Cisco Expo 2008

Connecting Enterprises Over Service Provider Networks

Boštjan Fele

Network Consulting Engineer
Advanced Services
WWSP WiMax Practice

Enable Your Network
Empower Your Business

Agenda

- **MPLS overview**

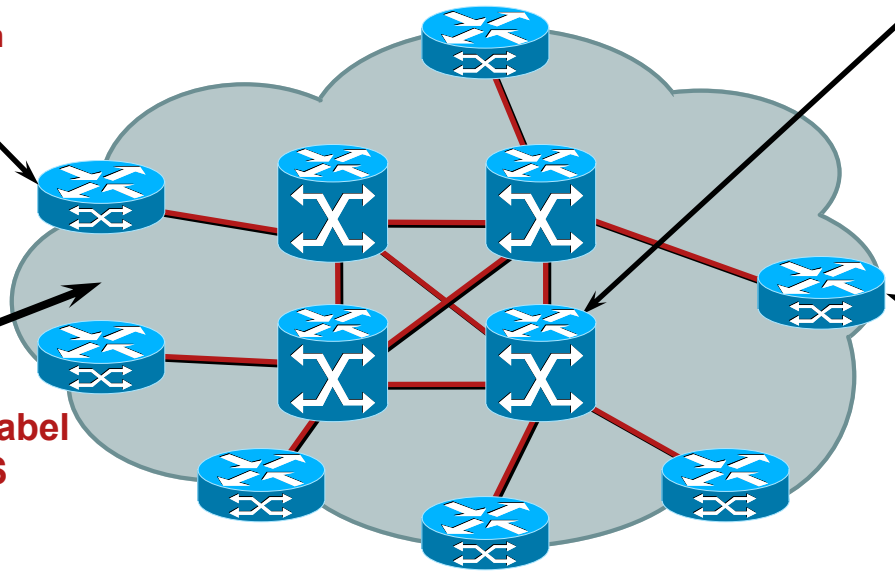
- VPNs overview
- L3 VPNs
- L2 VPNs

- Inter-AS VPNs

MPLS Concepts and Components

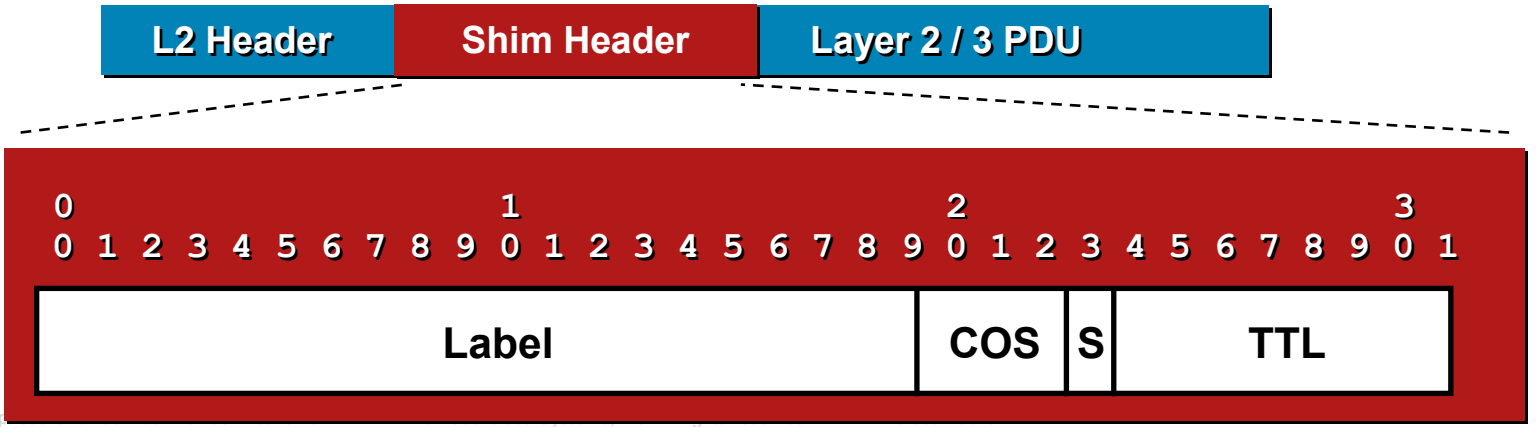
- Label Edge Router (LER)
  - Classify packets
  - Label imposition

- Label Switch Router (LSR)
  - Forward based on labels
  - Label indicates destination and service class
  - Label swapping and switching

