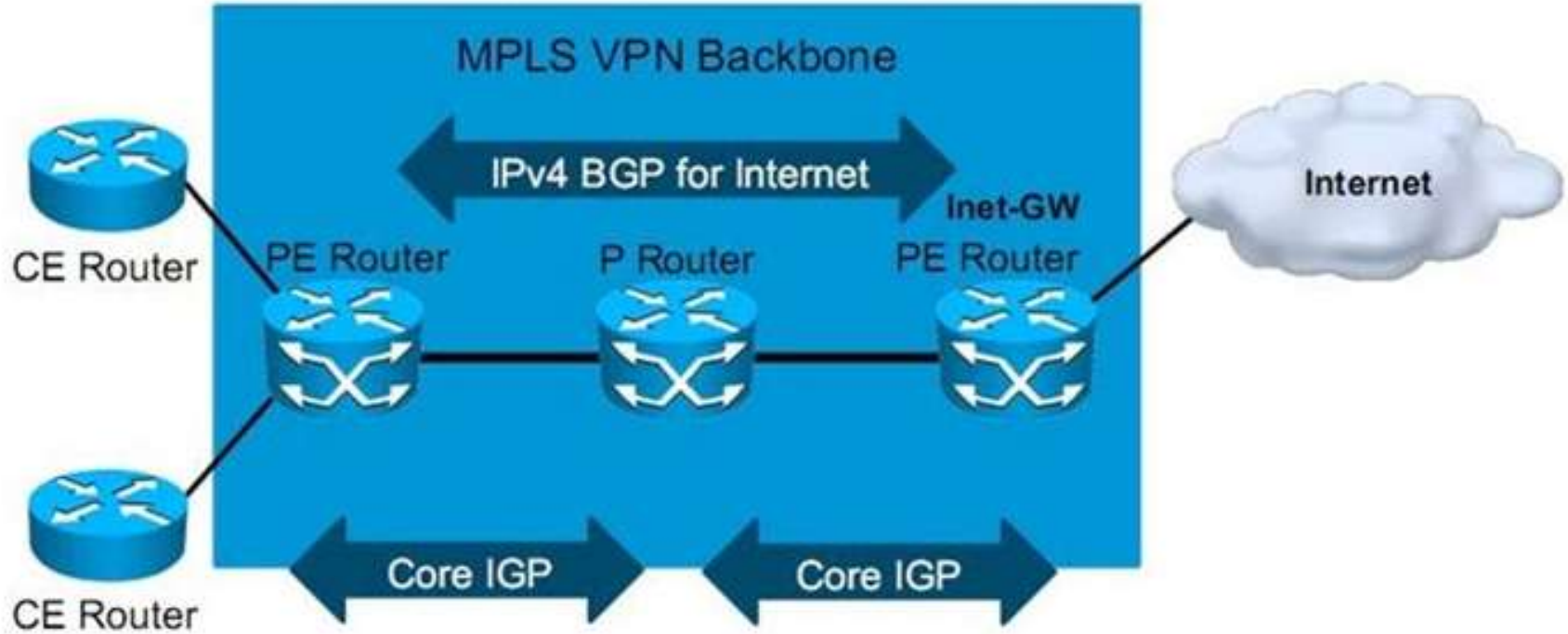
MPLS VPN Routing Model



Support for Internet Routing

PE routers can run standard IPv4 BGP in the global routing table:

