

---

# MPLS based Virtual Private Networks

## Sources:

V. Alwayn, *Advanced MPLS Design and Implementation*, Cisco Press  
B. Davie and Y. Rekhter, *MPLS Technology and Applications*, Morgan Kaufmann



# MPLS VPN Agenda

---

- Introduction to VPNs
- Where do Layer 2 and 3 VPNs fit?
- Layer 3 MPLS VPNs
  - VR and BGP Review
  - BGP/MPLS VPN Architecture Overview
    - ✓ VPN Routing and Forwarding (VRF) Tables
    - ✓ Overlapping VPNs
    - ✓ VPN Route Distribution
    - ✓ VPN Packet Forwarding

# MPLS VPN Agenda...

---

- Layer 2 MPLS VPN
  - ✓ Pseudo Wire Emulation Edge to Edge - PWE3
    - Martini Draft Encapsulation
    - Point to Point services
    - Encapsulation modes
- Provider Provisioned VPN - PPVPN

# VPNs

## *The market forces...*

---

- “VPNs are popular for enterprises and revenue-generating businesses for ISPs
- “If global telcos are to prosper in an increasingly difficult economic environment, they will need to build a convincing case for IP VPNs,.....”
  - Yankee Group

# VPNs

## *The market forces...*

---

### Service Providers

- Worldwide end-user VPN product and service expenditures will grow 275%, from \$12.8 billion to \$48.0 billion between 2001 and 2005
  - Source: Infonetics

### Network Equipment Manufacturers

- Service provider expenditures for metro network equipment will grow 175%, from \$6.3 billion to \$17.2 billion between 2000 and 2003 (and VPNs are a key requirement for this equipment)
  - Source: Infonetics

# mplsrc.com –

## *Examples of MPLS VPN deployments*

---

- Access:Seven
- Aleron
- AT&T
- Ardent Communications
- Aventel
- Bell Canada
- Beyond the Net
- British Telecom
- Cable & Wireless
- China Unicom
- Cistron
- Deutsche Telekom
- Energis UK
- Equant
- Global Crossing
- Infonet
- Iteroute .
- Japan Telecom
- Level 3
- Masergy Communications
- NetStream
- Nextra AS
- NTT
- OneSstar
- Song Networks
- Swisscom
- Telia Iberia
- Telecom Austria
- Telecom Italia
- Teleglobe
- Time Warner Telecom
- Tiscali
- UUNET/Worldcom
- Williams

Also go to: [http://www.cellstream.com/MPLS\\_List.htm](http://www.cellstream.com/MPLS_List.htm)

# VPNs – Main Concerns

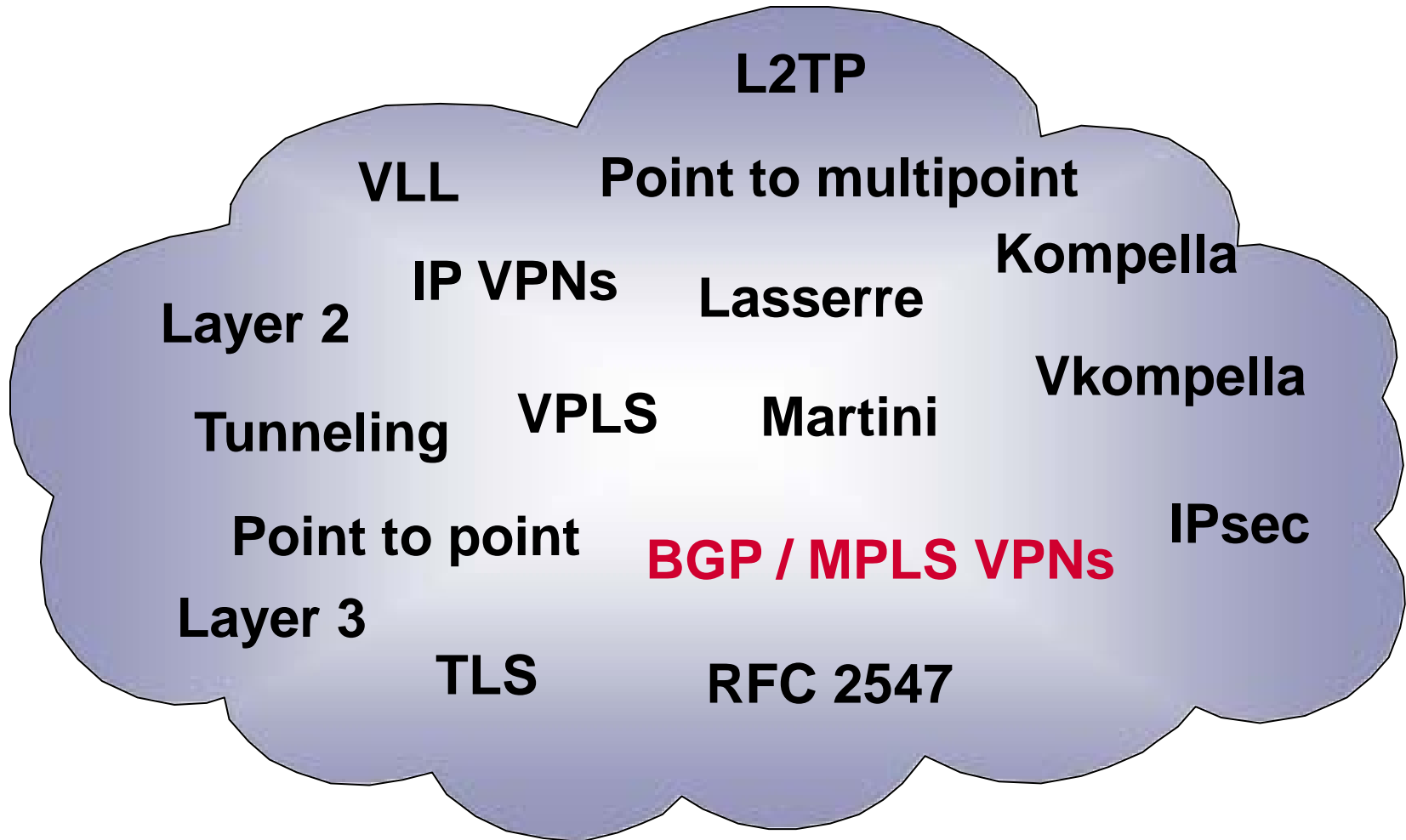
---

- **Private** networks: Security and privacy
  - How to transmit private data in a secure manner?
- **Virtual** private networks:  
Security, privacy, scalability and cost
  - How to transmit private data in a secure manner using public networks?
  - How to keep the cost down and how can it support a larger number of customers?
  - What technologies should be used?

# VPNs

## *What Are They ?*

---





# VPNs

## *What Are They ?*

VPN Type	Layer	Implementation
Leased Line	<b>1</b>	TDM/SDH/SONET
Frame Relay	<b>2</b>	DLCI
ATM	<b>2</b>	VC
GRE/UTI/L2TPv3	<b>3</b>	IP Tunnel
Ethernet	<b>2</b>	VLAN/Martini/H-VPLS
IP	<b>3</b>	MP-BGP/RFC2547/VR
IP	<b>3</b>	IPSec

# VPNs

## *How do they compare?*

	FR or ATM	IPSec	L3 MPLS	L2 MPLS
Point-to-multipoint	x	x	√	√
Multi-protocol	√	x	√	√
QoS and CoS	√	x	√	√
Low latency	√	x	√	√
Security	√	√	√	√
SLAs	√	x	√	√
Low cost	x	√	√	√

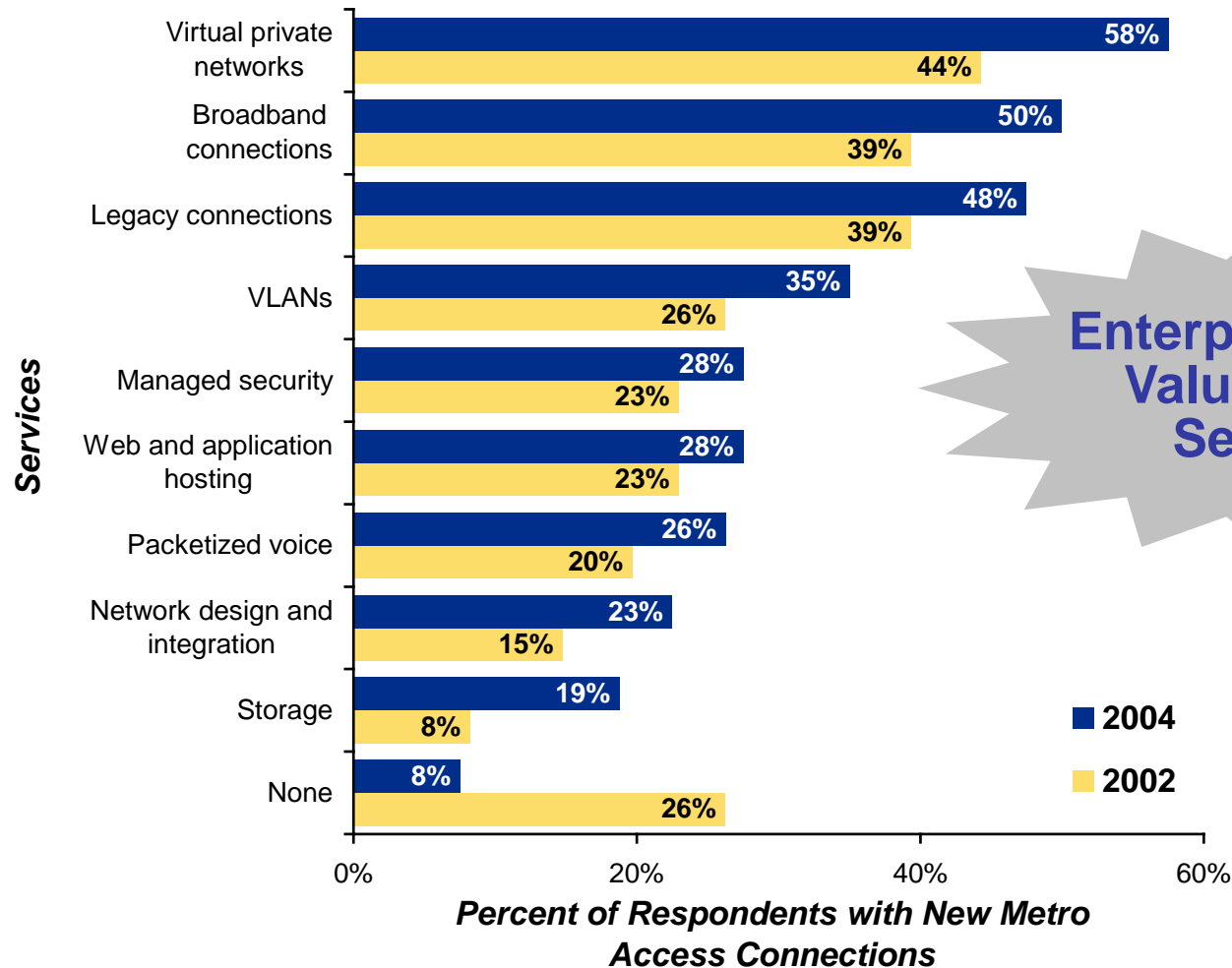
# VPNs

## *Applications*

LOCATION	APPLICATION	CONNECTION
Remote site connectivity	Telecommuter Single branch office	Point to point
Regional site connectivity	Distributed campuses Enterprise Intranets Customer Extranets Regional data centers Storage, backup, and recovery	Point to point Point to multipoint
National site connectivity	Regional access to Corp HQ Regional HQ to regional HQ Data center to data center	Point to point Point to multipoint

