Carrier-Based VPNs

GTER-14

Roosevelt Ferreira

Juniper Networks

roosevelt@juniper.net

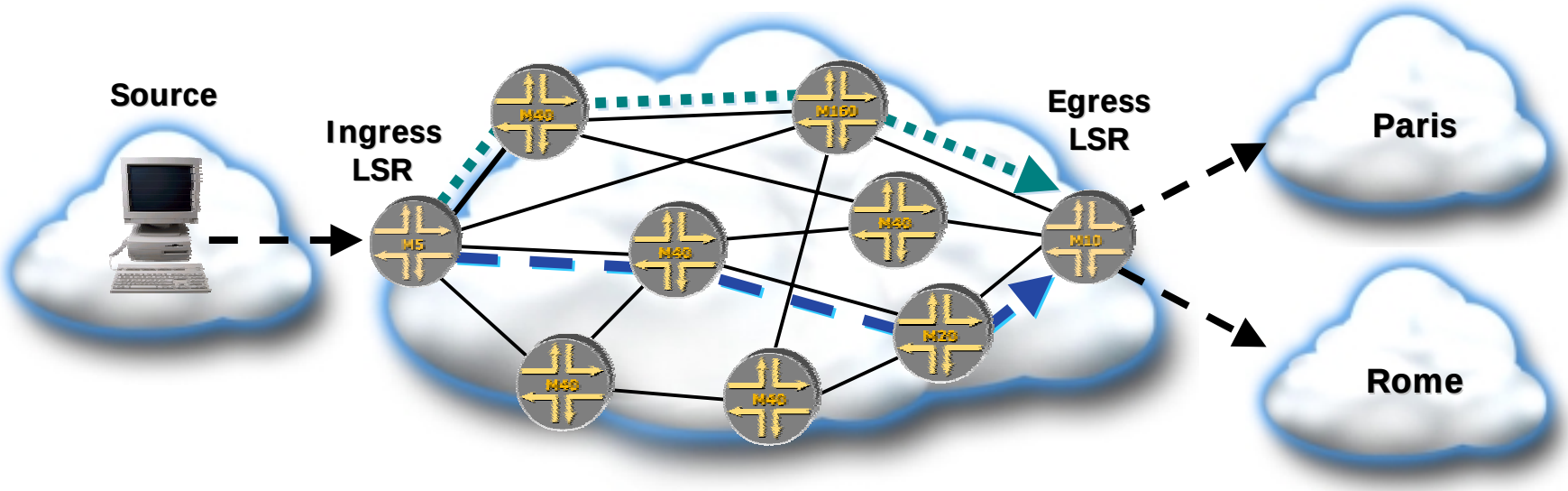
Agenda

- MPLS Overview
- Carrier-based VPNs
  - BGP/MPLS VPNs (RFC 2547bis)
  - MPLS Layer2 VPNs
  - MPLS Layer 2.5 VPNs (Interworking)
  - VPLS (Virtual Private LAN Services)
  - InterProvider VPNs
  - Carrier of Carrier VPNs

Agenda

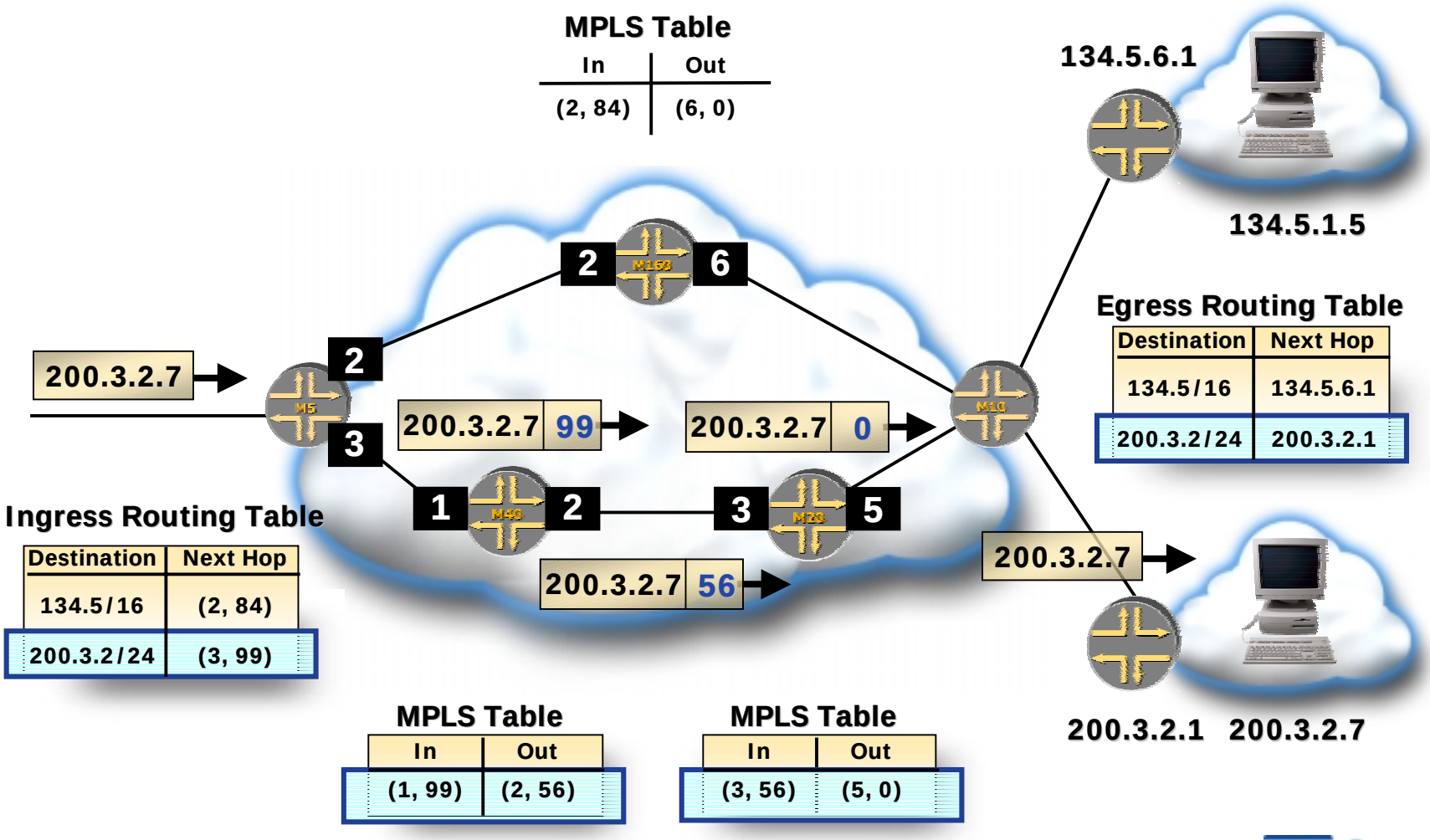
- **MPLS Overview**
- Carrier-based VPNs
  - BGP/MPLS VPNs (RFC 2547bis)
  - MPLS Layer2 VPNs
  - MPLS Layer 2.5 VPNs (Interworking)
  - VPLS (Virtual Private LAN Services)
  - InterProvider VPNs
  - Carrier of Carrier VPNs

MPLS Forwarding Model



- Ingress LSR determines FEC and assigns a label
  - Forwards Paris traffic on the Green LSP
  - Forwards Rome traffic on the Blue LSP
- Traffic is label swapped at each transit LSR
- Egress LSR
  - Removes MPLS header
  - Forwards packet based on destination address

MPLS Forwarding Example



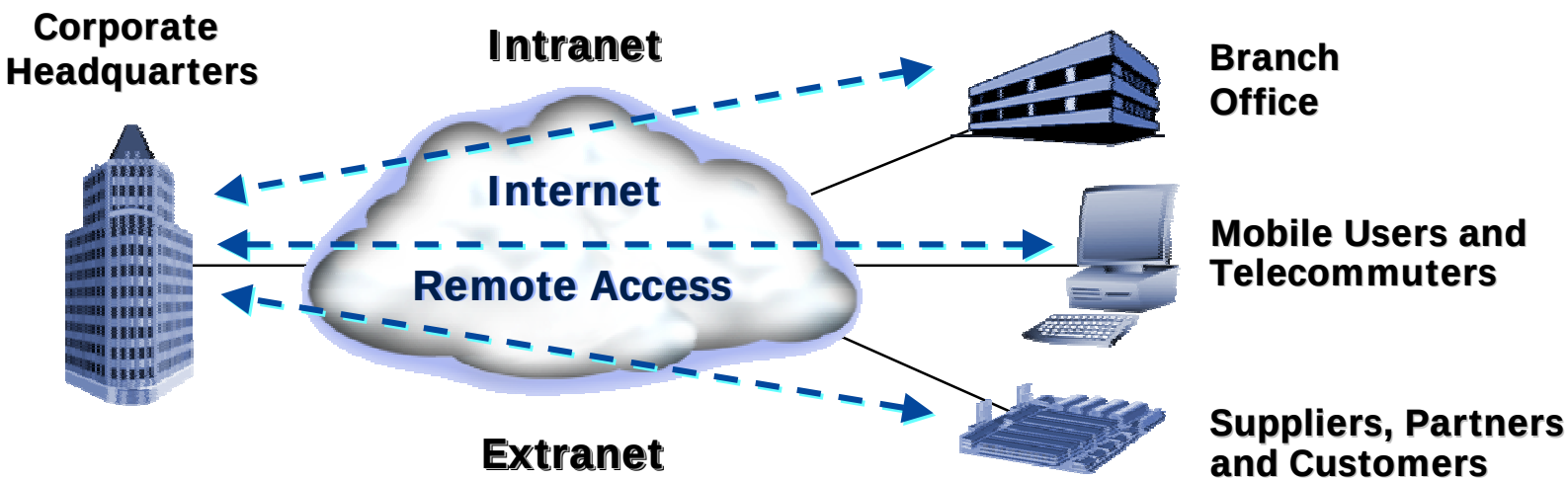
Agenda

- MPLS Overview
- **Carrier-based VPNs**
  - **BGP/MPLS VPNs (RFC 2547bis)**
  - **MPLS Layer2 VPNs**
  - **MPLS Layer 2.5 VPNs (Interworking)**
  - **VPLS (Virtual Private LAN Services)**
  - **InterProvider VPNs**
  - **Carrier of Carrier VPNs**