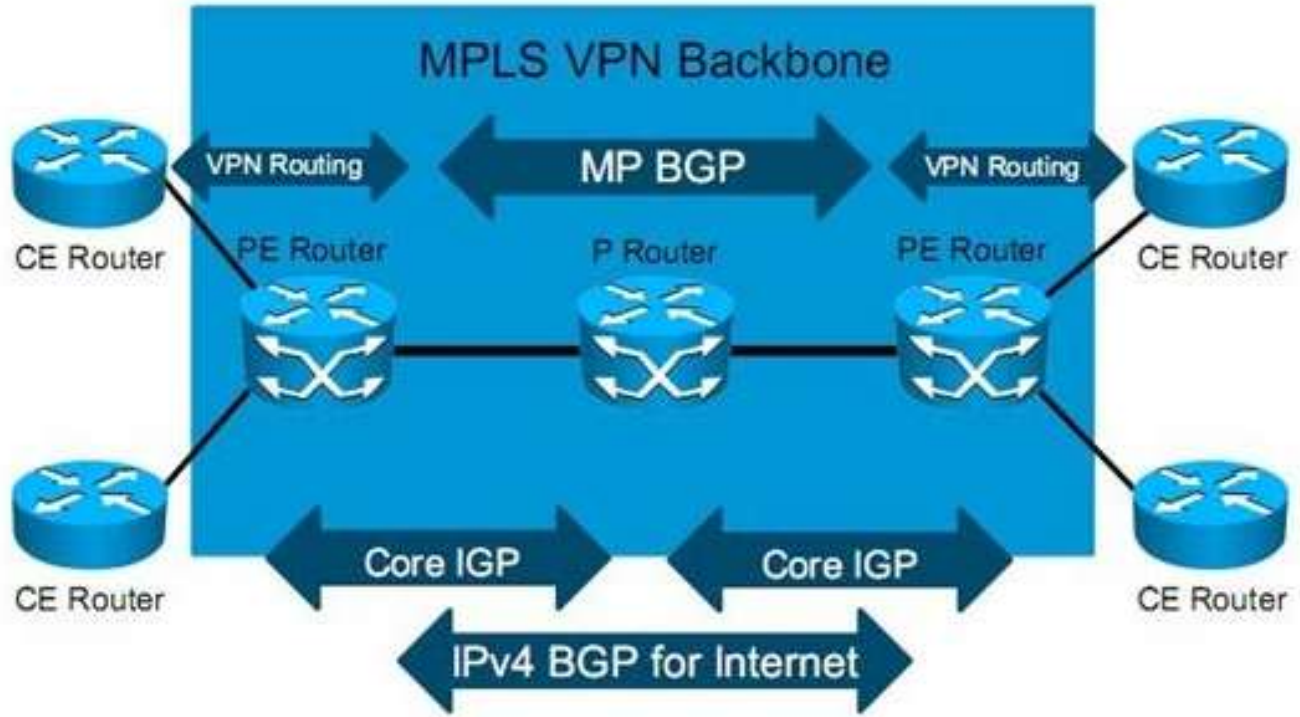
- PE routers exchange Internet routes with other PE routers.
- CE routers do not participate in Internet routing.
- P routers do not need to participate in Internet routing.



