Packet and Optical Multi-Layer VPN Architecture: Opportunities and Challenges

Hamid Ould-Brahim (Nortel)

Tomonori Takeda (NTT)

Bilel Jamoussi (Nortel)

Outline

- Packet and Optical VPNs?
- GMPLS VPNs in the Optical World
- Multi-Layer VPNs
- Summary and Challenges
- References

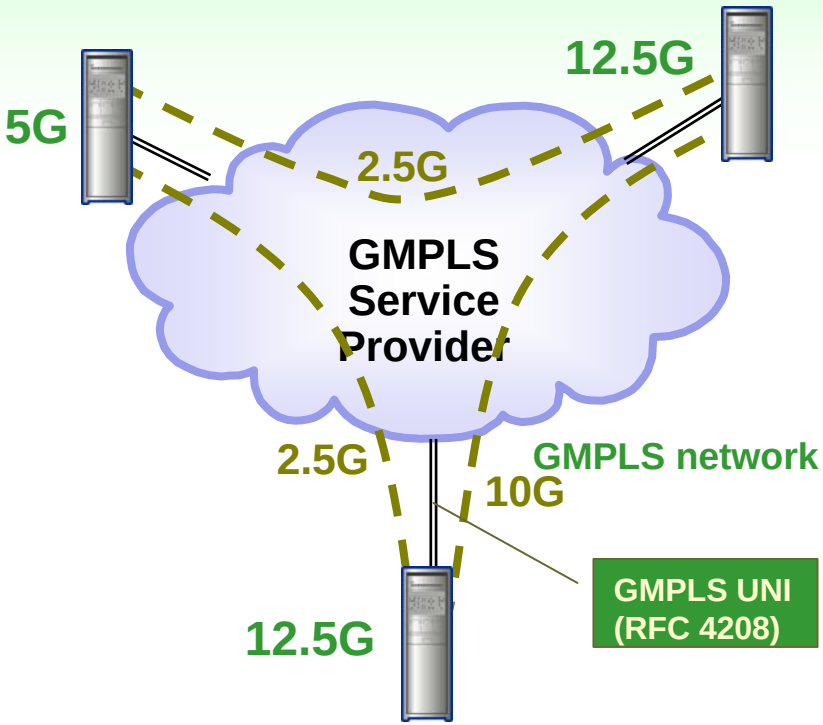
Packet and Optical VPNs

- What “Packet and Optical VPNs” means in this context?
  - A Packet-and-Optical provider network where Layer-1, 2 and layer-3 VPN services (or any combination thereof) can be offered as VPN services.
  - Packet client networks subscribing to GMPLS Layer-1 VPN network
    - Nested multi-layer VPNs
    - L1VPNs implemented using packet-based technology.
  - VPN services offered using Packet-based VPN protocol toolkit
    - A subset of l3 VPNs combined with an l2/l1 VPN dataplane.
- GMPLS VPNs current status:
  - applying GMPLS mechanisms to provide layer-1 VPN services.
  - Other uses:
    - GMPLS protocols in network inter-working between legacy layer-2 (ATM PNNI) and MPLS networks.
    - GMPLS protocols in the context of multi-segment pseudowires.
    - GMPLS control plane for point-to-point Ethernet connections.

GMPLS VPNs for Optical Networks

- Traditionally, in Optical network environments, VPNs are defined as partitioning provider network resources into independent private networks:
  - Customers subscribe and own internal capacity, (in a carrier's carrier deployment scenario)
    - Services are provided on top of this capacity.
- A GMPLS control plane redefined VPNs in the TDM/optic world from a broader perspective:
  - Private network partitioning is just one type of service model
  - Some service models are driven by the type of client devices (e.g., if clients are core routers then the VPN service model may offer limited topology view of resources for the purpose of efficient traffic engineering interworking with the client network.).
- In middle 2005 IETF created L1VPN working group in the routing area to look at defining L1VPNs using GMPLS.
  - Work started before in ITU-T on L1VPN requirement and architecture in 2004 and moved to IETF.
  - L1VPN WG reuses the GMPLS protocol toolkit

L1VPN Service Model 1: Basic Mode (Overlay Model)



Some New Challenges

- Simplified provisioning
- Overlapping private addresses
- Constrained/restricted connectivity.
- On demand bandwidth request.
- Privacy/independence with respect to addressing and routing.