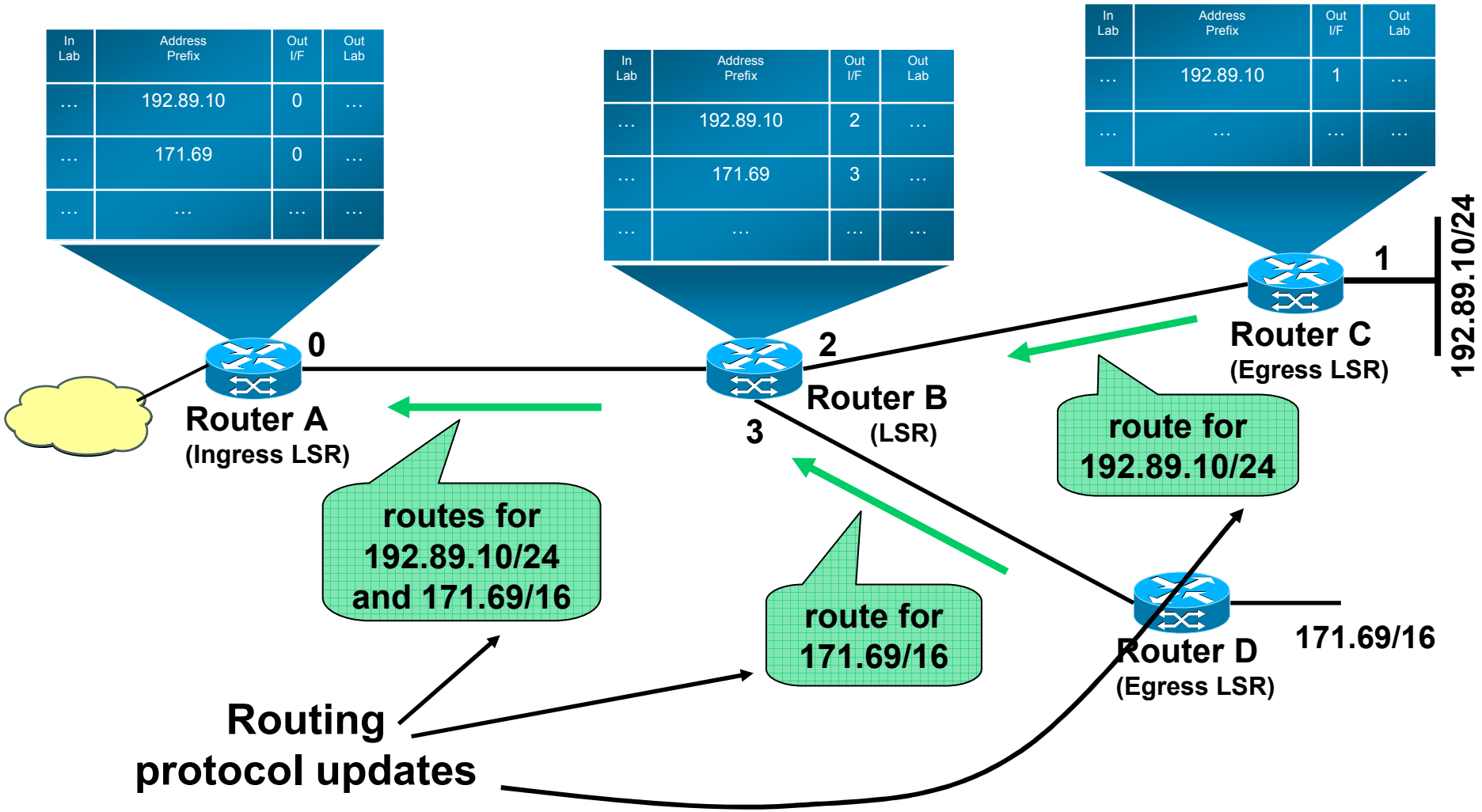


LDP distributes IP to label bindings across MPLS core

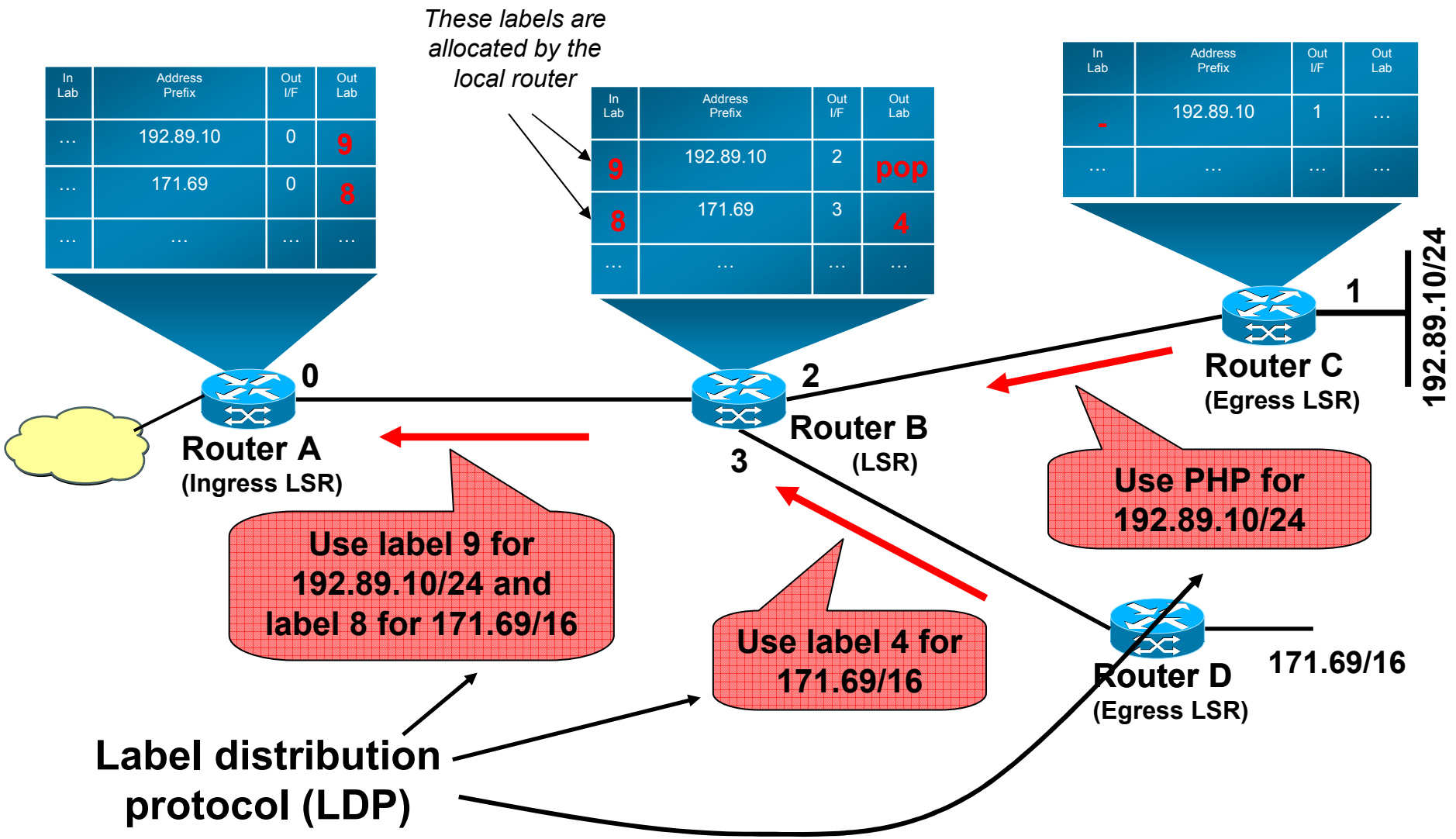
- Label Edge Router (LER)
  - Remove label and forward packets
  - Label disposition



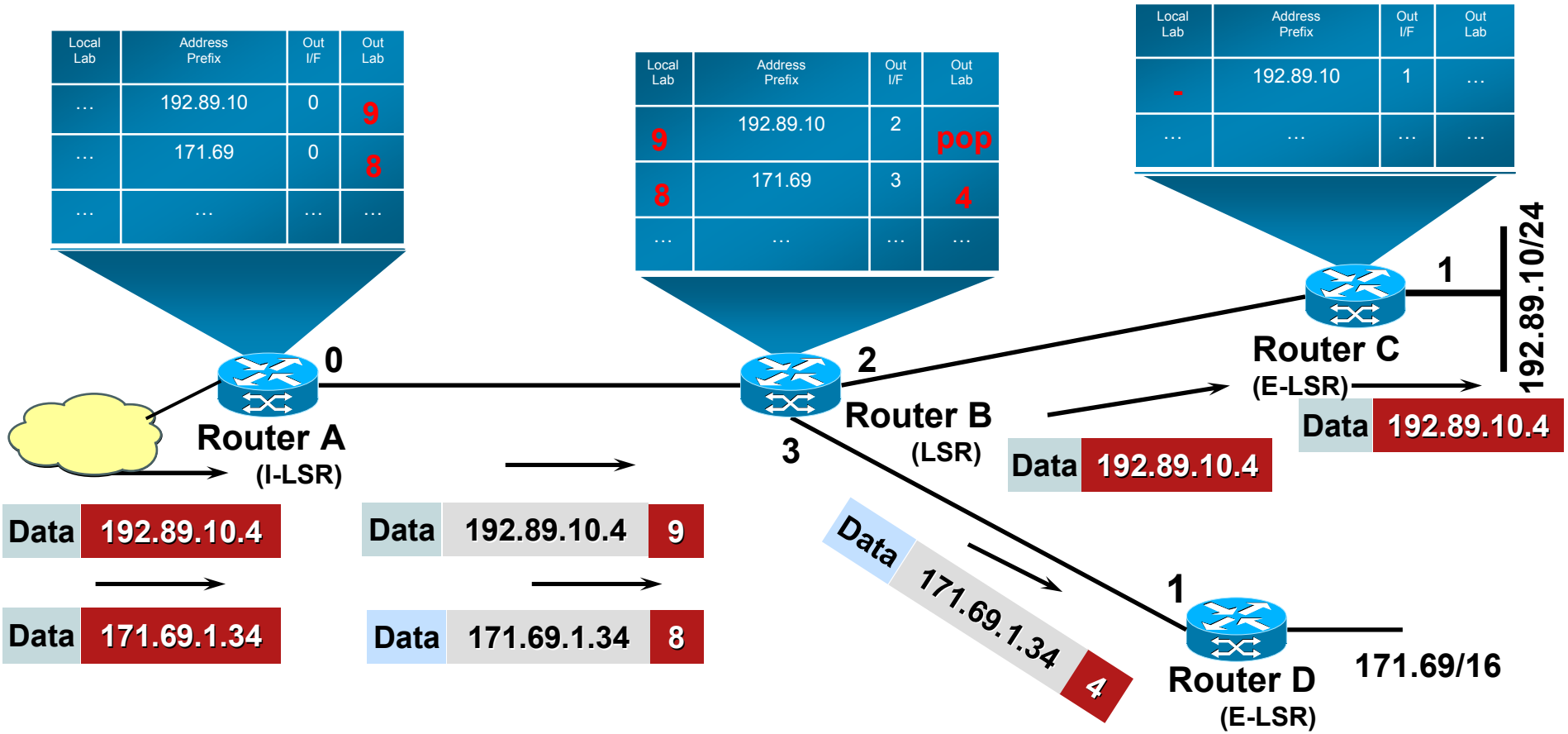
Step 1 (Control Plane): Building Routing Tables



Step 2 (Control Plane): Exchange Labels



Step 3 (Data Plane): Label Forwarding

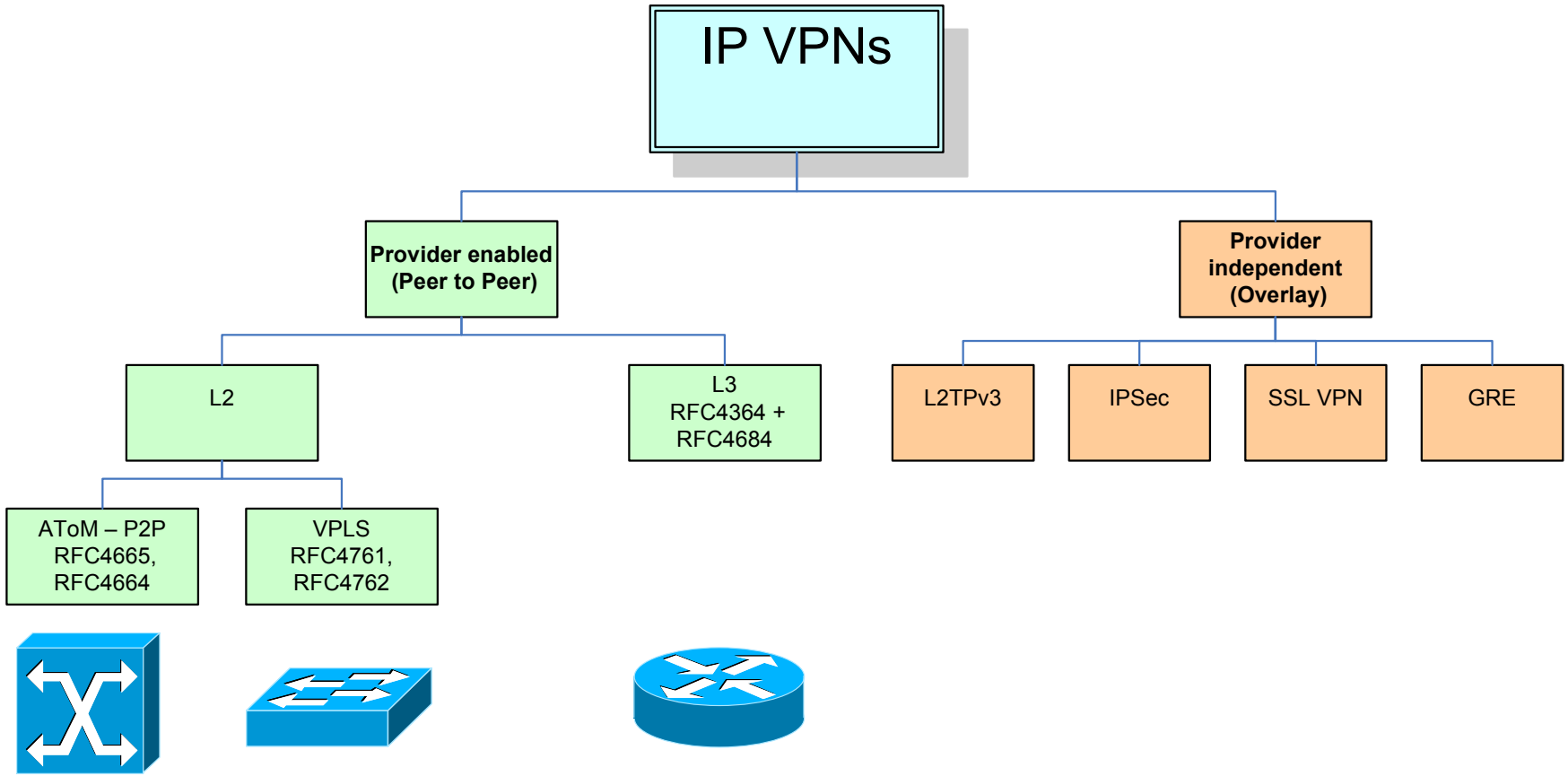


Agenda

- MPLS overview
- **VPNs overview**
- L3 VPNs
- L2 VPNs
- Inter-AS VPNs

IP VPNs

- VPN is a set of sites which are allowed to communicate with each other.

