VPLS for Carrier Ethernet Services

Tim McSweeney

Product Manager

**Layer 2 VPNs & Network Access**

Agenda - GARR

Consortium GARR Network Topology

	10 Gbps
	2.5 Gbps
	1 Gbps
	622 Mbps
	155 Mbps
	34 Mbps
	Opt. Fiber

- **What Is Driving L2VPNs?**

- **Foundations**

  MPLS and GMPLS

  Pseudo Wires

- **VPLS Overview**

  Why Deploy VPLS?

  VPLS in a Nutshell

  Hierarchical VPLS and Autodiscovery

  Manageability and Cisco Service Delivery Models

- **Customer Deployment Profiles**
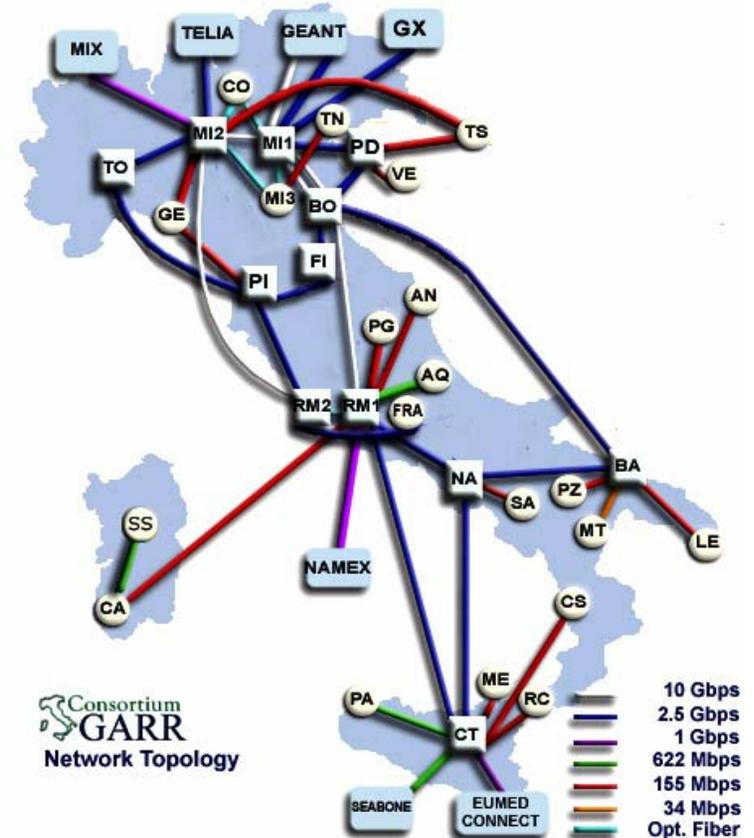
What Is Driving L2VPNs?
## The Ever Expanding Applications of Ethernet
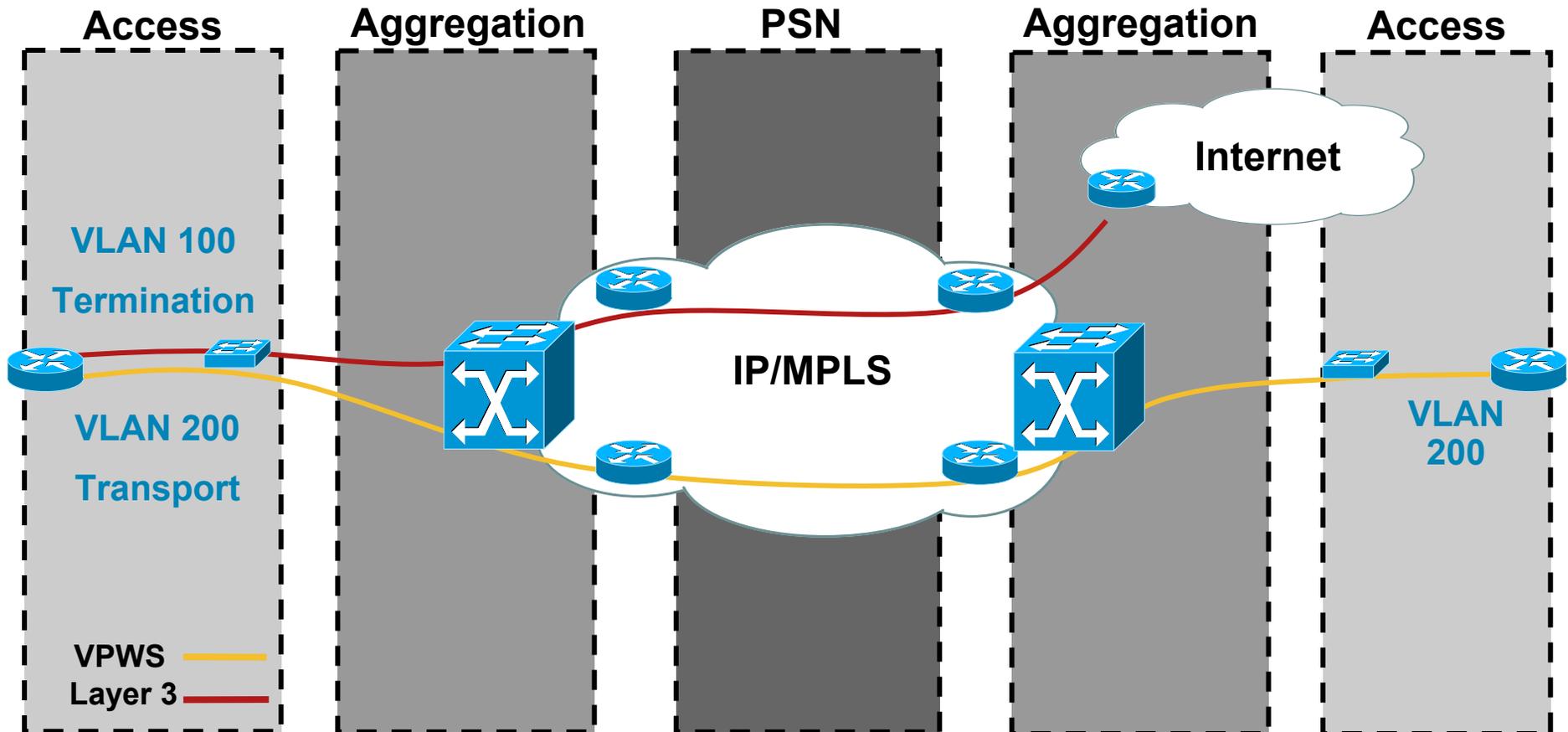
- **Fast becoming the access technology of choice**
- **Layer 2, Layer 3 and Internet services on a common port**
- **Extends the reach of metro area Ethernet networks**

