Alcatel·Lucent

Introduction to Multi-Protocol Label Switching (MPLS)

Matthew Bocci, Alcatel-Lucent IP Division

Agenda

History of MPLS Standardisation

MPLS Architecture

Control Plane

QoS and Traffic Engineering

Protection and Resiliency

MPLS Based Services:

- Layer 3 Virtual Private Networks
- Layer 2 Virtual Private Networks & Pseudowires

IP/MPLS in Carrier Networks

> Pt-pt & multicast scalability

> Service convergence over MPLS including VPLS

> Service enabling the edge
  - L3 based MPLS VPN

> Business enabling the core
  - MPLS attempt to enhance network resilience
  - MPLS-enhanced QoS

> Infrastructure optimization
  - Traffic engineering
  - Hierarchical core design

> Enhance forwarding performance of router networks

MPLS Applications

2005+
Multi-segment PWs, Multicast in VPLS / IPVPNs / pt-mp LSPs

2001-2004
Development of pseudowires / L2VPNs
Unified Control Plane for Non-Packet and Packet Networks

1999-2000
Enhanced Network Resilience

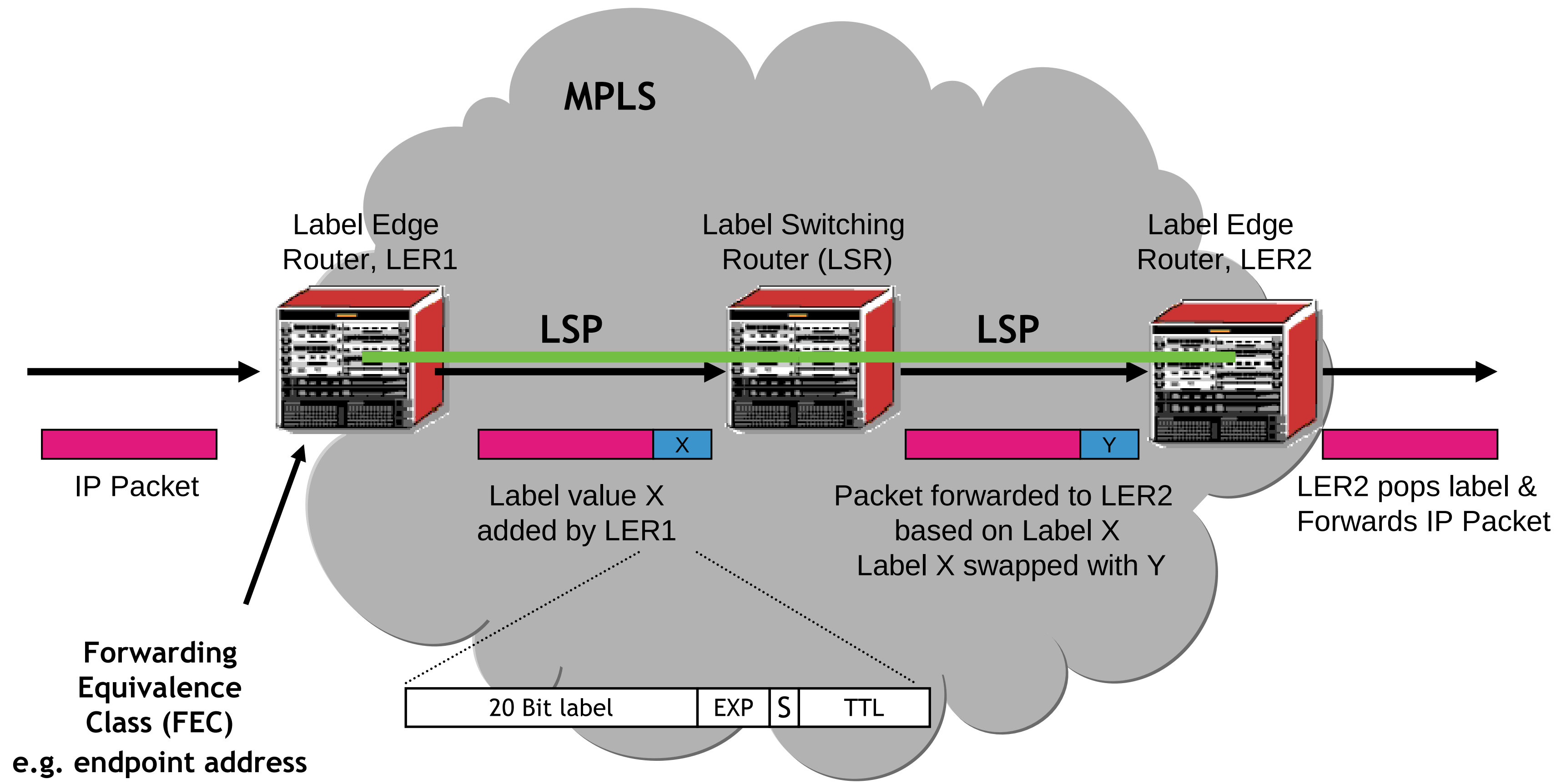
1998
Traffic Engineering
Virtual Private Networks

