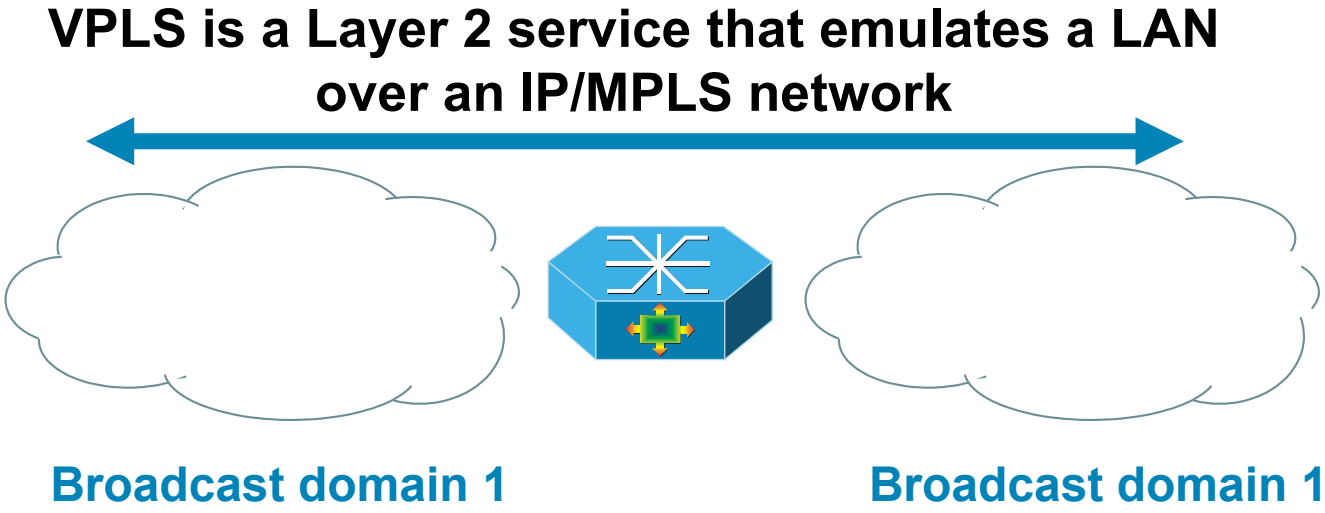
Virtual Private LAN Service (VPLS)