Agenda

- MPLS Overview
- **Carrier-based VPNs**
  - BGP/MPLS VPNs (RFC 2547bis)
  - MPLS Layer2 VPNs
  - MPLS Layer 2.5 VPNs (Interworking)
  - VPLS (Virtual Private LAN Services)
  - InterProvider VPNs
  - Carrier of Carrier VPNs

Deploying VPNs in the 21st Century



- **Subscriber requirements**
  - Lower cost of service
  - A single network connection for multiple services
- **Provider requirements**
  - Lower operational cost
  - A single network infrastructure for multiple services
- **Reduced CapEx, reduced OpEx**

Benefits of IP VPNs

- Lower equipment cost
  - Economies of scale with common backbone
- Lower service cost
- Lower management and support costs
  - Management can be outsourced to SP
  - End users can focus on core competency rather than on the network
- Better connectivity for end users
  - IP is everywhere

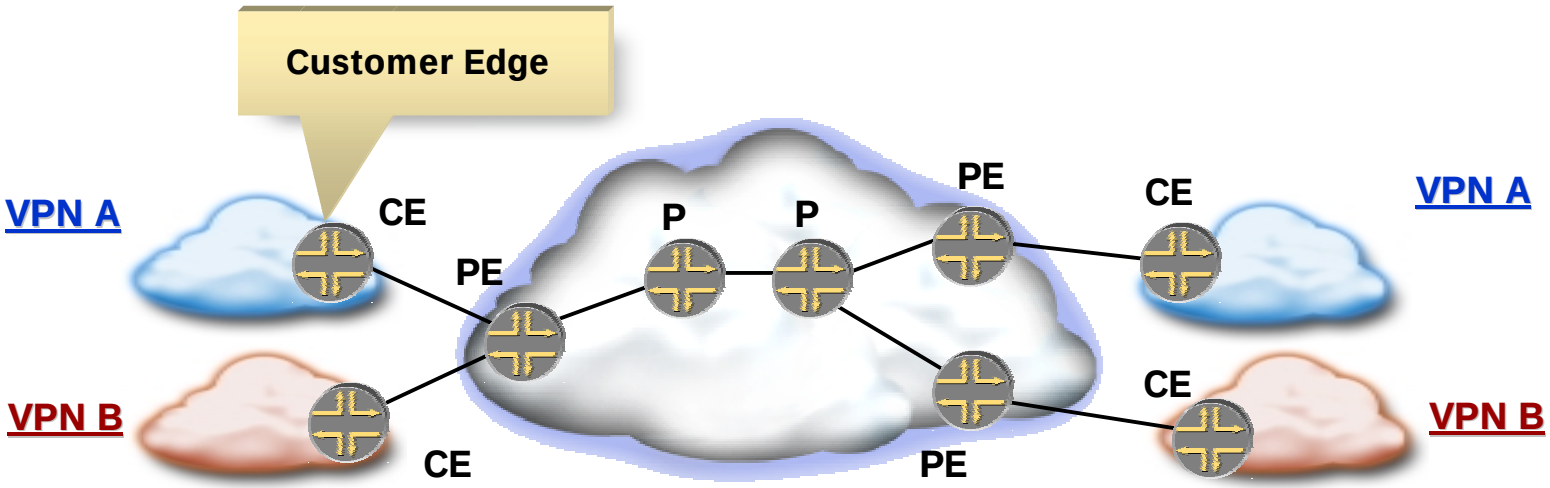
A Range of VPN Solutions

- Each customer has different
  - Security requirements
  - Staff expertise
  - Tolerance for outsourcing
- Customer networks vary by size and traffic volume
- Providers differ concerning
  - Customer base
  - Willingness to offer outsourcing
  - Handling managed router services

Agenda

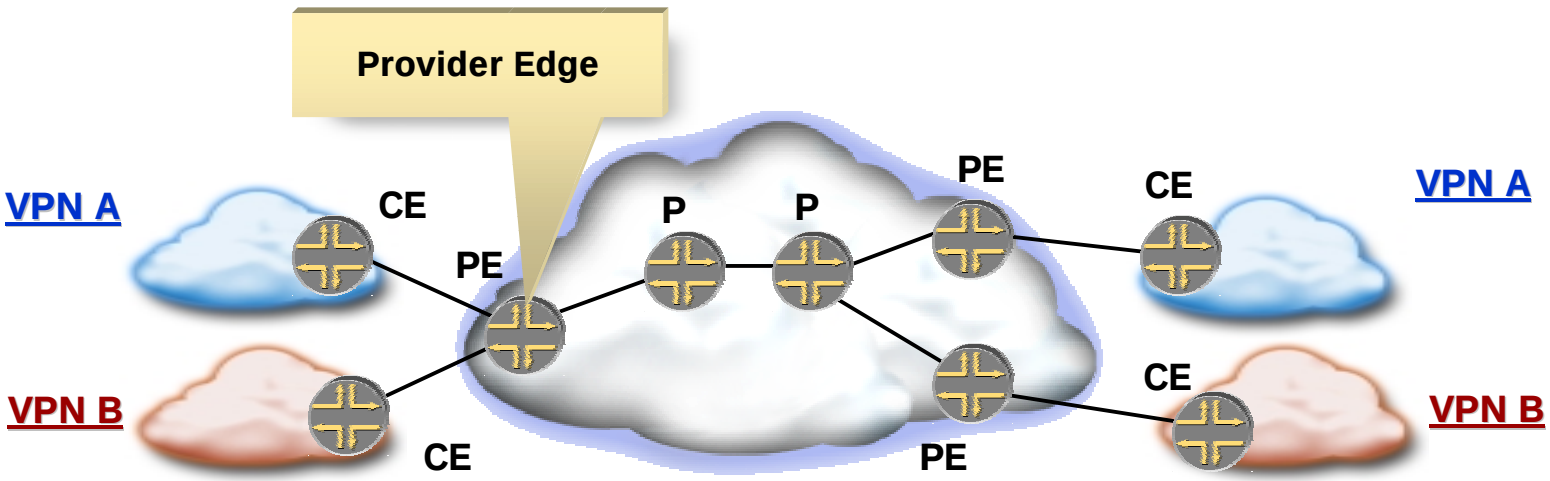
- MPLS Overview
- **Carrier-based VPNs**
  - **BGP/MPLS VPNs (RFC 2547bis)**
  - MPLS Layer2 VPNs
  - MPLS Layer 2.5 VPNs (Interworking)
  - VPLS (Virtual Private LAN Services)
  - InterProvider VPNs
  - Carrier of Carrier VPNs

Customer Edge Routers (2547bis)



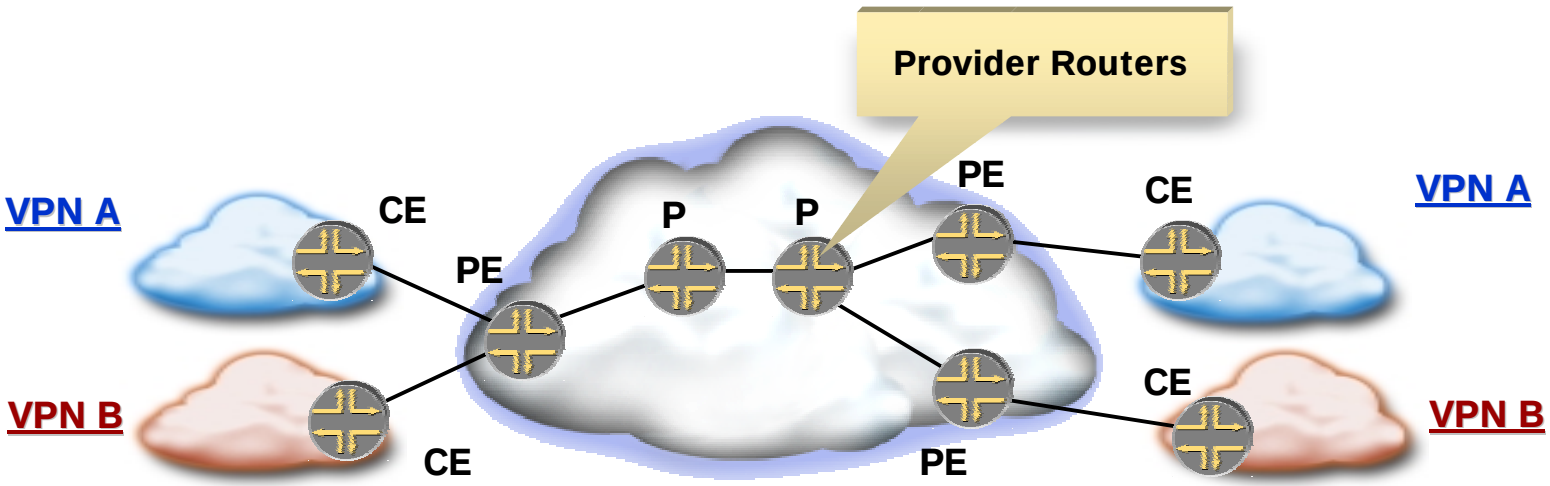
- **Customer Edge (CE) routers**
  - **Located at customer premises**
  - **Provide access to the service provider network**
  - **Can use any access technology or routing protocol for the CE/PE connection**

Provider Edge Routers (2547bis)



