WELCOME

APRICOT 2012

MPLS WORKSHOP – L2VPN

Alastair Johnson alastair.johnson@alcatel-lucent.com

February 2012

MPLS WORKSHOP
L2VPN

1. Introduction to L2VPN
   a. Background to VPNs
   b. Why L2VPNs
   c. Types of L2VPNs
2. Technology introduction
3. L2VPN – Ethernet Pseudowire (VLL, EPIPE)
4. L2VPN – Ethernet Virtual Private LAN Service (VPLS)
5. Advanced topics
6. Summary

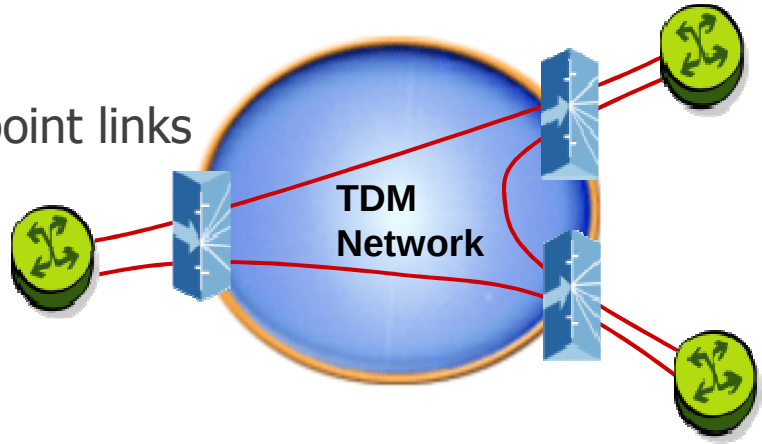
MPLS WORKSHOP

INTRODUCTION TO L2VPN

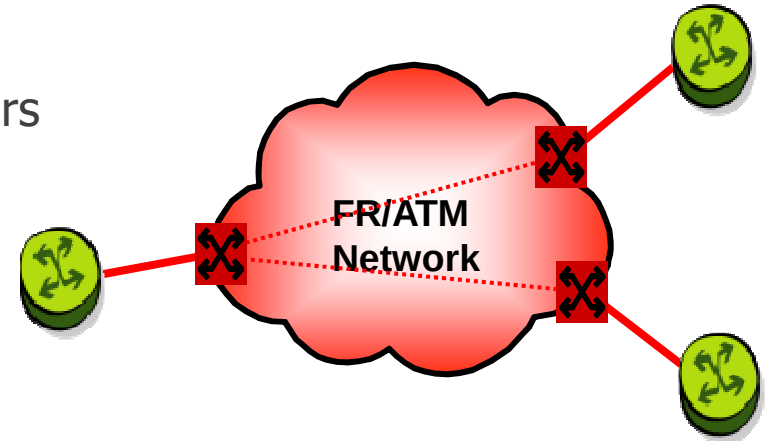
BACKGROUND TO VPNs

EXISTING SERVICE PORTFOLIO

- **Leased lines**
  - Customers subscribe to 'dedicated' point-to-point links
  - Cost prohibitive for customers

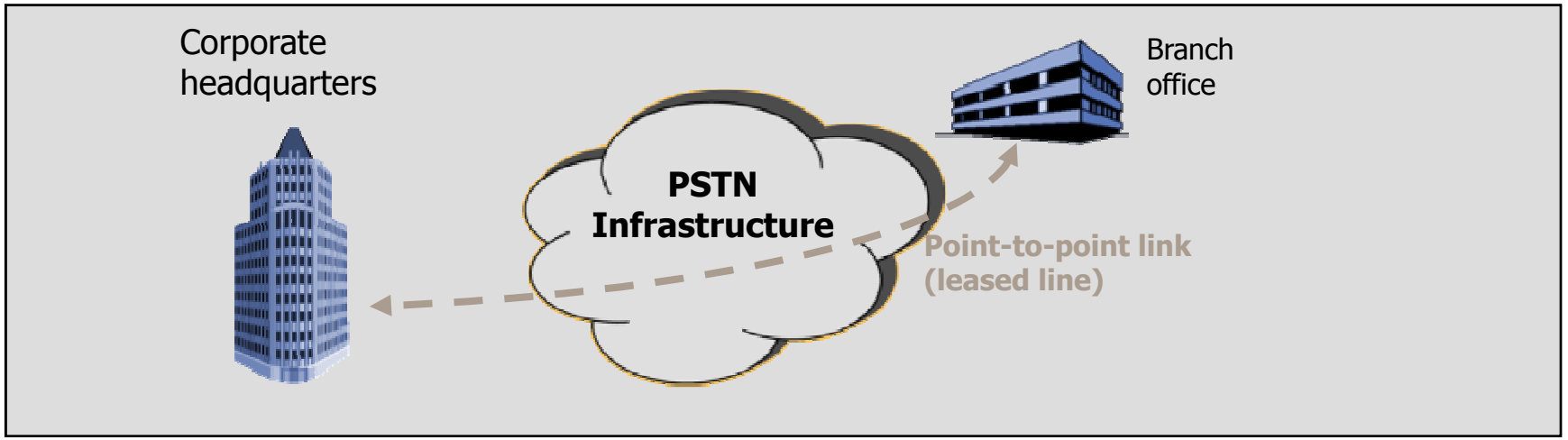


- **Frame Relay and ATM services**
  - Customers subscribe to point-to-point links to construct Hub and Spoke, Mesh or a Hybrid topology
  - Offered over a shared infrastructure that offers multiplexing advantages
  - Cheaper alternative to Leased line



THE ORIGIN OF PRIVATE NETWORKS

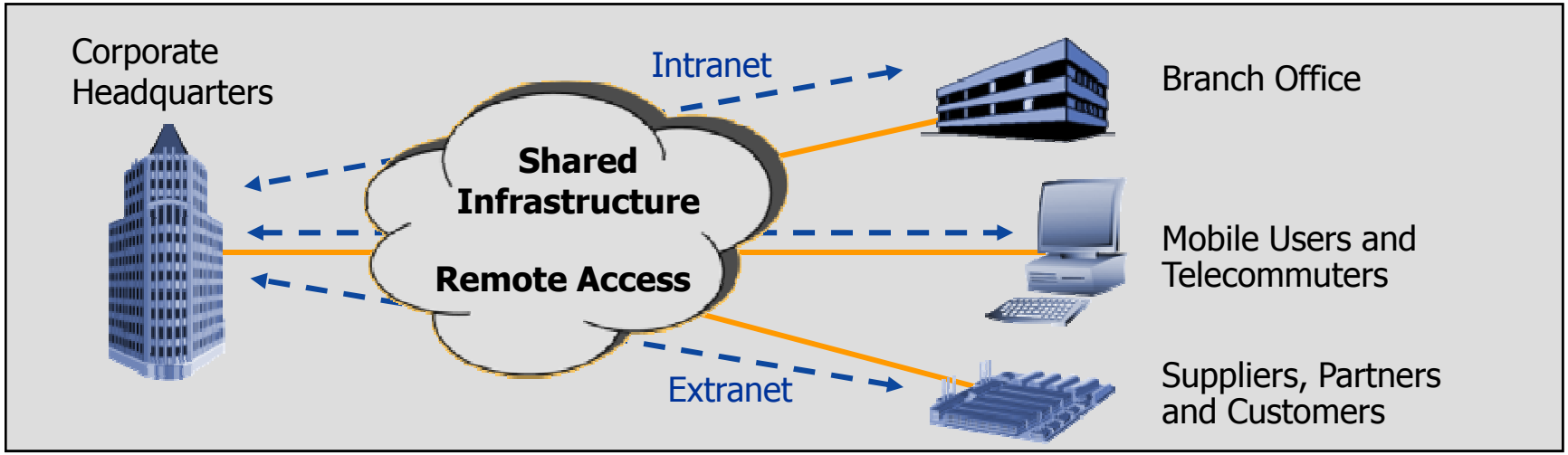
THE CORPORATE MODEL STARTED IN THE 80S



- **Large corporations having separate private networks**
  - Connected by means of leased lines for transmission throughout the PSTN-infrastructure
  - Voice focused, some data services (including packet switched, e.g. X.25)
- **Existing backbone wholesale solution but with limited opportunities for data core providers**
  - Transmission only
- **Point-to-Point links cannot address source mobility**

THE CURRENT IMPLEMENTATION OF VPNs

THE CORPORATE MODEL STARTED IN THE 90S



- **"A private network constructed over a shared infrastructure"**
  - Intranet
  - Extranet
  - Remote access
- **Opportunity for data core providers beyond transmission :**
  - Winning back corporate customers
  - high growth application area's such as e-commerce, Intranet, extranet, remote access provision
  - addressing source mobility

WHAT IS A VIRTUAL PRIVATE NETWORK (VPN)?

- VPNs emulate a private network over a shared Service Provider network
  - Interconnection of multiple private, geographically dispersed enterprise networks over a service provider network
  - Sharing service provider resources

- Virtual
  - No correspondent physical network
  - An emulated infrastructure utilizing underlying public network or networks

- Private
  - Access is restricted only to a defined set of entities

MPLS WORKSHOP

INTRODUCTION TO L2VPN

WHY L2VPN

WHY L2VPN

- Expanded service offerings by a service provider
- Offering of VPNs at a lower layer than IP
  - Because customers may not want service providers involved in IP routing
  - Transport of services which are not IP based
  - Services where IP routing is not required
- Consolidation of networks in a service provider domain
  - Consolidate ATM, Frame-Relay, Metro Ethernet, IPVPN onto a single IP core
  - Optimize our core network capacities
  - Remove legacy technologies and platforms from our network
- Service provider simplicity
  - No need to scale L3VPNs to thousands or millions of routes
  - Customers responsible for own routing – we only switch

