Next Generation Ethernet Transport

Monique Morrow

Santiago Alvarez

Future-Net, NYC

April 14, 2008

Agenda

- Industry Dynamics
- Ethernet Trends and Convergence
- Standards Overview
- Service Mapping and Applicability
- Summary

Industry Dynamics

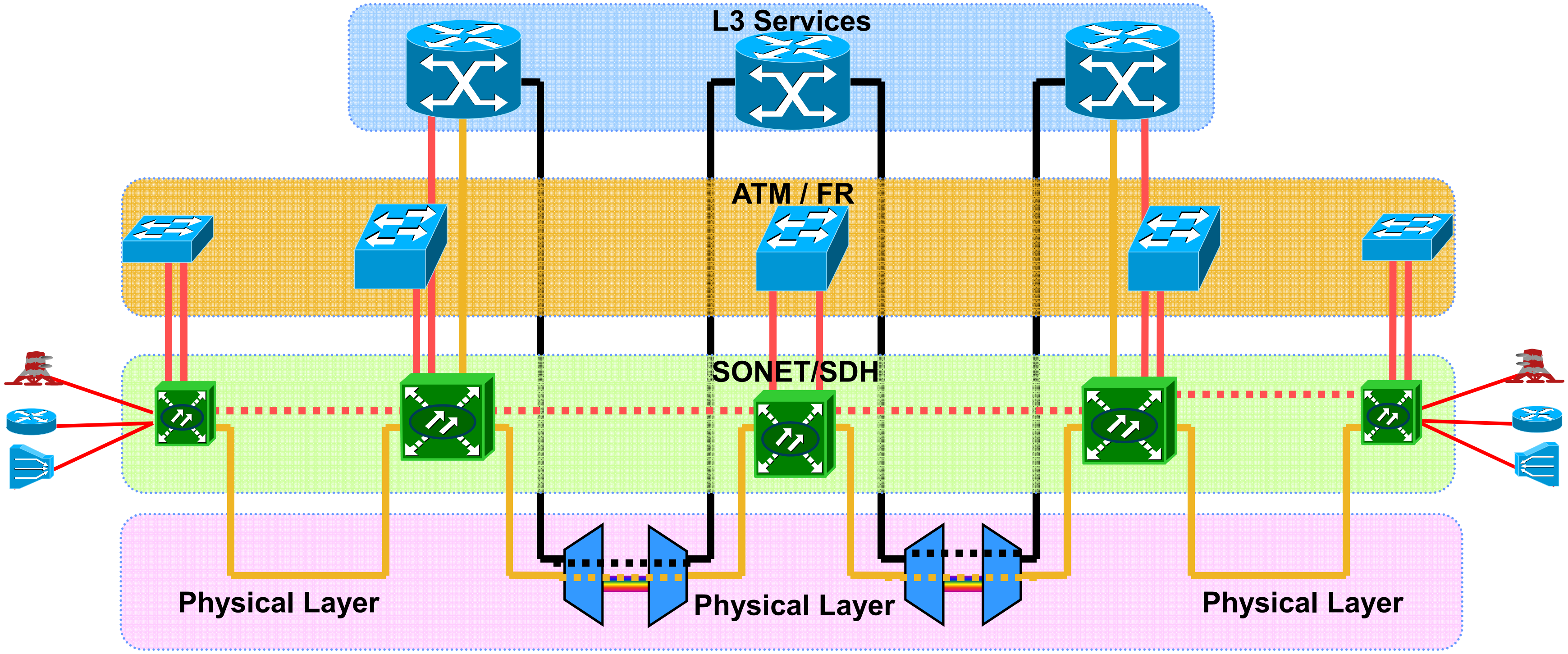
Market Trends and Focus

- Migration to IP/MPLS and Ethernet based core switching
- Ethernet at access for service aggregation
- Require service flexible architecture
- Capex and Opex efficient
- OAM and Network management key
- High availability and resiliency
- "Adaptation" of packet switching technologies to the transport domain
- Utilization of legacy strategy where ATM technology was used both as a "transmission" and a "switching" technology
- Elimination of unneeded control plane capabilities and functionalities in transmission applications
- Multiple overlay and supplemental proposals and techniques, including T-MPLS,PBB-TE, to adapt IP/MPLS and Ethernet to the transport arena

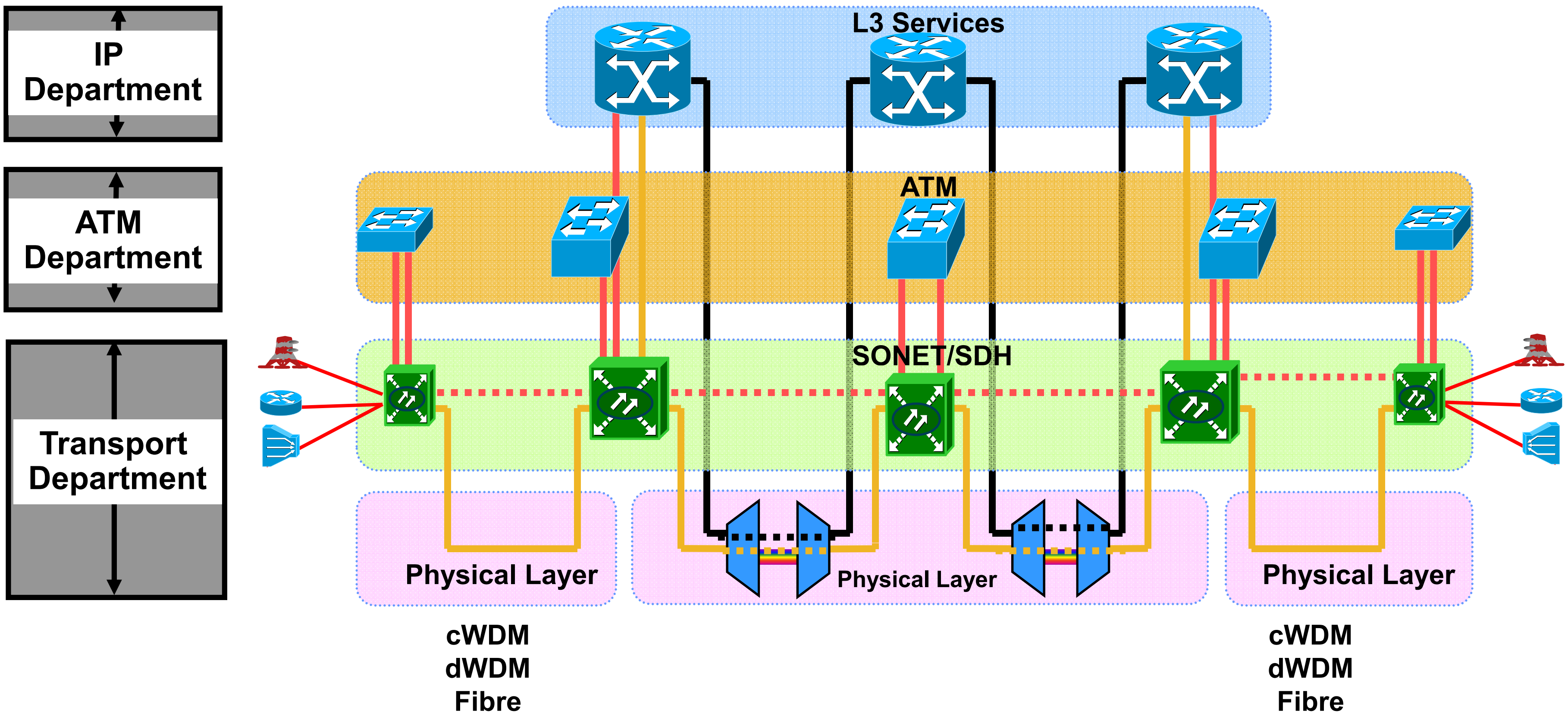
Packet Transport Market Dynamics

- Traditional circuit switched transport systems are migrating toward packet based technologies
- SDH/SONET platforms provide low speed bandwidth granularity network services and high speed long haul transmission services
- IP adoption and convergence simplifies packet transport networks in the access/aggregation and metro domains to reduce CapEx and OpEx in next generation networks

Where we are today !!



Existing roles and responsibilities



- Organisational lines drawn based on networks
- Cross charging between groups

  Transport to ATM, Transport to IP, ATM to IP

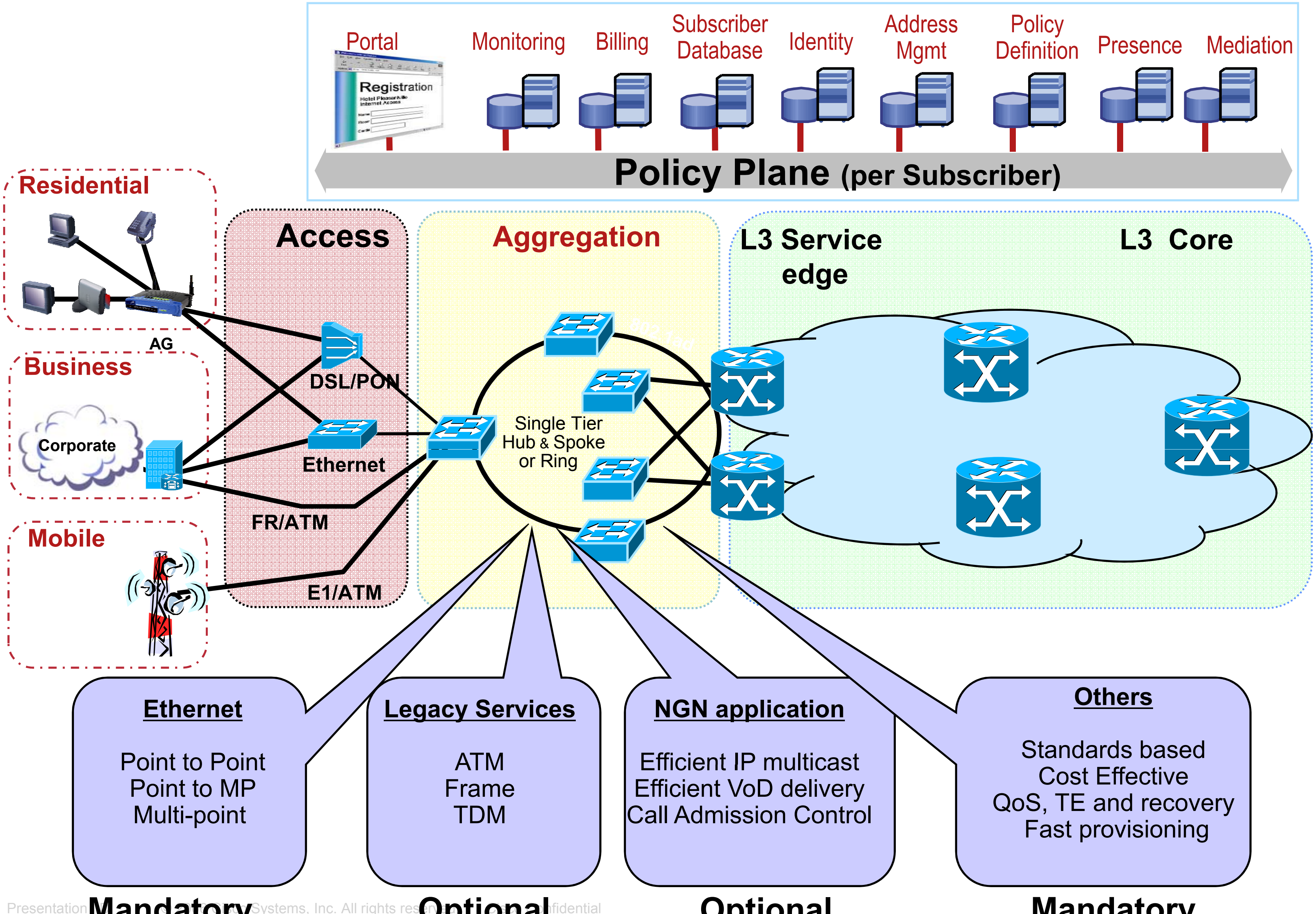
  Creates considerable friction

  Can cause organisational breakdowns (IP department buys dark fibre, dwdm gear)

Characteristics and issues

- Network centric
  - Circuit orientated
- Multiple networks
  - OPEX and CAPEX inefficiencies
  - Provisioning and service assurance complexities
  - Complexity between layers
- ATM and F/R technology is tailing off
  - Service capabilities
  - Bandwidth concerns
- NG SDH/SONET days numbered
  - TDM and circuits not well suited for packet transport
  - Acknowledged by transport vendors and SPs
  - Discussion is now about high performance packet networks
- Service capability may still be required
  - Regulation
  - Evolution may not be possible

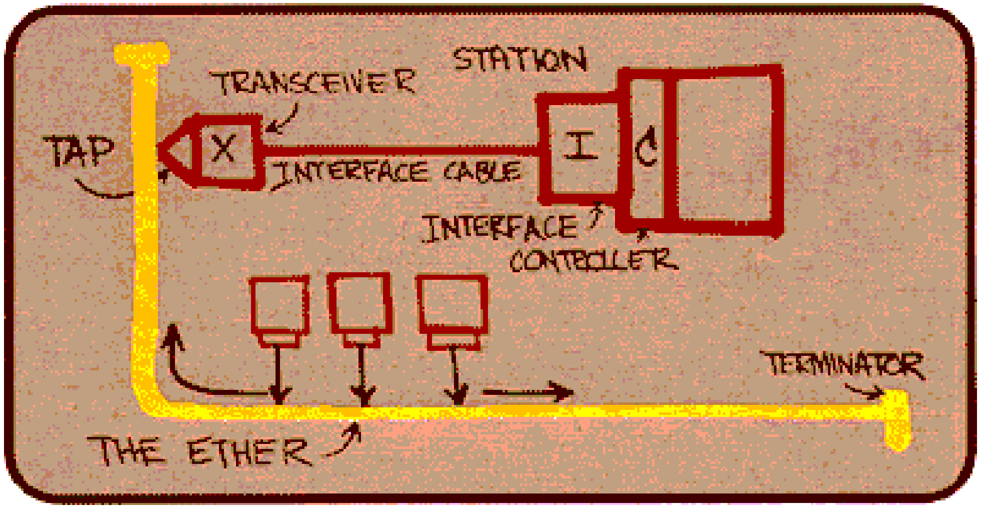
Next Generation Transport Requirements



Ethernet Trends and Convergence

Once Upon a Long Ago…

- 1972 Robert Metcalfe implemented Alto Aloha Network at Xerox Parc

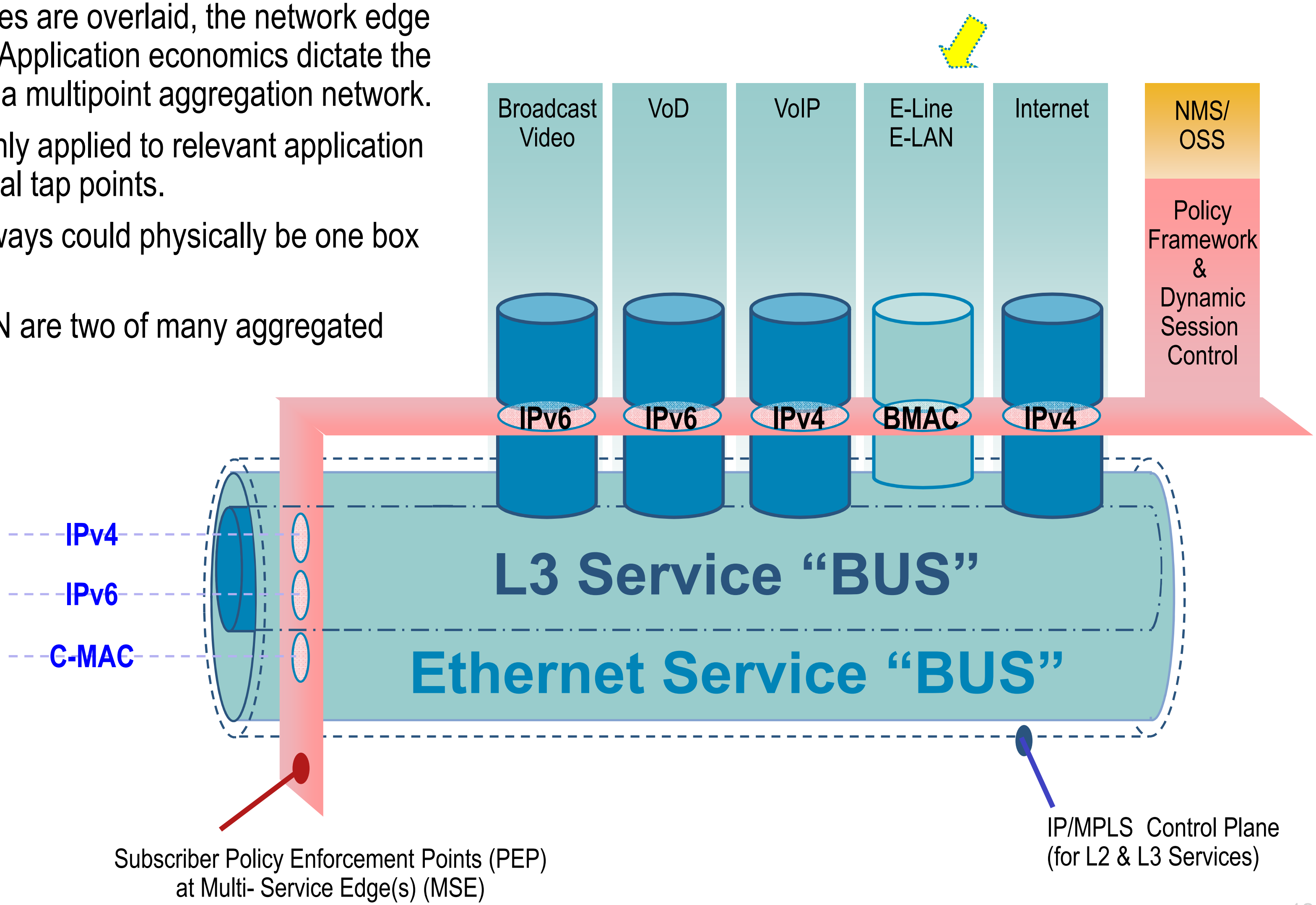


- 1976 name *Ethernet* coined
- Heritage is inherently *Multipoint* (i.e., multiple tap points on shared media.)