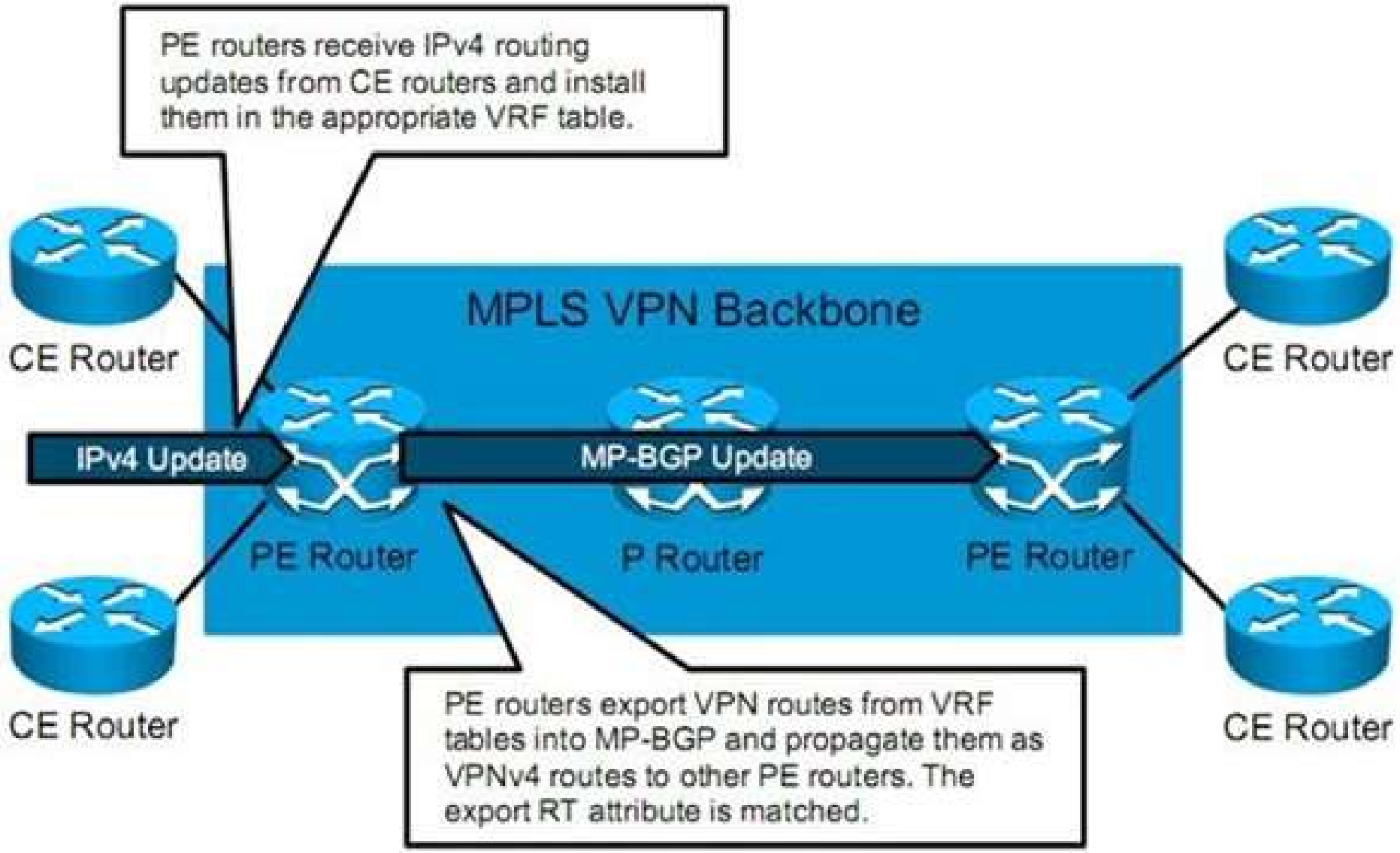
Routing Table for PE Router

PE routers contain a number of routing tables:

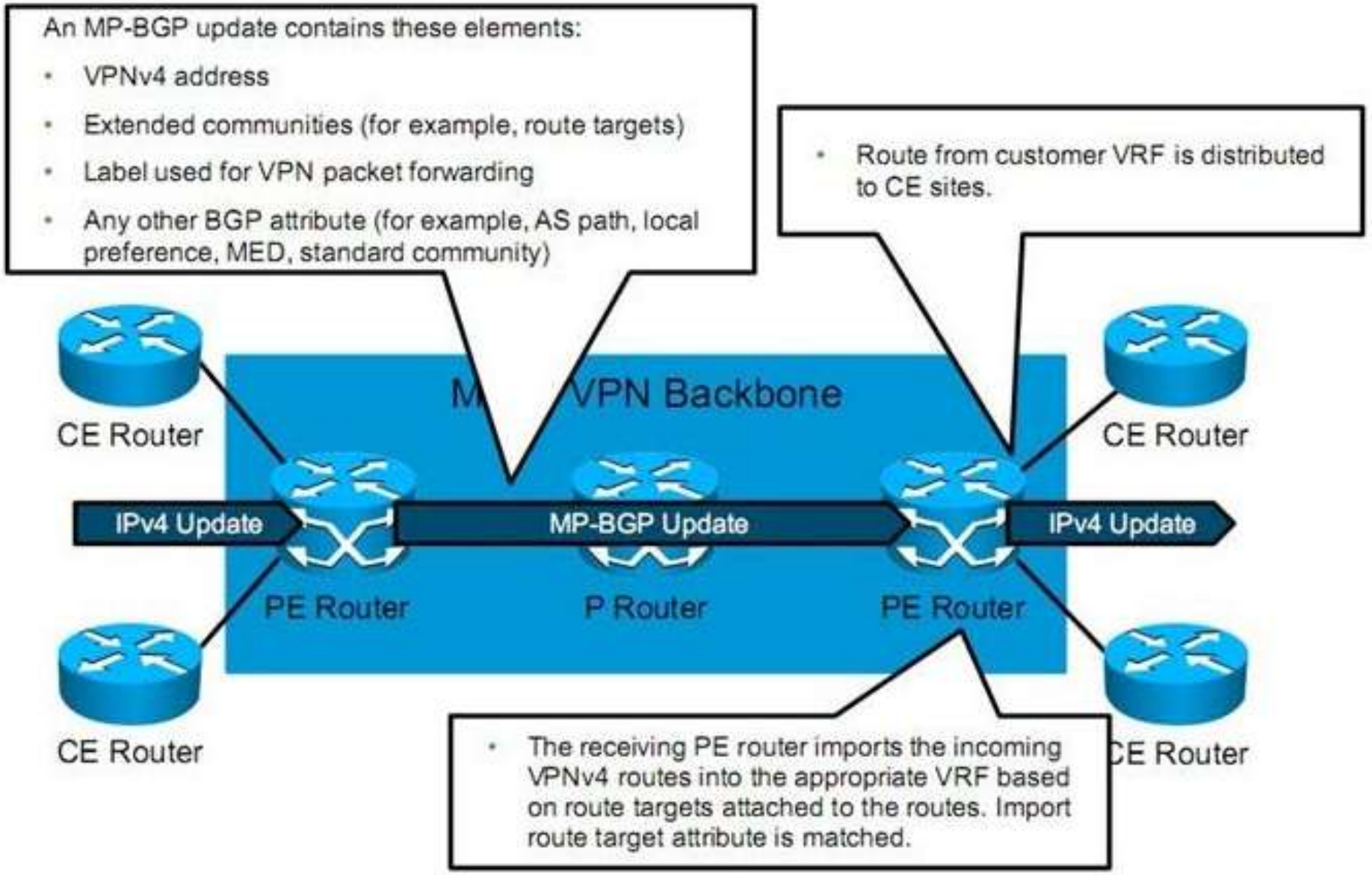
- The global routing table contains core routes (filled with core IGP) and Internet routes (filled with IPv4 BGP).
- The VRF tables contain routes for sites of identical routing requirements from local (IPv4 VPN) and remote (VPNv4 via MP-BGP) CE routers.