- What is VPLS?
- What Is Driving VPLS?
- Why Deploy VPLS?
- VPLS Features

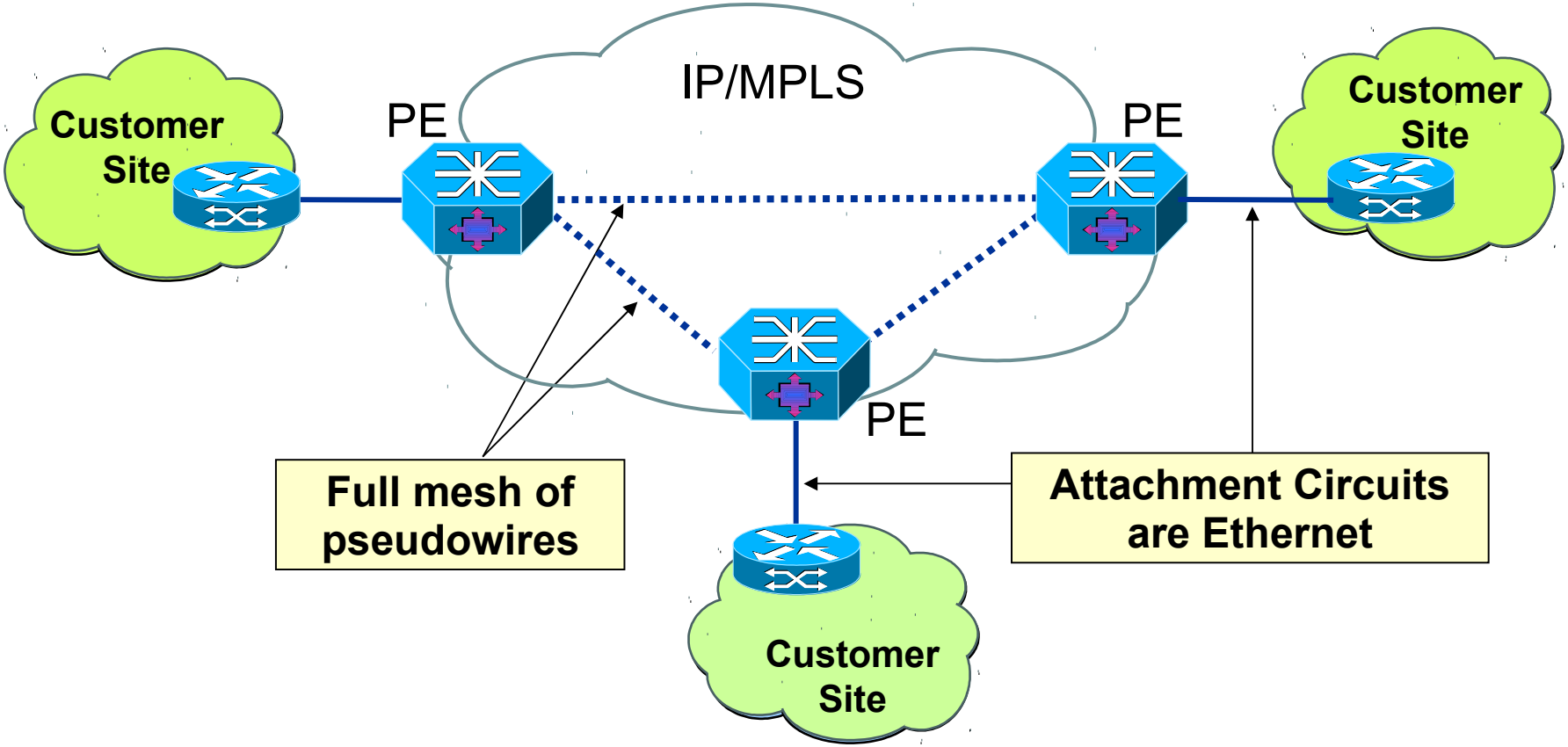
Introduction
Virtual Private LAN Service (VPLS)

- What is VPLS?



- VPLS extends the Ethernet broadcast domain between potentially geographically distant LAN segments
- Allows standard Ethernet devices communicate with each other as if connected to a common LAN segment

