MPLS based Virtual Private Network Services

Half Day Tutorial

http://www.mplsforum.org ***http://www.frforum.com***

MPLS VPN Tutorial Agenda

- Introduction to MPLS and MPLS VPNs
  - Defining Layer 2 and 3 VPNs
- Layer 3 MPLS VPN
  - BGP Review
  - RFC 2547bis Key Characteristics
  - BGP/MPLS VPN Architecture Overview
    - ✓ VPN Routing and Forwarding (VRF) Tables
    - ✓ Overlapping VPNs
    - ✓ VPN Route Distribution
    - ✓ VPN Packet Forwarding
    - ✓ Scaling L3VPNs and Route Reflectors

MPLS VPN Tutorial Agenda

- Layer 2 VPNs
  - IETF PWE3 and L2VPN WG update
  - Encapsulation and Label Stacking
  - Virtual Private Wire Services – VPWS
    - Pt-to-pt Ethernet, Pt-to-pt ATM, Pt-to-pt Frame Relay
  - Virtual Private LAN Services – VPLS
- Introduction to Multi-Service Interworking
  - Carrier Challenges at the Edge
  - Interworking History and Definition
  - Network and Service Interworking (FRF.5 and FRF.8.1)
  - MPLS FR Alliance Multi-Service Interworking Work Actions
- Carrier Migration Examples

VPN Tutorial Contributors

- Thomas Bopp - Marconi Communications
- Paul Izzo - Consultant
- Sunil Kandakar - Alcatel
- Gary Leonard - Riverstone Networks

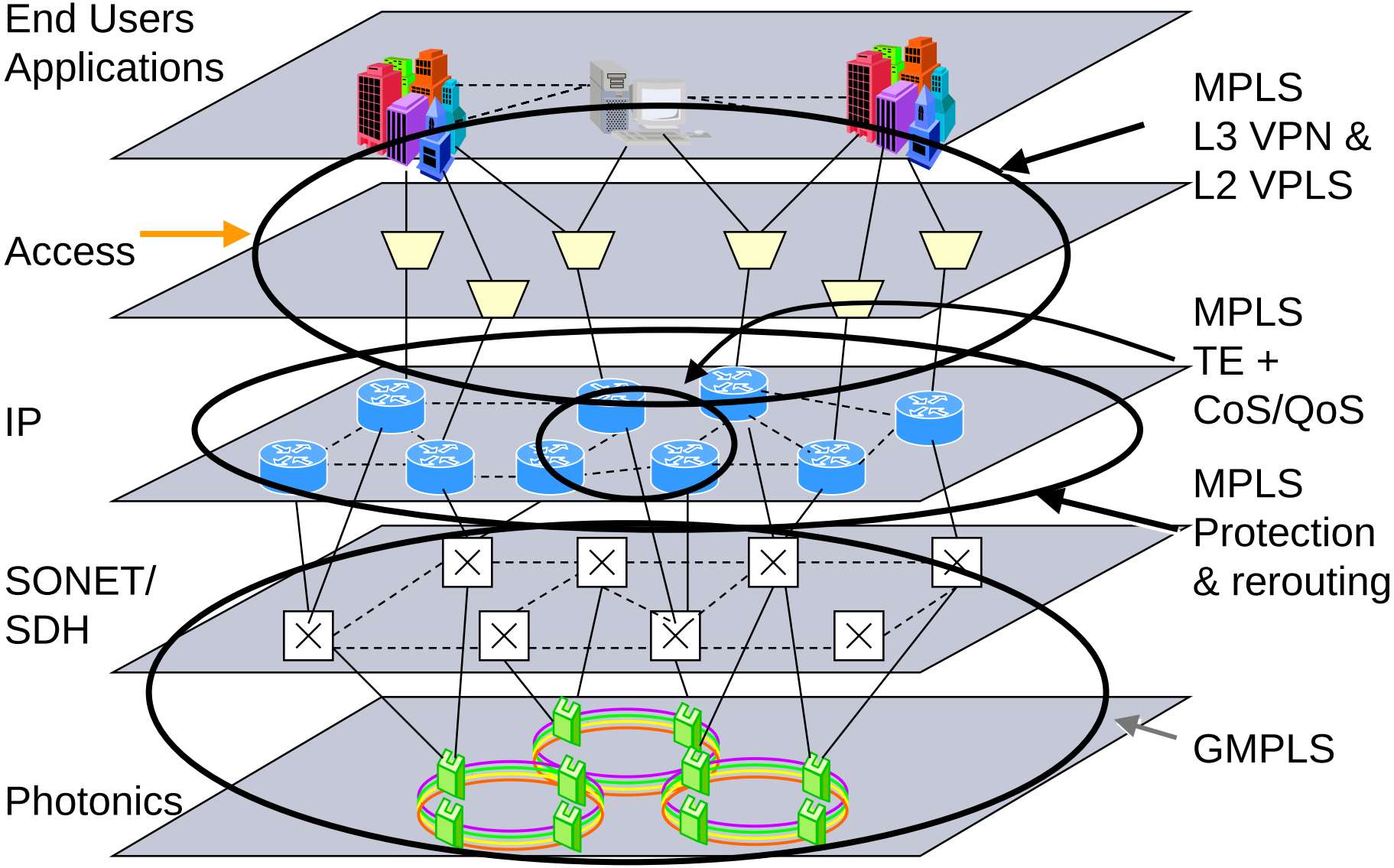
Why MPLS ?

A Common Control Plane

Best of the packet-switched and circuit-switched worlds

- Enhancement and scalability of IP
- Metro Ethernet Services
- Legacy Network Migration
- Differentiated Services - CoS and QoS
- Layer 2 and Layer 3 VPNs
- Link Resiliency and Path Protection

MPLS: Addresses many network needs



MPLS FR Alliance and the IETF

- **MPLS Frame Relay Alliance – Mission**
  - The MPLS Frame Relay Alliance is an international industry wide organization driving worldwide deployment of multi-vendor multi-service label switching networks and associated applications.
  - **Go to http://www.mplsforum.org**

- **IETF – Mission**
  - The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
  - **Go to http://www.ietf.org**

Virtual Private Networks

- Provide private line and private LAN connections between multiple sites
- Leverage public network to provide competitive service pricing and reduce service operating cost

Corporate Headquarters

Storage Facility

Public Network

Home office

Remote office

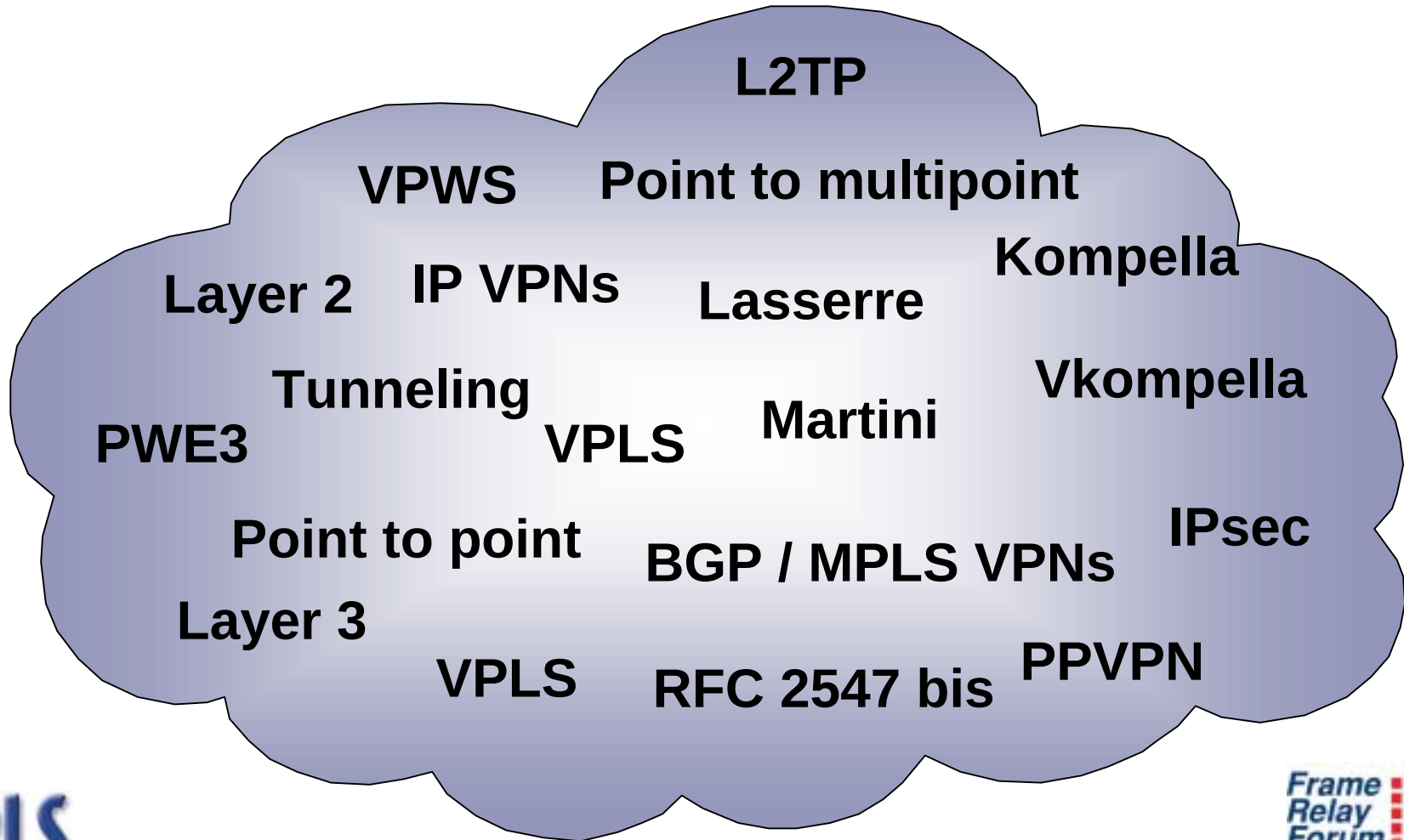
MPLS FORUM

Virtual Private Networks

- 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

MPLS, VPNs, and Standards

A lot of confusion



VPNs

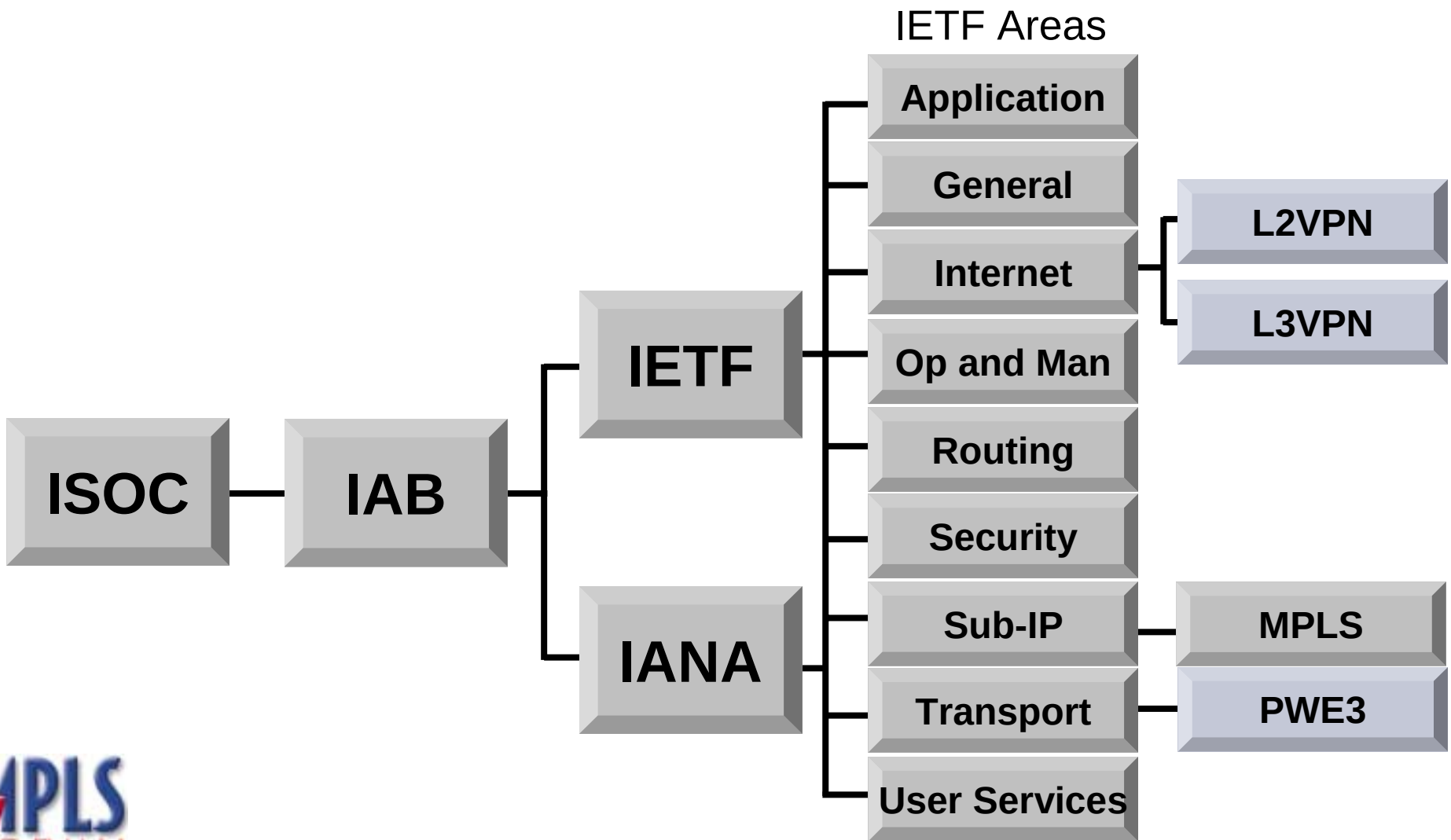
Types, Layers, and Implementations

VPN Type	Layer	Implementation
Leased Line	1	TDM/SDH/SONET
Frame Relay	2	DLCI
ATM	2	VC
GRE/UTI/L2TPv3	3	IP Tunnel
Ethernet	2	VLAN / VPWS / VPLS
IP	3	RFC2547bis / VR
IP	3	IPSec

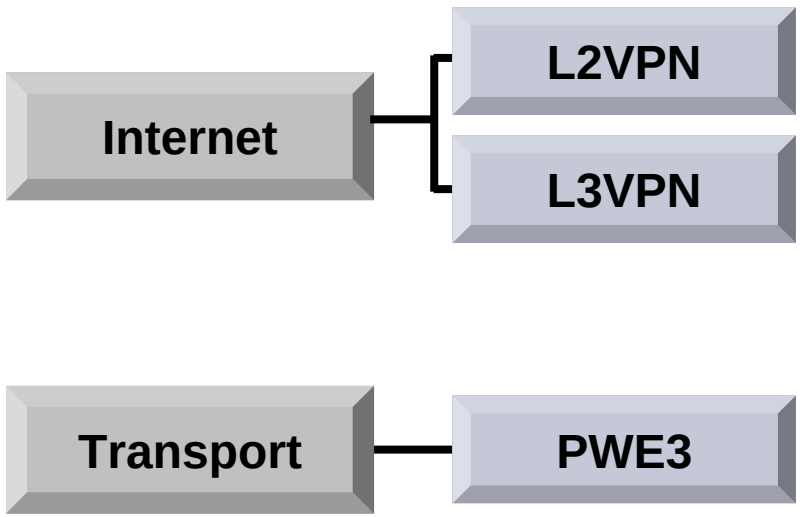
VPNs
How do they compare?

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

MPLS VPNs in the IETF



MPLS VPNs in the IETF

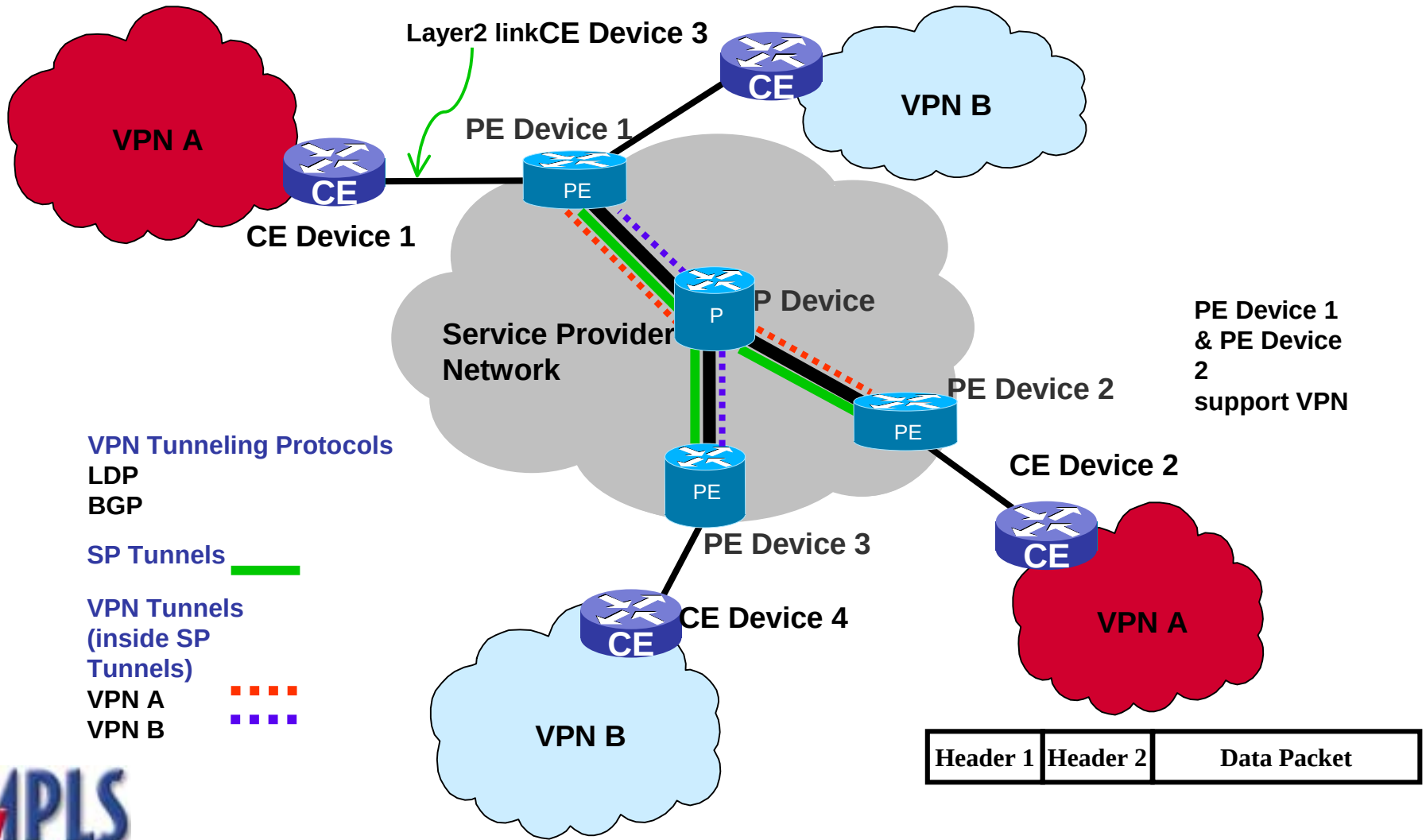


- Layer 2 VPNs
- Layer 3 VPLS
- Pt-to-Pt circuits
- Encapsulations
  - ATM
  - FR
  - Ethernet
  - PPP/HDLC
  - SONET/SDH

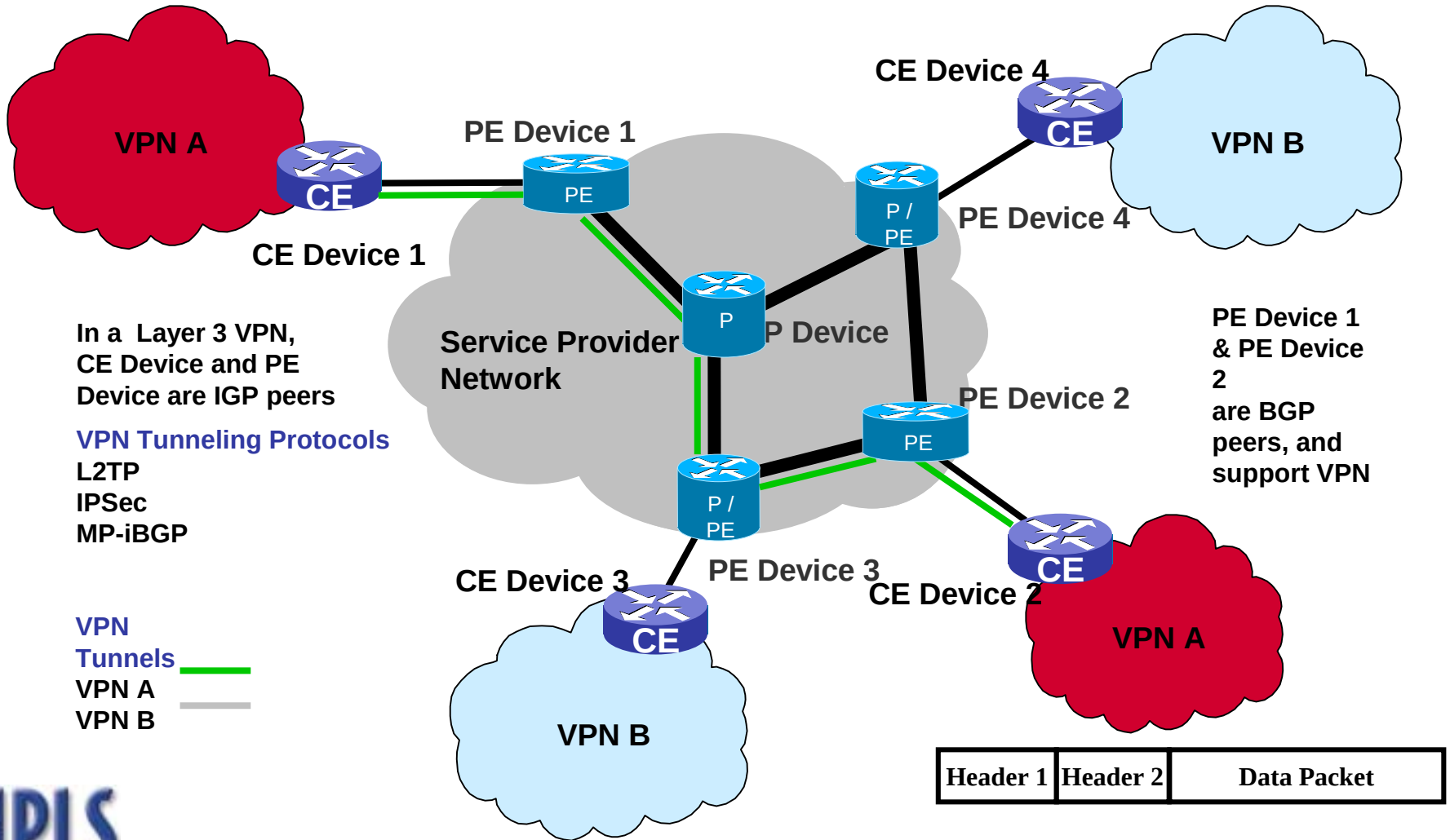
What are Layer 2, Layer 3 VPNs

- 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)
- VPNs based on tunneling at Layer 3 (Network Layer) are Layer 3 VPNs, (BGP/MPLS, VR, IPSec)

Visually - Layer 2 VPN



Visually - Layer 3 VPN



MPLS VPN Tutorial Agenda

- Introduction to MPLS and MPLS VPNs
  - Defining Layer 2 and 3 VPNs?
- Layer 3 MPLS VPN
  - BGP Review
  - RFC 2547bis Key Characteristics
  - BGP/MPLS VPN Architecture Overview
    - ✓ VPN Routing and Forwarding (VRF) Tables
    - ✓ Overlapping VPNs
    - ✓ VPN Route Distribution
    - ✓ VPN Packet Forwarding
    - ✓ Scaling L3VPNs and Route Reflectors

What is BGP?

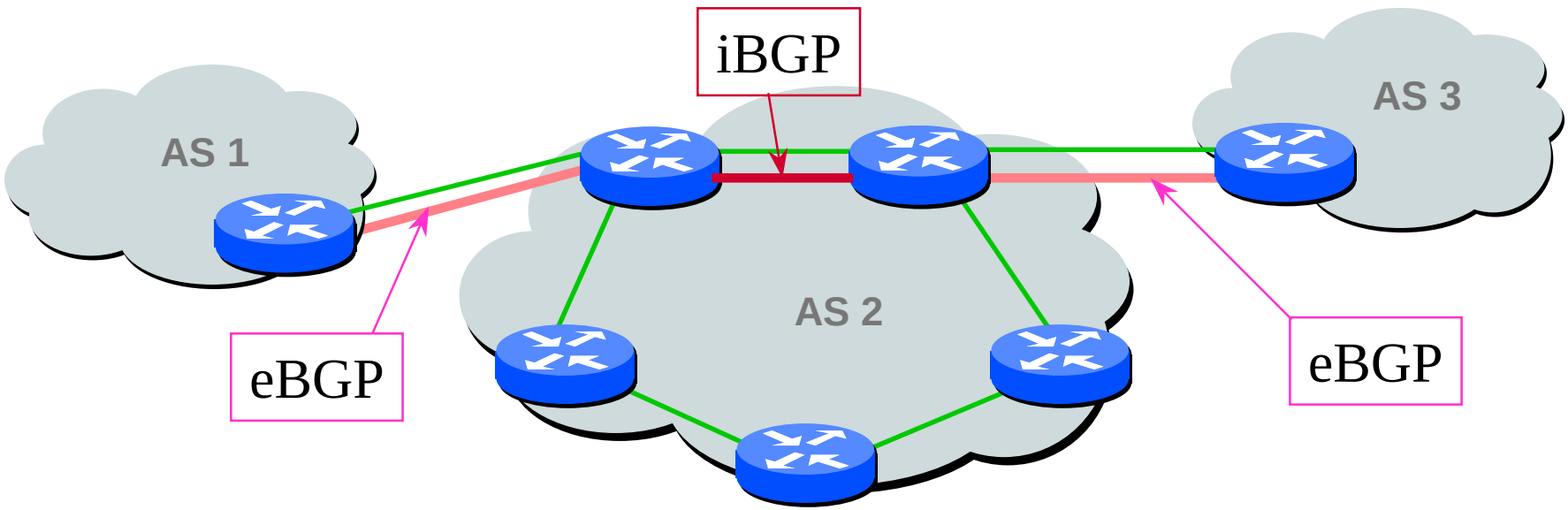
- BGP is an exterior gateway protocol that allows IP routers to exchange network reachability information.
- BGP became an internet standard in 1989 (RFC 1105) and the current version, BGP-4 was published in 1994 (RFC 1771).
- BGP is continuing to evolve through the Internet standards process.