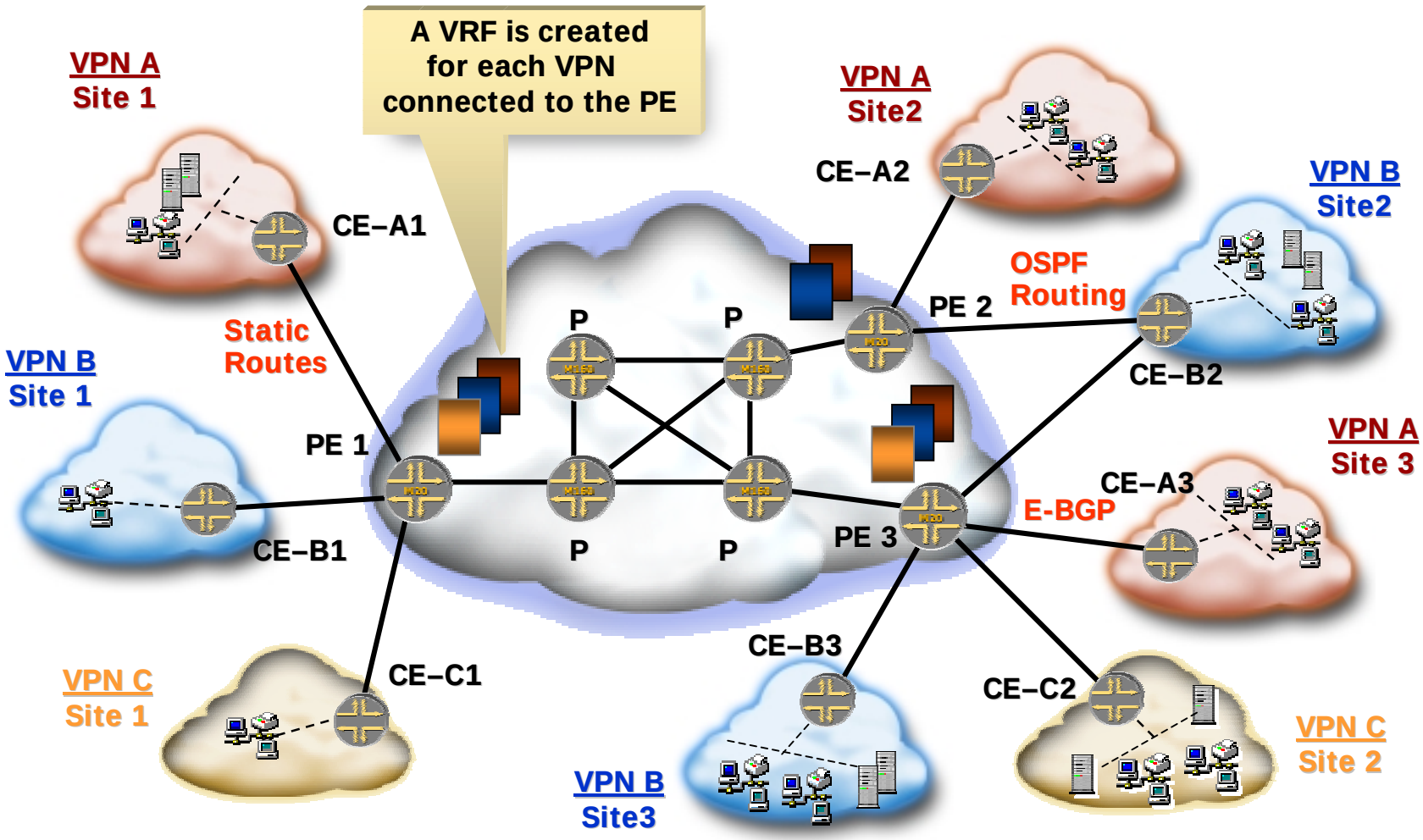
- **Provider Edge (PE) routers**
  - **Maintain VPN-specific forwarding tables**
  - **Exchange VPN routing information with other PE routers using BGP**
  - **Use MPLS LSPs to forward VPN traffic**

Provider Routers (2547bis)

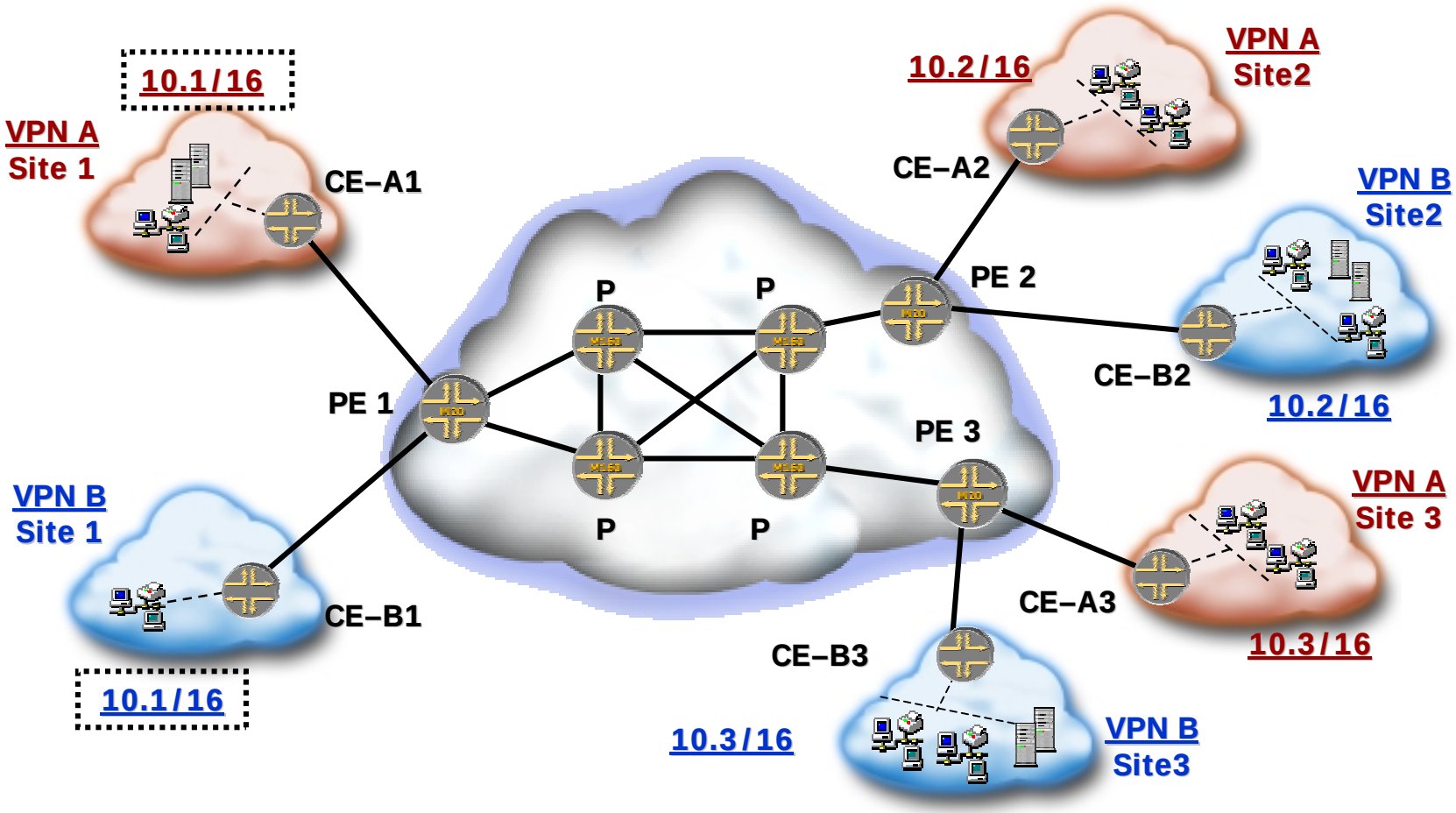


- **Provider (P) routers**
  - **Forward VPN data transparently over established LSPs**
  - **Do not maintain VPN-specific routing information**

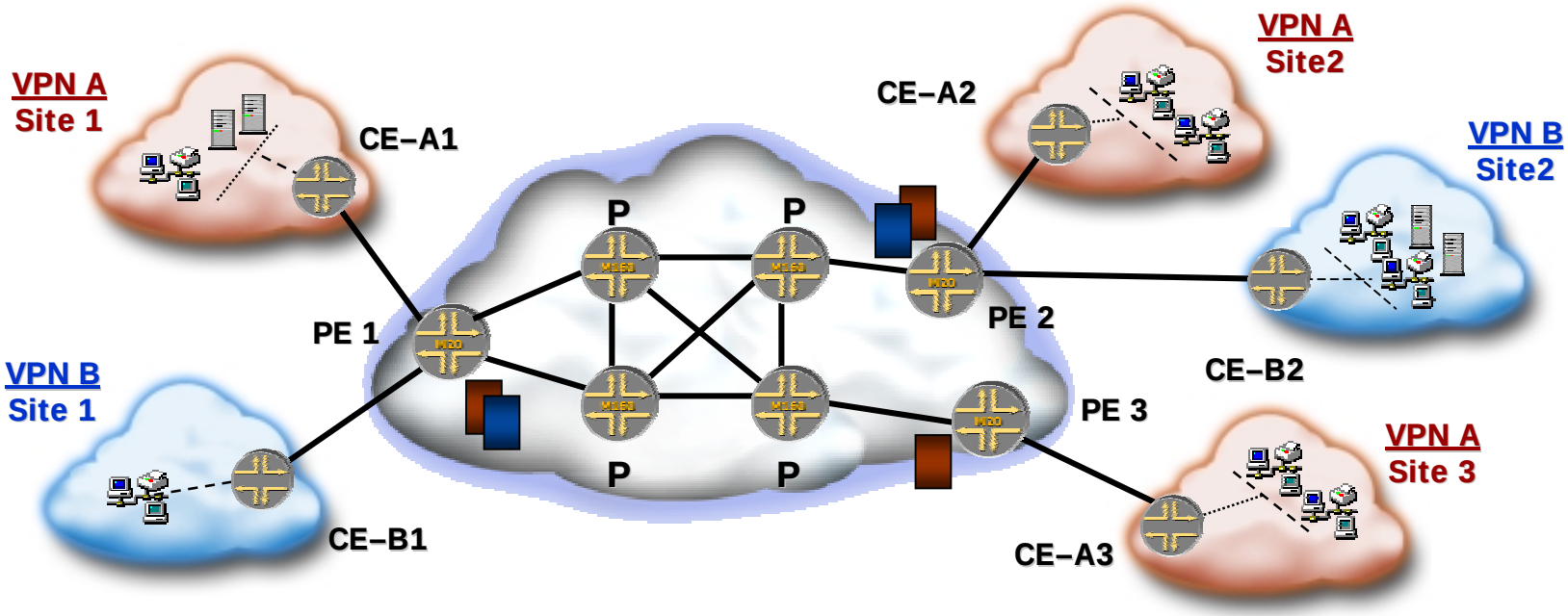
VPN Routing and Forwarding Tables (VRFs) (2547bis)