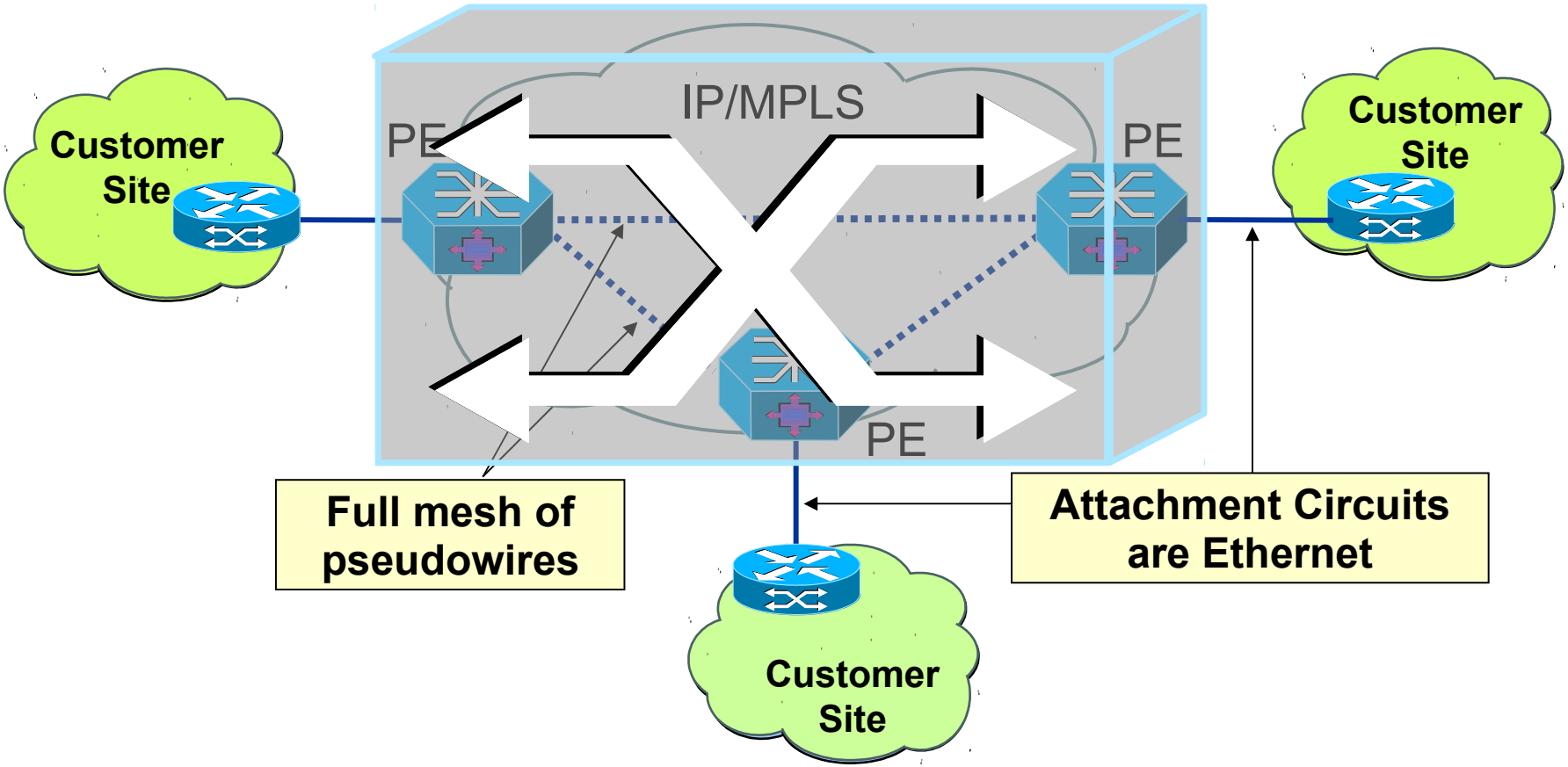
VPLS Reference Model



- The set of PE devices interconnected via PWs appears as a single emulated LAN to a customer