L2VPN Taxonomy

L2VPN Models

VPWS
Virtual Private Wire Service
Point to Point

VPLS
Virtual Private LAN Service
Point to Multipoint

L2TPv3

AToM

MPLS Core

IP Core

MPLS Core

Ethernet

Ethernet	Ethernet
Frame Relay	Frame Relay
ATM (AAL5 & Cell)	ATM (AAL5 & Cell)
PPP & HDLC	PPP & HDLC
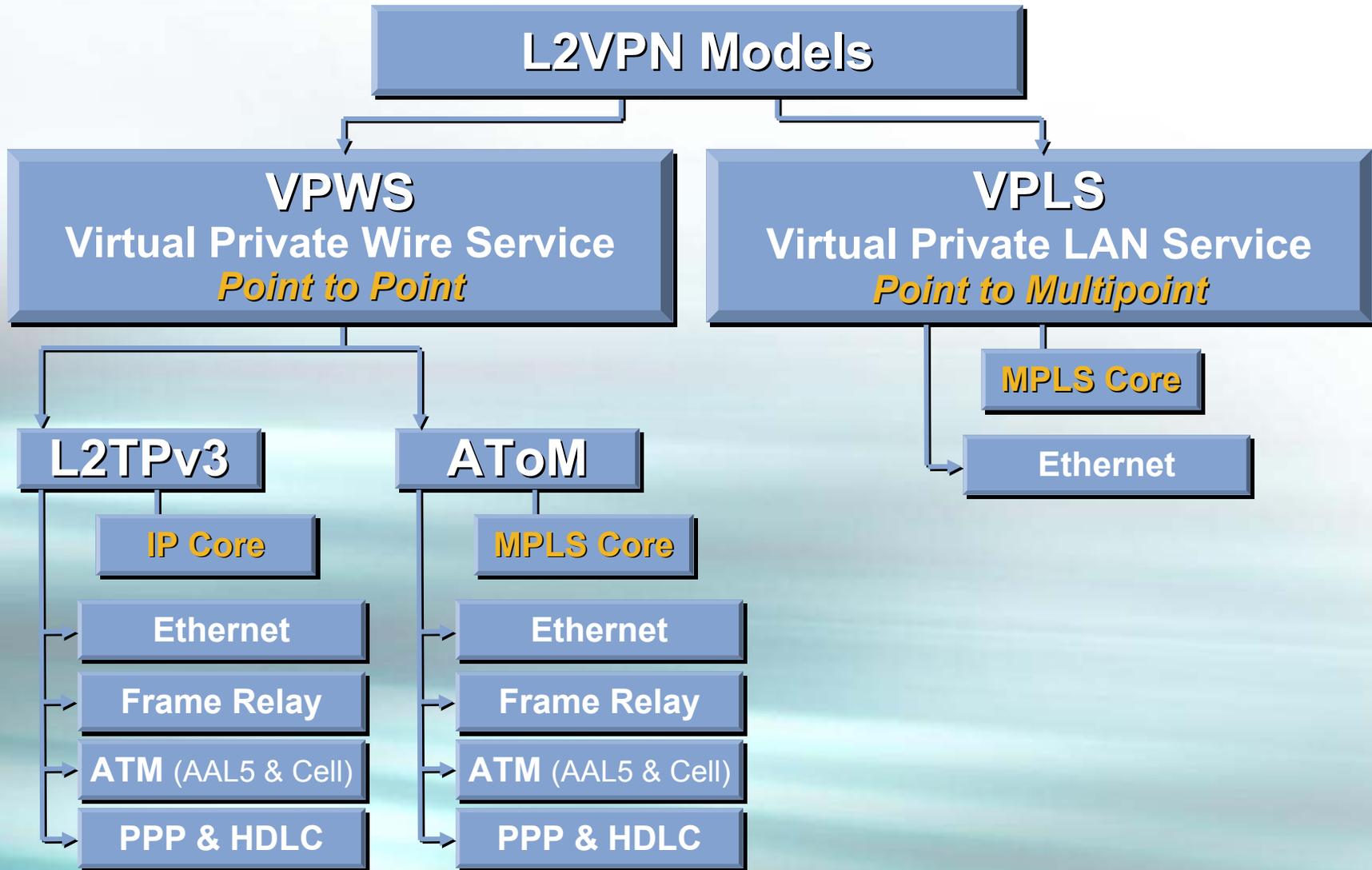
MPLS Operation Overview

3. Ingress Edge LSR receives and "labels" packets

4. LSR switches packets using label swapping

5. Egress Edge LSR removes label and delivers packet

Customer Site A

PE

P

P

PE

Customer Site B

1. Routing Protocols (OSPF, IS-IS) establish reachability to destination networks

2. Label Distribution Protocol (LDP) establishes label-to-destination network mappings

MPLS Encapsulation

One or More Labels Inserted into Packet Header

**PPP Header
(Packet over SONET/SDH)**

PPP Header	Label	Layer 2/L3 Packet

LAN MAC Label Header

MAC Header	Label	Layer 2/L3 Packet

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

Label – 20bits	EXP	S	TTL-8bits

EXP = Class of Service: 3 Bits; S = Bottom of Stack; TTL = Time to Live

MPLS VPN Security: Comparable to Frame Relay and ATM

- Miercom testing that proved that MPLS VPNs met or exceeded all of the security characteristics of a comparable Layer 2 VPN based on Frame Relay or ATM

- References

  RFC 4381: Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs), Feb 2006

  Cisco white paper: Security of the MPLS Architecture

  http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/mxinf_ds.pdf

Miercom
The leading edge in networking information

White Paper

Cisco MPLS based VPNs: Equivalent to the security of Frame Relay and ATM

March 30, 2001

Abstract: The purpose of this white paper is to present discussion and findings that conclude that Cisco MPLS-based VPNs are as secure as their layer 2 counterparts such as Frame-Relay and ATM. This document details a series of tests were carried out on a Cisco router test bed validating that MPLS based VPNs (MPLS-VPN) provide the same security as Frame-Relay or ATM.

ATM and Frame-Relay have a reputation in the industry as being secure foundations for enterprise connectivity. Essential items that make ATM and Frame-Relay a secure network were considered and tested on an MPLS-VPN.

- Address and routing separation equivalent to layer 2 models
- A service provider core network that is not visible to the outside world
- A network that is resistant to attacks

The test results show that MPLS-VPNs provide the previous features at or above the level of a layer 2 VPN such as Frame-Relay or ATM.

As described in greater detail through out this paper a test bed of 22 Cisco routers was used, including- two Cisco 12000 series Internet routers, two 7505s, four 7206 VXRs, five 3640s, five 2611s, and four 1750s running IOS version (12.0) and (12.1) to implement the necessary functions to provide a stable and secure MPLS core.

Copyright © 2001, Miercom
All rights reserved

410 Hightstown Road
Princeton Junction, NJ 08550
609-490-0200; fax 609-490-0610
info@mier.com www.mier.com

Source: Cisco MPLS based VPNs: Equivalent to the security of Frame Relay and ATM, Miercom, March 2001, http://www.miercom.com/_gfx/nav/acrobat.gif

GMPLS Overview

GMPLS provides Unified Control Plane across different layers

- GMPLS extends MPLS/MPLS-TE control plane

  GMPLS extends these control planes to support ANY class of interfaces (i.e. layers)

  Provides Bi-directional LSPs

- GMPLS supports 5 types of interfaces:

  PSC - Packet Switching Capable: IP/MPLS

  L2SC - Layer-2 Switching Capable: ATM, FR, Ethernet

  TDM - Time-Division Multiplexing: SONET, SDH, G.709 ODUk

  LSC - Wavelength Switching: Lambda, G.709 OCh

  FSC - Fiber Switching

- With MPLS-TE, GMPLS enables:

  Connection Protection/Restoration capabilities

  Separation between transmission, control and management plane

  Network management using SNMP (dedicated MIB)