Now… SP Ethernet Aggregation Vision

From: Network per Service *To:* IP/Ethernet Convergence

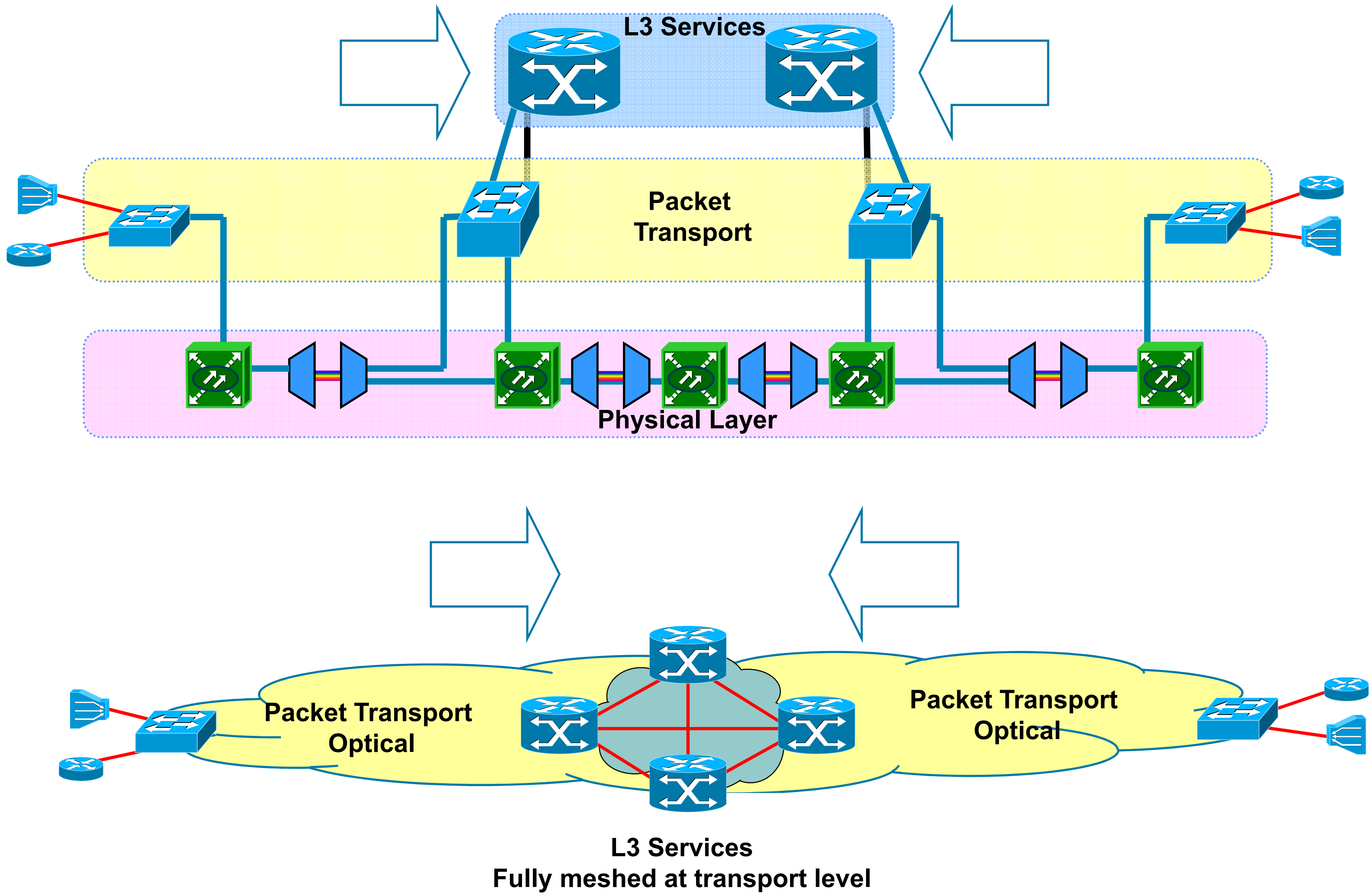
- As new services are overlaid, the network edge decomposes. Application economics dictate the Tap Points on a multipoint aggregation network.
- Policies are only applied to relevant application traffic at optimal tap points.
- Service Gateways could physically be one box or many
- E-Line / E-LAN are two of many aggregated services



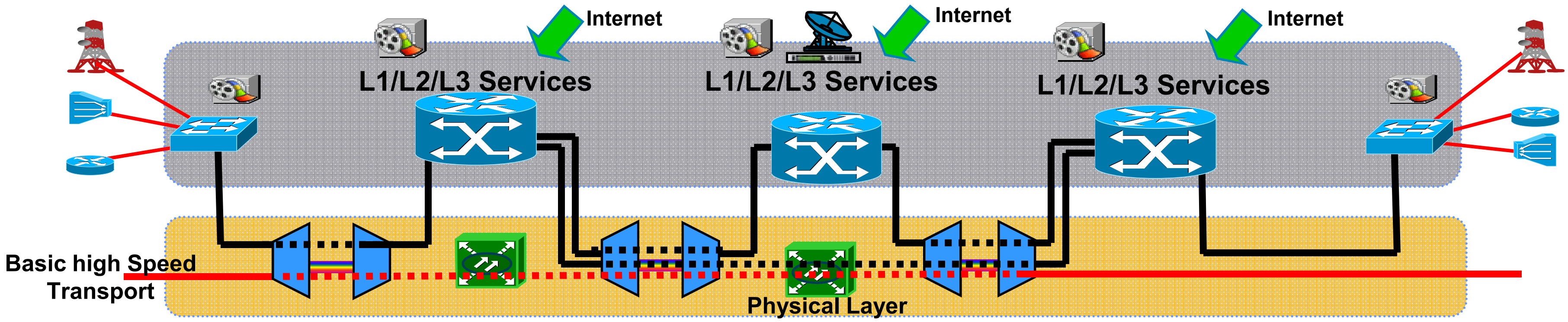
Moving forward

- IP will be an extremely important component of the NGN
  - No debate that IP is the protocol of the future
- Differing views on what an IP network is !!!
  - Routing IP packets (IP routing and optical)
  - AND / OR
  - Transporting IP packets (Ethernet and optical)
- IP is the service protocol
  - Not Ethernet, Not optical, Not MPLS
  - Other than dumbest optical transport all NGN networks need IP disciplines
  - So do the organisations running them
- ATM is dying rapidly
  - New services and bandwidth concerns
- SDH/SONET days numbered
  - Acknowledged by transport vendors
  - Discussion is more about high performance packet networks
  - They are moving towards :- Ethernet transport and optical

NGN: Transport Orientated View



NGN: Service Oriented View



- Optical layer
  - Dark fibre and / or DWDM
  - Basic non-oversubscribed point to point high bandwidth services
  - Under lying transport for IP/MPLS infrastructure
- IP/MPLS
  - End to end IP/MPLS control plane
  - IP/MPLS equipment directly integrating with optical layer – dark fibre or DWDM
  - Concurrent support of L1, L2, L3 services
- Flexible Service Edge
  - Service termination
  - Content injection
- Minimal layering
  - Rapid adaptation and provisioning
  - CAPEX and OPEX efficiencies

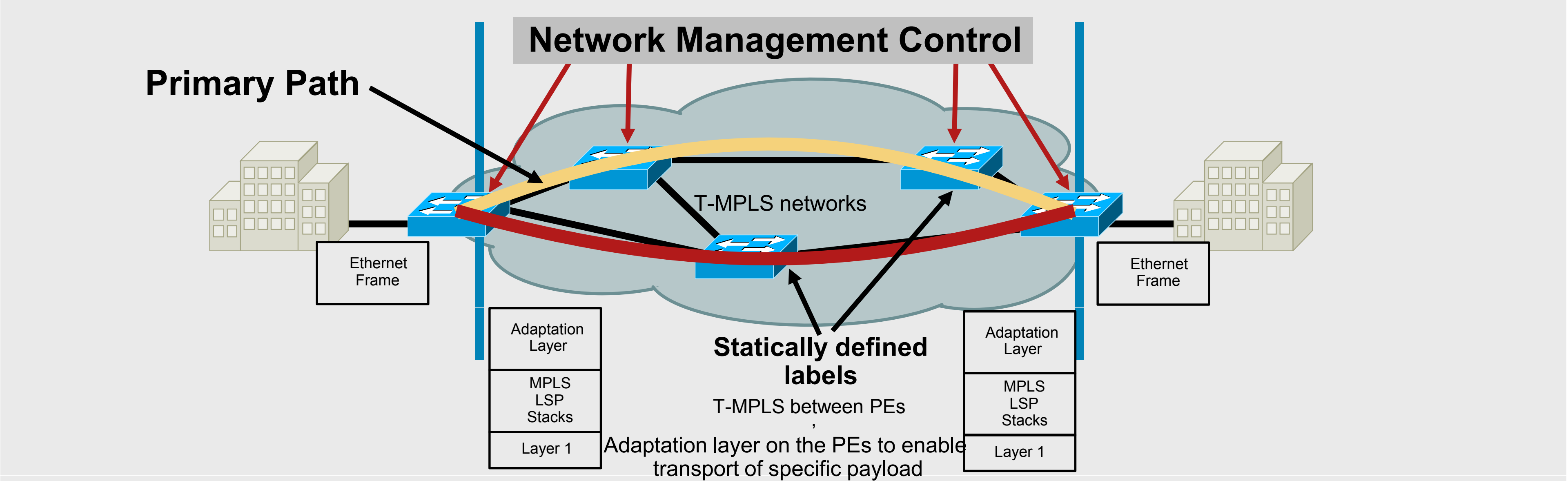
Service Requirements

Consumer	Business	Wholesale	Evolved services
Internet Voice / Video / data **Voice** PSTN / Multimedia **Video** Over the Top Walled Garden **Mobility**	**TDM/ATM→Ethernet** **L2 VPNs** Pt2Pt Pt2MPt MPt2MPt **L3 VPNs** Connectionless **Value-add Services** Based on L3 visibility	**TDM/ATM→ Ethernet** **L2 VPNs** Pt2Pt Pt2MPt MPt2MPt **L3 VPNs** L2TP Connectionless	**PSTN** Migrate **Mobile** RAN backhaul IP transition **TDM** Migrate and evolve to Ethernet **ATM** Migrate and evolve to Ethernet **F/R** Evolve to Ethernet

A service orientated architecture

- Flexible content injection
  - Centrally or distributed, or combination
- Multi-Service capability
  - IP, Ethernet, ATM, TDM services
- Connectionless Services
  - Multi-point and point to multipoint services
- Connection Orientated Services
  - Point to Point Services
- Rapid service turn up and provisioning
  - User self management
  - Minimal in-house provisioning
- Integrated into Service Control plane
  - Easily integrated with TISPAN, IMS and policy environment
- Operation and planning
  - Simple capacity planning and operational models
  - Service centric network instrumentation
- Service and Network Security

What is T-MPLS ?



- Definition: Transport MPLS
  - Forwarding Plane: MPLS labels with simplifications (bidirectional LSPs, no ECMP, no PHP)
  - Control Plane: Phase 1: static provisioning of labels using OSS/NMS
  - OAM proposal based on Y.1731 and Y.1711
- Services: Phase 1 : P2P connection orientated services only
- Standards:
  - ITU-T based set of standards

What is T-MPLS?

- Connection oriented packet switched transport over an optical transport network
  - Architecture based on ITU-T G.805
- Its main characteristics are:
  - Bidirectional trail (Point to point)
  - “Client-server” model
  - Control plane: no control plane (phase 1); GMPLS later?
  - OAM based on transport concept (i.e. AIS/RDI, CV: ITU-T Y.1711 phase 1, quality control still missing -> Y17.tom and Y.17tor)
  - Protection switching and Survivability based on ITU-T Y.1720/G.8131 (linear protection switching 1+1, 1:1, shared mesh options) and Y.mrps (ring protection switching)
  - Use same data-link protocol ID (e.g. EtherType), frame format and forwarding semantics as defined for MPLS frames
- T-MPLS is another MPLS “pseudowire” with bi-directional traffic engineered paths

T-MPLS Uses MPLS Features but…

- T-MPLS defined to use "same profile" as MPLS but:
  - Use of bidirectional LSPs
  - No Penultimate Hop Popping (PHP)
  - No LSP merging option
  - No FRR support
    - Requires LSP merge
  - No Equal Cost Multiple Path (ECMP)
- T-MPLS is a subset of MPLS but …
  - Interoperability with existing MPLS platform is a challenge

How is it Positioned?

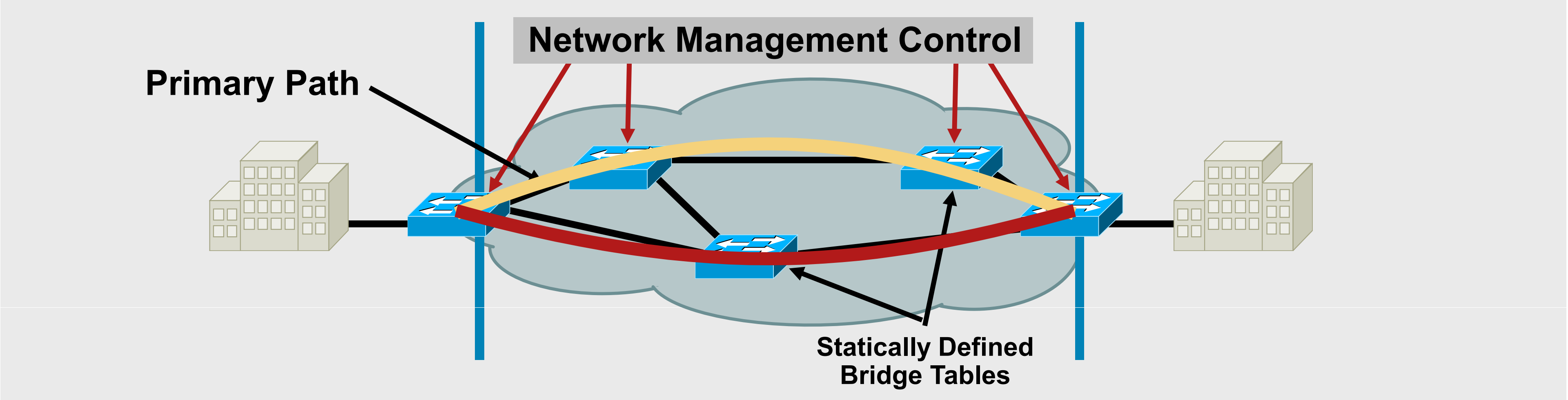
- Next Generation SONET/SDH with tight integration to Metro Ethernet and Access: Transport Ethernet frames over point-to-point VCs
- Offers a transition path to SPs/Carriers who have a huge SONET/SDH infrastructure and moving toward packet

  Re-usability of OTN networks without expensive upgrade (e.g. Introduction of control plane might require more memory or device forklift)

- Next Generation Packet Transport: Layer 2 hollow core

  Claim: cheaper OPEX, easier to operate and deploy

What is PBT / PBT-TE ?