Basic Mode=Private connections between CEs in a given port topology ➔ Signaling only, no routing exchange

See draft-fedyk-l1vpn-basic-mode-01.txt for more information

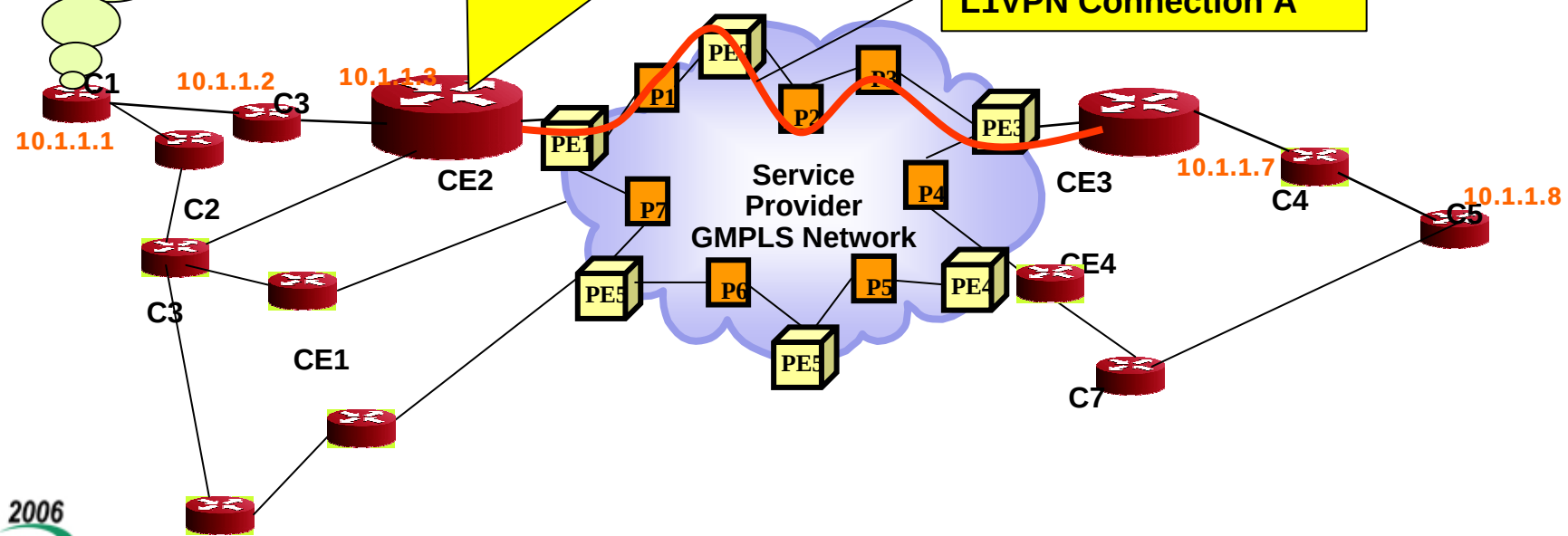
Basic Mode TE limitations

Limited TE capabilities and
Weak utilization of on-demand capabilities

Need to configure
N square routing peering

I know only about connection A => I can use it for TE path computation

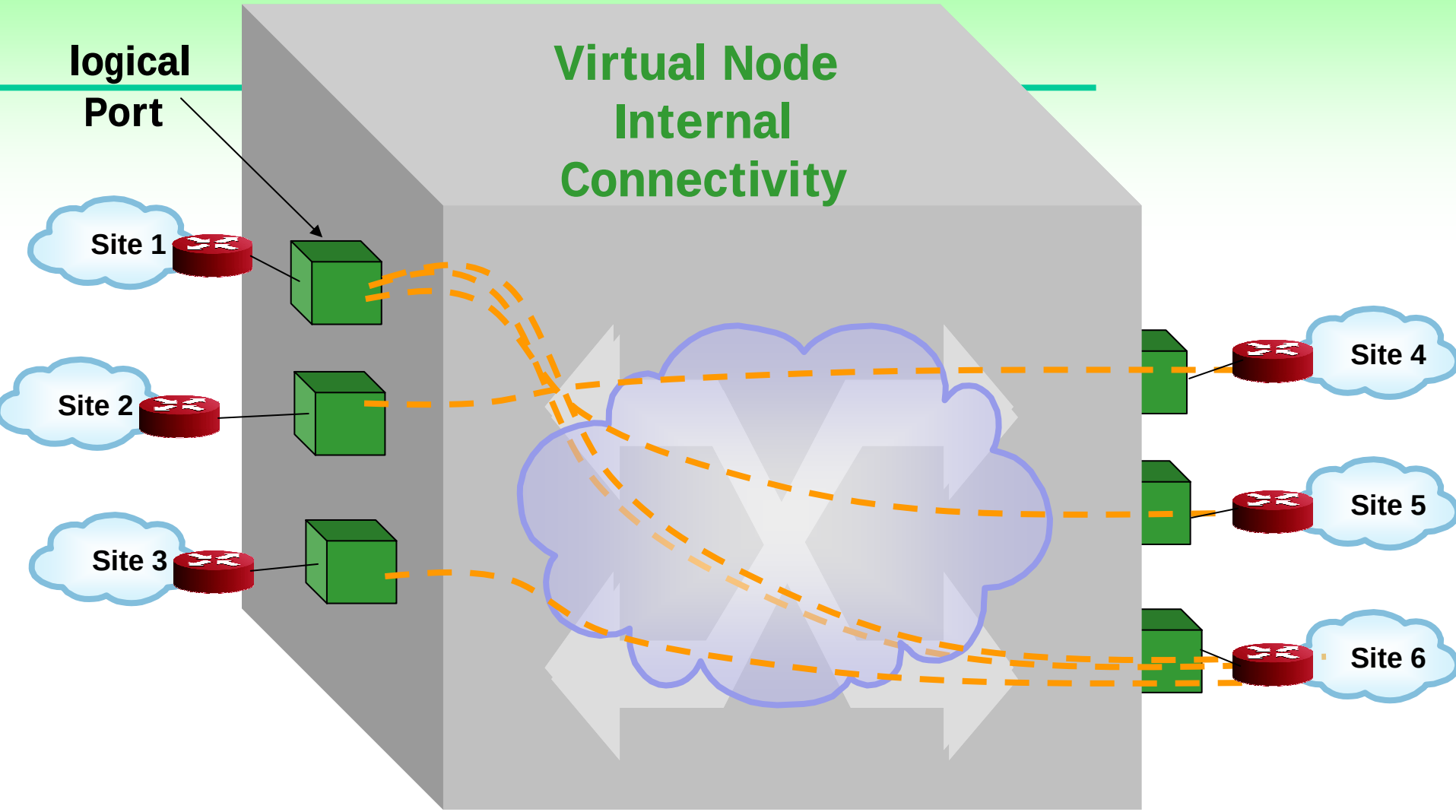
2. Configure Routing and advertise routing updates across the (G)MPLS connection A (need to use the same instance of GMPLS control plane that created the connection)



L1VPN Enhanced Mode

- Enhanced Mode implies the exchange both routing and signaling between client network and provider edge devices.
- Four Service models defined:
  1. Overlay Extension Model
     - In this model a CE receives a list of TE link addresses to which it can request a VPN connection (a list of addresses within the same VPN). This may include additional information concerning these TE links (e.g., switching type
  2. Virtual Link
     - Virtual links created between provider edge nodes and exported externally to client networks → CEs have visibility of the virtual links
  3. Virtual Node
     - The whole provider network is represented as a virtual node. The customer perceives the provider network as one single node. The CE receives routing information about CE-PE links and remote customer sites.
  4. Per-VPN peer
     - The provider partitions the TE links within the provider network per VPN, and discloses per-VPN TE link information to corresponding CEs. As such, a CE receives routing information about CE-PE links, remote customer sites, as well as partitioned portions of the provider network

L1VPN Virtual Node Concept



Provider provides/manages a single Virtual node per customer
Client sees only his Virtual node