# VPNs

## What Enterprises Want

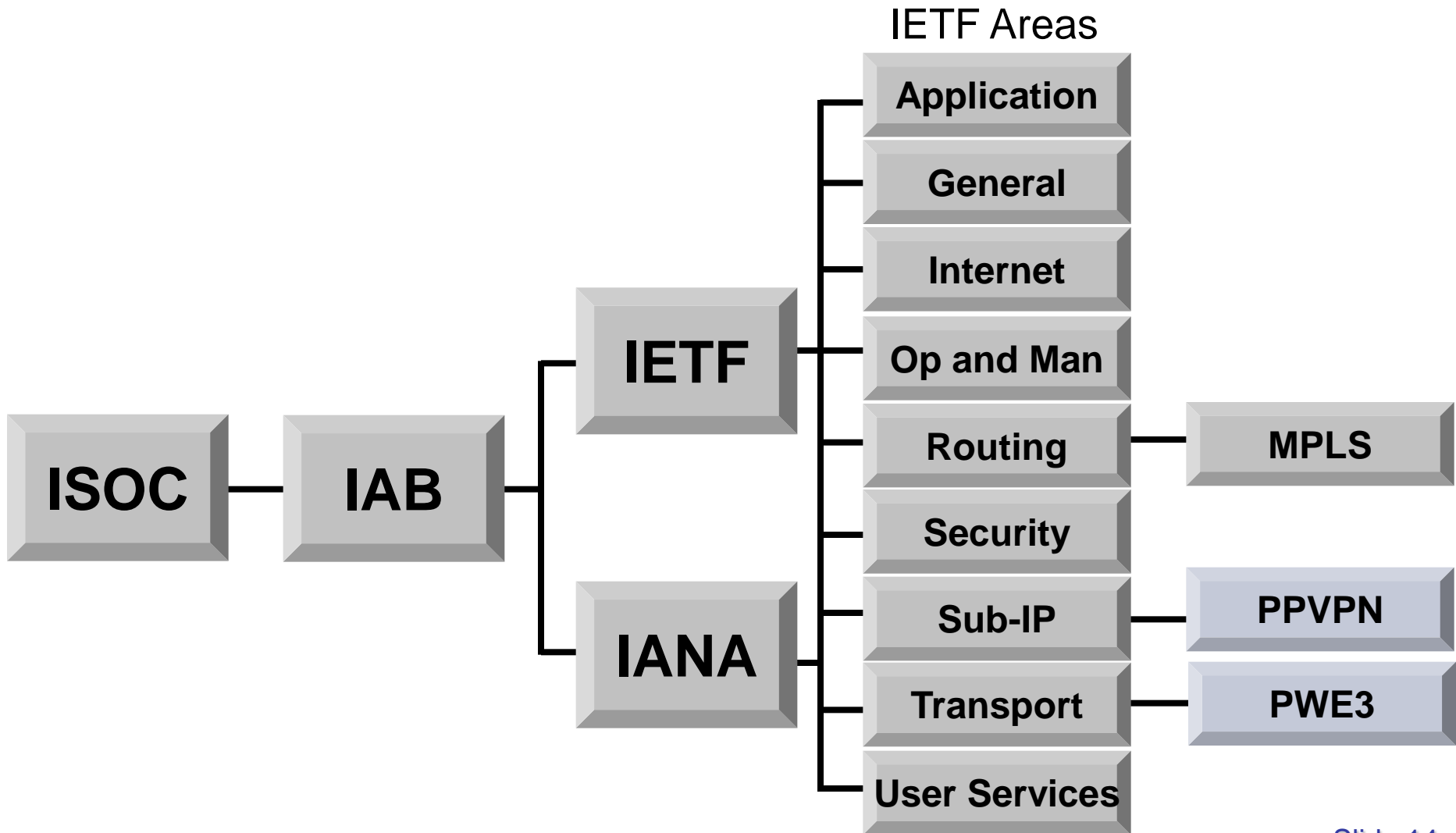


# What are Layer 2 and Layer 3 VPNs

---

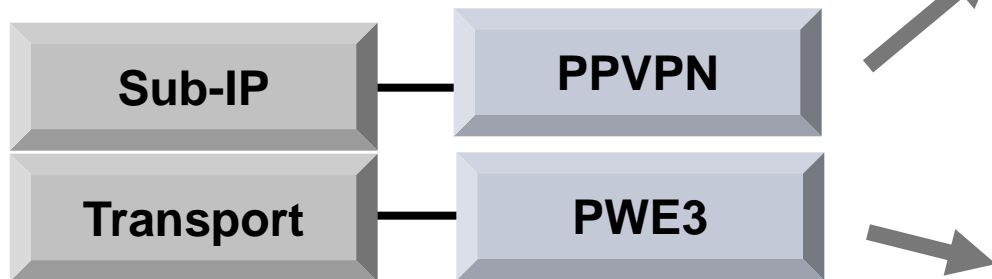
- VPNs based on a layer 2 (Data Link Layer) technology and managed at that layer are defined as layer 2 VPNs
  - ATM, Frame Relay, Ethernet, PPP, etc
- VPNs based on tunneling at layer 3 (Network or IP Layer) are Layer 3 VPNs
  - IPSec, VR, MPLS RFC 2547 bis IP VPNs

# Where Do VPNs fit ?



# Where Do VPNs fit ?

---



- Layer 3 VPNs
- Layer 2 VPLS
- Logical PE
  
- Pt-to-Pt circuits
- Martini
  - ATM
  - FR
  - Ethernet
  - PPP

VPLS: Virtual Private LAN Services

PPVPN: Provider Provisioned VPNs

PWE3: Pseudo Wire Emulation Edge to Edge

# What is a Virtual Private Network?

---

- VPN (Virtual Private Network) is simply a way of using a **public network for private communications**, among a set of users and/or sites
- Remote Access: Most common form of VPN is dial-up remote access to corporate database - for example, road warriors connecting from laptops
- Site-to-Site: Connecting two local networks (may be with authentication and encryption) - for example, a Service Provider connecting two sites of the same company over its shared network



# What are Layer 2, Layer 3 & IP VPNs?

---

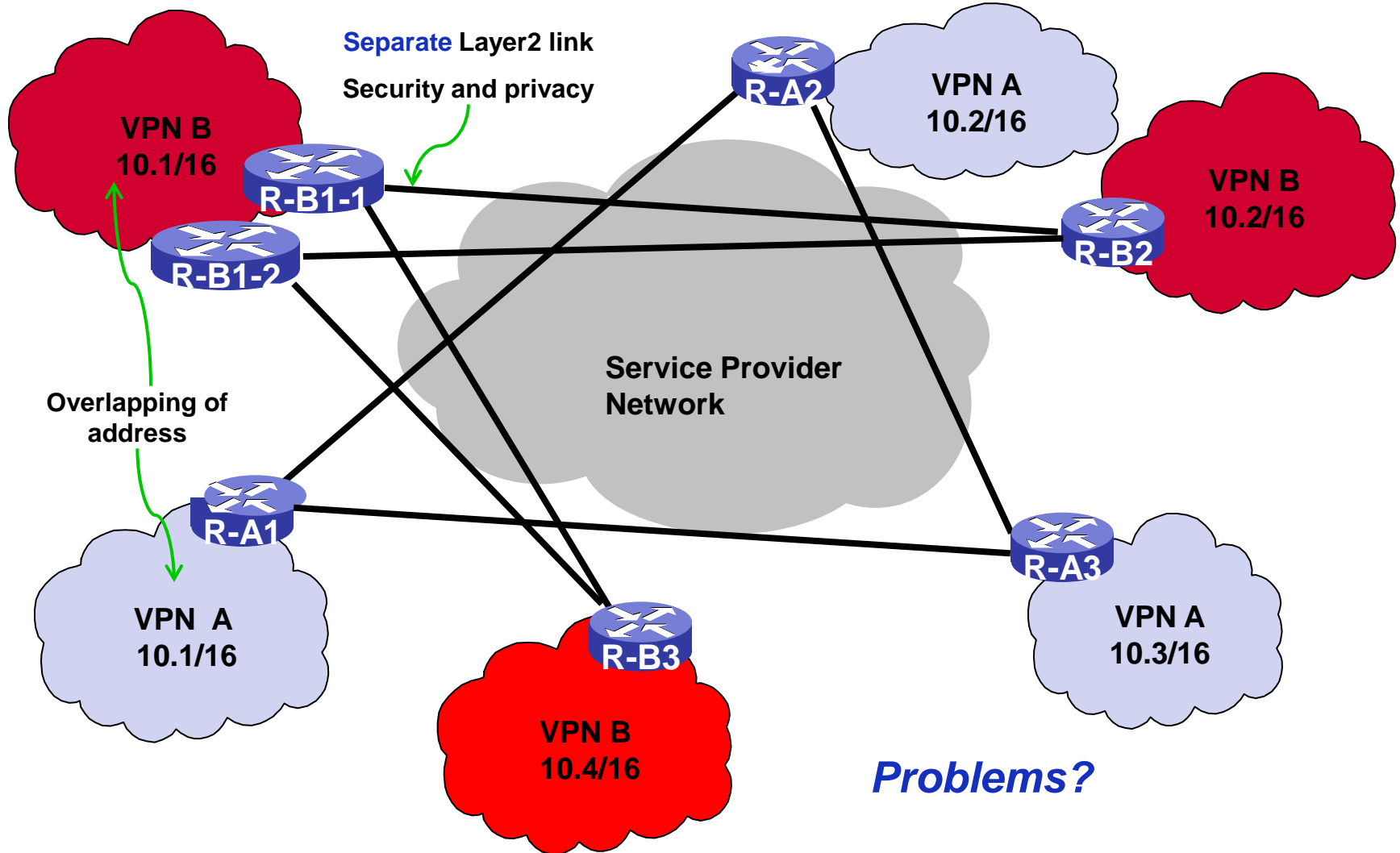
- VPNs based on a layer 2 (Data Link Layer) technology and managed at that layer are defined as layer 2 VPNs (MPLS, ATM, Frame Relay) - ref. OSI Layer model
- VPNs based on tunneling above layer 3 (Transport Layer) are Layer 3 VPNs, (L2TP, IPSec, BGP/MPLS)
- IP-VPNs are a type of layer 3 VPNs, which are managed purely as an IP network (L2TP, IPSec)