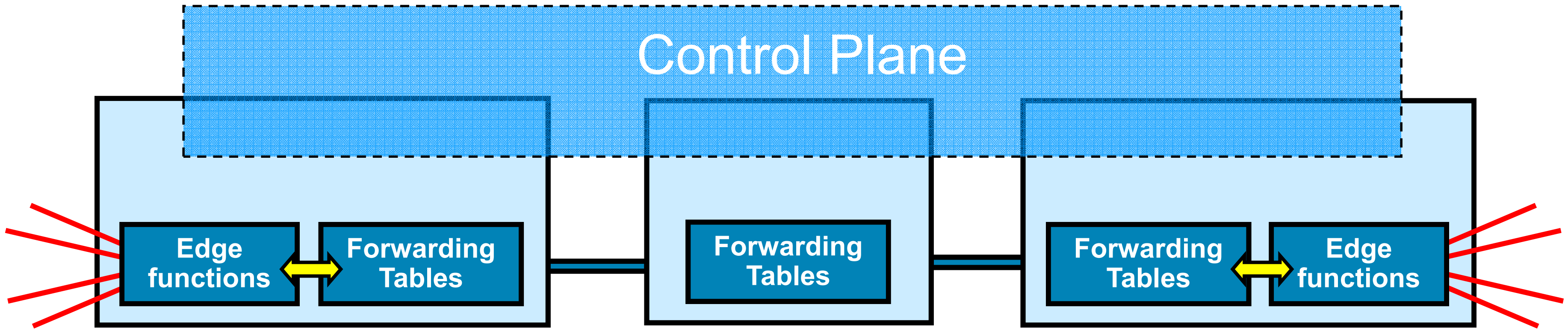


- Definition: Provider Backbone Transport (PBT), Provider Backbone Bridge – Traffic Engineering
  - Forwarding Plane: 802.1ah encapsulation from Provider Backbone Bridging
  - Control Plane: An OSS/NMS replaces IEEE control plane elements
  - OAM based on 802.1ag (with modifications)
- Services: P2P connection orientated services only
- Standards:
  - PBT is proprietary
  - PBB-TE standardization initiated in 2006 as 802.1Qay

Who are the Target Customers?

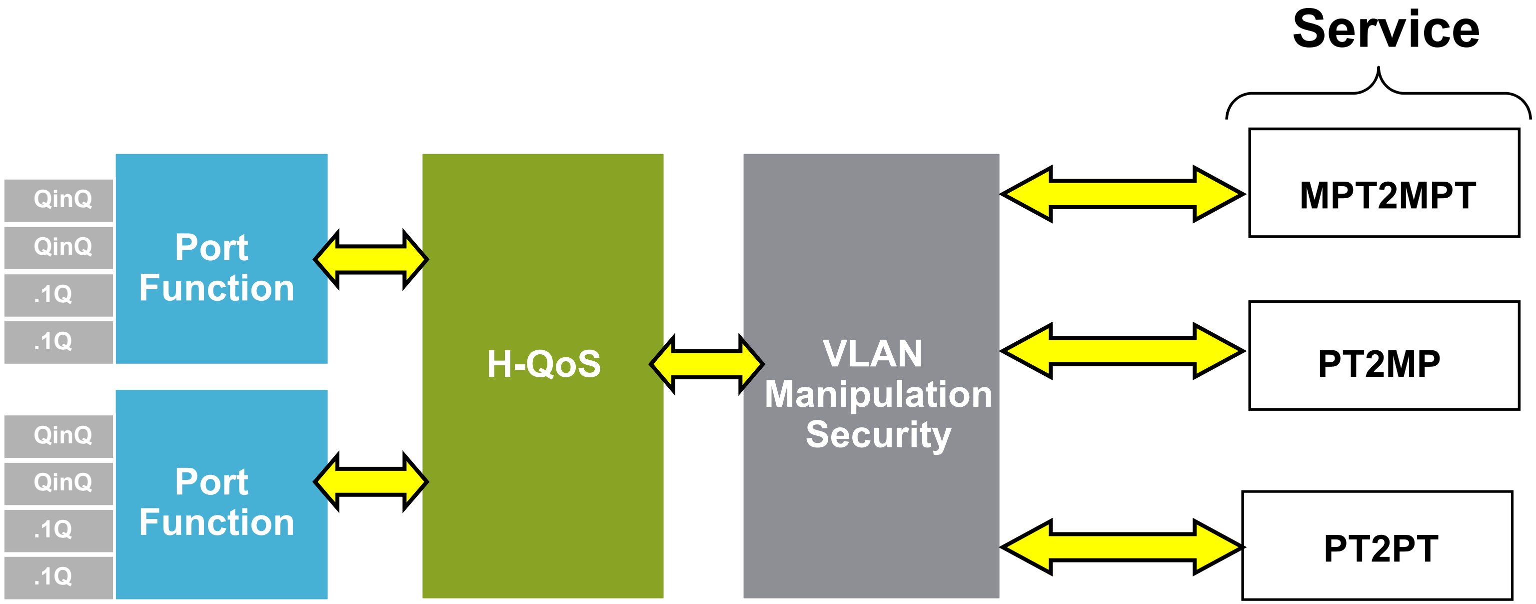
- A PRIMARY target for PBT are customers with legacy SONET/SDH switching and NMS solutions
- Operators who want to offer Ethernet services over Ethernet Infrastructure
- Existing operators who currently deploy IEEE 802.1ad (QinQ) Metro Ethernet network and want to evolve to IEEE 802.1ah/PBT network

Comparing solutions



- Edge functions
  - Conditions customer connections
  - Vital component but not part of the base transport
- Data plane
  - Encapsulation of the packets and forwarding paradigm
- Control plane
  - The set-up and control of the forwarding plane for different services

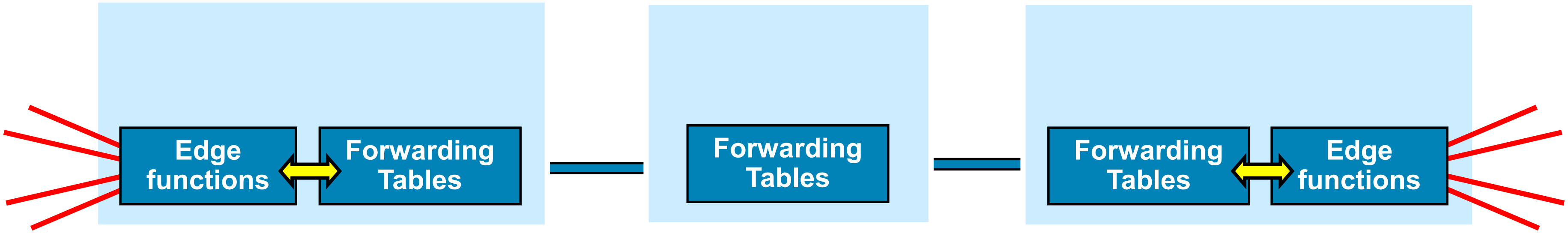
T-MPLS, PBB-TE versus IP/MPLS Edge functionality



- Defines the users SLA
- PBB-TE / T-MPLS tend to sell MEF QoS capabilities
- Reality is much more complicated (H-QoS, VLAN manipulation etc etc)

A vital component

T-MPLS, PBB-TE versus IP/MPLS
Forwarding plane

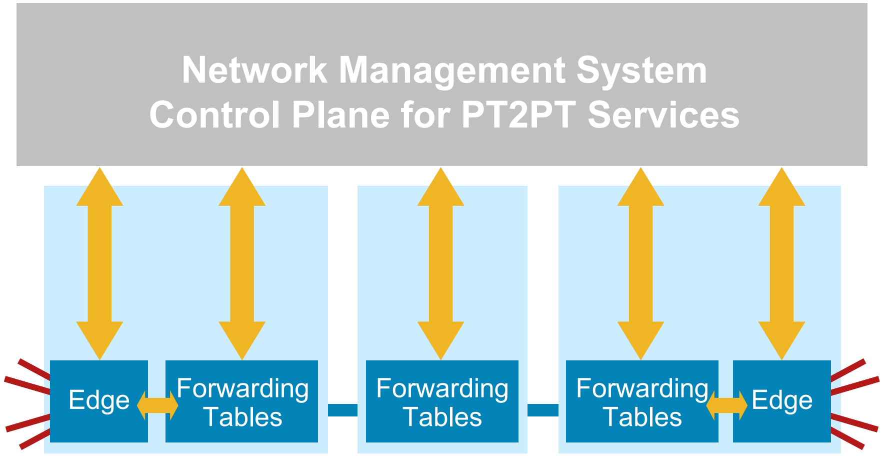


- **IP/MPLS**
  - Customer packet encapsulated in an MPLS label stack
  - Forwarding based on a label switch
- **T-MPLS**
  - Customer packet encapsulated in MPLS label
  - Forwarding based on a label switch
- **PBT**
  - Customer packet encapsulated in 802.1ah
  - Forwarding with modified Ethernet switching

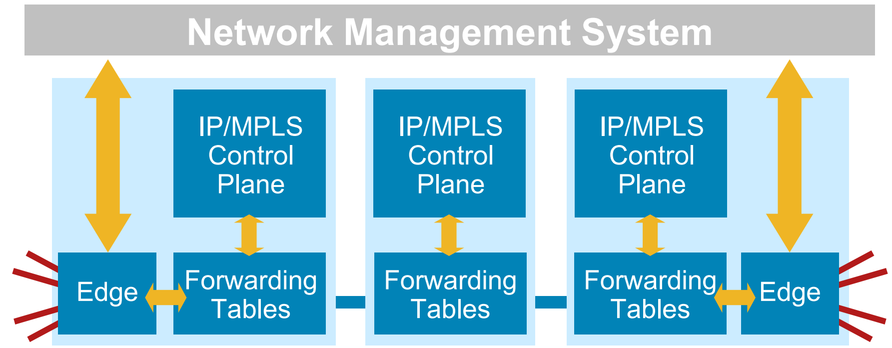
Strong similarities

PBT/PBB-TE and T-MPLS versus IP/MPLS Control Plane

PBT/PBB-TE and T-MPLS



IP/MPLS

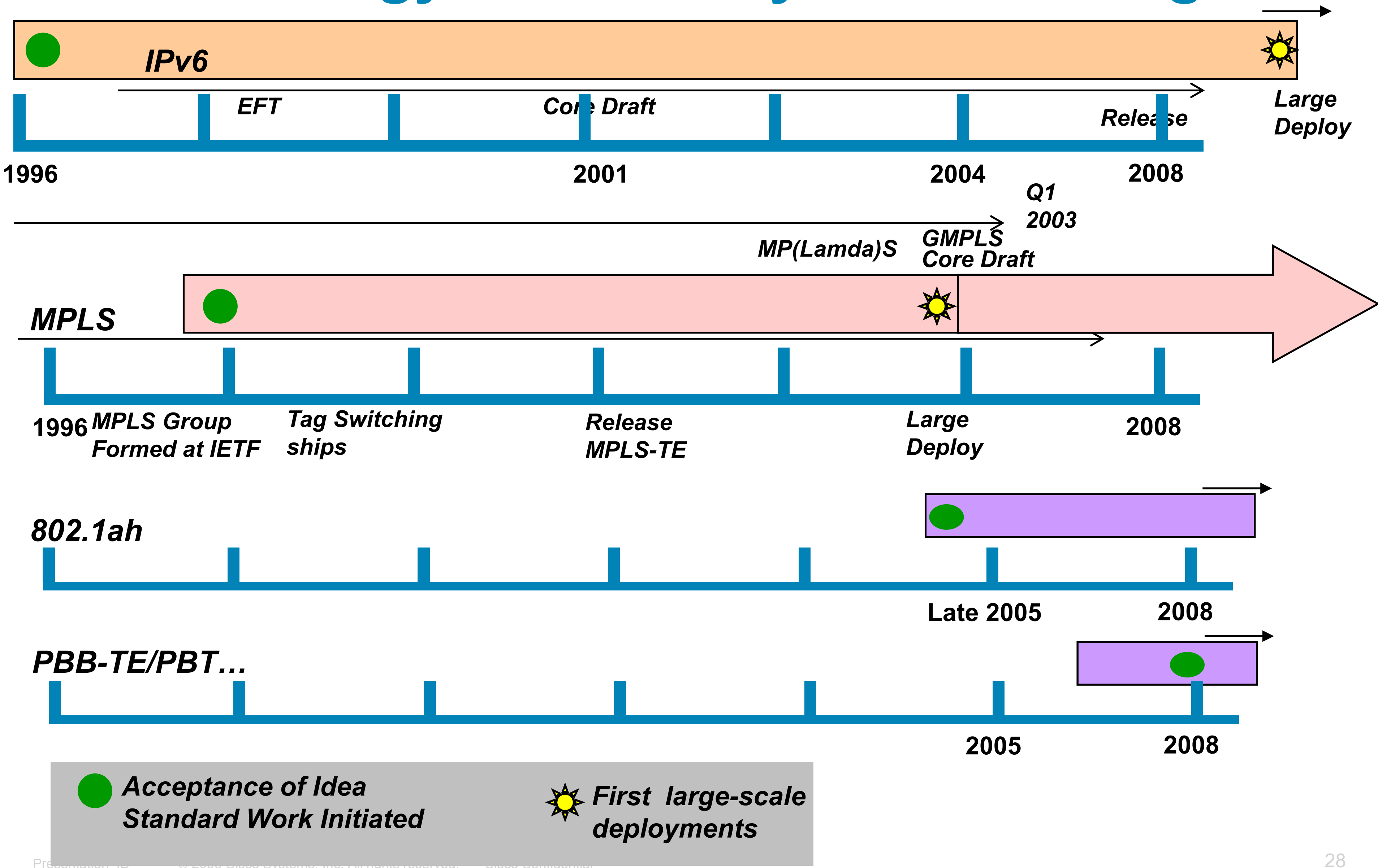


- **NMS based Control Plane**
- **Long term support integrated control plane?**
  - **PBT/PBB-TE → G-MPLS, 802.1aq / 802.1at**
  - **802.1aq / G-MPLS – Link state Protocol, RSVP etc**
- **Single Service Control Plane**
  - **Pt2Pt Only**

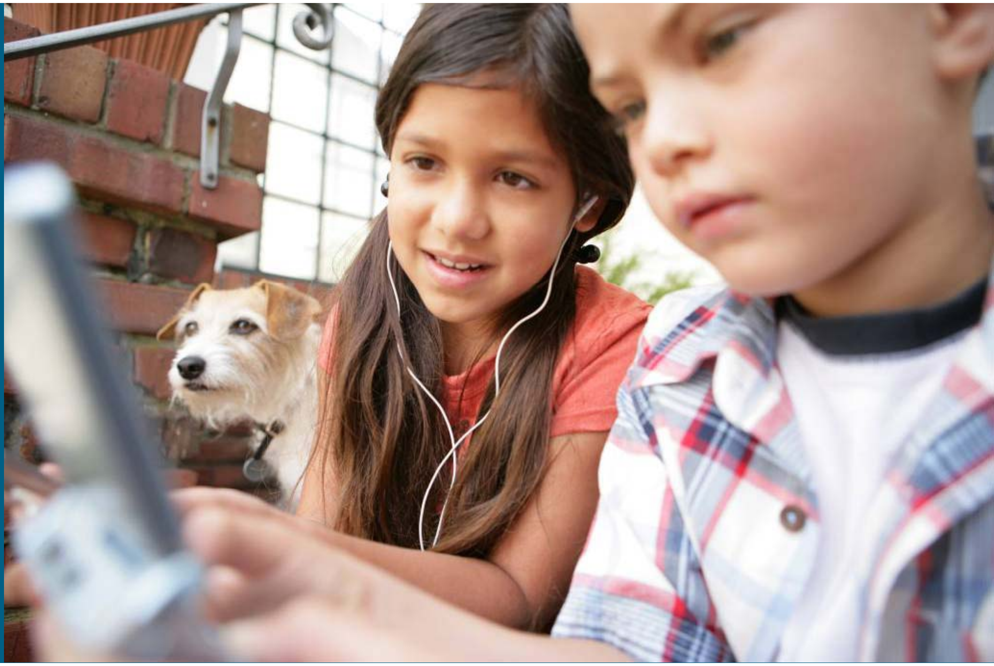
- **Integrated Control Plane**
- **Multi-service Control Plane**
  - **L1, L2, L3**
  - **Pt2Pt, Multipoint**

PBB-TE / T-MPLS :
Short term : Moves complexity to mgmt layer
Long term: Similar protocols and complexities