Ref: RFC 4762 Virtual Private LAN Service over LDP, January 2007

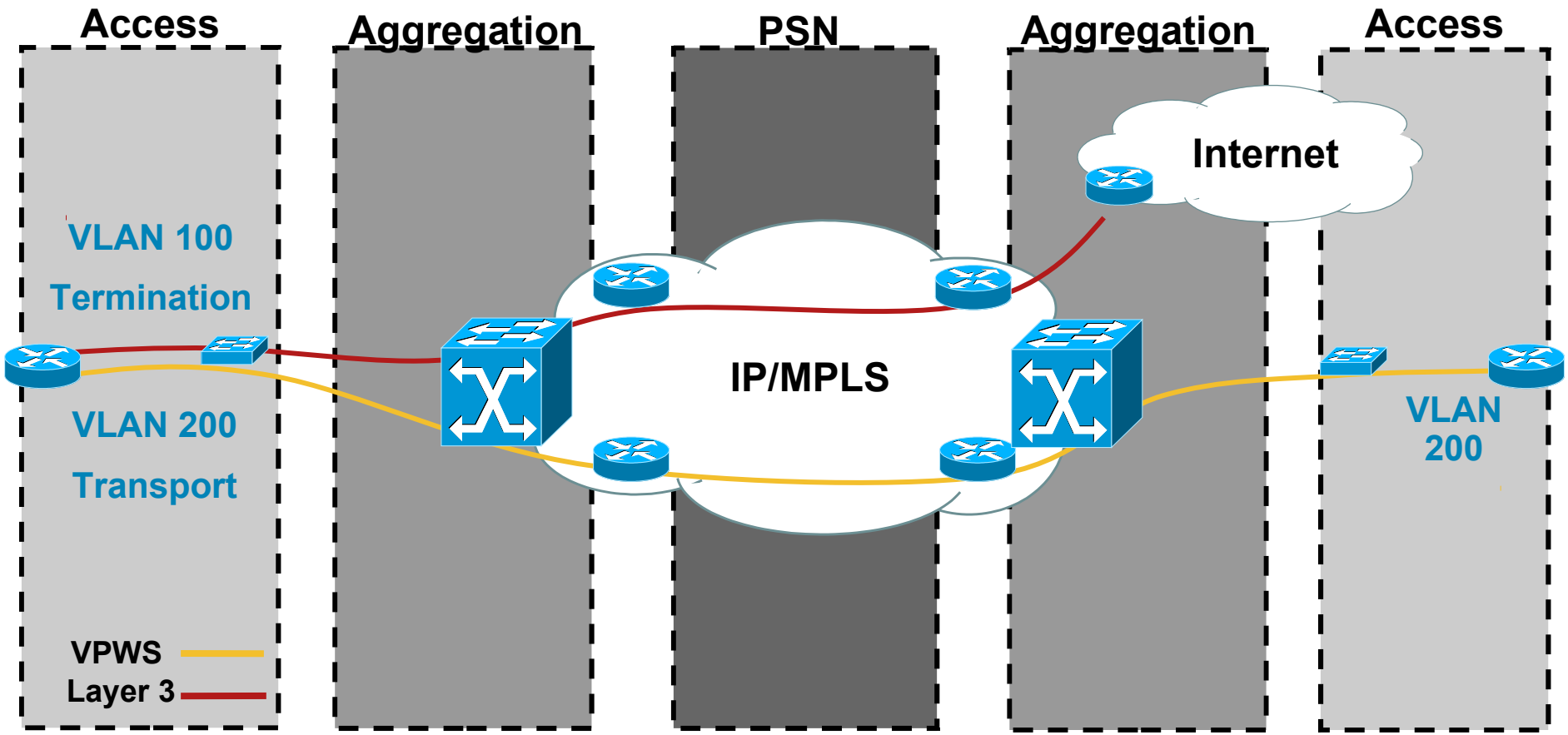
VPLS Reference Model



- The set of PE devices interconnected via PWs appears as a single emulated LAN to a customer

Ref: RFC 4762 Virtual Private LAN Service over LDP, January 2007

What Is Driving VPLS?
The Expanding Use of Ethernet

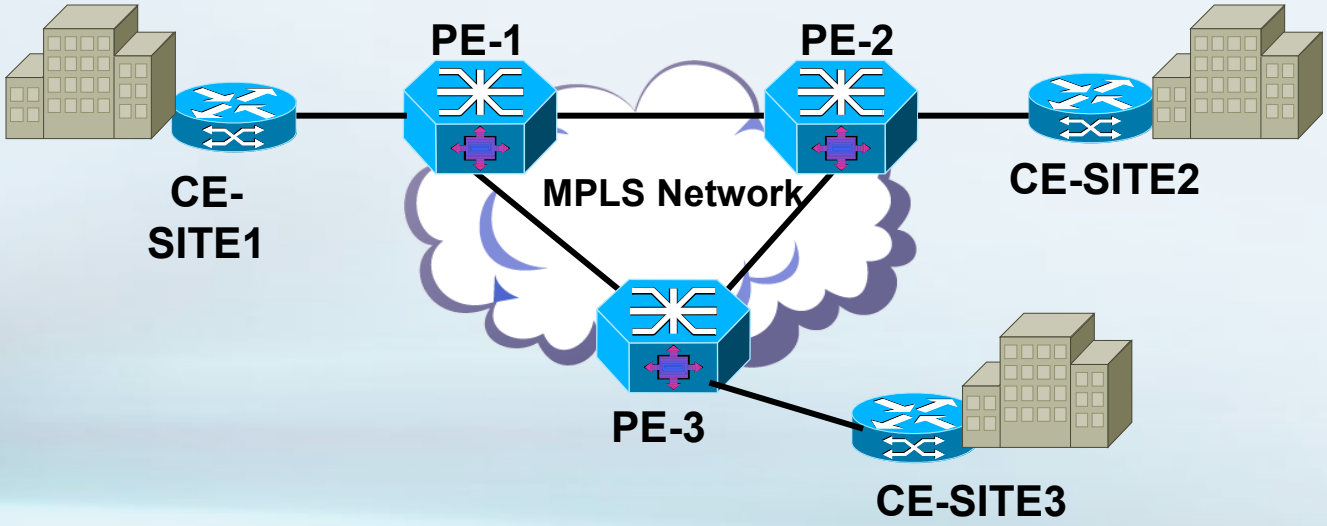


- **Ethernet: Fast becoming the access technology of choice**
  - **Layer 2, Layer 3, and Internet services on a common port**
- **VPLS: Extends the reach of Metro Area Ethernet networks**

Why Deploy VPLS?