End-to-End Routing Update Flow Example



End-to-End Routing Update Flow Example (cont)

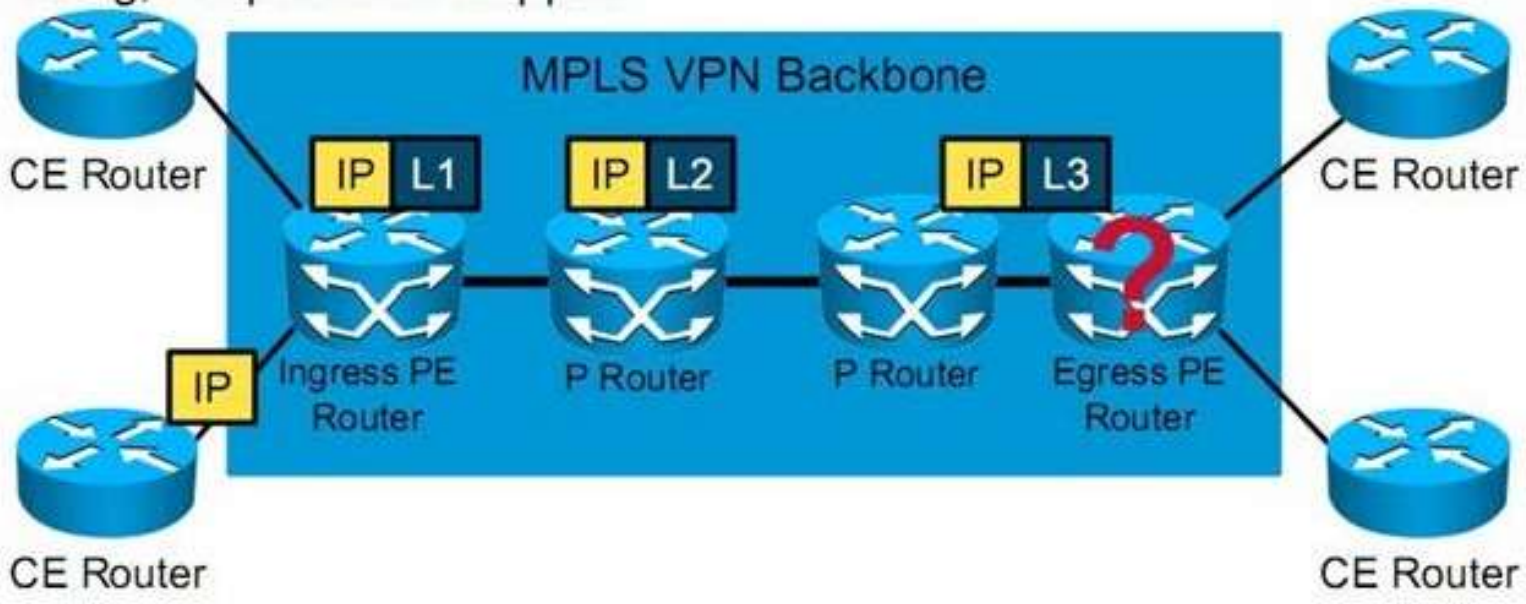


VPN Packet Forwarding Across an MPLS VPN Bacbone – Approach 1

Approach 1: The PE routers will label the VPN packets with an LDP label for the egress PE router, and forward the labeled packets across the MPLS backbone.

Results:

- The P routers perform the label switching, and the packet reaches the egress PE router.
- Because the egress PE router does not know which VRF to use for packet switching, the packet is dropped.

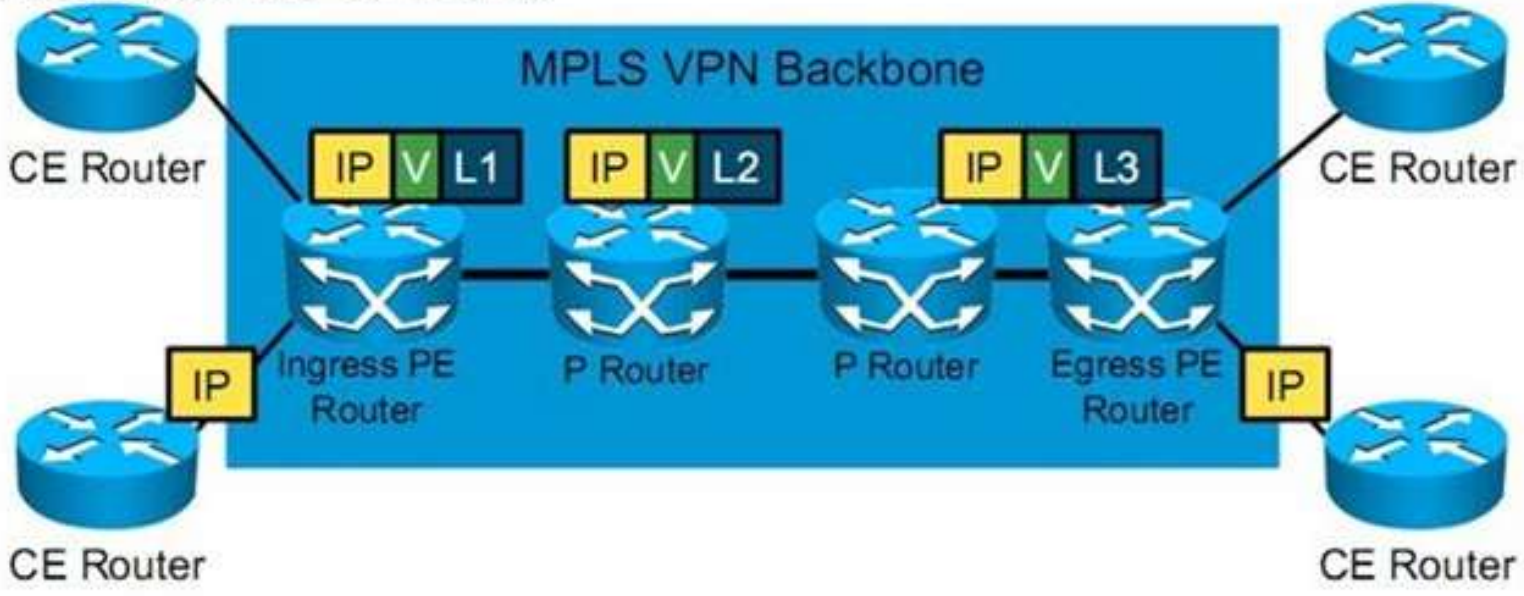


VPN Packet Forwarding Across an MPLS VPN Bacbone – Approach 2

Approach 2: The PE routers will label the VPN packets with a label stack, using the LDP label for the egress PE router as the top label, and the VPN label assigned by the egress PE router as the second label in the stack.