Technology Uncertainty / Forecasting



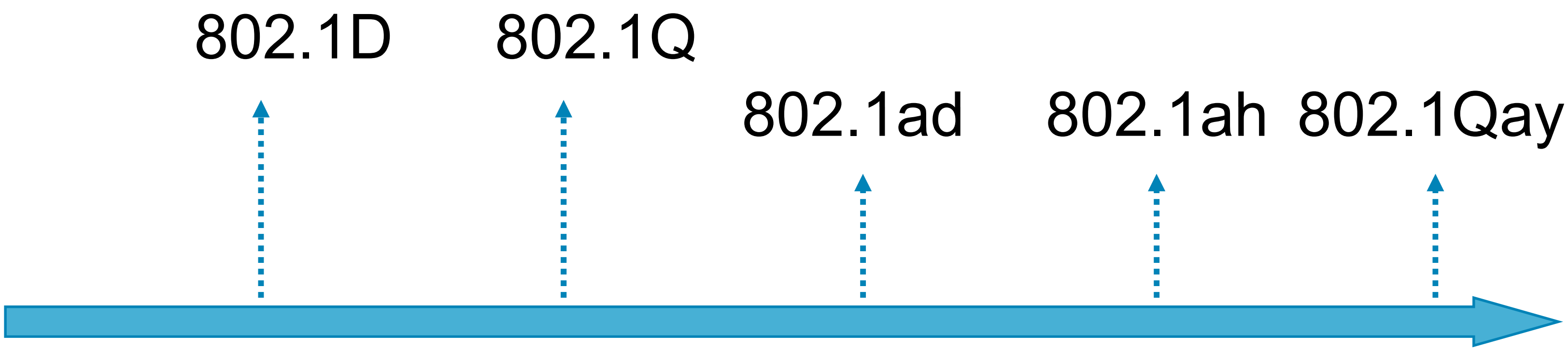
Standards Overview



Topics

- Ethernet evolution
- Ethernet OAM
- Ethernet over MPLS
- MPLS Protection and OAM
- PBT/PBB-TE
- T-MPLS

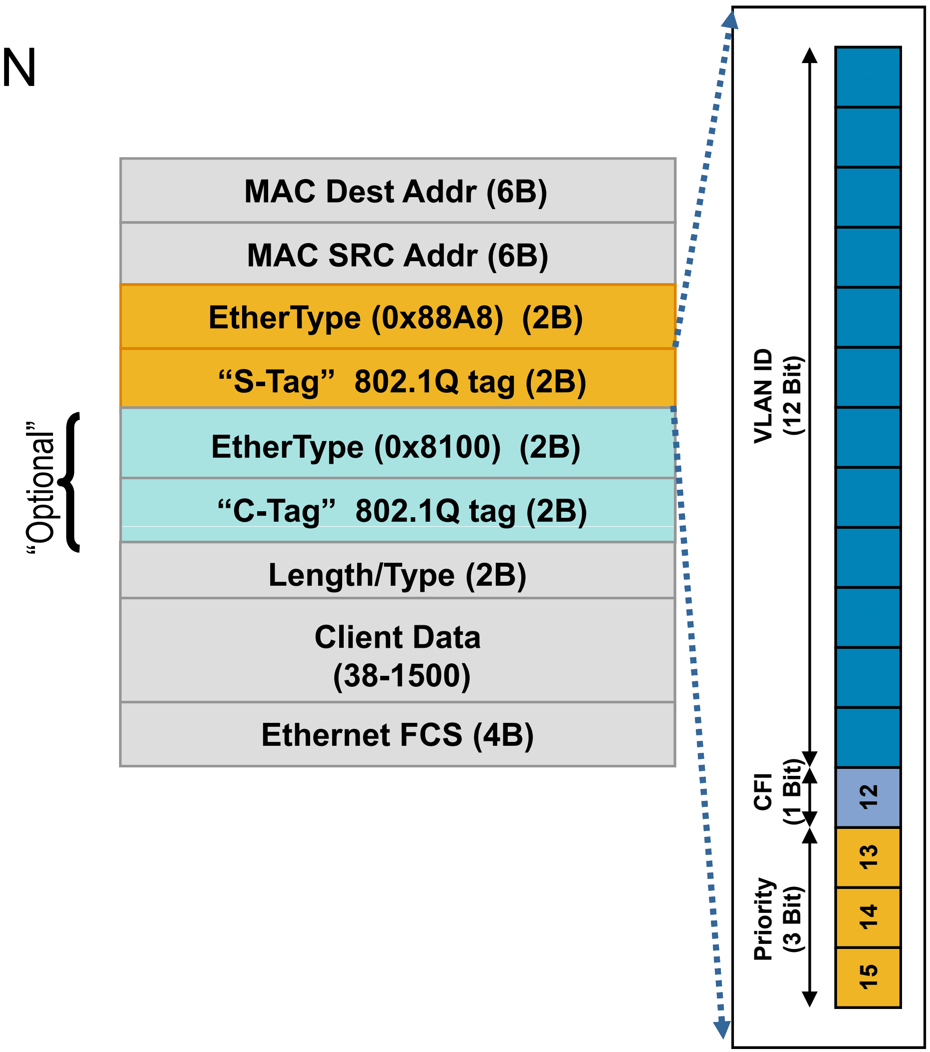
Ethernet Evolution



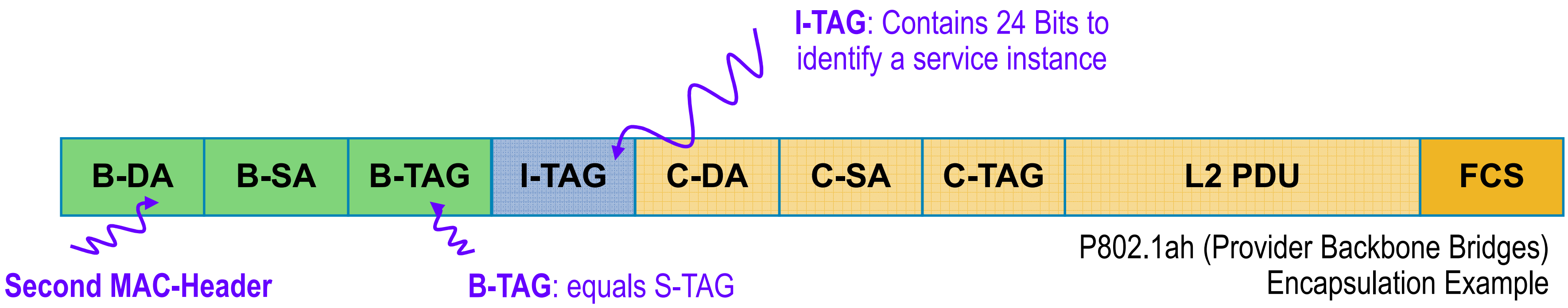
- 802.1D – Media Access Control (MAC) Bridges
  Ethernet bridging / Spanning Tree Protocol
- 802.1Q – Virtual Bridged Local Area Networks
  Tagged frame / Multiple Spanning Tree Protocol
- 802.1ad – Provider Bridges
  VLAN stacking (amendment to 802.1Q)
- 802.1ah – Provider Backbone Bridges
  MAC/VLAN stacking (amendment to 802.1Q)
- 802.1Qay – Provider Backbone Bridges Traffic Engineering
  Traffic engineering extensions based on 802.1ah

IEEE 802.1ad Provider Bridges

- Standardized version of QinQ (VLAN Stacking)
- Customer VLAN Transparency
- Defines C-VLAN and S-VLAN
- Separate customer and provider L2CP
- 4096 service instances
- New Ethertype: 0x88A8



IEEE 802.1ah Provider Backbone Bridges
Main Ideas/Concepts



- Service Scalability

  Define a new "Service Instance Identifier" – 24 Bits wide (taking the place of the former "VLAN"): I-TAG.

- Domain Isolation, MAC-Address Scalability

  Encapsulate Customer MAC-frames at the edge of the network into a "Provider MAC-Frame": New MAC-Header with B-TAG.

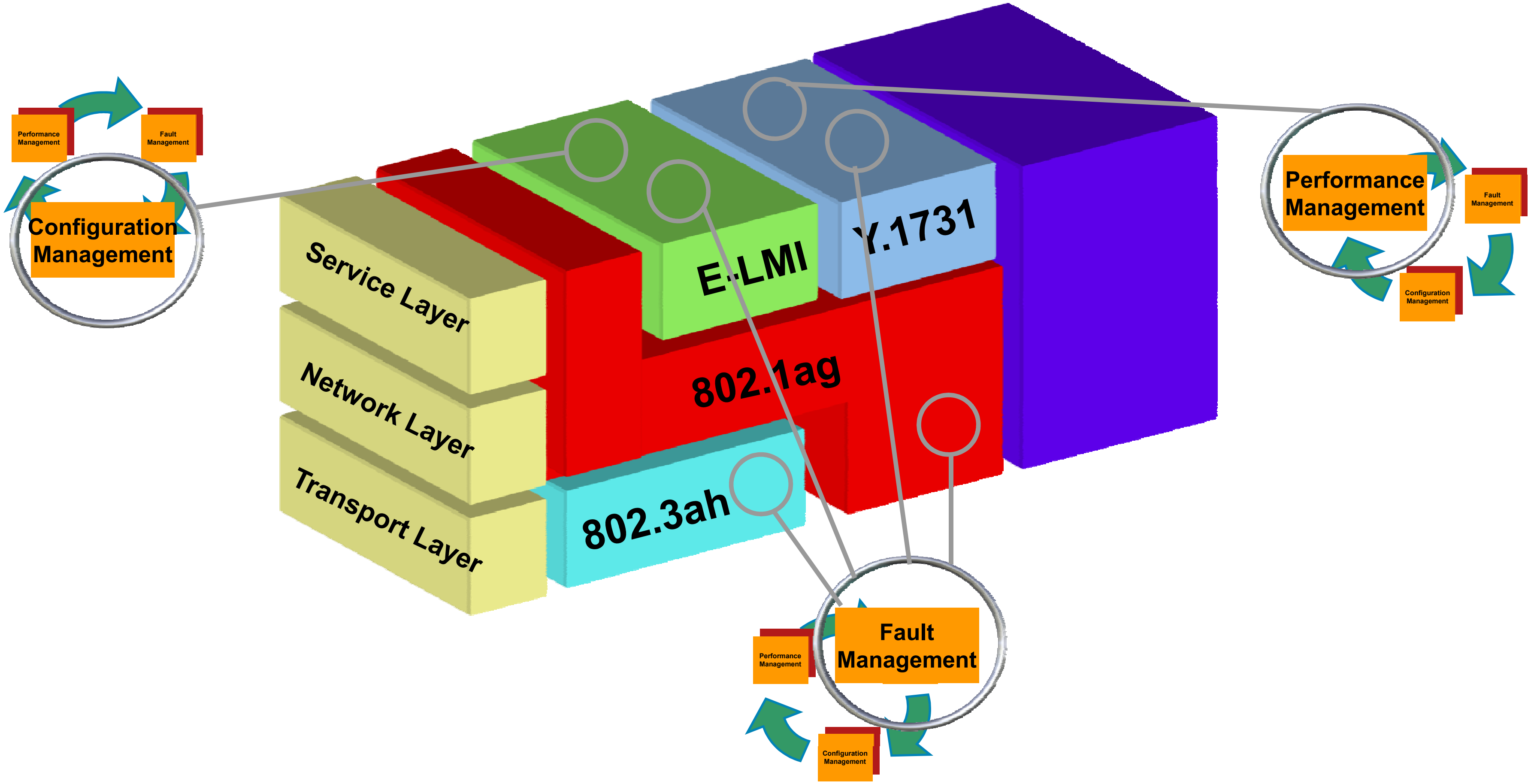
- "Backward Compatibility" to 802.1ad

  Packet header of Provider Backbone Bridges (PBB, P802.1ah) and Provider Bridges (PB, P802.1ad) look the same

IEEE 802.1Qay Provider Backbone Bridges Traffic Engineering

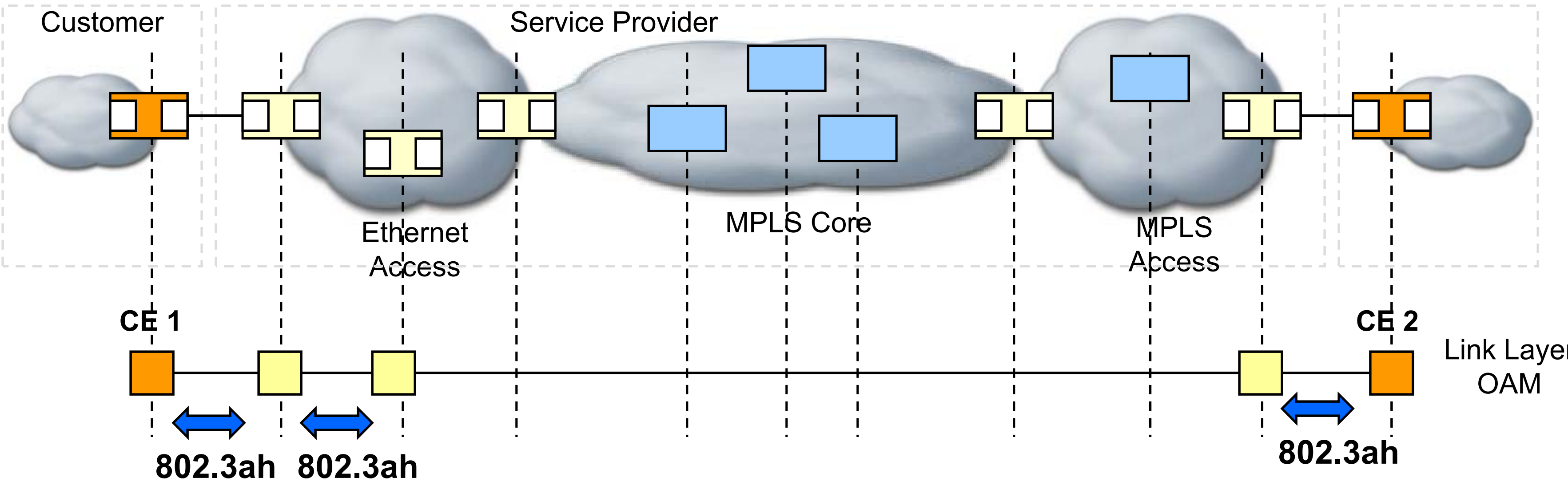
- New work item to define traffic engineering extensions for 802.1ah
- IEEE 802.1 Project Authorization Request (PAR) approved in November 2006
- Standardization expected to take at least 3 years
- Motivated by provider backbone transport (PBT) discussion
- How similar/different PBB-TE and PBT will look is unknown

Ethernet OAM



- IEEE 802.1ag: Connectivity Fault Management (CFM)
- ITU-T Y.1731: OAM functions and mechanisms for Ethernet based networks
- IEEE 802.3ah: Ethernet Link OAM (EFM OAM)
- MEF E-LMI: Ethernet Local Management Interface
- Performance Management using IP, CFM and Y.1731 Mechanisms

802.3ah



- Link Level OAM
- Operates on point-to-point link, not propagated beyond a single hop.
- Slow Protocol (Max rate of 10 frames per second)
- Functions:

  OAM discovery – Discover OAM capabilities on peer device

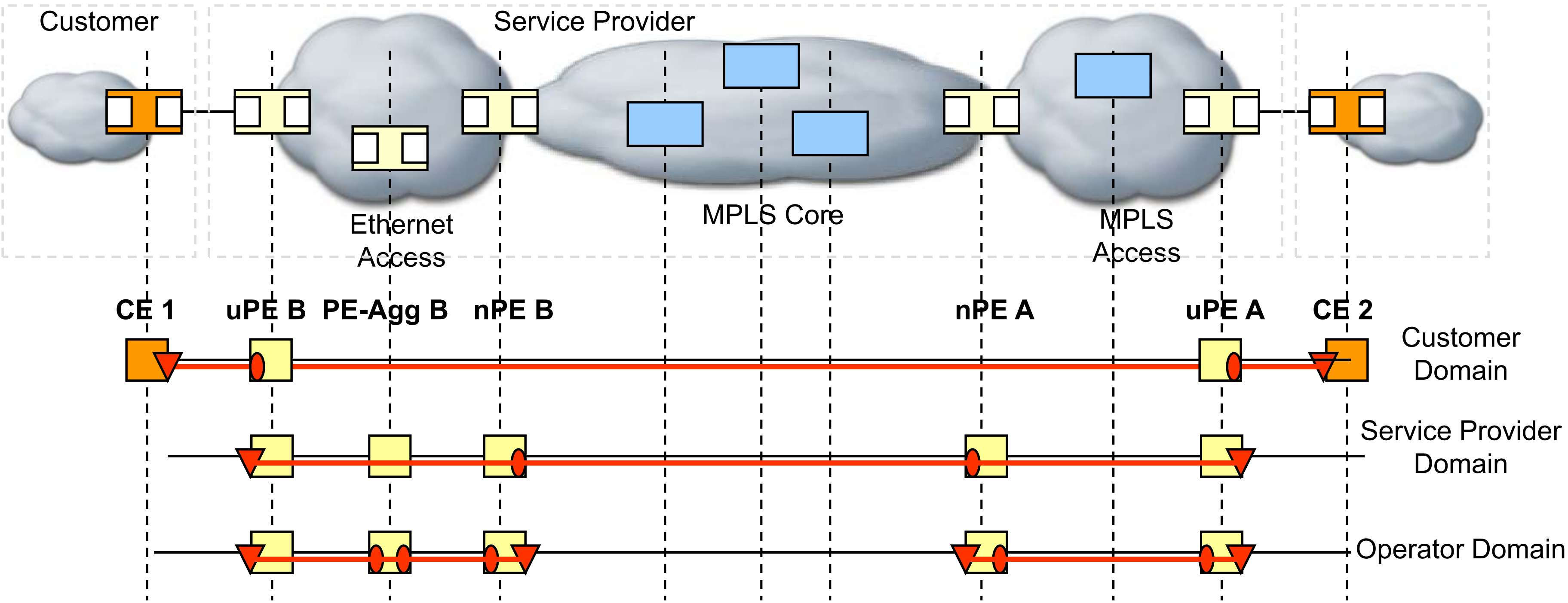
  Link monitoring – Event notification when error thresholds exceeded

  Remote MIB Variable Retrieval – Polling and response (but not writing) of 802.3ah MIB

  Remote Failure indication – Inform peer that receive path is down.