Feature	Benefits
MPLS core network emulates a flat LAN segment	▪ Overcomes distance limitations of Ethernet-switched networks → Enables Virtual Private LAN Services ▪ Customers maintain routing and administrative autonomy
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

“Flat” VPLS Deployment Model: Customers Attach Directly to VPLS Service



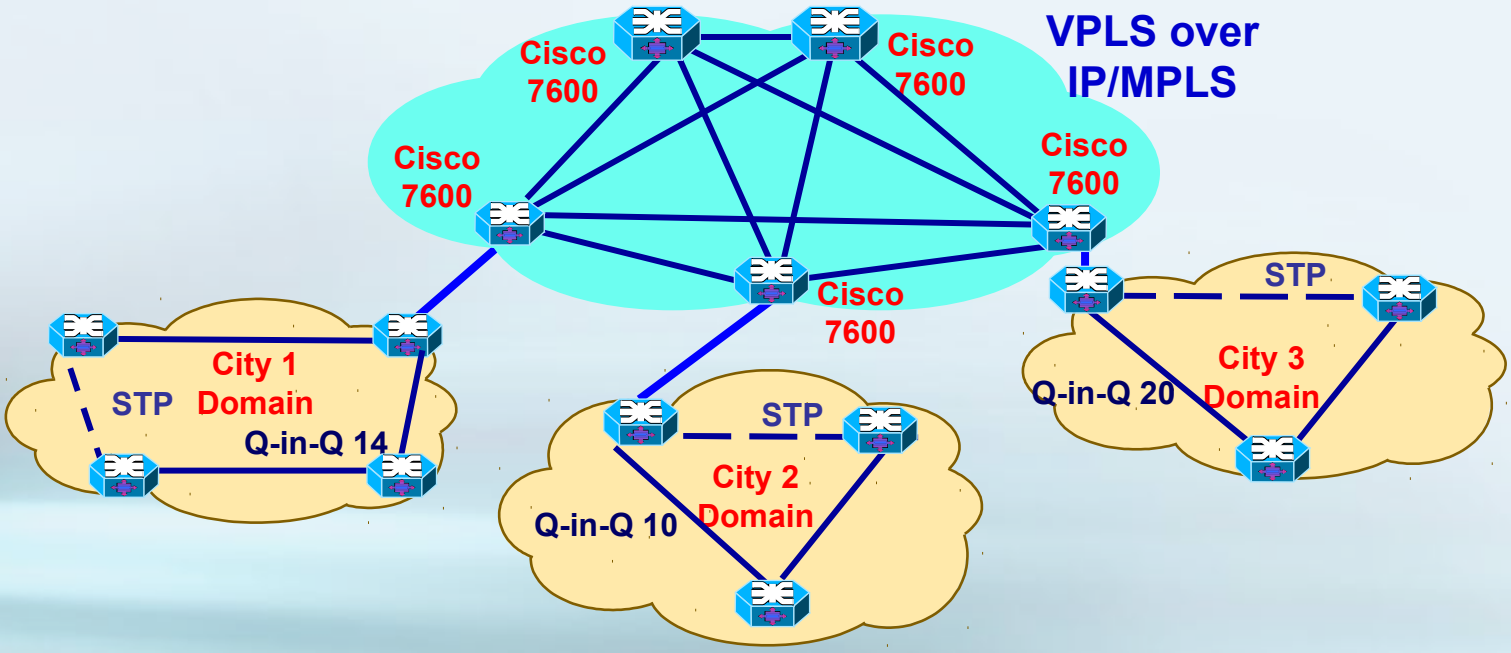
Description: Customers directly attach to VPLS service at Provider Edge