1996-1997
Forwarding Performance

MPLS Standardisation Activities

Multiprotocol Label Switching Architecture

MPLS Shim label added to each packet
Forwarding decisions are based on label, to follow a label switched path (LSP)
Runs over many link layers – SDH, Ethernet, etc



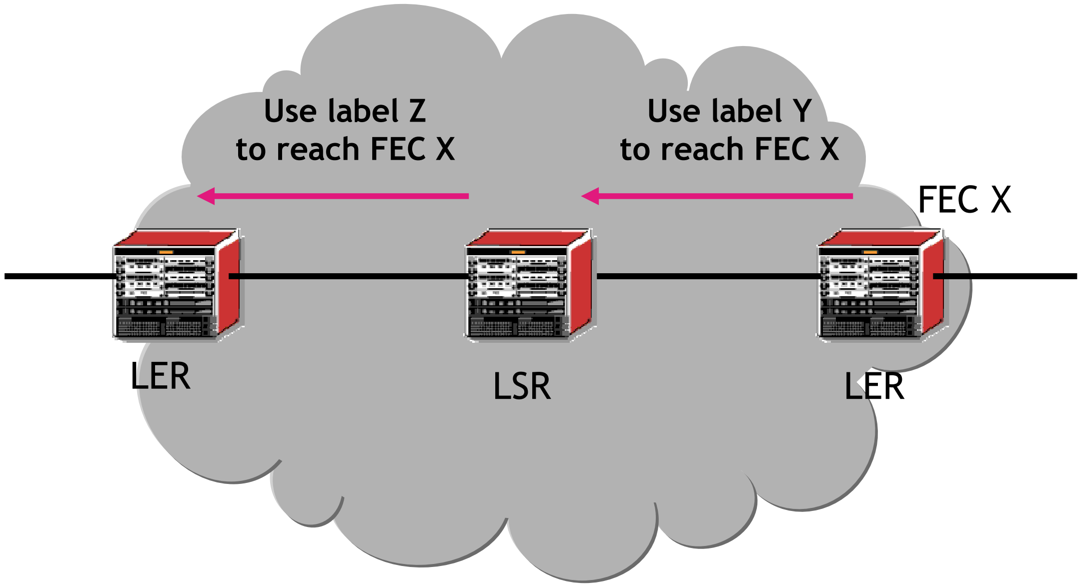
MPLS Architecture: IETF RFC 3031

MPLS Control Plane

Distribute FEC/Label bindings between LSRs

- Label Distribution Protocol (LDP) for non-TE LSPs
  - Simple protocol that exchanges label bindings with peer LSRs

- RSVP-TE for traffic engineered LSPs
  - Soft-state protocol enabling BW parameters & path to be signalled