  Remote Loopback – Puts peer in (near-end) intrusive loopback state. Statistics can be collected while testing link.

802.1ag Connectivity Fault Management (CFM)

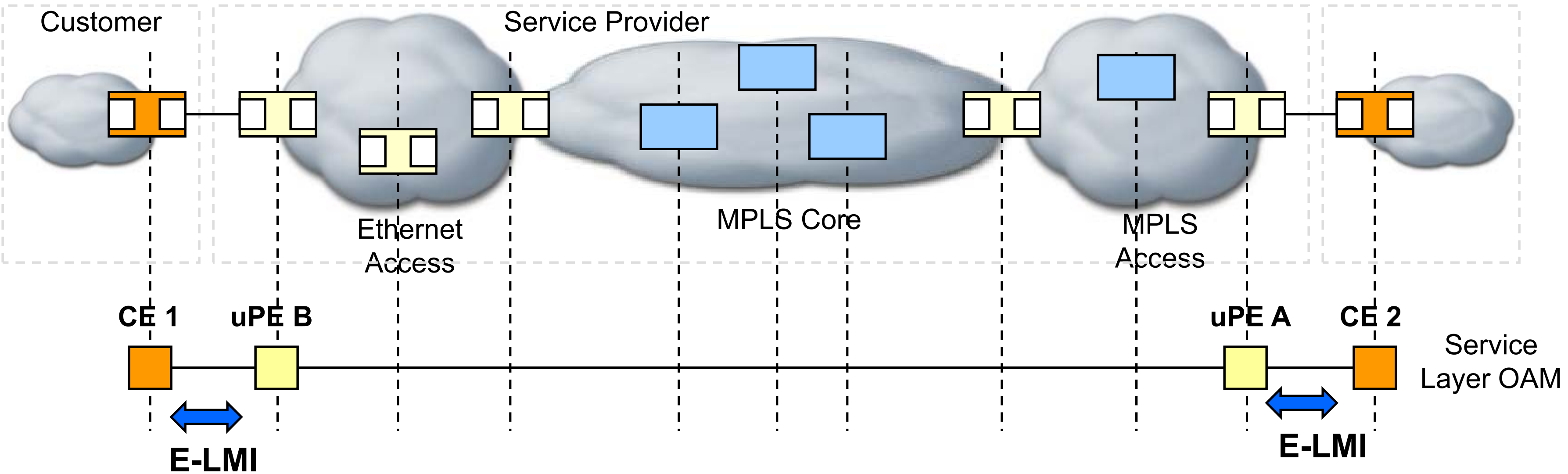


- End to End per EVC OAM
- Hierarchical Maintenance Domains
  - MEPs/MIPs
- Standard Ethernet Frames (in-band)
  - Continuity Check
  - Loopback
  - Link Trace

Y.1731

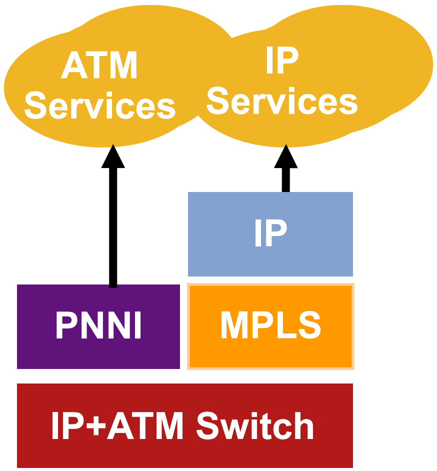
- CFM plus…
  - ETH-LCK (out of service diagnostics)
  - Multicast Loopback
  - AIS
  - TEST
  - Maintenance Communication Channel
  - Experimental OAM
  - Performance Management (Delay, Packet loss, Jitter)

E-LMI

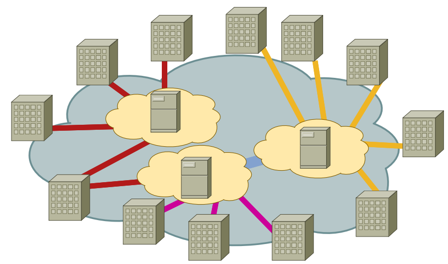


- Asymmetric protocol, applicable on UNI only (uPE to CE)
- Specifies procedures & message formats exchanged and NOT how uPE collects OAM data – relies on Service/Network OAM running uPE to uPE
- Allows uPE to communicate to CE:
  - EVC Status
  - Remote UNI Status
  - CE-VLAN to EVC Map
  - BW Profiles

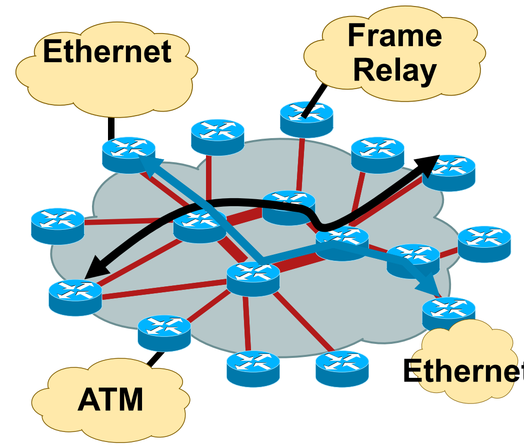
MPLS Evolution



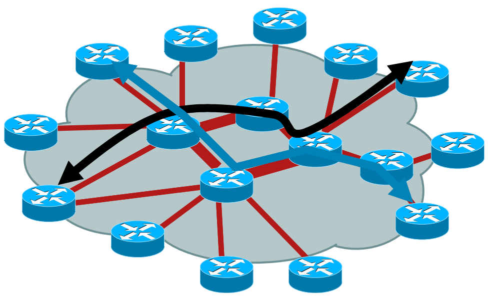
IP + ATM Integration



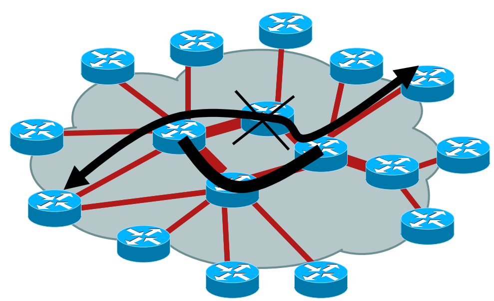
MPLS VPNs: Scalable Network based VPNs



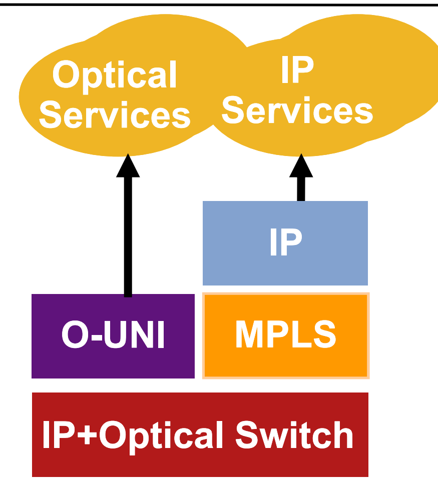
Layer 2 Integration for a converged network



Traffic Engineering: Bandwidth Optimization of traffic

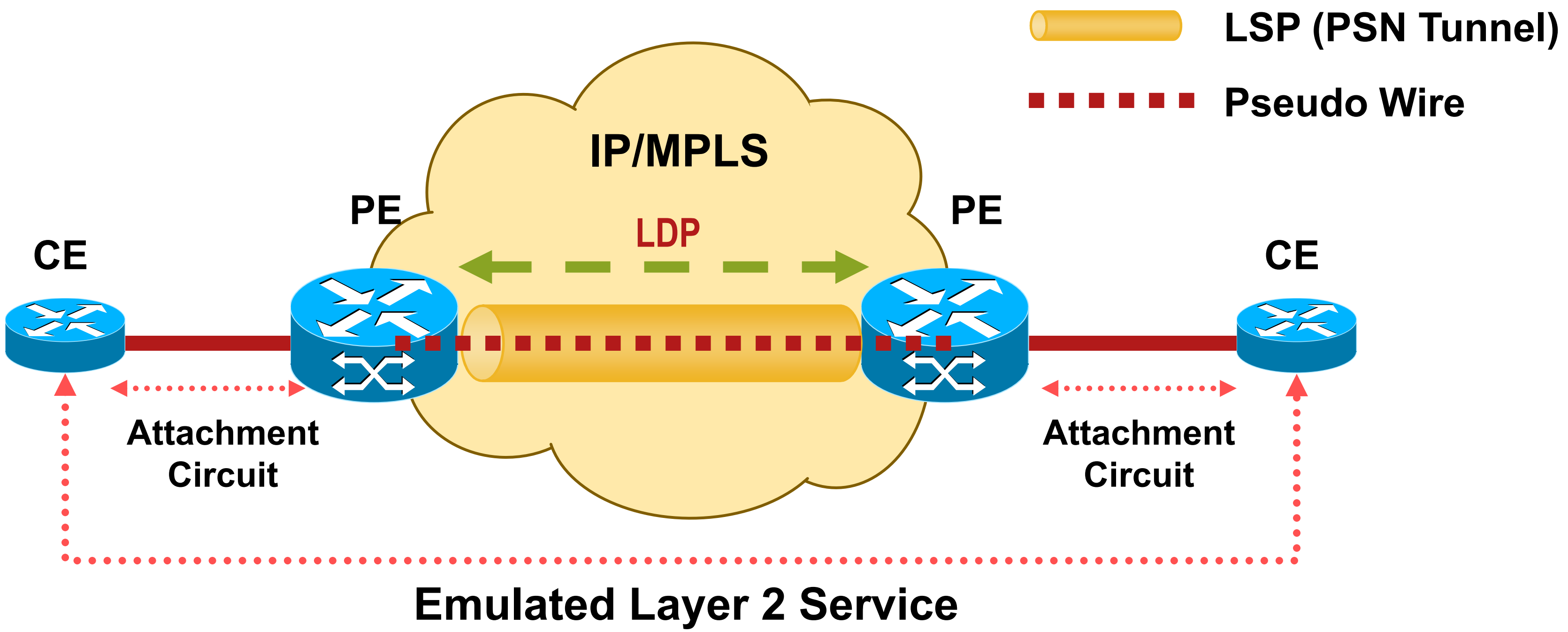


Bandwidth Protection and Resiliency



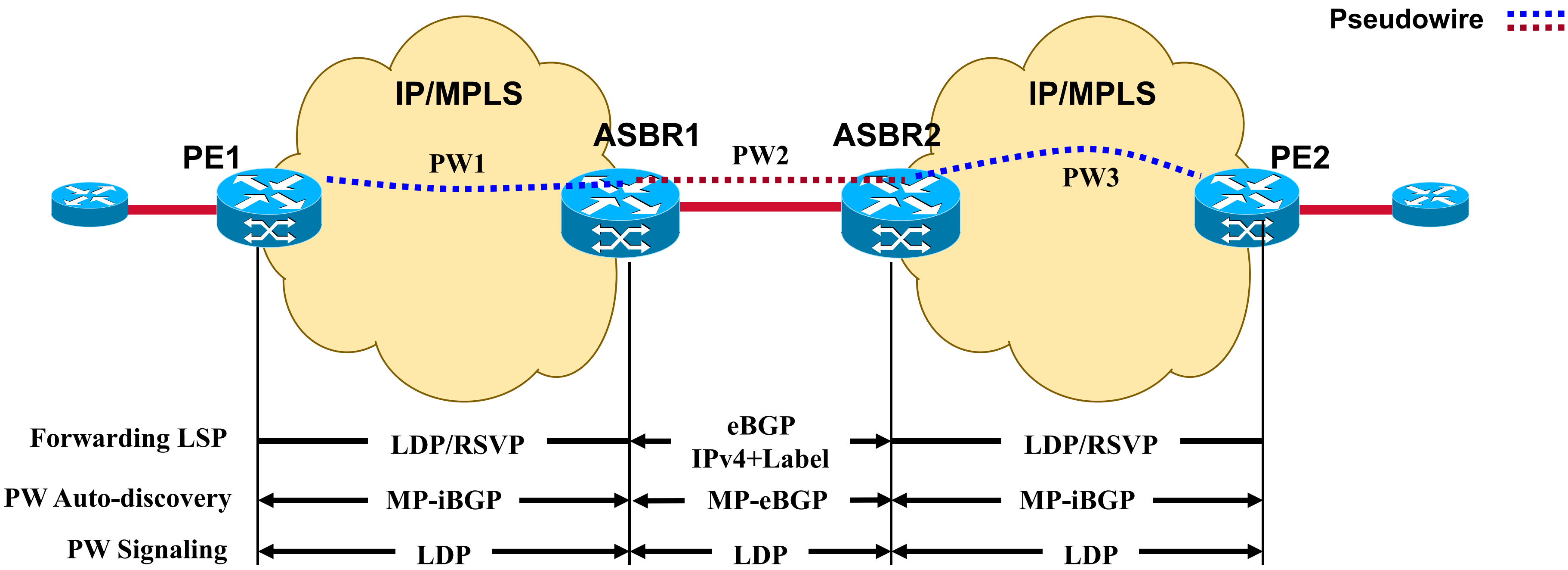
IP+Optical Integration

Pseudo Wire Reference Model



- A pseudowire (PW) connects native Layer 2 attachment circuits
- Establishment of PWs is signaled between PEs using LDP
- LSP ultimately carries PW traffic between PEs