Overlapping Address Spaces (2547bis)



Operational Model Overview (2547bis)

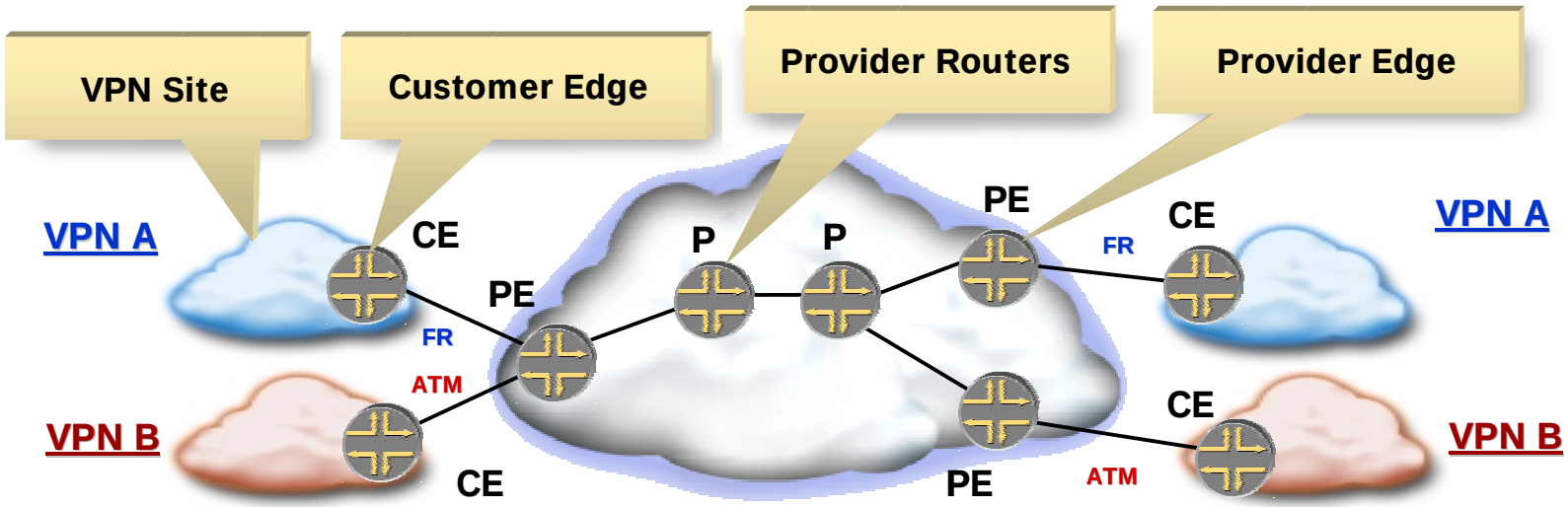


- **Control Flow**
  - Routing information exchange between CE and PE (static, IGP, BGP)
  - Routing information exchange between PEs (M-BGP)
  - LSP establishment between PEs (RSVP or LDP signaling)
- **Data flow**
  - Forwarding user traffic

Agenda

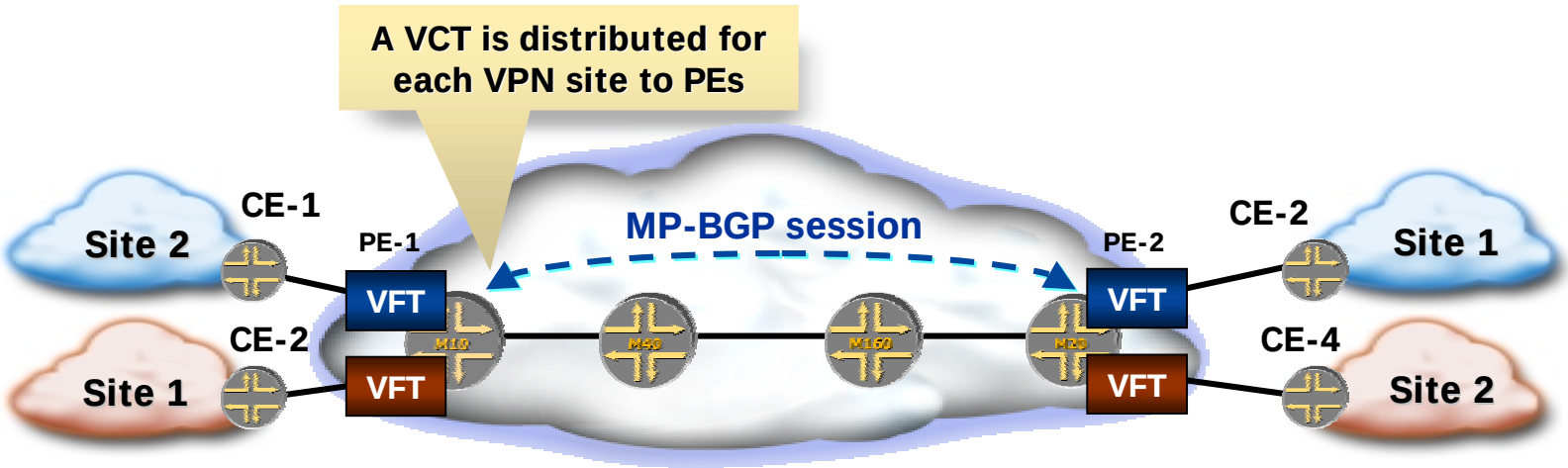
- MPLS Overview
- **Carrier-based VPNs**
  - BGP/MPLS VPNs (RFC 2547bis)
  - **MPLS Layer2 VPNs**
  - MPLS Layer 2.5 VPNs (Interworking)
  - VPLS (Virtual Private LAN Services)
  - InterProvider VPNs
  - Carrier of Carrier VPNs

Terminology (Layer2 VPN)



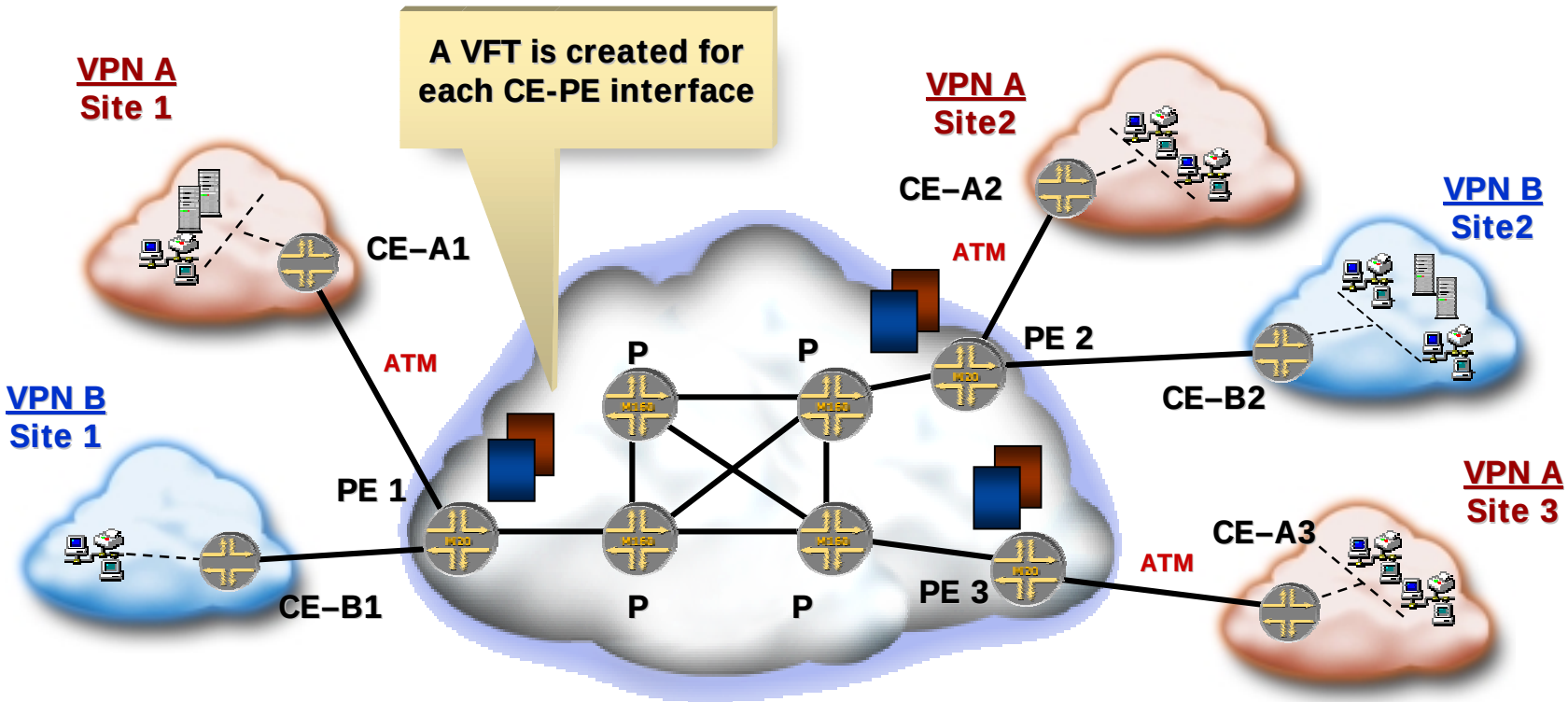
- Customer Edge device: device located on customer premises
- Provider Edge device: maintains VPN-related information, exchanges VPN information with other Provider Edge devices, encapsulates/decapsulates VPN traffic
- Provider router: forwards traffic VPN-unaware

VPN Connection Tables (VCT) (L2 VPN)



- VCT is configured info about the PE-CE connection
- Analogous to PE-CE routes in RFC 2547 VPNs
- VCTs are distributed among the PEs via MP-BGP