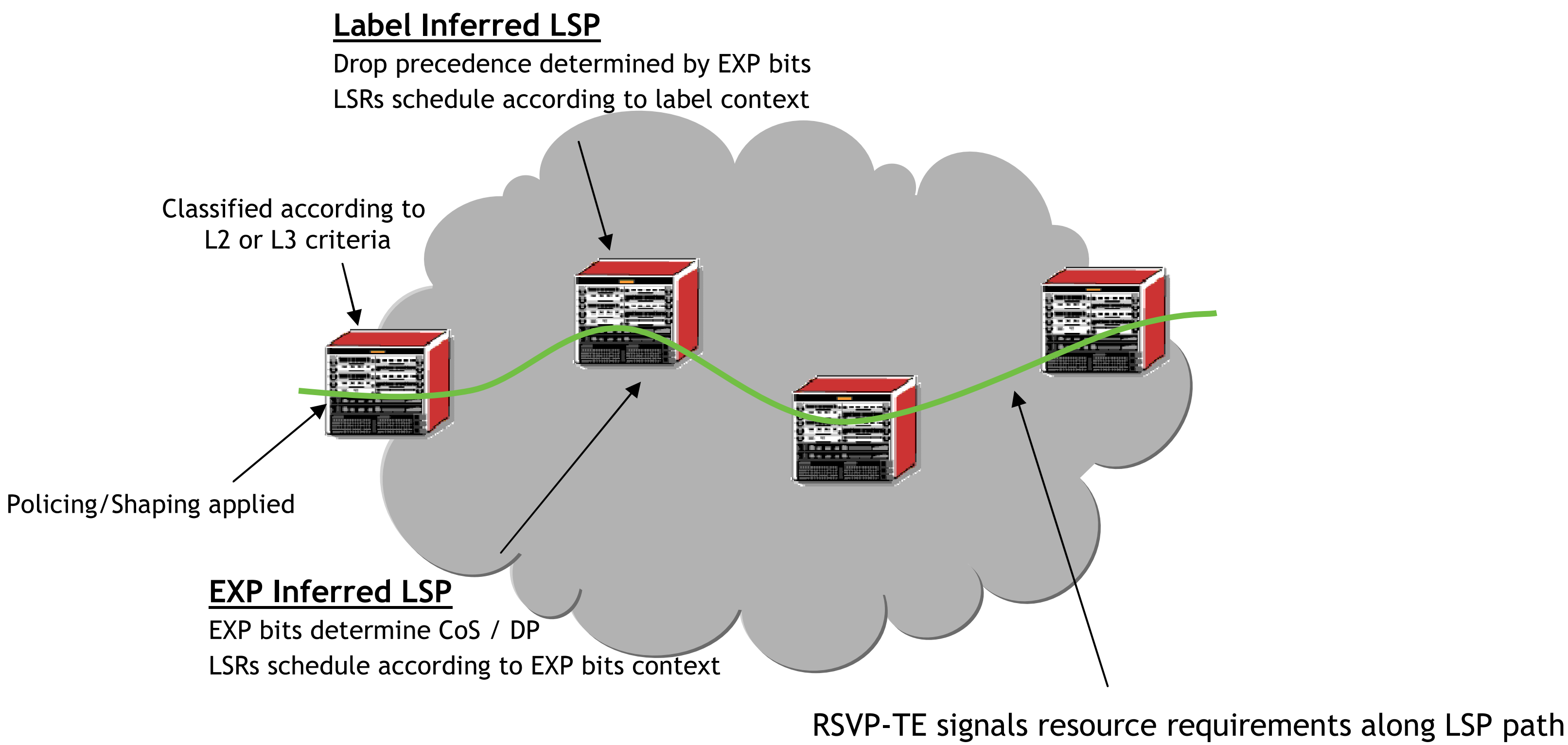
QoS and Traffic Engineering

MPLS Label:

20 Bit label	EXP		TTL

Encode CoS and/or DP

Control plane to determine LSP path and reserve resources along path



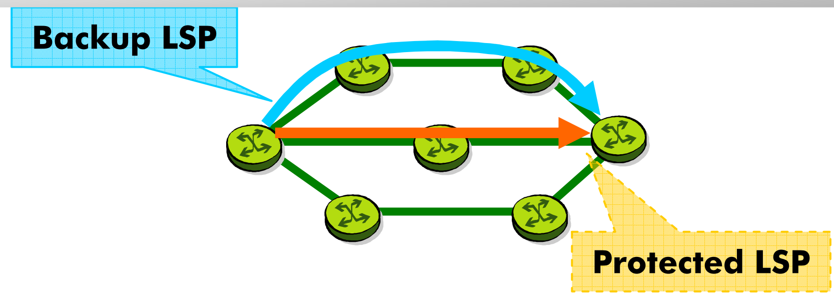
Alcatel·Lucent

Protection and Resiliency

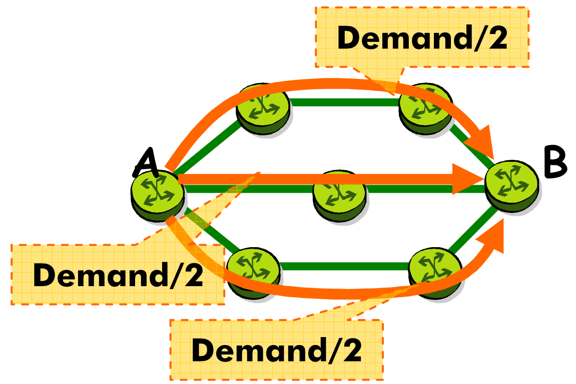
MPLS provides a common protection layer, independent of underlying transport mechanisms

Wide range of options

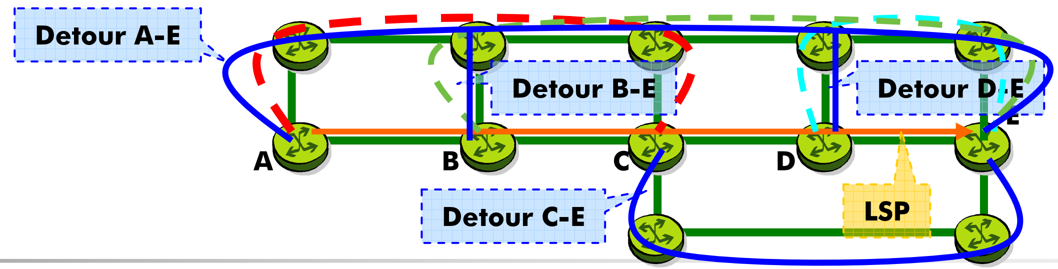
Path protection:



Load balancing:



Local protection:



Alcatel·Lucent

MPLS based Services and Virtual Private Networks

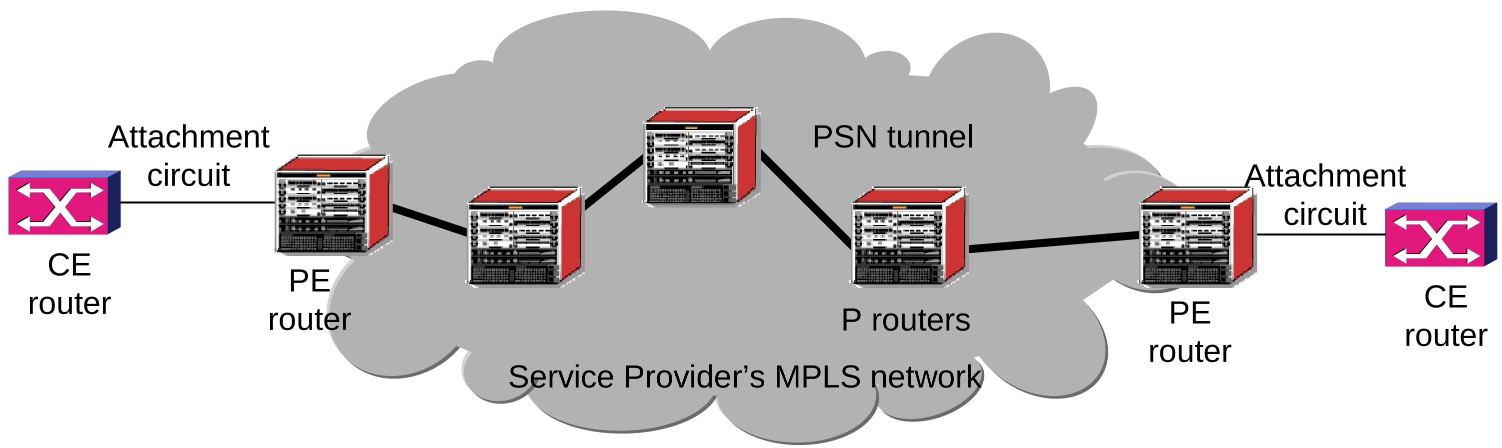
LSP tunnels segregate customer traffic in network