IGP vs. EGP

- **Interior Gateway Protocol**
  - **RIP, OSPF, IS-IS**
  - **Dynamic, some more than others**
  - **Define the routing needed to pass data *within* a network**
- **Exterior Gateway Protocol**
  - **BGP**
  - **Less Dynamic than IGPs**
  - **Defines the routing needed to pass data *between* networks**

Internal Border Gateway Protocol

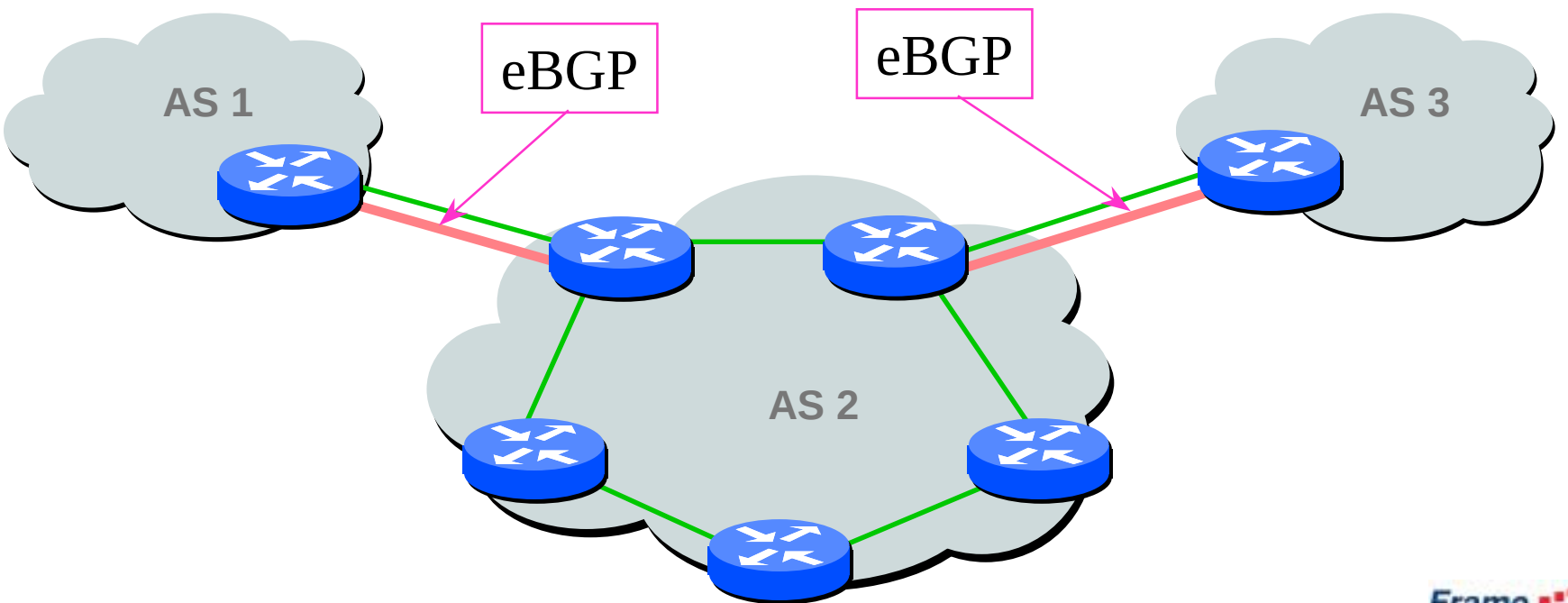
i**BGP** - BGP between routers in the same AS.



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

External Border Gateway Protocol

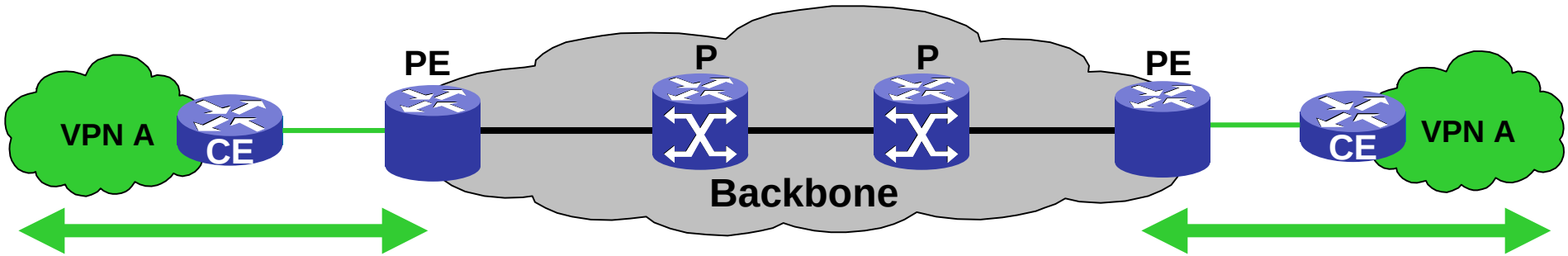
eBGP - BGP between routers in two different AS's.



MPLS VPN Tutorial Agenda

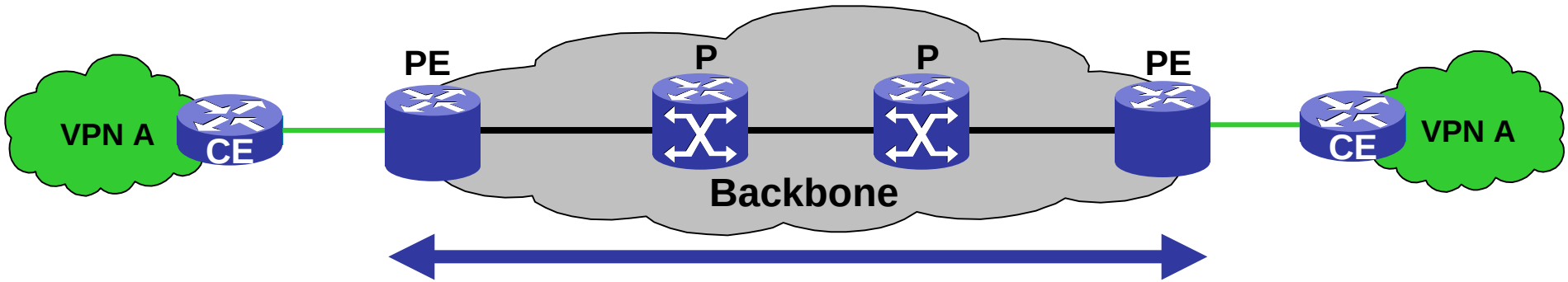
- Introduction to MPLS and MPLS VPNs
  - Defining Layer 2 and 3 VPNs?
- Layer 3 MPLS VPN
  - BGP Review
  - RFC 2547bis Key Characteristics
  - BGP/MPLS VPN Architecture Overview
    - ✓ VPN Routing and Forwarding (VRF) Tables
    - ✓ Overlapping VPNs
    - ✓ VPN Route Distribution
    - ✓ VPN Packet Forwarding
    - ✓ Scaling L3VPNs and Route Reflectors

RFC 2547bis BGP/MPLS VPNs
Key Characteristics



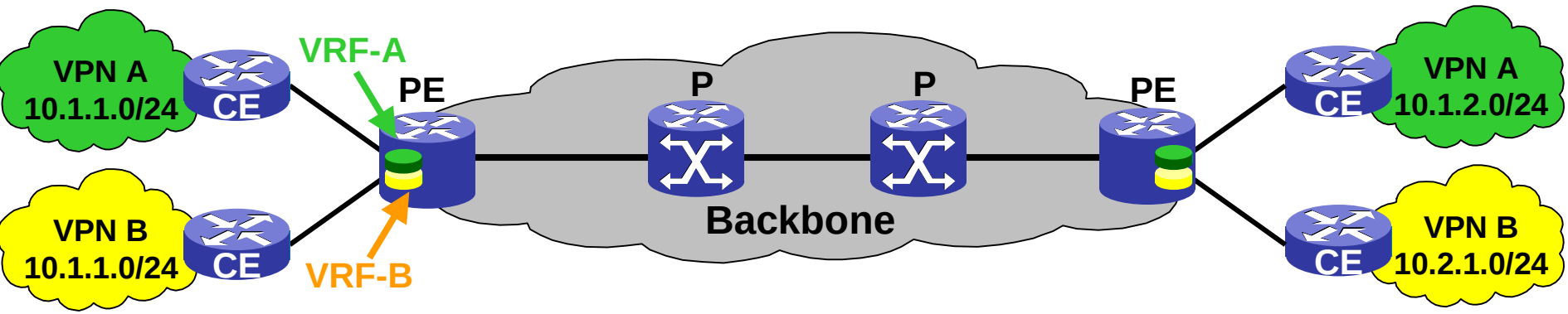
- Requirements:
  - Support for overlapping, private IP address space
  - Different customers run different IGPs (i.e. RIP, OSPF, IS-IS)
- Solution:
  - VPN network layer is terminated at the edge (PE)
    - ✓ PE routers use plain IP with CE routers

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

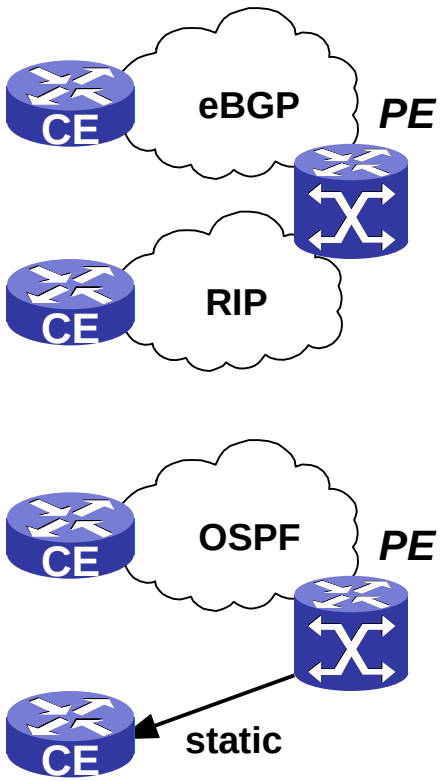
VPN Routing and Forwarding (VRF) Tables



- 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

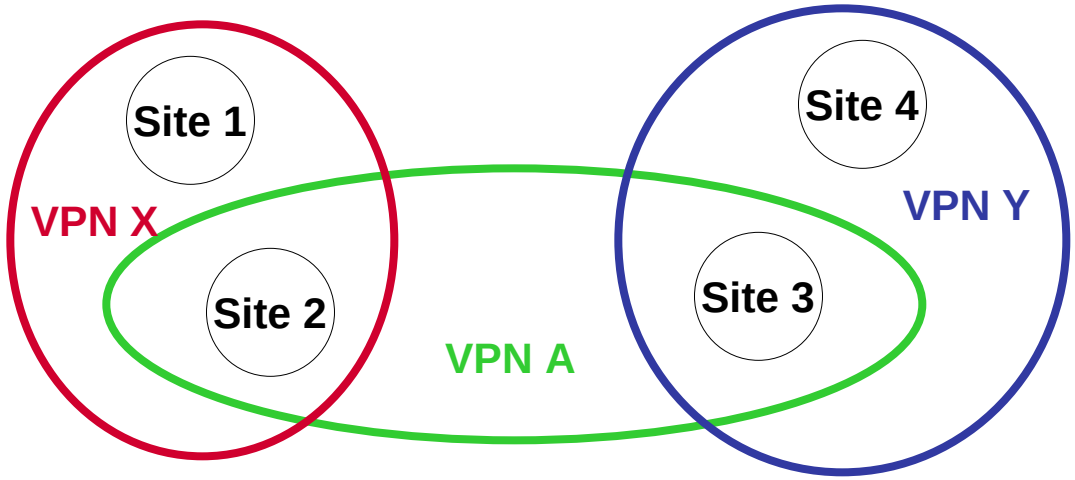
VPN Routing and Forwarding (VRF)

PE to CE Router Connectivity



- Protocols used between CE and PE routers to populate VRFs with customer routes
  - BGP-4
    - ✓ useful in stub VPNs and transit VPNs
  - RIPv2
  - OSPF
  - static routing
    - ✓ particularly useful in stub VPNs
- Note:
  - Customer routes need to be advertised between PE routers
  - Customer routes are not leaked into backbone IGP

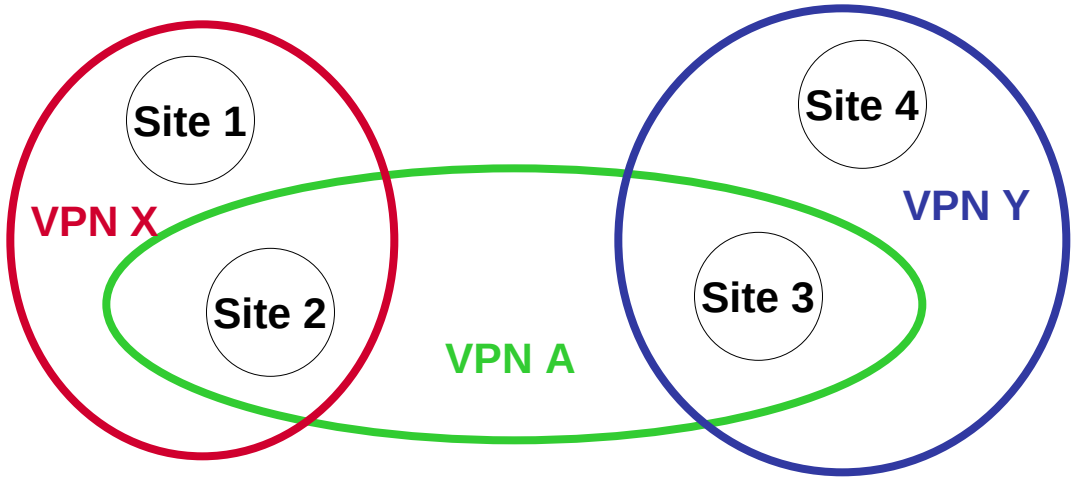
VPN Routing and Forwarding (VRF)
Overlapping VPNs



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)

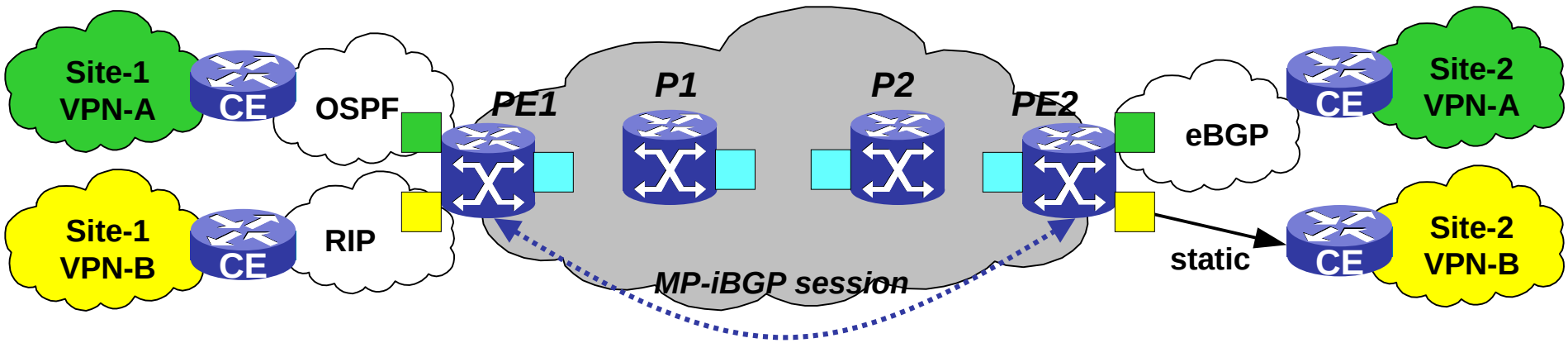
VPN Routing and Forwarding (VRF)
Overlapping VPNs



Examples:
- Extranet
- VoIP Gateway

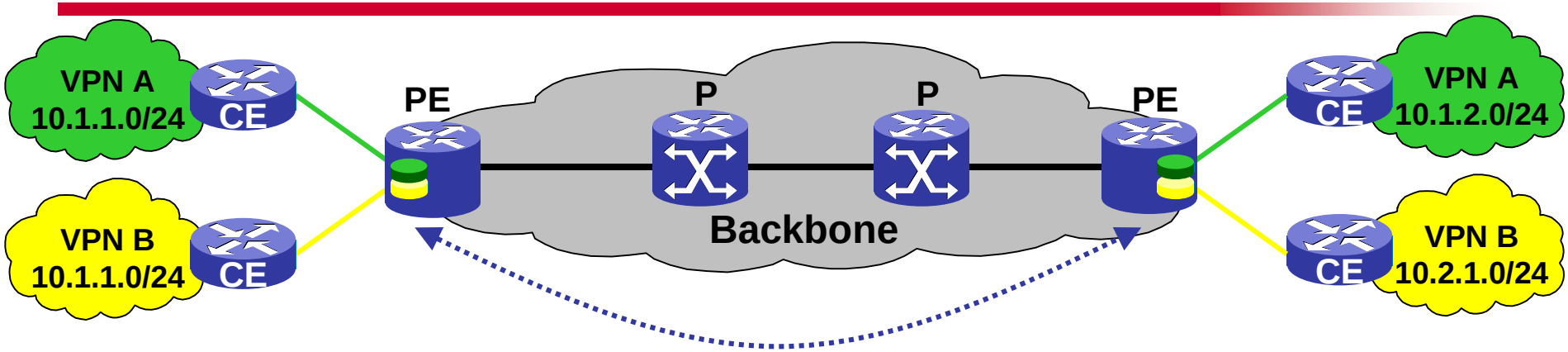
- A site can be part of different VPNs
- A site belonging to different VPNs *may* or *may not* be used as a transit point between VPNs
- If two or more VPNs have a common site, address space must be unique among these VPNs

VRFs 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
- Different IGPs or eBGP supported between PE and CE peers

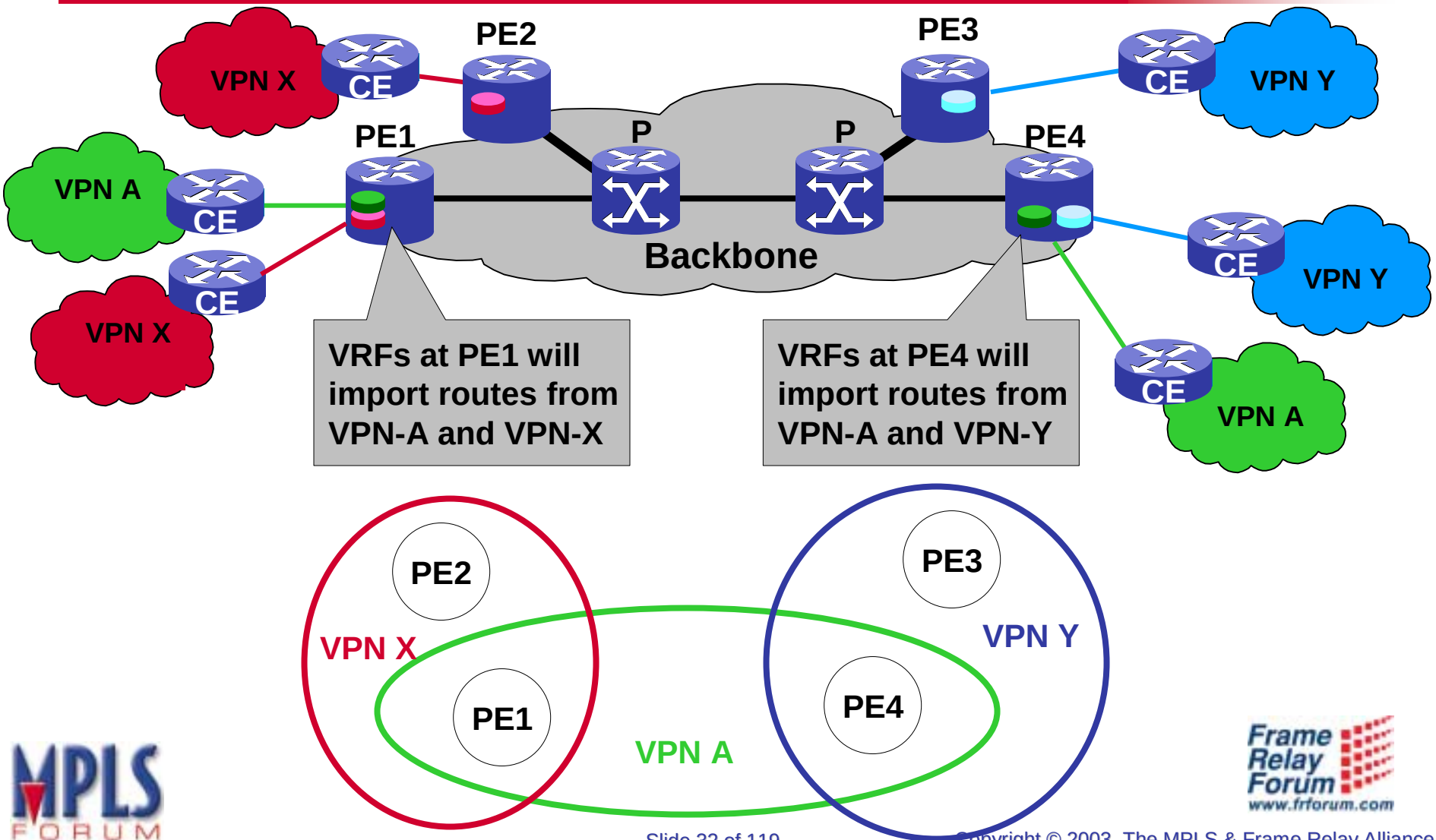
VPN Route Distribution
Route Targets



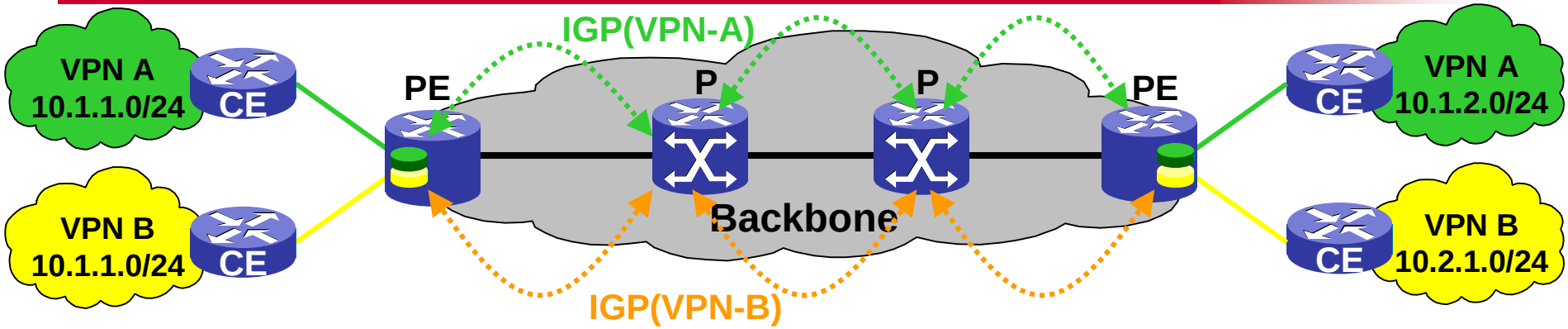
- Route Target attributes
  - "Export" Route Target: Every VPN route is tagged with one or more route targets when it is exported from a VRF (to be offered to other VRFs)
  - "Import" Route Target: A set of routes targets can be associated with a VRF, and all routes tagged with at least one of those route targets will be inserted into the VRF

VPN Route Distribution

Route Targets



VPN Route Distribution

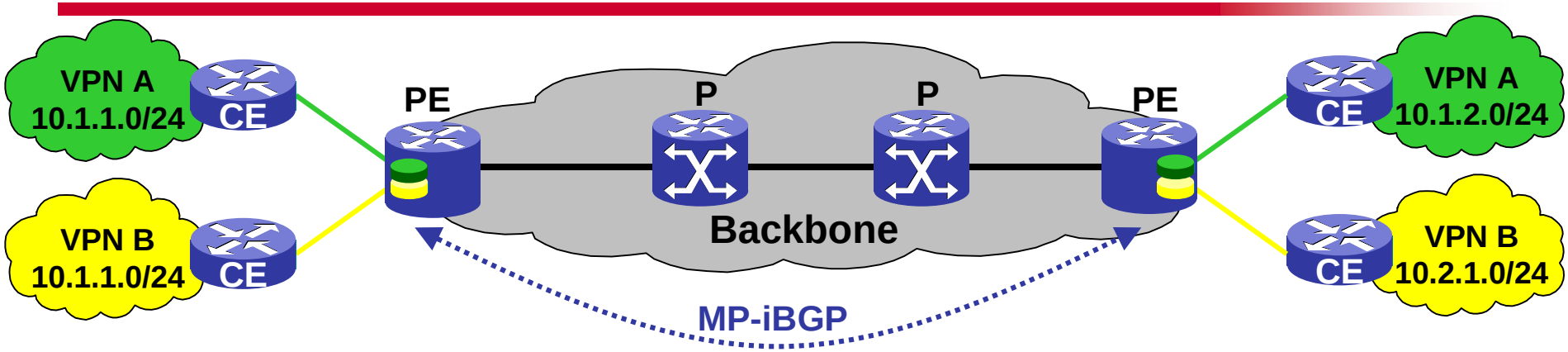


- *How will the PE routers exchange information about VPN customers and VPN routes between themselves?*

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



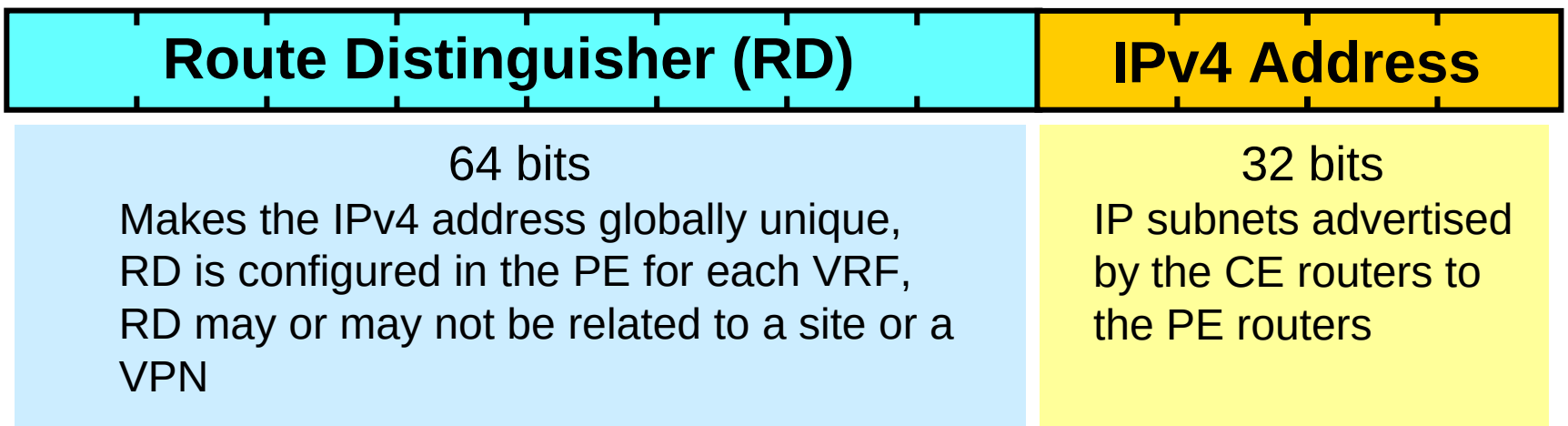
- *How will the PE routers exchange information about VPN customers and VPN routes between themselves?*

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.