Network Hierarchy: GMPLS/MPLS Integration

GMPLS Network - OTN

MPLS Network

MPLS Network

PE1

G-PE1

GMPLS LSP

G-PE2

PE2

MPLS LSP

GMPLS LSP

MPLS LSP

Ethernet Frame

MPLS Layer

MPLS Layer

GMPLS LSP Stacks

L1, L2, L3

GMPLS connection between PEs

MPLS Layer

GMPLS LSP Stacks

L1, L2, L3

Ethernet Frame

MPLS Layer

MPLS LSP between customer networks over GMPLS

VPLS connection between customers PEs
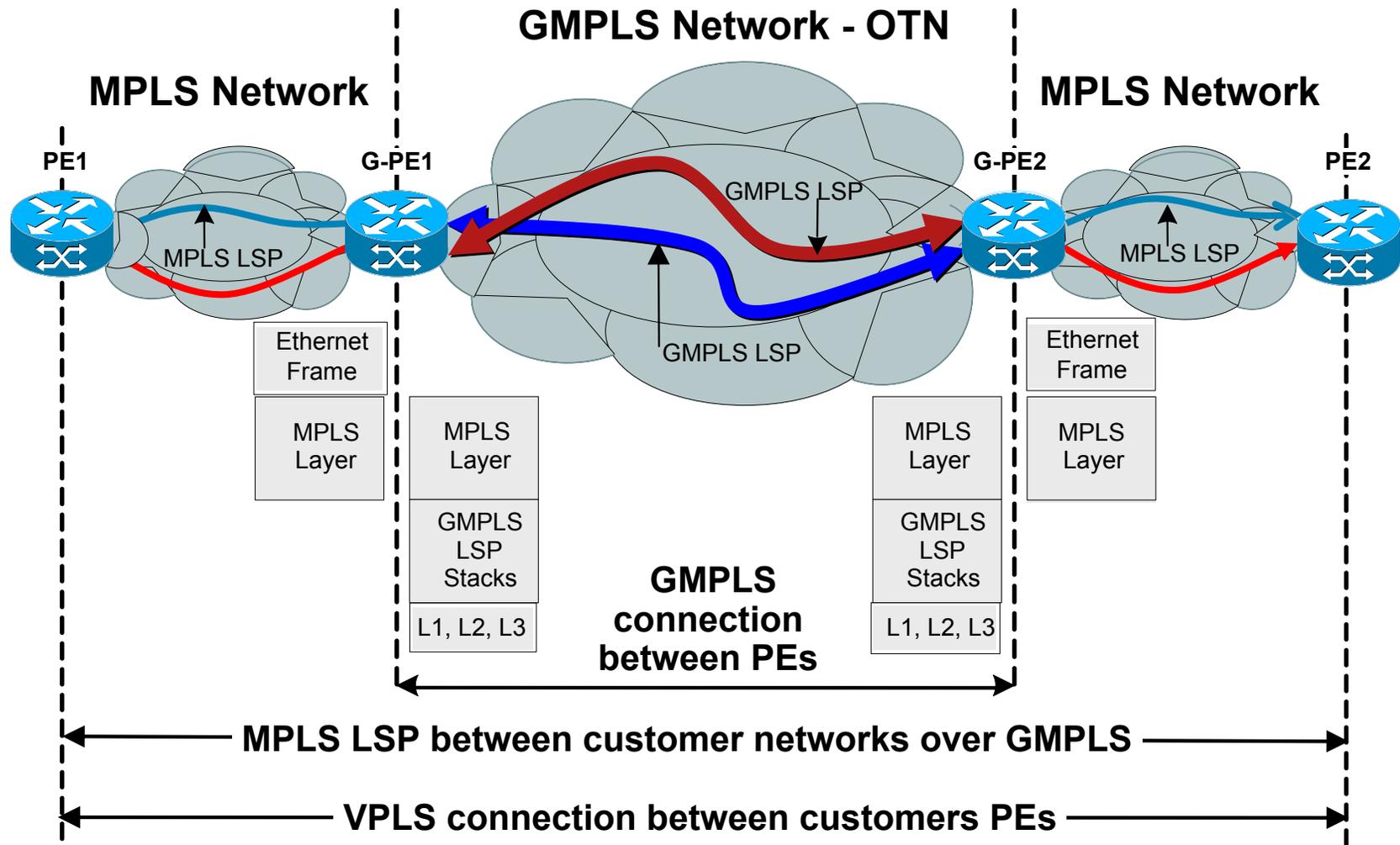
GMPLS/MPLS Integration

- Cisco actively involved in private and public interoperability (for example, ISOCORE – www.iscocore.com)
  - Main focus: IP/Optical integration – proof of concept and interoperability across GMPLS/MPLS layers
  - Optical Dynamic GMPLS LSPs signalled and advertised in the MPLS layer
  - L3VPNs, TE, VPLS, PW, Multicast services running over the GMPLS LSP
  - If you are interested let us know!!!
- GMPLS deployment
  - Service providers in Japan – have done testing and ready for deployment
  - Typical services: L3VPN, TE, PW

GMPLS available for customer evaluation on Cisco routers

- **Cisco CRS-1**
- **Cisco 12000**
- **Cisco 7600**

Pseudo Wires Enable… VPLS, AToM, L2TPv3

- Transport over non-Native Backbones

- Co-existence with other Encapsulations

- Service Interworking

SP Network

Bridged Ethernet over ATM

CE

EoMPLS Pseudo Wire

Ethernet example

Ethernet VLAN

CE
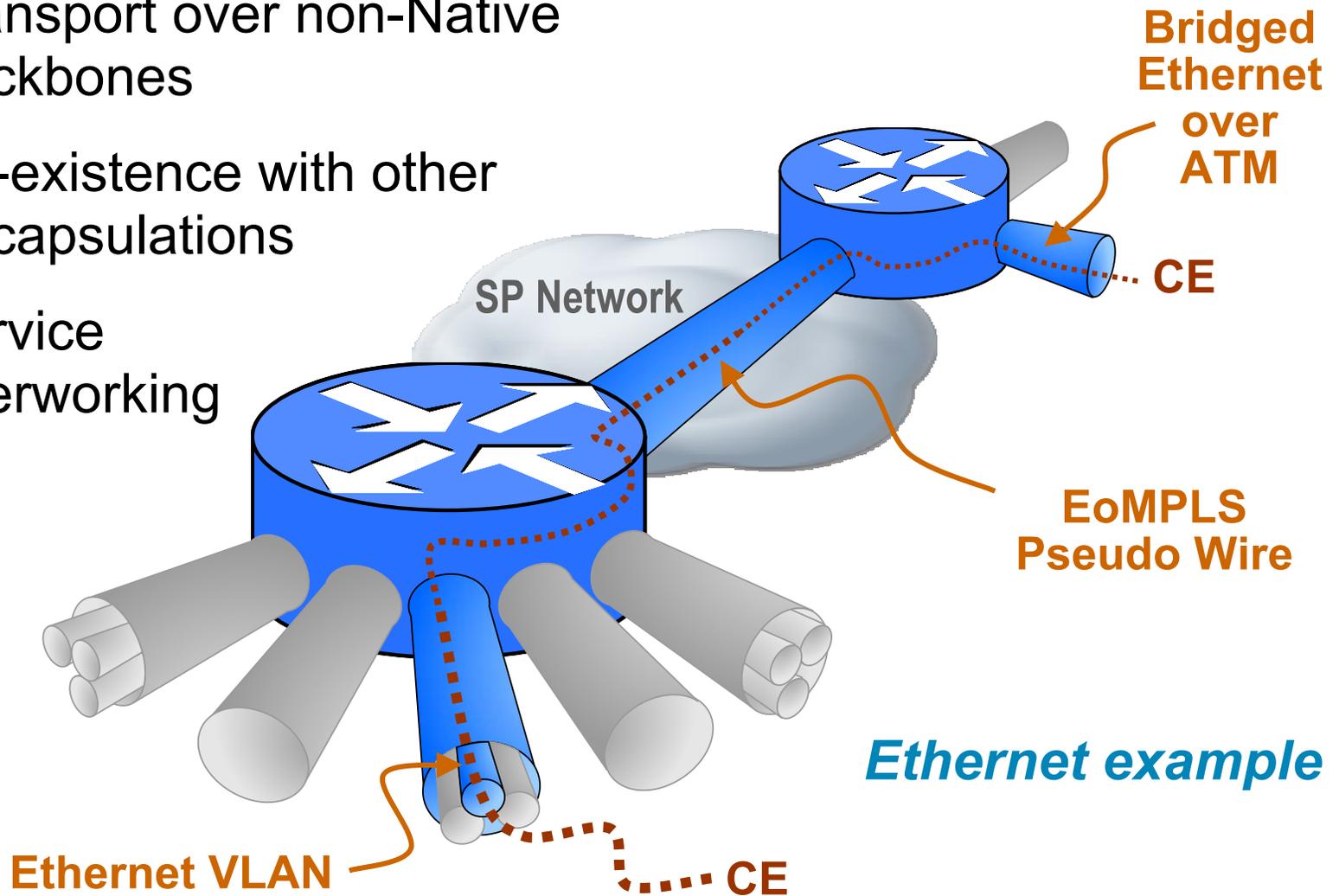
Why Deploy VPLS?