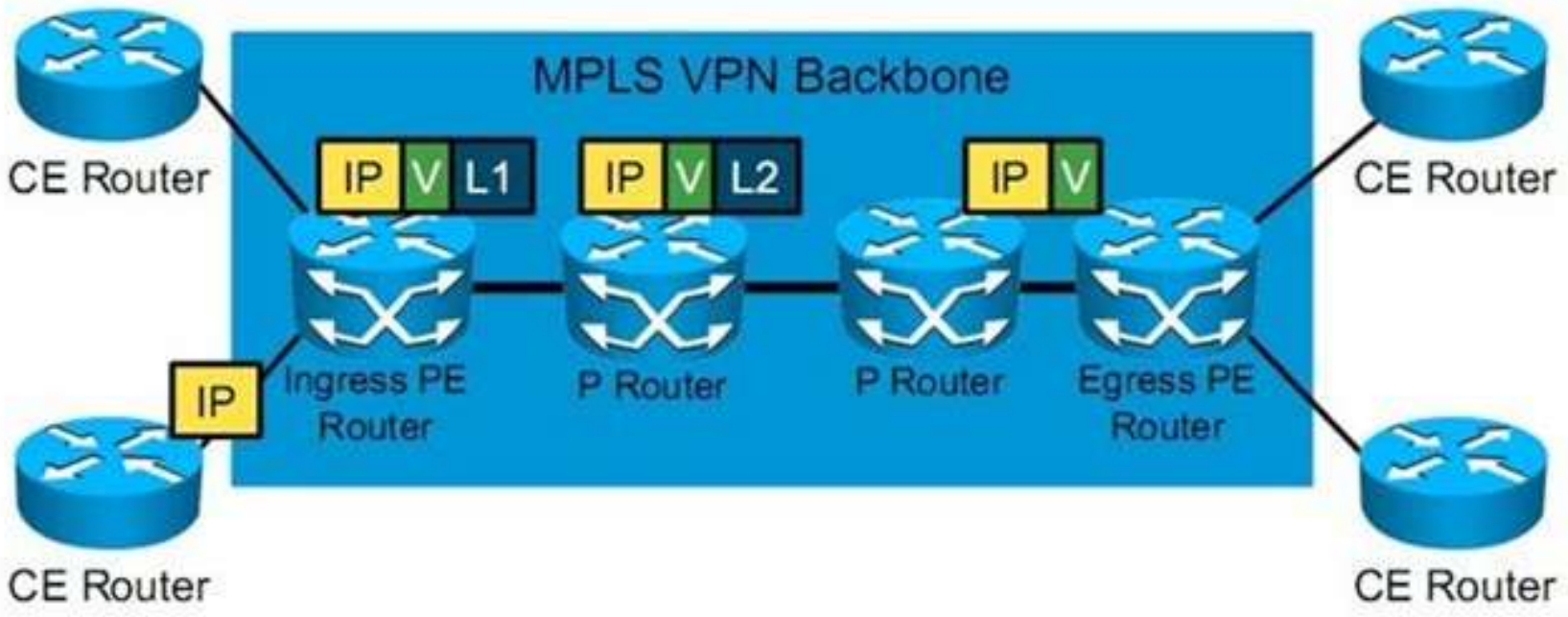
Results:

- The P routers perform label switching using the top label, and the packet reaches the egress PE router. The top label is removed.
- The egress PE router performs a lookup on the VPN label and forwards the packet toward the CE router.