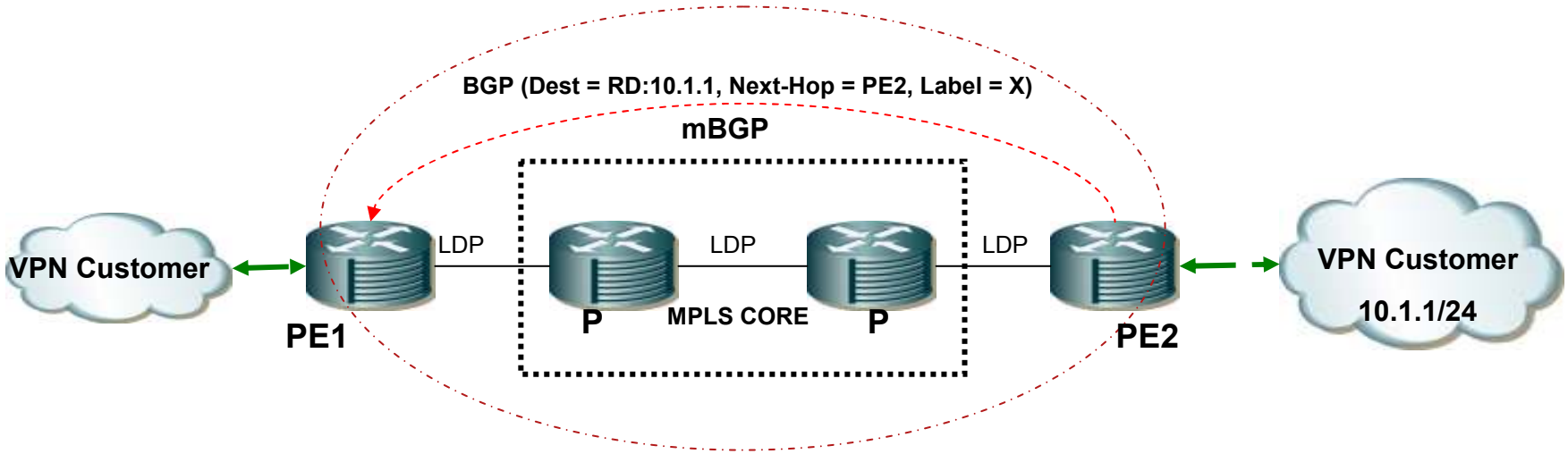


Agenda

- MPLS overview
- VPNs overview
- **L3 VPNs**
- L2 VPNs
- Inter-AS VPNs

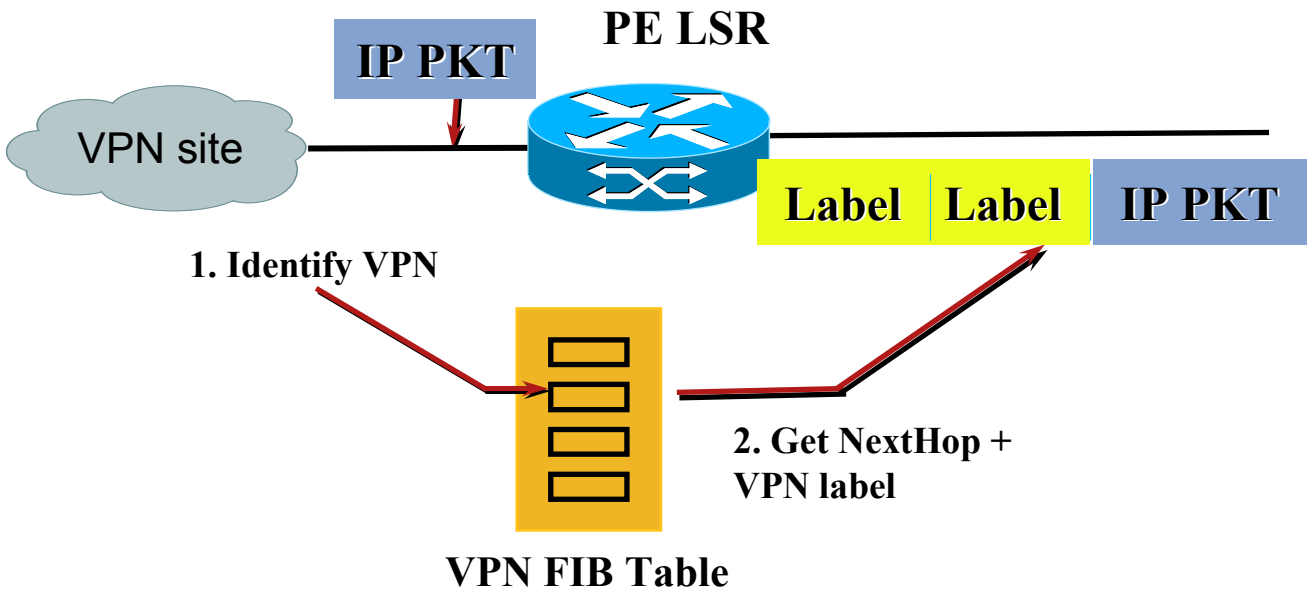
L3 VPN – Control Plane

- LDP establishes labeled transport path between MPLS routers (PE and P).
- CE-PE routers exchange routing information or static routes are configured.
- BGP redistributes routes with VPN labels between PE routers connecting same VPN.



L3 VPN – Forwarding Plane

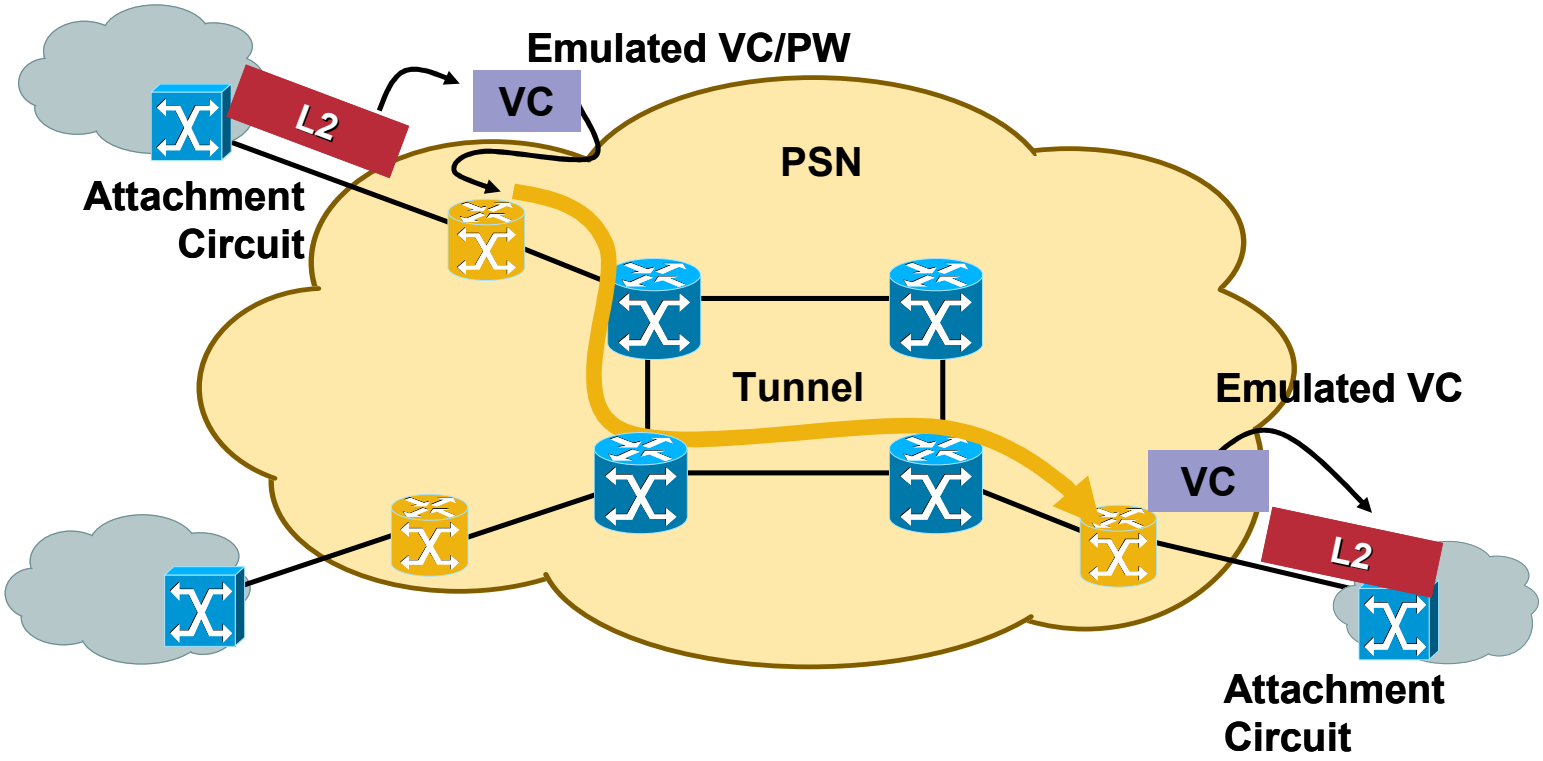
- PE router receives packet in VPN interface.
- Forwarding is done on VPN FIB. Get next-hop + VPN label.
- Next hop info is used to get transport label (IGP / LDP).