MPLS WORKSHOP

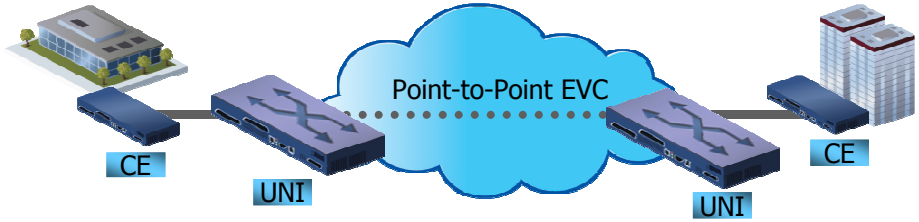
INTRODUCTION TO L2VPN

TYPES OF L2VPN

TYPES OF L2VPN

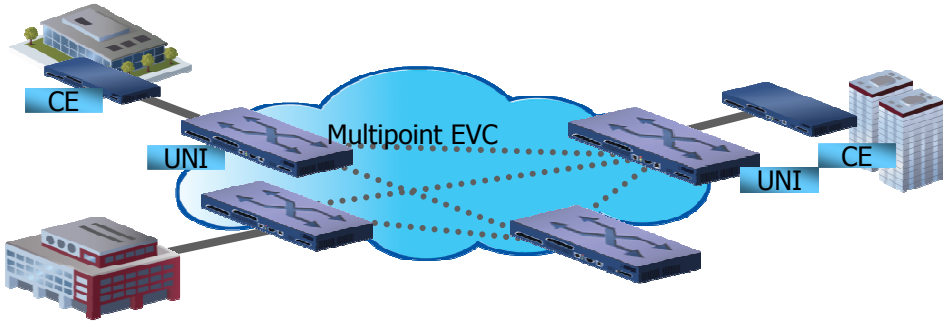
METRO ETHERNET FORUM SERVICE TYPES

E-LINE



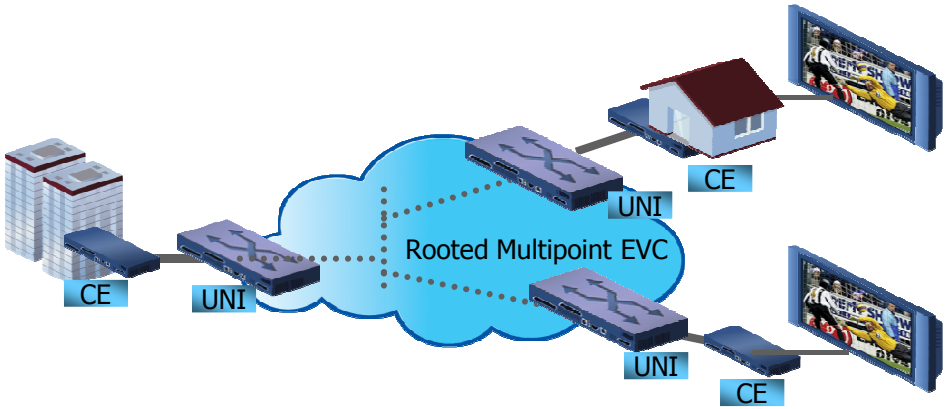
Point to Point
Service Type used to create
- Ethernet Private Lines
- Virtual Private Lines
- Ethernet Internet Access

E-LAN



Multi-Point to Multi-Point
Service Type used to create
- Multipoint Layer 2 VPNs
- Transparent LAN Service

E-TREE



Point to Multi-Point
- Efficient use of Service Provider ports
- Foundation for Multicast networks e.g. IPTV

TYPES OF L2VPN
OTHER TYPES OF VPN

- Layer 2 Transport focused
  - ATM
    Transport of ATM services over an IP/MPLS pseudowire, allowing the transport of legacy services and interfaces, or the optimization of your core networks for bandwidth
  - Frame Relay
    Transport of Frame Relay services over an IP/MPLS pseudowire, allowing the transport of legacy services and interfaces, or the optimization of your core networks for bandwidth
  - Circuit Emulation (TDM)
    Transport of TDM interfaces (T1/E1/DS3/etc) over an IP/MPLS pseudowire, allowing the transport of legacy services and interfaces – but not really an optimization of core network bandwidth
  - IP
    Interworking of discrete technologies (e.g. FR and Ethernet) at the IP layer, allowing separate interfaces to be interworked at the IP layer

MPLS WORKSHOP
TECHNOLOGY INTRODUCTION

THE PSEUDOWIRE REFERENCE MODEL

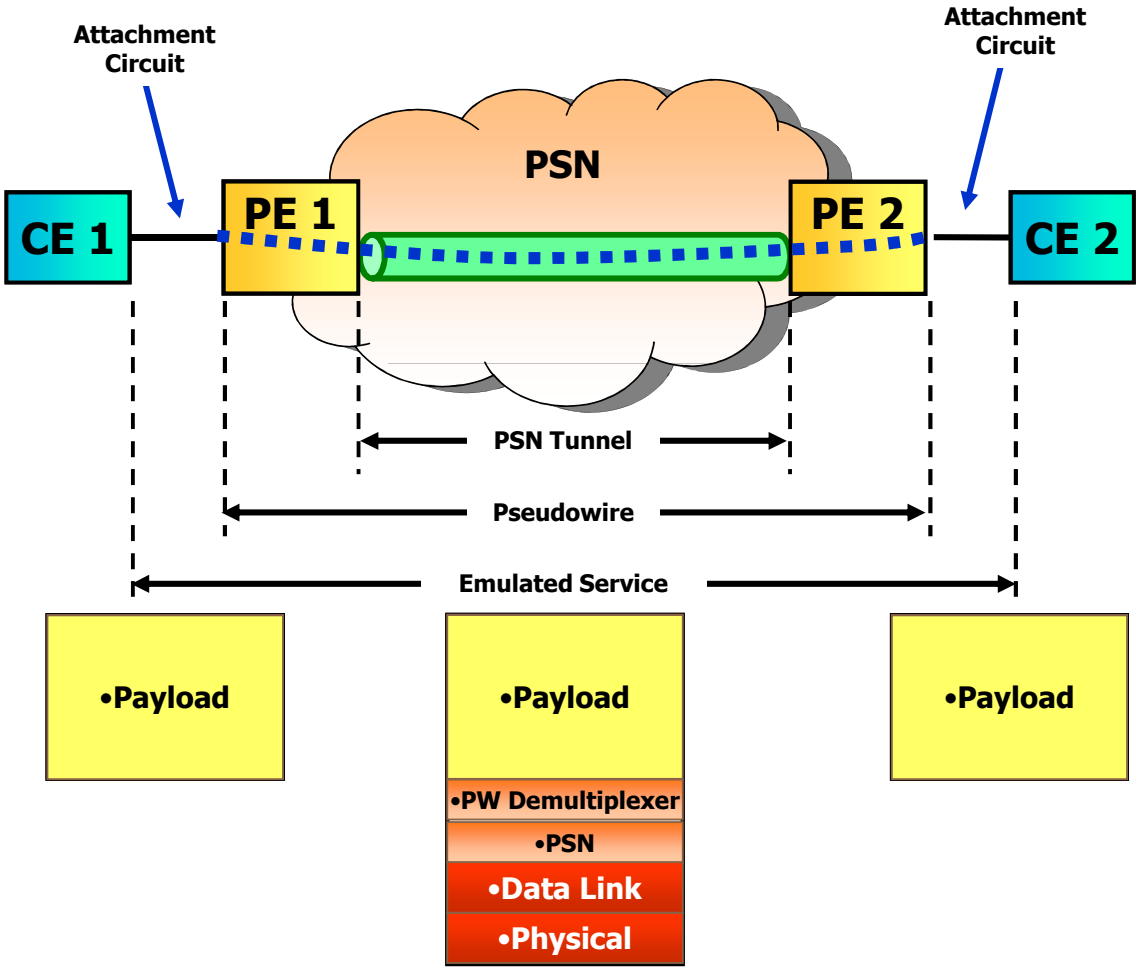
Pseudowires, Pwires, PWs, PWEs, or PWE3s:

- Key enabling technology for delivering Ethernet services over MPLS
- Specified by the **pwe3** working group of the IETF
- Originally designed for Ethernet over MPLS (EoMPLS) – initially called Martini tunnels
- Now extended to many other services – ATM, FR, Ethernet, TDM
- Encapsulates and transports service-specific PDUs/Frames across a Packet Switched Network (PSN) tunnel
- The use of pseudowires for the emulation of point-to-point services is referred to as Virtual Private Wire Service (VPWS)
- IETF definition (RFC3985):

  "...a mechanism that emulates the essential attributes of a telecommunications service (such as a T1 leased line or Frame Relay) over a PSN. PWE3 is intended to provide only the minimum necessary functionality to emulate the wire with the required degree of faithfulness for the given service definition."

PWE3 REFERENCE MODEL

- Generic PWE3 Architectural Reference Model:

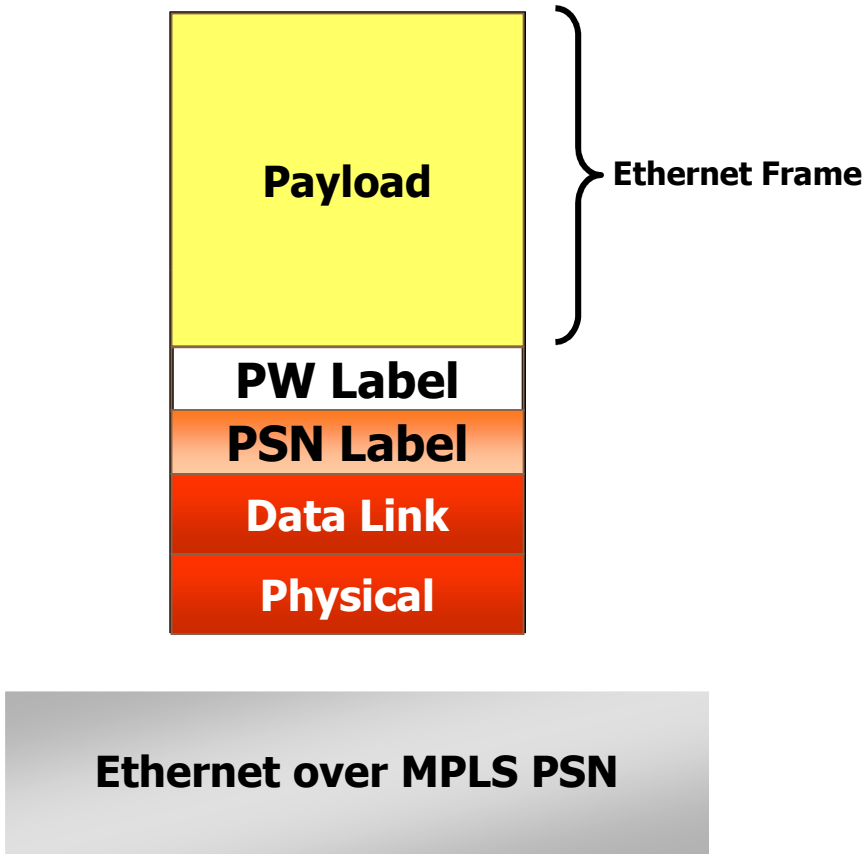


PWE3 TERMINOLOGY

- Attachment circuit (AC)
  - The physical or virtual circuit attaching a CE to a PE
- Customer Edge (CE)
  - A device where one end of a service originates and/or terminates
- Forwarder (FWRD)
  - A PE subsystem that selects the PW to use in order to transmit a payload received on an AC
- Packet Switched Network (PSN)
  - Within the context of PWE3, this is a network using IP or MPLS as the mechanism for packet forwarding
- Provider Edge (PE)
  - A device that provides PWE3 to a CE
- Pseudo Wire (PW)
  - A mechanism that carries the essential elements of an emulated service from one PE to one or more other PEs over a PSN
- PSN Tunnel
  - A tunnel across a PSN, inside which one or more PWs can be carried
- PW Demultiplexer
  - Data-plane method of identifying a PW terminating at a PE