VPN PHP

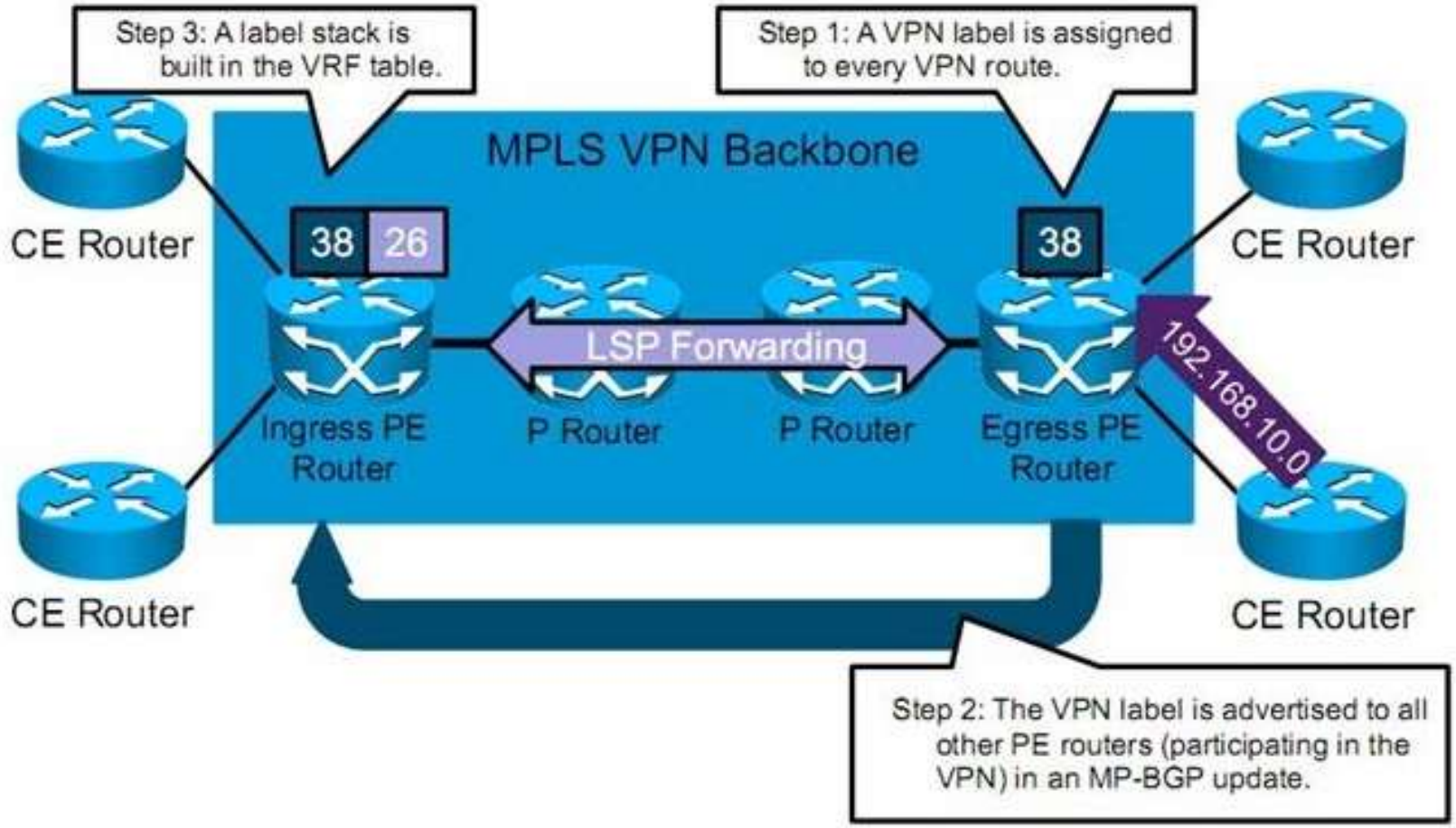
- PHP on the LDP label can be performed on the last P router.
- The egress PE router performs label lookup only on the VPN label, resulting in faster and simpler label lookup.
- IP lookup is performed only once—in the ingress PE router.



VPN Lable Propagation

Question: How will the ingress PE router get the second label in the label stack from the egress PE router?

Answer: Labels are propagated in MP-BGP VPNv4 routing updates.