Feature	Benefits
MPLS core network emulates a flat LAN segment	▪ Overcomes distance limitations of Ethernet-switched networks → Offer Virtual Private LAN Services *Formerly called Transparent LAN Services (TLS)*
Extends Ethernet broadcast capability across WAN →Point to Multipoint Connectivity	▪ Connects each customer site to many or all other customer sites – A single CE-PE link transmits Ethernet packets to multiple remote CE routers – Fewer connections required to get full connectivity among customer sites → OpEx Savings
Multipoint plug-and-play provisioning	▪ Adding, removing or relocating a CE router requires configuring only the directly attached PE router → OpEx Savings

VPLS Reference Model
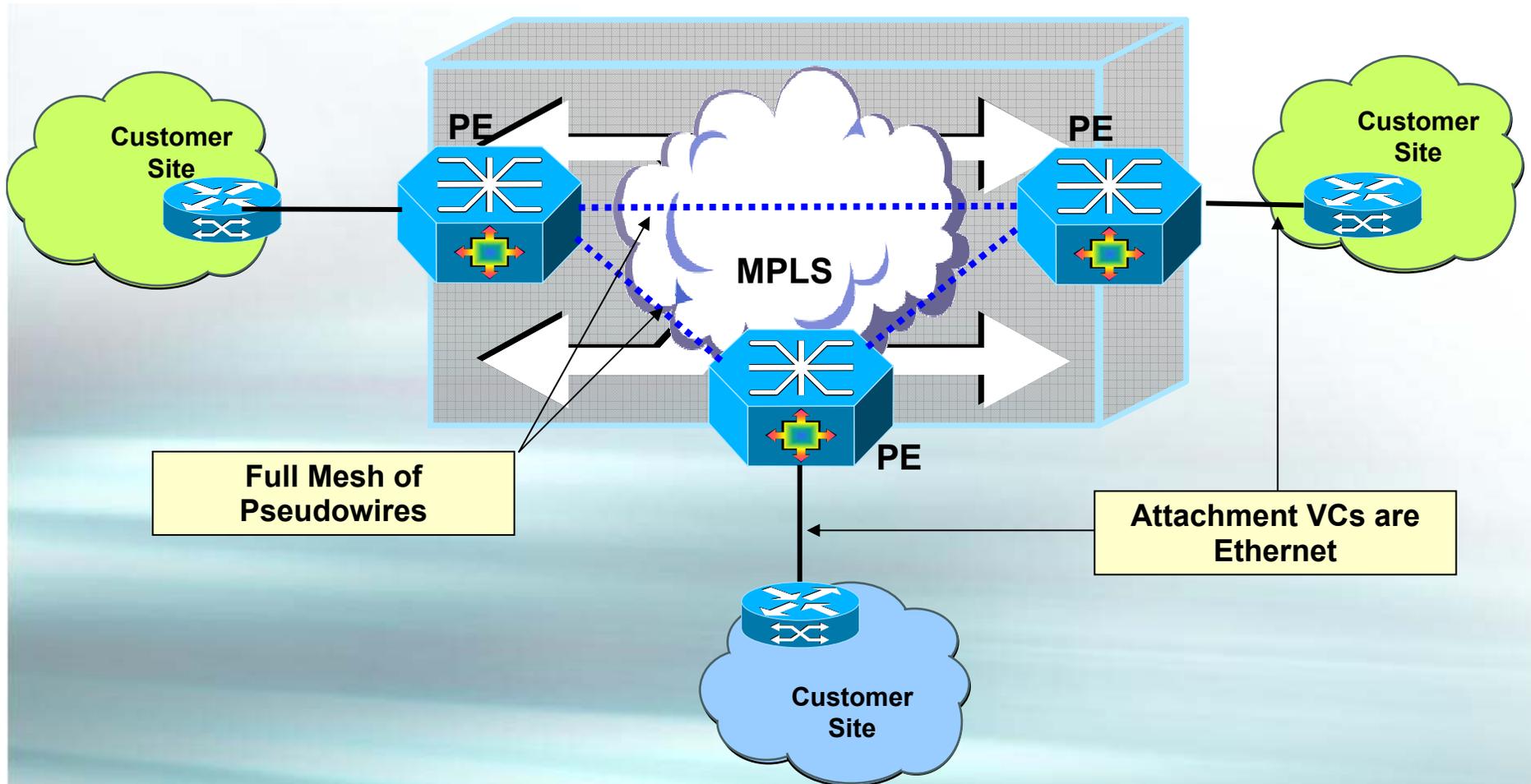
A full mesh of pseudo wires (PWs) is used to connect all provider edge (PE) devices which support a given VPLS VPN

VPLS and Hierarchical VPLS

VPLS

192.168.11

192.168.11.11/24

192.168.11.1/24

192.168.11.2/24
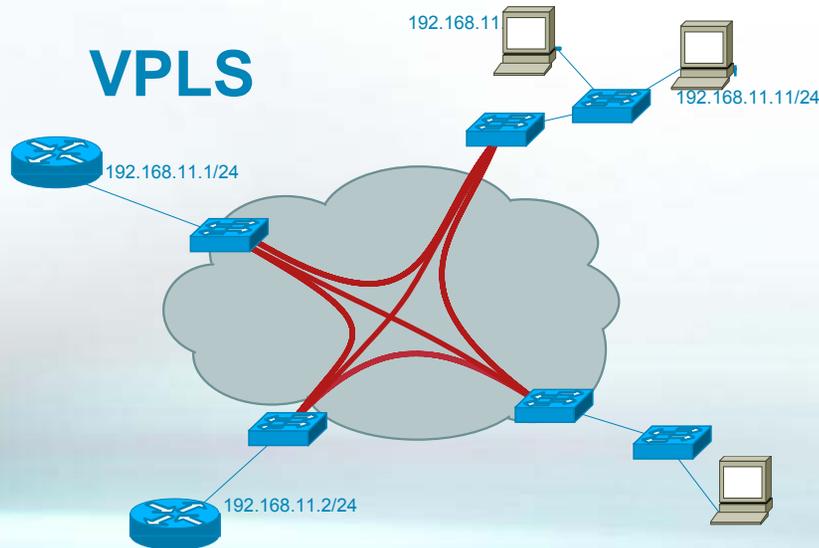
- **VPLS**
  - **- Single flat hierarchy**
  - **- MPLS to the EDGE**
  - **- MPLS Core**

- **Hierarchical VPLS**
  - **- Two (or More) Tier Hierarchy**
  - **- MPLS or Ethernet at the Edge**
  - **- MPLS Core**