PSEUDOWIRE PROTOCOL LAYERING

- The PW demultiplexing layer provides the ability to deliver multiple PWs over a single PSN tunnel

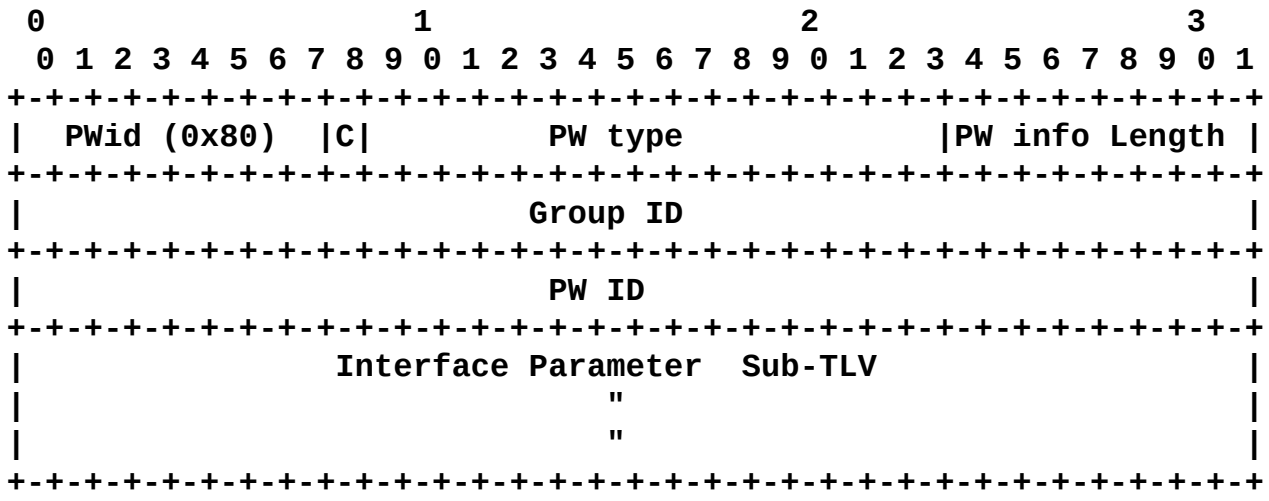


ETHERNET VIRTUAL PRIVATE WIRE SERVICE
SETUP AND MAINTENANCE

- Signalling specified in RFC4447 – "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)"
- The MPLS Label Distribution Protocol, LDP [RFC5036], is used for setting up and maintaining the pseudowires
  - PW label bindings are distributed using the LDP downstream unsolicited mode
  - PEs establish an LDP session using the LDP Extended Discovery mechanism a.k.a Targeted LDP or tLDP
- The PSN tunnels are established and maintained separately by using any of the following:
  - The Label Distribution Protocol (LDP)
  - The Resource Reservation Protocol with Traffic Engineering (RSVP-TE)
  - Static labels

ETHERNET VIRTUAL PRIVATE WIRE SERVICE
SETUP AND MAINTENANCE

- LDP distributes FEC to label mappings using the PWid FEC Element (popularly known as FEC Type 128)
- Both pseudowire endpoints have to be provisioned with the same 32-bit identifier for the pseudowire to allow them to obtain a common understanding of which service a given pseudowire belongs to.

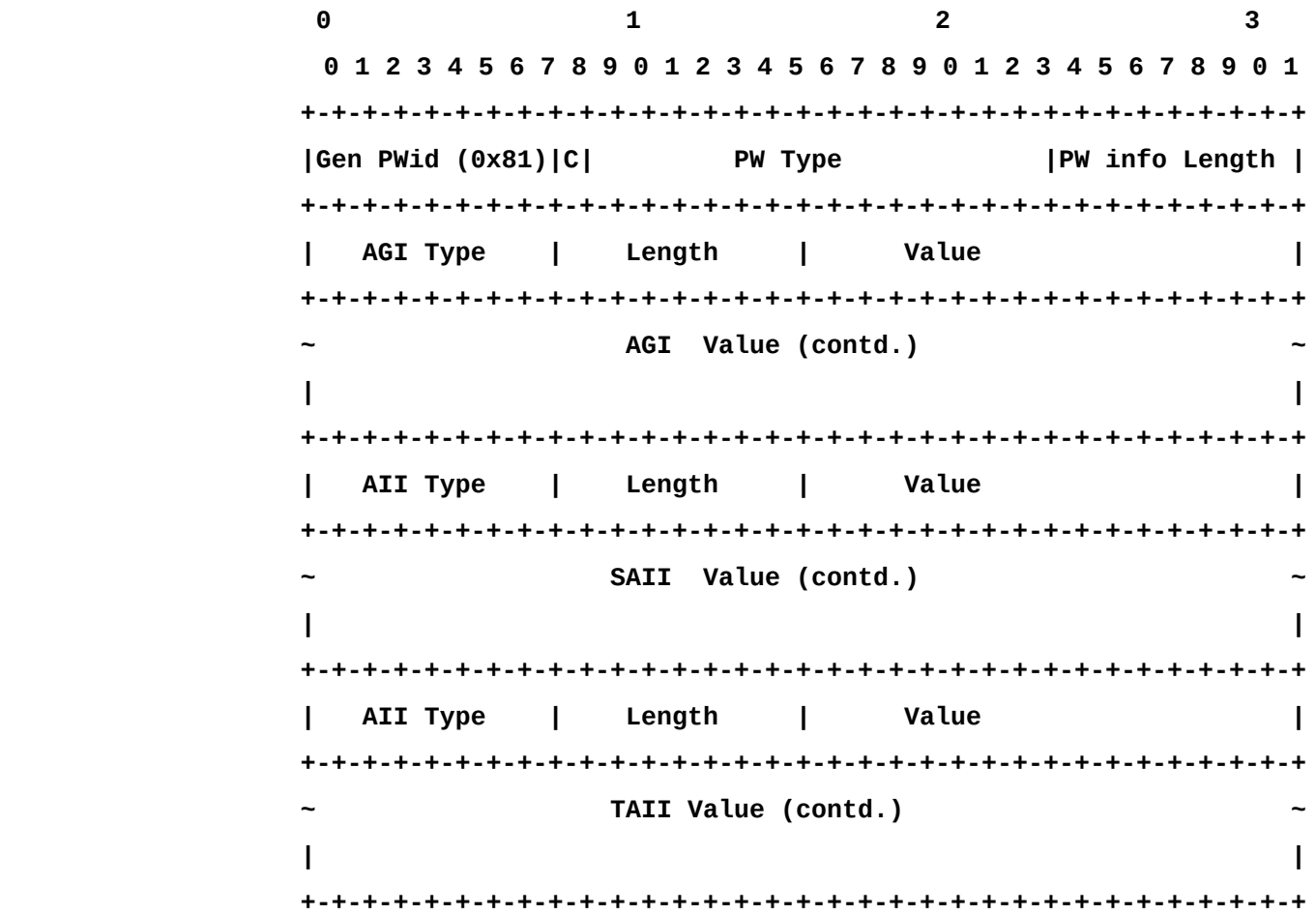


ETHERNET VIRTUAL PRIVATE WIRE SERVICE
SETUP AND MAINTENANCE

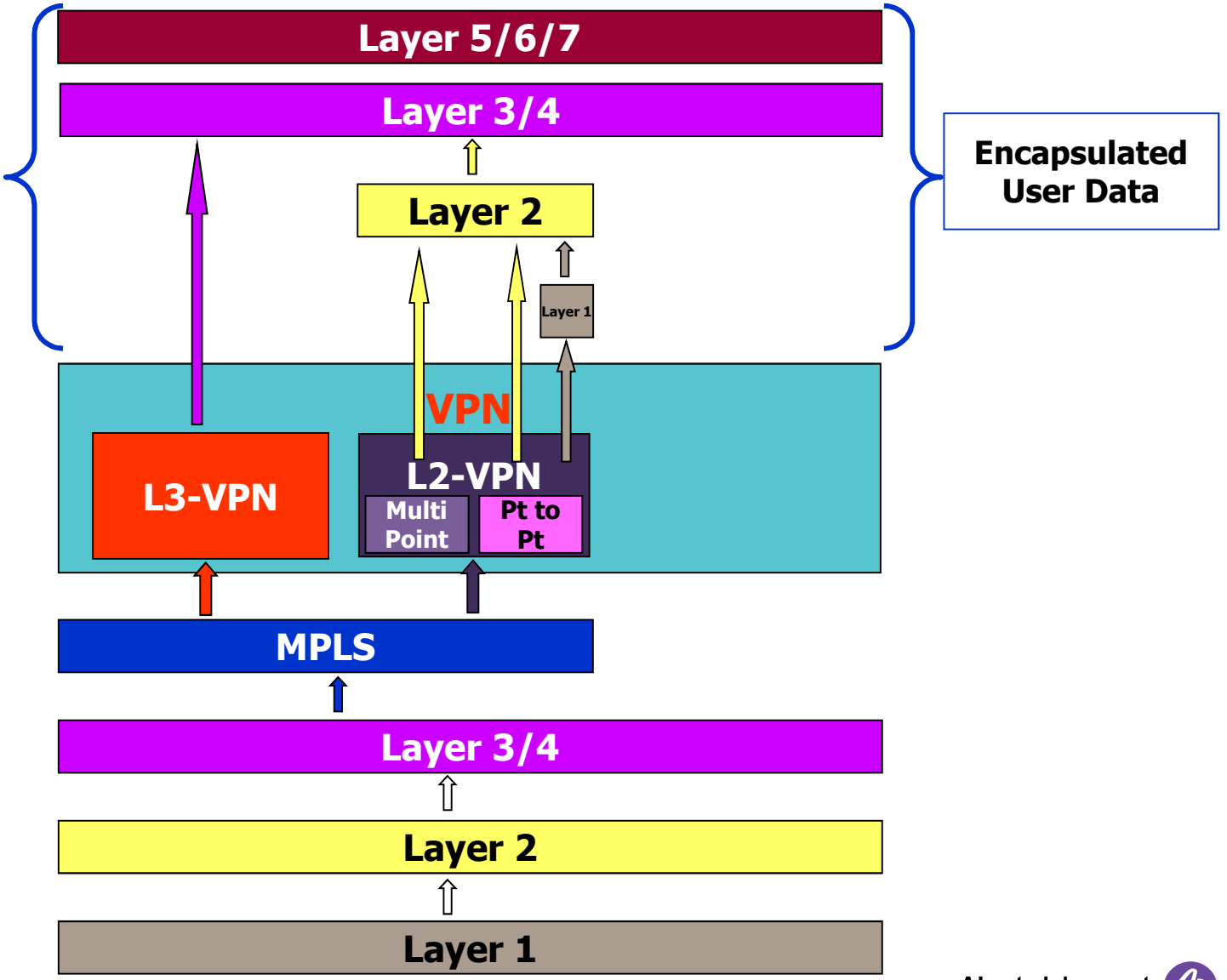
- A new TLV, the Generalized PWid FEC Element (popularly known as FEC Type 129) has also been developed but is not widely deployed as yet
- The Generalized PWid FEC element requires that the PW endpoints be uniquely identified; the PW itself is identified as a pair of endpoints. In addition, the endpoint identifiers are structured to support applications where the identity of the remote endpoints needs to be auto-discovered rather than statically configured.