Agenda

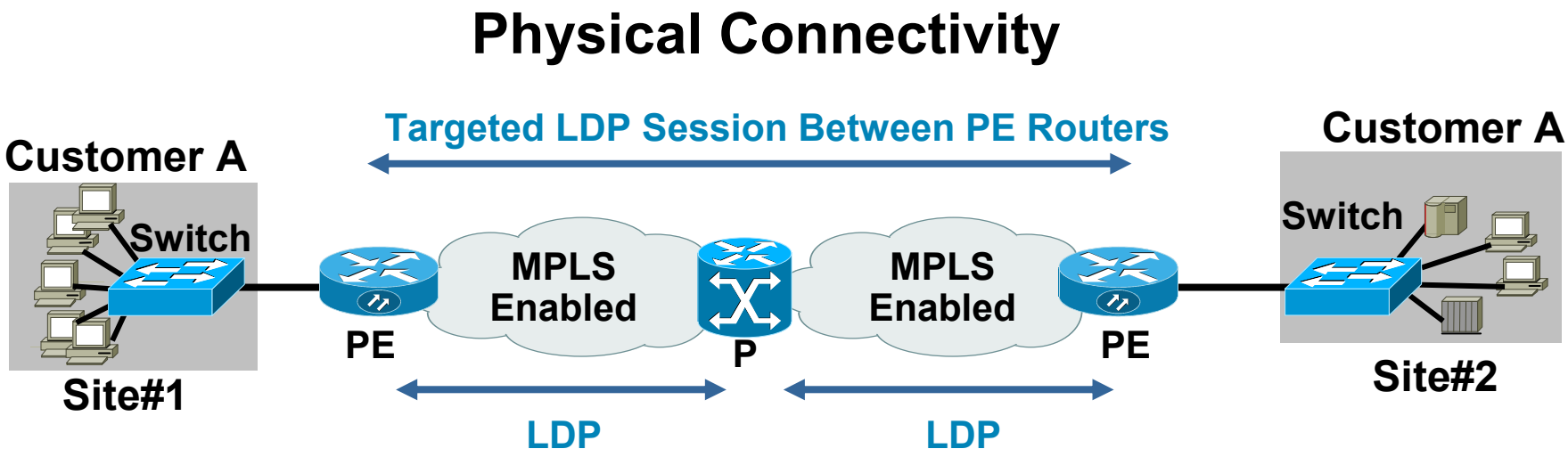
- MPLS overview
- VPNs overview
- L3 VPNs
- **L2 VPNs**
- Inter-AS VPNs

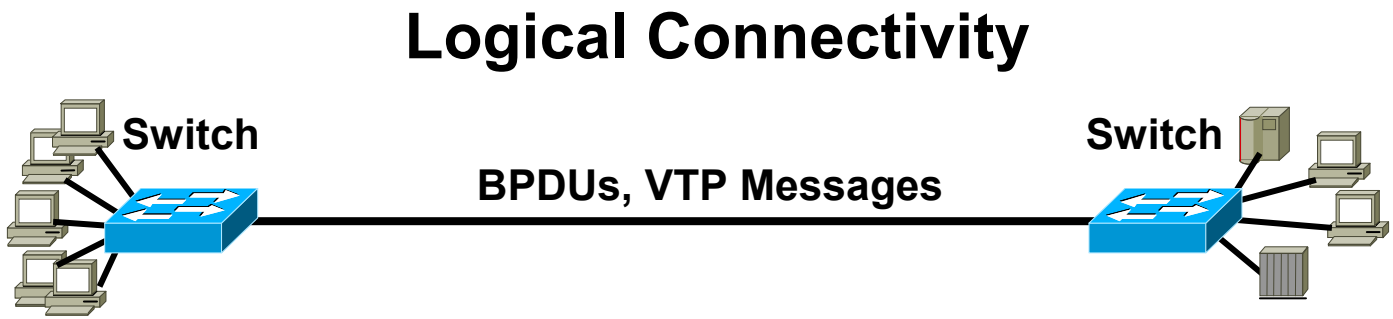
Generic L2 VPN



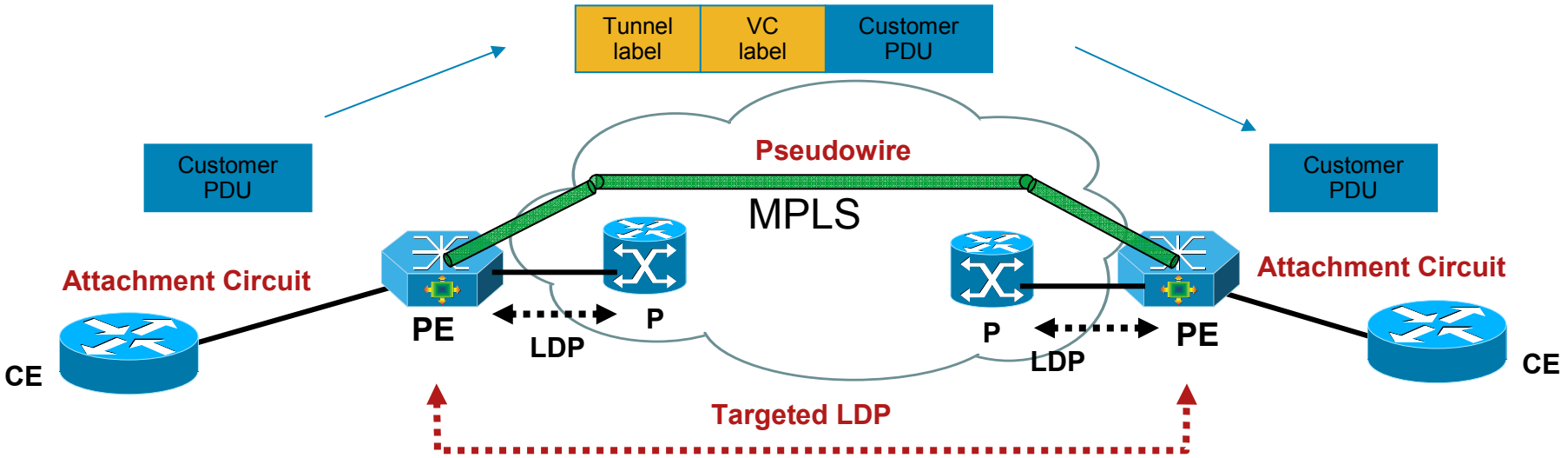
- Attachment VCs (e.g. FR DLCI, PPP / HDLC, Ethernet, VLAN) mapped to emulated VCs
- Connecting like-to-like interfaces (ATM – ATM, FR – FR, Ethernet – Ethernet) or with interworking but **P2P**
- Signaling with LDP

EoMPLS Reference Model



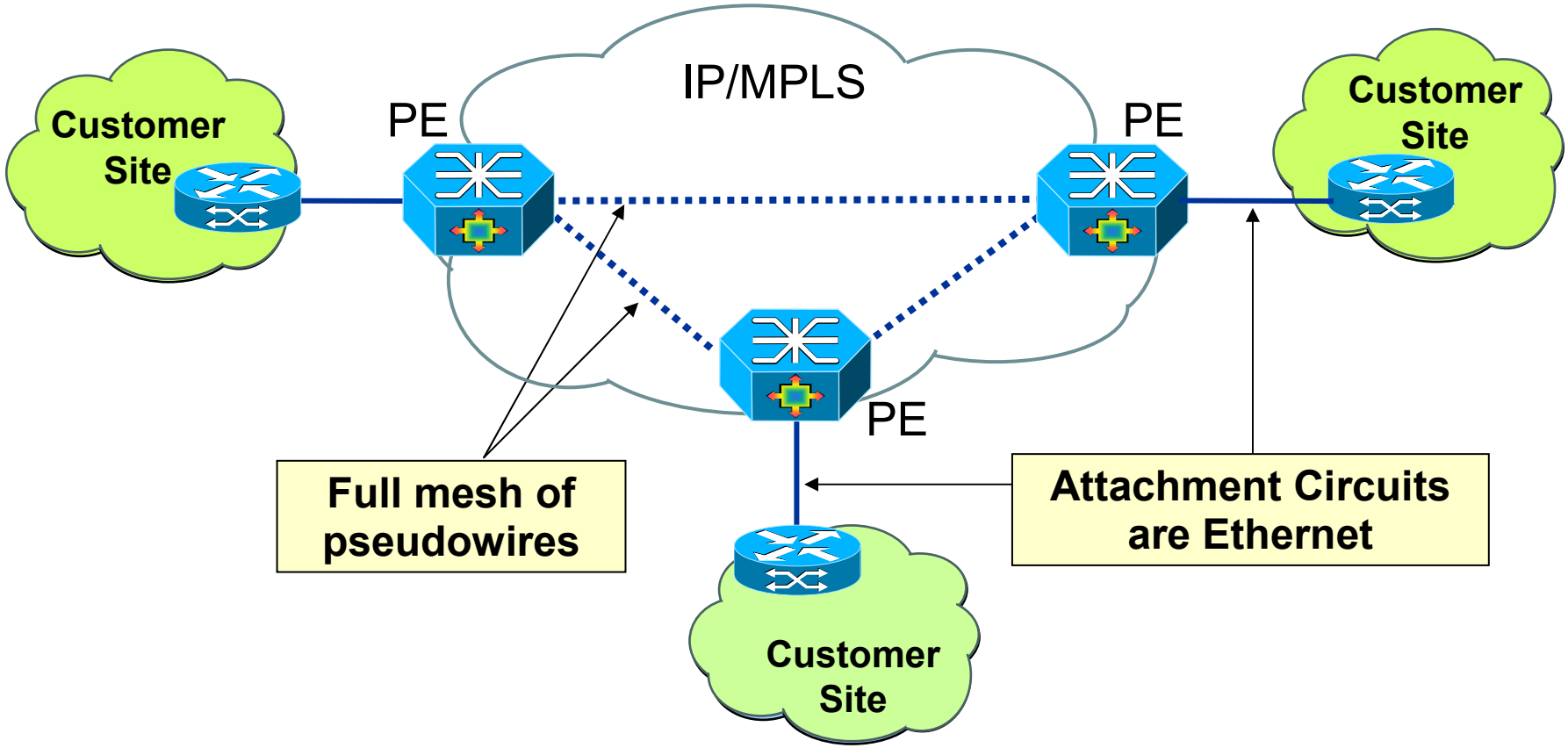


EoMPLS Overview



- MPLS in the core, normal LDP sessions per hop to exchange Tunnel label
- Targeted (AKA directed) LDP session between PEs to exchange VC (AKA PW label) label
- Tunnel label is used to forward packet from PE to PE
- VC label is used to identify L2VPN circuit
- Attachment Circuit (AC) – Connection to CE, it could be a physical Ethernet port, a logical Ethernet port - VLAN, and ATM PVC carrying Ethernet frames, etc
- Attachment circuit is mapped to EoMPLS PW.