H-VPLS

u-PE
PE-CLE
MTU-s

n-PE
PE-POP
PE-rs

n-PE
PE-POP
PE-rs

u-PE
PE-CLE
MTU-s

GE

PW

ETHERNET EDGE
Point-to-Point or Ring

MPLS CORE

MPLS EDGE
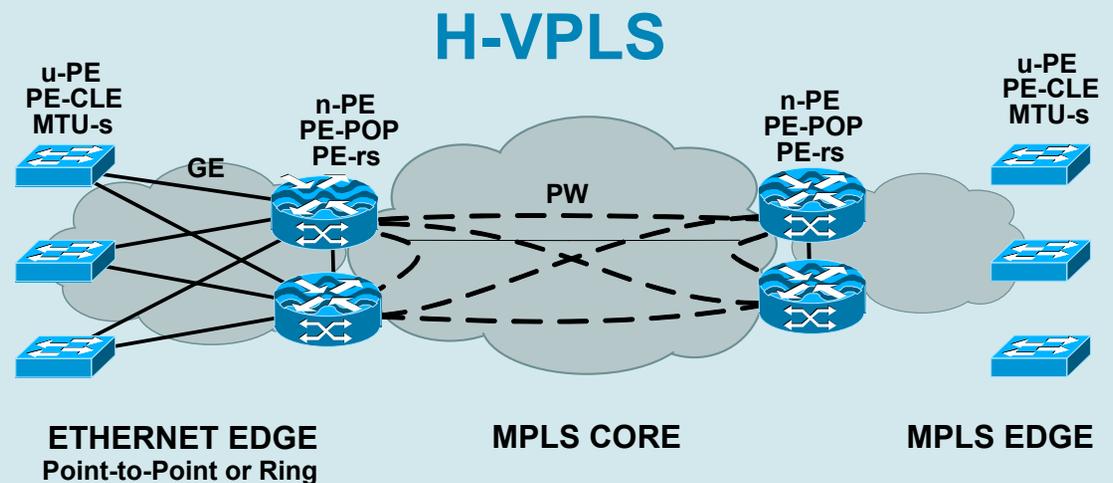
"Flat" VPLS Deployment Model: Customers Attach Directly to VPLS Service
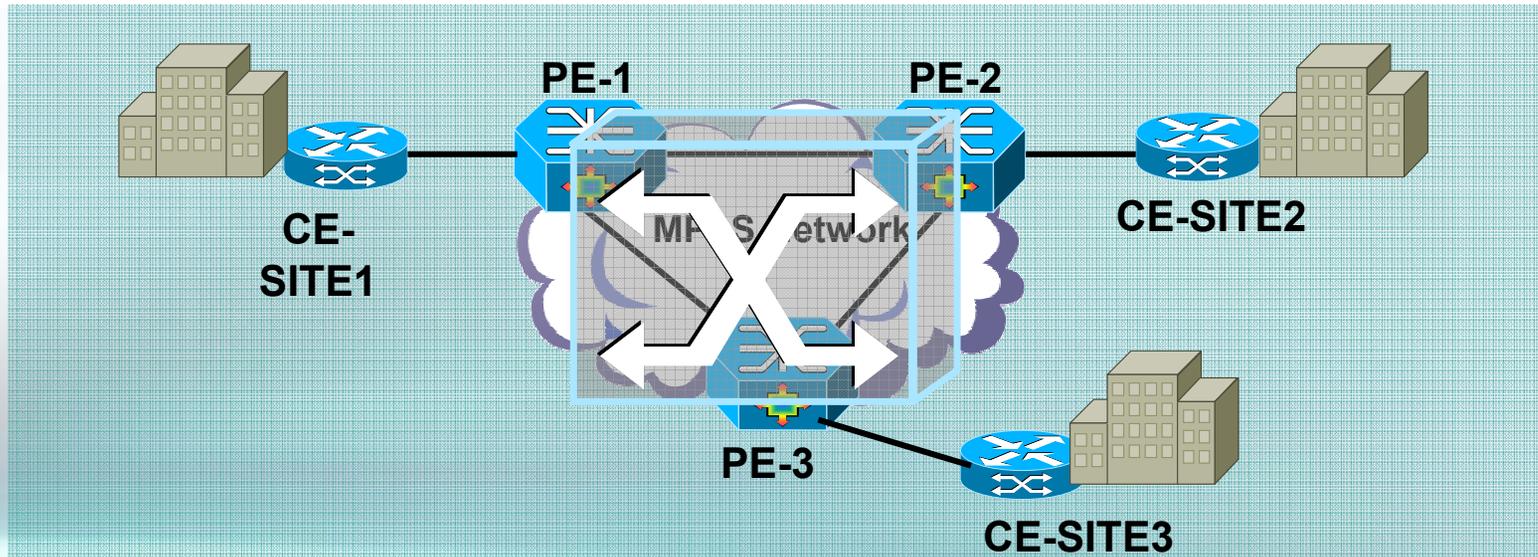
Description: Customers directly attach to VPLS service at Provider Edge

- **Suitable for small customer implementations**
- **Simple provisioning**
- **Full mesh of directed LDP sessions required between participating PEs**
- **VLAN and port level support (no QinQ)**

Challenge: Limited scalability

- **Full mesh causes classic scaling issue — N*(N-1)/2**

Hierarchical VPLS Deployment Model: Hub-and-Spoke
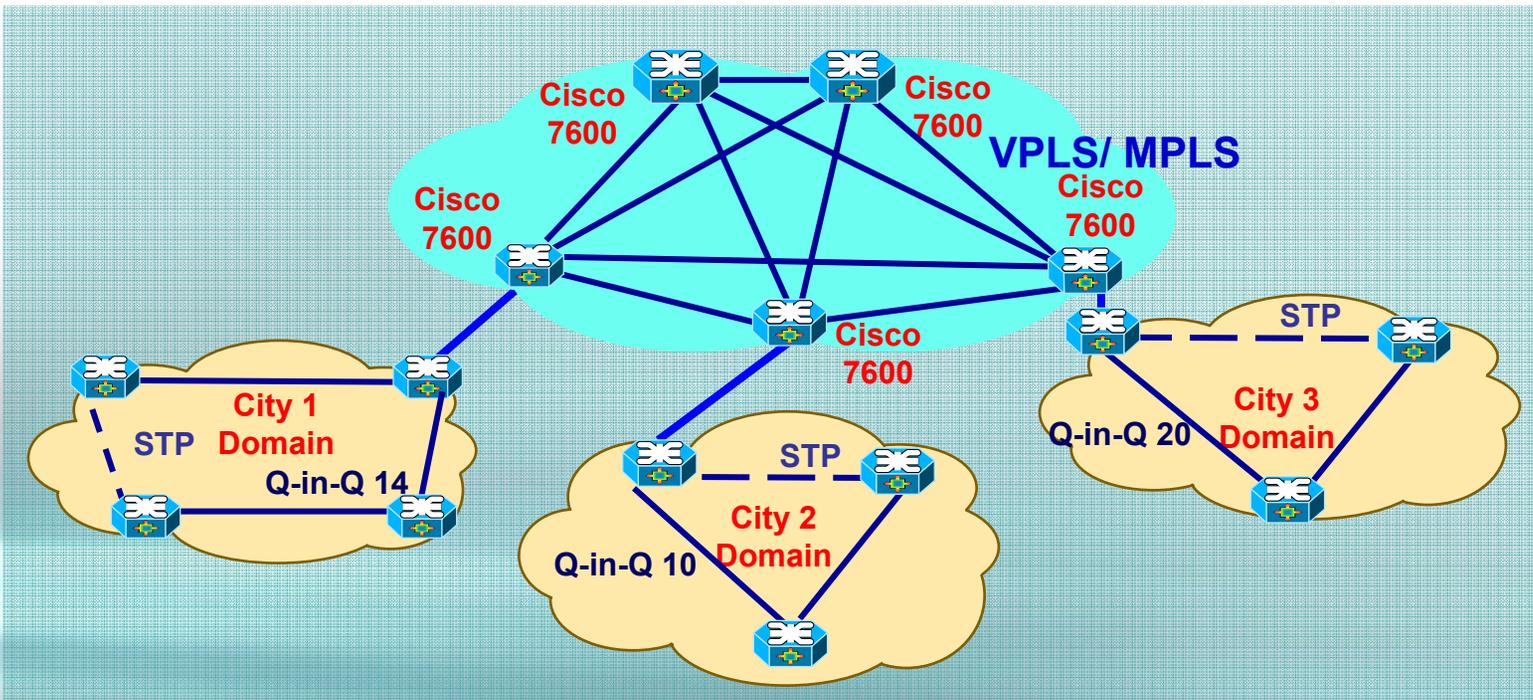
Description:
- **Customers attach to Regional Metro Ethernet networks**
- **VPLS links the Metro Ethernet Regions**

Benefit: Scales to support larger Ethernet deployments
- **Full mesh for core tier (hub) only**

A Comprehensive Solution: Robust, Flexible, Scalable, Manageable

VPLS Autodiscovery and Signaling

VPN Discovery	Centralized DNS Radius Directory Services	Distributed BGP

Signaling	Label Distribution Protocol
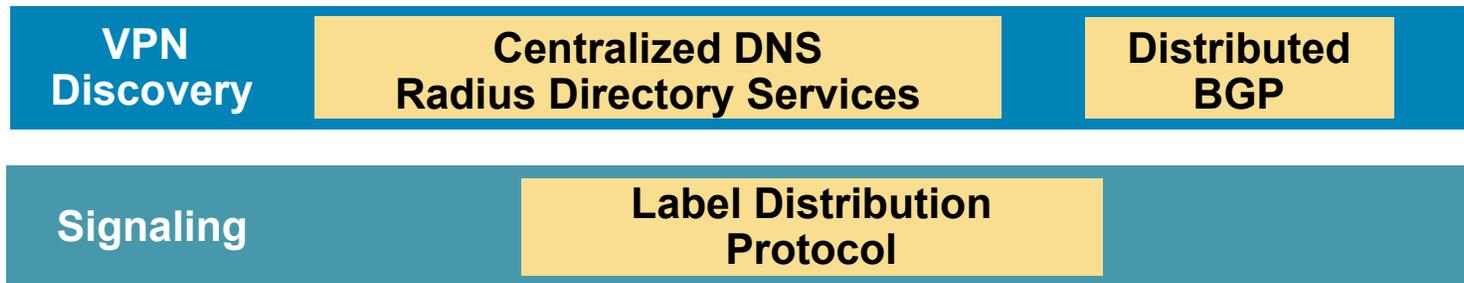
- **Autodiscovery: BGP is the configuration agent**

  True autodiscovery of VPN members (e.g., no need to explicitly list them)

- **Signaling: LDP sets up a standard PW**

  PWs signal other information such as attachment circuit state, sequencing information, etc.