ETHERNET VIRTUAL PRIVATE WIRE SERVICE
SETUP AND MAINTENANCE

- The Generalized PWid FEC Element (popularly known as FEC Type 129)

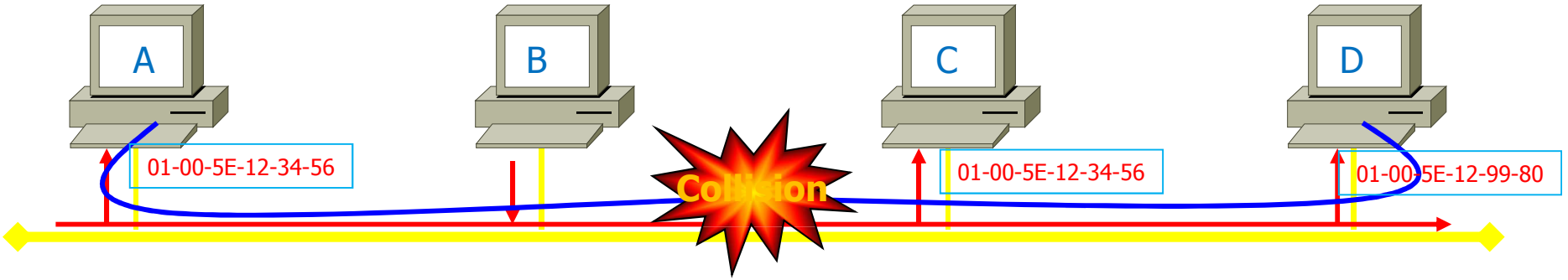


MPLS BASED VPN BUILDING BLOCKS



ETHERNET – BASIC : QUICK REFRESHER…

- A device is defined by its Media Access Control (MAC) address (6 bytes long: 00-dd-01-1e-ba-37).
- The MAC address must be unique
- The device MAC address usually don't change (often burned-in at manufacturing)
- Special MAC: **Broadcast:** → "ff-ff-ff-ff-ff-ff" **Multicast:** "01-00-5E-xx-xx-xx" (IGMP)



Device	Layer 2
A	MAC-A
B	MAC-B
C	MAC-C
D	MAC-D

A device listens to :

1. **Unicast** with its MAC (Dst: MAC-D)
2. **Broadcast** Packet (Dst: ff-ff-ff-ff-ff-ff)
3. **Multicast** where it is registered (Dst: 01-00-5E-12-34-56)

- Only **one device can speak** at a time on a segment
- If more than one device speak at the same time → **Collision**
- When a collision happens, information are **discarded** and need to be **resend** using a various delay mechanism – CSMA/CD

STANDARDS – PWE3

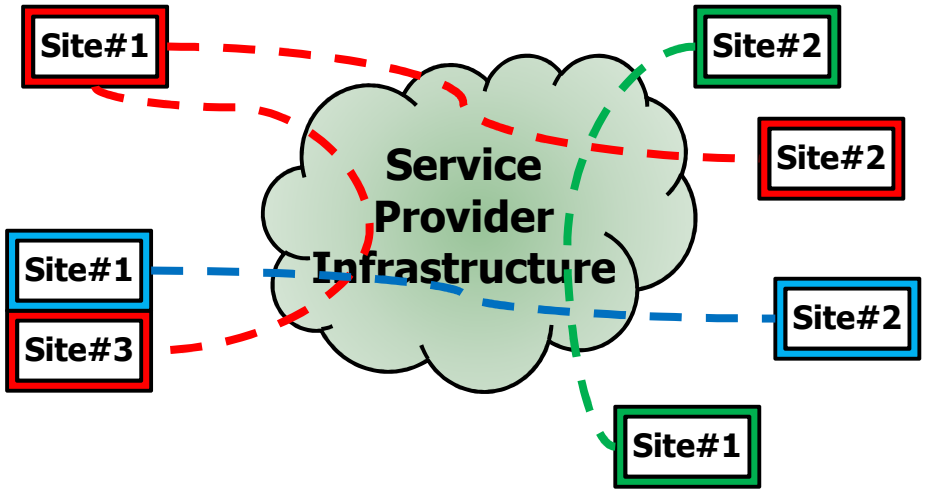
Standard	Title	Standard	Title
RFC3916	Requirements for PWE3 Edge-to-Edge	draft-ietf-pwe3-oam-msg-map	Pseudowire OAM Message Mapping
RFC3985	PWE3 Edge-to-Edge	draft-ietf-l2vpn-arp-mediation	ARP Mediation for IP Interworking of Layer 2 VPNs
RFC4385	PWE3 Control Words	RFC6073	Segmented pseudowires
RFC4717	Encapsulation Methods for ATM Transport over MPLS	draft-ietf-pwe3-dynamic-ms-pw	Dynamic placement of multisegment pseudowires
RFC4816	PWE3 ATM Transparent Cell Transport Service	draft-ietf-pwe3-redundancy-bit	Pseudowire preferential forwarding status bit definition
RFC4448	Encapsulation Methods for Transport of Ethernet over MPLS	draft-ietf-pwe3-redundancy	Pseudowire redundancy
RFC4619	Encapsulation Methods for Transport of Frame-Relay over MPLS		
RFC4446	IANA Allocations for PWE3		
RFC4447	Pseudowire setup and maintenance using LDP		
RFC5085	Pseudowire Virtual Circuit Connectivity Verification		
RFC5659	An architecture for multi-segment pseudowire emulation edge-to-edge		
draft-ietf-l2vpn-vpws-iw-oam	OAM Procedures for VPWS Interworking		

MPLS WORKSHOP

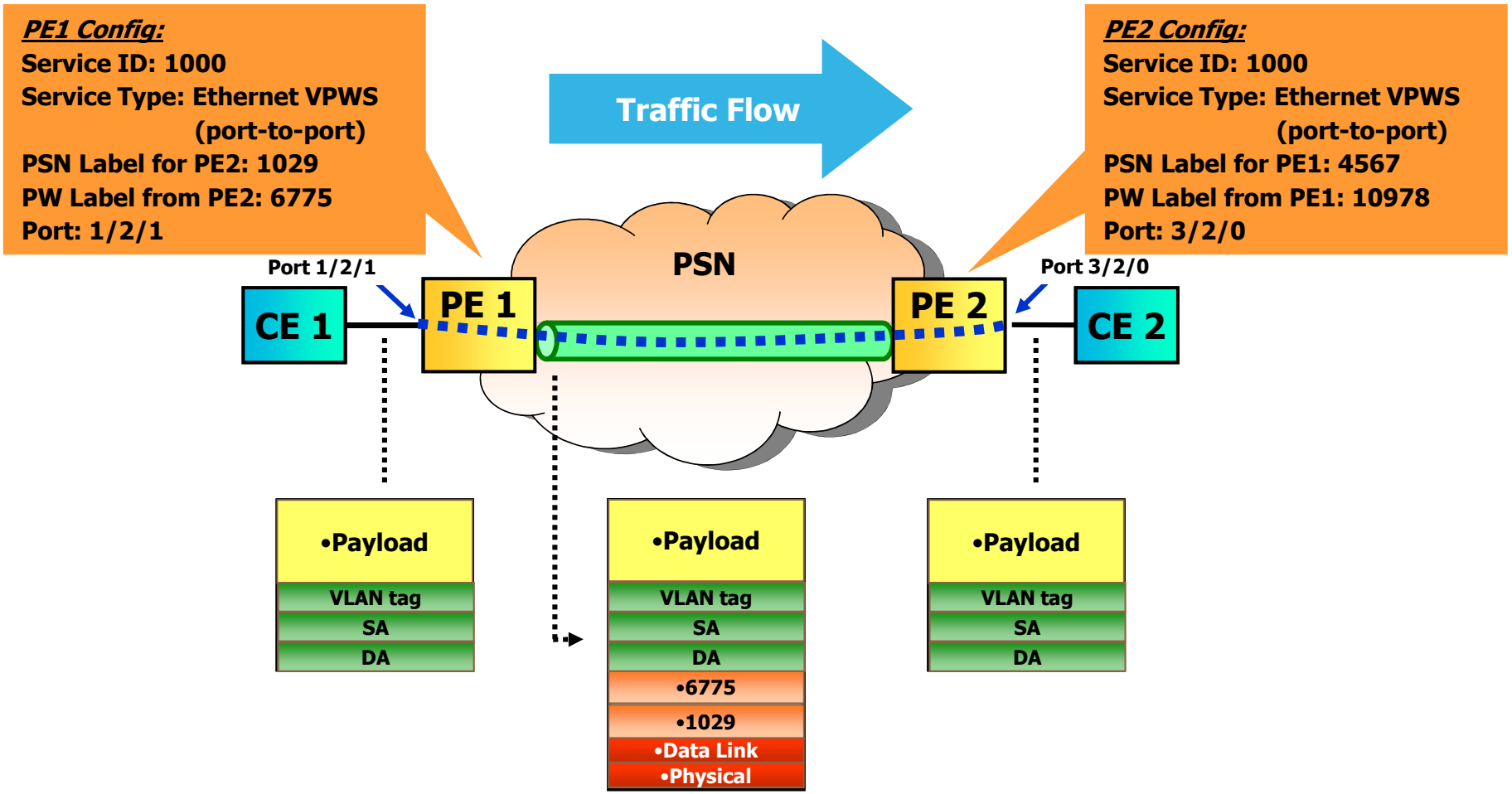
L2VPN – ETHERNET PSEUDOWIRES

POINT TO POINT LAYER 2 CONNECTION: VIRTUAL LEASED LINE (E-LINE)