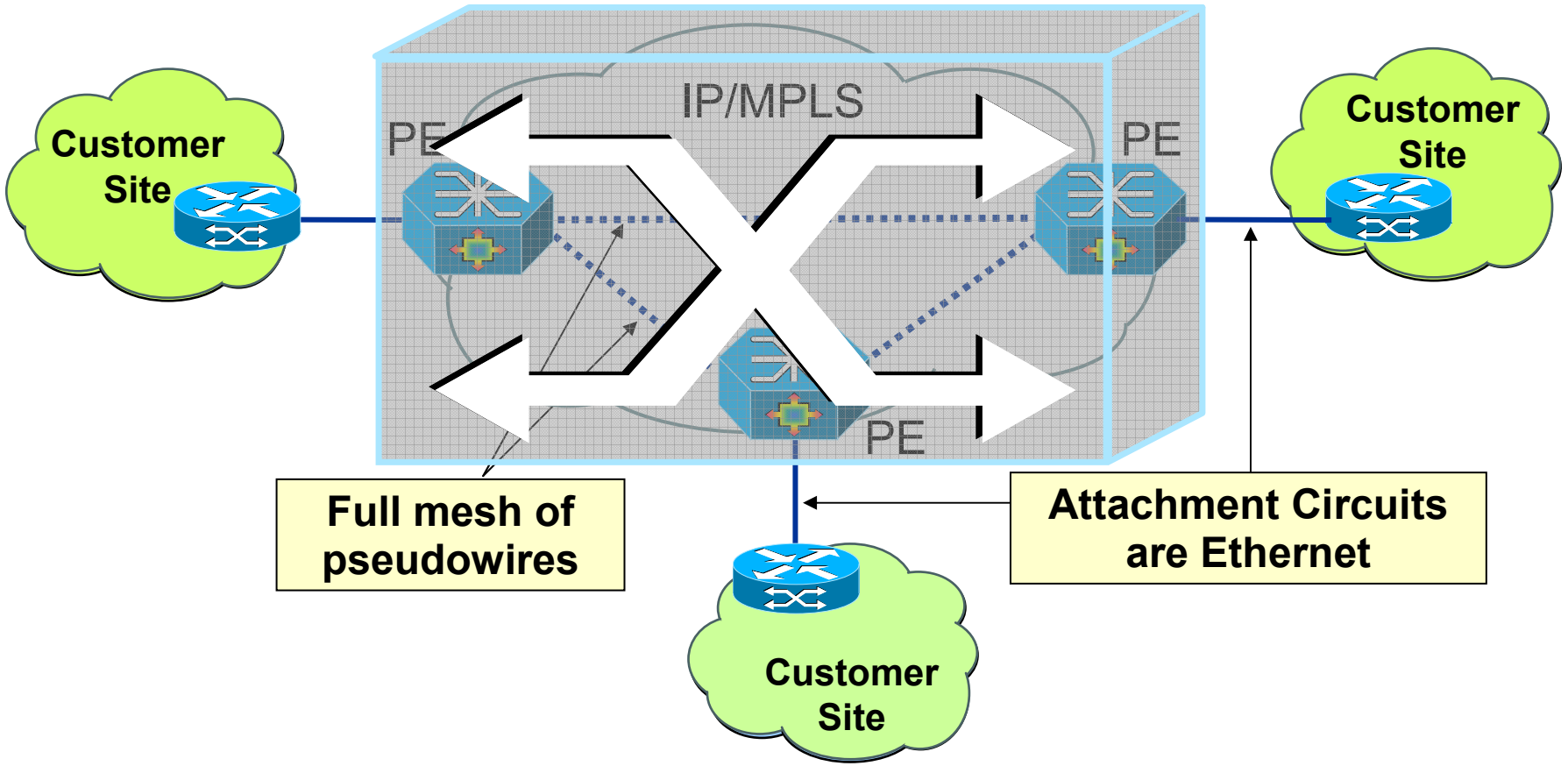
VPLS Reference Model



- The set of PE devices interconnected via PWs appears as a single emulated LAN to a customer

Ref: RFC 4762 Virtual Private LAN Service over LDP, January 2007

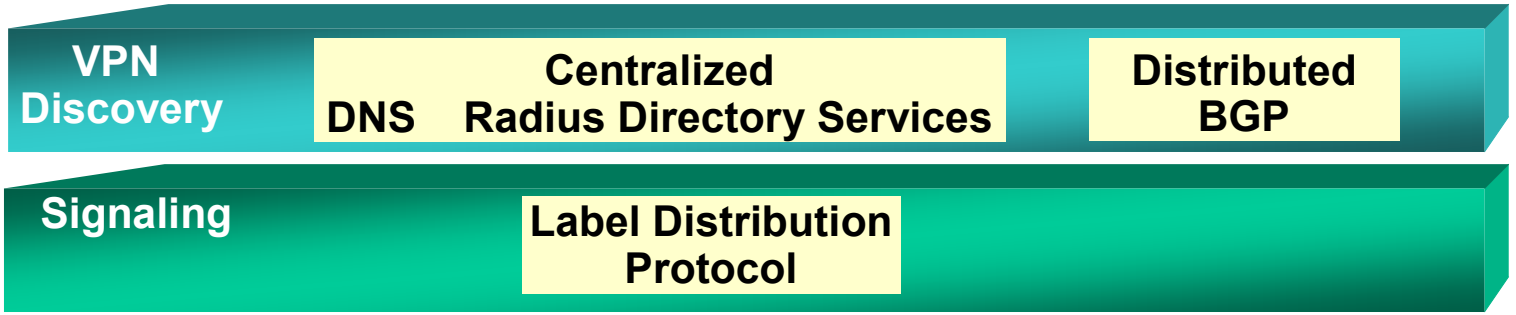
VPLS Reference Model



- The set of PE devices interconnected via PWs appears as a single emulated LAN to a customer

Ref: RFC 4762 Virtual Private LAN Service over LDP, January 2007

Control plan - VPLS Auto-discovery & Signaling



- Auto-discovery of VPN membership
  - Reduces VPN configuration and errors associated with configuration.
  - Draft-ietf-l2vpn-vpls-ldp-01 does not mandate an auto-discovery protocol. It can be BGP, Radius, DNS, AD based.
  - **BGP is the configuration agent for AutoDiscovery of VPN members.**

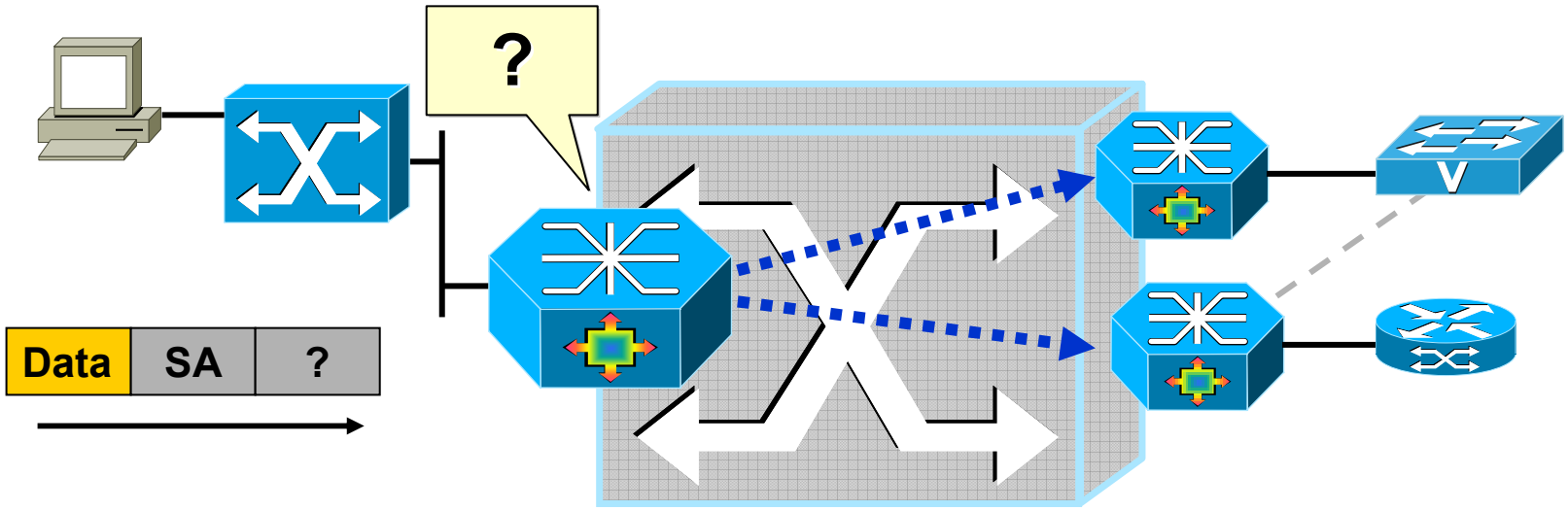
- Signaling of connections between PE devices associated with a VPN.
  - Same as EoMPLS, using directed LDP session to exchange VC information.

Layer 2 Forwarding Instance Requirements

A Virtual Switch MUST operate like a conventional L2 switch!