Virtual Node used in a packet-based client network

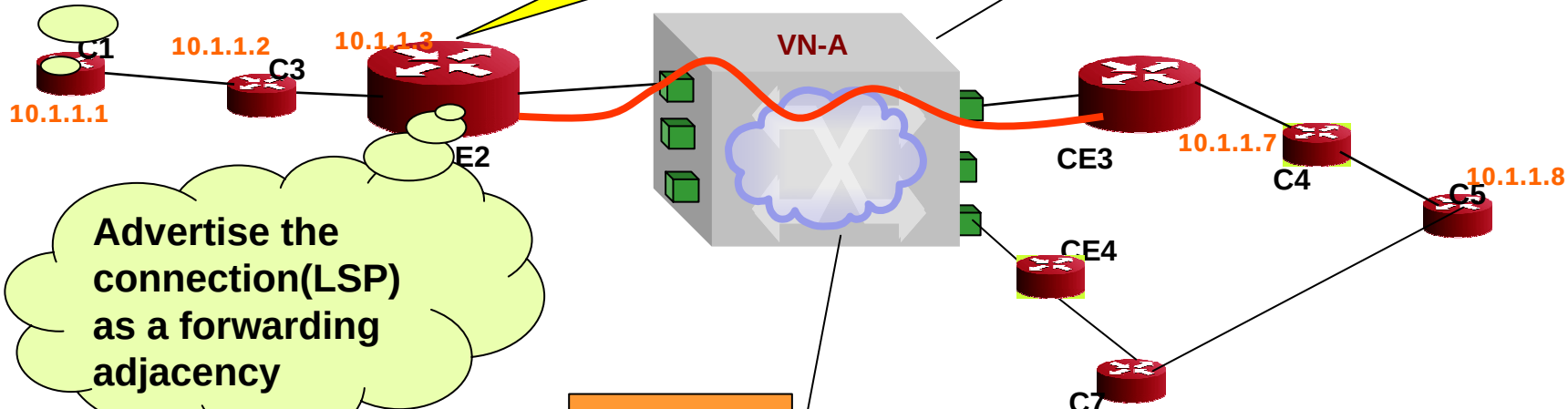
Efficient TE capabilities

I know about CE-CE connections AND CE-PE links (VN links) in my routing database

Configure Routing betwee
CE-PE link not between CEs.
Establish connections between CEs (can be done upon CE2 receiving an internal LSP request)

No n square routing
Peering

Same client OSPF area!!!



Advertise the connection(LSP) as a forwarding adjacency

L1VPN Service

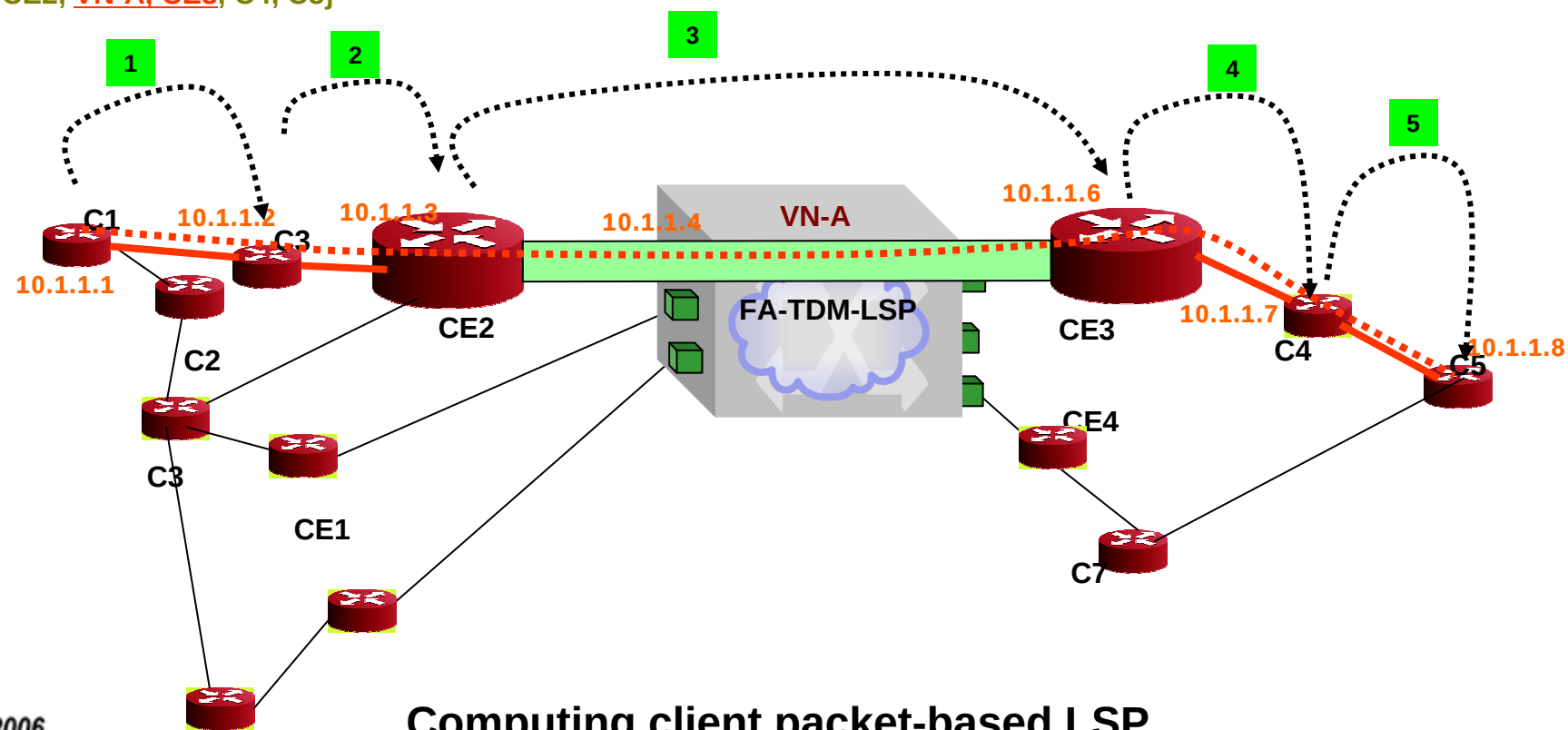
Similar problem solved by MPLS-layer-3 VPNs (RFC2547bis, and Virtual Router) for data networks but not exactly the same approach and the same context