- 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

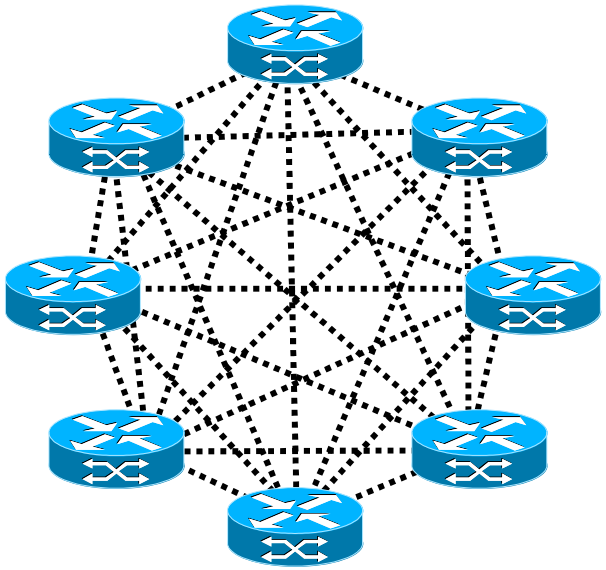
Benefit: Scales to support larger Ethernet deployments

- Full mesh for core tier (hub) only

A Comprehensive Solution: Robust, Flexible, Scalable, Manageable

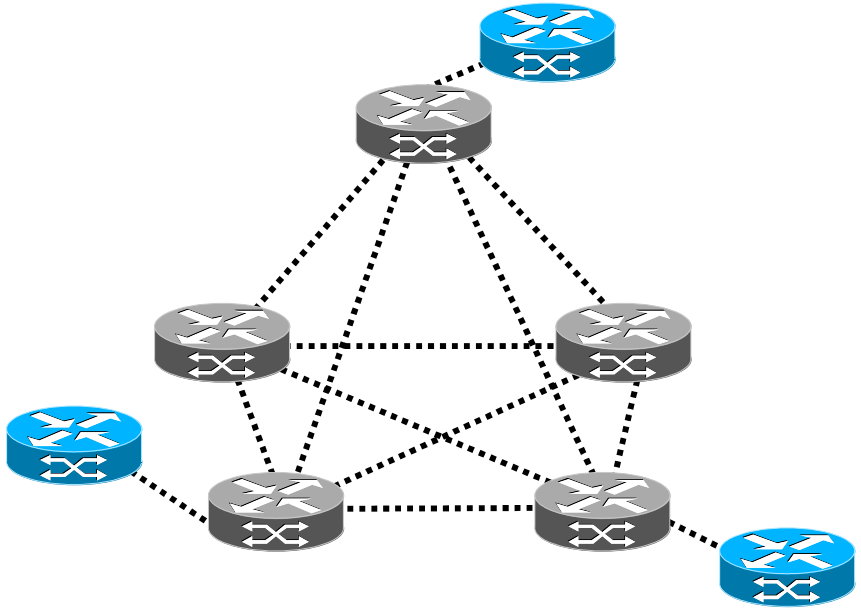
Why H-VPLS? Greater Scale

Flat VPLS



- Full PW mesh from the edge
- Higher signaling overhead
- Packet replication done at the edge
- Node discovery and provisioning extend end-to-end