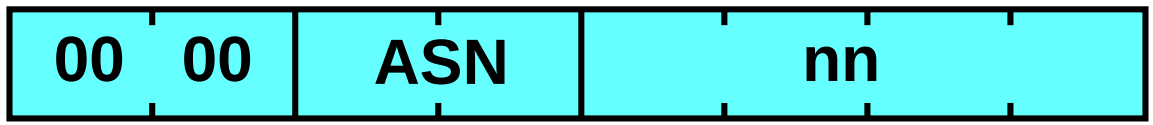
VPN Route Distribution
VPN-IPv4 Addresses

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

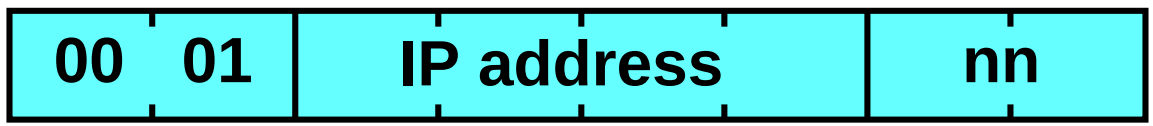


VPN Route Distribution
VPN-IPv4 Addresses

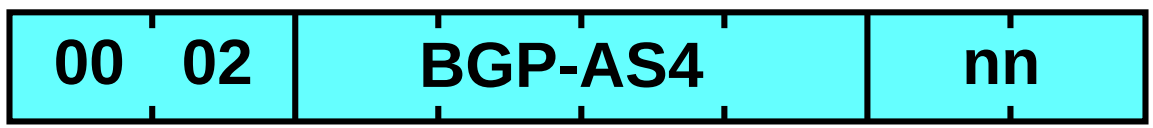
- Route Distinguisher format



  - ASN:nn
    - ✓ Autonomous System Number (ASN) assigned by Internet Assigned Number Authority (IANA)



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



  - BGP-AS4:nn
    - ✓ 4-byte Autonomous System Number (BGP-AS4)

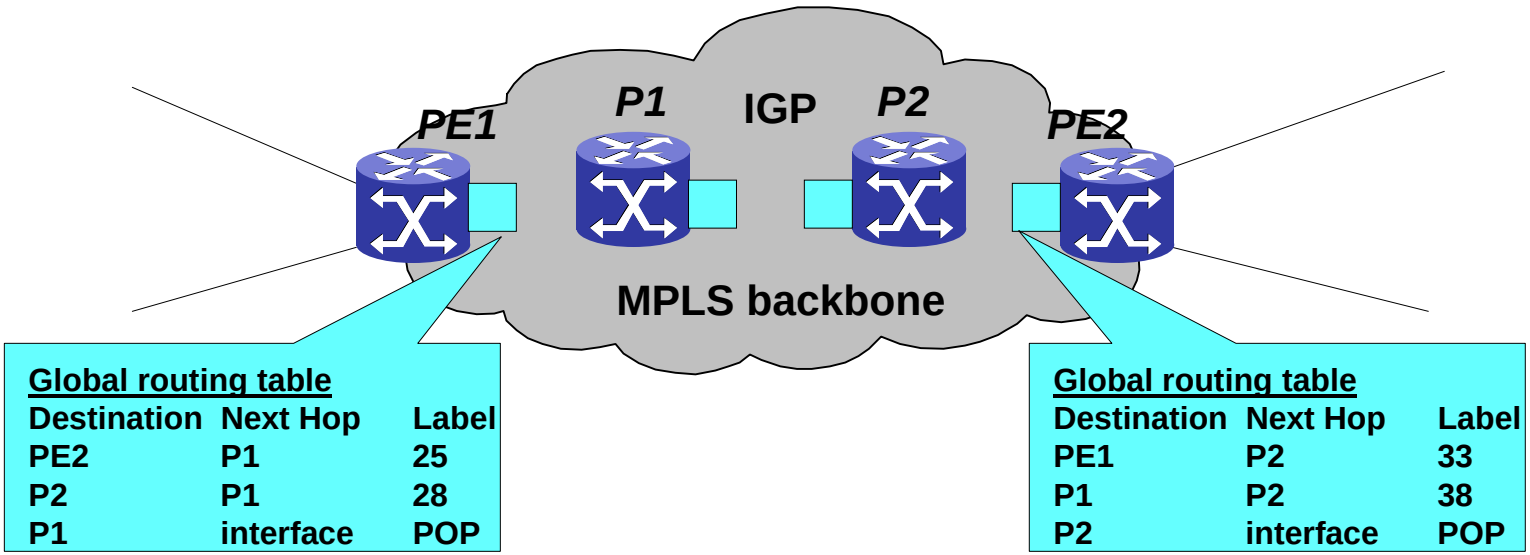
VPN Route Distribution
BGP with Multiprotocol Extensions

- *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 (PE)
  - propagates VPN-IPv4 addresses
  - carries additional BGP route attributes (e.g. route target) called extended communities

VPN Route Distribution
BGP with Multiprotocol Extensions

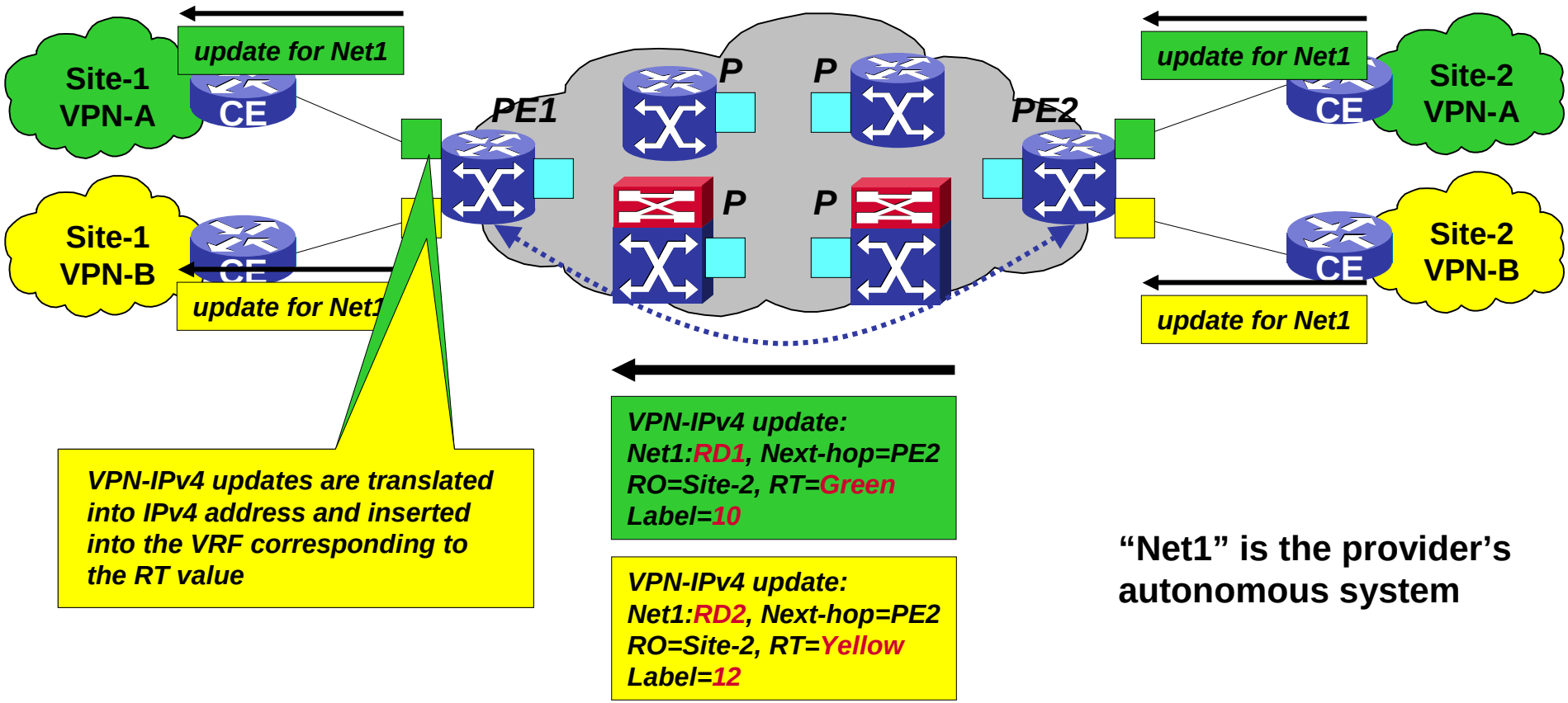
- A BGP route is described by
  - standard BGP Communities attributes (e.g. Local Preference, MED, Next-hop, AS_PATH, Standard Community, etc.)
  - extended BGP Communities attributes
- Extended Communities
  - Route Target (RT)
    - ✓ identifies the set of sites the route has to be advertised to
  - Route Origin (RO)/Site of Origin
    - ✓ identifies the originating site
    - ✓ to prevent routing loops with multi-homed customer sites

IGP Label Distribution



- 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



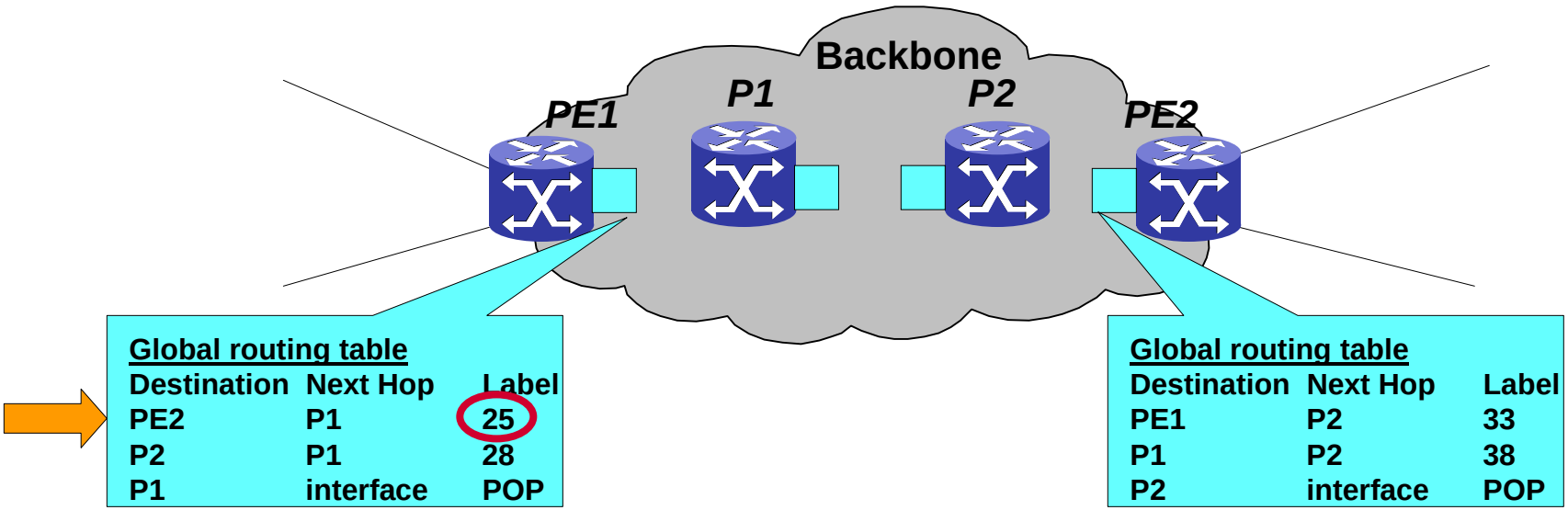
"Net1" is the provider's autonomous system

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.

MP-BGP = BGP with Multiprotocol Extensions

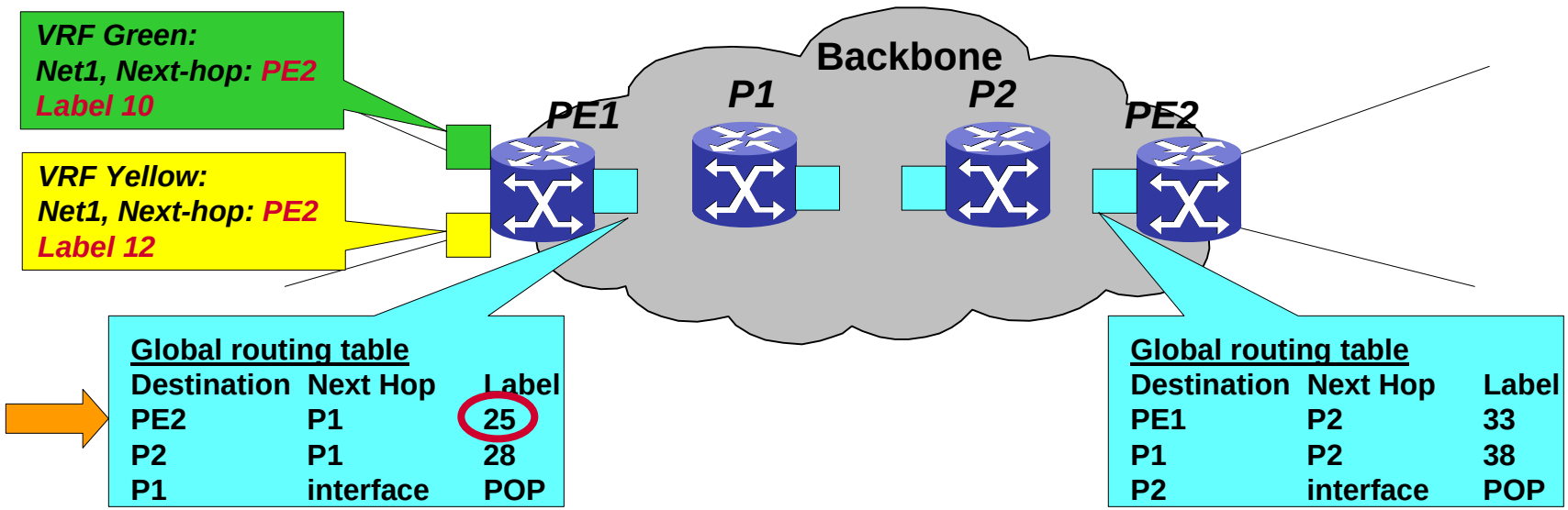
VPN Packet Forwarding



PE-to-PE connectivity via LSPs

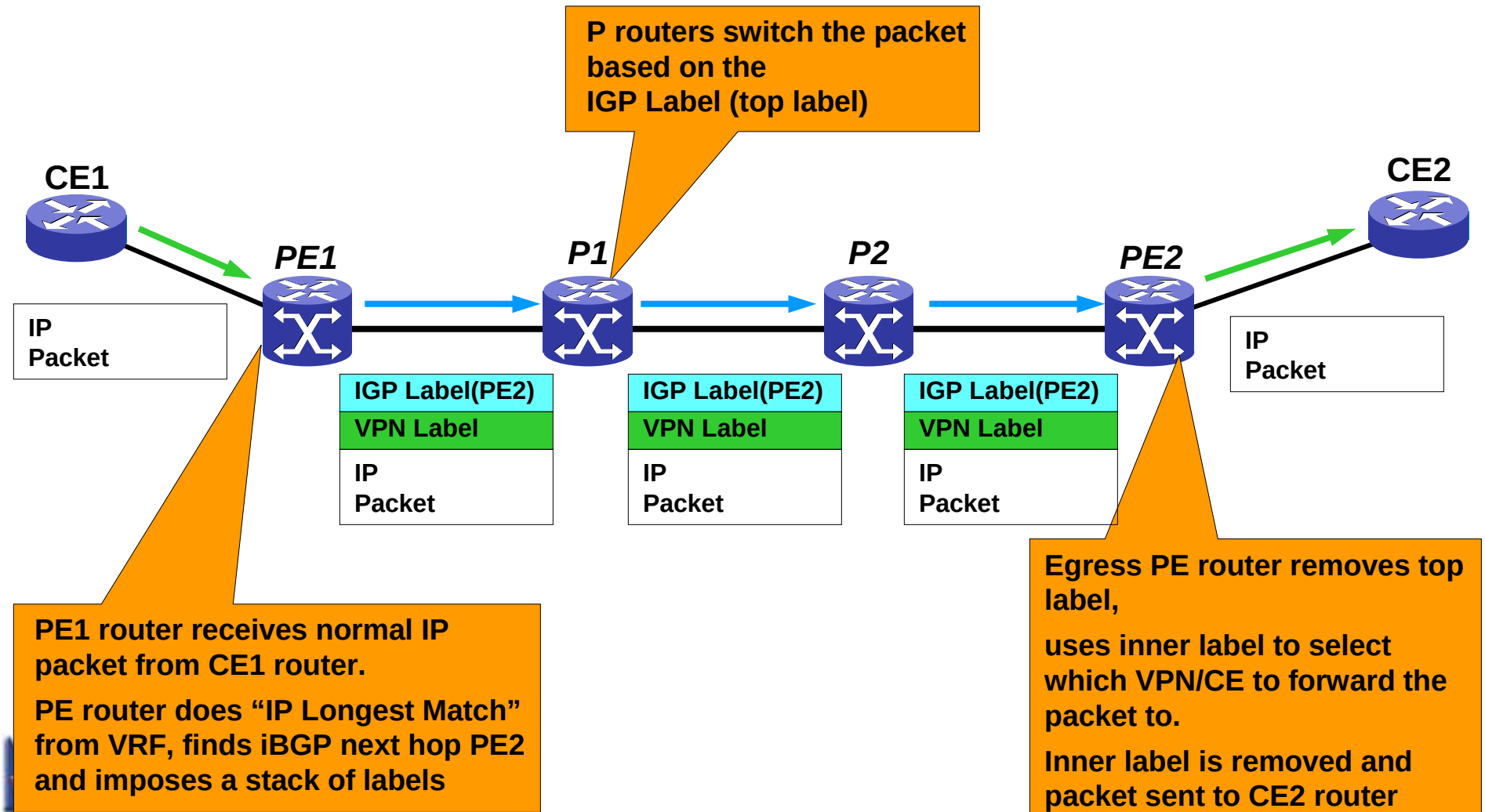
- All routers (P and PE) run an IGP and a label distribution protocol
- Each P and PE router has routes for the backbone nodes and a label is associated to each route
- MPLS forwarding is used within the backbone

VPN Packet Forwarding
Label Stacking

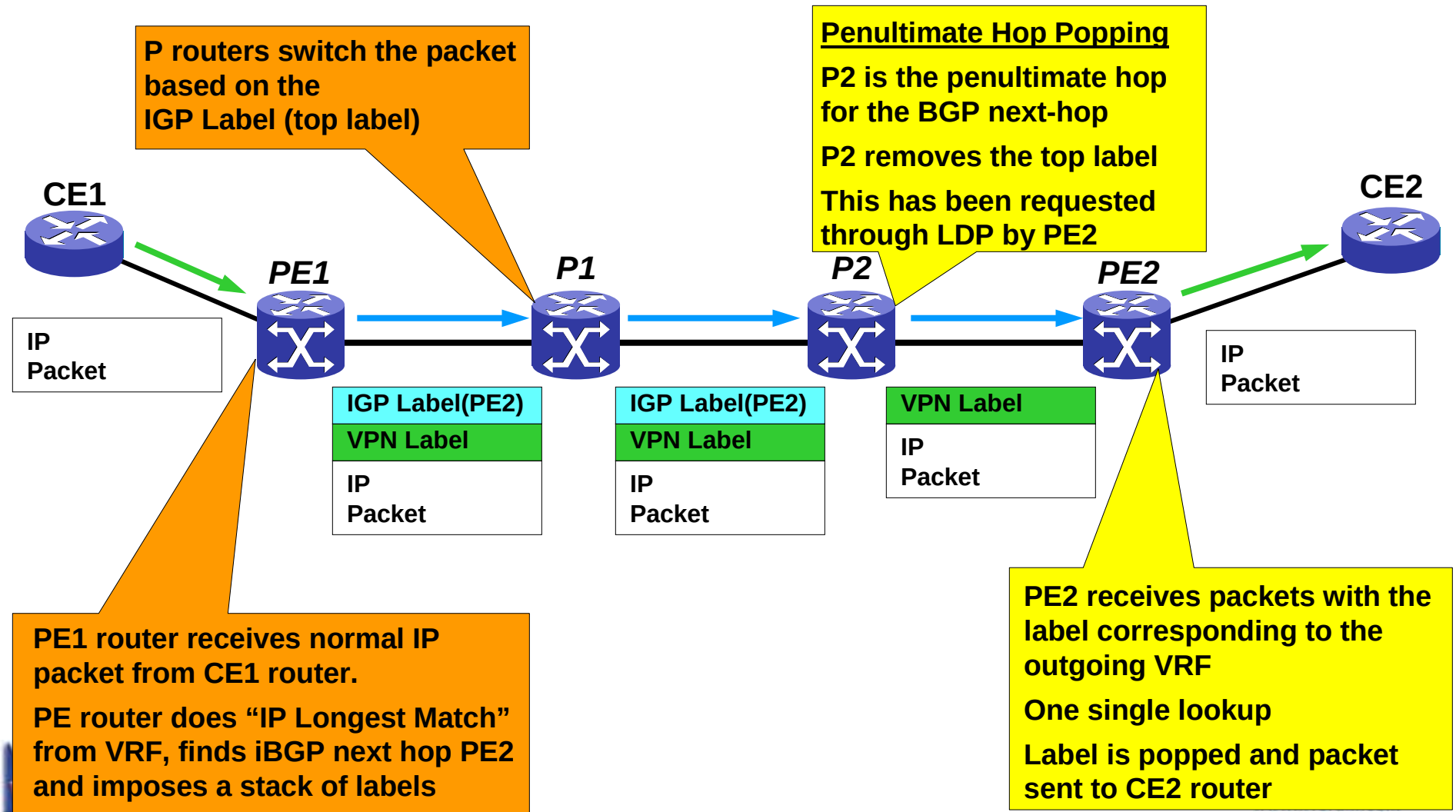


- Ingress PE router uses <u>two-level label stack</u>
  - **VPN label** (inner label) assigned by the egress PE router
  - **IGP label** (top label) identifying the PE router
- Label stack is attached in front of the VPN packet
- The MPLS packet is forwarded across the P network

VPN Packet Forwarding
Label Stacking

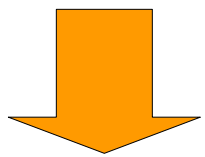


VPN Packet Forwarding
Penultimate Hop Popping



Core Routers (P Routers)

- not involved in MP-BGP
- does not make routing decision based on VPN addresses
- forwards packet based on the top label value



- P routers do not need to carry VPN routing information or Internet routing information, thus providing better network scalability

Scaling BGP/MPLS VPNs

- Scalability of BGP/MPLS VPNs
  - Expanding the MPLS core network
    - ✓ without impact on the VPN services, e.g. adding P routers (LSRs), new or faster links
  - Label stacking
    - ✓ allows reducing the number of LSPs in the network core and avoiding LSP exhaustion
  - VPN Route Distribution
    - ✓ Route Reflectors

Scaling BGP/MPLS VPNs
Route Reflectors

- BGP Route Reflectors
  - Existing BGP technique, can be used to scale VPN route distribution
    - ✓ PEs don't need full mesh of BGP connections, only connect to RRs
    - ✓ By using multiple RRs, no one box needs to have all VPN routes
  - Each edge router needs only the information for the VPNs it supports
    - ✓ directly connected VPNs

Reference Material

Books:

"BGP4 Inter-Domain Routing in the Internet" by John Stewart ISBN 0-201-37951-1

"Internet Routing Architectures" by Bassam Halabi ISBN 1-56205-652-2

"Interconnections: Bridges and Routers" by Radia Perlman ISBN

“Internetworking with TCP/IP Volume 1” by Douglas Comer ISBN 0-13-468505-9

“TCP/IP Network Administration - Second Edition” by Craig Hunt ISBN 1-56592-322-7

"Routing in the Internet" by Christian Huitema ISBN 0-13-132192-7

Mail Lists:

SSR mailinglist - majordomo@cabletron.com

GateD mailinglists - See www.gated.org

North American Network Operators Group (NANOG) mailist - See www.merit.org

Reference Material
Request For Comments - RFCs

08/98 - RFC2385PS "Protection of BGP Sessions via the TCP MD5 Signature Option"
02/98 - RFC 2283PS "Multiprotocol Extensions for BGP-4"
01/97 - RFC 2042 "Registering New BGP Attribute Types"
08/96 - RFC 1998 "An Application of the BGP Community Attribute in Multi-home Routing"
08/96 - RFC 1997 "BGP Communities Attribute"
06/96 - RFC 1966 "BGP Route Reflection An alternative to full mesh"
06/96 - RFC 1965 "Autonomous System Confederations for BGP"
10/95 - RFC 1863 "A BGP/IDRP Route Server alternative to a full mesh routing"
08/95 - RFC 1817 “CIDR and Classful Routing”
03/95 - RFC 1774 "BGP-4 Protocol Analysis"
03/95 - RFC 1773 "Experience with the BGP-4 protocol"
03/95 - RFC 1772 "Application of the Border Gateway Protocol in the Internet"
03/95 - RFC 1771 "A Border Gateway Protocol 4 (BGP-4)
12/94 - RFC 1745 "BGP4/IDRP for IP---OSPF Interaction"
07/94 - RFC 1657 "Definitions of Managed Objects for BGP-4 using SMIv2"
09/93 - RFC 1520 “Exchanging Routing Information Across Provider Boundaries in CIDR”
09/93 - RFC 1519 “CIDR; an Address Assignment and Aggregation Strategy”
09/93 - RFC 1518 “An Architecture for IP Address Allocation with CIDR”

Reference Material
Internet Drafts

08/98 "LDP Specification"
08/98 "Border Gateway Multicast Protocol (BGMP): Protocol Specification"
08/98 "A Framework for Inter-Domain Route Aggregation"
08/98 "Routing Policy Configuration Language (RPCL)"
08/98 "Carrying Label Information in BGP-4"
08/98 "Capabilities Negotiation with BGP-4"
08/98 "BGP Security Analysis"
08/98 "A Border Gateway Protocol 4 (BGP-4)"
07/98 "Using RPSL in Practice"
07/98 "Multiprotocol Label Switching Architecture"
06/98 "NHRP for Destinations off the NBMA Subnetwork"
05/98 "BGP Route Flap Damping"
04/98 "BGP-4 Capabilities Negotiation for BGP Multiprotocol Extensions"
03/98 "To Be Multihomed: Requirements & Definitions"
03/98 "BGP-4 over ATM and Proxy PAR"
02/98 "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing"
02/98 "Carrying Label Information in BGP-4"
01/98 "DNS-base NLRI origin AS verification in BGP"

Reference Material
Internet Drafts – L3VPN

General

- Guidelines of Applicability Statements for PPVPNs
- A Framework for Layer 3 Provider Provisioned Virtual Private Networks
- Generic Requirements for Provider Provisioned VPN
- Service requirements for Layer 3 Provider Provisioned Virtual Private Networks
- Framework for PPVPN Operations and Management
- Definition of Textual Conventions for Provider Provisioned Virtual Private Network Management
- Security Framework for Provider Provisioned Virtual Private Networks
- Using BGP as an Auto-Discovery Mechanism for Provider-provisioned VPNs
- **CE-to-CE Member Verification for Layer 3 VPNs**

BGP/MPLS VPN

- Applicability Statement for BGP/MPLS IP VPNs
- BGP/MPLS IP VPNs
- OSPF as the PE/CE Protocol in BGP/MPLS VPNs
- Use of PE-PE IPsec in RFC2547 VPNs
- Use of PE-PE GRE or IP in RFC2547 VPNs
- BGP-MPLS VPN extension for IPv6 VPN
- **MPLS/BGP Virtual Private Network Management Information Base Using SMIv2**

Virtual Router

- Applicability Statement for Virtual Router-based Layer 3 PPVPN approaches
- Network based IP VPN Architecture using Virtual Routers
- Virtual Router Management Information Base Using SMIv2

IPSEC

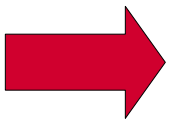
- An Architecture for Provider Provisioned CE-based Virtual Private Networks using IPsec

MPLS based Virtual Private Network Services

Break

http://www.mplsforum.org *http://www.frforum.com*

MPLS VPN Tutorial Agenda



- Layer 2 VPNs
  - IETF PWE3 and L2VPN WG update
  - Encapsulation and Label Stacking
  - Virtual Private Wire Services – VPWS
    - Pt-to-pt Ethernet, Pt-to-pt ATM, Pt-to-pt Frame Relay
  - Virtual Private LAN Services – VPLS
- Introduction to Multi-Service Interworking
  - Carrier Challenges at the Edge
  - Interworking History and Definition
  - Network and Service Interworking (FRF.5 and FRF.8.1)
  - MPLS FR Alliance Multi-Service Interworking Work Actions
- Carrier Migration Examples

MPLS L2 VPN Market Drivers

What can we conclude?