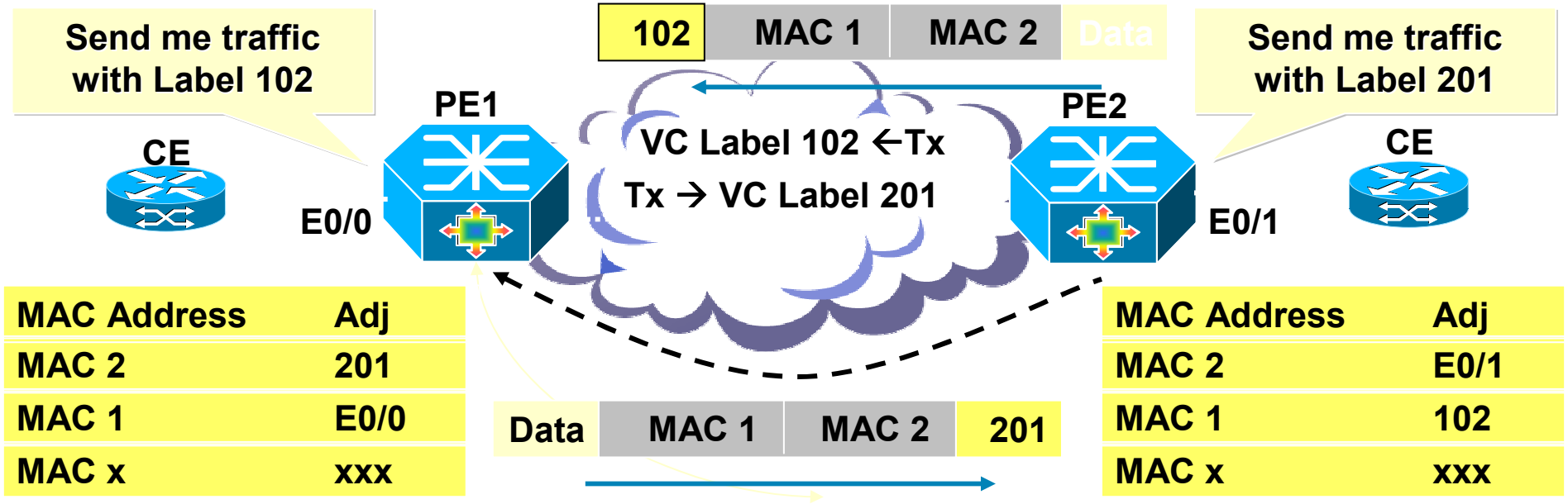
- Flooding/Forwarding:
  - Forwarding based on [VLAN, Destination MAC Address]
  - Unknwon Ucast/Mcast/Broadcast – Flood to all ports (IGMP snooping can be used to constrain multicast flooding)
- MAC Learning/Aging:
  - Dynamic learning based on Source MAC and VLAN
  - Refresh aging timers with incoming packet
- Loop Prevention:
  - Split Horizon + Full Mesh
  - Spanning Tree (possible but not desirable)

Flooding & Forwarding



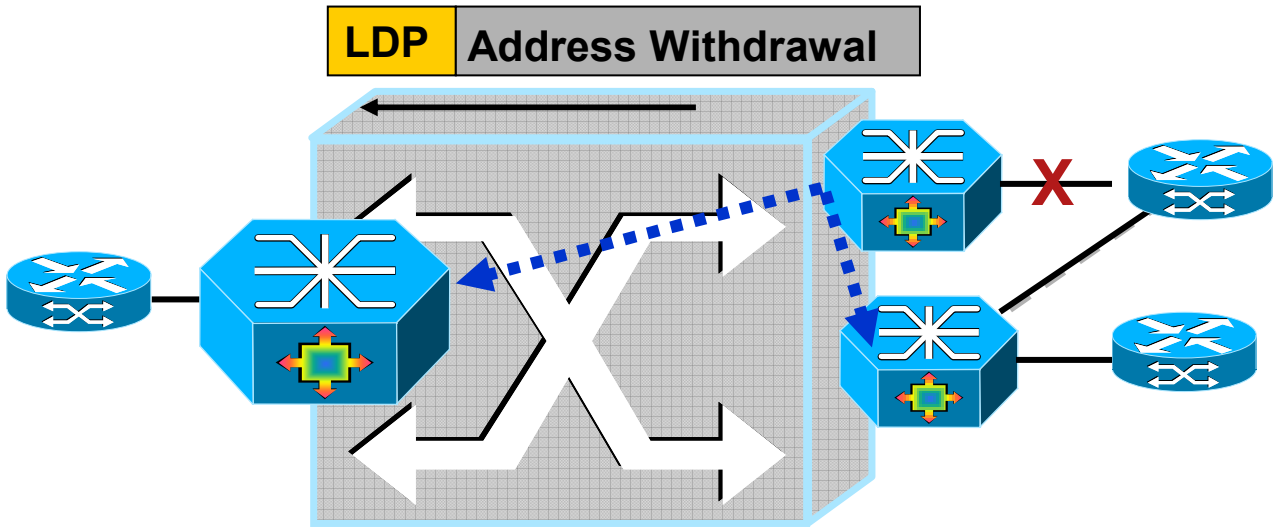
- Flooding (Broadcast, Multicast, Unknown Unicast) (IGMP snooping can be used to constrict multicast flooding)
- Dynamic learning of MAC addresses on PHY and VCs
- Forwarding
  - -Physical port
  - -Virtual circuit
- VSI will participate in learning, forwarding process

MAC Address Learning



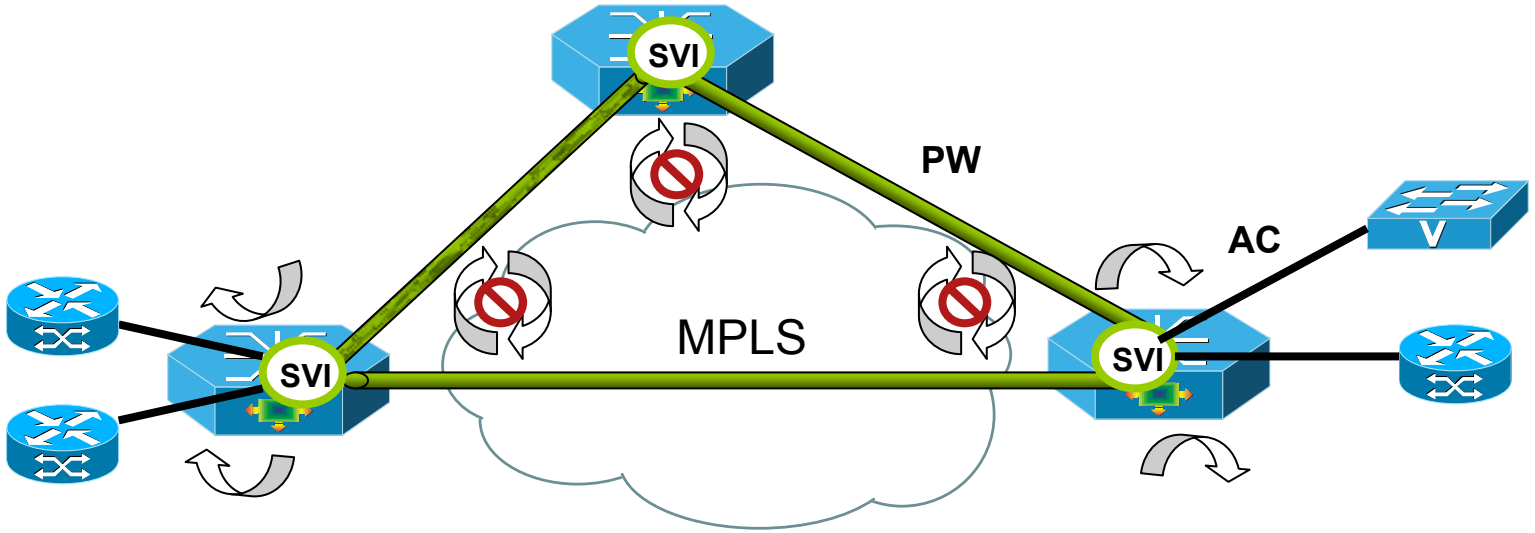
- Broadcast, Multicast, and unknown Unicast are learned via the received label associations
- Two LSPs associated with an VC (Tx & Rx)
- If inbound or outbound LSP is down, then the entire circuit is considered down
- MAC address will age out as regular L2 switch

MAC Address Withdrawal



- Primary link failure triggers notification message
- PE removes any locally learned MAC addresses and sends LDP address withdrawal (RFC3036) to remote PEs in VPLS
- New MAC TLV is used

VPLS Redundancy and Loop prevention



- Customer STP is transparent to the SP / customer BPDUs are dropped or forwarded transparently. VPLS only tunnel BPDU, not participate STP
- VPLS use “full mesh PW + split horizon” to achieve redundancy and for loop prevention
- Full mesh PWs among all the participating PEs
- Split horizon - Traffic received from the network (PW) will not be forwarded back to the network (PW). Only forwarded to ACs. Exception for H-VPLS with split-horizon turn off