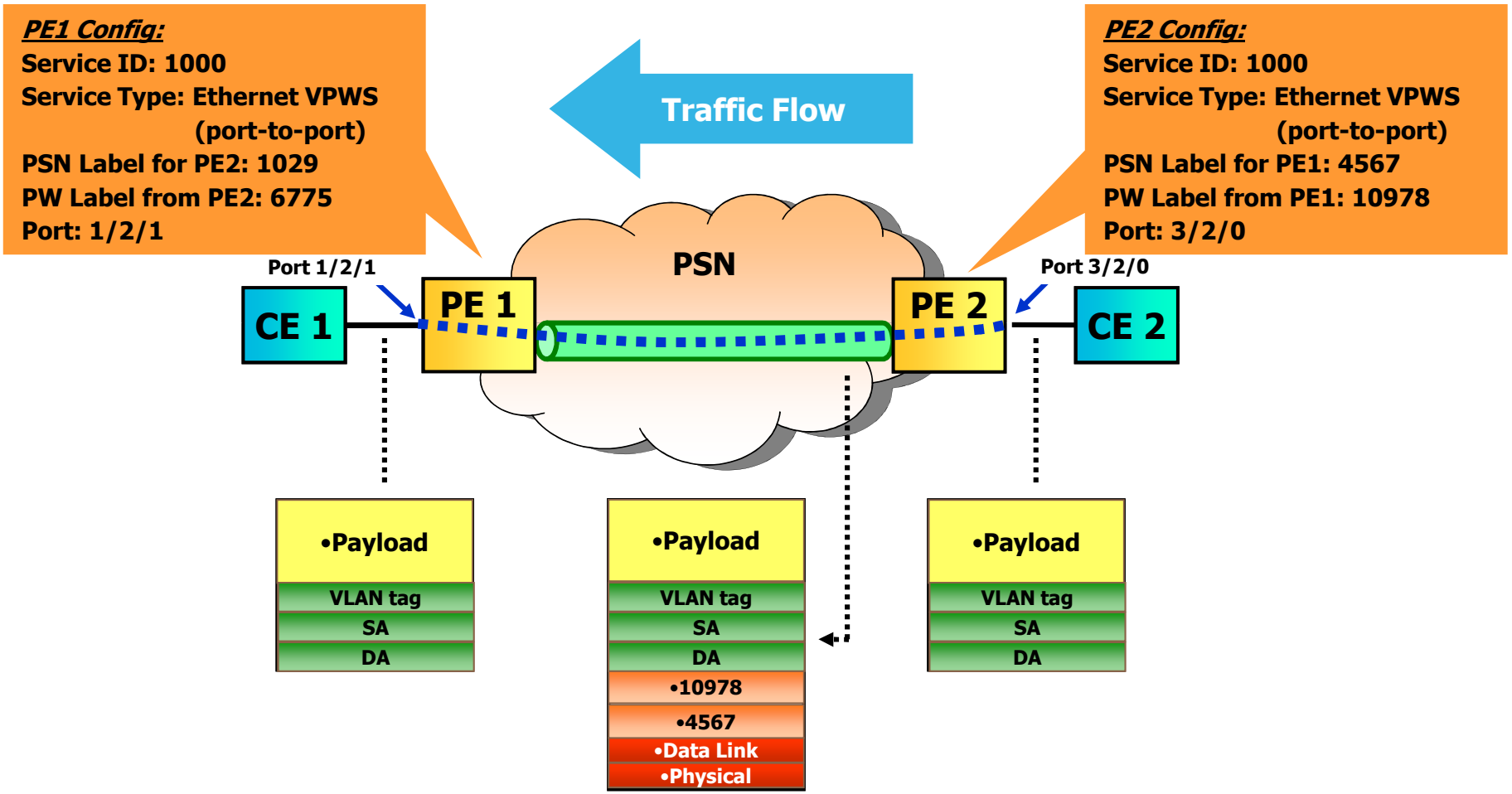
- Virtual Leased Line
- Draft-martini → **RFC-4905**
- Point-to-point FR, ATM, and Ethernet services
- Packet infrastructure is transparent to the end customer