# Main VPN Models

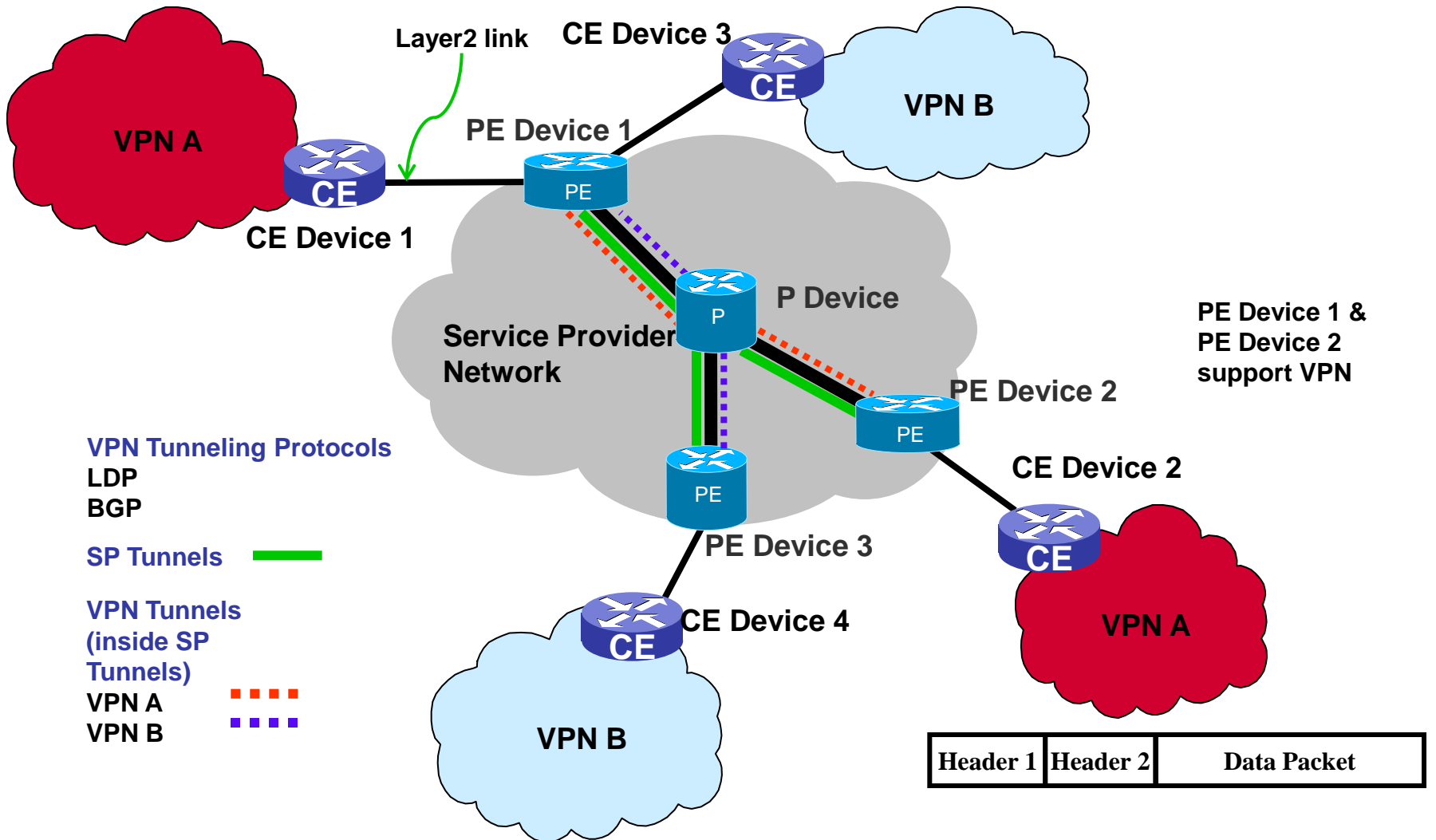
---

- Overlay model
  - Each site has a router that is connected via point-to-point links to routers in other sites.
- Peer model
  - Layer 3 VPNs built around key technologies:
    - ✓ User's concerns: security and privacy
      - Constrained distribution of routing information
      - Multiple forwarding tables
    - ✓ Service Provider's concerns: scalability
      - Simple configuration, including addition or removal of sites
      - Use of a new type of addresses, VPN-IP addresses
      - Tunneling: MPLS or even IP

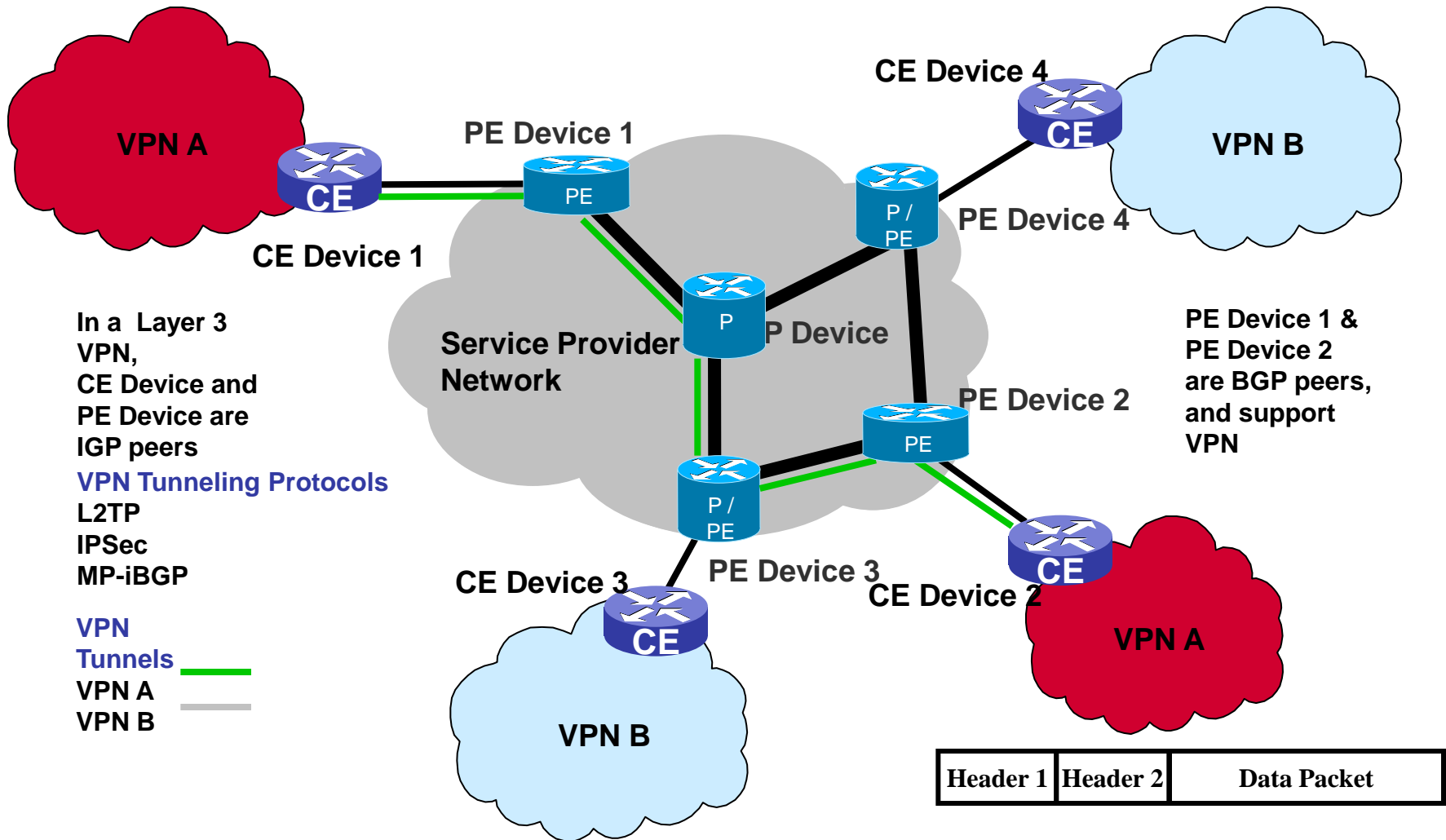
# Overlay Model



# Peer (PE & CE) Model - Layer 2 VPN



# Peer (PE& CE) Model - Layer 3 VPN



# Overlay Model vs. Peer Model

---

- Overlay Model

- Secure and isolate among customers
- Scalability and cost
  - ✓ Using virtual routers can help, but still ...

- Peer Model

- Simple and support large-scale VPN services
- **How to bring the benefits of the overlay model?**
- Built around key technologies:
  - ✓ **Constrained distribution** of routing info: what and how?
  - ✓ **Multiple separate routing/forwarding tables**
  - ✓ Use of a new type of addresses, **VPN-IP addresses**
  - ✓ MPLS (or IP) **tunneling**

# VPNs - The Basics

---

- Components:
  - A core network
  - VPN peers (typically at the edge of the core network)
- Steps for VPN set up:
  - Peer **discovery** mechanism
  - **Control** protocol exchange (VPN specific)
  - **Data** transport mechanism
    - ✓ necessary encapsulation
    - ✓ **encapsulation** and “de-encapsulation” capability

# VPN - The Basics...

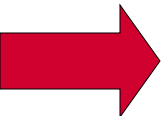
---

- As an example, for a Layer 3 BGP/MPLS VPN (over an MPLS network)
  - Peer **discovery** mechanism = iBGP, LDP
  - **Control** protocol exchange (VPN specific) = iBGP, LDP
  - **Data** transport mechanism
    - ✓ necessary encapsulation = Data+BGP label+MPLS label
    - ✓ encapsulation and “de-encapsulation” capability
  - Necessary protocol exchange for the core network = OSPF/ISIS & RSVP-TE/LDP



# MPLS VPN Agenda

---

- Introduction to VPNs
- Where do Layer 2 and 3 VPNs fit?
-  Layer 3 MPLS VPN
  - VR and BGP Review
  - Provider Provisioned VPN - PPVPN
  - RFC 2547bis Key Characteristics
  - BGP/MPLS VPN Architecture Overview
    - ✓ VPN Routing and Forwarding (VRF) Tables
    - ✓ Overlapping VPNs
    - ✓ VPN Route Distribution
    - ✓ VPN Packet Forwarding

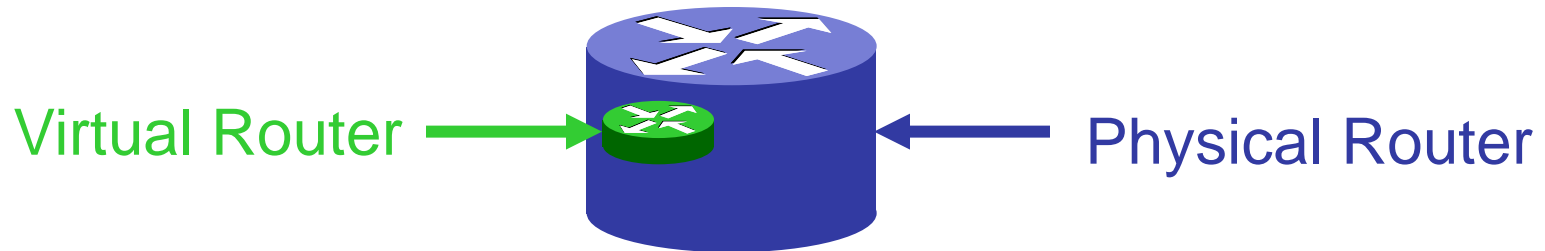
# Separate routing/forwarding - Virtual Router (VR)

---

- Customer sides: Protocol decided by VPN customer requirements (“IP cloning”)
- Whatever a given IP stack supports is available to the VPN customer
  - Basic IP
  - Domain services
  - Advanced services (e.g., multicast)

# What is a Virtual Router?

---



- A virtual router (VR) is an emulation of physical router.
- Any existing mechanism used in physical router applies to virtual router without any change.
  - configuration, management, monitoring, troubleshooting
  - transport of unicast and multicast IP traffic with differentiated or absolute QoS, configurable on a VPN-by-VPN basis

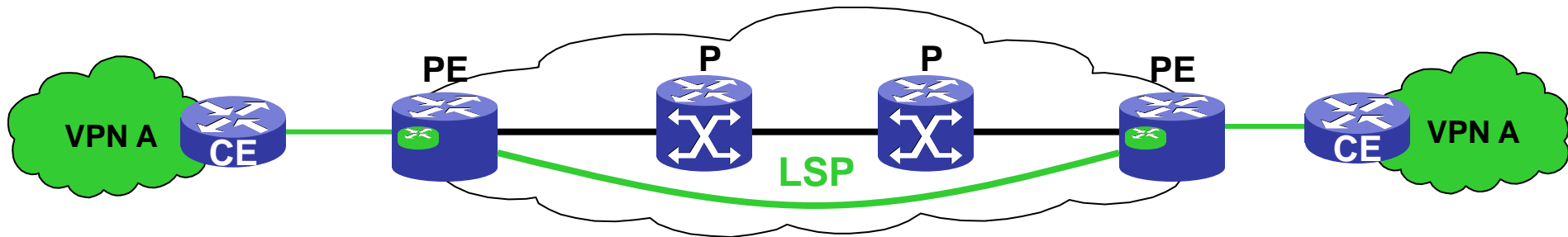
# What is a Virtual Router?