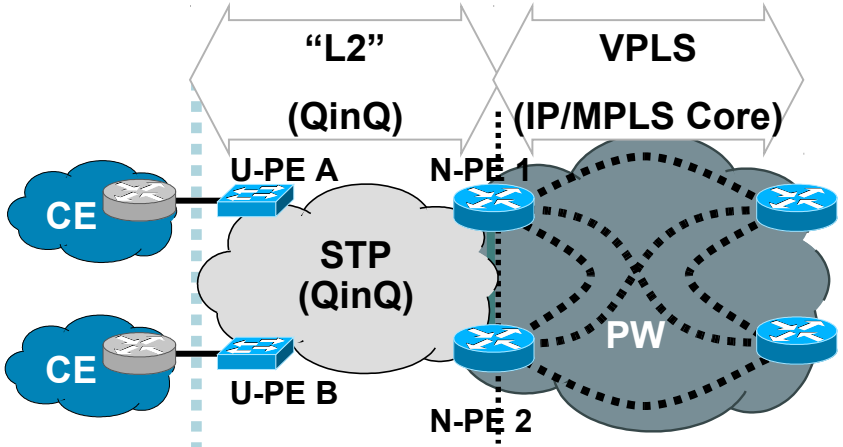
H-VPLS



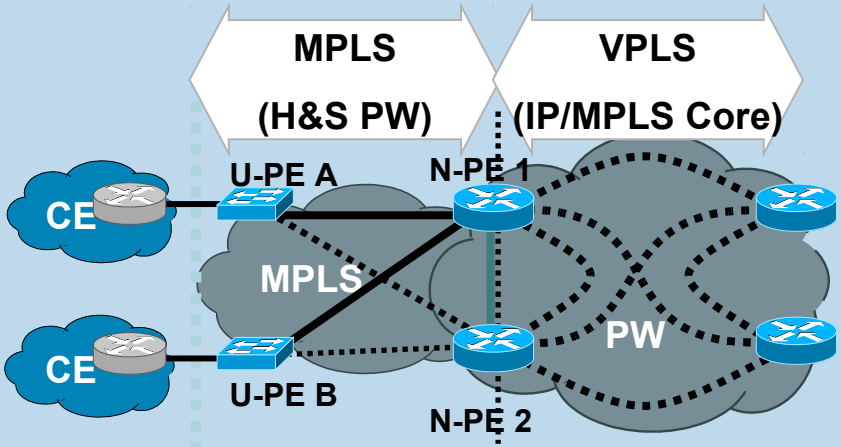
- Full PW mesh only within core
- Minimizes signaling overhead
- Packet replication done in the core only
- Partitions node discovery into smaller domains

H-VPLS Access: QinQ or MPLS at Edge

- H-VPLS with QinQ Access
- Access domain defined by IEEE 802.1ad (QinQ)



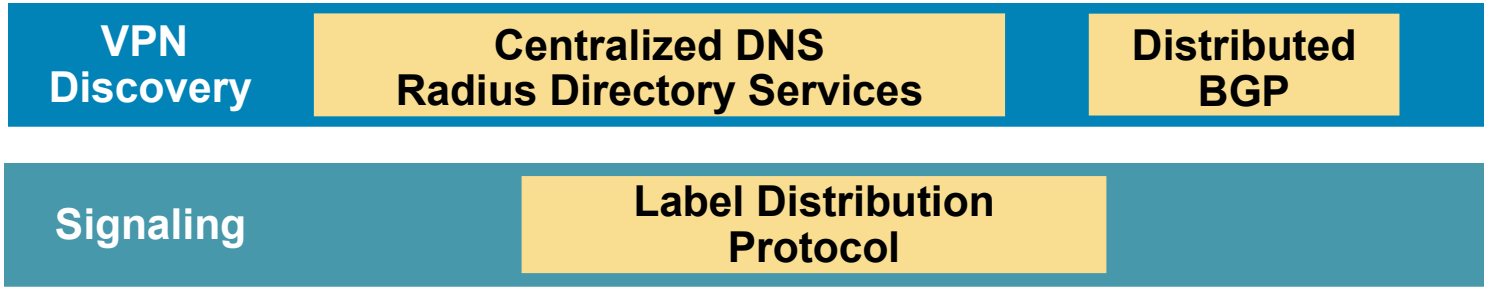
- H-VPLS with MPLS Access
- Uses PW EoMPLS circuit to backhall traffic from U-PE to N-PE



VPLS Features

- VPLS Autodiscovery
- Pseudowire Redundancy
  (see AToM for example)
- N-PE Redundancy
  with MAC Address Withdrawal

VPLS Autodiscovery and Signaling



- **Autodiscovery: BGP is the configuration agent**
  - True autodiscovery of VPN members
  - 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 session & activate it for the VPLS address-family
2. Create VPLS instance & associated interfaces to it
3. (Optional) Establish import/export rules (or use the default mode)