VPN Forwarding Tables (VFTs) (L2 VPN)

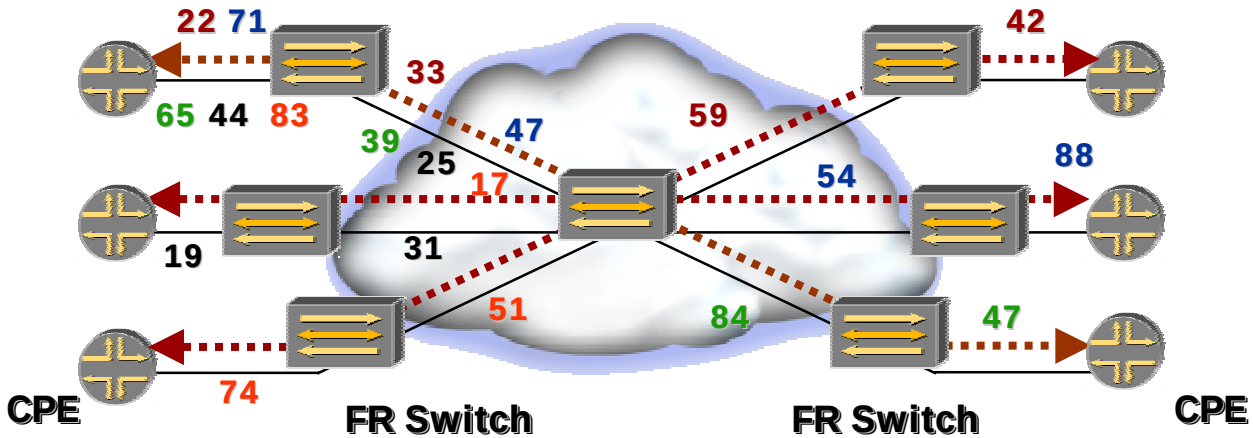


- Each VFT at a PE is derived from:
  - The local VCT at this PE
  - VCTs for the same VPN received from other PEs via MP-BGP
- Analogous to VRFs in RFC 2547

Provisioning Is the Key (L2 VPN)

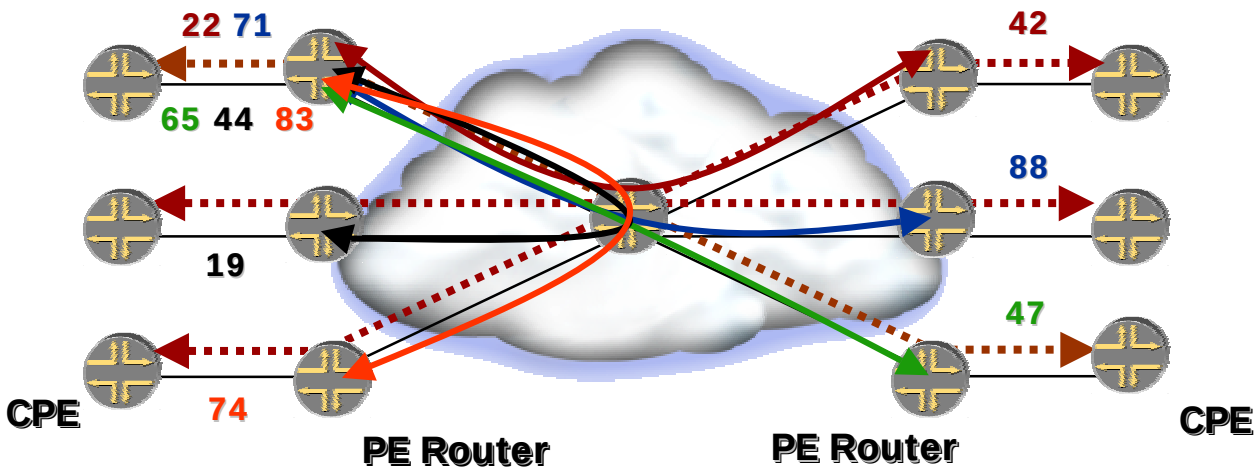
1. **Provision only boxes you have to**
   - Provision non-edge boxes just once
   - Provision only those edge boxes on which a VPN site is to be added, changed or deleted
   - Provision each edge box independently
2. **Use all the (protocol) help you can get**
   - Autodiscovery, signaling of “inner” labels
3. **Reuse common infrastructure, paradigms, management, monitoring, accounting**
   - Commonality with IP VPNs (RFC 2547)
4. **Keep it simple!**

Provisioning Frame Relay VPNs



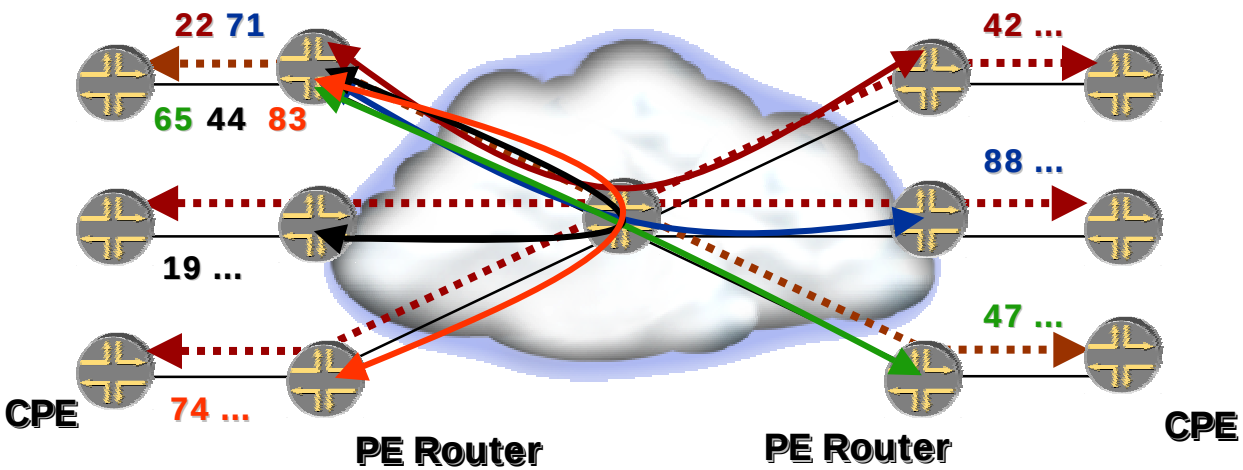
- Have to provision every switch in the path
- Have to 'touch' non-edge switch
  - A mistake here would affect many customers
  - Usually more than one non-edge switch

LDP-based Provisioning (L2 VPN)



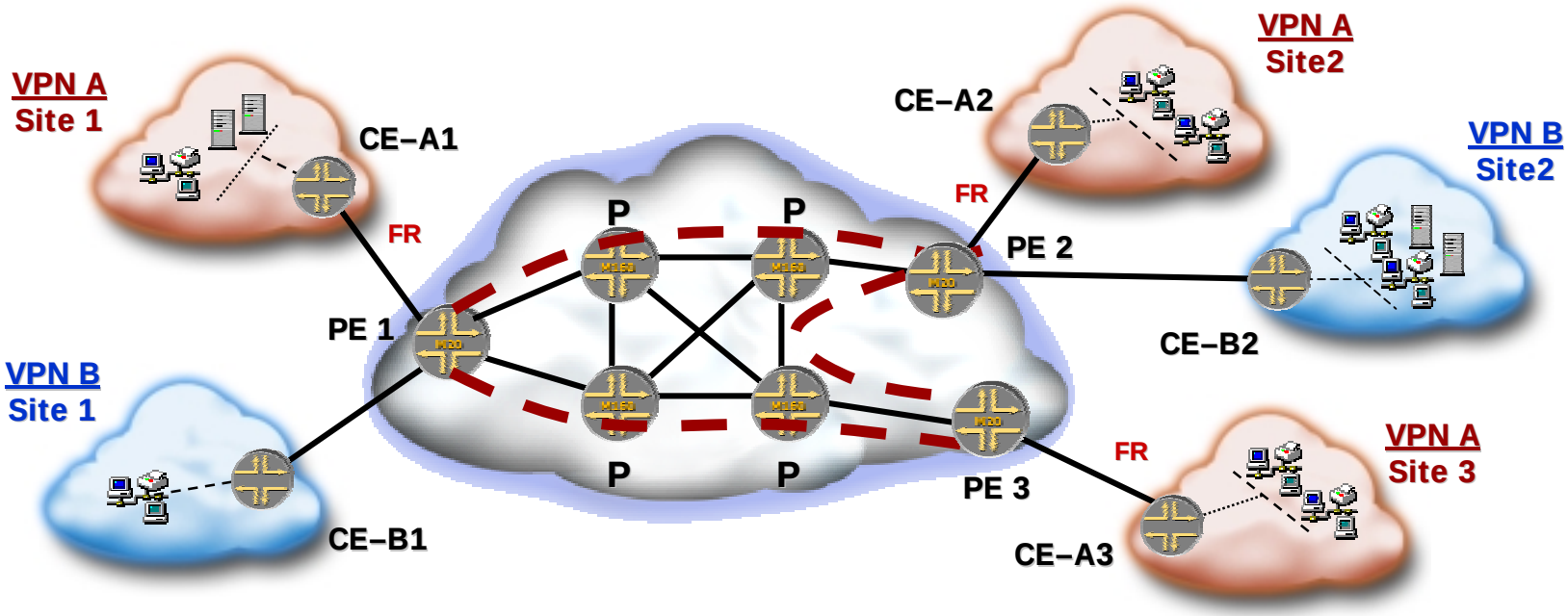
- Don’t have to provision non-edge boxes (+)
- Have to provision each *pair* of PE routers (-)
- Each added site means provisioning between 2 and N sites (--)

BGP-based Provisioning (L2 VPN)