GMPLS VPNs in Packet-to-Optical Scenarios

Sonet/SDH Virtual Node/L1VPN with Customer packet based LSP

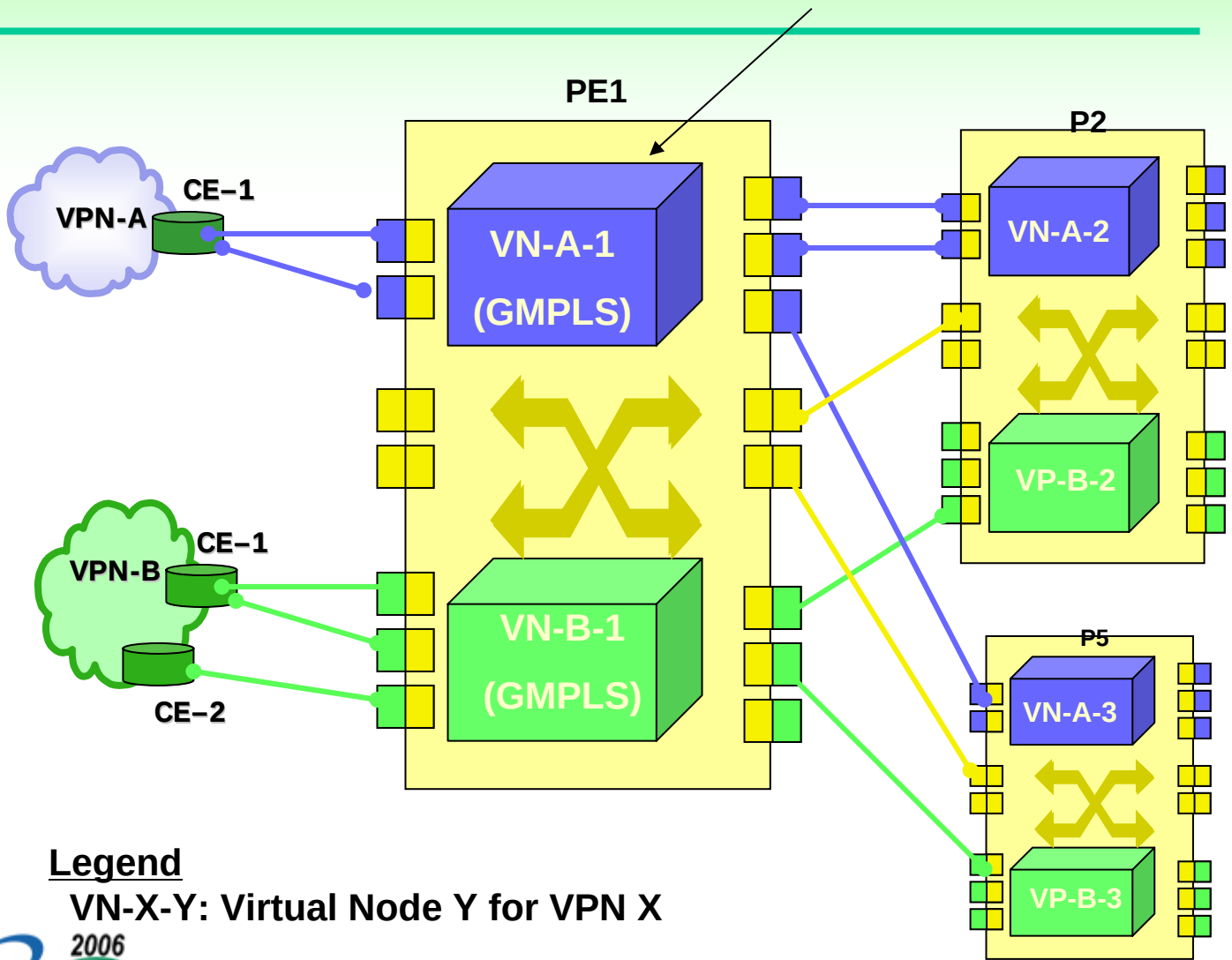
Connection request:
Source address=10.1.1.1,
Destination address=10.1.1.8
Path={C3, CE2, VN-A, CE3, C4, C5}

CE2: Establish a signaling adjacency (CE2-CE3)
Nest the packet based LSP into the TDM-LSP
New Packet_LSP Path={TDM-LSP-Endpoint, C4, C5}