---



- VRs share CPU, bandwidth, and memory resources
- Each VR can run any combination of routing protocols (OSPF, RIP, BGP-4, etc.)
- VRs connect to a **specific routing domain** (logically discrete)
  - As a physical router can support multiple VRs, a physical router supports multiple (logically discrete) routing domains
- Each VR maintains **separate routing and forwarding tables**. No unintended leak between routing domains

# Data Forwarding



- Data Forwarding between PEs, 3 options:
  - An LSP with best-effort characteristics that all VPNs can use
  - An LSP dedicated to a VPN and traffic engineered by the VPN customer
  - A private LSP with differentiated characteristics

# What is BGP?

---

- BGP is an **exterior** gateway protocol that allows IP routers to exchange network reachability information.
  - BGP became an internet standard in 1989 (RFC 1105) and the current version, BGP-4 was published in 1994 (RFC 1771).
- BGP is continuing to evolve through the Internet standards process.

# IGP vs. EGP

---

- **Interior Gateway Protocol**

- RIP, OSPF, IS-IS
- Dynamic, some more than others
  - ✓ Constantly sending update messages
- Define the routing needed to pass data within a network

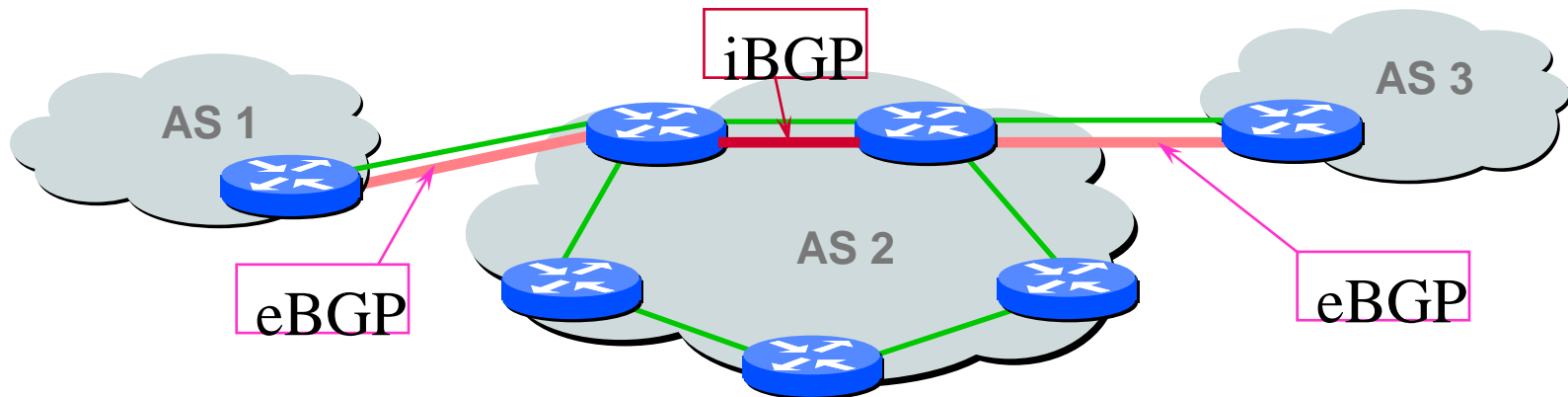
- **Exterior Gateway Protocol**

- BGP
- Less Dynamic than IGPs
  - ✓ Once BGP is established, only changes are populated.
- Defines the routing needed to pass data between networks

# Internal Border Gateway Protocol

**iBGP** - BGP between routers in the same AS:

- Forward BGP policy across an AS
- BGP neighbors even if they are not directly connected

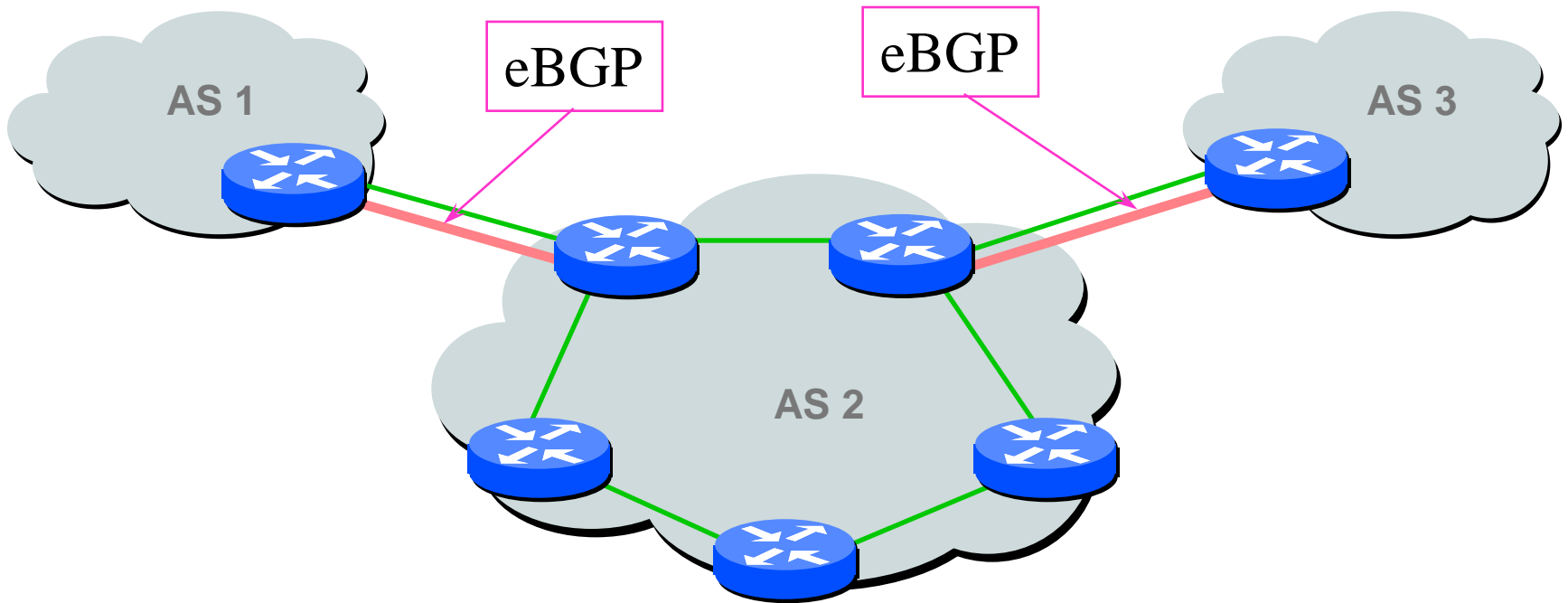


Provides a **consistent view** within the AS of the routes exterior to the AS.



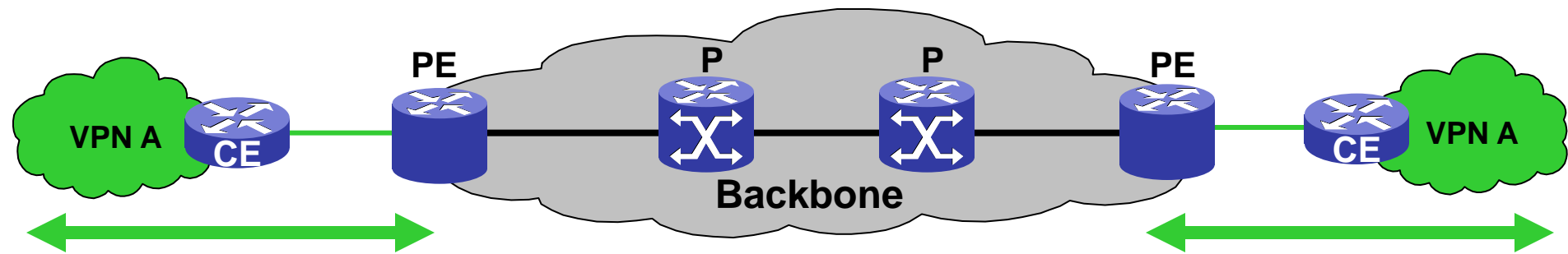
# External Border Gateway Protocol

**eBGP** - BGP between routers in two different AS's.



# BGP/MPLS VPNs

## Key Characteristics



- Requirements:

- Support for overlapping, **private IP address space**
- Different customers run **different IGPs** (i.e. RIP, OSPF, IS-IS)

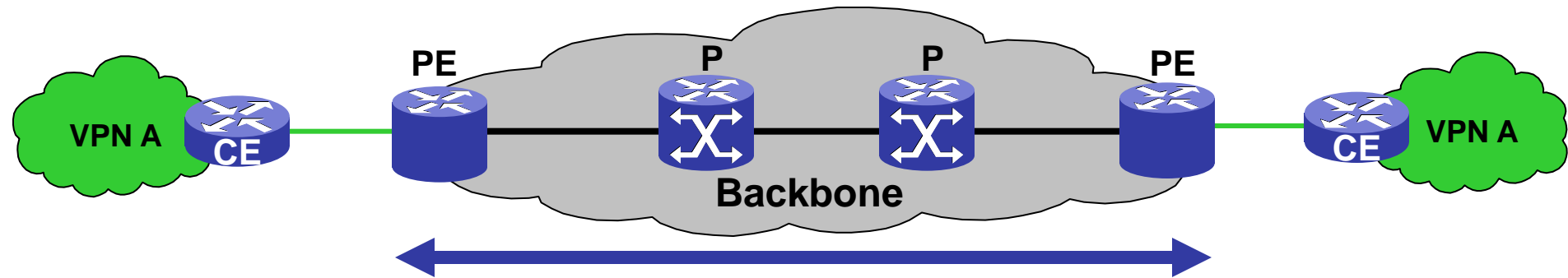
- Solution:

- VPN network layer is terminated at the edge (PE)
  - ✓ PE routers use plain IP with CE routers

# BGP/MPLS VPNs

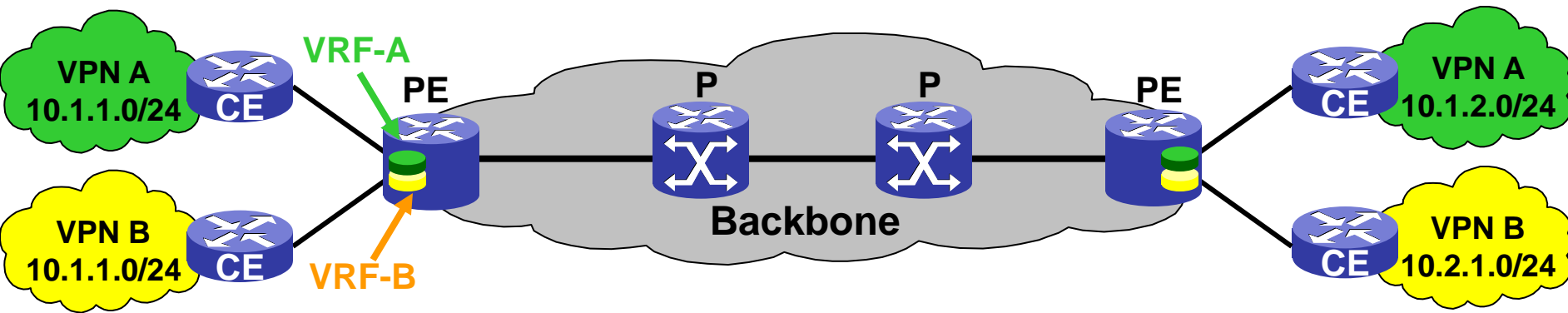
## *Key Characteristics*

---



- P routers (LSRs) are in the core of the MPLS cloud
- P and PE (LERs) routers run an IGP and a label distribution protocol
  - Labelled VPN packets are transported over MPLS core
- PE routers are MP-iBGP fully meshed
  - for dissemination of **VPN membership and reachability information** between PEs