Agenda

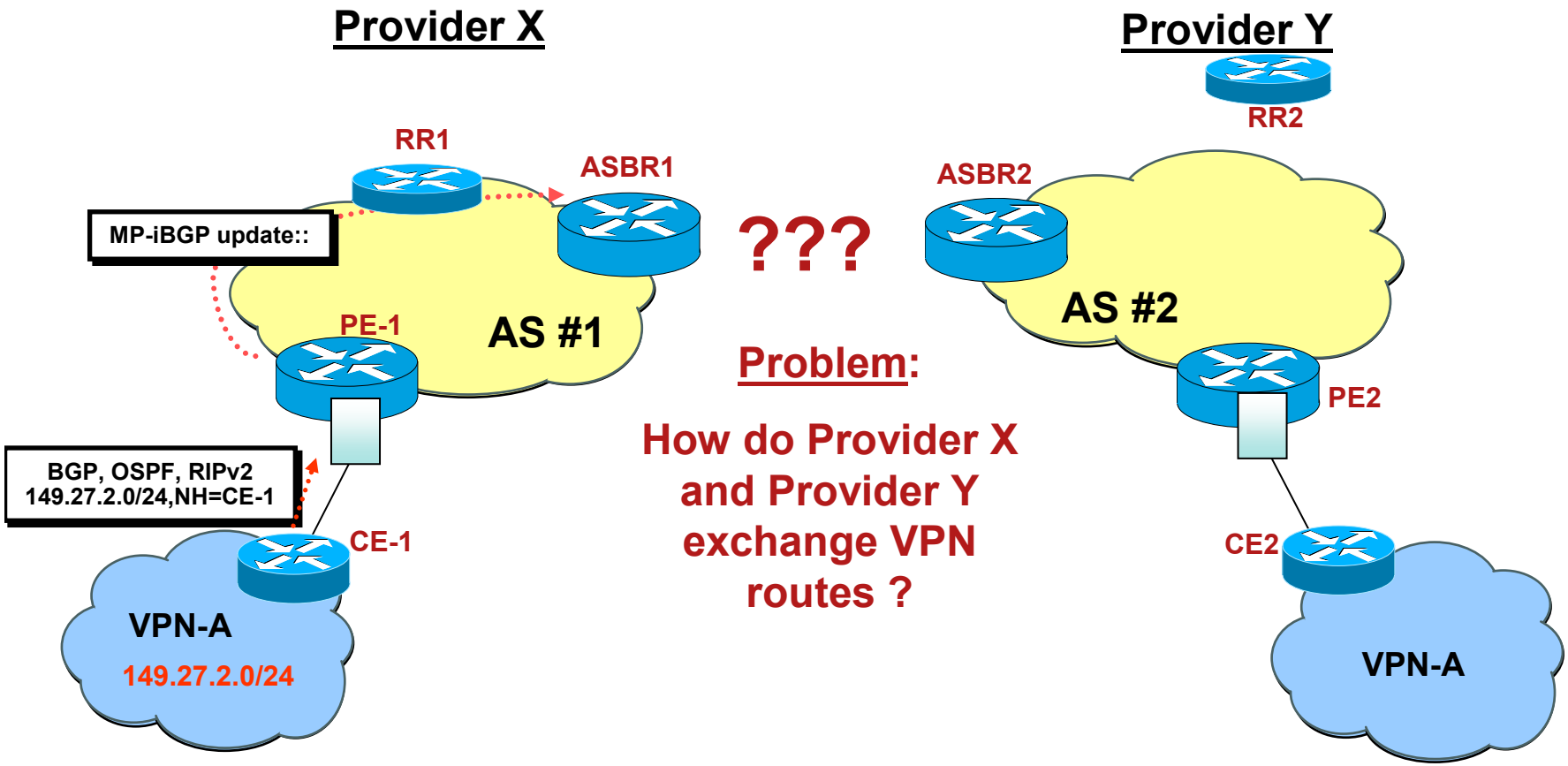
- MPLS overview
- VPNs overview
- L3 VPNs
- L2 VPNs
- **Inter-AS VPNs**

Why do IP/MPLS Providers Interconnect?

- MPLS VPN customers connected to different MPLS network due to:
  - –Address geographical diversity
  - –Customer sites receive VPN service from different providers
- Service Providers want to increase their coverage and competitiveness
  - –Domestic providers have limited international coverage
  - –Global & Regional service providers have limited in-country coverage
- Level of Trust and Information shared across Providers is important factor to consider

Inter Autonomous System (Inter-AS) VPN addresses the need for Inter-Provider Networking

MPLS VPN Inter-AS Overview

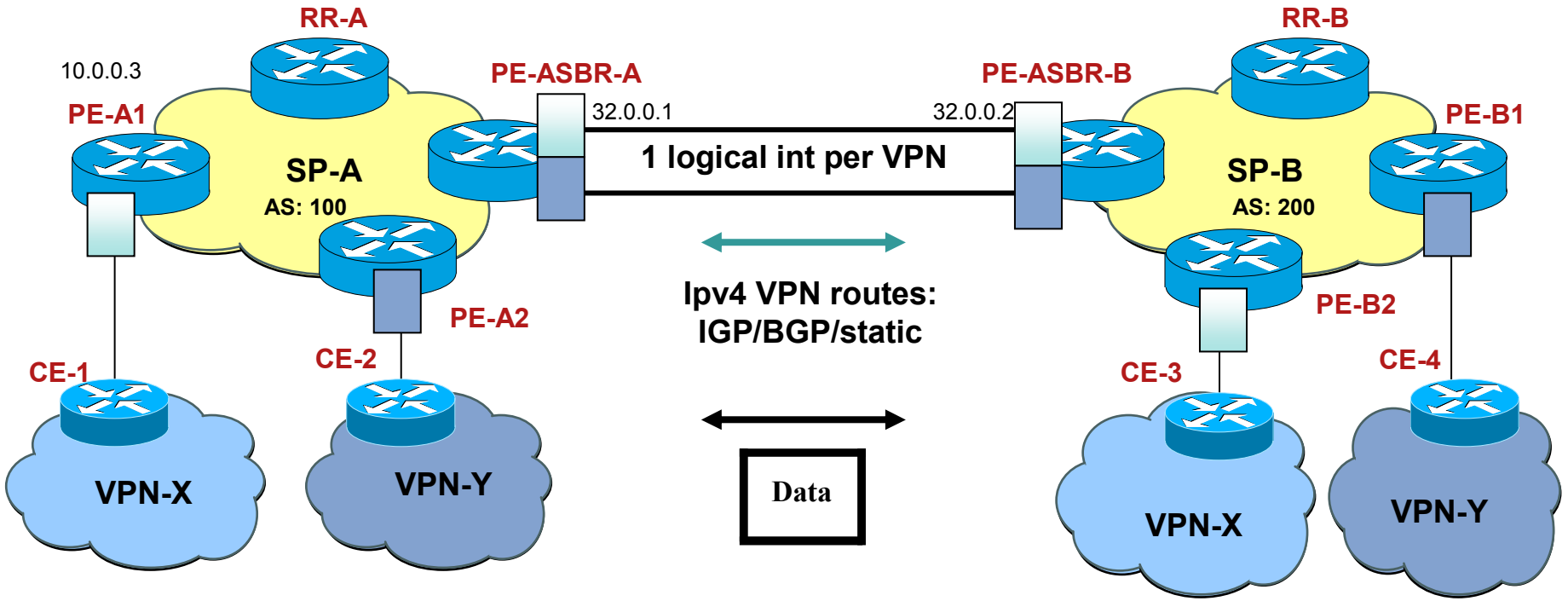


Options

- Reference RFC 4364, Section 10 - Multi-AS Backbones
- Three possible implementations described under sub-heading a), b) and c) in section 10
- Commonly referred as Option A, Option B and Option C
- Also referred as 10A, 10B, 10C

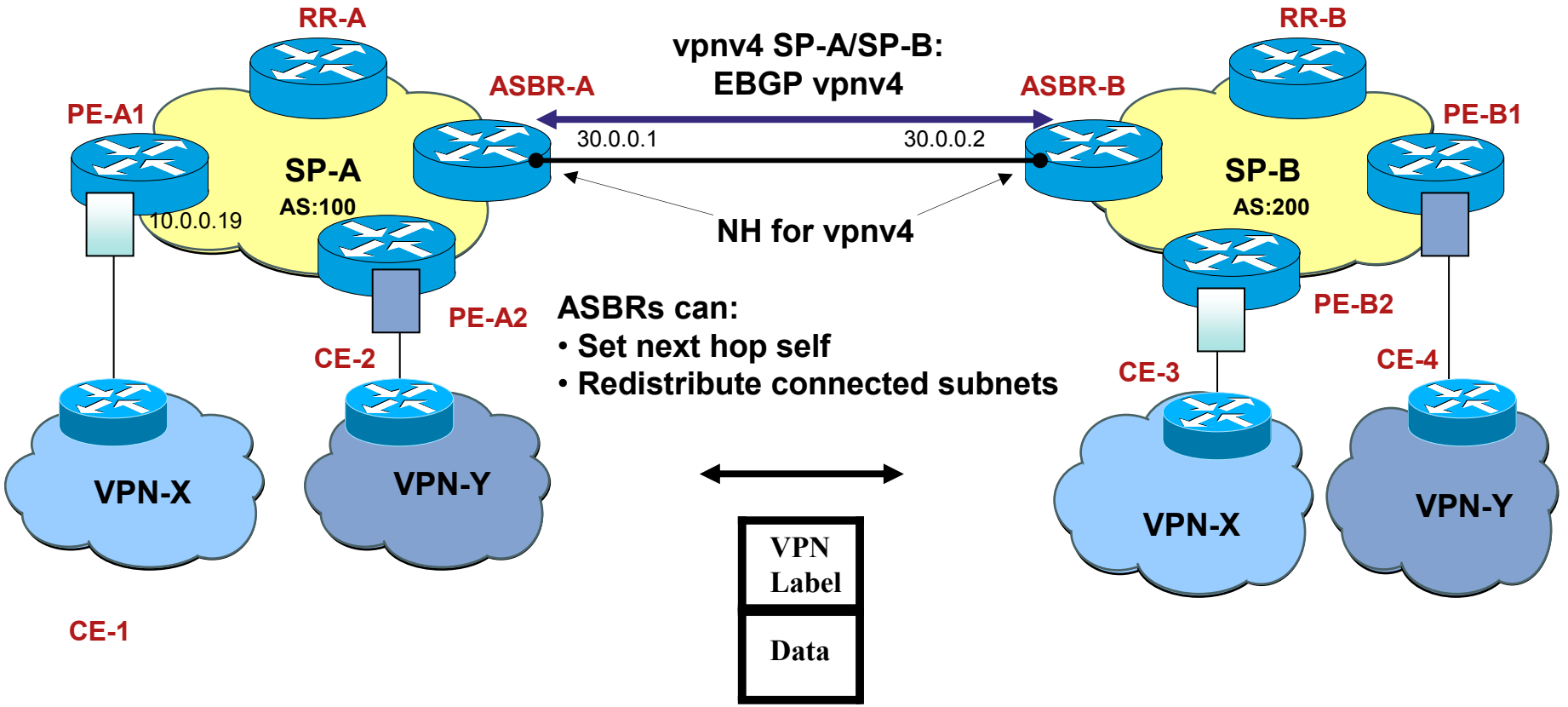
- Option AB (aka option D) is a recent enhancement and currently internal to Cisco