  Cisco IOS supports targeted LDP for AToM and VPLS

Autodiscovery Configuration Steps
1. Establish BGP sessions & activate it for the L2VPN/VPLS address-family
2. Create VPLS instance & associated interfaces to it
3. (Optional) Establish import/export rules (or use the default mode)

Discovery & Signaling

- **Signaling & discovery are separable parts of L2VPN establishment**

    - Discovery (finding members of an L2VPN) is a point-to-multipoint task

    - Signaling (establishing the pseudowires) is a point-to-point task

- **By separating the tasks, you can choose a suitable protocol for each:**

    - LDP, L2TPv3 for PW Signaling

    - BGP, RADIUS, etc. for Discovery

LDP vs. BGP for PW Signaling

- For VPLS scaling, full mesh is not a significant problem

- LDP provides lighter-weight solution

LDP	BGP
Point-to-Point Information Only	Broadcasts All Information to All Peers
No Policy	Complex Policy, Often Changing Information Advertised
Mostly Idle	Can Have Significant Churn Due to Broadcast

Pseudowire Redundancy:
Protects from Key Potential Faults
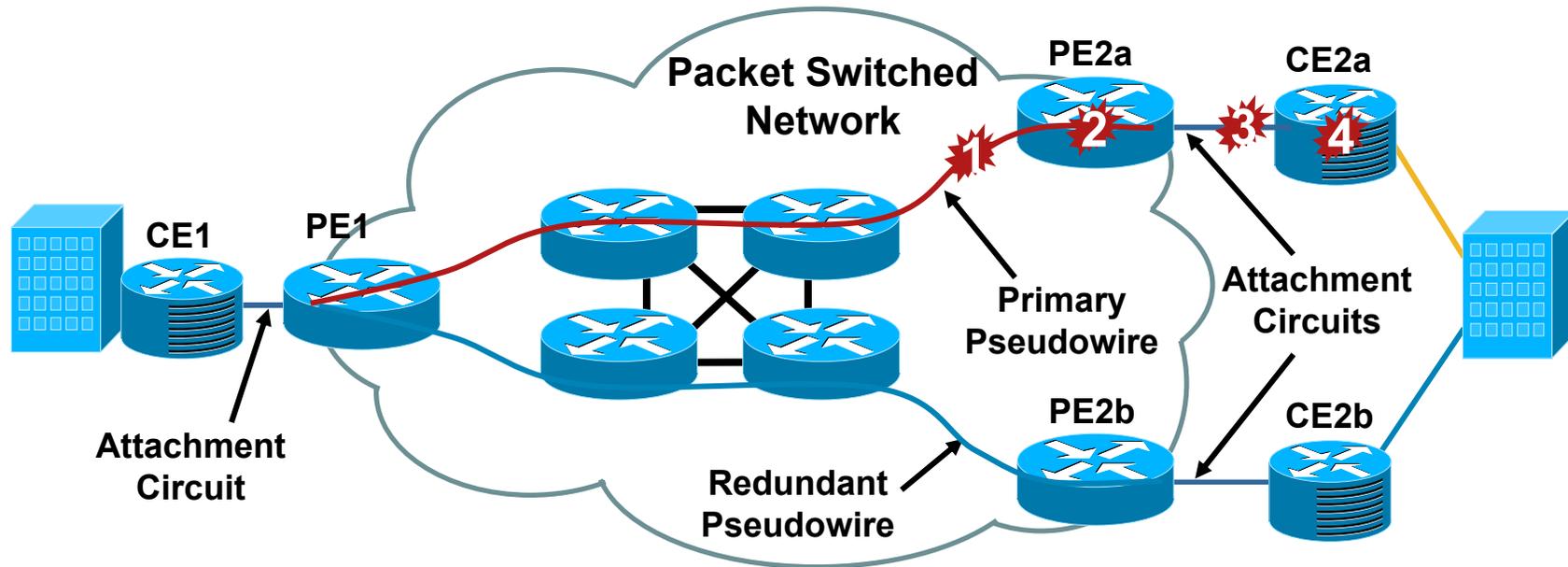
Protects from fault in four key areas

1 PSN failure due to end-to-end routing failure

2 PE failure due to HW or SW fault

3 Attachment circuit failure due to line break

4 CE failure due to HW or SW fault

Inter-Autonomous System Pseudowires
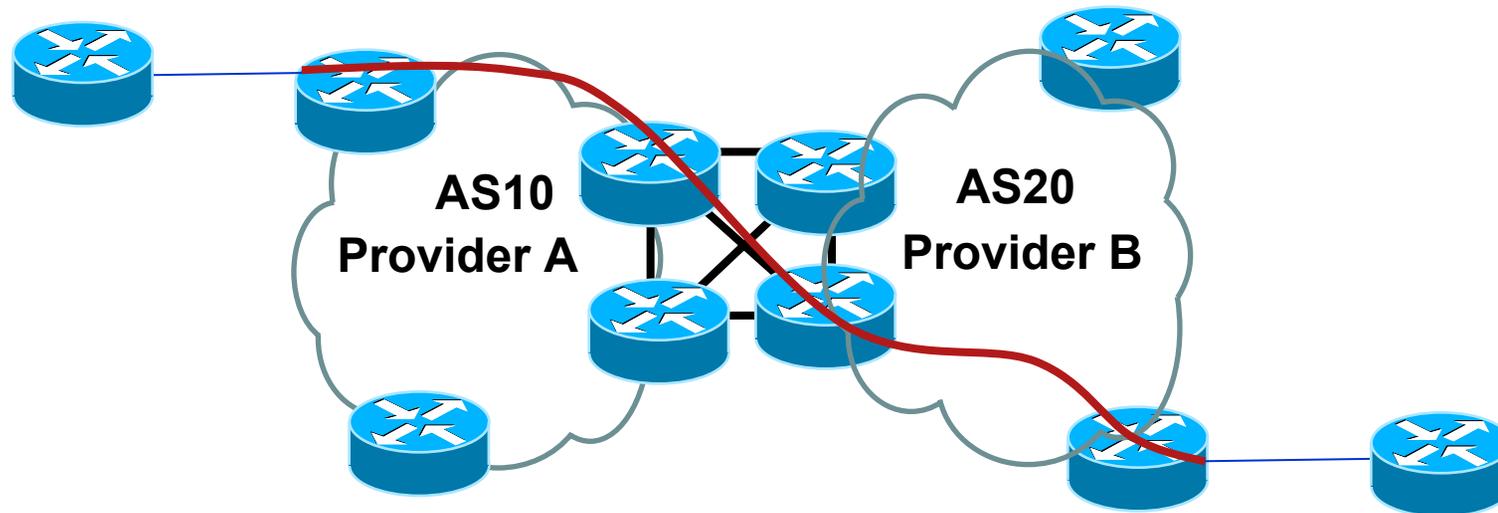
- **Inter-Autonomous System (Inter-AS) model: When a pseudowire spans at least 2 different service provider or administrative domains**

Goal:

- **Extend end-to-end pseudowire deployment across multiple ASes using VPLS**

Inter-Autonomous Systems: Pseudowire Switching

AS10 Provider A

AS20 Provider B
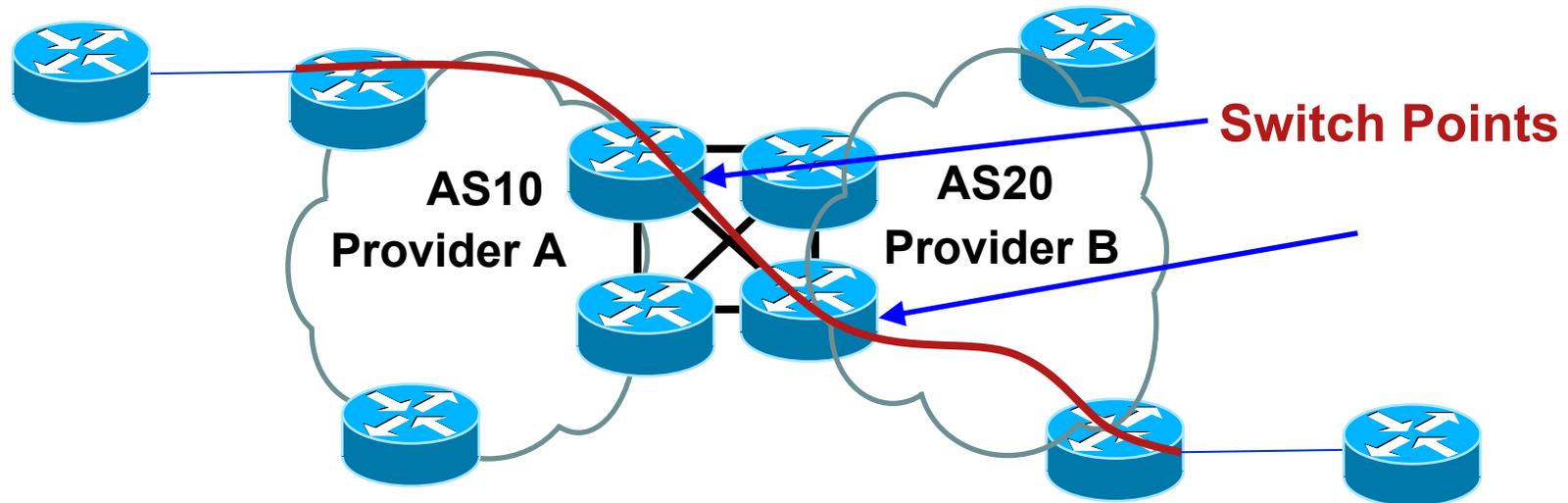
Switch Points

- **Pseudowire switching interconnects pseudowires belonging to different autonomous systems, thus providing an end-to-end path**
  - **Switch point refers to the ASBR where pseudowire switching is performed**
  - **Achieved through inter-working of data and control planes at the switch point**

Pseudowire Switching Model

attached-circuit 3

attached-circuit 1

pwvc 11

PE-1

AS 1

PE-3

pwvc 111

pwvc 151

pwvc 112

AS 2

PE-2

pwvc 12

ASBR-1

ASBR-2   pwvc 152

attached-circuit 4

PE-4

attached-circuit 6

attached-circuit	pseudo-wire	pseudo-wire	pseudo-wire	attached-circuit
L2 signalling (UNI)	LDP / L2TPv3	LDP/L2TPv3	LDP / L2TPv3	L2 signalling (UNI)
	VPWS	VPWS	VPWS	
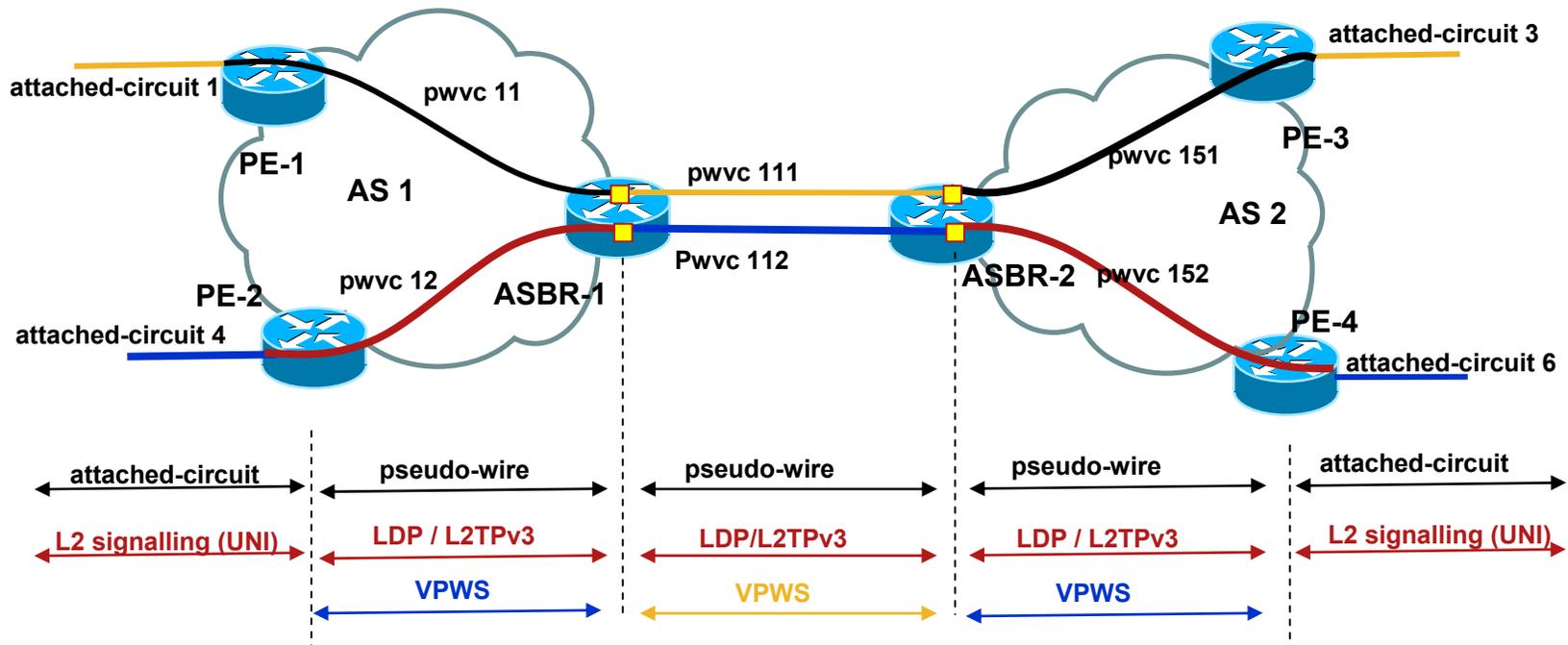
- **Pseudowires that comprise the end-to-end solution can be of the same (VPLS-to-VPLS) or different types (VPLS-to-AToM)**

- **Each pseudowire segment can independently employ draft-martini or L2TPv3 signaling and encapsulations**

- **The ASBRs are responsible for "cross-connecting" the pseudowire control channels and pseudowire data planes**