# VPN Routing and Forwarding (VRF) Tables

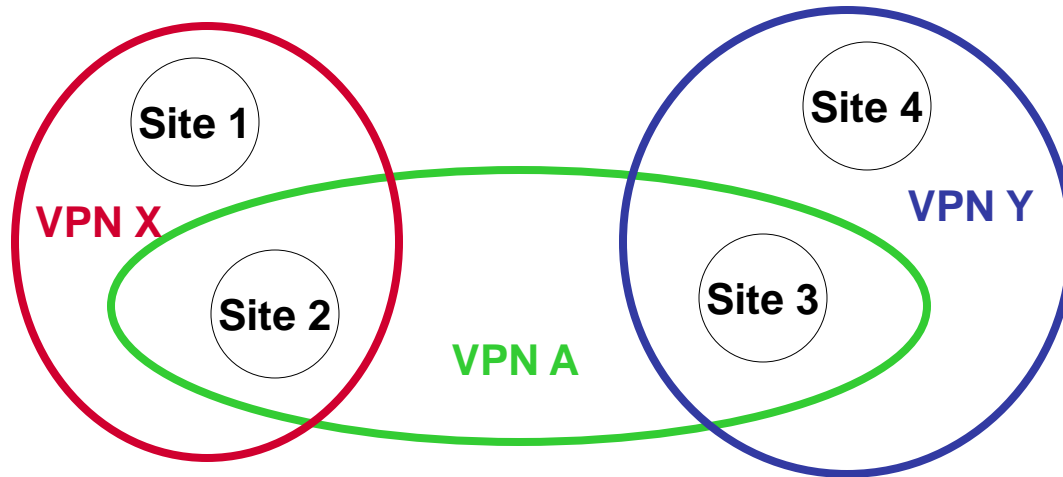


- Each VPN needs a **separate VPN routing and forwarding instance (VRF)** in each PE router to
  - Provides **VPN isolation**
  - Allows overlapping, **private IP address** space by different organizations

# VPN Routing and Forwarding (VRF)

## Overlapping VPNs

---



**Examples:**

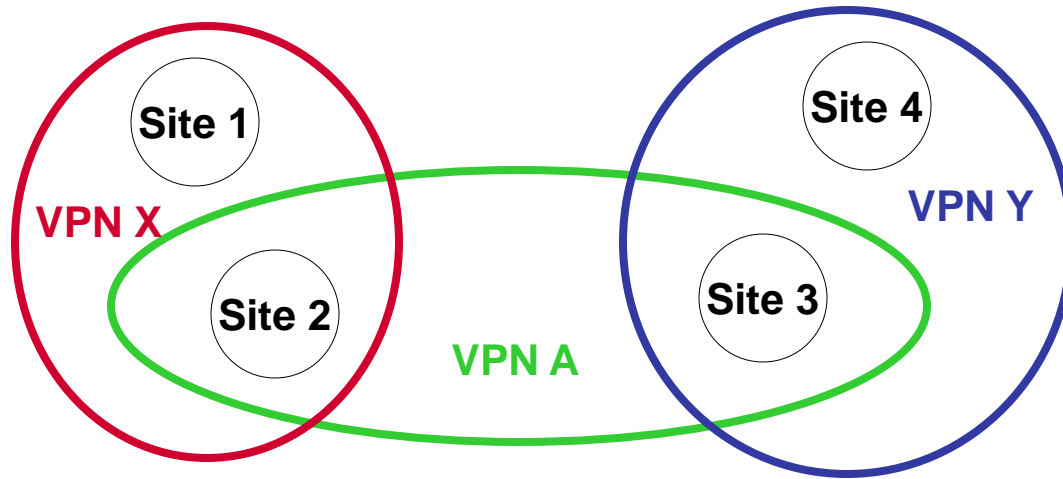
- Extranet
- VoIP Gateway

- A VPN is a collection of sites sharing a common routing information (routing table)
- A VPN can be viewed as a **community** of interest (or Closed User Group)

# VPN Routing and Forwarding (VRF)

## Overlapping VPNs

---



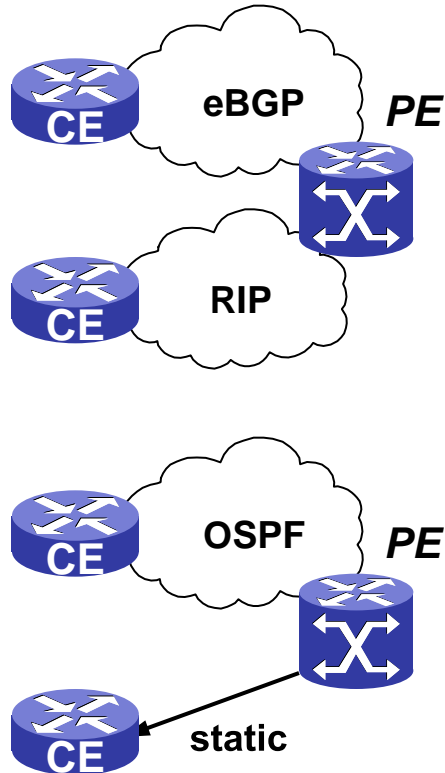
**Examples:**

- Extranet
- VoIP Gateway

- A site can be part of different VPNs
- A site belonging to different VPNs *may* or *may not* be used as a transit point between VPNs
- If two or more VPNs have a common site, address space must be unique among these VPNs

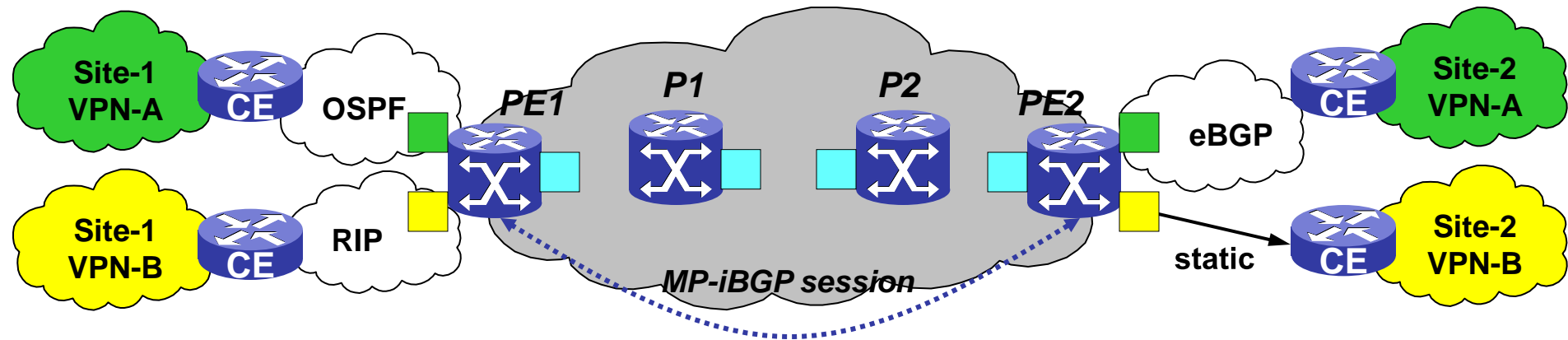
# VPN Routing and Forwarding (VRF)

## PE to CE Router Connectivity



- *What protocols can be used between CE and PE routers to populate VRFs with customer routes?*
  - BGP-4
  - RIPv2
  - OSPF
  - static routing
- **Note:**
  - Customer routes need to be advertised between PE routers
  - Customer routes are not leaked into backbone IGP

# VPNs and Route Distribution

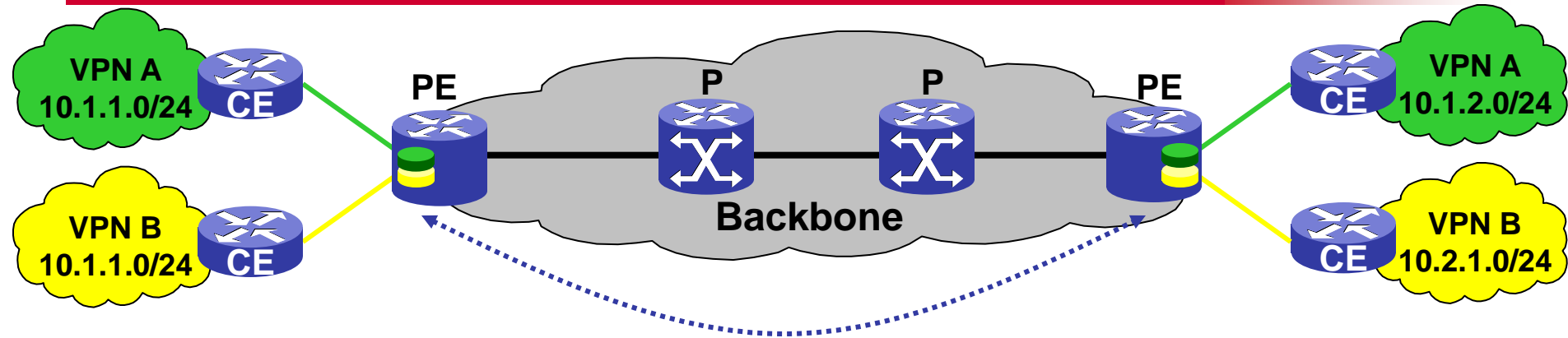


- Multiple VRFs are used on PE routers
- The PE learns customer routes from attached CEs
- Customer routes are distributed to other PEs with **MP-BGP**
  - There are many PEs, which one to distribute customer-specific or VPN-specific information?
  - **BGP's community attribute** enables route filtering



# VPN Route Distribution

## Route Targets



- Route Target attributes
  - BGP/MPLS VPN model [RFC2547bis]
- Encoded as community Route Targets [BGP-EXTCOMM].
  - **“Export”** Route Target: Every VPN route is tagged with one or more route targets when it is exported from a VRF (to be offered to other VRFs)
  - **“Import”** Route Target: A set of route targets can be associated with a VRF, and all routes tagged with at least one of those route targets will be inserted into the VRF