Two VPN classes:

Layer 3 VPNs: IP

Layer 2 VPNs:

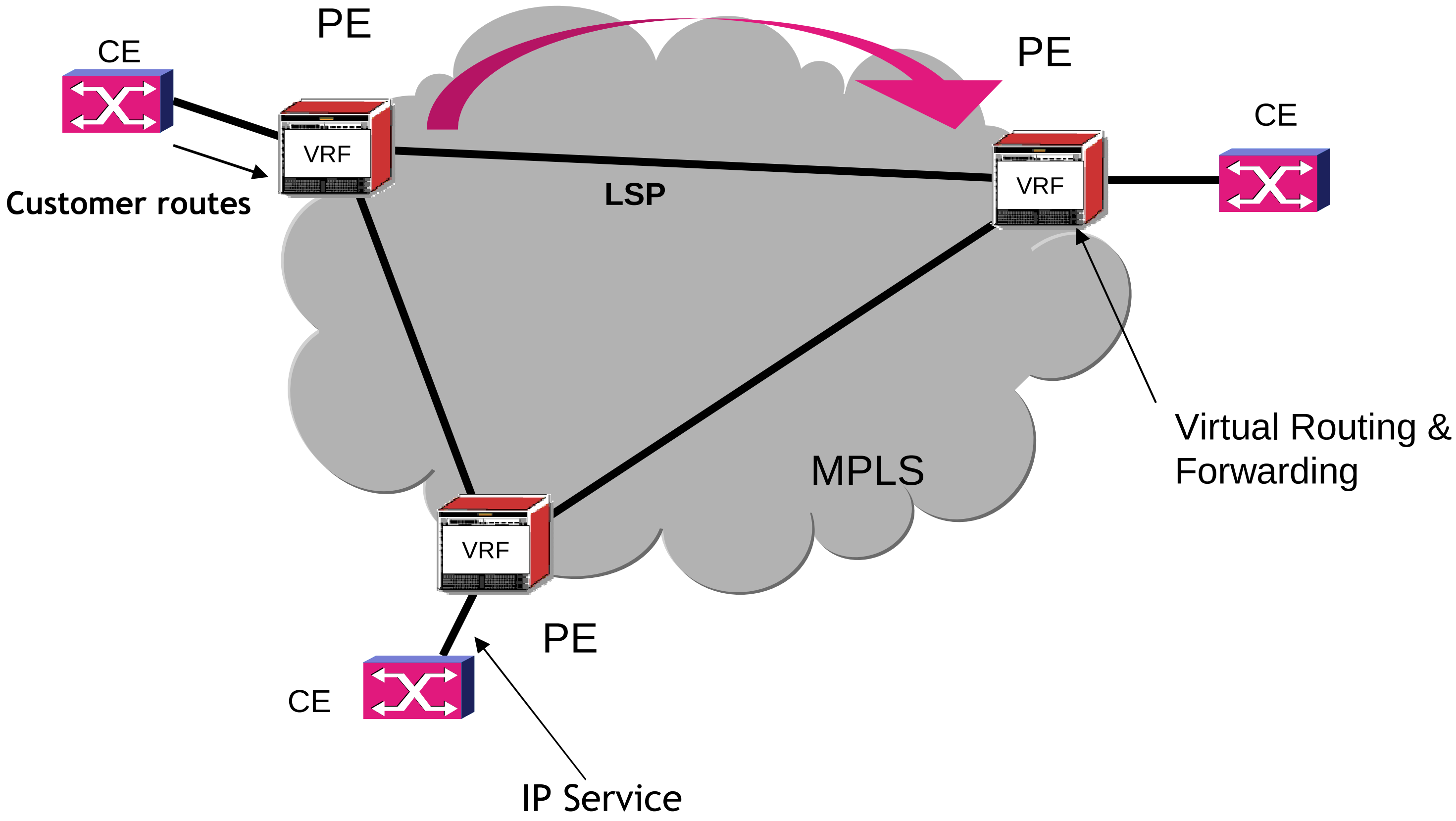
- Virtual Private Wire Service (pt-pt Ethernet, FR, ATM, etc)
- Virtual Private LAN Service (mp-mp Ethernet)