Computing client packet-based LSP using CE-PE TE L1 VPN links

Enhanced Mode: Per VPN Peer Service Model



Legend

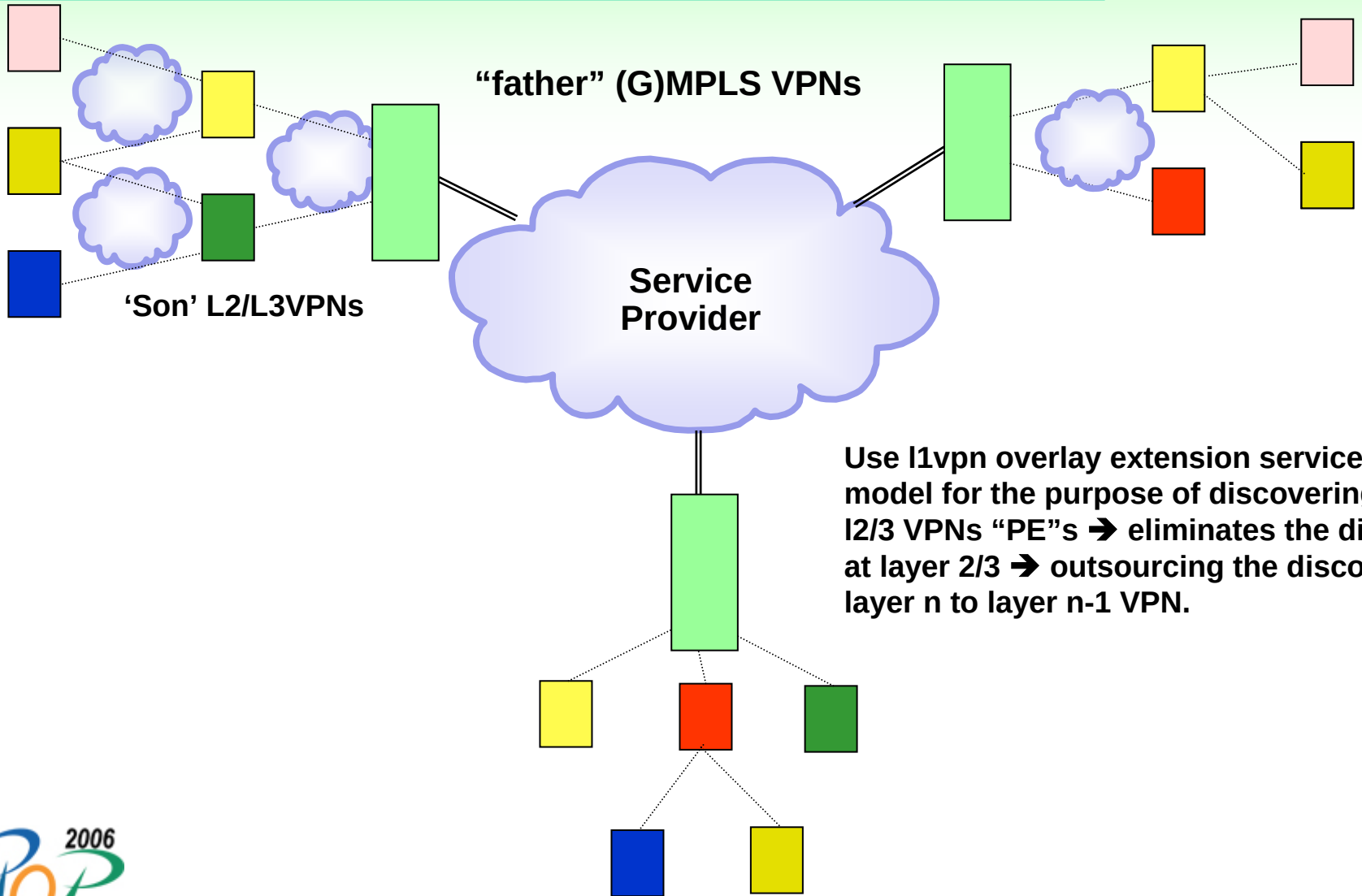
VN-X-Y: Virtual Node Y for VPN X

Multi-Layer VPNs: Combining (G)MPLS VPNs

- VPNS such as L2 and L3 VPNs have been specified independently and vertically.
  - However they may co-exist in the same provider network.
  - Some L2 services may terminate on an L3VPN service
  - An L2 access network may be connected to an L2 VPNs Service.
  - The same customer may subscribe to an L3VPN and subscribes for other reasons to an L2VPNs.
  - In a carrier's carrier model, an CE may provide L2 and L3 VPNs across an L1 VPNs, and so on.
  - An 802.1ah/ad attached to an "infrastructure" VPLS in the core.
- Little has been done on optimizing Multi-VPN service deployments. Optimization can come from:
  - Optimized VPN functions when Multi VPNs are provided.
- Multi VPN deployment may offer opportunities for additional service enhancements