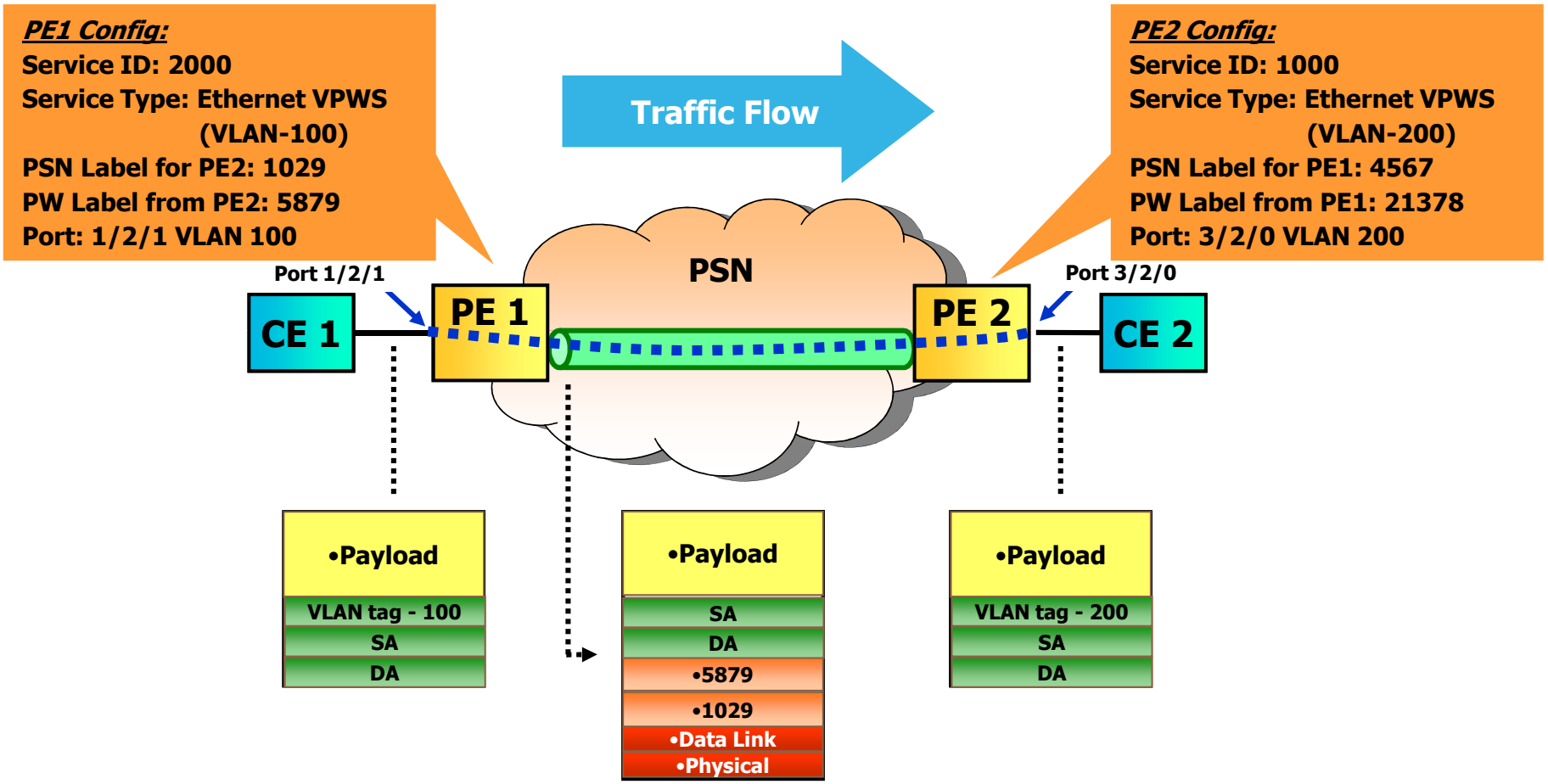
ETHERNET VPWS EXAMPLE 1
PORT BASED



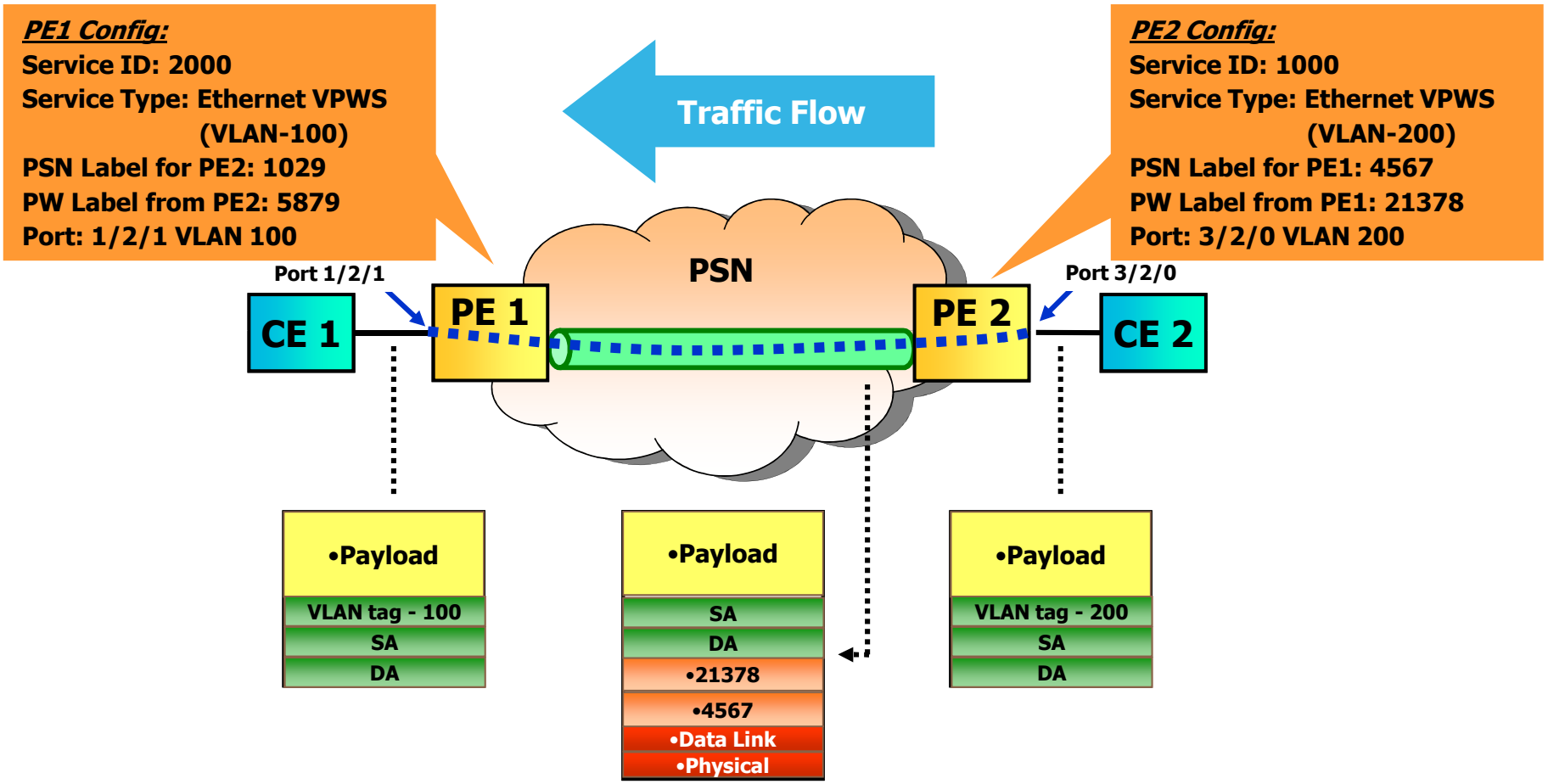
ETHERNET VPWS EXAMPLE 1
PORT BASED



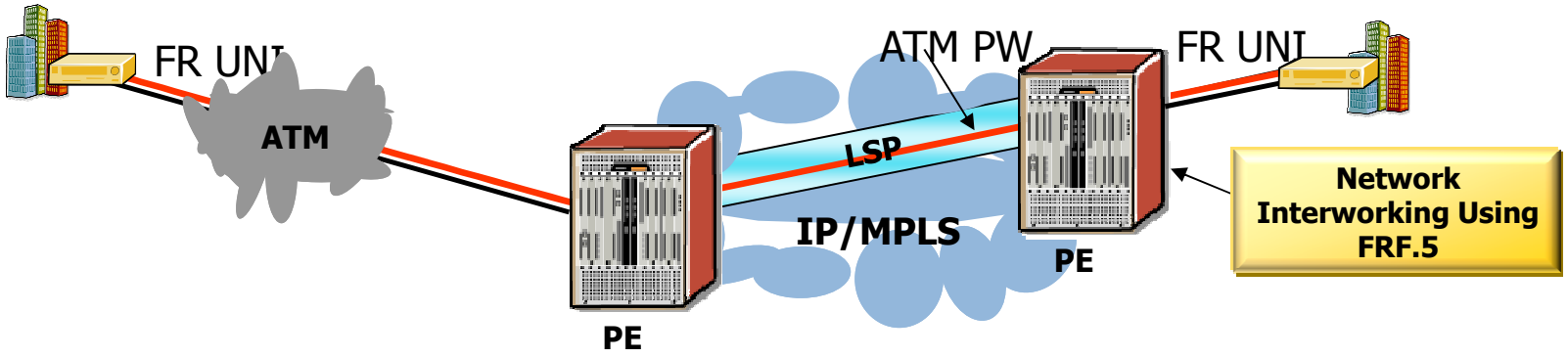
ETHERNET VPWS EXAMPLE 2
VLAN BASED



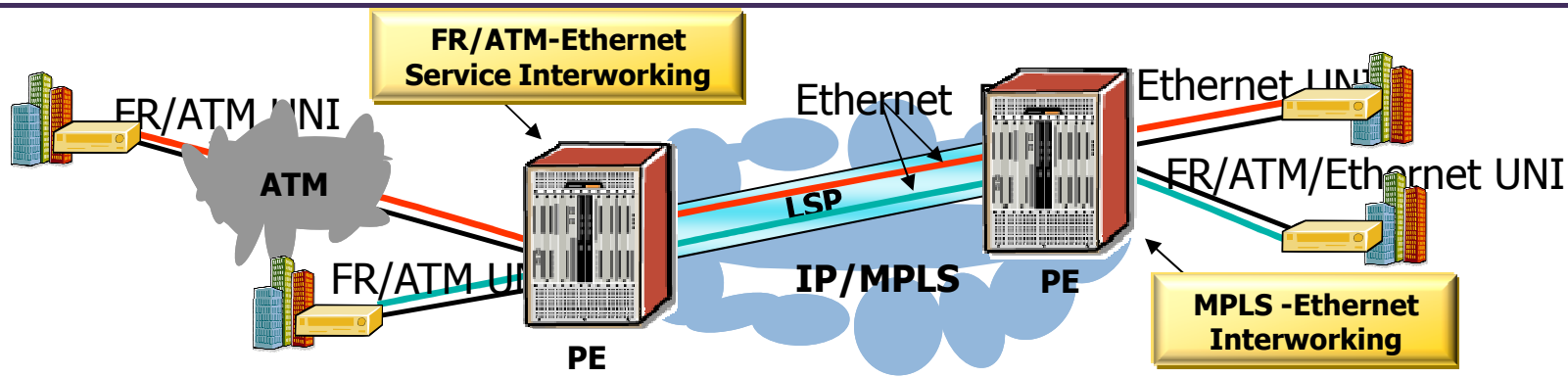
ETHERNET VPWS EXAMPLE 2
VLAN BASED



FR-ATM INTERWORKING AND ETHERNET INTERWORKING

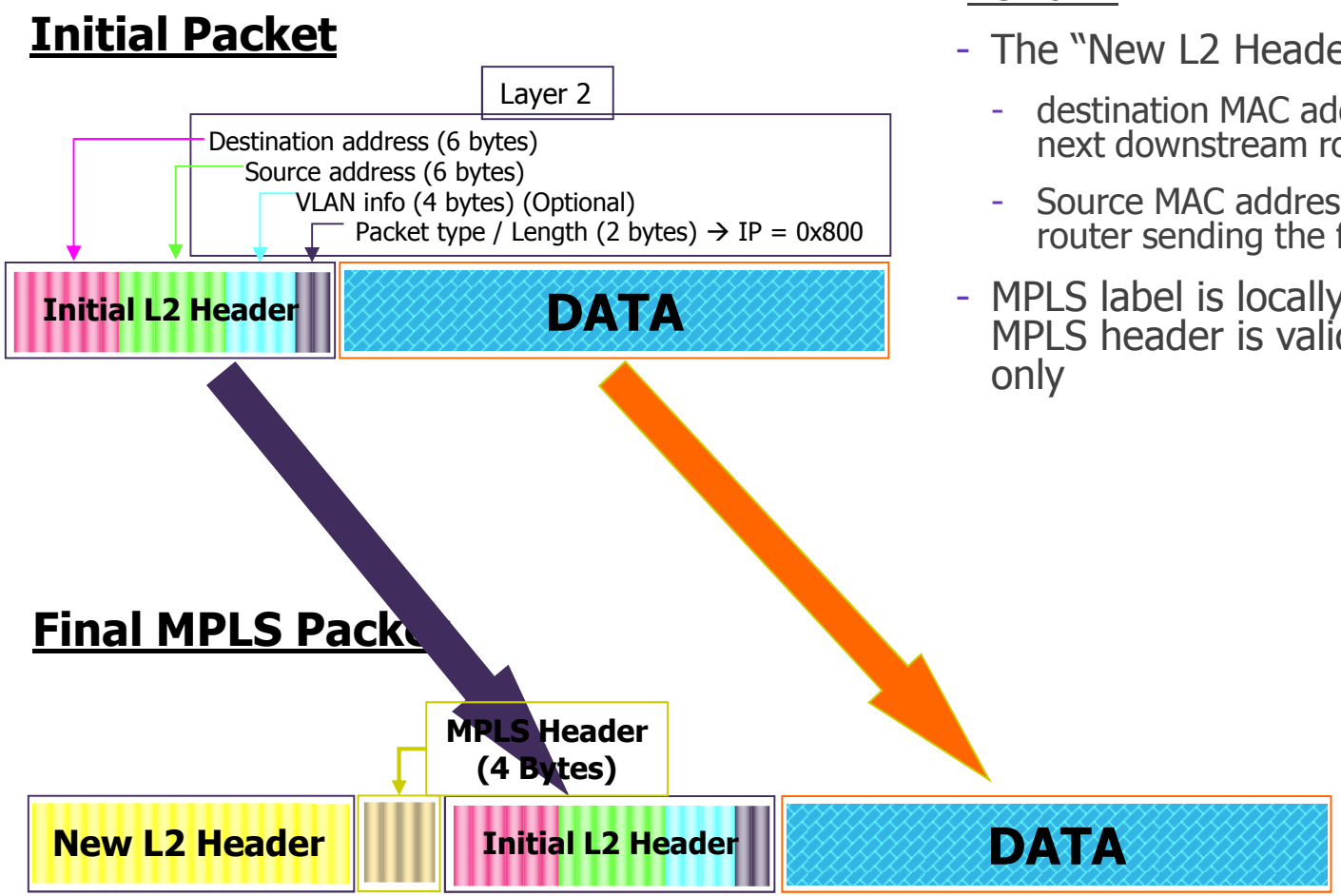


FR and ATM interworking ensures service continuity across the IP/MPLS network



Ethernet interworking provides ATM or FR access to an Ethernet endpoint and ensures service continuity across the IP/MPLS network

PSEUDOWIRE ENCAPSULATION



- Remark:
  - The "New L2 Header" is made using as
    - destination MAC address the MAC of the next downstream router
    - Source MAC address, the MAC of the current router sending the frame
  - MPLS label is locally significant so the MPLS header is valid for the current link only

WHERE ARE L2VPN/VLLs USEFUL?