IETF RFC 4664

Border Gateway Protocol (BGP) Layer 3 VPNs

MP-BGP* exchanges VPN membership/reachability info



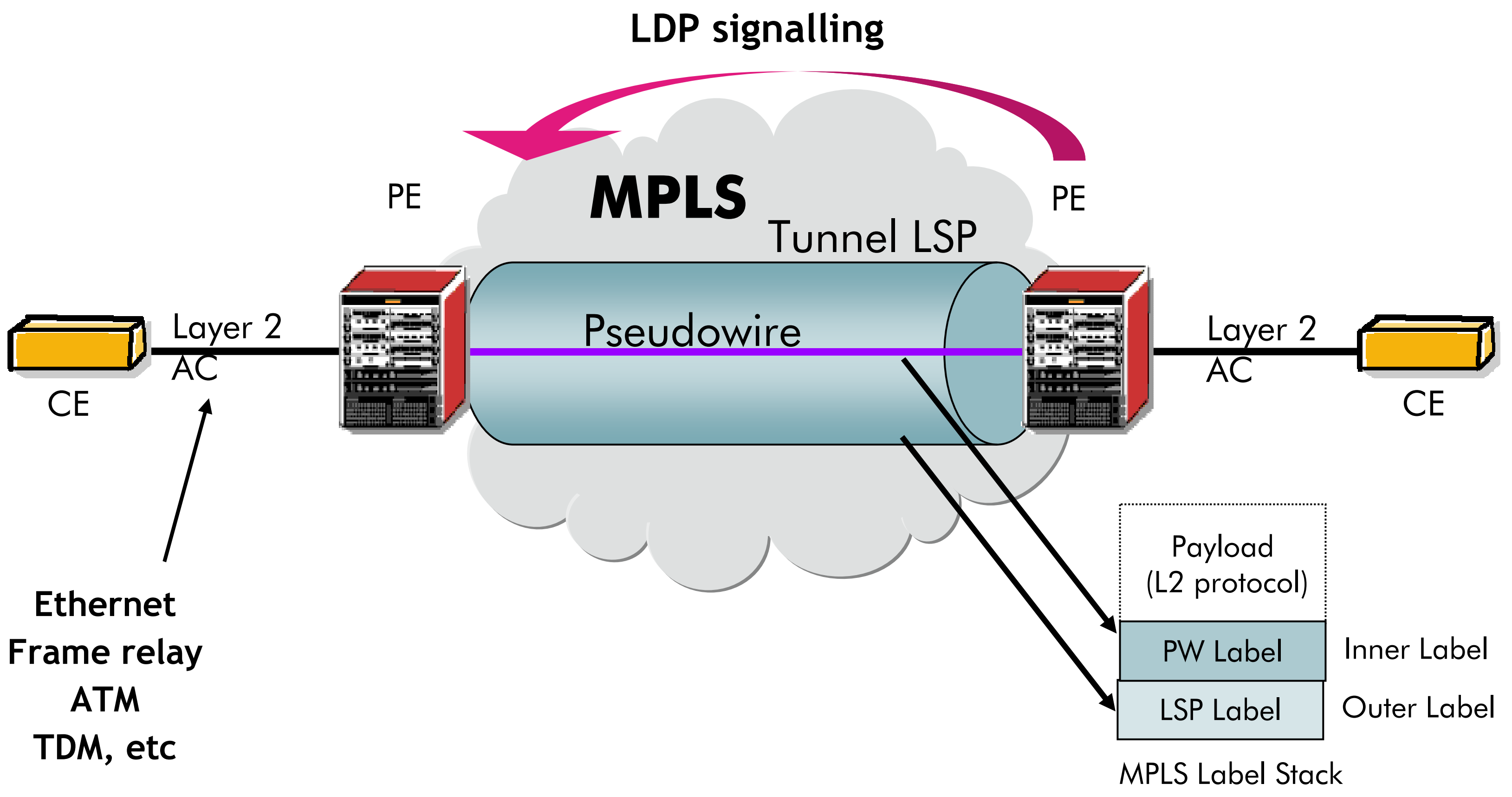
IETF RFC 4364

*MP-BGP : Multiprotocol BGP