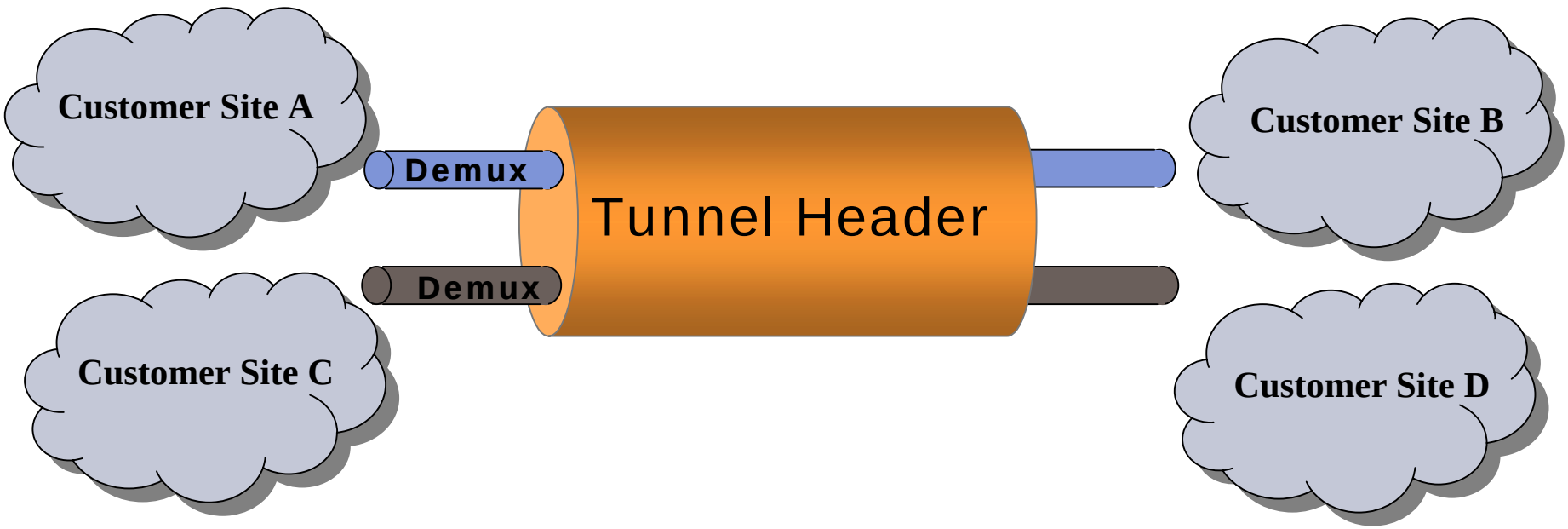
- Layer 3 IP is not the only traffic
  - Still a lot of legacy SNA, IPX etc
  - Large enterprises have legacy protocols
- Layer 3 IP VPNs are not the whole answer
  - IP VPNs cannot handle legacy traffic
- Layer 2 legacy traffic widely deployed

Carriers need to support Layer 2 and Layer 3 VPNs

MPLS Layer 2 VPNs

- Point-to-point layer 2 solutions
  - **Virtual Private Wire Services** - VPWS
  - Similar to ATM / FR services, uses tunnels and connections (LSPs)
  - Customer gets connectivity only from provider
  - Ongoing work to encapsulate Ethernet, ATM, FR, TDM, SONET, etc
- Multi-point layer 2 solutions
  - **Virtual Private LAN Services** - VPLS
  - Virtual Private LAN Services (VPLS) aka TLS
  - Ethernet Metro VLANs / TLS over MPLS
  - Independent of underlying core transport
  - All drafts “currently” support PWE3 (Martini) Ethernet encapsulation
  - Differences in drafts for discovery and signaling

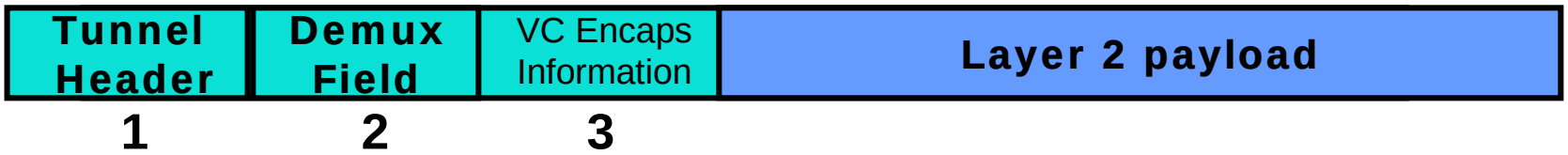
MPLS Point-to-Point Service



- Tunnel Label determines path through network
- VC Label identifies VLAN, VPN, or connection at the end point

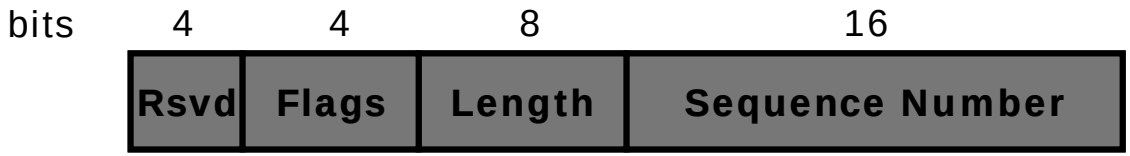
MPLS Point-to-Point Services

Label Stacking



- Three Layers of Encapsulation
  1) Tunnel Header: Contains information needed to transport the PDU across the IP or MPLS network
  2) Demultiplexer Field: Used to distinguish individual emulated VCs within a single tunnel
  3) Emulated VC Encapsulation: Contains the information about the enclosed PDU (known as Control Word)
- Tunnel Header determines path through network
- Demultiplexer Field identifies VLAN, VPN, or connection at the end point
- All services look like a Virtual Circuit to MPLS network

Encaps Information Field



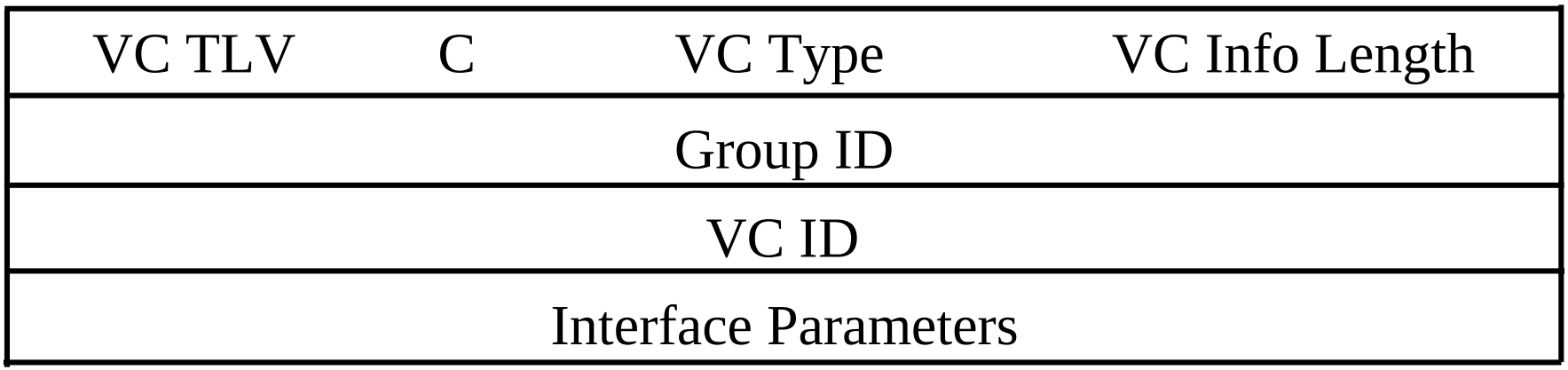
Control Word

- Layer 2 header fields may be discarded at ingress
- Control word carries “flag” bits depending on encapsulation
  - (FR: FECN, BECN, C/R, DE, ATM: CLP, EFCI, C/R, etc)
- Length required when padding small frames on links which have a minimum frame size
- Sequence number is optional. It is used to detect out of order delivery of frames.

LDP - Label Mapping Message

Label Mapping	Message Length
Message ID	
FEC TLV	
Label TLV	
Label Request Message ID TLV	
LSPID TLV (optional)	
Traffic TLV (optional)	

New VC FEC Element Defined



- Virtual Circuit FEC Element
  - C - Control Word present
  - VC Type - FR, ATM, Ethernet, HDLC, PPP, ATM cell
  - VC Info Length - length of VCID field
  - Group ID - user configured - group of VCs representing port or tunnel index
  - VC ID - used with VC type to identify unique VC
  - Interface Parameters - Specific I/O parameters

Layer 2 Encapsulation
Ongoing work in PWE3

- draft-ietf-pwe3-requirements-06.txt – 06/03
  - "This document describes base requirements for the Pseudo-Wire Emulation Edge to Edge Working Group (PWE3 WG). It provides guidelines for other working group documents that will define mechanisms for providing pseudo-wire emulation of Ethernet, ATM, Frame Relay, raw HDLC, and MPLS. "
- draft-ietf-pwe3-arch-05.txt – 08/03
  - "This document describes an architecture for Pseudo Wire Emulation Edge-to-Edge (PWE3). It discusses the emulation of services (such as Frame Relay, ATM, Ethernet TDM and SONET/SDH) over packet switched networks (PSNs) using IP or MPLS. It presents the architectural framework for pseudo wires (PWs), defines terminology, specifies the various protocol elements and their functions."

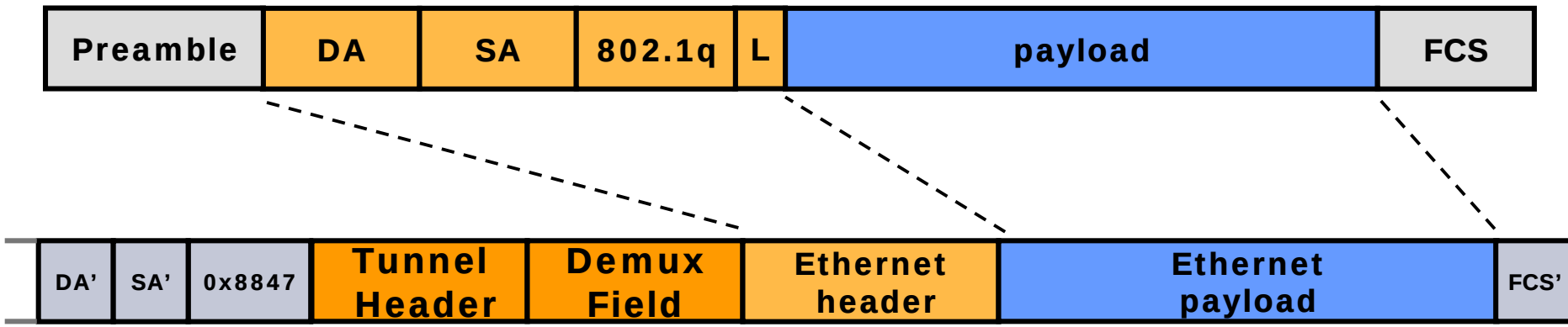
Layer 2 Encapsulation *PWE3*
WG documents (original Martini work)

- Pseudowire Set-up and Maintenance using LDP
  - ✓ draft-ietf-pwe3-control-protocol-03.txt – June 03
- ATM AAL5 and ATM cell
  - ✓ draft-ietf-pwe3-atm-encap-02.txt – June 03
- Frame Relay
  - ✓ draft-ietf-pwe3-frame-relay-01.txt – July 03
- Ethernet / 802.1q VLAN
  - ✓ draft-ietf-pwe3-ethernet-encap-03.txt - June 03
- PPP/HDLC
  - ✓ draft-martini-ppp-hdlc-encap-mpls-00.txt

MPLS Ethernet Encapsulation

draft-ietf-pwe3-ethernet-encap-03.txt

Original Ethernet frame

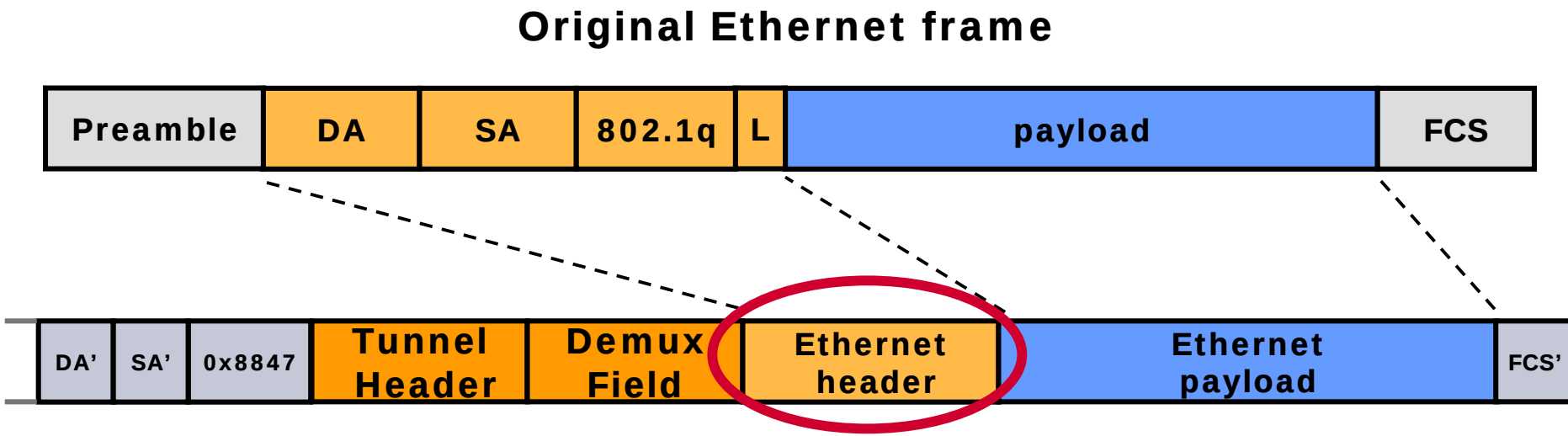


Encapsulated Ethernet over MPLS over Ethernet Transport

- Ingress device strips the Ethernet preamble and FCS
- Ethernet header becomes “control word”
- New MPLS Ethernet header (type 0x8847) and new FCS is added to MPLS Ethernet packet

MPLS Ethernet Encapsulation

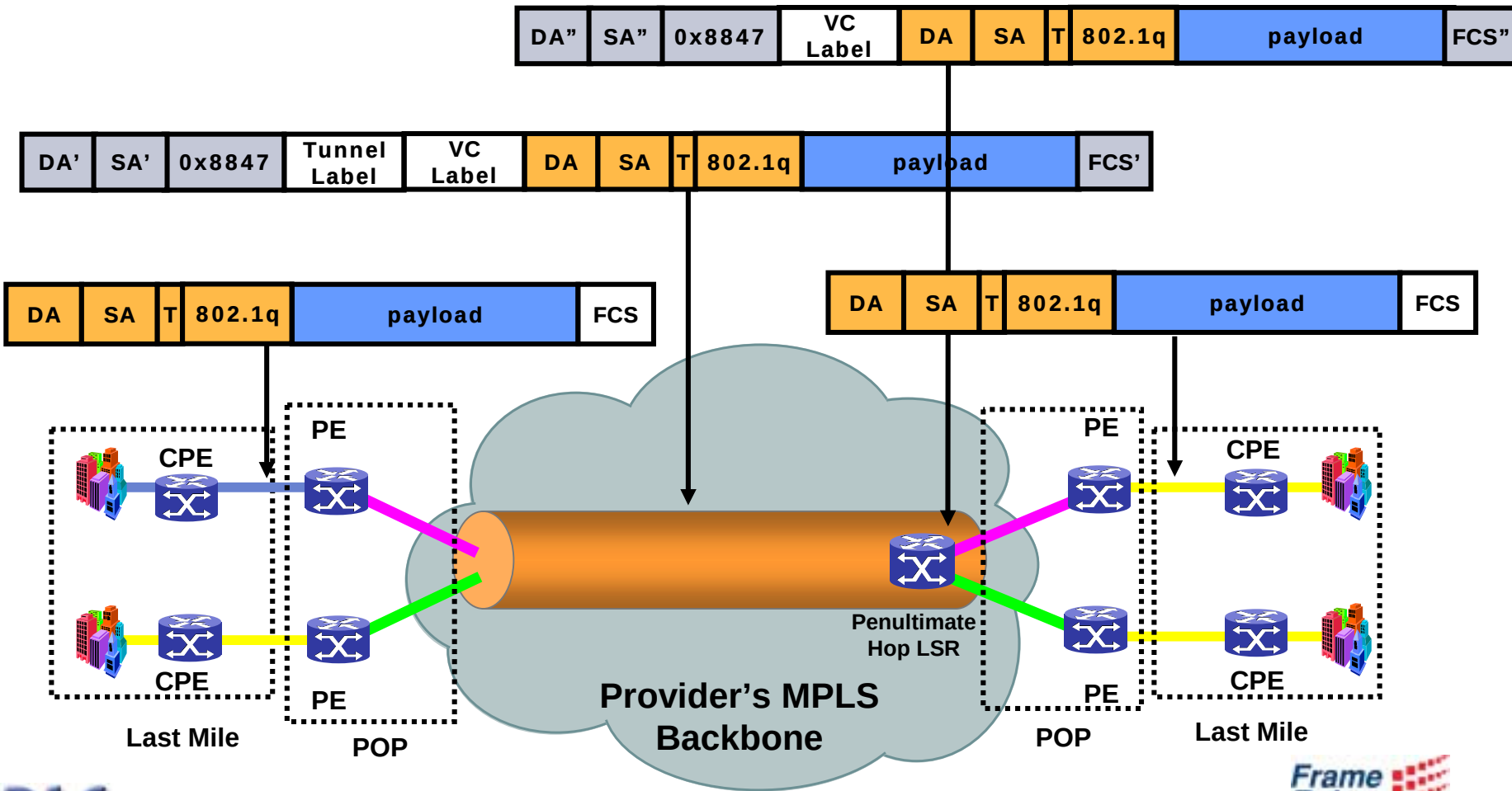
draft-ietf-pwe3-ethernet-encap-03.txt



- Martini VC Encaps field is normally 32 bits
- Ethernet VC Encaps field equals
  - DA and SA at 6 bytes each
  - Length at 2 bytes
  - 802.1q VLAN at 4 bytes
  - Total at 18 bytes (144 bits vs 32 bits)

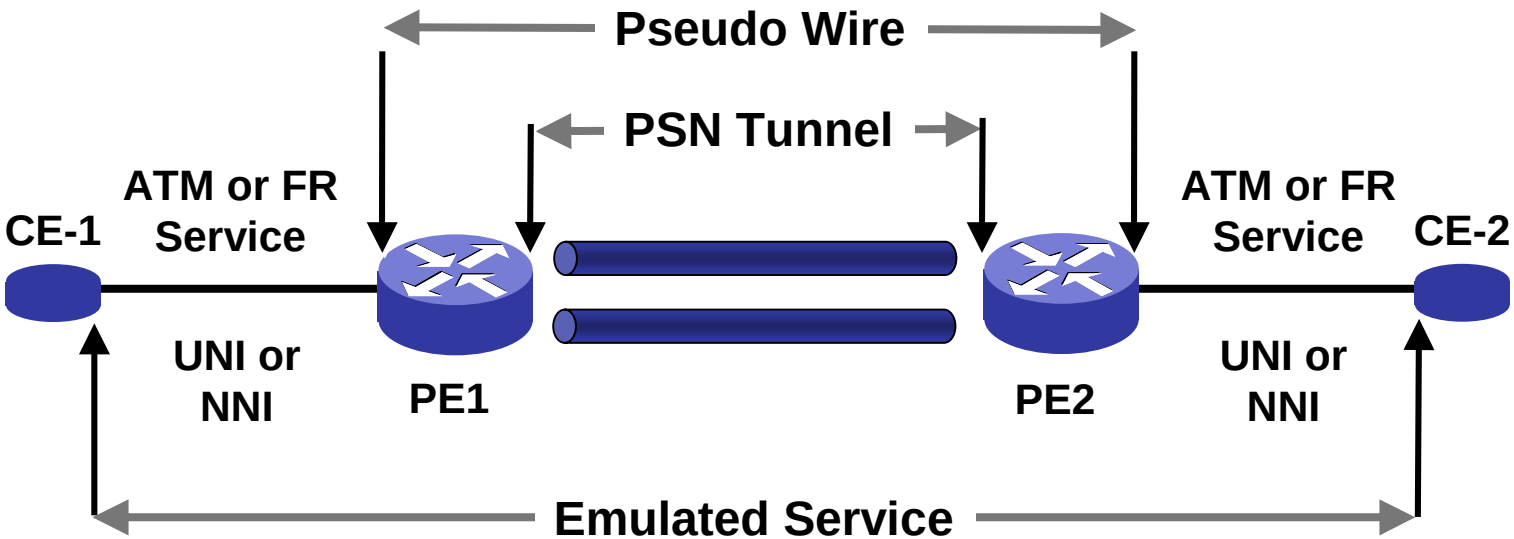
Life of a Frame

Ethernet over Ethernet MPLS



ATM and Frame Relay Service

Reference Model

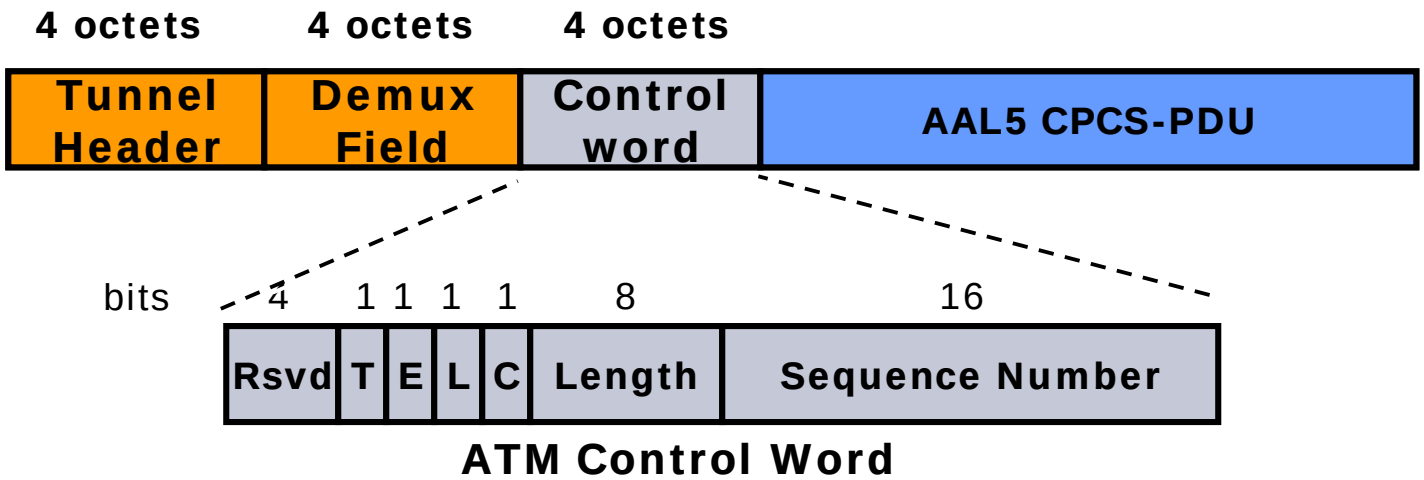


PE = Provider Edge
CE = Customer Edge

Requirements for Pseudo Wire Emulation Edge-to Edge (PWE3)