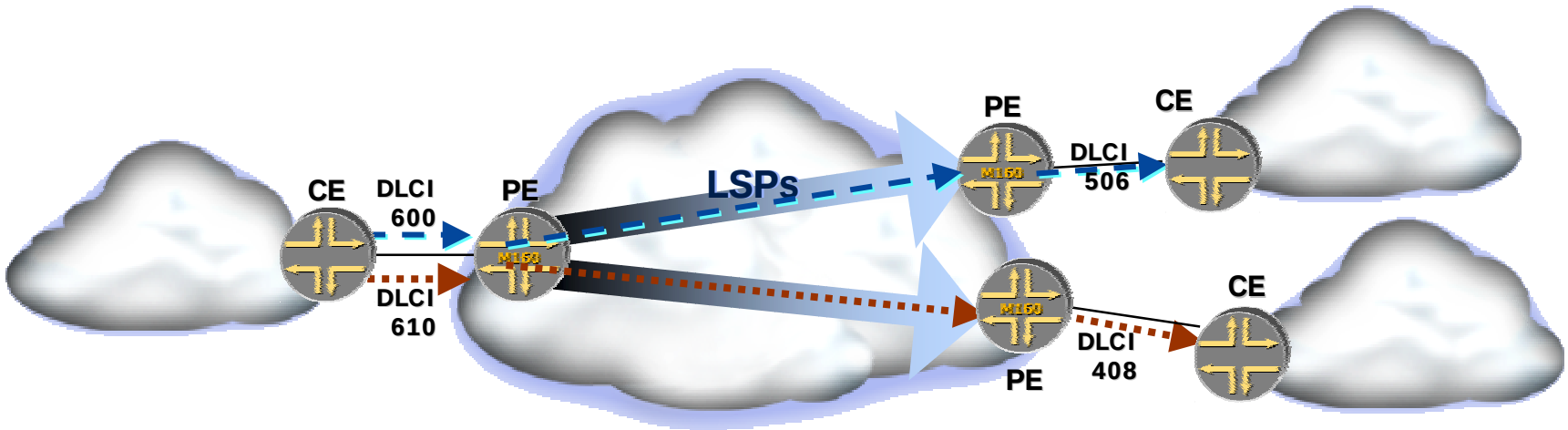
- Don't have to provision non-edge boxes (+)
- Provision each PE router independently (++)
- Can "over-provision", in which case each change only requires touching one PE (++)

Provisioning Non-edge Boxes Once (L2 VPN)



- LSPs between PEs must be pre-established
  - *Signaled* using LDP or RSVP-TE
- LSPs may be used for many services: Internet, VoIP, L2 and L3 VPNs, and Circuit Emulation
- P routers need not be configured again ☺

“Point-to-point” Layer 2 VPNs



- Customer frames are switched based on DLCI / VCI / VLAN
  - Each DLCI from a CE identifies a path to a remote CE
- The (LSP+inner label) is essentially a continuation of Frame Relay virtual circuit
  - If a frame sent on DLCI 600 goes to CE x, then a frame received on DLCI 600 comes from CE x
- Customer’s experience is exactly the same as with a traditional Frame Relay VPN

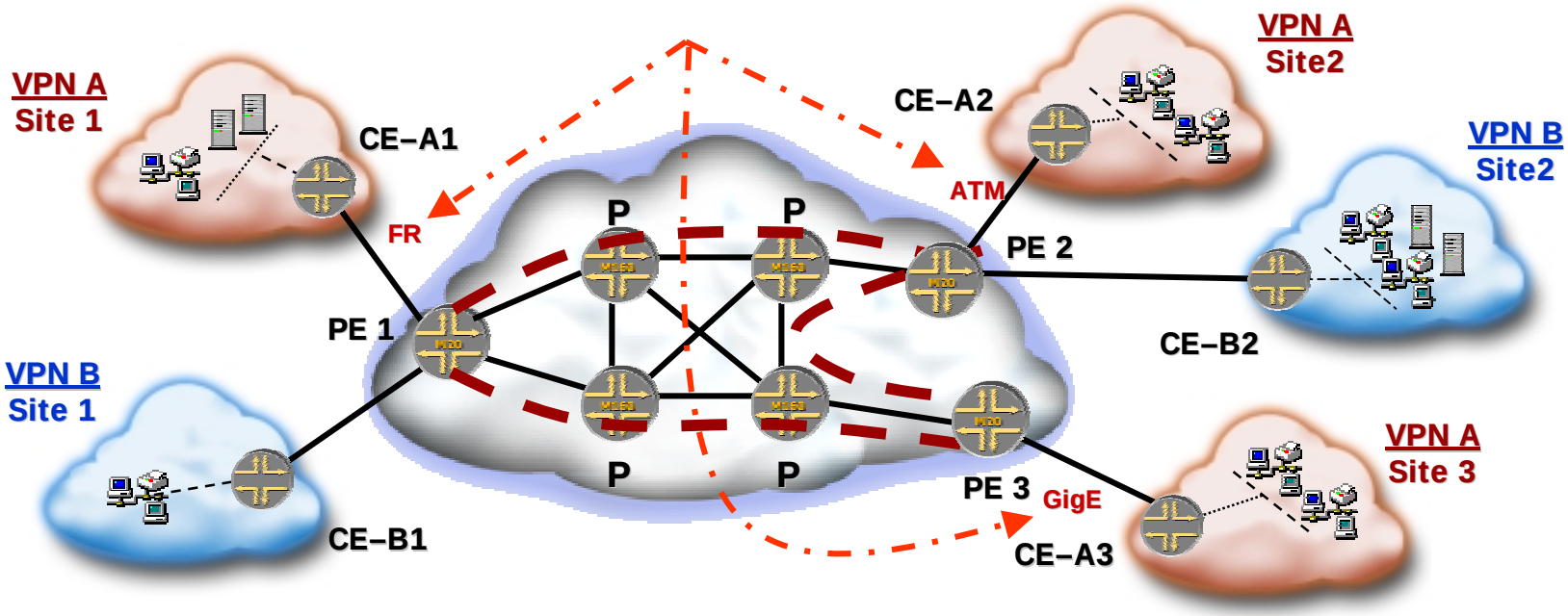
Layer 2 Frame Transport (L2 VPN)

- Encapsulation of FR/ATM/Ethernet is per draft-martini-l2circuit-encap-mpls
  - Used both for L2 VPNs and L2 Circuits
- For example, for Frame Relay: at the ingress, the DLCI is removed, replaced by a two-label stack and a control word
- At the egress, the label stack is popped, the control word consulted and removed, and a new DLCI is added

Agenda

- MPLS Overview
- **Carrier-based VPNs**
  - BGP/MPLS VPNs (RFC 2547bis)
  - MPLS Layer2 VPNs
  - **MPLS Layer 2.5 VPNs (Interworking)**
  - VPLS (Virtual Private LAN Services)
  - InterProvider VPNs
  - Carrier of Carrier VPNs

IP Interworking



- In a pure Layer 2 network, all access circuits should be the same – e.g., all Frame Relay
- IP interworking mode allows the access circuits to be different: Frame Relay, ATM, Gig Ethernet

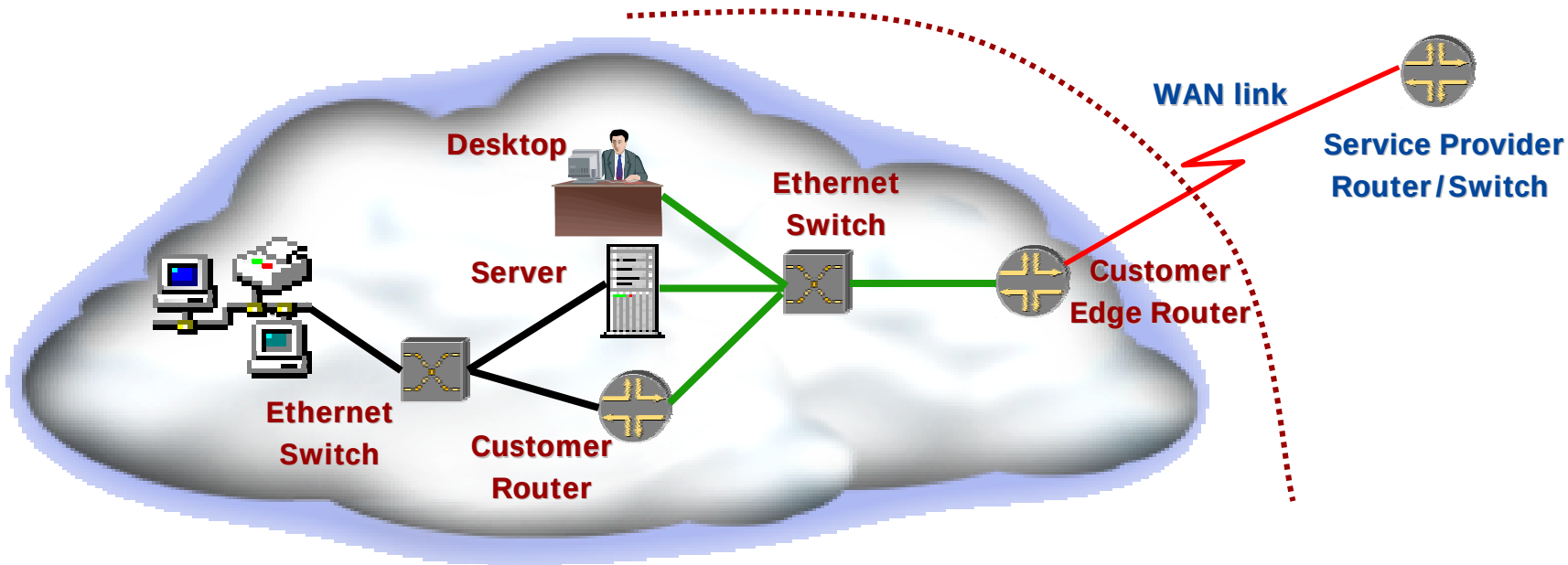
“Layer 2.5” VPN

- In IP Interworking, switching is done based on Layer 2 address
- However, this is restricted to IP packets
  - Gives up Layer 3 independence
  - Gains Layer 2 independence
- This avoids recognizing and carrying L3 protocol across the SP network
- This does not preclude standard interworking (such as Frame Relay↔ATM)