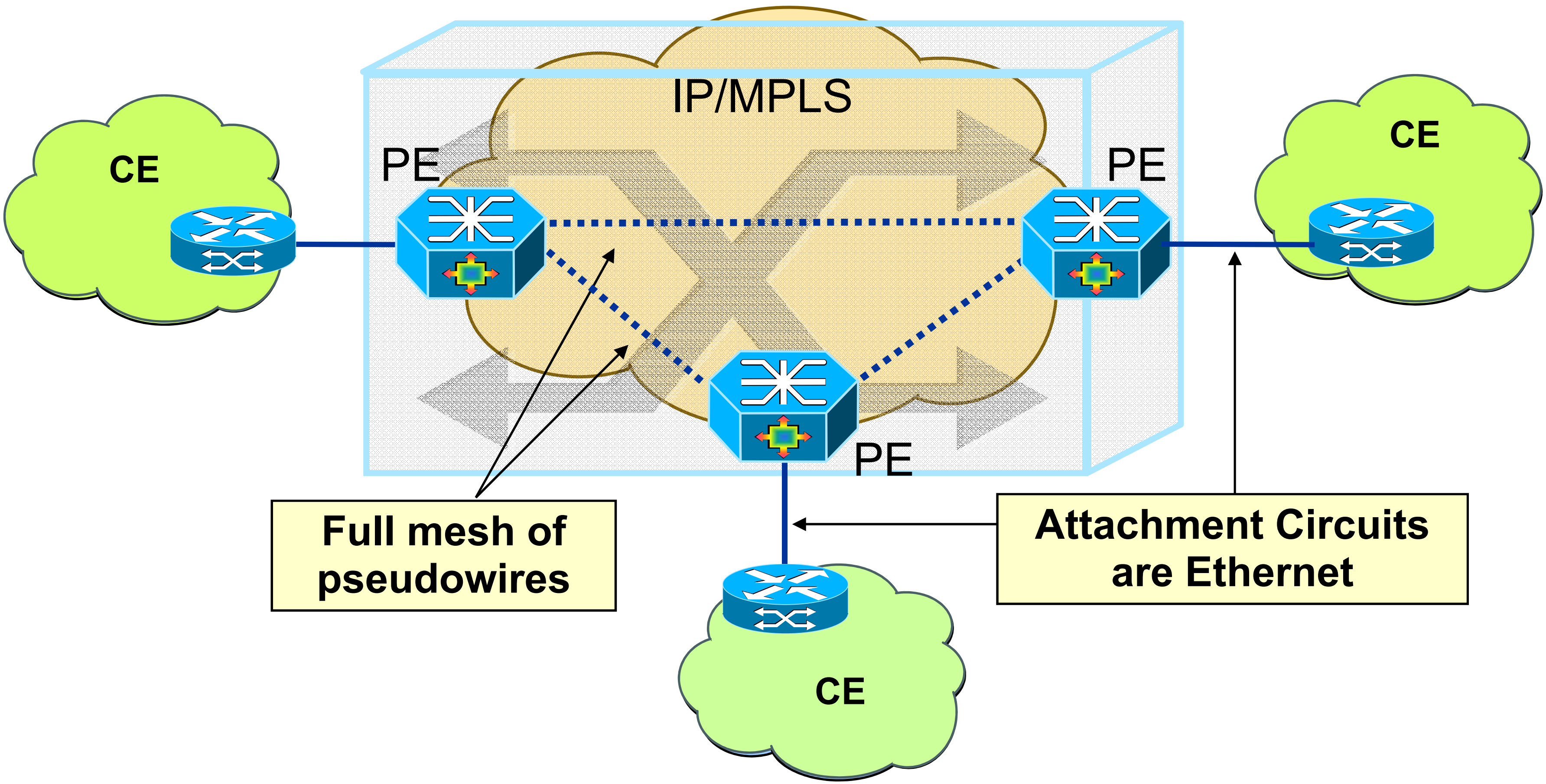
Multi-Segment Pseudowire



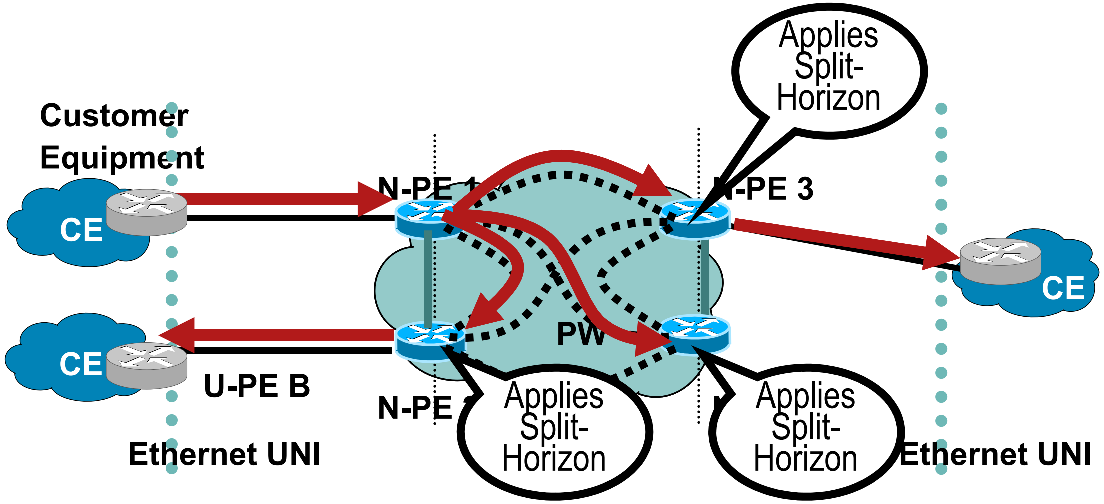
- Provides isolation between administrative domains
- Single (labeled) interface between ASBRs
- Single peering point (only one PW endpoint address leaked between ASs)
- PE and P devices do not learn remote PW endpoint addresses

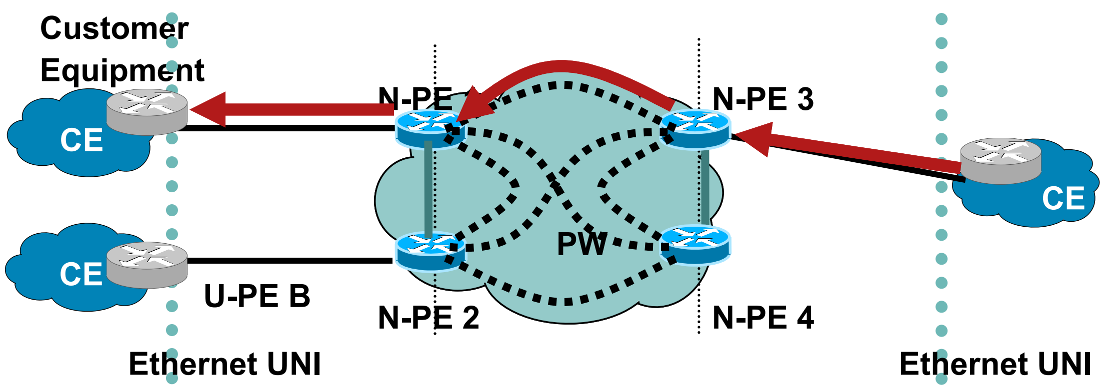
Virtual Private LAN Service (VPLS)

Emulates a multi-point Ethernet domain between a set of PE devices interconnected via pseudowires



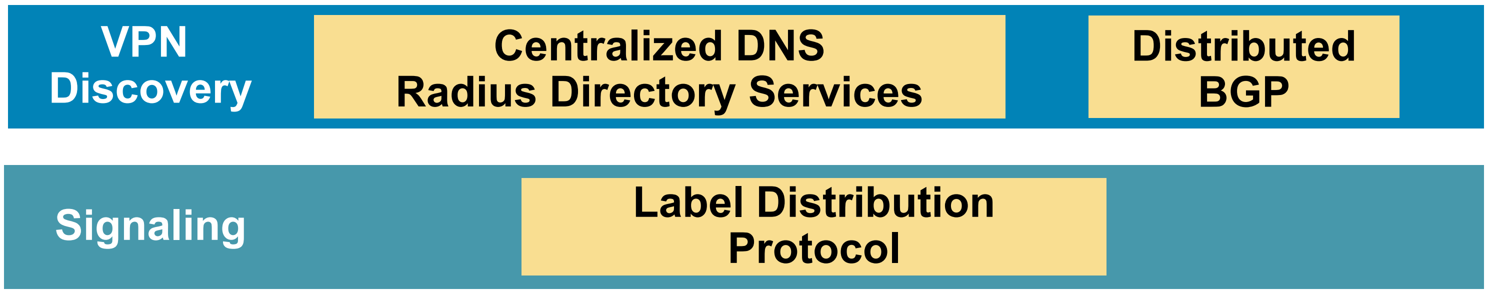
How VPLS works...





- Flooding (Broadcast, Multicast, Unknown Unicast)
- Dynamic learning of MAC addresses on PHY and VCs
- Forwarding
  - Physical Port
  - Virtual Circuit
- VPLS uses Split-Horizon and Full-Mesh of PWs for loop-avoidance in core
  - SP does not run STP in the core

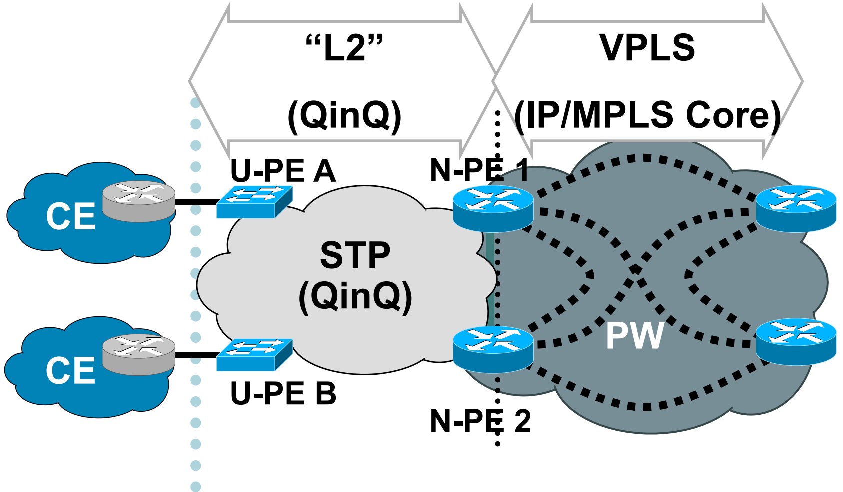
VPLS Autodiscovery and Signaling



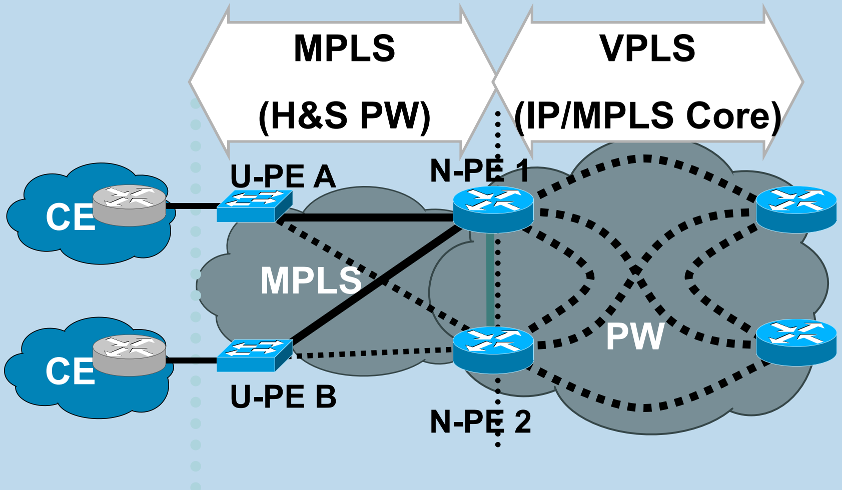
- **Autodiscovery: BGP is the configuration agent**
  - True autodiscovery of VPN members
  - No need to explicitly list them
- **Signaling: LDP sets up a standard PW**
  - PWs signal other information such as attachment circuit state, sequencing information, etc.

H-VPLS Access: QinQ or MPLS at Edge

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

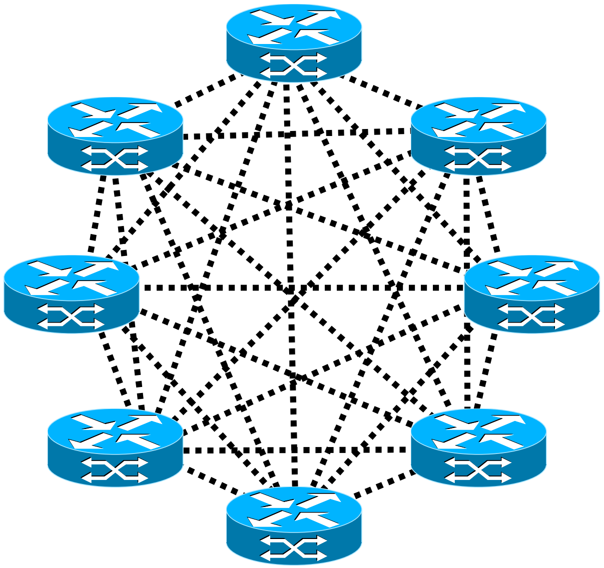


- H-VPLS with MPLS Access
- Uses PW EoMPLS circuit to backhaul traffic from U-PE to N-PE



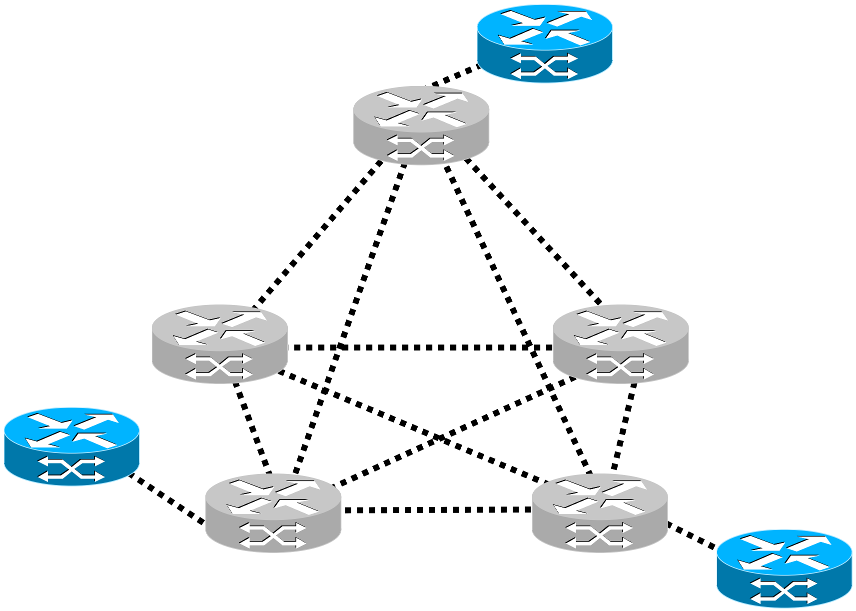
Why H-VPLS? Greater Scale

Flat VPLS



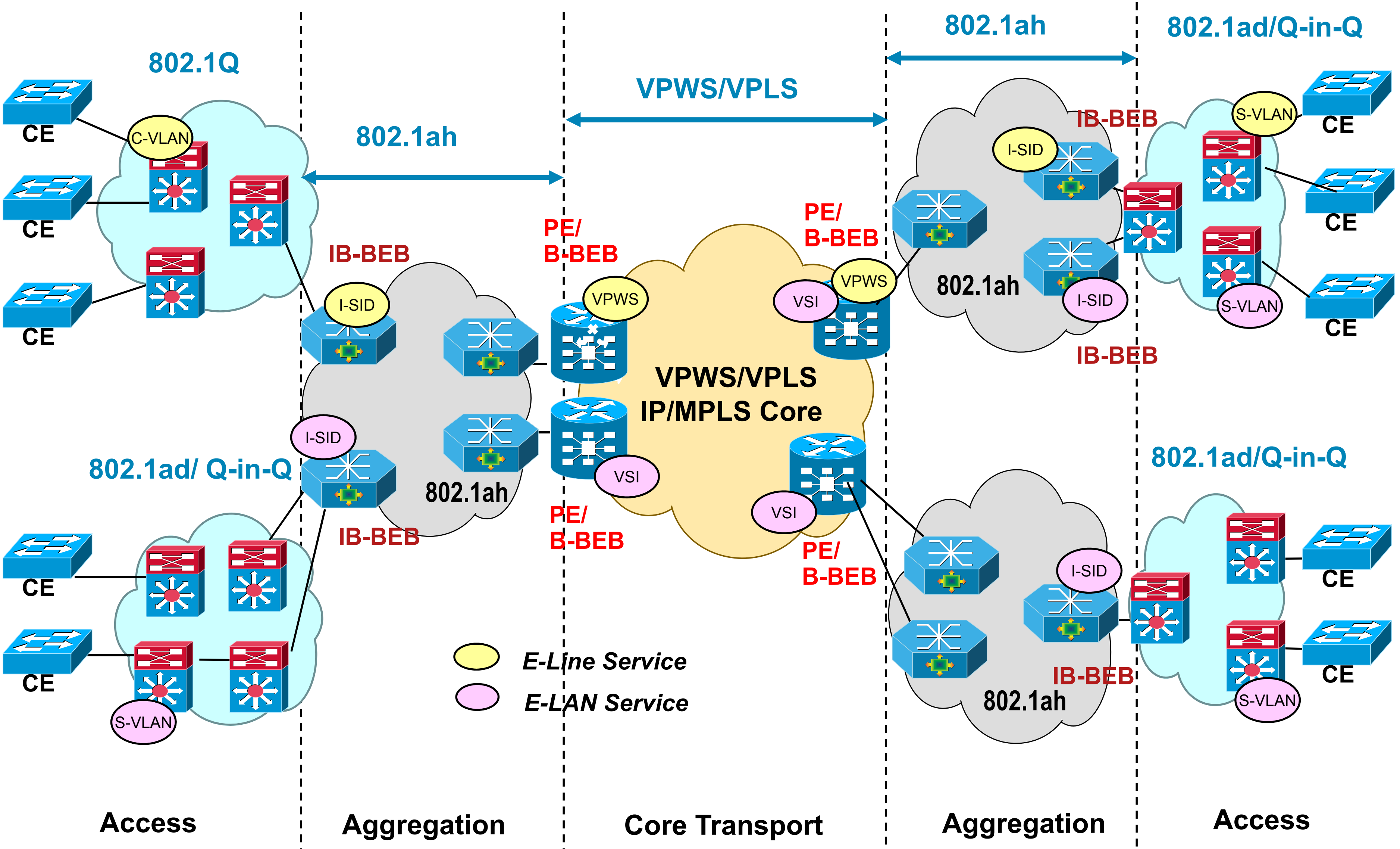
- Full PW mesh from the edge
- Higher signaling overhead
- Packet replication done at the edge
- Node discovery and provisioning extend end-to-end

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 with 802.1ah Aggregation



Characteristics of 802.1ah Aggregation over MPLS core

- Improved scalability for native Ethernet aggregation

  Service Instances scaling: from 4K of 802.1ad to 16M of 802.1ah

  MAC scaling: MAC-in-MAC: customer MAC address hiding.