ATM AAL5 Encapsulation

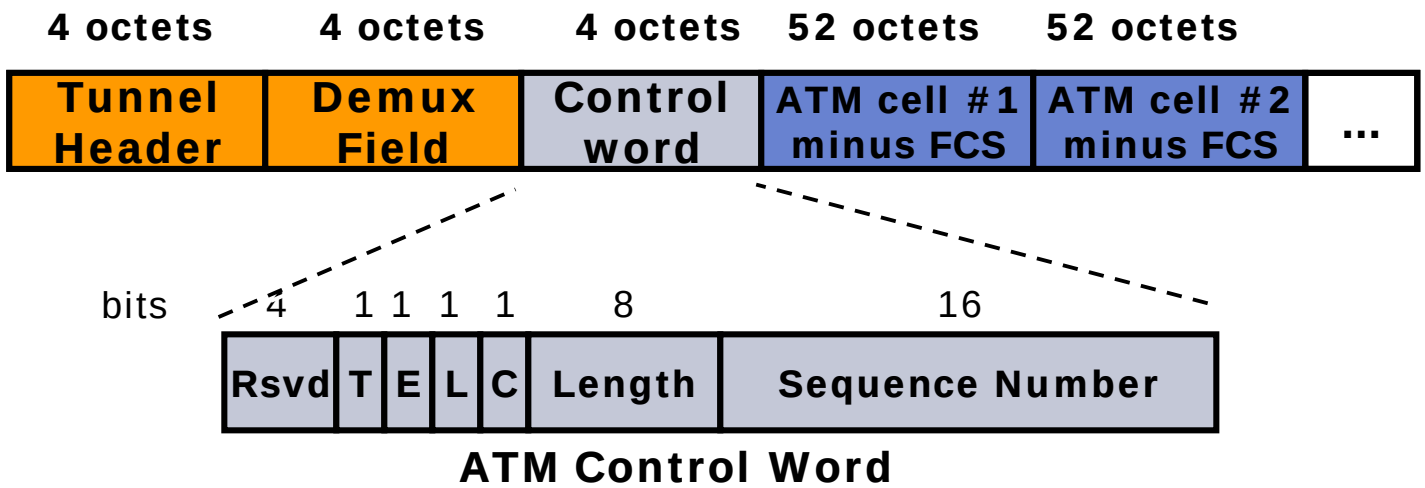
draft-ietf-pwe3-atm-encap-02.txt



- Ingress reassembles AAL5 frames and strips 8 octet AAL5 trailer
- Required control word includes:
  - T = Transport type bit
    - ✓ Common Part Convergence Sublayer-Protocol Data Unit (AAL5 CPCS-PDU)
    - ✓ Or ATM Cell
  - E = EFCI bit - Efficient Forward Congestion
  - L = CLP bit - Cell Loss Priority
  - C = Command / Response bit

ATM Cell Mode Encapsulation

draft-ietf-pwe3-atm-encap-02.txt



- Ingress performs no reassembly
- Control word is optional:
  - Length may be used to infer number of cells
  - Flags set to zero

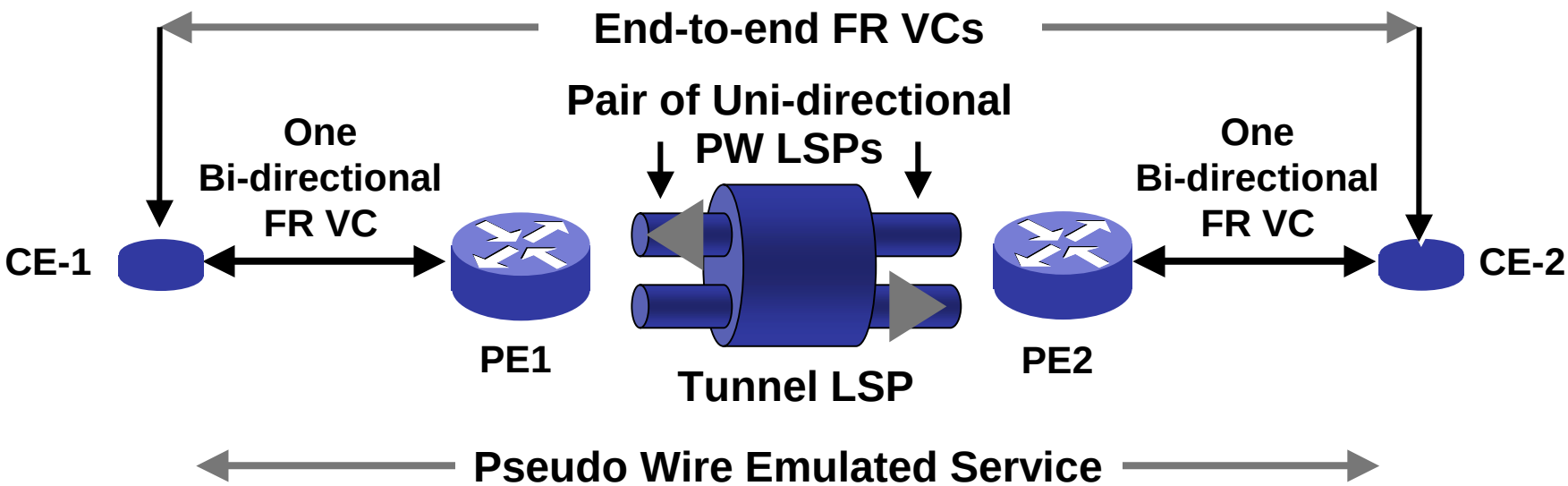
MPLS PWE3 FR Encapsulation

draft-ietf-pwe3-frame-relay-01.txt

- Main Functions: FR over Pseudo Wire - FRoPW
  - Encapsulation of FR specific information in a suitable FRoPW packet (ingress function)
  - Transfer of a FRoPW packet through IP / MPLS network
  - Extraction of FR specific information from a FRoPW packet (egress function)
  - Generation of native FR frames at egress
  - Other operations to support FR services

MPLS PWE3 FR Encapsulation

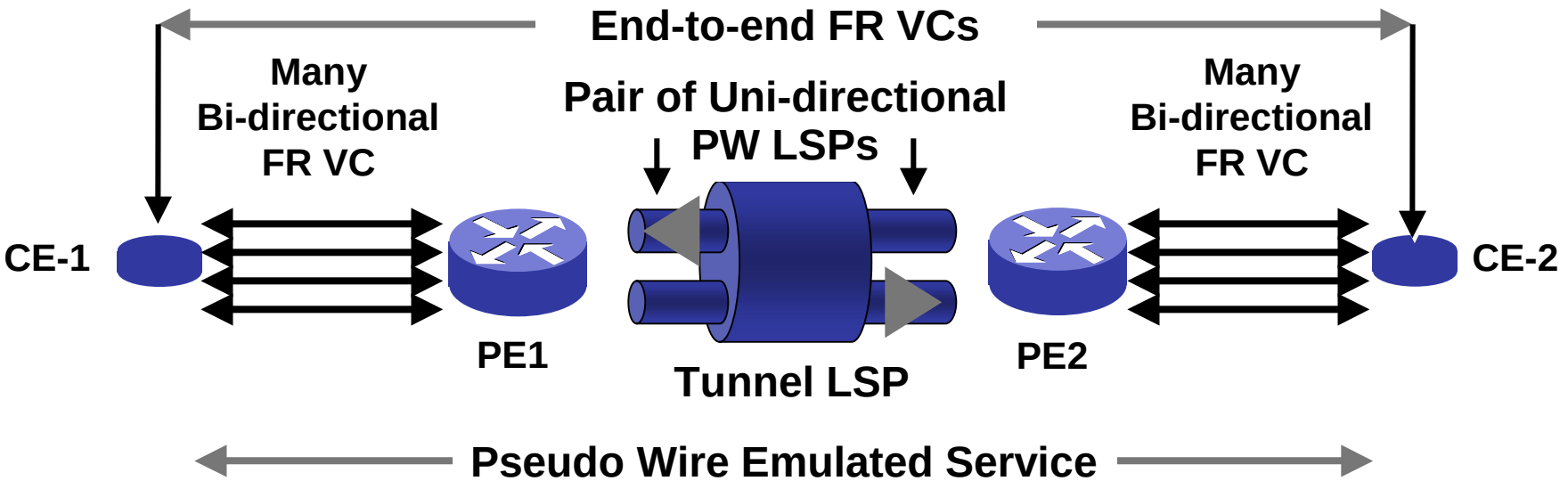
draft-ietf-pwe3-frame-relay-01.txt



- Two Mapping modes defined between FR VCs and FR PWs
  - One-to-one mapping
  - One FR VC mapped to a pair of unidirectional PWs

MPLS PWE3 FR Encapsulation

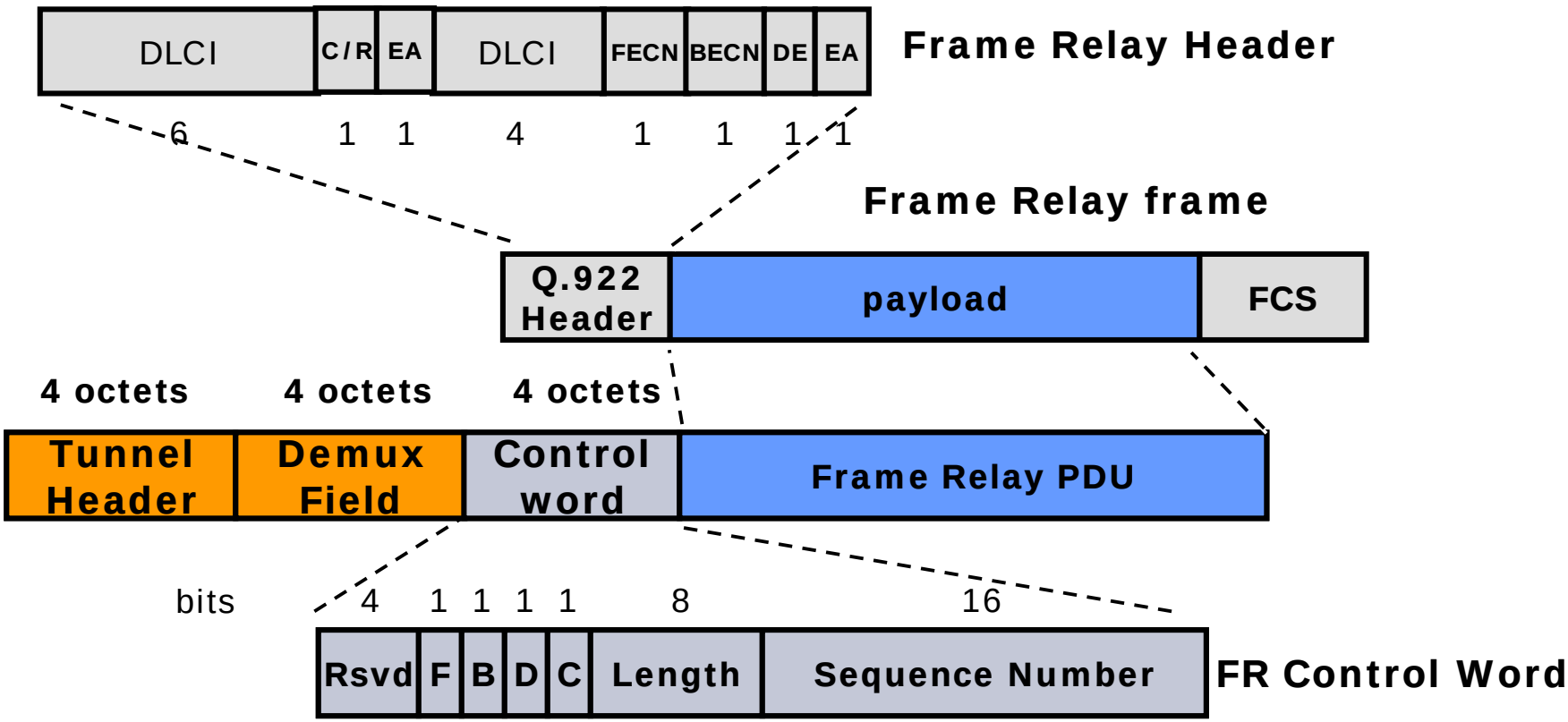
draft-ietf-pwe3-frame-relay-01.txt



- Two Mapping modes defined between FR VCs and FR PWs
  - Many-to-one or port mode mapping (Optional – w / header)
  - Many FR VCs mapped to a pair of Unidirectional PWs

MPLS Frame Relay Encapsulation

draft-ietf-pwe3-frame-relay-01.txt



- F = FECN (Forward Explicit Congestion Notification)
- B = BECN (Backward Explicit Congestion Notification)
- D = DE (Discard Eligibility Indicator)
- C = C/R (Command / Response Field)

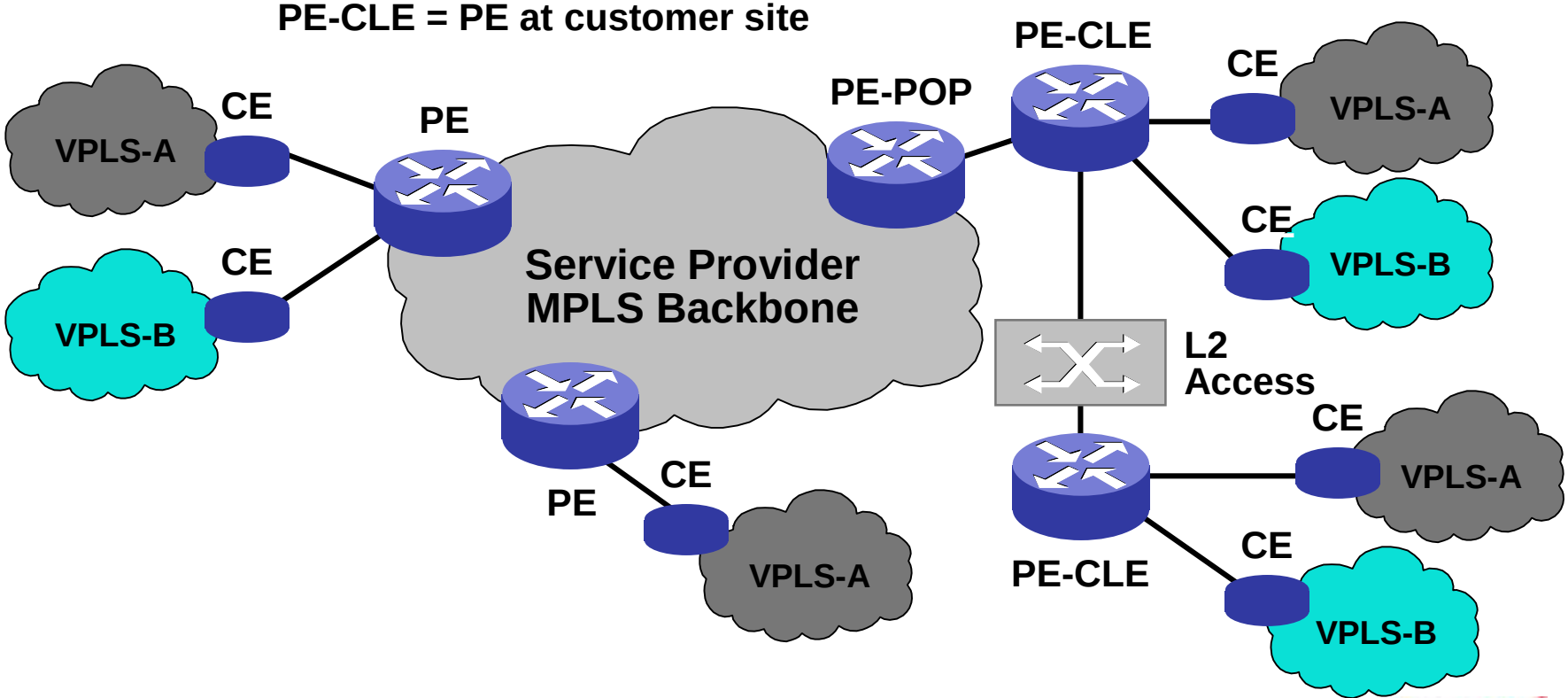
MPLS VPN Tutorial Agenda

- Layer 2 VPNs
  - IETF PWE3 and L2VPN WG update
  - Encapsulation and Label Stacking
  - Virtual Private Wire Services – VPWS
    - Pt-to-pt Ethernet, Pt-to-pt ATM, Pt-to-pt Frame Relay
  - Virtual Private LAN Services – VPLS
- Introduction to Multi-Service Interworking
  - Carrier Challenges at the Edge
  - Interworking History and Definition
  - Network and Service Interworking (FRF.5 and FRF.8.1)
  - MPLS FR Alliance Multi-Service Interworking Work Actions
- Carrier Migration Examples

MPLS Layer 2 Multipoint Services
IETF Virtual Private LAN Services - VPLS

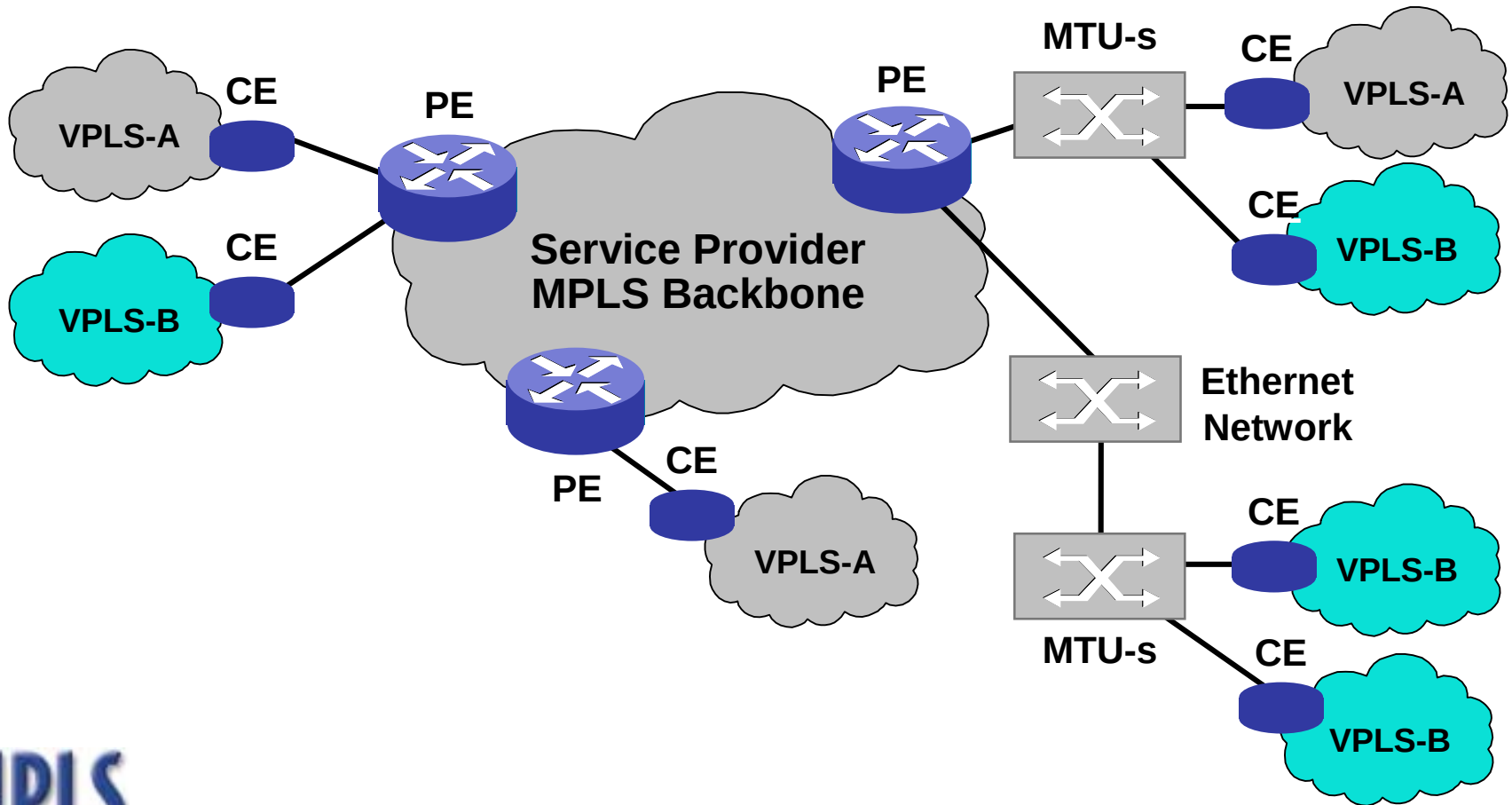
- draft-ietf-ppvpn-vpls-requirements-01.txt – 10/02
  - Describes service requirements related to emulating a Virtual Private LAN segment over an IP or MPLS network
  - VPLS topology “may” be;
    - ✓ Point-to-point, Point-to-multipoint, Any-to-any (full mesh), Mixed (partial mesh), Hierarchical
  - Service to the customers “must” retain the typical LAN any-to-any connectivity
- draft-ietf-ppvpn-l2-framework-02.txt - 01/03

MPLS VPLS
Architecture



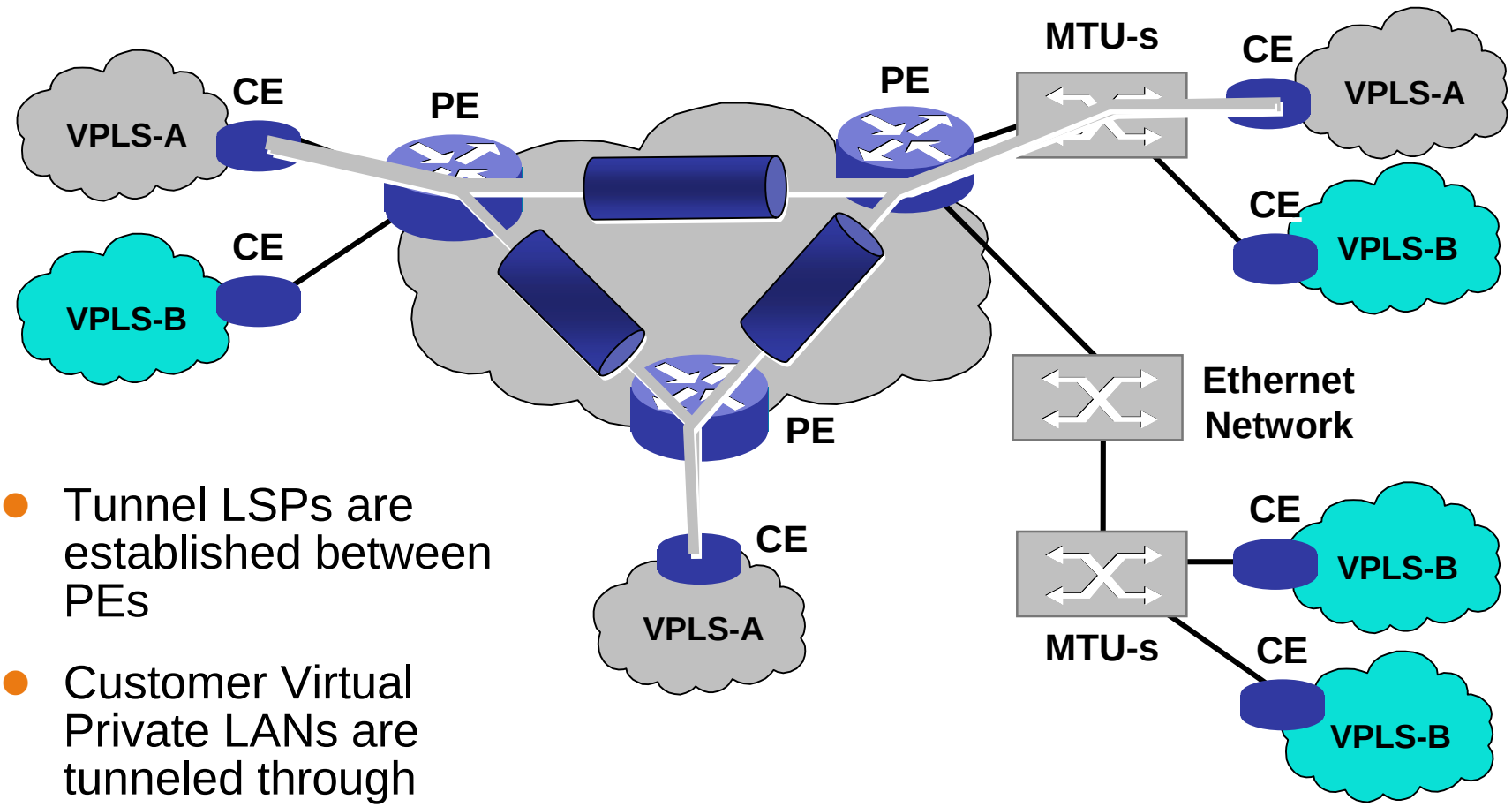
MPLS VPLS

VPLS Reference Model



MPLS VPLS

VPLS Reference Model



- Tunnel LSPs are established between PEs
- Customer Virtual Private LANs are tunneled through MPLS network