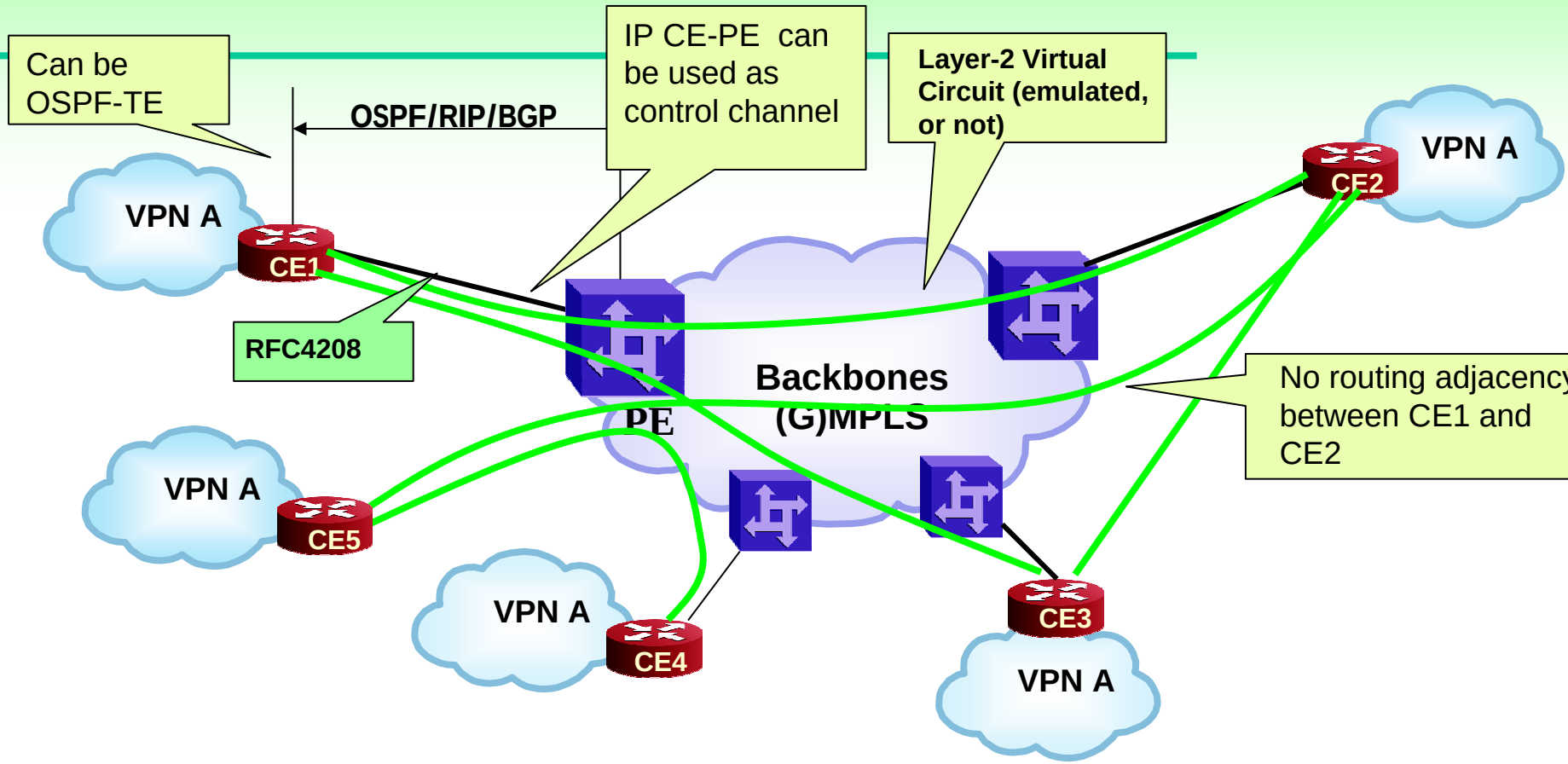
All provider-based (G)MPLS VPN services share for most part the same attributes and all can be implemented using a common VPN functionality toolkit.

Carrier's Carrier for Multi-layer VPNs



Use l1vpn overlay extension service model for the purpose of discovering l2/3 VPNs "PE"s ➔ eliminates the discovery at layer 2/3 ➔ outsourcing the discovery at layer n to layer n-1 VPN.