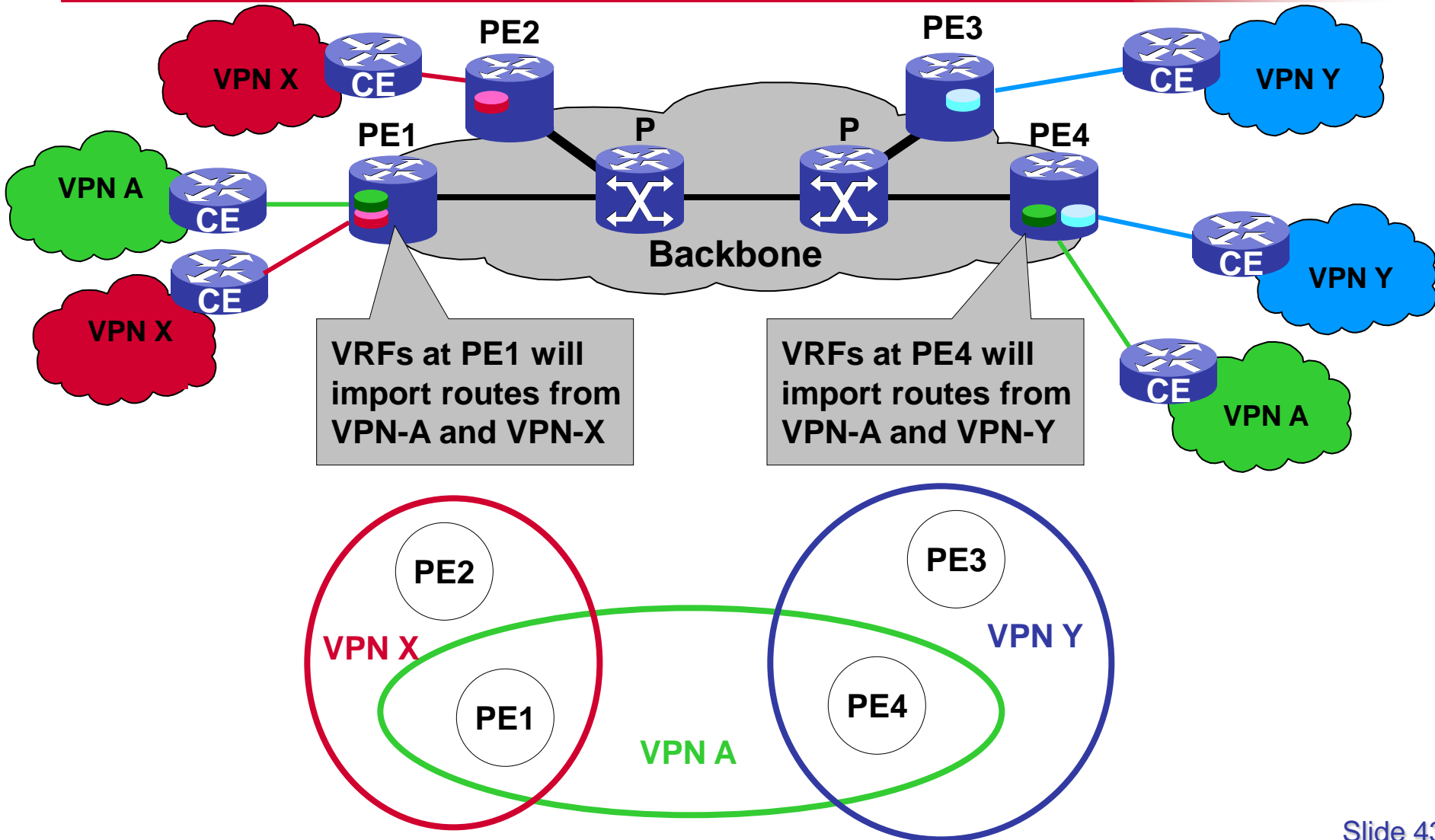
# Route Targets

---

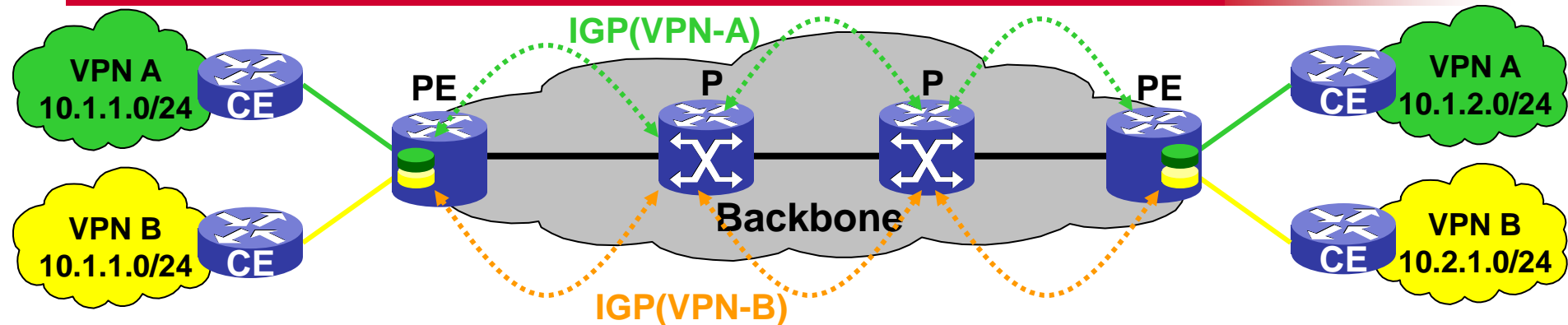
- BGP attributes are encoded as BGP extended Community Route Targets.
- Each VRF in a PE:
  - Associated with 1 or more RT attributes (“import”)
- Each site attached to a PE
  - Associated with 1 or more RT attributes (“export”)
- Each PE
  - Learns from its associate CEs (“import” RTs)
  - Distributes to other PE with the same RTs (“export”)

# VPN Route Distribution

## Route Targets



# VPN Route Distribution

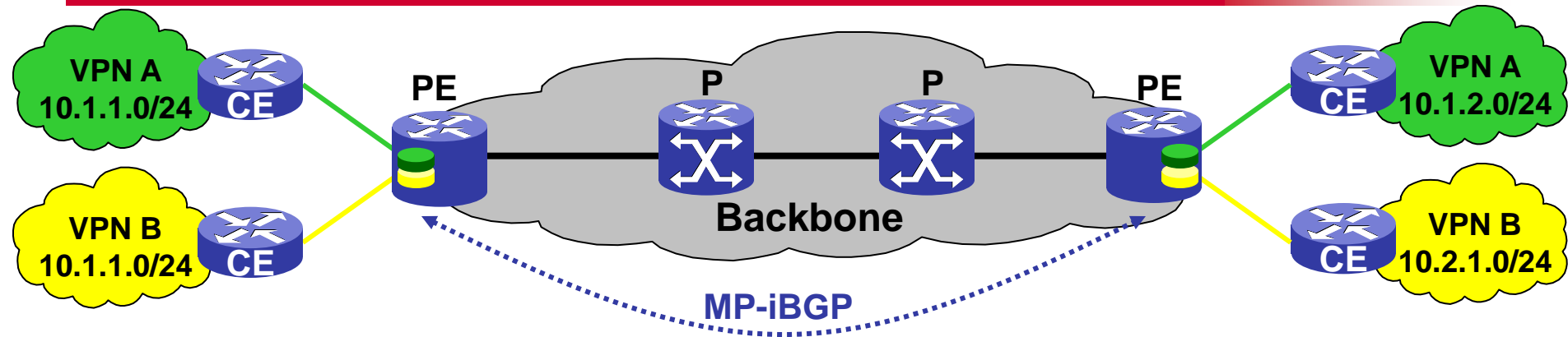


- *How will the PE routers exchange information about VPN customers and VPN routes between themselves?*

Option #1: PE routers run a different routing algorithm for each VPN

- Scalability problems in networks with a large number of VPNs
- Difficult to support overlapping VPNs

# VPN Route Distribution



- *How will the PE routers exchange information about VPN customers and VPN routes between themselves?*

Option #2: BGP/MPLS VPN - PE routers run a single routing protocol to exchange all VPN routes

- Problem: Non-unique IP addresses of VPN customers. BGP always propagates one route per destination not allowing address overlap.

# VPN Route Distribution

## *VPN-IPv4 Addresses*

---

- VPN-IPv4 Address

- VPN-IPv4 is a globally unique, 96bit routing prefix

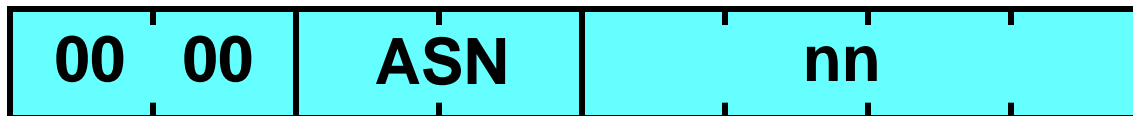
Route Distinguisher (RD)	IPv4 Address
<p>64 bits</p> <p>Makes the IPv4 address globally unique, RD is configured in the PE for each VRF, RD may or may not be related to a site or a VPN</p>	<p>32 bits</p> <p>IP subnets advertised by the CE routers to the PE routers</p>

# VPN Route Distribution

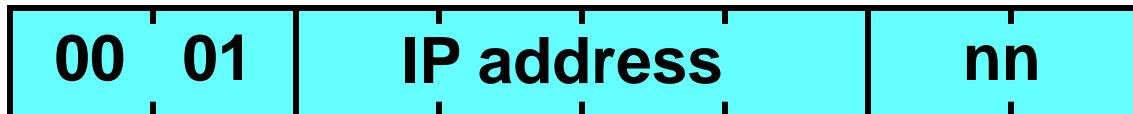
## VPN-IPv4 Addresses

---

- Route Distinguisher format



- ASN:nn
  - ✓ Autonomous System Number (ASN) assigned by Internet Assigned Number Authority (IANA) or RIRs, so that it is unique per service provider



- IP-address:nn
  - ✓ use only if the MPLS/VPN network uses a private AS number

# VPN Route Distribution

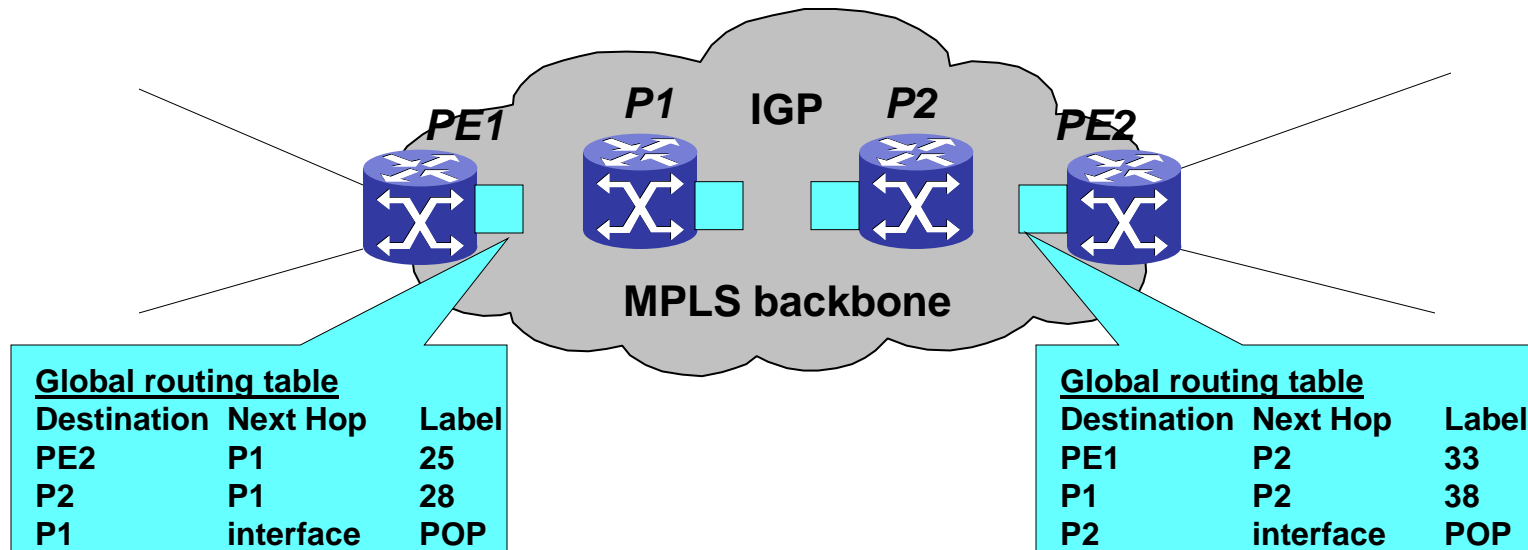
## *BGP with Multiprotocol Extensions*

---

- *How are 96-bit VPN-IPv4 routes exchanged between PE routers?*
- BGP with Multiprotocol Extensions (MP-BGP) was designed to carry such routing information between peer routers (PEs)
  - propagates VPN-IPv4 addresses
  - carries additional BGP route attributes (e.g. route target) called **extended communities**