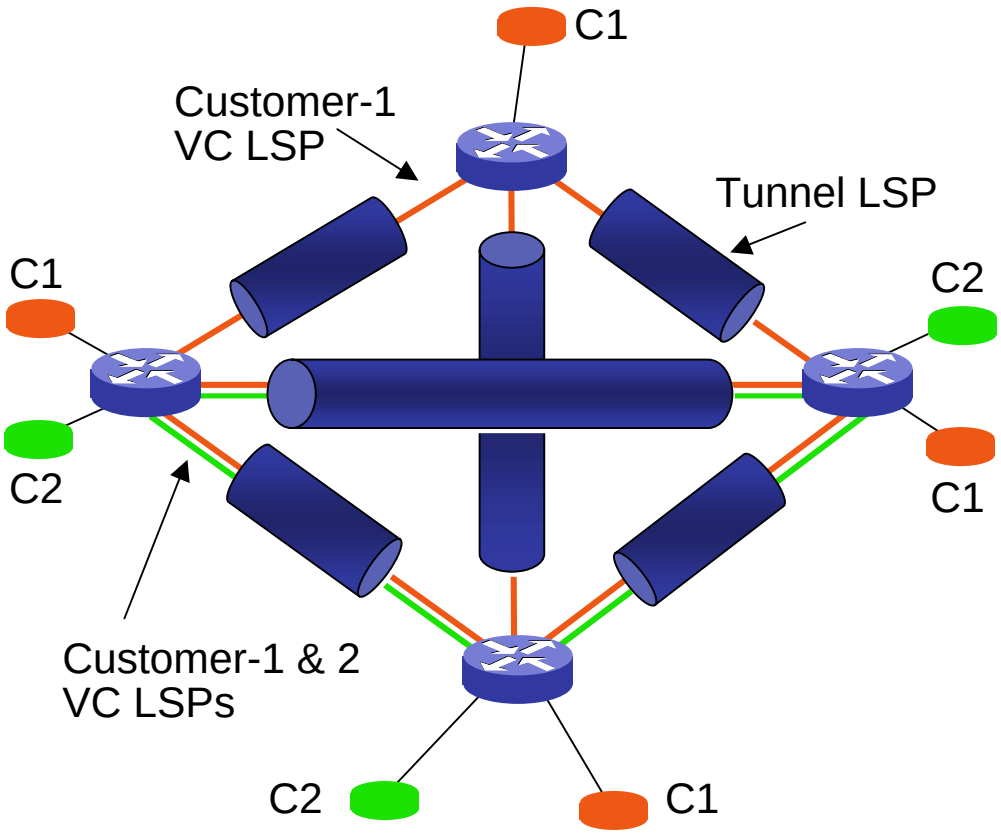
Virtual Private LAN Services

draft-ietf-l2vpn-vpls-ldp-00.txt

- Updated June 2003
- Defines an Ethernet (IEEE 802.1D) learning bridge model over MPLS Martini Ethernet circuits
- Defines the LER (PE) function for an MPLS VPLS network
- Creates a layer 2 broadcast domain for a closed group of users
- MAC address learning and aging on a per LSP basis
- Packet replication across LSPs for multicast, broadcast, and unknown unicast traffic
- Includes Hierarchical VPLS
  - ✓ formerly draft-khandekar-ppvpn-hvpls-mpls-00.txt

Virtual Private LAN Services

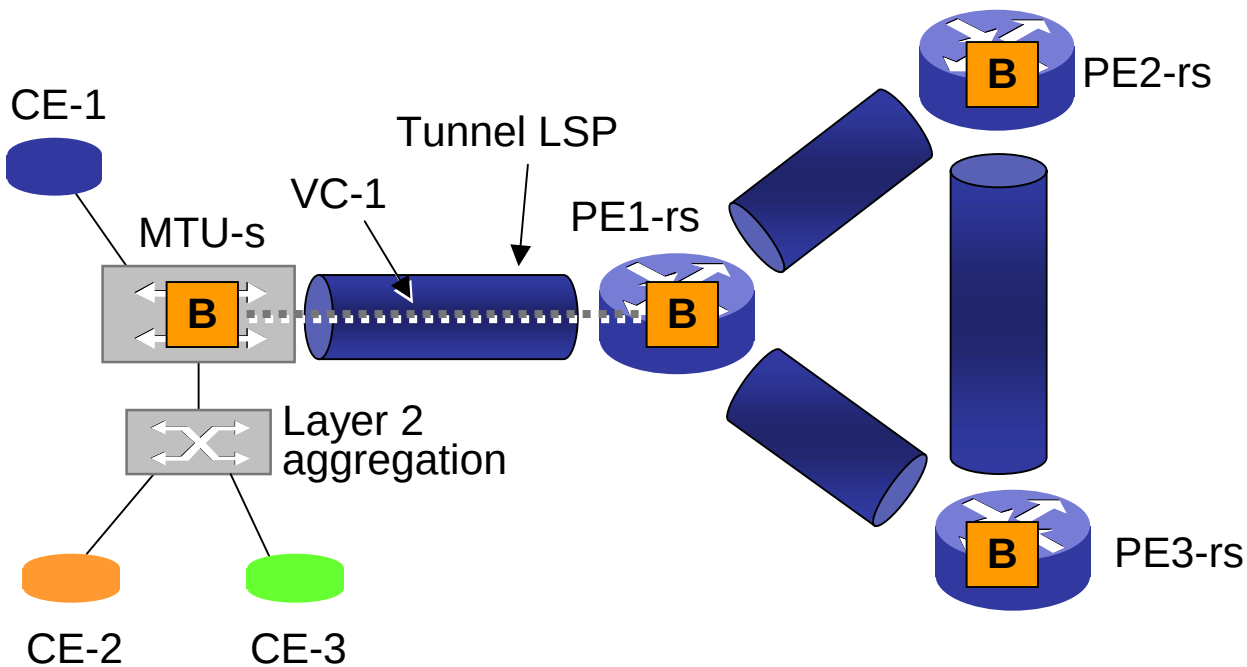
draft-ietf-l2vpn-vpls-ldp-00.txt



- Tunnel LSPs are established between PEs
- Customers designated C1 and C2 are part of two independent Virtual Private LANs
- Layer 2 VC LSPs are set up in Tunnel LSPs
- Core MPLS network acts as a LAN switch

Virtual Private LAN Services

draft-ietf-l2vpn-vpls-ldp-00.txt



- **Reduces signaling and packet replication to allow large scale deployment of VPLS**
- **Uses Martini VC / LSPs between edge MTU and VPLS aware PE devices**

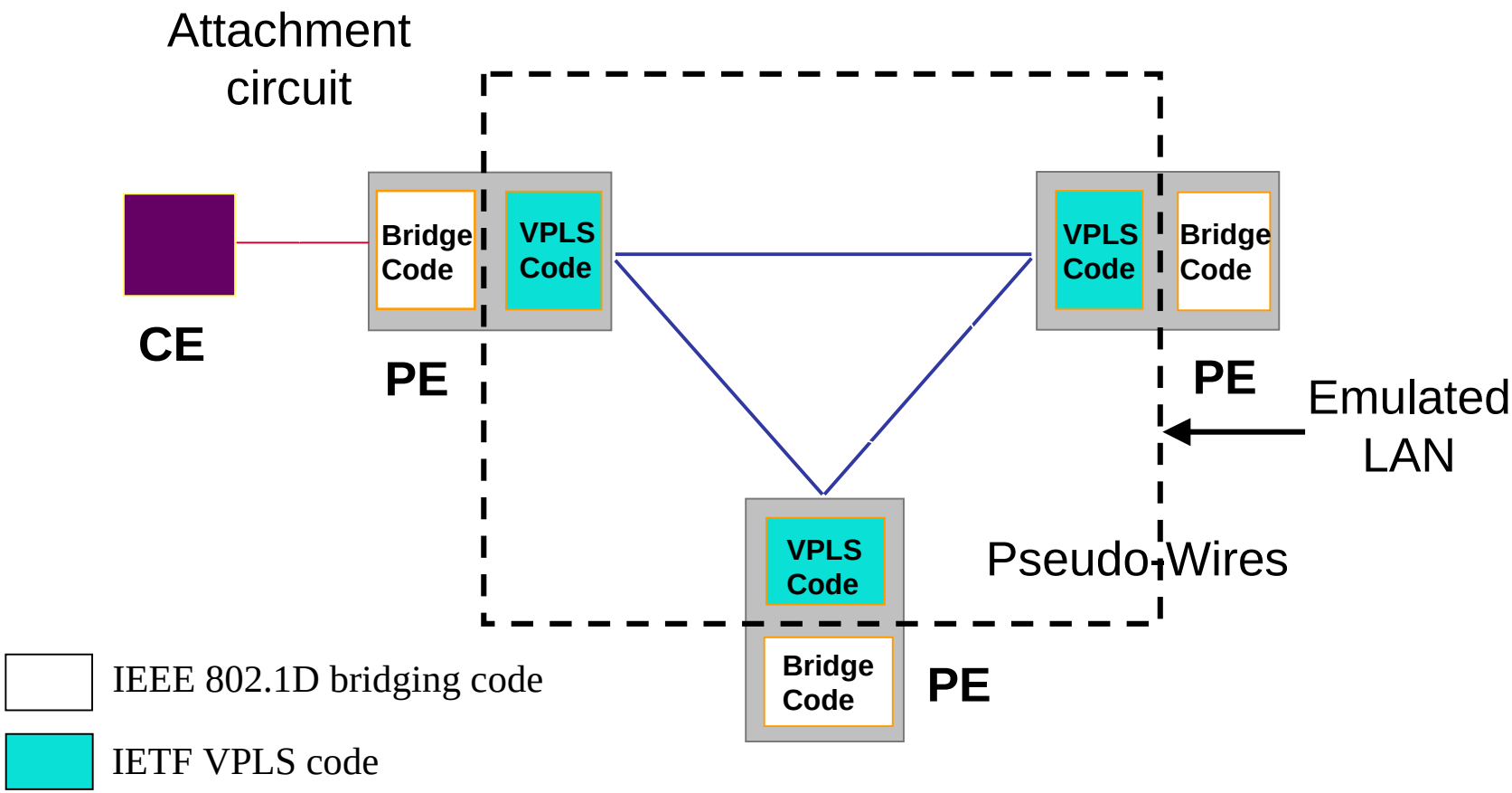
VC-1 = Single pt-to-pt Martini Tunnel LSP

MTU-s = Bridging Capable MTU (Multi Tenant Unit)

PE-rs = VPLS Capable PE

B = Virtual VPLS (Bridge) Instance

VPLS Internal PE Architecture



VPLS Code

- VPLS Forwarding
  - Learns MAC addresses per pseudo-wire (VC LSP)
  - Forwarding based on MAC addresses
  - Replicates multicast & broadcast frames
  - Floods unknown frames
  - Split-horizon for loop prevention
- VPLS Signaling
  - Establishes pseudo-wires per VPLS between relevant PEs
- VPLS Discovery (Manual, LDP, BGP, DNS)

Bridging Code

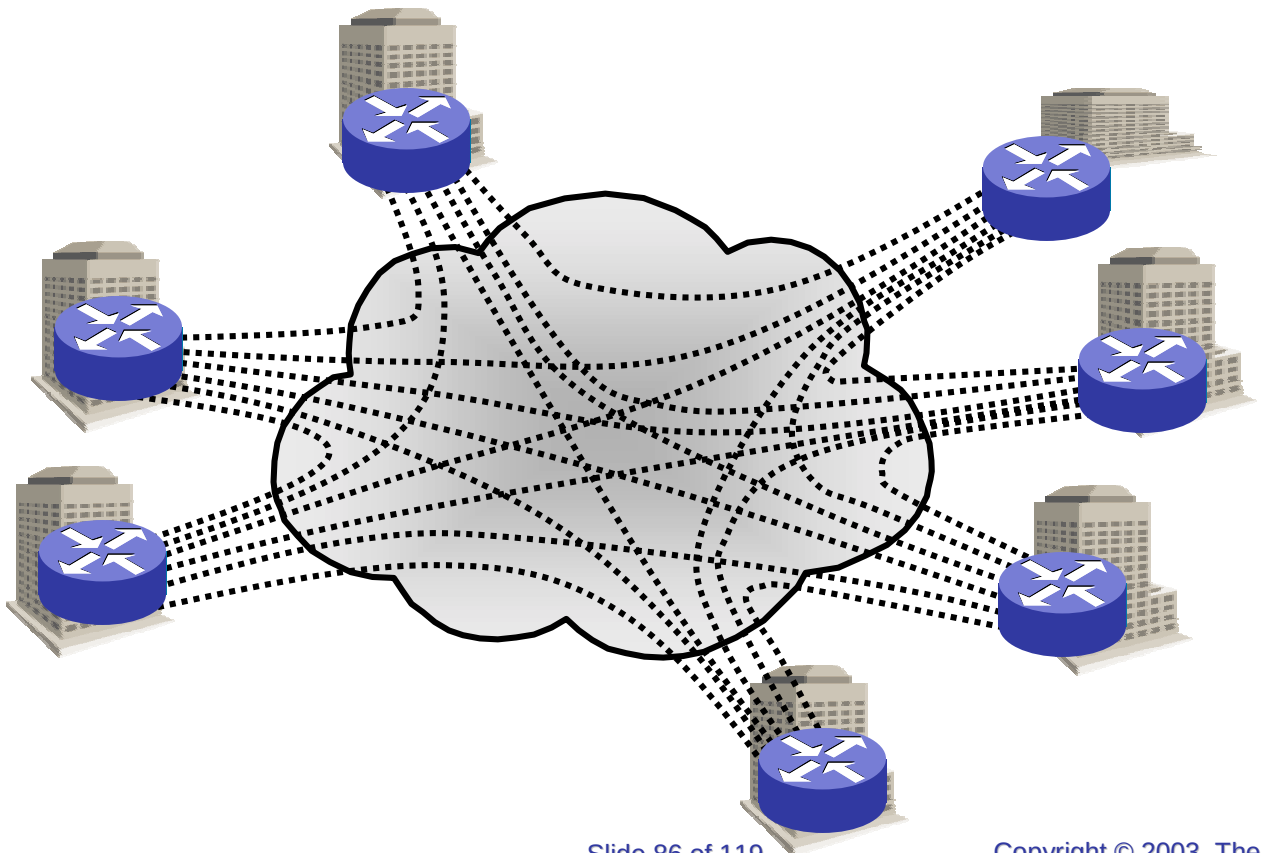
- Standard IEEE 802.1D code
  - Used to interface with customer facing ports
  - Might run STP with CEs
  - Used to interface with VPLS
  - Might run STP between PEs

VPLS Scalability
Parameters

- Number of MAC Addresses
- Number of replications
- Number of LSPs
- Number of VPLS instances
- Number of LDP peers
- Number of PEs

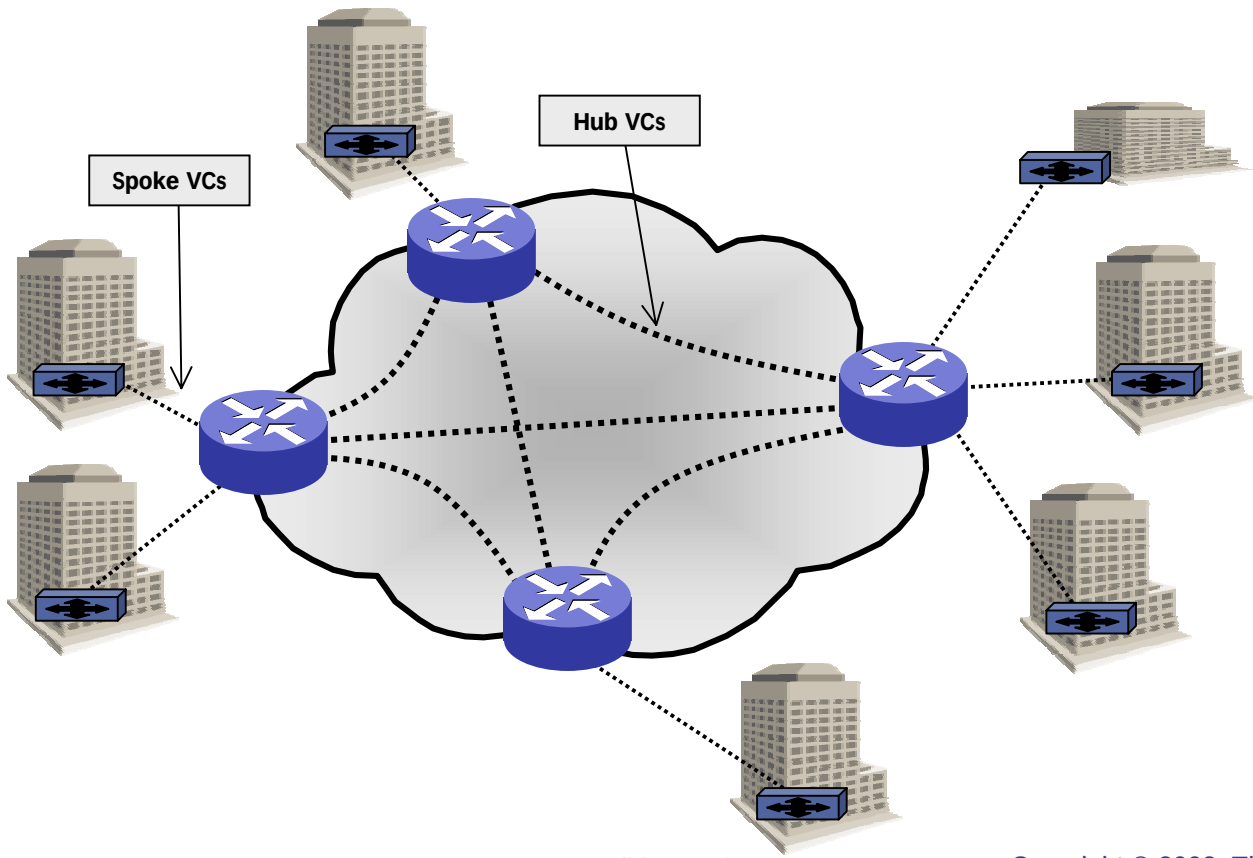
VPLS Scalability
Signaling Overhead – Flat Topology

- Architecture has a direct impact on the Signaling Overhead (control plane)



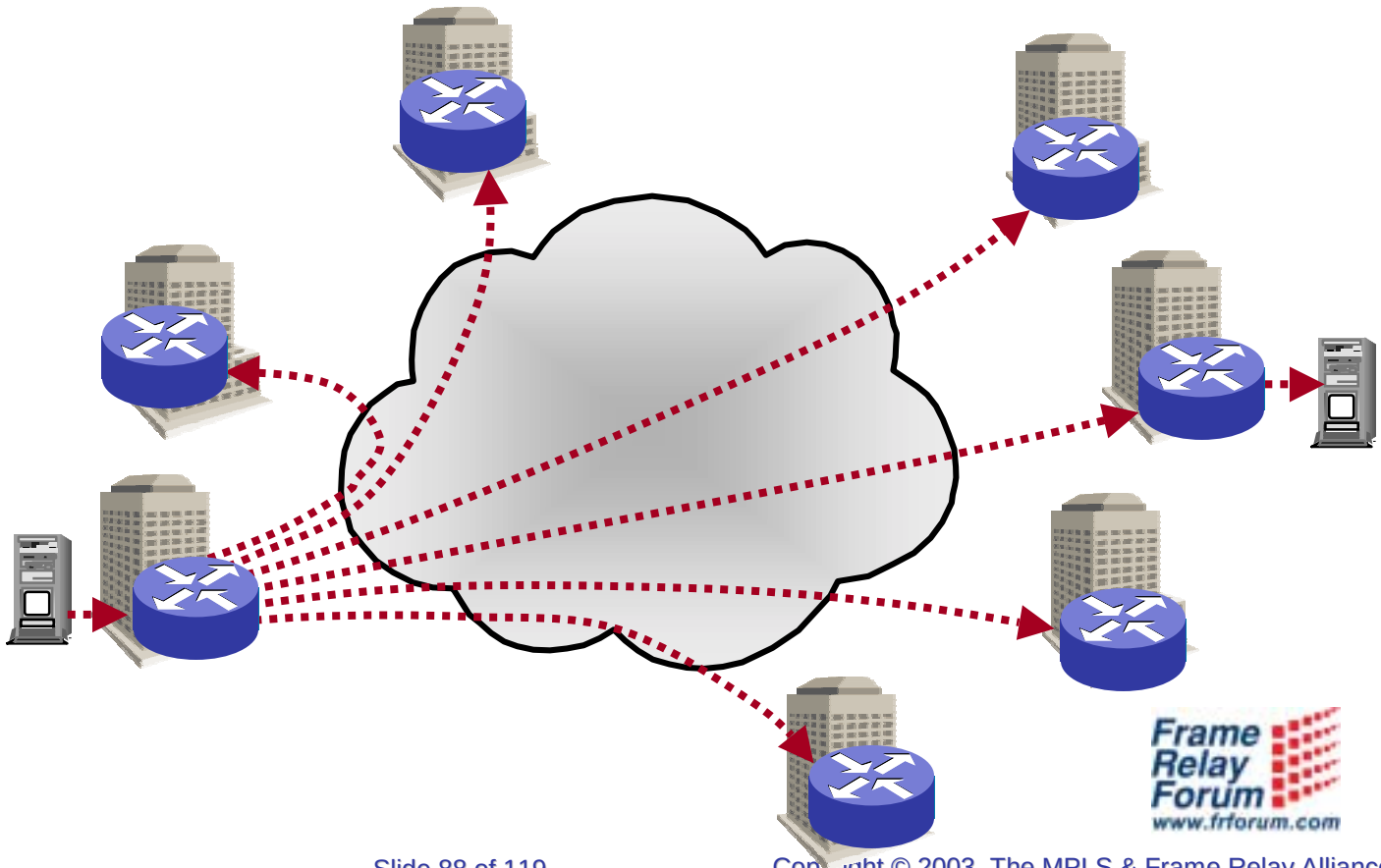
VPLS Scalability
Signaling Overhead – Hierarchical Topology

- Architecture has a direct impact on the Signaling Overhead (control plane)



VPLS Scalability
Replication Overhead – Flat Topology

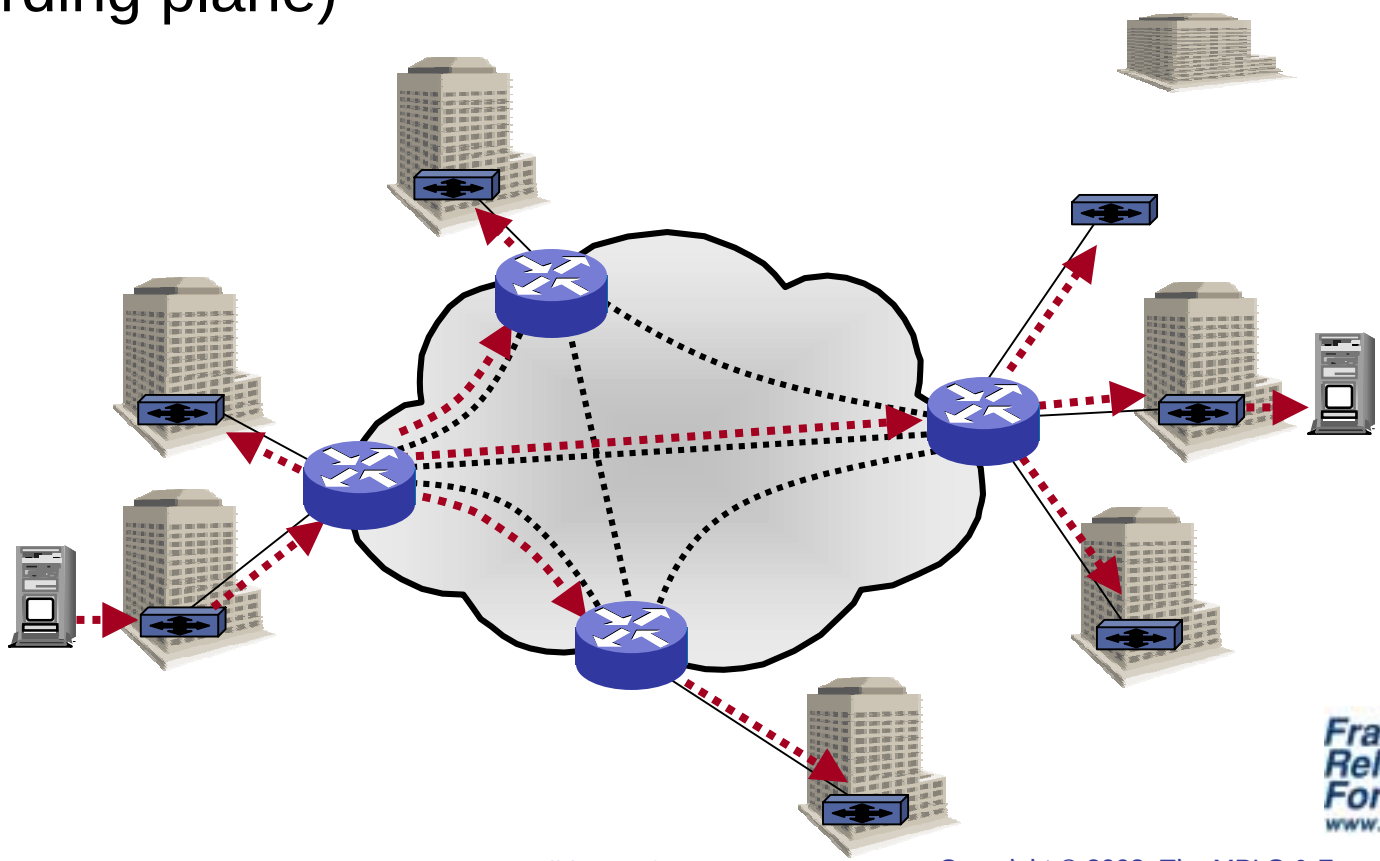
- Architecture has a direct impact on Replication Overhead (forwarding plane)



VPLS Scalability

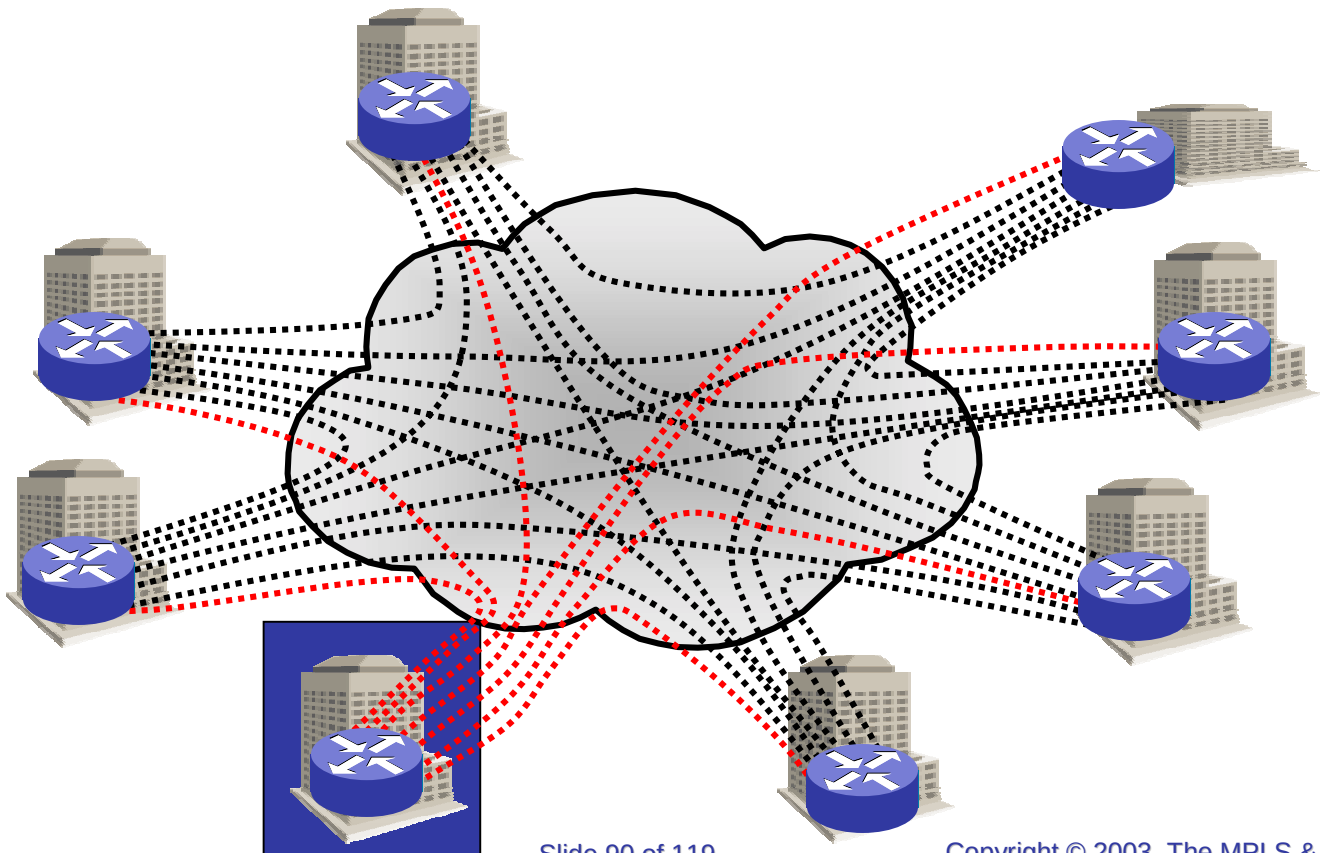
Replication Overhead – Hierarchical Topology