Inter-AS Option A – Back-to-Back VRF



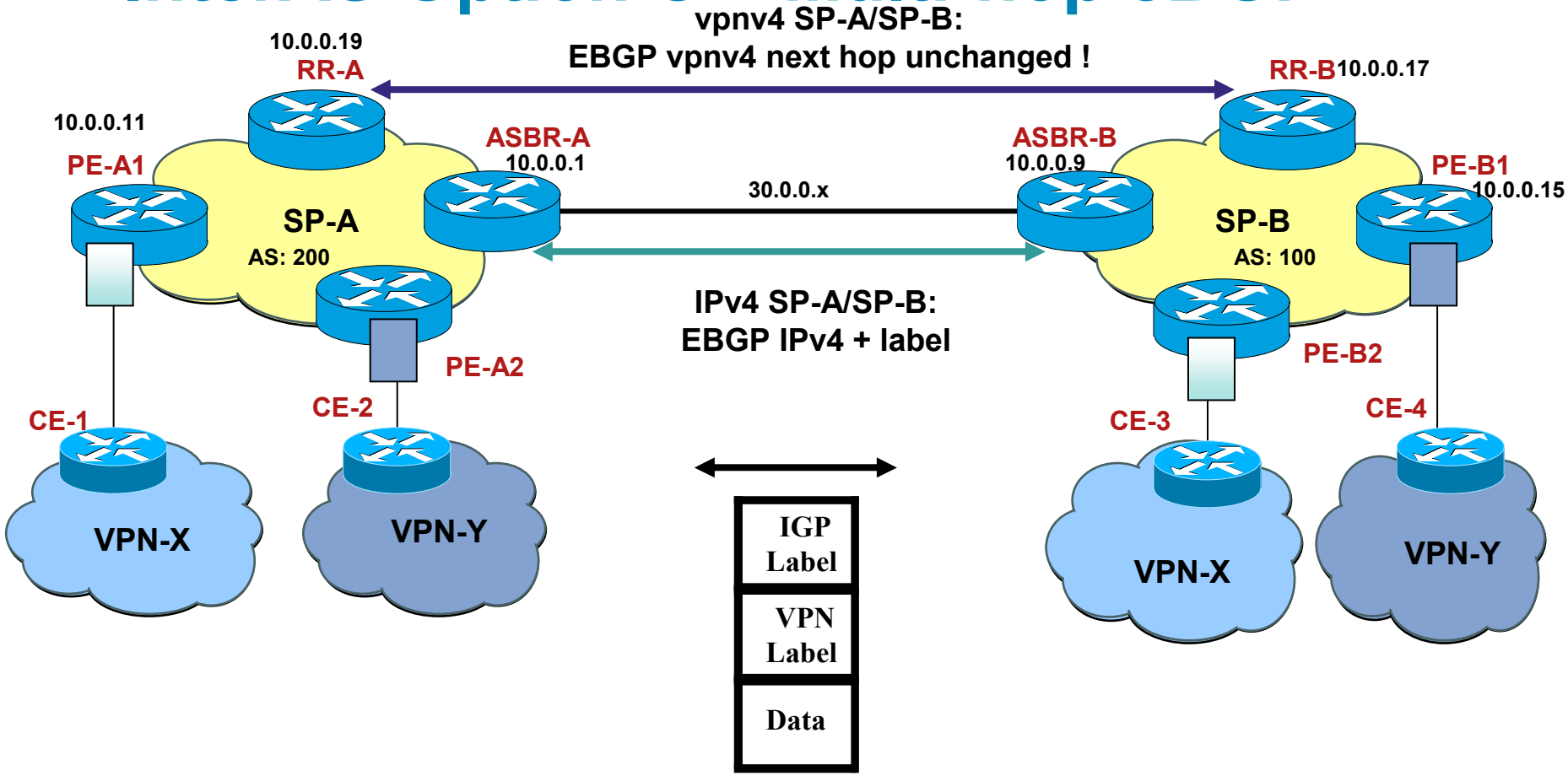
- Simple Concept (extension to Basic VPN – RFC 2547). Each ASBR treats peer ASBR as a CE.
- Inter-AS link is IP Only, hence security similar to RFC 2547
- Each advertised VRF across AS is enabled in separate interface or sub-interface in the ASBR. This limits scalability.
- ASBR contains all shared VRF routes (advertised by all PEs)

Inter-AS Option B – eBGP redistribution



- ASBR forward based on vpnv4 prefix label entries.
- ASBRs have MP-eBGP session with peer ASBR and local PE. LSP includes eBGP link.
- ASBR has VPNv4 prefixes (RD+IPv4) in MFI but not in RIB/CEF
- ASBR can either set ‘next-hop-self’ or redistribute connected subnets to its IGP.

InterAS Option C – Multi-hop eBGP



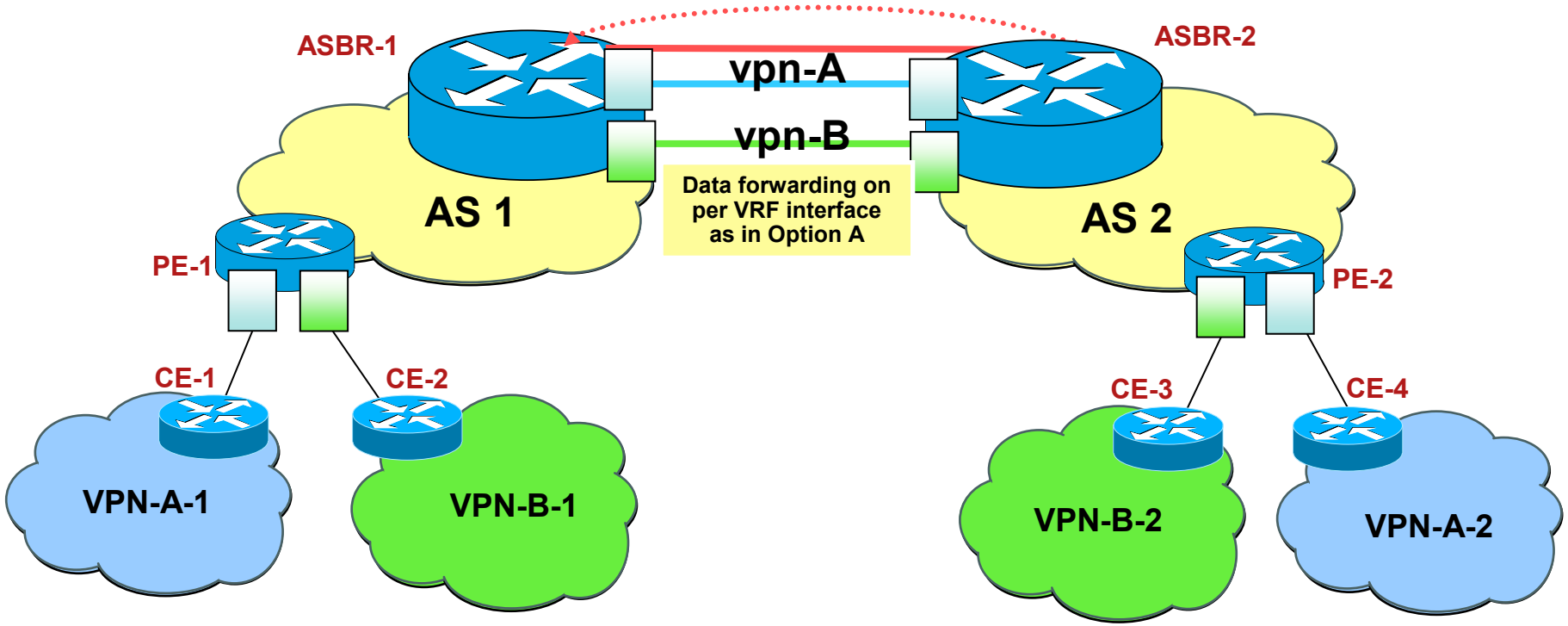
- Control Plane MP-BGP session setup between PEs across AS. RR usually used
- LSP formed between PE-A1 to PE-B1. eBGP used for labels exchange in Inter-AS link.
- ASBRs act as P routers for forwarding VPNv4 across AS (DMZ) boundary
- Use Route Maps to tightly control exchange of IP addresses across AS

Comparative model - Inter-AS Options

	Option A	Option B	Option C
Feature Availability	1st	2nd	3rd
Scalability	Low	Medium	High
ASBR hold VPNv4 routes	Yes	Yes	No
Technical Simplicity	High	Medium	Low
Security	High	Medium	Low
Protocol between ASBRs	Any PE-CE	MP-eBGP	eBGP
Visibility into other AS	None	ASBR	PE loopback, RR
VPN user must Trust	All providers	All providers	All providers
Service Provider must Trust	None	None	Peer Provider
Suited for Inter-Provider	Yes	Yes	No

Inter AS - Option AB

MP-EBGP between ASBRs on a control plane interface in global table, Option B



- Combines the benefits of Option A & Option B.
- Single MP-EBGP peer session between ASBRs as in Option B leading to better scaling and reduced configurations.
- Separate per VRF interface between ASBRs for data forwarding as in Option A which provides security and QoS benefits of IP forwarding on the IAS link.

Q and A