Agenda

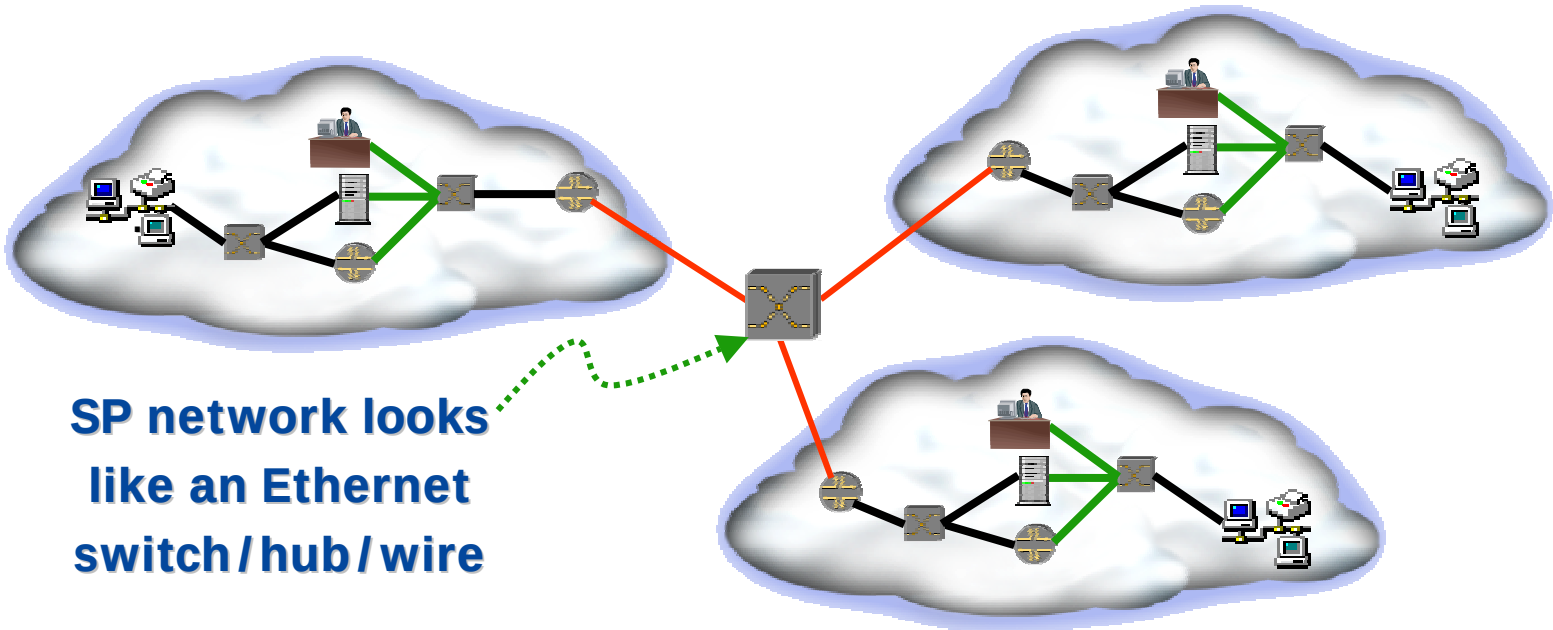
- MPLS Overview
- **Carrier-based VPNs**
  - BGP/MPLS VPNs (RFC 2547bis)
  - MPLS Layer2 VPNs
  - MPLS Layer 2.5 VPNs (Interworking)
  - **VPLS (Virtual Private LAN Services)**
  - InterProvider VPNs
  - Carrier of Carrier VPNs

Typical Corporate Network



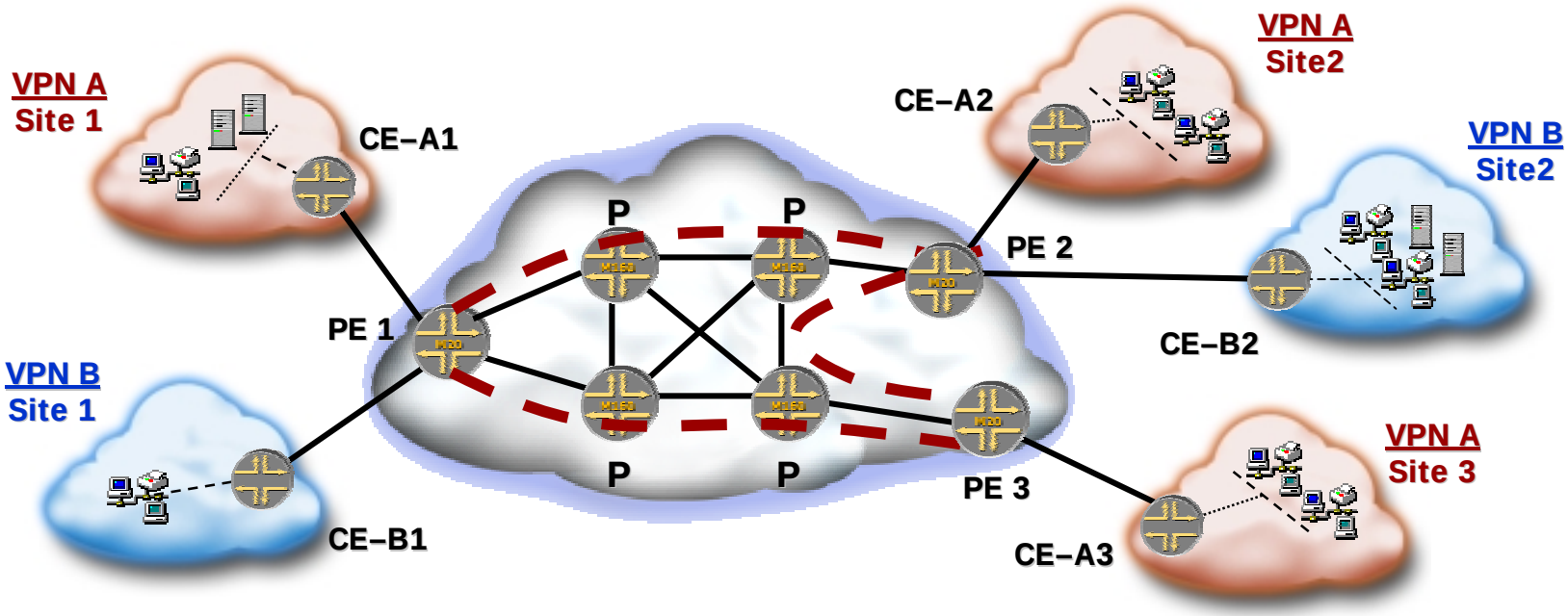
- Intra-building connectivity via Ethernet
- Broadcast domains (LANs) broken up by routers
- External connectivity via a WAN link from a router

New Corporate Network



- Intra-building connectivity via Ethernet
- Broadcast domains (LANs) broken up by routers
- External connectivity via VPLS – just another Ethernet

Virtual Private LAN Service



- **Make SP network look like an Ethernet switch / hub / wire segment to the CEs**
  - **Depends on how much is emulated**

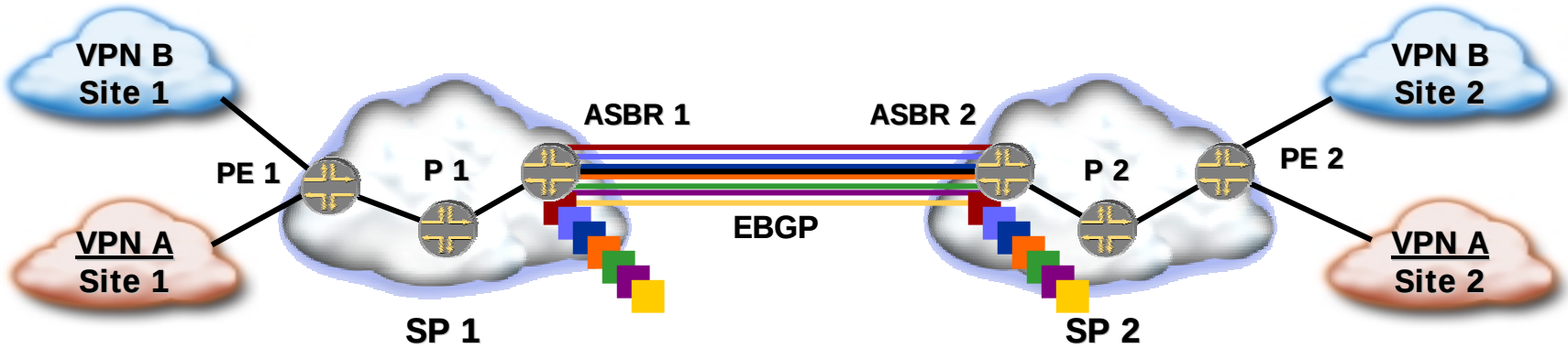
VPLS Operation

- Sending to an unknown MAC address
  - “Flood” to all members of the VPLS
- Sending to a known MAC address
  - Mapping to <outer label, inner label> exists
- Receiving from some MAC address y
  - Identify the sender; find the label stack that will reach that sender, and map MAC address y to that label stack in the MAC address cache
- Periodically, age out unused entries from the MAC address cache