- Architecture has a direct impact on Replication Overhead (forwarding plane)



VPLS Scalability
Adding a New Site – Flat Topology

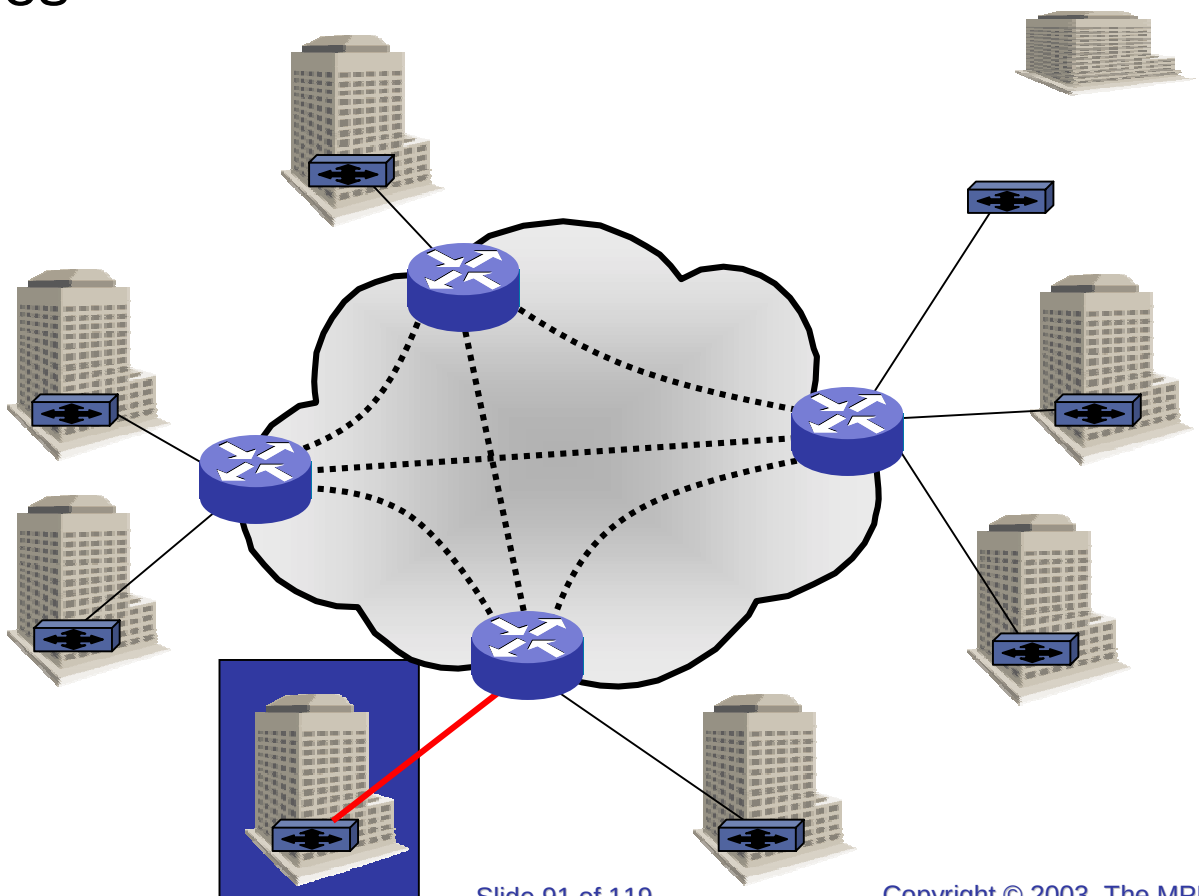
- Architecture affects Provisioning & Signaling between all nodes



VPLS Scalability

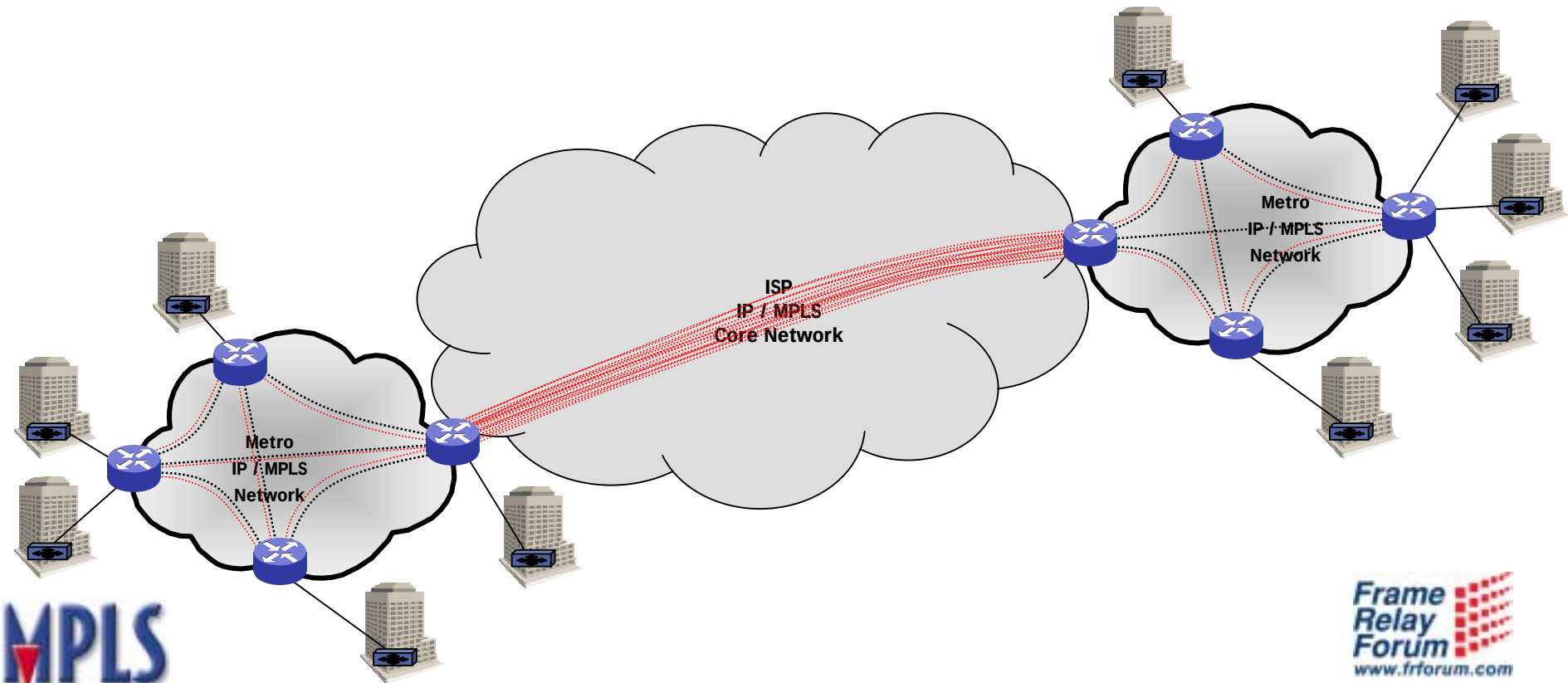
Adding a New Site – Hierarchical Topology

- Architecture affects Provisioning & Signaling between all nodes



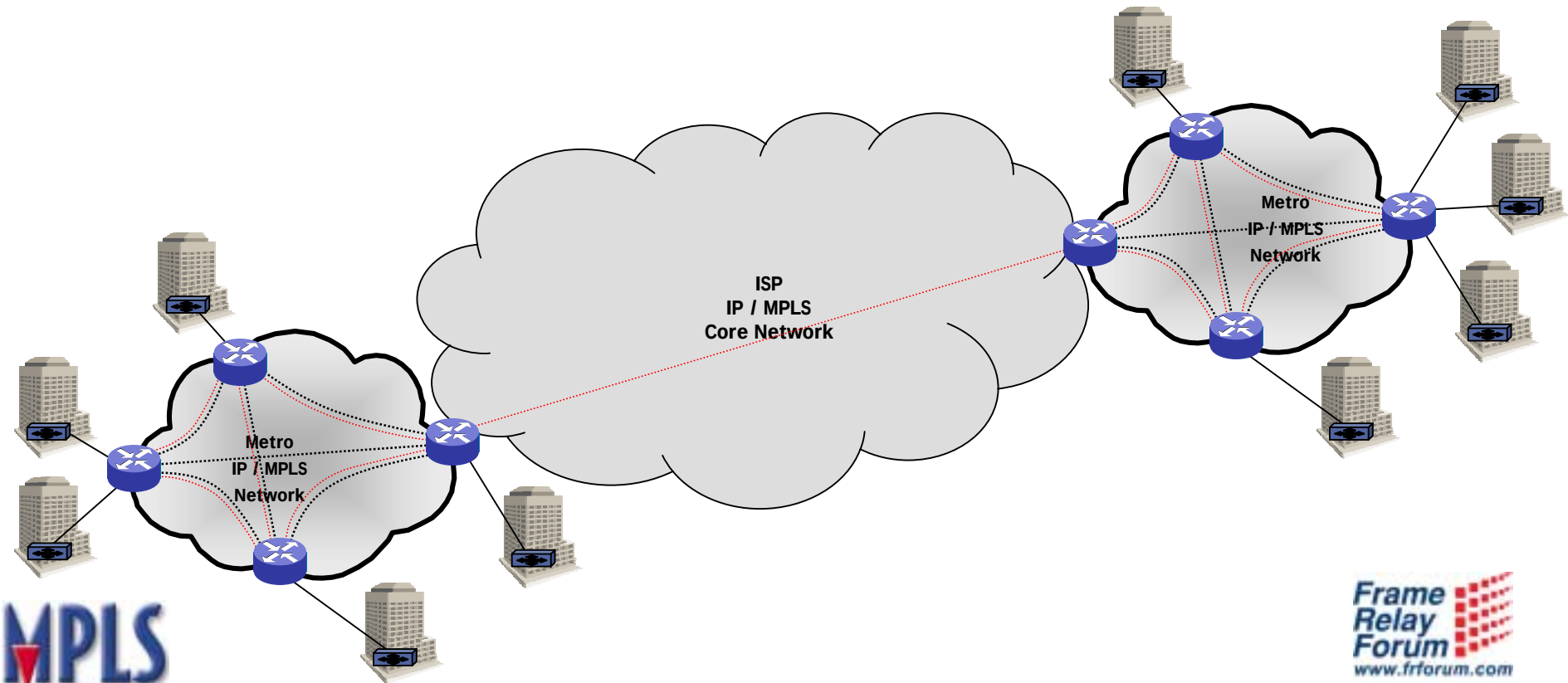
VPLS Scalability
Inter-Metro Service

- Architecture has a direct impact on ability to offer Inter-Metro Service



VPLS Scalability
Inter-Metro Service

- Architecture has a direct impact on ability to offer Inter-Metro Service



VPLS Scalability
FIB Size

- VPLS FIB size depends on the type of Service Offering:
  - Multi-protocol Inter-connect service
    - ✓ Mimics the DSL Tariff Model
    - ✓ Customers are charged per site per block of MAC addresses
  - Router Inter-connect
    - ✓ One MAC address per site
- Same Network Design principles apply for
  - MAC FIB Size of VPLS Service and,
  - Route Table Size of VPRN Service

MPLS Layer 2 Multipoint Services
Other VPLS Drafts

- draft-ietf-l2vpn-vpls-bgp-00.txt 05/03
  - Describes the use of BGP for discovery and signaling
- draft-rosen-ppvpn-l2-signaling-02.txt
  - Describes and compares signaling issues
- Draft-shah-ppvpn-ipls-02.txt
  - IP only LAN service
- draft-radoaca-ppvpn-gvpls-02.txt 06/03
  - GVPLS/LPE - Generalized VPLS Solution based on LPE Framework
- draft-stokes-vkompella-ppvpn-hvpls-oam-02.txt 06/03
  - Testing Hierarchical Virtual Private LAN Services

VPLS Conclusion

- VPLS standardization
  - PWE3 encapsulation and control
  - L2VPN VPLS draft convergence and momentum
  - Signaling and Discovery options
  - IEEE 802.1ad Provider Bridge WG actions
- Next IETF meeting Minneapolis MN 11/9 – 11/14 2003

MPLS VPNs Summary

- Layer 2 versus Layer 3
  - Apples and Oranges
- Layer 3 MPLS VPNs
  - Deployed and at RFC stage
- Layer 2 MPLS VPNs
  - Lot's of Interest from Carriers and Vendors
  - Many new drafts – lots of consolidation
  - We are in "concept" stage
  - Solutions available 2003

MPLS VPN Tutorial Agenda

- Layer 2 VPNs
  - IETF PWE3 and L2VPN WG update
  - Encapsulation and Label Stacking
  - Virtual Private Wire Services – VPWS
    - Pt-to-pt Ethernet, Pt-to-pt ATM, Pt-to-pt Frame Relay
  - Virtual Private LAN Services – VPLS
- Introduction to Multi-Service Interworking
  - Carrier Challenges at the Edge
  - Interworking History and Definition
  - Network and Service Interworking (FRF.5 and FRF.8.1)
  - MPLS FR Alliance Multi-Service Interworking Work Actions
- Carrier Migration Examples

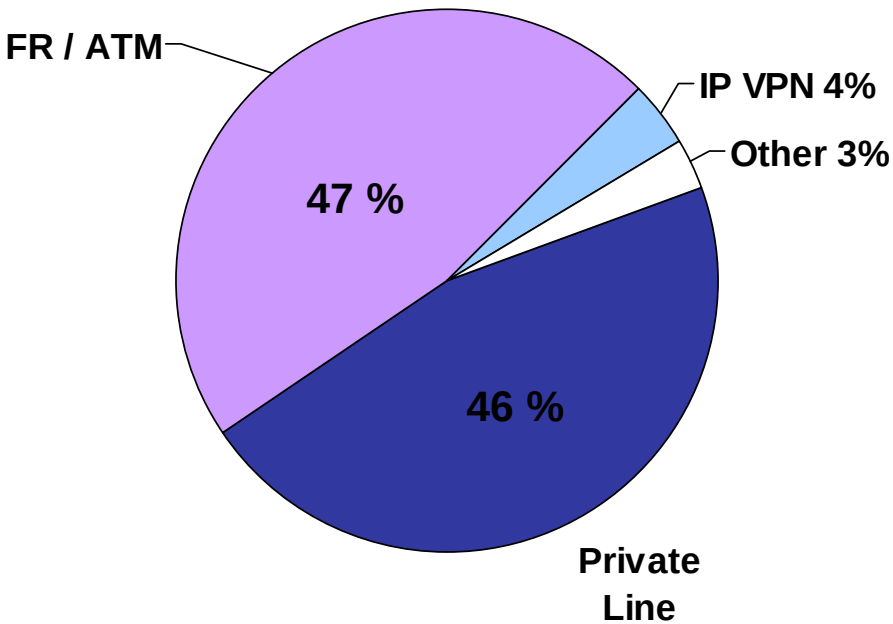
Why Interwork?

- Carriers want a common edge infrastructure to support and “Interwork” with legacy and new services
- Carriers want to support all legacy transports technologies and services
- Carriers are planning to converge on an IP / MPLS core
- Carriers want to seamlessly introduce Metro Ethernet services and IP VPNs

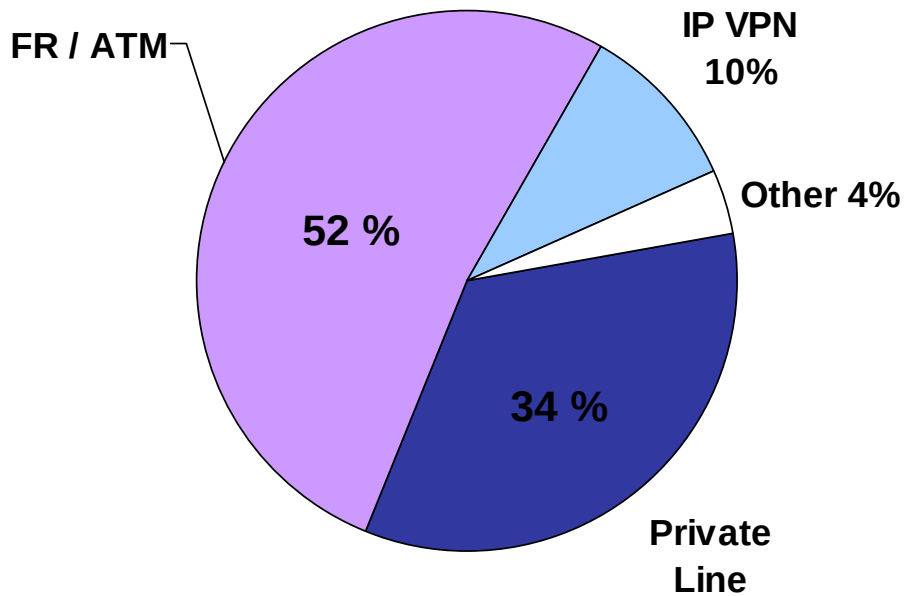
Network Services Market

Broadband Data Services Growth Projections

2003 Total = $26B



2007 Total = $37B



- **Private Lines, FR, and ATM comprise 93 % of the $26B US broadband business services market now, and 86 % of the projected $37B total in 2007**
- **Other above includes Ethernet, X.25, etc**

Source: Vertical Systems Group July 2003

Interworking

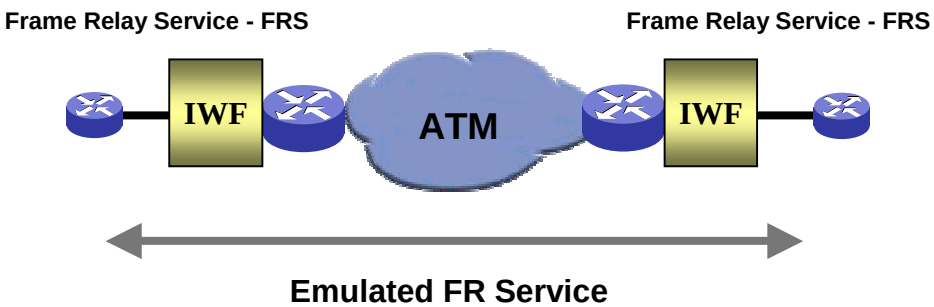
History

- The Frame Relay Forum defined the Network Interworking function between Frame Relay and ATM in the FRF.5 document finalized in1994.
- The Frame Relay Forum defined the Service interworking function between Frame Relay and ATM in the FRF.8.1 document finalized in 2000.
- Why define FR and ATM interworking?
  - ATM cores with FR access services deployed
  - ATM and Frame Relay circuits are point-to-point
  - Both data links have services that are somewhat similar in nature even though the signaling is different

InterWorking Function - IWF

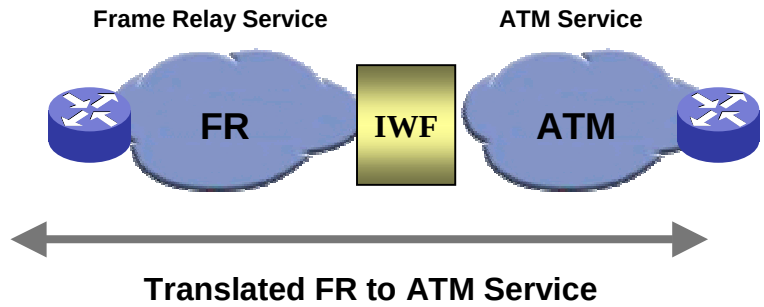
Network vs Service IWF

Network Interworking



- Network Interworking is used when one protocol is "tunneled" across another "intermediary" network / protocol
- The Network Interworking function "terminates" and "encapsulates" the protocol over a Pt-to-Pt connection

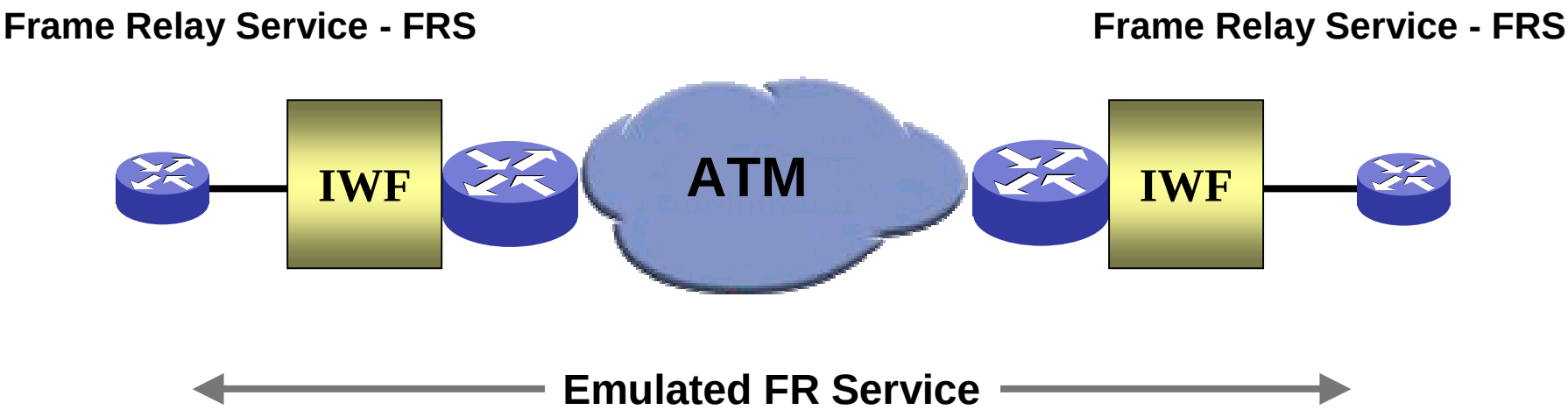
Service Interworking



- Service Interworking is required to "translate" one protocol to another protocol – used between two unlike protocols
- The Service Interworking function "translates" the control protocol information transparently by an interworking function (IWF)

Network Interworking FRF.5

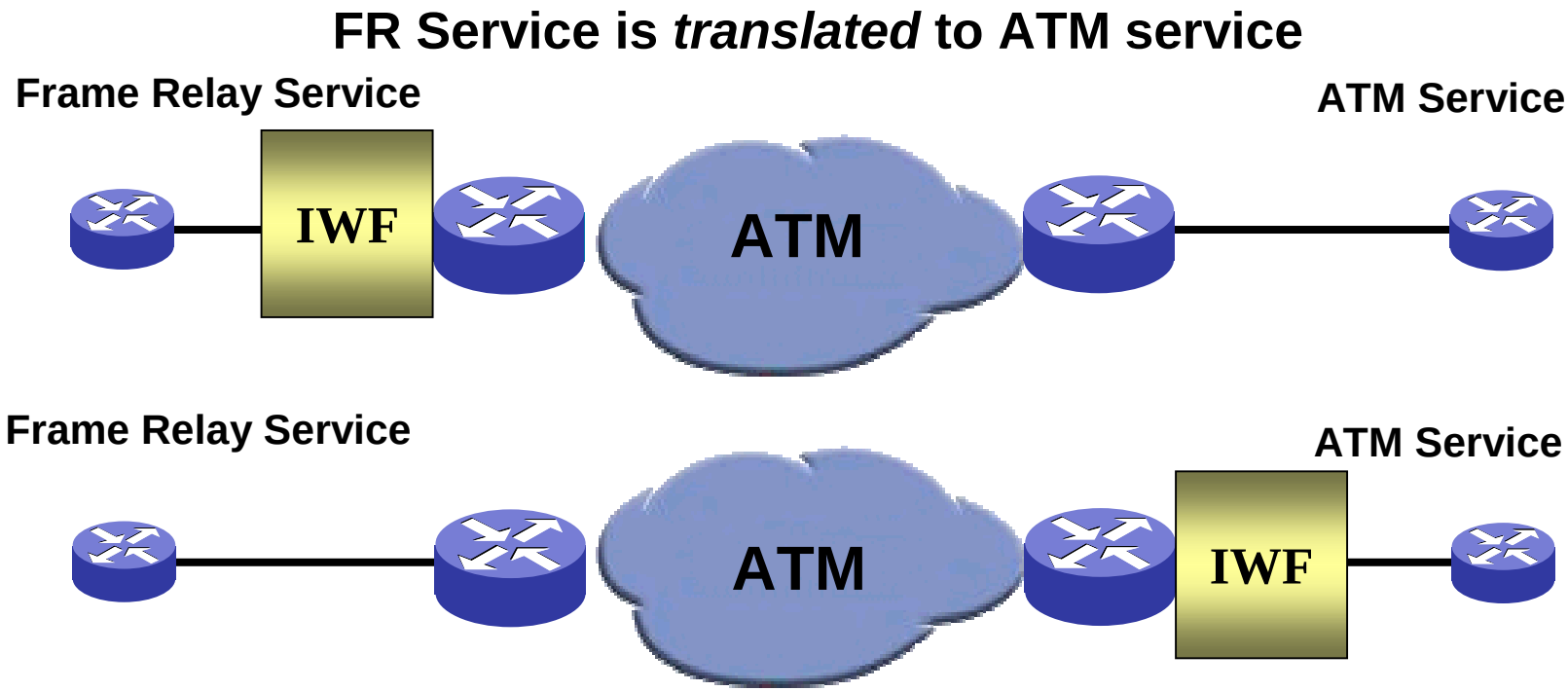
Reference Model



- *Network* Interworking *encapsulates* the L2 Service
- FRS is *encapsulated* and sent across ATM network
- Service at the end points *have to be* the same

Service Interworking FRF.8.1

Reference Model



- *Service* Interworking *translates* the L2 Service
- FR service is *translated* into ATM service
- Services at the end points *are not* the same

Why not continue with ATM IW?