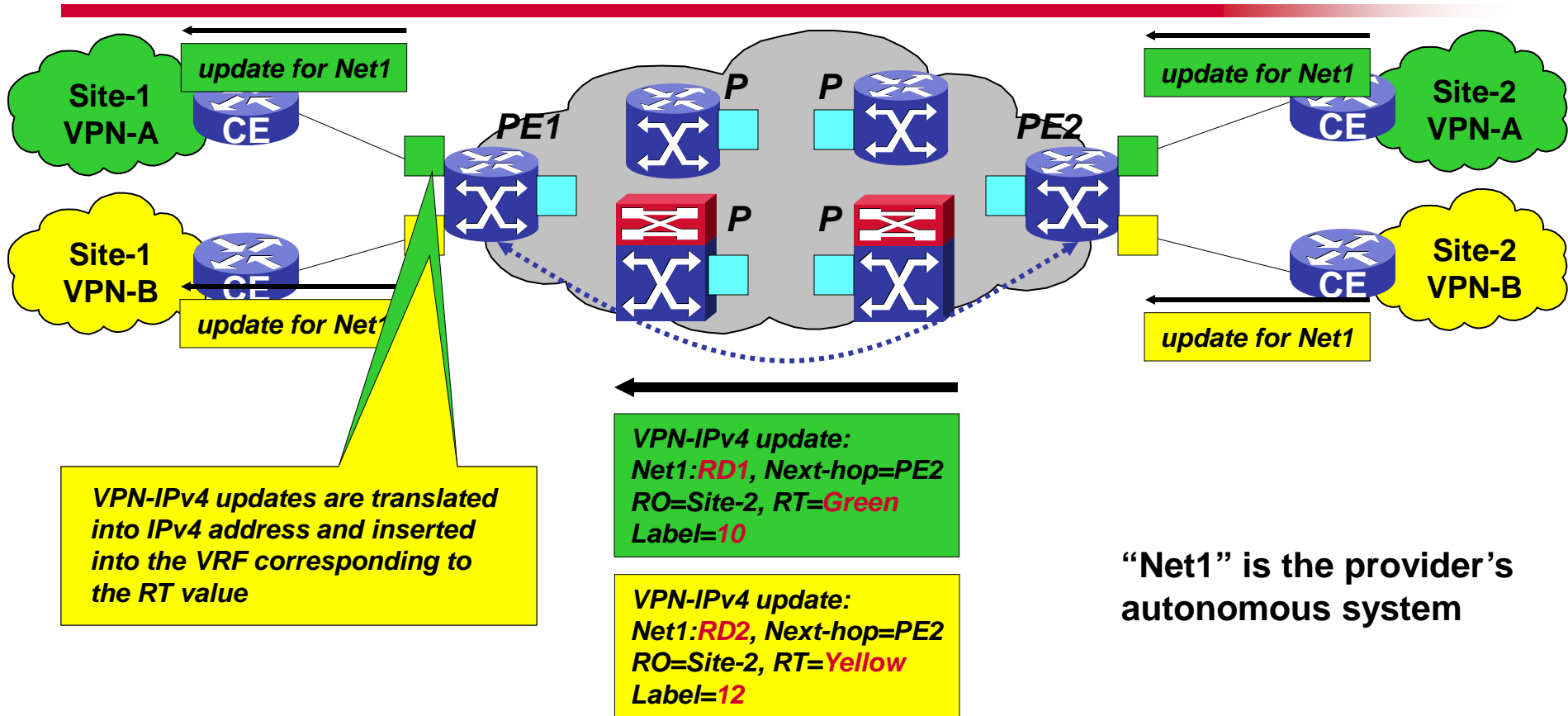


# IGP and Label Distribution in the Backbone



- All routers (P and PE) run an IGP and a label distribution protocol
- Each P and PE router has routes for the backbone nodes and a label is associated to each route
- MPLS forwarding is used within the backbone

# MP-BGP Route Distribution



# MP-BGP Route Distribution

## *Summary*

---

- VPN Routing and Forwarding (VRF) Table
  - Multiple routing tables (VRFs) are used on PEs
    - ✓ VPNs are **isolated**
- Customer addresses can **overlap**
  - Need for unique VPN route prefix
  - PE routers use MP-BGP to distribute VPN routes to each other
- For **security** and **scalability**, MP-BGP only propagates information about a VPN to other routers that have interfaces with the same route distinguisher value.

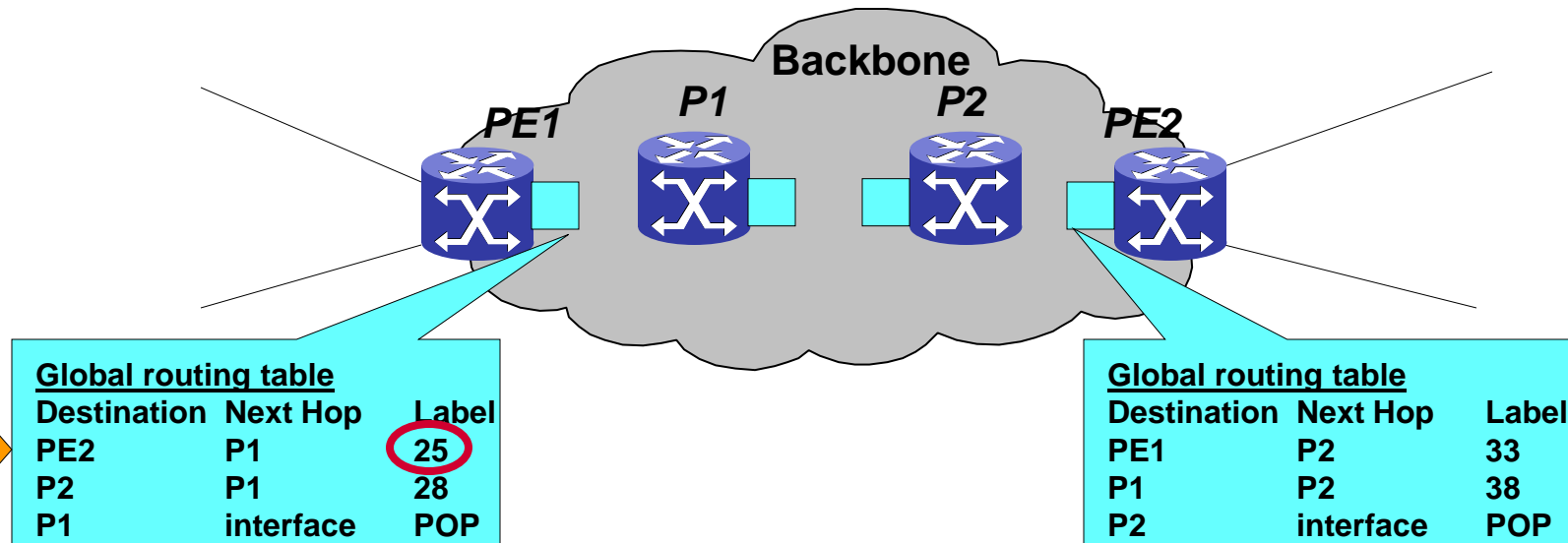
# VPN Packet Forwarding

---

- PE routers store different kinds of labels in their Label Forwarding Information Bases (LFIB)
  - Labels learned through the LDP / CR-LDP / RSVP-TE protocol and assigned to IGP routes
    - ✓ stored in global routing table
  - Labels learned through MP-BGP and assigned to VPN routes
    - ✓ stored in VRF

# VPN Packet Forwarding

## *IGP Label Allocation*



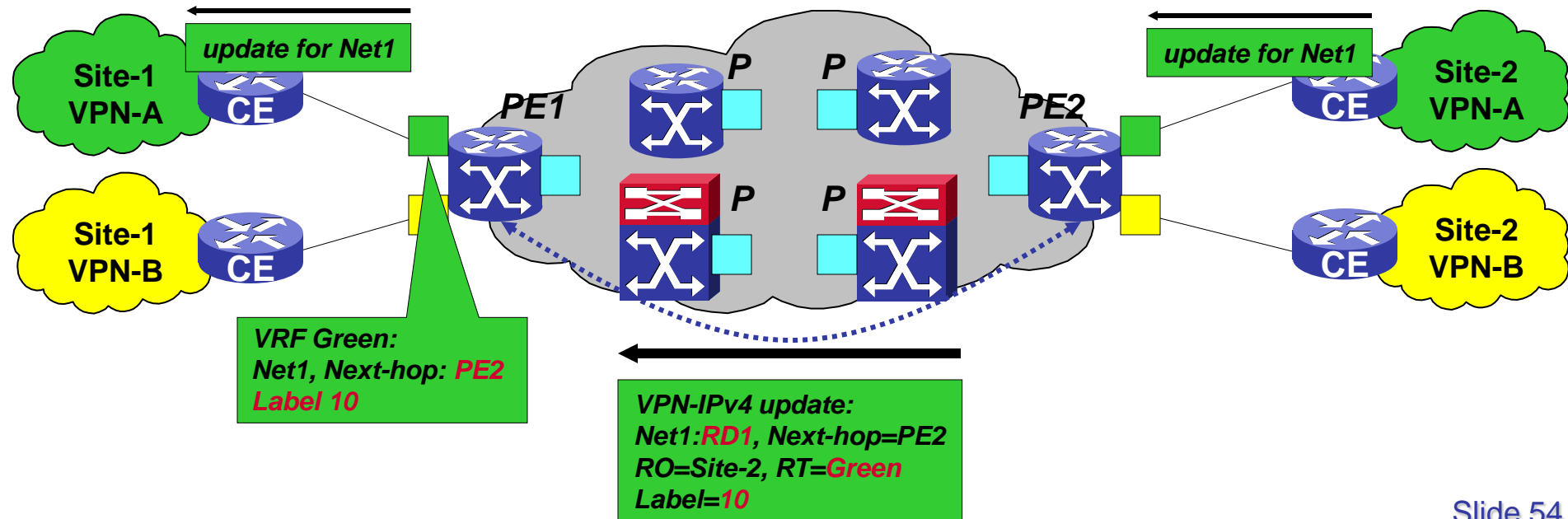
### PE-to-PE connectivity via LSPs

- All routers (P and PE) run an IGP and a label distribution protocol
- Each P and PE router has routes for the backbone nodes and a label is associated to each route
- MPLS forwarding is used within the backbone