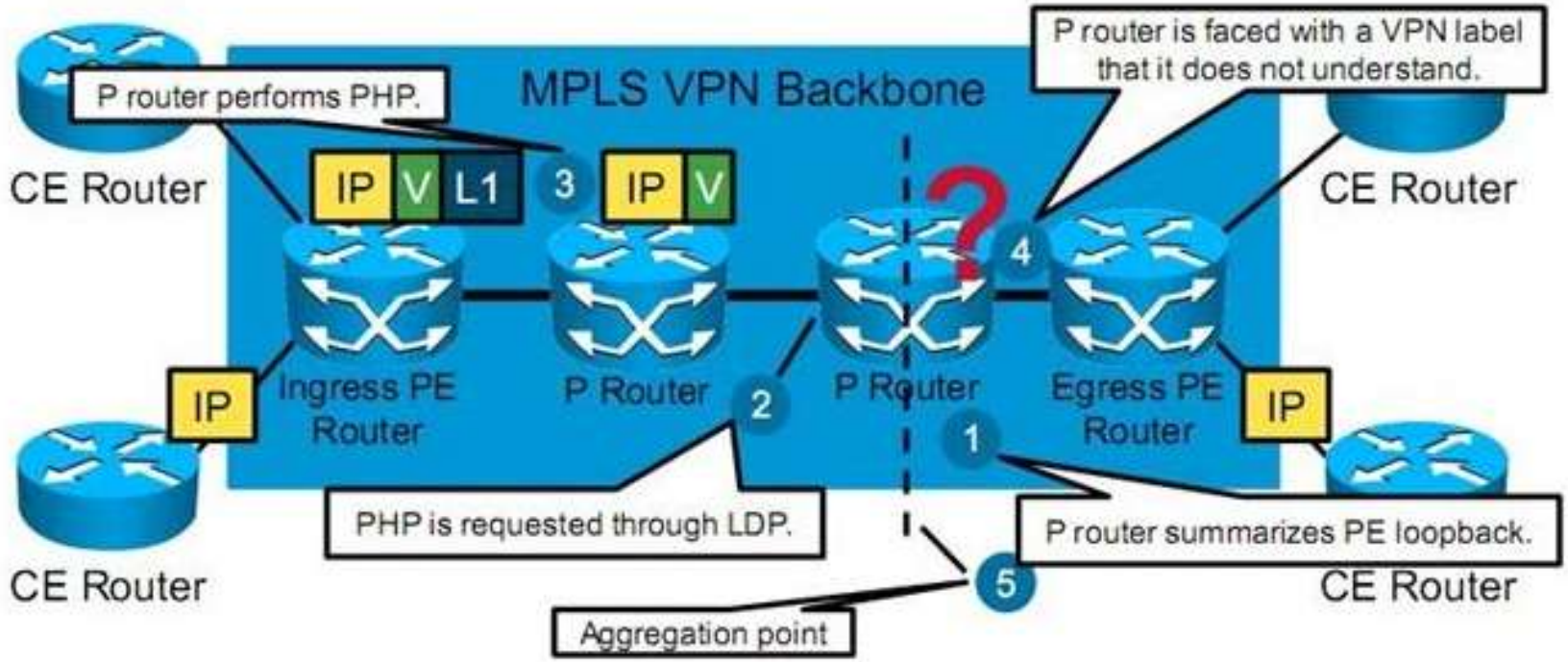


MPLS VPNs and Lable Propagation

- The VPN label must be assigned by the BGP next hop.
- The BGP next hop should not be changed in the MP-IBGP update propagation.
  - Do not use the **next-hop-self** command on confederation boundaries.
- The PE router must be the BGP next hop.
  - Use the **next-hop-self** command on the PE router.
- The label must be reoriginated if the next hop is changed.
  - A new label is assigned every time that the MP-BGP update crosses the AS boundary where the next hop is changed.

MPLS VPNs and Packet Forwarding

- The VPN label of the BGP route is understood by only the egress PE router.
- An end-to-end LSP tunnel is required between the ingress and egress PE routers.
- BGP next-hop addresses must be IGP routes.
  - LDP labels will be assigned to addresses in the global routing table.
  - LDP labels are not assigned to BGP routes (BGP routes receive VPN labels).
- BGP next hops announced in IGP must not be summarized in the core network.
  - Summarization breaks the LSP tunnel.



Summary

- The most scalable method of exchanging customer routes across a provider network is the use of an MP-BGP between PE routers.
  - RDs transform non-unique 32-bit addresses into 96-bit unique addresses.
  - RTs are used to identify VPN membership in overlapping topologies.
- In MPLS VPNs:
  - CE routers run standard routing protocols to the PE routers.
  - PE routers provide the VPN routing and services via MP-BGP.
  - P routers do not participate in VPN routing, and only provide core IGP backbone routing to the PE routers.
- PE routers forward packets across the MPLS VPN backbone using label stacking.


CISCO