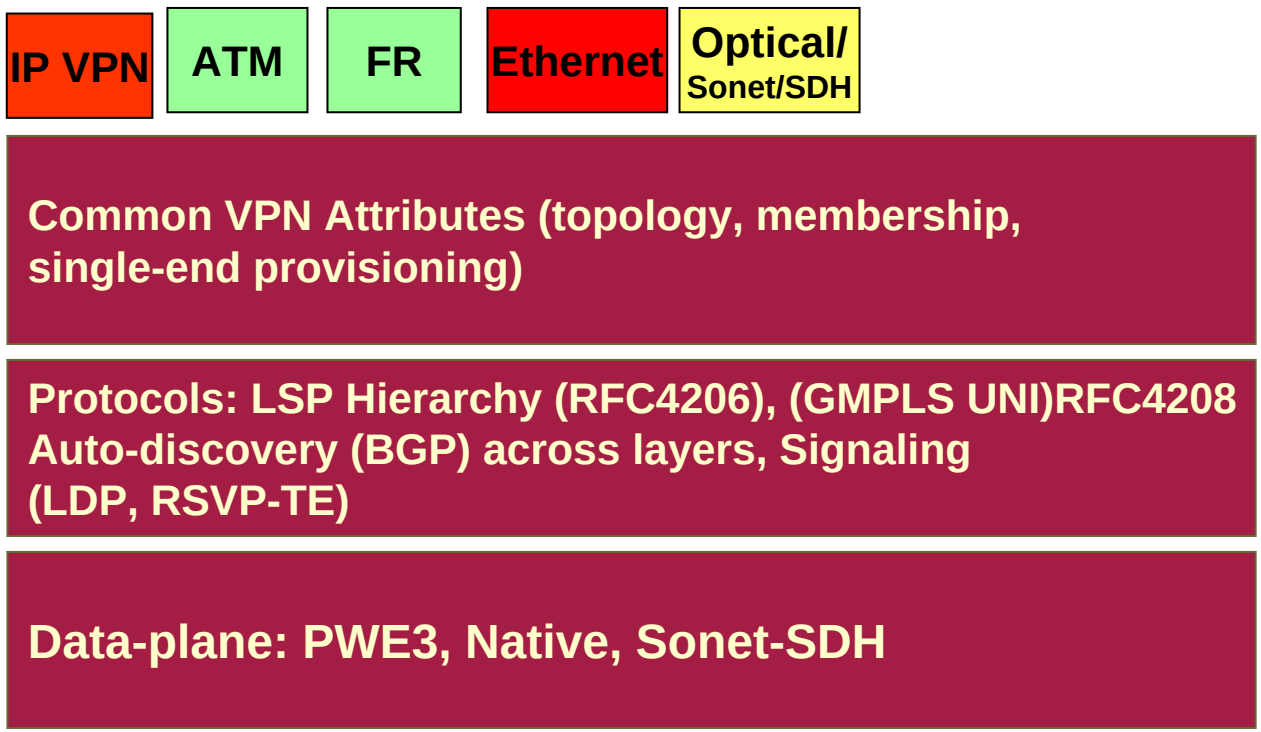
Combining L3 and L2 VPN Technology



1. CE peers only with attached PE at the routing level using RFC2547 "Control".
2. CE discovers ports of remote CEs and establishes on demand l2 (emulated) circuits. Note that the l2vpn topology can be based on l3vpn topology.

Backup: Multi-Layer VPN Toolkit

- Decomposing the VPN problem from vertical solutions to reusable building blocks.



Summary and Challenges

- L1VPN specifications in their first phase definition
  - Planned to be finished by year end 2006/early 2007
- Emerging GMPLS Ethernet infrastructure
  - Solving the data-plane first
  - Reuse l1vpn mechanisms for providing GMPLS Ethernet VPNs
- Applying GMPLS back to the packet world
  - Now GMPLS-based standard RFCs have been completed.
  - Consistent Control plane data plane separation in GMPLS has advantages.
  - Overcoming the challenges for building business cases for GMPLS-based applications without disrupting work done in MPLS-VPNs/PWE3 work.

- Can GMPLS Applications such as GMPLS VPNs complement MPLS VPN applications?
  - In a packet and Optical environments, the answer is definitely yes.
  - In a transition phase the answer is...still yes!

References

- “Framework and Requirements for Layer 1 Virtual Private Networks”, draft-ietf-l1vpn-framework-01.txt
- ‘L1VPn Basic Mode”, draft-fedyk-l1vpn-basic-mode-01.txt
- “BGP-based Auto-Discovery for L1VPNs”, draft-ouldbrahim-l1vpn-bgp-auto-discovery-01.txt
- RFC4206: “Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)”
- RFC4208: “Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model”
- “GVPN: Generalized Provider-provisioned VPNs using BGP and GMPLS”, draft-ouldbrahim-ppvpn-gvpn-bgpgmpls-06.txt