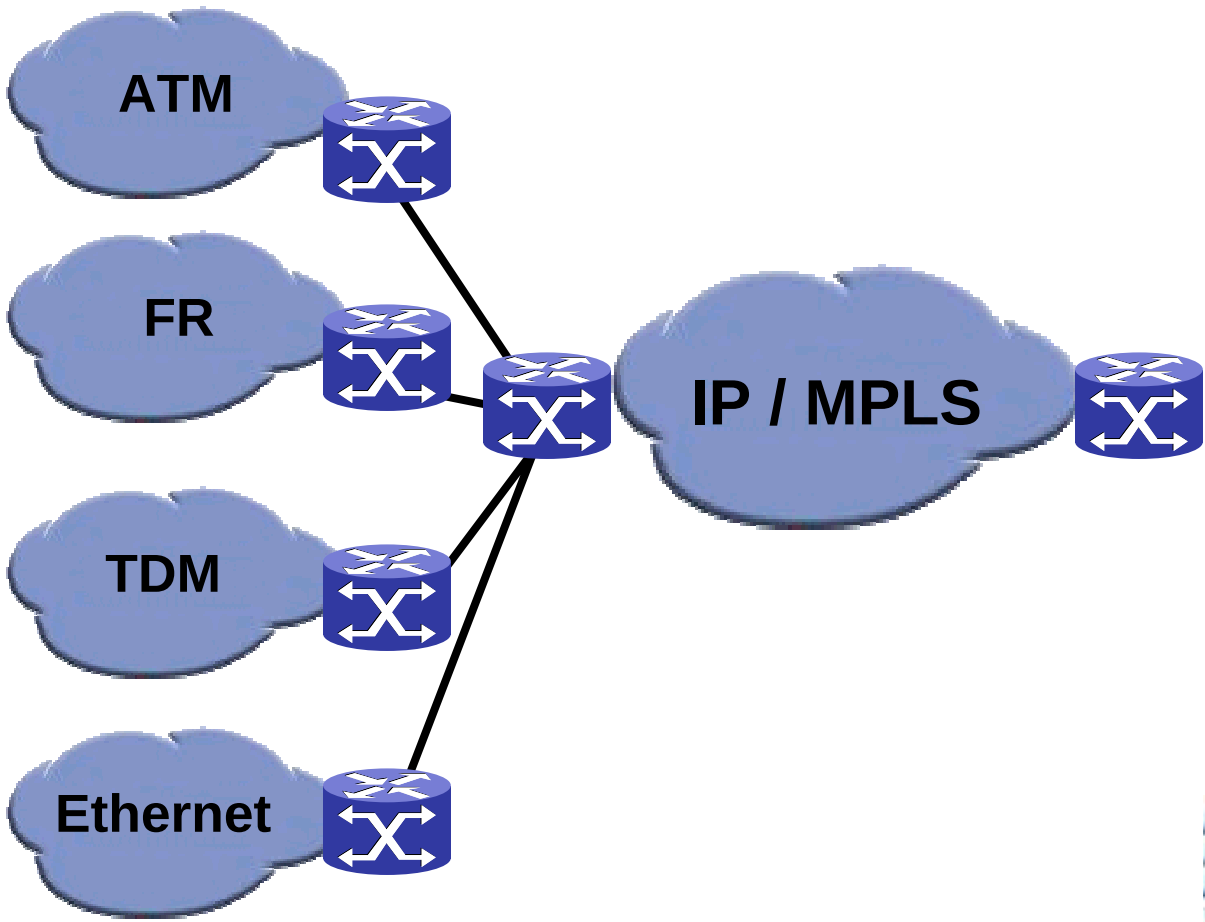
- ATM is optimized for voice transport – cell overhead etc
- Cells are simply fixed length packets and can be carried unchanged across an MPLS network
- Packets are not cells and must be adapted to be carried across ATM
- MPLS is optimized for packet transport
- Carriers want to converge on IP/MPLS cores supporting both new and legacy services

Why Migrate to MPLS?

- MPLS allows service providers to converge onto a single infrastructure while offering existing services
- MPLS enables new service offerings and simplifies service provisioning
- MPLS supports rapid growth in IP applications and services
- MPLS allows the integration of services management into a common OSS strategy
- MPLS supports the integration of packet technologies and optical cores

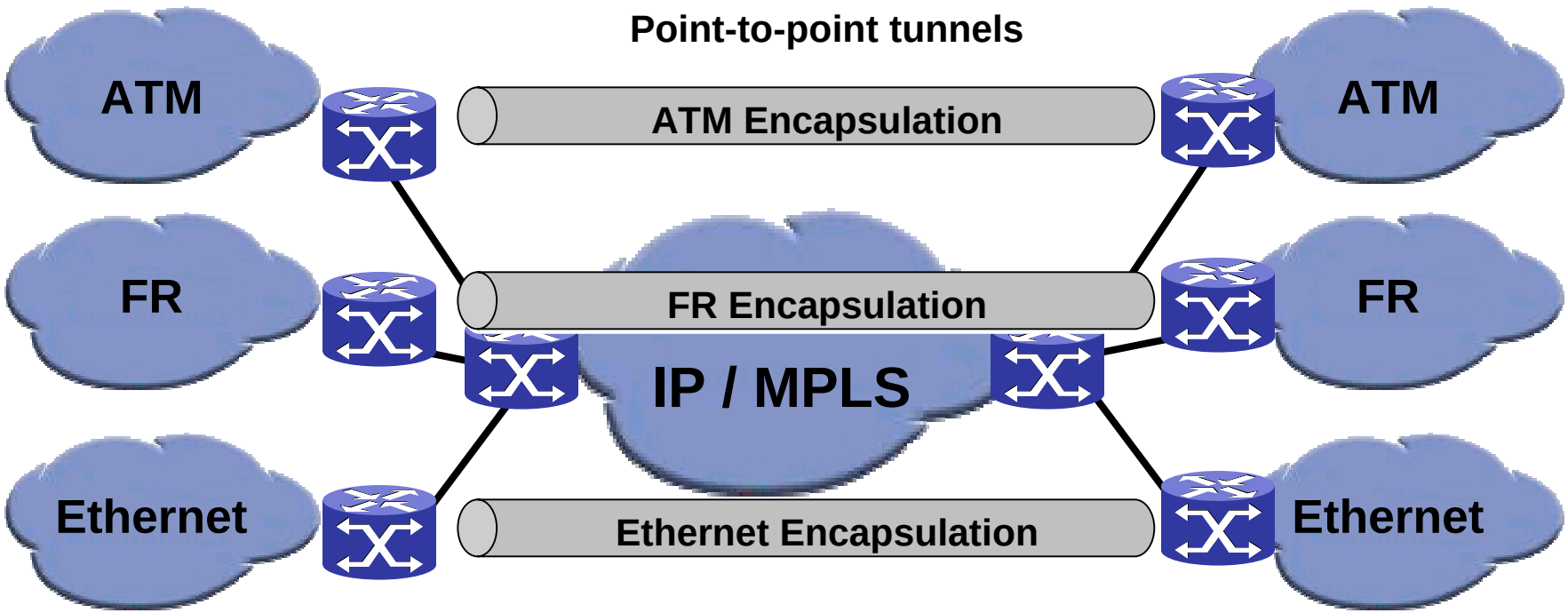
MPLS Multi-Service Interworking

MPLS Connects Services at the Edge



MPLS Network Interworking

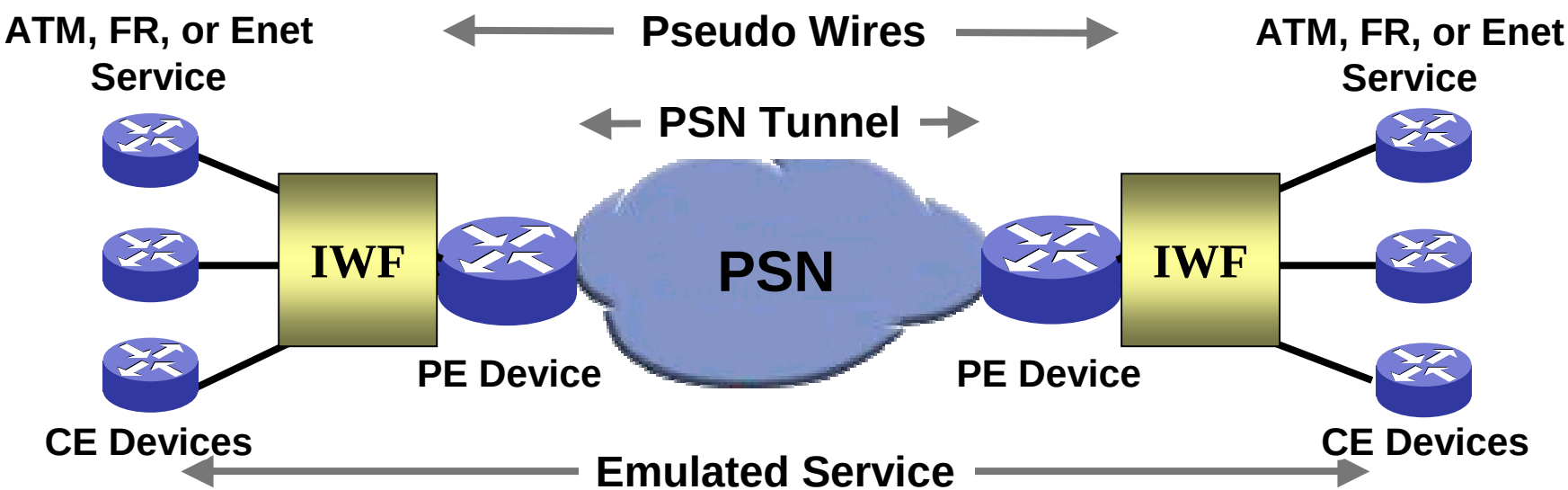
IETF PWE3 Pt-to-Pt Encapsulation



Service has to be pt-to-pt between like services: ATM to ATM, FR to FR, Enet to Enet, etc

MPLS Multi-Service Interworking

Reference Model



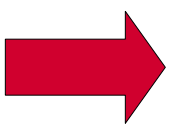
PE = Provider Edge
CE = Customer Edge
PSN = Packet Switched Network
IWF = InterWorking Function
Multi-Service: Services equal to FR, ATM, Ethernet

Standards and Alliance Work

- IETF RFCs
  - RFC 2684 for ATM (previously 1483) and 2427 for FR (previously 1490) define an encapsulation for carrying layer 2 or layer 3 PDUs over ATM and FR respectively
- MPLS FR Alliance
  - Scope and Requirements Baseline Text
    - ✓ Mpls2003.043.00 July 2003
    - ✓ Mpls2003.114.00 September 2003
- Metro Ethernet Forum
  - Ethernet Internetworking Function (E-IWF) draft Shah

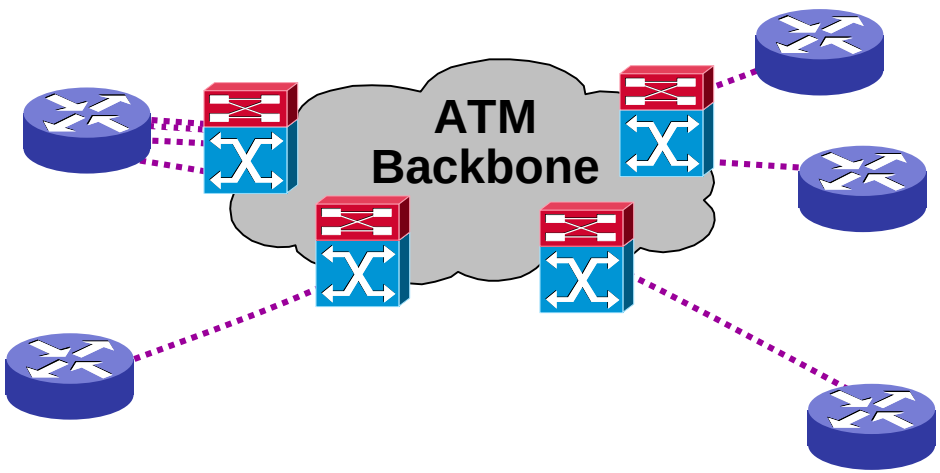
MPLS VPN Tutorial Agenda

- Layer 2 VPNs
  - IETF PWE3 and L2VPN WG update
  - Encapsulation and Label Stacking
  - Virtual Private Wire Services – VPWS
    - Pt-to-pt Ethernet, Pt-to-pt ATM, Pt-to-pt Frame Relay
  - Virtual Private LAN Services – VPLS
- Introduction to Multi-Service Interworking
  - Carrier Challenges at the Edge
  - Interworking History and Definition
  - Network and Service Interworking (FRF.5 and FRF.8.1)
  - MPLS FR Alliance Multi-Service Interworking Work Actions
- Carrier Migration Examples



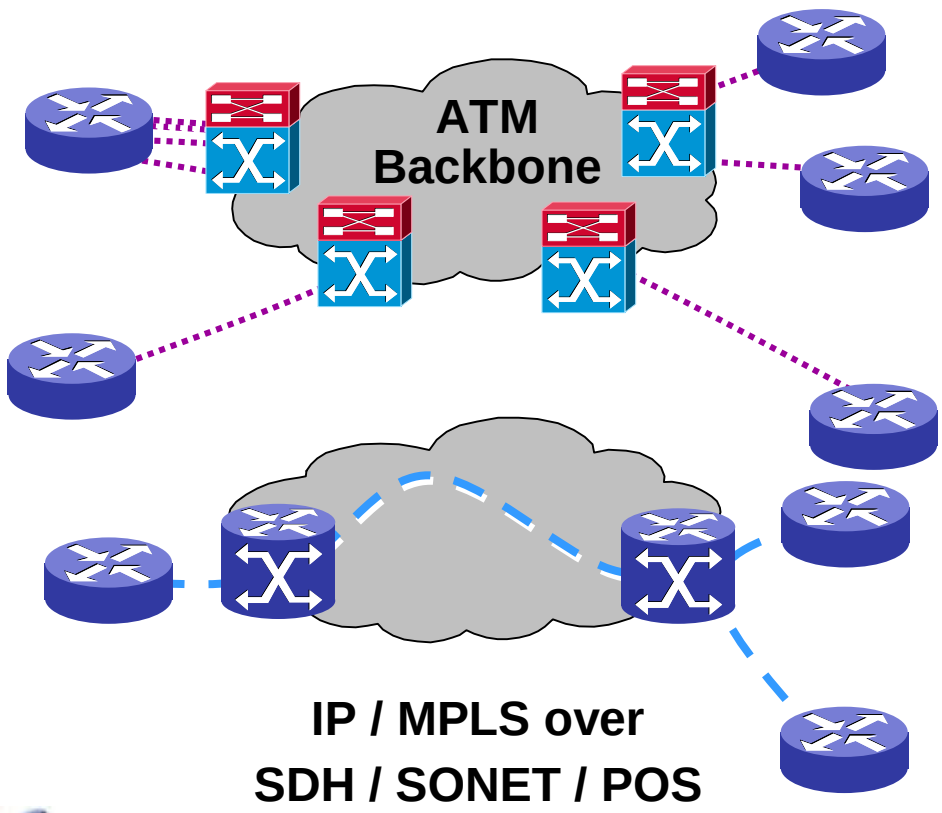
Frame Relay Forum
www.frforum.com

Existing Frame Relay / ATM Network



- **Typical Scenario**
  - Multiple networks
  - Multiple services
    - Voice, Video, Data
  - FR, ATM, DSL, IP, etc

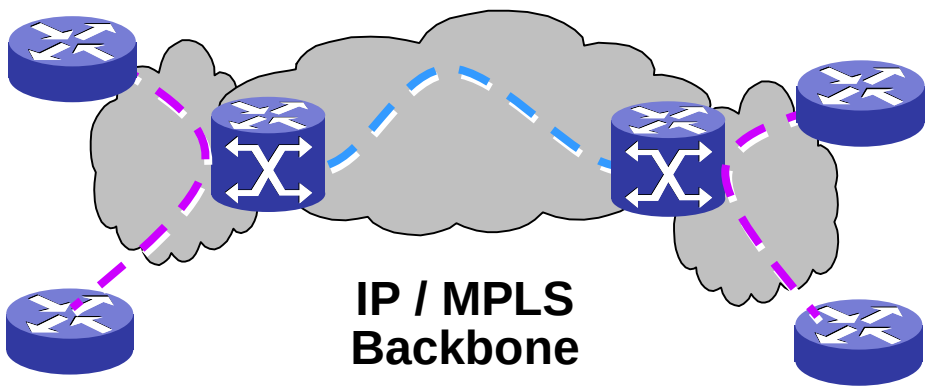
Existing IP / MPLS Network



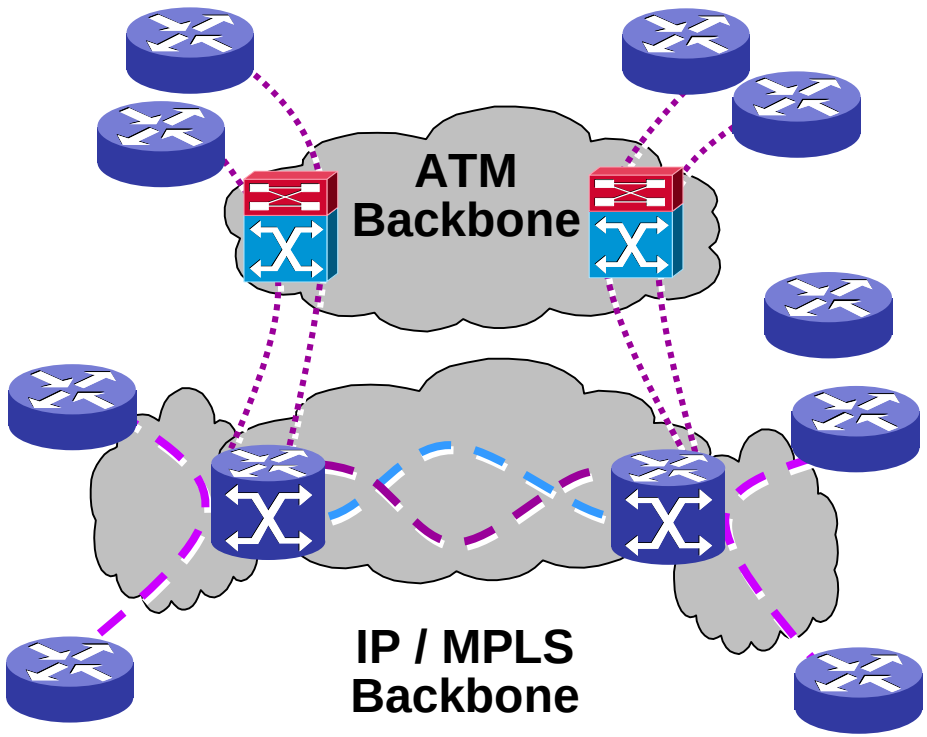
- **Typical Scenario**
  - Multiple networks
  - Multiple services
    - Voice, Video, Data
  - FR, ATM, DSL, IP, etc
- **IP / MPLS network**
  - SDH/SONET transport
  - Separate from ATM
  - IP Routed Network
  - MPLS deployed ?
  - RFC 2547bis IP VPNs ?

Offer Ethernet VPLS

- **Layer 2 VPLS**
  - PWE3 Encapsulation
  - Layer 2 Ethernet VPLS

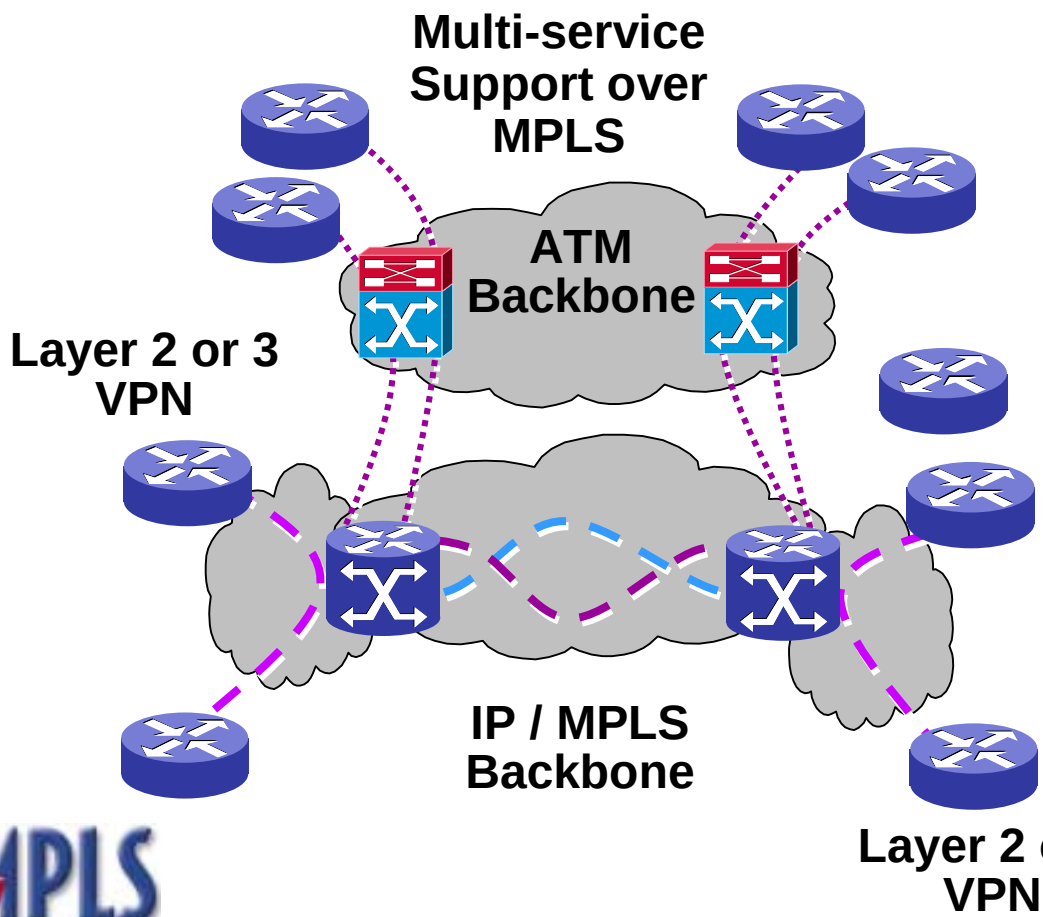


Frame Relay / ATM Migration



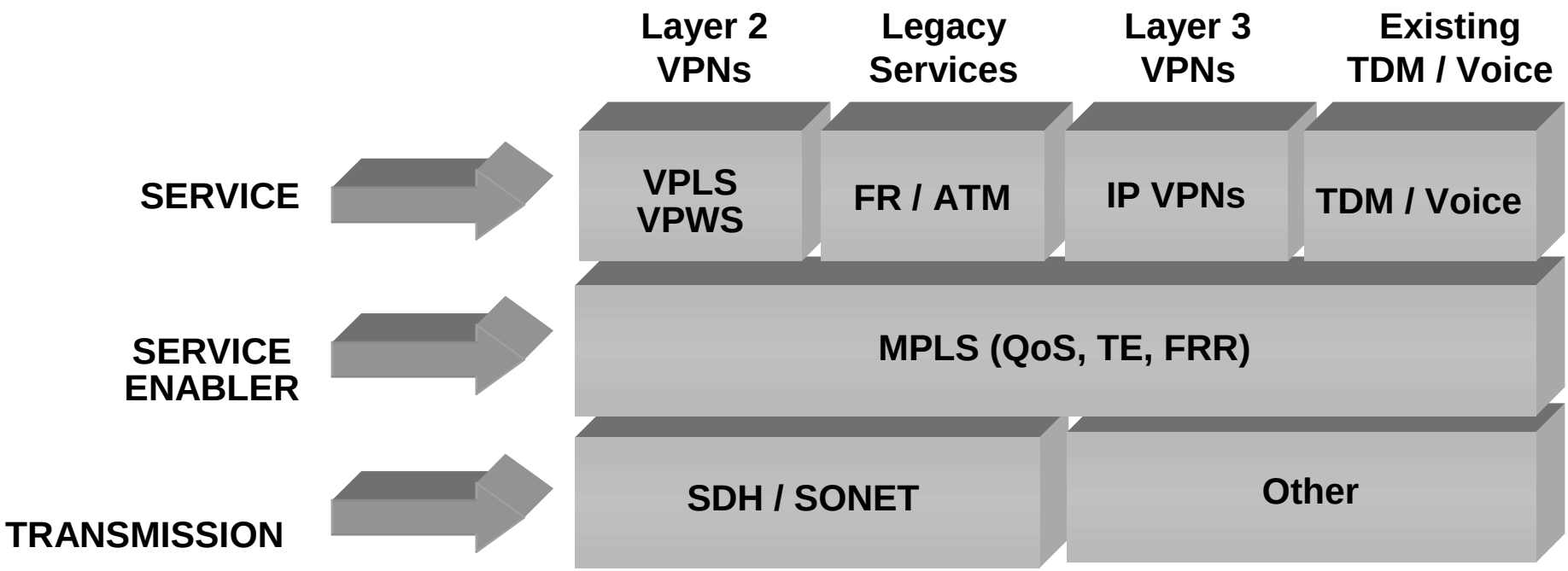
- **Layer 2 VPWS**
  - Add pt-to-pt ATM encapsulation
  - Add pt-to-pt FR encapsulation

Complete MPLS VPN Solution



- **MPLS VPNs**
  - PWE3 Encapsulation
  - Layer 2 Ethernet VPLS
  - ATM legacy migration
  - FR legacy migration
  - Layer 3 2547bis VPNs
  - Combined multiple services
  - New Multi-Service Interworking

MPLS as a Service Enabler



VPLS = Virtual Private LAN Services

VPWS = Virtual Private Wire Services

L3 IP VPN = RFC2547-bis

For More Information. . . .

- http://mplsforum.com
- http://www.mplsforum.org/board/
- http://www.frforum.com
- http://www.ietf.org
- http://www.itu.int
- http://www.atmforum.com
- http://www.mplsrc.com

MPLS based Virtual Private Network Services

Thank You

gleonard@riverstonenet.com

http://www.mplsforum.com