Agenda

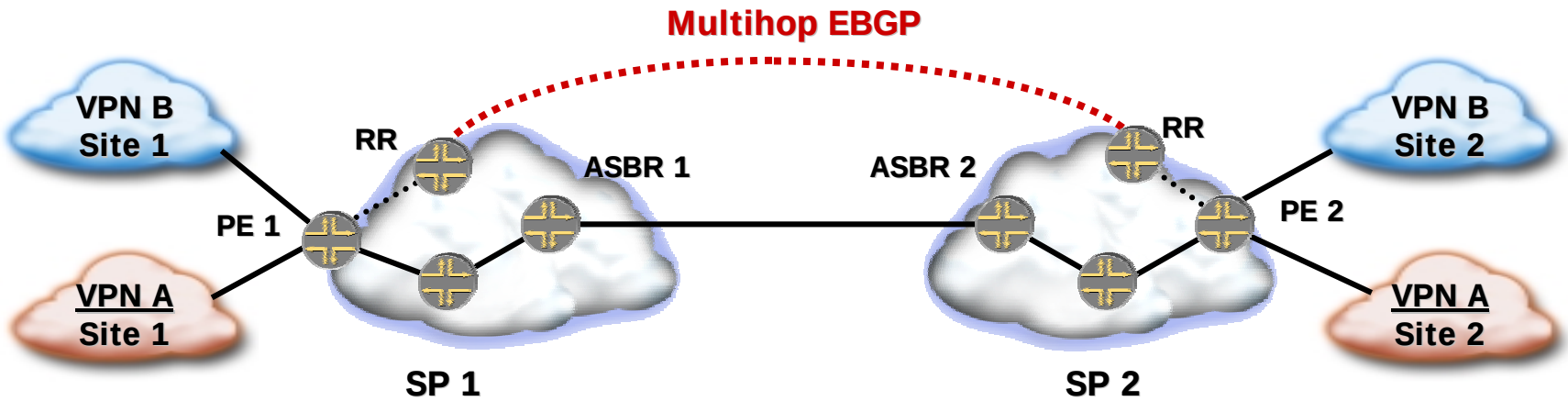
- MPLS Overview
- **Carrier-based VPNs**
  - BGP/MPLS VPNs (RFC 2547bis)
  - MPLS Layer2 VPNs
  - MPLS Layer 2.5 VPNs (Interworking)
  - VPLS (Virtual Private LAN Services)
  - **InterProvider VPNs**
  - Carrier of Carrier VPNs

Inter-AS Operation: VRF-to-VRF Connections Between ASBRs



- AS boundary routers act as PEs
  - Connected directly together
  - A separate sub-interface is required for every VRF
- Each ASBR/PE treats the other as a CE
- Questionable scalability

Inter-AS Operation: Multihop EBGP



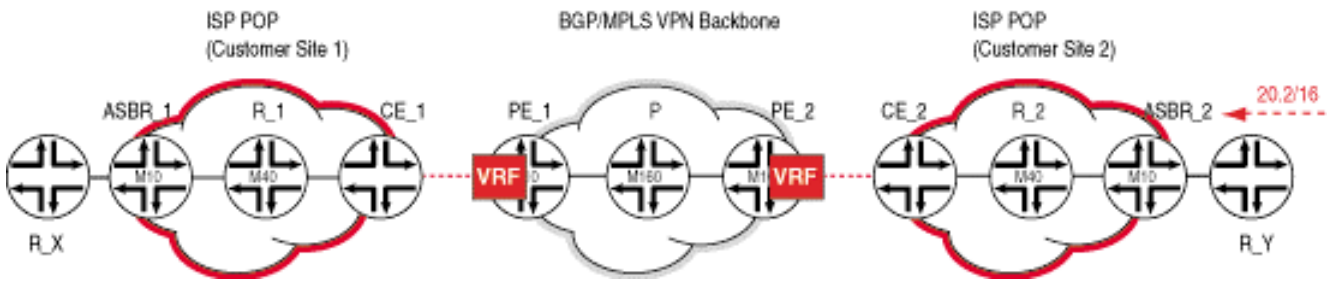
- Advertise labeled IPv4 /32 routes into other AS
- Establish LSP between ingress and egress PE
- Use multihop EBGP
- If /32 PE addresses not advertised to P router can use 3-level label-stack
- ASBR is not aware of VPN-IPv4 routes

Agenda

- MPLS Overview
- **Carrier-based VPNs**
  - BGP/MPLS VPNs (RFC 2547bis)
  - MPLS Layer2 VPNs
  - MPLS Layer 2.5 VPNs (Interworking)
  - VPLS (Virtual Private LAN Services)
  - InterProvider VPNs
  - **Carrier of Carrier VPNs**

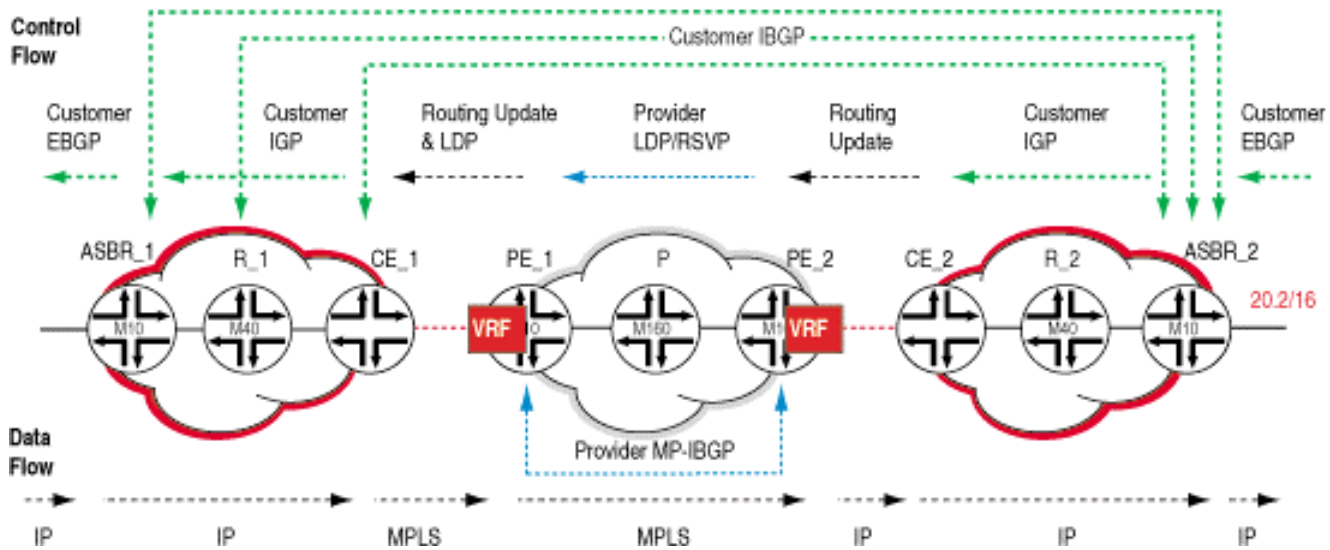
Carrier of Carrier VPNs

- **Two separate cases contained in RFC2547bis:**
  1) **Carrier customer is just a basic Internet Service Provider**
  2) **Carrier customer is another L2 / L3 VPN service provider**
     - **Also known as hierarchical carrier of carriers BGP/MPLS VPNs**
- **Goal: Carrier's Carrier to avoid learning full Internet / IP VPN routes from customer carrier's CE**
- **Internal Vs External routes.**



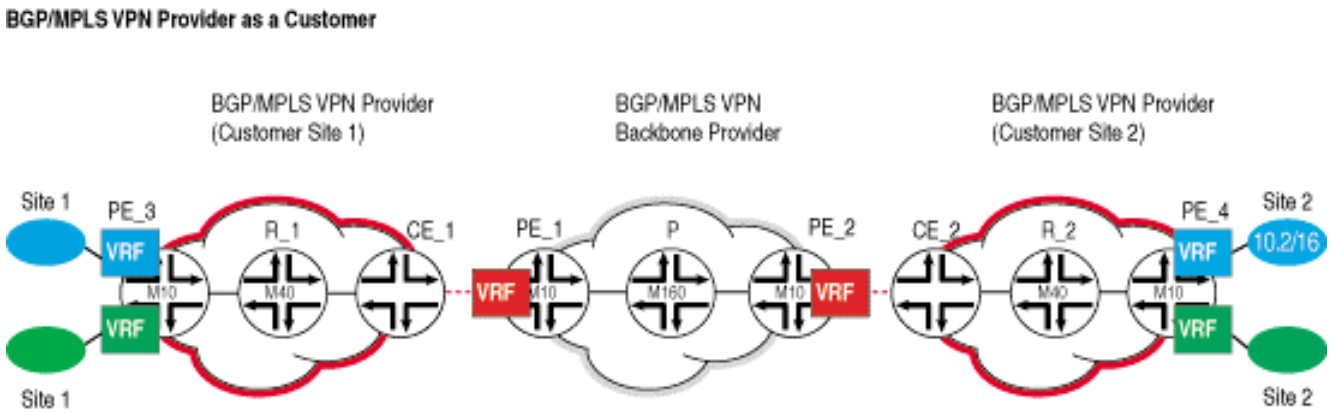
Carrier's Carrier – ISP Customer

- Customer carrier provides basic Internet services to its customers
  - MPLS not required in the customer carrier's network.
  - MPLS needed:
    - Within the carrier's carrier backbone network
    - Between the CE of the customer carrier and the PE of the carrier's carrier
      - MP-BGP label distribution for IPv4 routes (RFC 3107) or
      - LDP & IGP



Carrier's Carrier - VPN SP customer

- Customer carrier provides L3/L2 VPN services to their customers
  - Also known as hierarchical carrier of carriers BGP/MPLS VPNs
  - MPLS connectivity between customer carrier PE routers required (below, this would be PE_3 and PE_4).
  - Once MPLS connectivity is operational between carrier PE routers, both L2 and L3 VPNs can be provisioned



Agenda

- MPLS Overview
- Carrier-based VPNs
  - BGP/MPLS VPNs (RFC 2547bis)
  - MPLS Layer2 VPNs
  - MPLS Layer 2.5 VPNs (Interworking)
  - VPLS (Virtual Private LAN Services)
  - InterProvider VPNs
  - Carrier of Carrier VPNs
- Summary

Summary

Customers want:

- **Point-to-point Layer 2 VPNs**
  - **Sometimes, with IP interworking**
- **Virtual Private LAN Service**
- **IP VPNs (RFC 2547)**

Service Providers can offer all of the above:

- **over a common infrastructure (MPLS)**
- **with a common framework (MP-BGP)**
- **with common concepts (RD, RT, VFTs, …)**

References

- draft-ietf-ppvpn-rfc2547bis
- draft-kompella-ppvpn-l2vpn
- draft-kompella-ppvpn-vpls
- draft-kompella-ppvpn-dtls
- draft-lasserre-vkompella-ppvpn-vpls
- draft-martini-l2circuit-encap-mpls
- draft-martini-l2circuit-trans-mpls

Obrigado!

http://www.juniper.net

roosevelt@juniper.net