# VPN Packet Forwarding

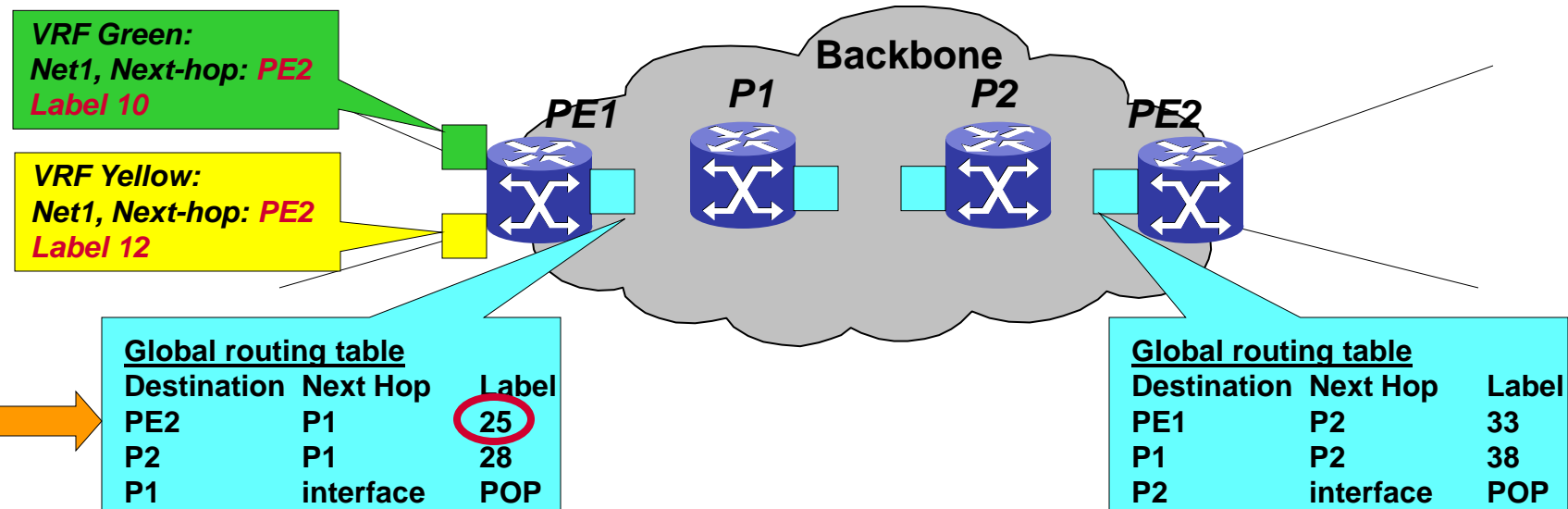
## VPN Label Allocation and Distribution

- Each PE router allocates a **unique label** for each route in each VPN routing and forwarding (VRF) instance
- These labels are propagated together with the corresponding routes through MP-BGP to all other PE routers
- The PE routers receiving the MP-BGP update install the received **route and the label** in their VRF tables



# VPN Packet Forwarding

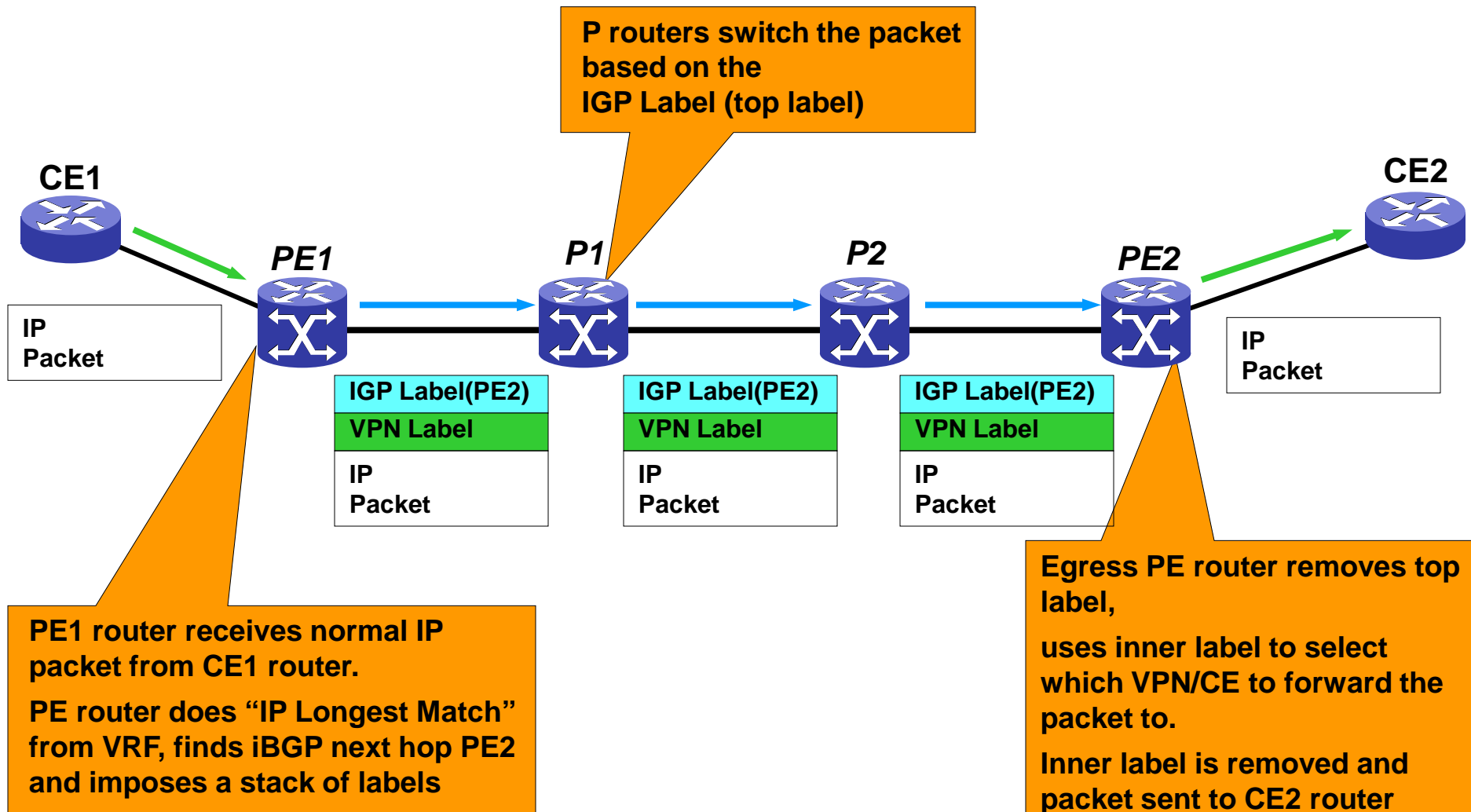
## Label Stacking



- Ingress PE router uses two-level label stack
  - **VPN label** (inner label) assigned by the egress PE router
  - **IGP label** (top label) identifying the PE router
- Label stack is attached in front of the VPN packet
- The MPLS packet is forwarded across the P network

# VPN Packet Forwarding

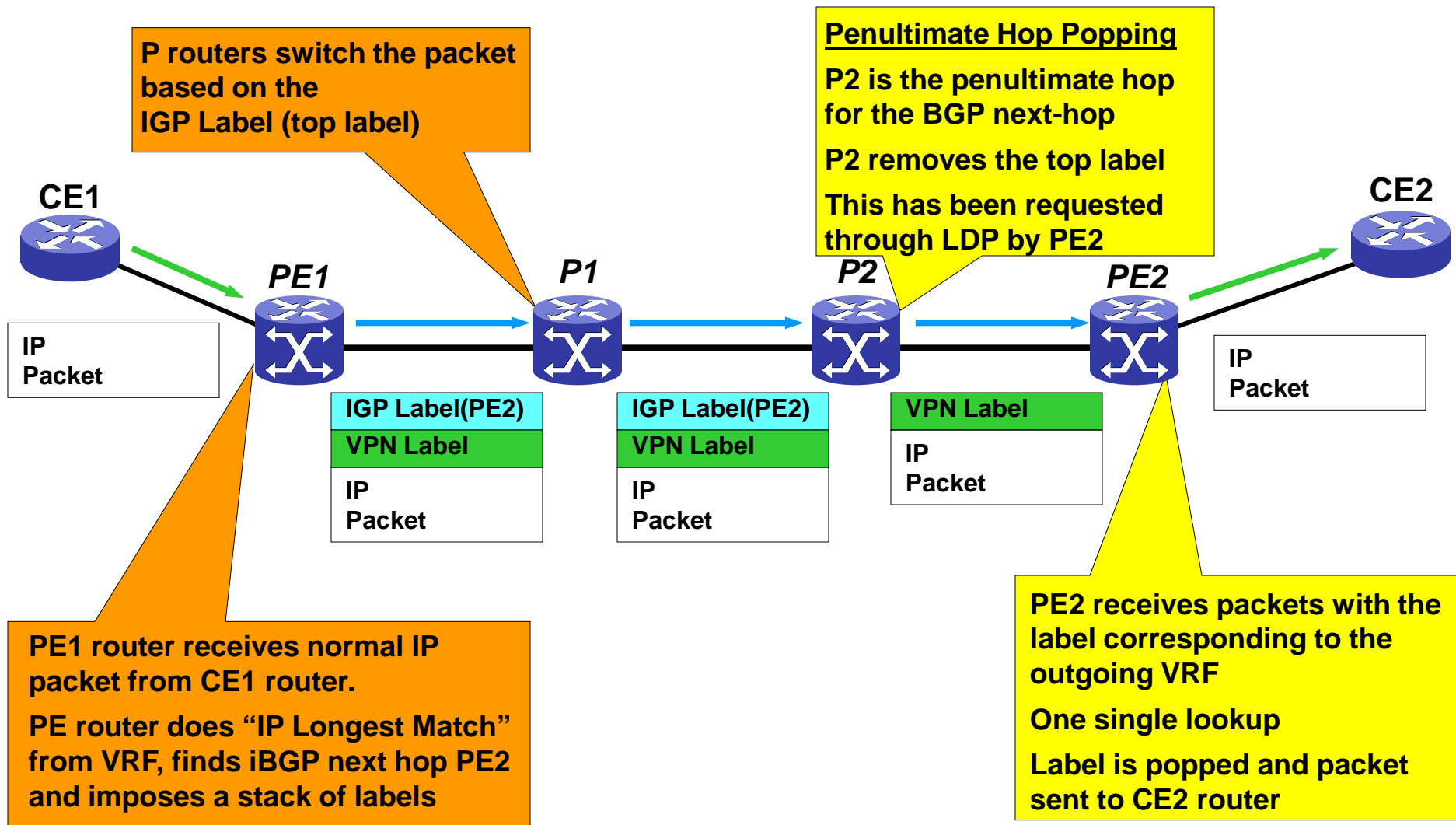
## Label Stacking





# VPN Packet Forwarding

## Penultimate Hop Popping



# Scalability

---

- BGP/MPLS: independent of the total # of sites within a VPN.
  - The amount of routing peering that a CE router has to maintain is constant.
  - The amount of configuration changes needed due to additions or deletions is constant.
  - Routing information handling: P routers don't maintain any VPN routing information.
  - PE routers have to maintain routing info, but they only have to maintain the info for the VPNs whose sites are directly connected to that PE router.
  - BGP Router Reflectors (RR) can be used to support large amount of routing information by partitioning RR among VPNs.

# Security

---

- Goal: packets from one VPN should not be sent to another VPN.
- How to achieve that?
  - How can a packet arrive at a CE?
- BGP/MPLS VPN Approach is comparable to that provided by FR and ATM-based VPNs.

# QoS Support

---

- Challenges : support QoS for VPN customers
  - Flexible for a wide range of VPN customers; and
  - Scalable for a large number of VPN customers.
- Two models:
  - Pipe
    - ✓ QoS guarantees for the traffic from one CE to another: Int-Serv
    - ✓ Example: guaranteed minimum bandwidth between two sites
    - ✓ Similar to FR or ATM-based solutions.
    - ✓ Customers need to know the complete traffic matrix.
  - Hose
    - ✓ Certain guarantees for the traffic that the customer's CE router sends to and receives from other CEs within the same VPN. No need to know the complete traffic matrix.
    - ✓ Ingress Committed Rate (ICR) and Egress Committed Rate (ECR).
    - ✓ Diff-Serv
  - P routers can still only maintain queuing state on an aggregate basis, rather than on a per-VPN basis