# Manageability & Cisco Service Delivery Models

Unified L2 VPN Management

Cisco IP Solution Center
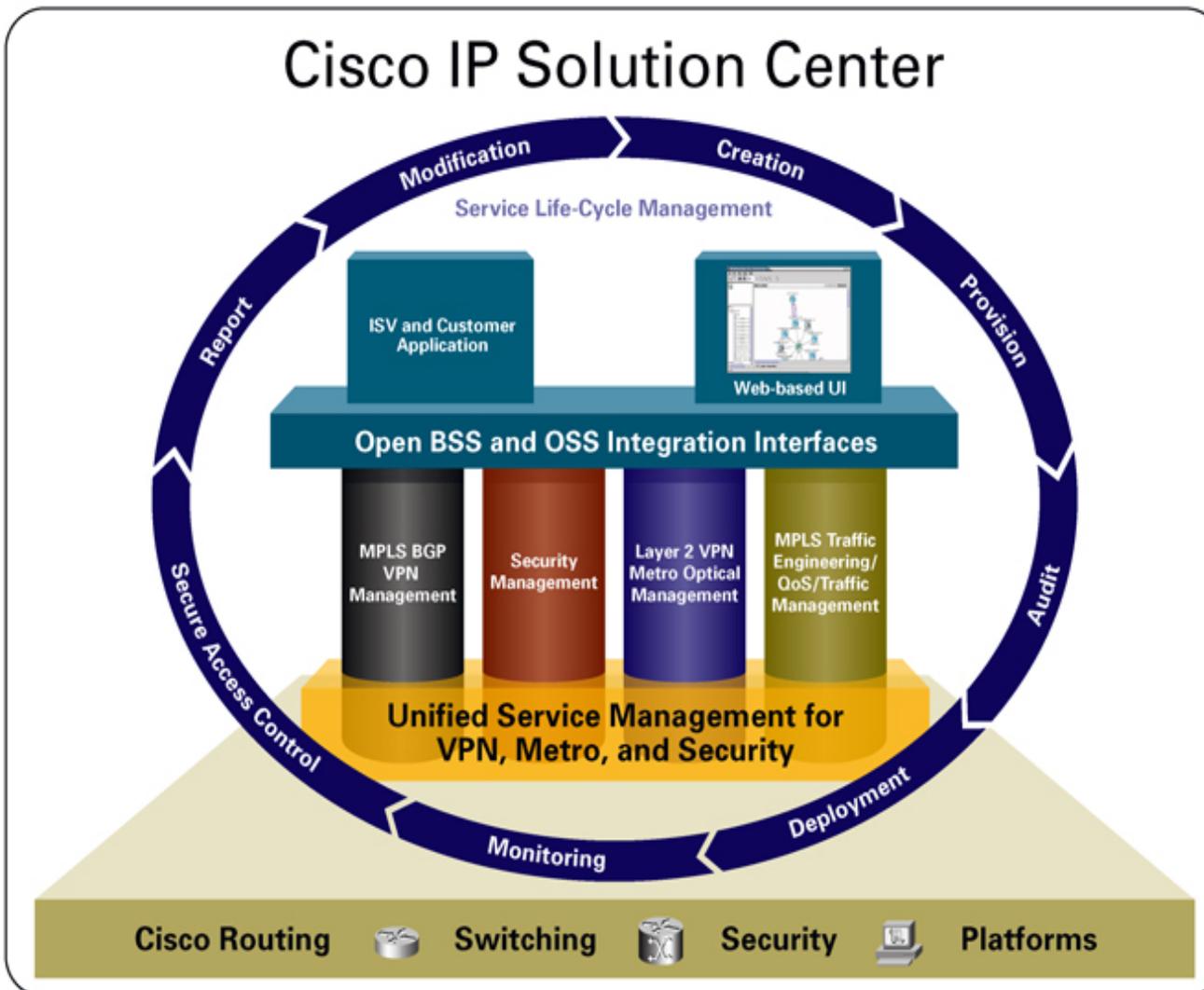
Integrated network management platform to manage:

- **Metro Ethernet Services** (switched as well as Ethernet transport over MPLS Core) services.

- **MPLS BGP VPN** services

- **AToM** (ATM/FR transport over MPLS) services

- **DiffServ/IP/ MPLS CoS** treatment for MPLS services above

Business Ethernet Services Architecture

Service

EoMPLS PW

Business L3 VPN
- Port, 1:1 VLAN — Ethernet / QinQ — **MPLS-VPN** — *Ethernet UNI*
- Port, 1:1 VLAN — **MPLS NNI**

Business E-LAN
- Port, 1:1 VLAN — **VPLS** — *Ethernet UNI*
- Port, 1:1 VLAN — **H-VPLS** — *MPLS NNI*

Business E-LINE
- Port, 1:1 VLAN — *Ethernet UNI*
- Port, 1:1 VLAN — *MPLS NNI*

Efficient Access	*Large Scale* Aggregation	*Intelligent* Edge	*Multiservice* Core

MSE

Access Node

Aggregation Node
E-MSE for MPLS NNI

Distribution Node

MSE

DSL, Ethernet | **MPLS / IP** | **IP, MPLS** | **MPLS**

VPLS Deployment Profiles

VPLS for Service Differentiation and Revenue Growth

PCCW (Hong Kong)

- Leading telecommunications provider
- Deployed VPLS on 28 C7600 Series routers & Catalyst 3750-ME switches

News@Cisco
News Release

Cisco Delivers IP NGN Convergence with Carrier Ethernet

New products and features strengthen Cisco's leadership in Triple Play and Business-Class IP services

LAS VEGAS (Telecom '05) - October 25, 2005 - Cisco Systems ® today solidified its global leadership in the Carrier Ethernet market by introducing new platforms and service-enabling features that will help service providers reach new markets, offer differentiated new services, and help them increase their business through additional revenue streams, while improving their efficiency of existing operations.

PCCW Limited, the leading communications provider in Hong Kong, deployed a combination of Cisco 7600 Series routers and Cisco Catalyst 3750 Metro Ethernet switches to build its VPLS network. PCCW's VPLS architecture allowed it to converge a number of different services into one network.

"PCCW is pleased to have deployed the Cisco VPLS Carrier Ethernet solution for the provision of our next generation data services," said Larry Wong, Director of Marketing and Products of Commercial Group, PCCW Limited based in Hong Kong. "Cisco's VPLS Carrier Ethernet technology allows us to create service differentiation and increase revenue growth in the enterprise and commercial markets, as it enables flexible bandwidth utilization, service customization, multiple connectivity, and high level of QoS and availability."

VPLS for Scalable Ethernet Services

- ## WebPartner (Denmark)
  - VPLS-based Ethernet broadband services
  - Cisco Catalyst 6500 series switches

LIGHT READING

WebPartner Deploys Cisco Switches

APRIL 27, 2005

SPONSORED BY

PR Newswire
United Business Media

COPENHAGEN -- Cisco Systems(R) (NASDAQ:CSCO) today announced that Danish Ethernet service provider WEBPARTNER is deploying Cisco IOS MPLS Virtual Private LAN (VPLS)-based Ethernet broadband services using the Cisco Catalyst(R) 6500 series switch. In a related announcement, WEBPARTNER also today announced that SBS Radio A/S, which is behind the radio stations The Voice and Radio2, is consolidating the networking for its Danish operations onto this multipoint Ethernet service.

VPLS provides a way for service providers to deliver scalable Ethernet services to support multiple branch locations over a common central infrastructure. "In contrast to traditional Layer2 VPN Services like Frame-relay & ATM, WEBPARTNER is now able to offer Layer2 VPN services to its customer base without needing to establish multiple site to site VPN mesh connections for each customer location." This will help WEBPARTNER to simplify the management of its Ethernet services as well as reduce operational costs, in order to help deliver services to a broader range of customers.

"We evaluated a number of technologies to support our service rollout, but decided that Cisco's approach to VPLS offered us a very scalable way to take advantage of our existing understanding of Cisco equipment and software to deliver new Layer 2 Ethernet-based VPN services to our customers," commented Nicolaj Ottsen, Chief Technical Officer of WEBPARTNER. "As our customers converge more services onto their internal networks, they need a broadband solution that can scale to support growing bandwidth requirements, as well as greater simplicity in their WAN connectivity."

VPLS Customer Deployment Profiles

- ## SP (USA)
  - VPLS used to link 16 Metro Ethernet regions
  - Deployed 80 C7600 running VPLS

- ## Financial (USA)
  - Deployed VPLS in November 2004
  - Provides integrated information and technology applications in the global financial services industry

- ## SP (Brasil)
  - Developing rollout of triple play services to the DSL and Metro Ethernet market in the city of São Paulo
  - Network has independent Layer 2 aggregation domains interconnected via pseudowires for customers that need to cross domains
  - Will use TE and Pseudowire Redundancy on the inter-domain connections

VPLS Customer Deployment Profile

- **SP (North America)**
  - Converting existing Layer 2 access and aggregation Metro Ethernet service offering to complete VPLS
  - Objectives:
    - Minimize spanning tree domain
    - Unify routing scheme so VPLS endpoints and multicast video share the same paths
    - Simplify troubleshooting by not having divide troubleshooting between L2 and L3 expert teams
    - Unify QoS, routing, and convergence policies across all services