- Anywhere transparency and MAC learning are really important
  - VLL has no MAC learning or encapsulation requirements
- Point-to-point services for customers
  - Office A to Office B networking where transparency is important
  - Customer wants to run their own encapsulation or possibly own MPLS network over the service – e.g. we must really act like a piece of wire
- Point-to-point services for infrastructure
  - Backhauling DSLAMs/MSANs over Metro Ethernet infrastructure from remote sites to central POPs
  - Backhauling cell site services
- Replacing legacy technologies
  - Replacement for FR or ATM services, where the logical service multiplexing (DLCI, VPI-VCI, or VLAN) is useful and high bandwidth requirements are needed

MPLS WORKSHOP

L2VPN – ETHERNET VIRTUAL PRIVATE LAN SERVICE

MULTI POINT LAYER 2 CONNECTION:
THE INITIAL IDEA

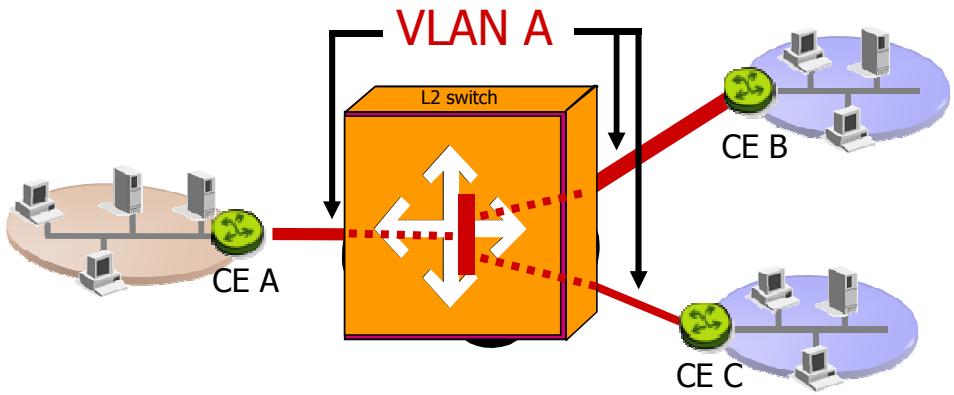
- How to interconnect multiple sites to multiple sites for a layer 2 connectivity using an MPLS based solution?

- Full mesh of point-to-point pseudowires
  - Create different pseudo-wires to each provider locations (PE)
  - Present those pseudo-wires to the outside world (CE) as different interfaces (Physical or Logical)
  - Connect those interfaces to a "customer switch"
    - Multiple connections going to the same customer
    - Manual creation of the pseudo-wire connections

- Virtual Private LAN Service
  - Create different pseudo-wires to each provider locations (PE) (Full Meshed)
  - Terminate those pseudo-wires inside an "internal process" of the PE router
  - The "Internal Process" must act as a Layer 2 switch
  - Add one external link (Physical or logical) to the Customer Edge (CE)
    - One connection is going to the customer
    - Full mesh of pseudo-wire can be automated

VPLS (ELAN):
CUSTOMER VIEW

- All locations appear to be on the same Ethernet LAN
- Entire provider network appears to be a Layer 2 switch

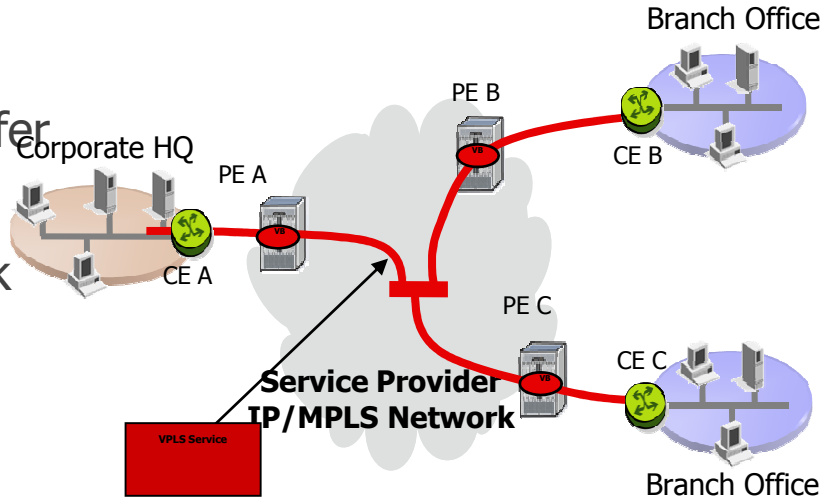


CE-PE interface

- Simple Ethernet interface
- Removes L2 protocol conversion between LAN and WAN
- No additional training required on WAN technologies such as FR

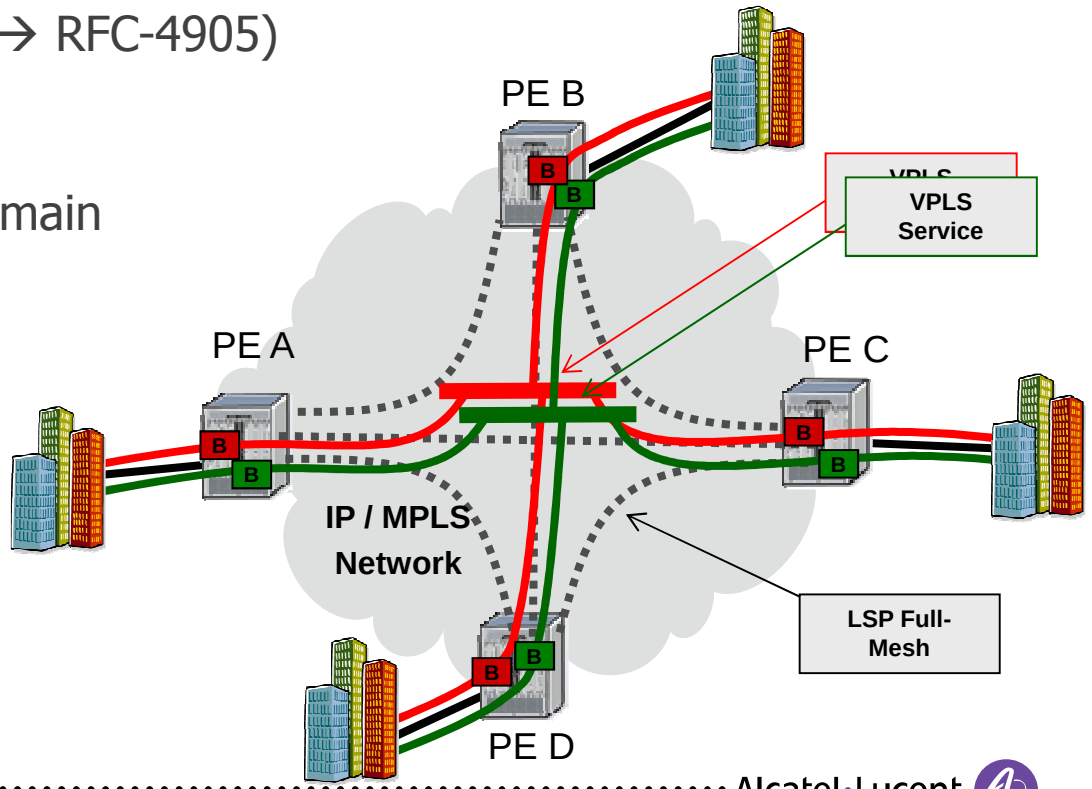
WHAT IS VIRTUAL PRIVATE LAN SERVICE ?

- VPLS
  - Is a class of VPN that allows the connection of **multiple sites** in a **single bridged domain** over a provider-managed MPLS network
- Customer perspective
  - It looks as if all sites are connected to a single switched VLAN
  - No interference with the Service Provider network
- Service provider
  - can reuse the IP/MPLS infrastructure to offer multiple services
  - No interference with the customer network



HOW IS VPLS PROVIDED OVER MPLS?

- Bridging capable PE routers
  - connected with a full mesh of MPLS LSP tunnels
- Per-Service VC labels
  - Negotiated using draft-Martini (→ RFC-4905)
- Unknown/broadcast
  - Traffic replicated in a service domain
- MAC learning
  - Over tunnels and access ports
  - Separate FIB per VPLS



VC LABEL SIGNALING

- VC-label Signaling between PEs per VPLS service instance
  - Each PE initiates a targeted LDP session to the far-end System IP address
  - Tells far-end what VC label to use when sending packets for each service

PE1->PE2: For Svc-id 101 UseVC-label pe2-1

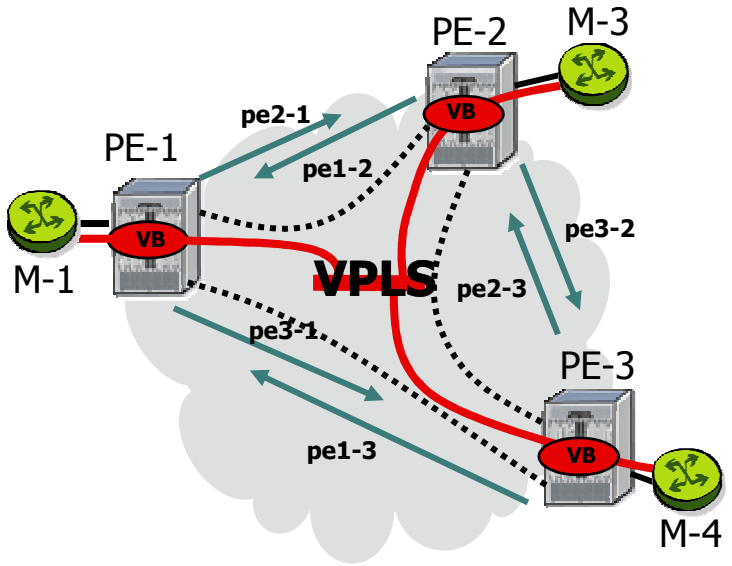
PE2->PE1: For Svc-id 101 Use VC-label pe1-2