Discovery & Signaling

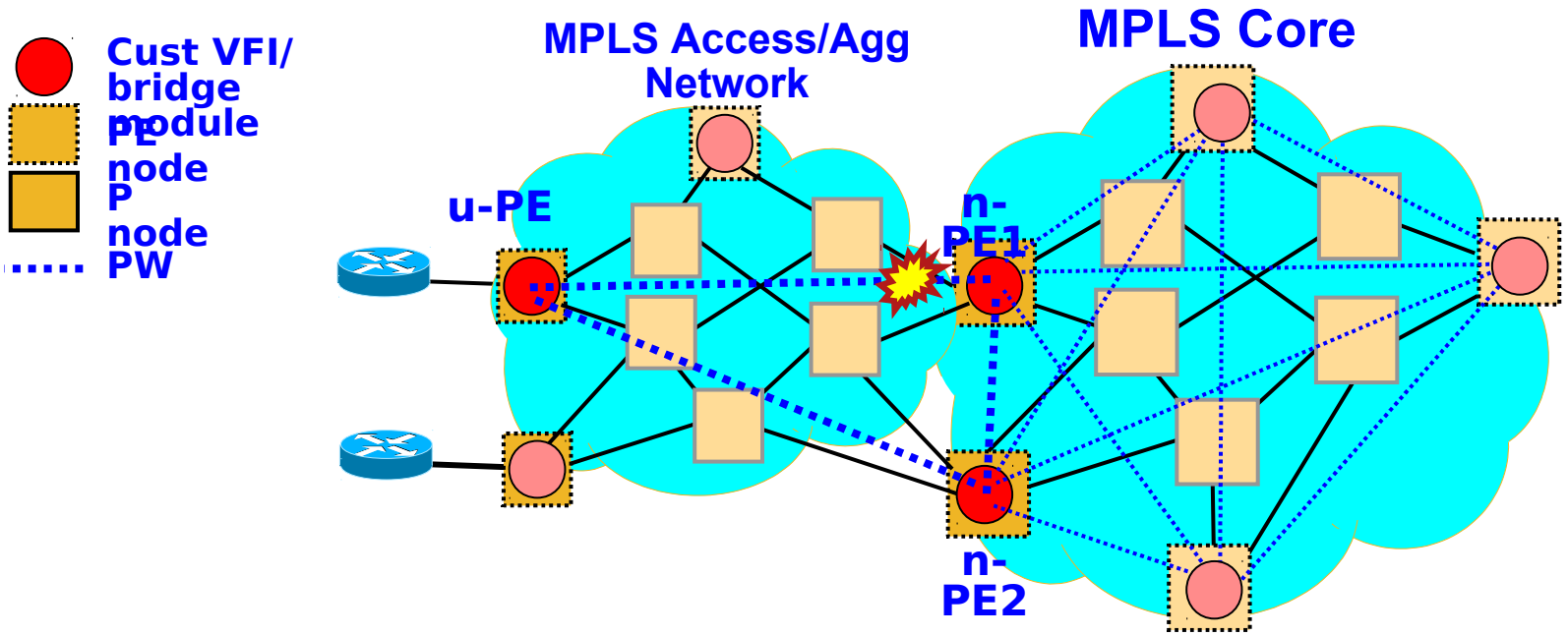
- **Discovery & signaling are separable parts of L2VPN establishment**
  - **Discovery (finding members of an L2VPN) is a point-to-multipoint task**
  - **Signaling (establishing the pseudowires) is a point-to-point task**
- **By separating the tasks, you can choose a suitable protocol for each:**
  - **BGP, RADIUS, etc. for Discovery**
  - **LDP, L2TPv3 for PW Signaling**

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

H-VPLS N-PE Redundancy for MPLS Access



Feature Description: Upon PW failure detection by u-PE, PW redundancy selects the backup n-PE, and then a MAC address withdrawal message is sent by the u-PE to the n-PE2 backup

This H-VPLS redundancy feature has three components:

1. **PW loss-of-connectivity detection (includes signaling of PW Status)**
2. **PW Redundancy anchored at the u-PE and terminated at n-PE1 & n-PE2**
3. **MAC Address Withdrawal**

References
Virtual Private LAN Service (VPLS)

- RFC 4447 Pseudowire Setup and Maintenance Using LDP, April 2006
  http://www.ietf.org/rfc/rfc4447.txt
- RFC 4448 Encapsulation of Ethernet over MPLS, April 2006
  http://www.ietf.org/rfc/rfc4448.txt
- RFC 4762 Virtual Private LAN Service over LDP, January 2007
  http://www.ietf.org/rfc/rfc4762.txt