Alcatel·Lucent

Layer 2 VPNs

Pseudowires are building blocks of layer 2 VPNs

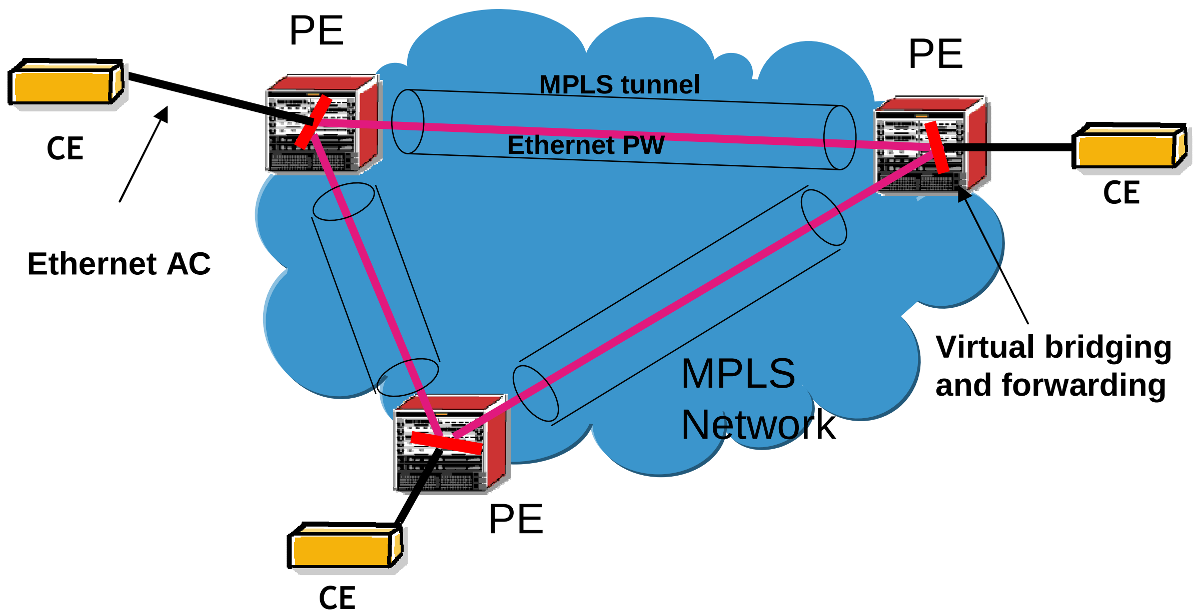


IETF RFC 3985

Virtual Private LAN Service (VPLS)