PE1->PE3: For Svc-id 101 Use VC-label pe3-1

PE3->PE1: For Svc-id 101 Use VC-label pe1-3

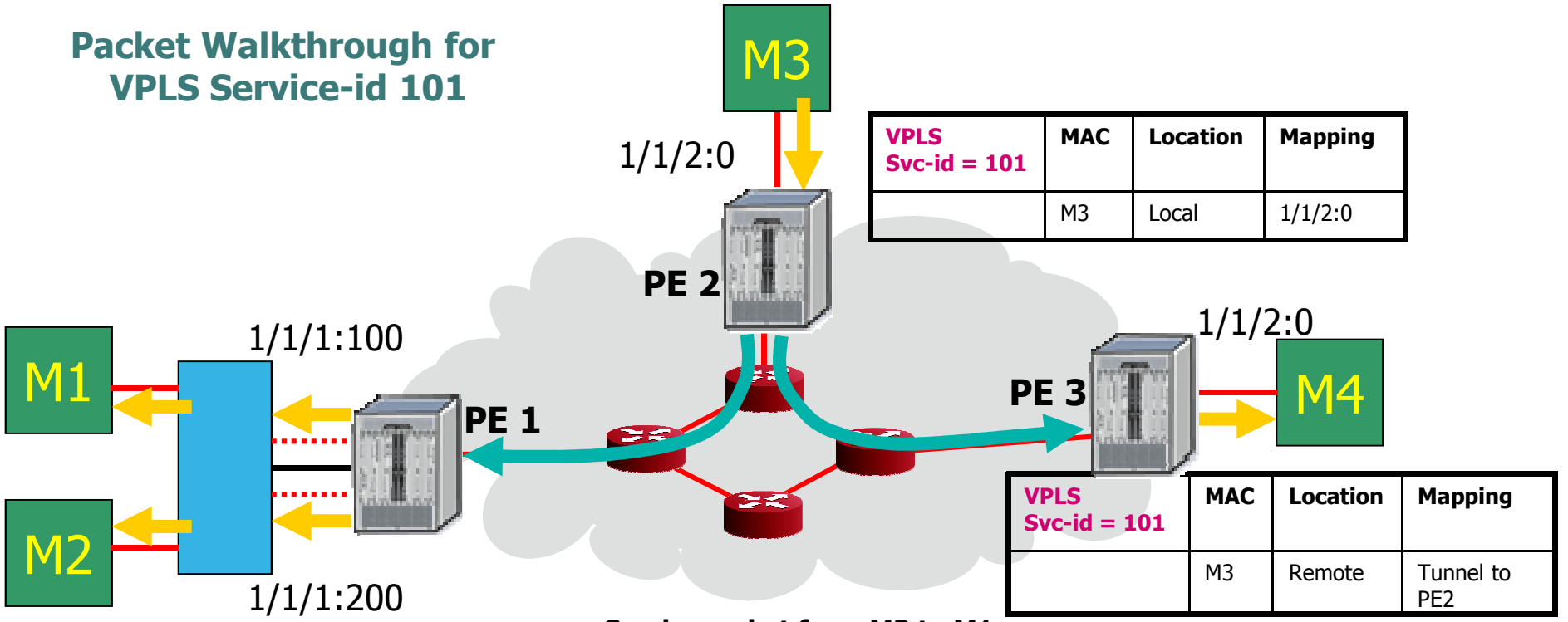
PE3->PE2: For Svc-id 101 Use VC-label pe2-3

PE2->PE3: For Svc-id 101 Use VC-label pe3-2



VPLS LEARNING

Packet Walkthrough for VPLS Service-id 101



VPLS Svc-id = 101	MAC	Location	Mapping
	M3	Local	1/1/2:0

VPLS Svc-id = 101	MAC	Location	Mapping
	M3	Remote	Tunnel to PE2

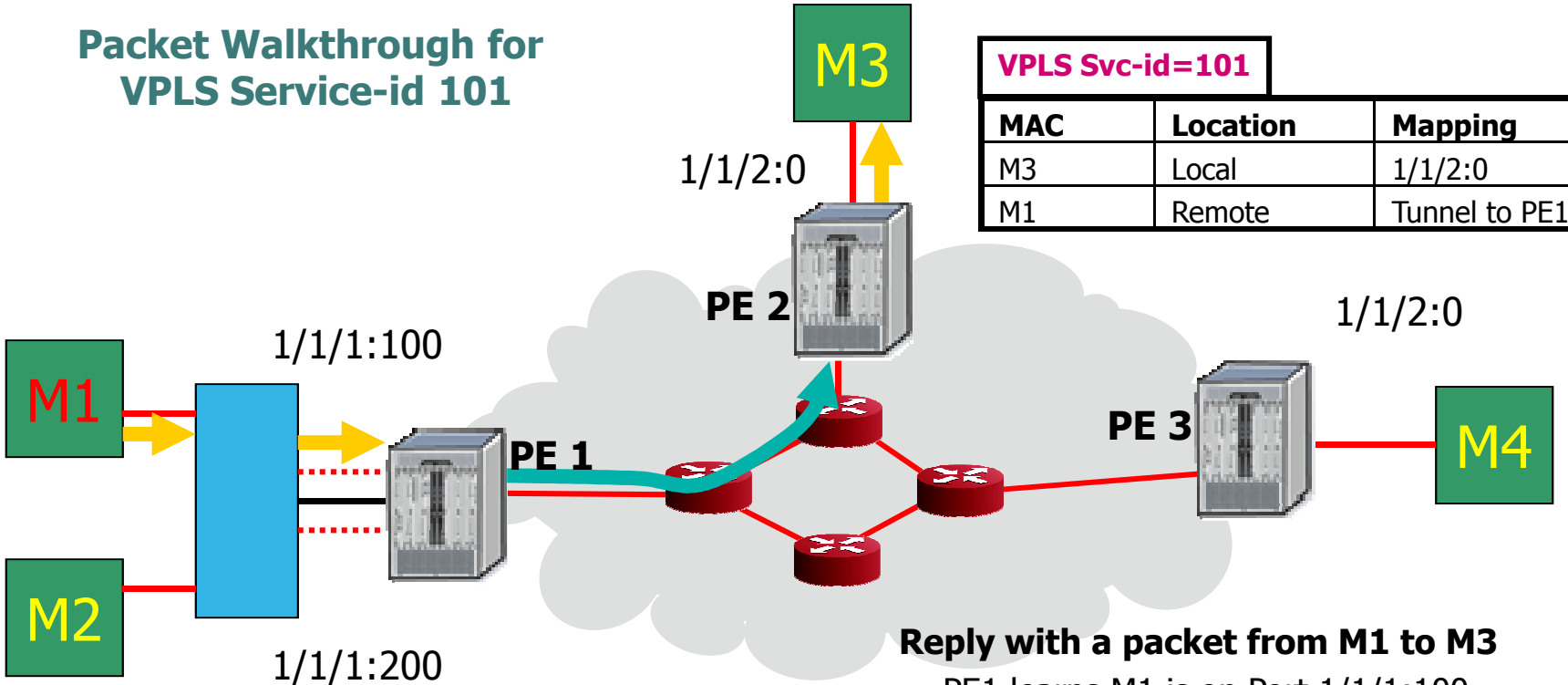
VPLS Svc-id = 101	MAC	Location	Mapping
	M3	Remote	Tunnel to PE2

Send a packet from M3 to M1

- PE2 learns that M3 is reached on Port 1/1/2:0
- PE2 floods to PE1 with VC-label pe2-1 and PE3 with VC-label pe2-3
- PE1 learns from the VC-label pe2-1that M3 is behind PE2
- PE1 sends on Port 1/1/1:100 & 1/1/1:200
- M1 receives packet
- PE3 learns from the VC-label pe2-3that M3 is behind PE2
- PE3 sends on Port 1/1/2:0

VPLS PACKET FORWARDING

Packet Walkthrough for VPLS Service-id 101



VPLS Svc-id=101

MAC	Location	Mapping
M3	Local	1/1/2:0
M1	Remote	Tunnel to PE1

VPLS Svc-id=101

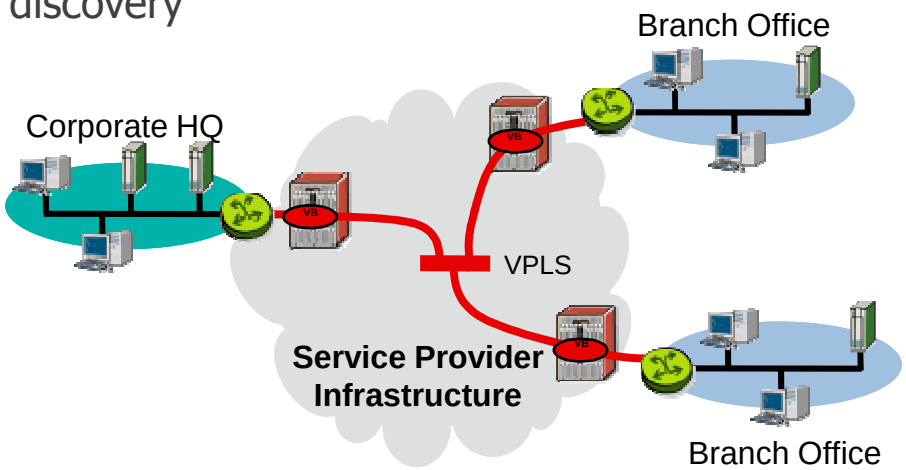
MAC	Location	Mapping
M3	Remote	Tunnel to PE2
M1	Local	1/1/1:100

Reply with a packet from M1 to M3

- PE1 learns M1 is on Port 1/1/1:100
- PE1 knows that M3 is reachable via PE2
- PE1 sends to PE2 using VC-label pe1-2
- PE2 knows that M3 is reachable on Port 1/1/2:0
- M3 receives packet

VPLS AND STANDARDIZATION

- 2 standards exist
  - RFC4761 (K. Kompella)
    - Uses BGP for both signaling and Auto-Discovery
  - RFC4762 (Laserre/V. Kompella)
    - Uses LDP for signaling
    - Optionally may use RADIUS for auto-PE discovery
- Multipoint Ethernet Service
- Customer hand-off is Ethernet



WHERE ARE VPLS USEFUL?

- Where MAC learning and multipoint topologies are important, but transparency may be sacrificed
- Multipoint services for customers
  - Office A to B, C, D, connectivity
  - Virtual switch in the sky
  - Multipoint topology for Carrier-supporting-Carrier
- Multipoint services for infrastructure
  - Bridging internal VLANs across multiple sites for datacenters, network management, etc
  - Some service backhaul (broadband, etc)
- Efficient Multicast services for customers or infrastructure

MPLS WORKSHOP
ADVANCED TOPICS

L2VPNs
ADVANCED TOPICS

- Scaling VPLS
  - H-VPLS
  - PBB-VPLS
- Scaling signalling
- Inter-AS connectivity
- Redundancy
  - In the metro Ethernet core
  - In the PE-CE (UNI) interface
- Multi segment pseudowires
- OAM

MPLS WORKSHOP
SUMMARY

L2VPNs
SUMMARY

- L2VPNs are a useful toolkit for service providers and end customers to build networks
- Most commonly deployed L2VPNs focus on Ethernet services
  - Standardized service offerings are defined by Metro Ethernet Forum (MEF)
- L2 services may also be used to transport other protocols
  - Mobile backhaul
  - Network transformation or legacy technology retirement
  - Unique protocol support requirements
- L2 services are not without deployment problems in the service provider and end user networks
  - Service scaling
  - Bandwidth consumption
  - And so on

L2VPN
COMPARISON OF VPN SERVICE TYPES

	IP-VPN	VPLS	VLL	Other PWE
Routing interaction	Required	No	No	No
Protocol support	IP only	Any	Any	Any
Topology paradigms	Any-to-Any	Any-to-Any Hub-spoke	Point-to-Point	Point-to-Point
VLAN Support	No	Yes	Yes	Depends
Interface types	Any	Many, but usually Ethernet	Many, but usually Ethernet	ATM FR CES Etc
Transport services	No	No	Ethernet only	Yes

AT THE SPEED OF IDEAS™

Alcatel·Lucent

AT THE SPEED OF IDEAS™

Alcatel·Lucent

www.alcatel-lucent.com