- Use cases:

  SP has converged MPLS core and prefer to use native Ethernet aggregation to interconnect the 802.1ad (PBN)/Q-in-Q/802.1Q islands.

- Operation:

  – The ingress IB-BEB maps a 12-bit S-VLAN ID from the PBN to a 24-bit I-SID in the I-Tag of 802.1ah PBBN.

  – B-VID is used to build point-to-point or multipoint tunnels between BEB's.

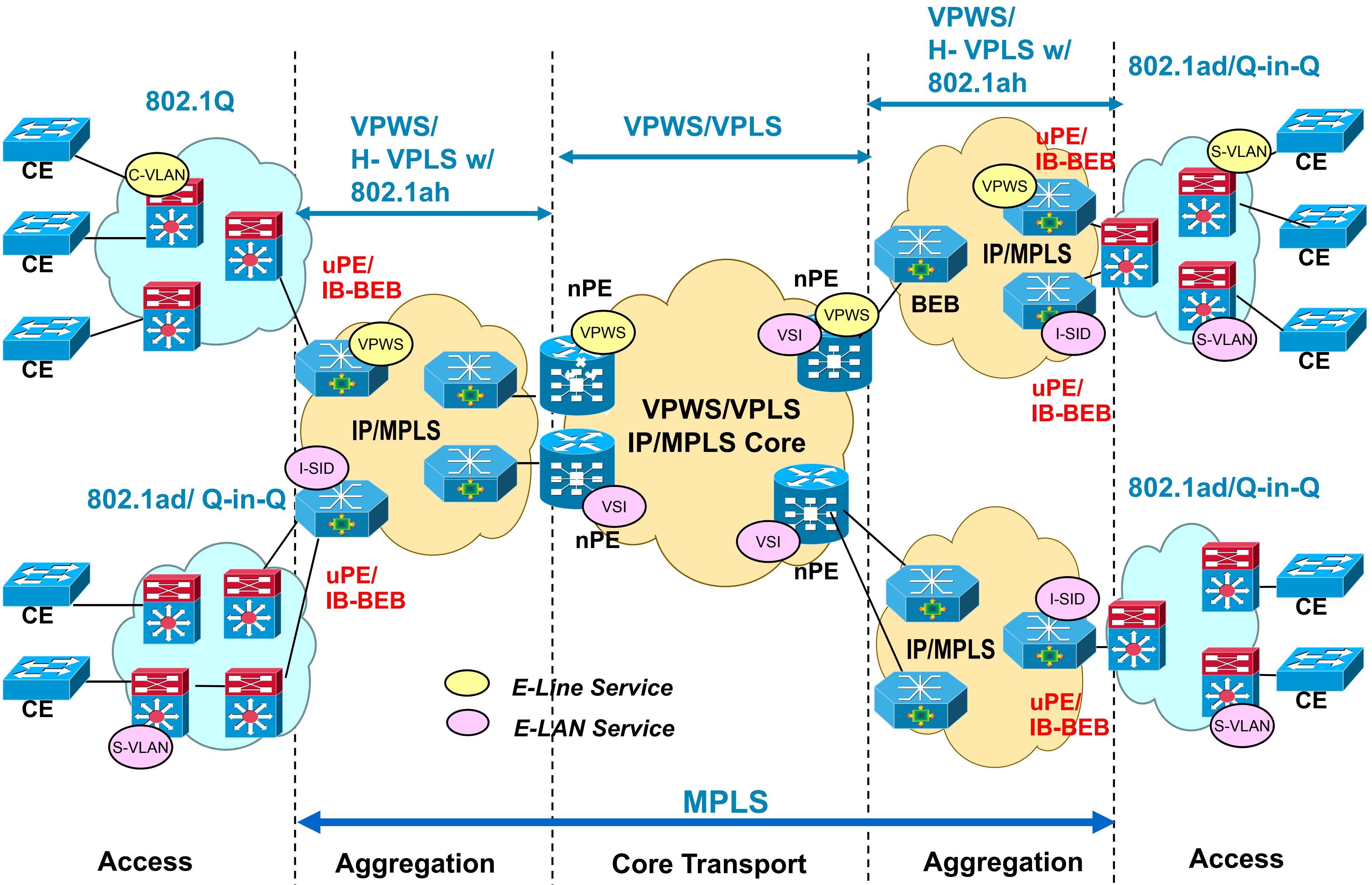
  – Path selection in PBBN is based on STP (alternative is turning off STP and use NMS). STP in PBN are confined in its own island, not in PBBN.

  – Signaling for B-VID registration is based on GVRP, MVRP. Otherwise, B-VID can be provisioned

  – A PBBN assigns a multicast MAC address per I-SID for flood/broadcast containment

  – At the PE/B-BEB, B-VID or I-SID, or group of I-SID is mapped to the VSI depending on the topologies and interface type used.

H-VPLS with MPLS Aggregation and 802.1ah Extension



Characteristics of H-VPLS w/ 802.1ah extension

- Improved scalability for native Ethernet aggregation

  Service Instances scaling: from 4K of 802.1ad to 16M of 802.1ah

  MAC scaling: MAC-in-MAC: customer MAC address hiding.

- Use cases:

  SP has converged MPLS core and MPLS in the Aggregation/Access.

- Operations:

  – The ingress IB-BEB maps a 12-bit VLAN ID from the PBN to a 24-bit I-SID in the I-Tag of PBBN (802.1ah)

  – A Backbone VLAN ID (B-VID) is used to build point-to-point or multipoint tunnels between BEB's.

  – MPLS control plane for core and aggregation provides simplified operation

    • Single VSI for an customer E-LAN connections

    • Auto-discovery aids provisioning

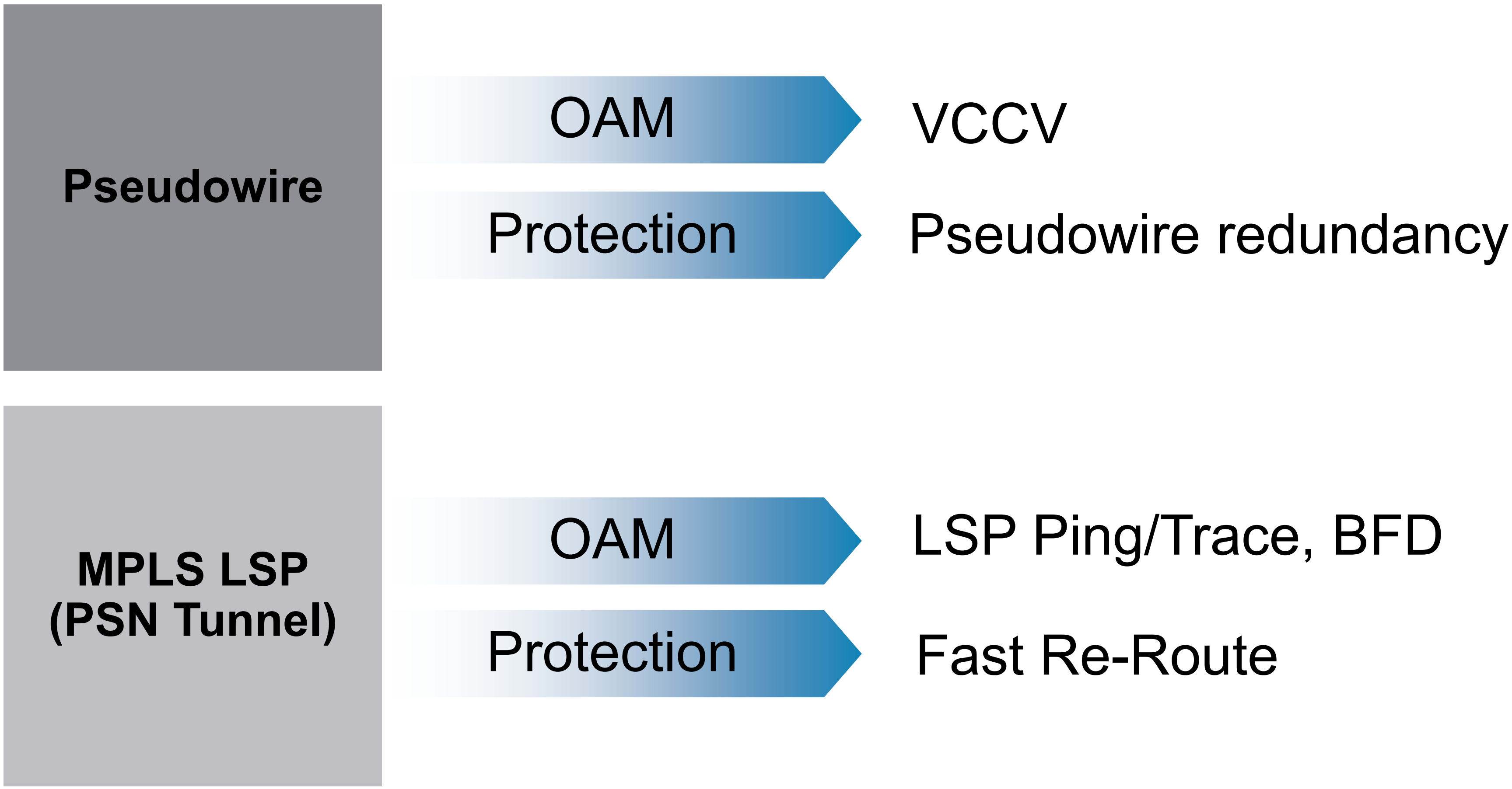
    • No STP

    • Using MPLS DiffServ, HA, p2mp, TE, and OAM

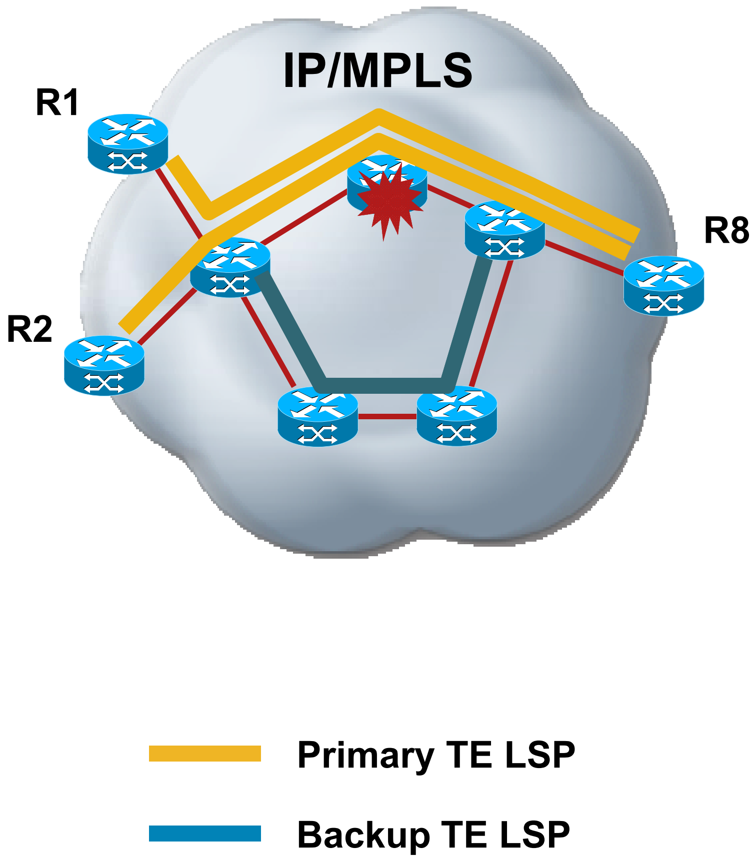
Standardization Status for Ethernet Transport over MPLS

- RFC 3985 (informational)
  PWE3 Architecture
- RFC 4447 (standards track)
  Pseudowire Setup and Maintenance using the Label Distribution Protocol (LDP)
- RFC 4448 (standards track)
  Encapsulation Methods for Transport of Ethernet Over MPLS Networks
- RFC 4385 (standards track)
  Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
- draft-ietf-pwe3-segmented-pw
  Segmented Pseudo Wire
- draft-ietf-pwe3-dynamic-ms-pw
  Dynamic Placement of Multi Segment Pseudo Wires
- RFC 4762 (standards track)
  VPLS Using LDP Signaling
- draft-ietf-l2vpn-signaling
  Provisioning, Autodiscovery, and Signaling in L2VPNs

Pseudowire OAM and Protection



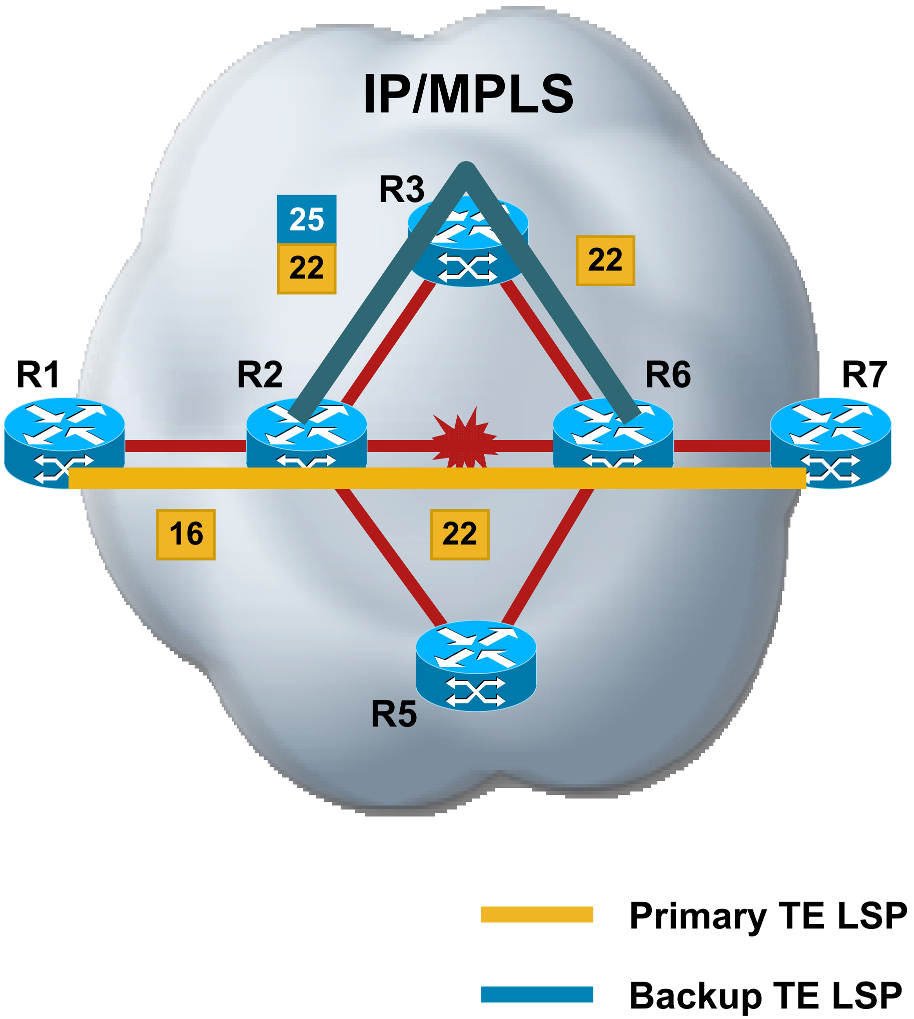
MPLS TE Fast Re-Route (FRR)



- Local protection
- Subsecond recovery against node/link failures
- Scalable 1:N protection
- Greater protection granularity
- Bandwidth protection
- Supports different LSP types (P2P, P2MP, MP2P, MP2MP)
- BFD may help with failure detection