Transparent L2 VPN for Ethernet

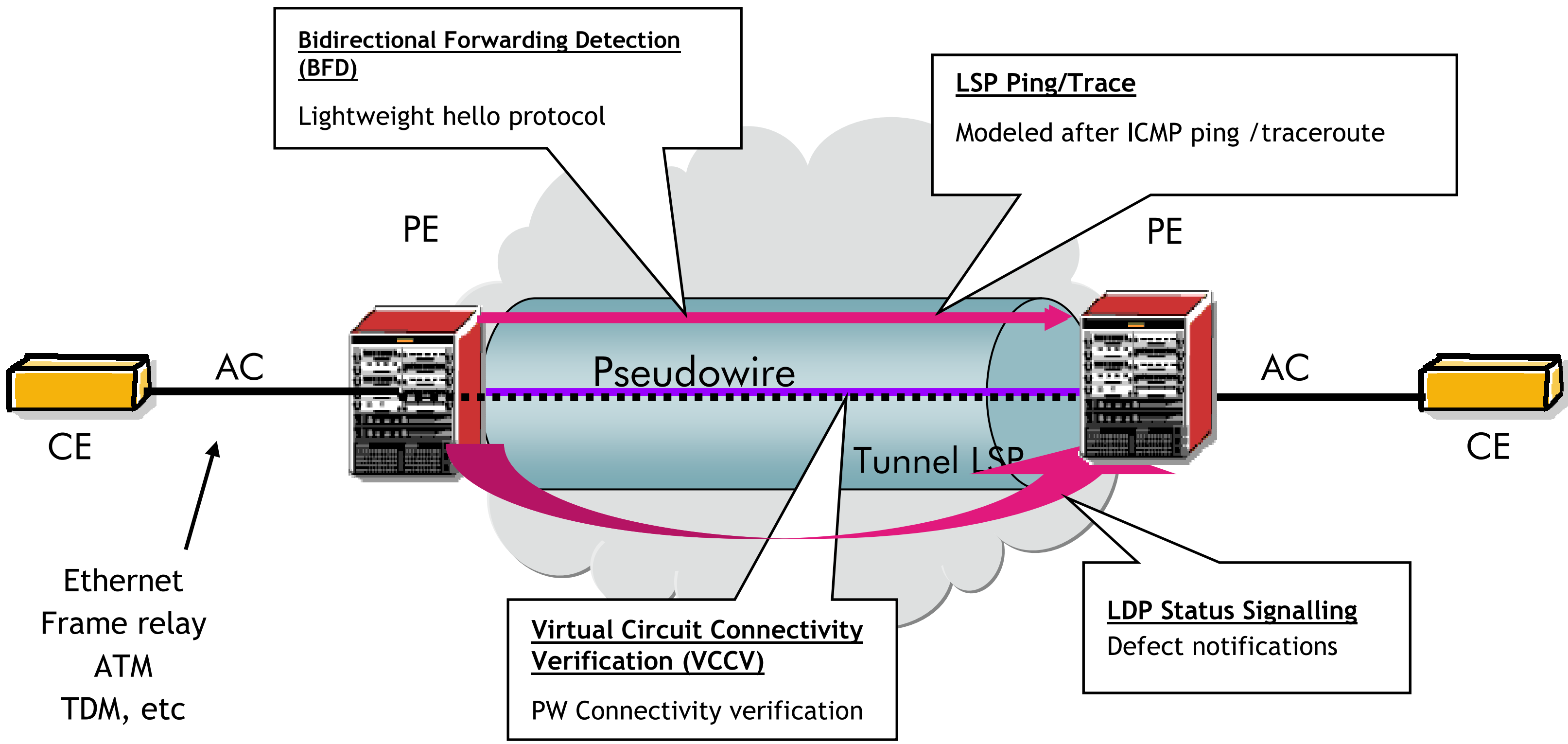
- Learns MAC addresses per PW
- Forwarding based on MAC addresses
- Split-horizon forwarding for loop prevention
  - Does not use Spanning Tree
- Uses hierarchy to improve scaling (H-VPLS)



IETF RFC 4762

OAM in a Converged MPLS Network

OAM tools for each layer of the converged network



Alcatel·Lucent

Summary: Why is MPLS Important?

MPLS adds label to a packet to enable it to be switched through a PSN

- Full set of TE, OAM, and protection mechanisms
- Enhance to support both Layer 2 and Layer 3 services

Core carrier networks moving rapidly to using MPLS

- Driven by expected lower CAPEX/OPEX of a converged network and demands of new servces
  - Ethernet services need MPLS QoS/TE/Protection
  - Enables Ethernet transport layer to support range of legacy (TDM, ATM…) and new services

www.alcatel-lucent.com