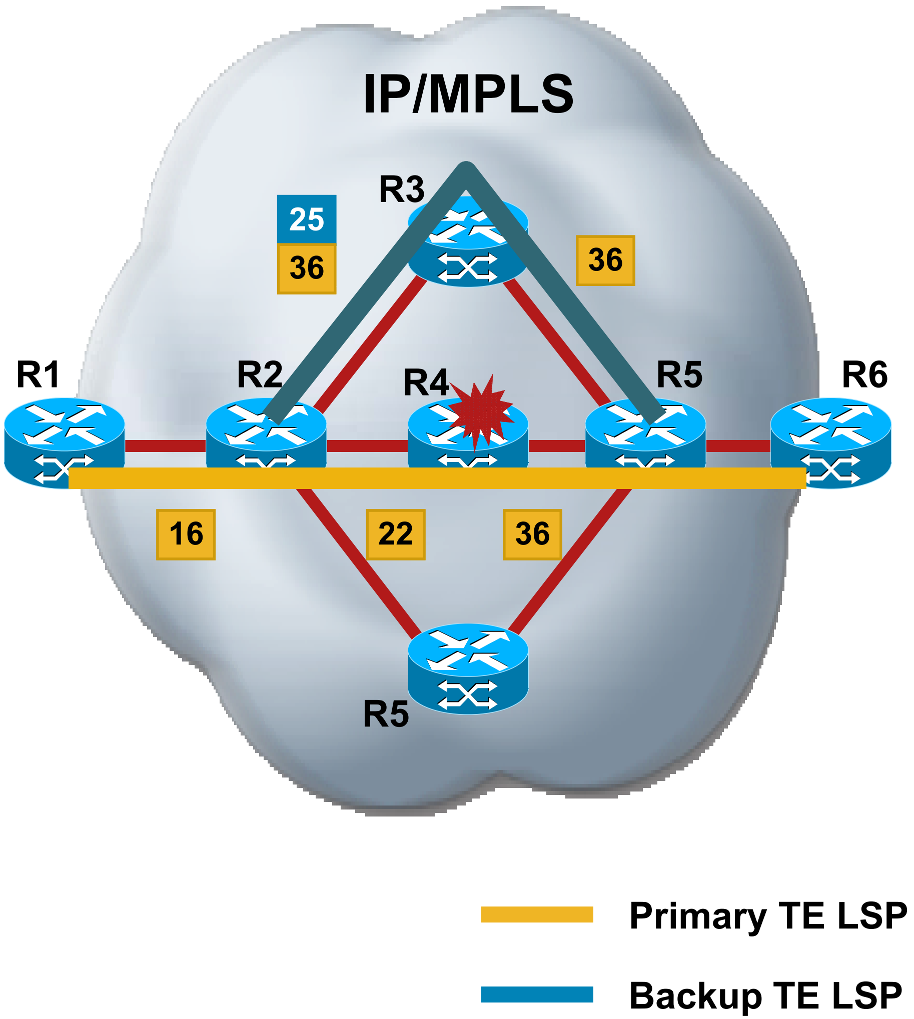
FRR Link Protection Operation

- Requires next-hop (NHOP) backup tunnel
- Point of Local Repair (PLR) swaps label and pushes backup label
- Backup terminates on Merge Point (MP) where traffic rejoins primary
- Restoration time expected under ~50 ms (local protection)



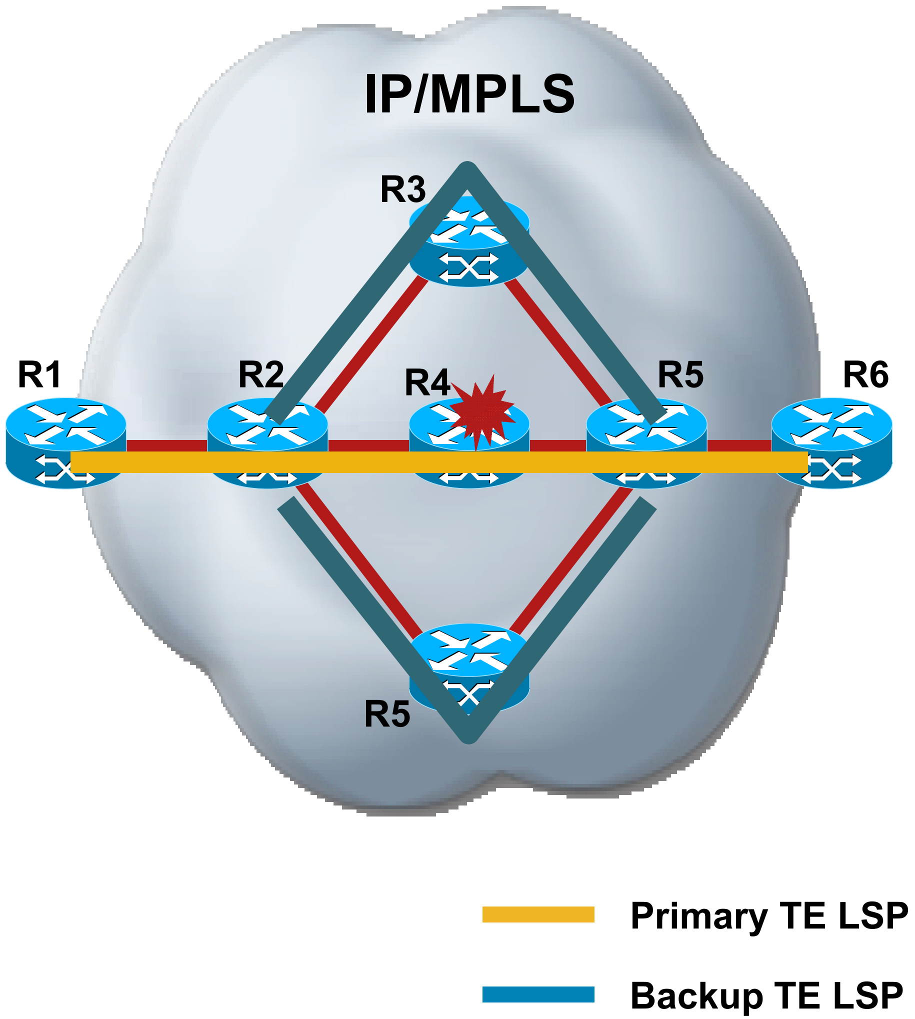
FRR Node Protection Operation

- Requires next-next-hop (NNHOP) backup tunnel
- Point of Local Repair (PLR) swaps next-hop label and pushes backup label
- Backup terminates on Merge Point (MP) where traffic rejoins primary
- Restoration time depends on failure detection time, but minimized (local protection)



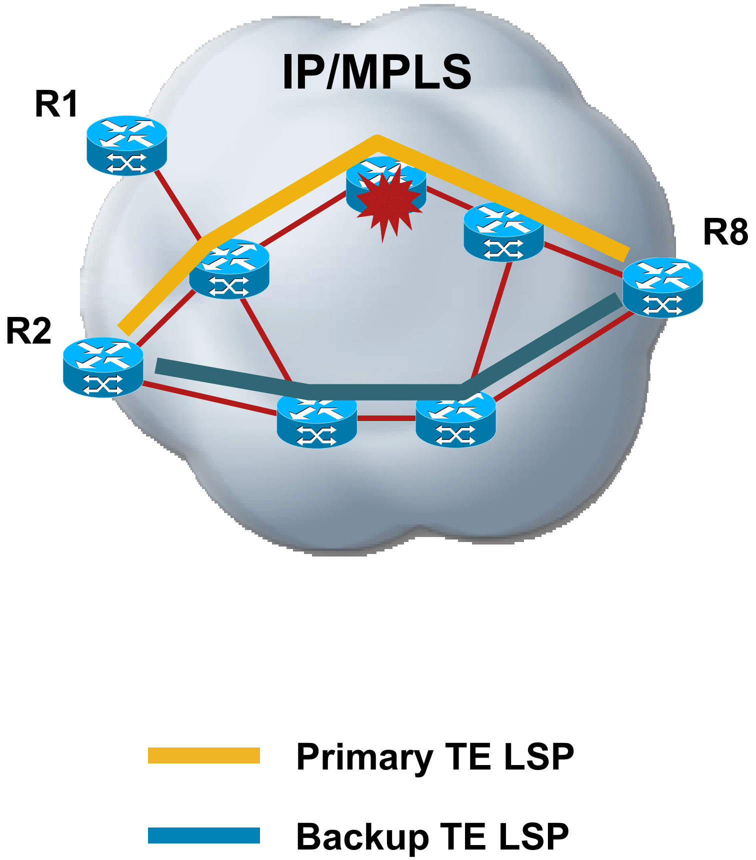
Bandwidth Protection

- Backup tunnel with associated bandwidth capacity
- Backup tunnel may or may not actually signal bandwidth
- PLR will decide best backup to protect primary (nhop/nnhop, class-type, node-protection flag)

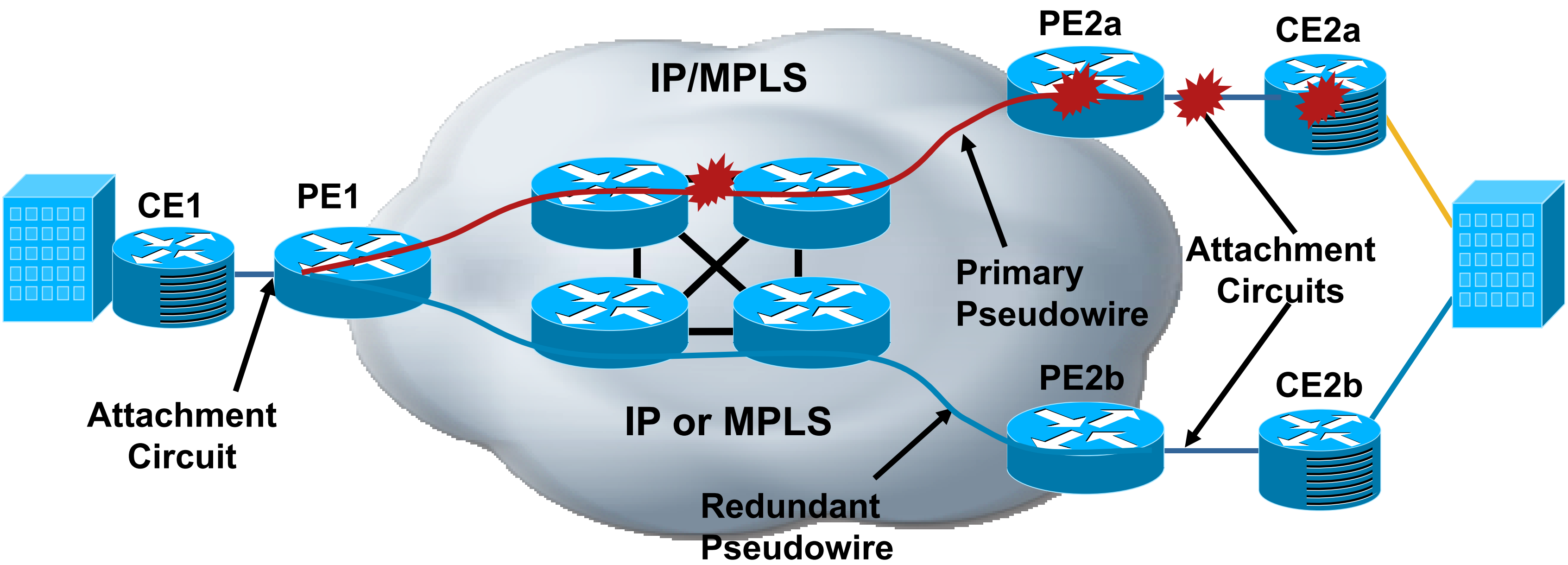


What about Path Protection?

- Primary and backup share head and tail, but diversely routed
- Expected to result in higher restoration times compared to local protection
- Doubles number of TE LSPs (1:1 protection)



Pseudowire Redundancy



- Failure notification via LDP
- Failure detection possible via VCCV+BFD
- Failures within MPLS network to be protected by MPLS FRR

Standardization Status for MPLS Protection

- RFC 4420 (Standards Track)

  RSVP-TE: Extensions to RSVP for LSP Tunnels

- RFC 4090 (Standards Track)

  Fast Reroute Extensions to RSVP-TE for LSP Tunnels

MPLS OAM

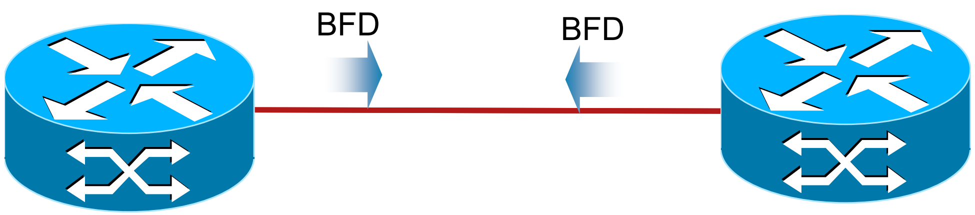
Fault	Detection	MPLS BFD
	Notification	MPLS MIBs / SNMP traps
	Verification	MPLS LSP Ping (ping mode)
	Isolation	MPLS LSP Ping (trace mode)
Performance Management		MPLS LSP Ping (ping mode)

MPLS LSP Ping/Traceroute

Requirement	▪ Detect MPLS traffic black holes or misrouting ▪ Isolate MPLS faults ▪ Verify data plane against the control plane ▪ Detect MTU of MPLS LSP paths ▪ Support different LSP types (P2P, P2MP, MP2P)
Solution	• MPLS LSP ping (ICMP) for connectivity checks • MPLS LSP traceroute for hop-by-hop fault localization • MPLS LSP traceroute for path tracing
Applications	▪ IPv4 LDP prefix, VPNv4 prefix: tunnel monitoring ▪ TE tunnel ▪ L2 VPNs
RFC Standards	• RFC 4377, RFC 4378, RFC4379

Bidirectional Forwarding Detection (BFD)

- Simple, fixed-field, hello protocol
- Nodes transmit BFD packets periodically over respective directions of a path
- If a node stops receiving BFD packets some component of the bidirectional path is assumed to have failed
- May operate in asynchronous or demand modes



MPLS BFD vs. LSP Ping

Method	Data Plane Failure Detection	Control Plane Consistency	Protocol Overhead
LSP ping	YES	YES	Higher than BFD
MPLS BFD	YES	NO	Low

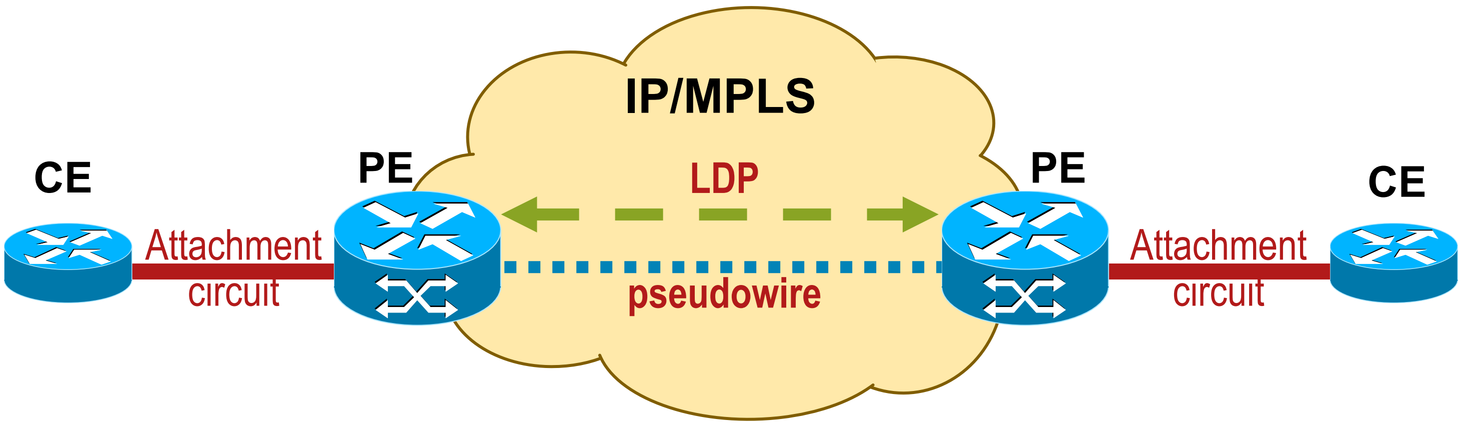
MPLS BFD complements LSP Ping to Detect a Data Plane Failure in the Forwarding Path of a MPLS LSP

Supported FECs:
RSVP IPv4/IPv6 Session, LDP IPv4/IPv6 Prefix
VPN IPv4/IPv6 Prefix, Layer 2 VPN, Layer 2 Circuit ID

Virtual Circuit Connection Verification (VCCV)

Requirement	• Ability to provide end-to-end fault detection and diagnostics for an emulated pseudowire service One tunnel can serve many pseudowires MPLS LSP ping is sufficient to monitor the PSN tunnel (PE-PE connectivity), but not VCs inside of tunnel
Solution	▪ VCCV allows sending control packets in band of pseudowires (PW) ▪ Two components Signaling component: communicate VCCV capabilities as part of VC label advertisement Switching component: cause the PW payload to be treated as a control packet Type 1: uses Protocol ID of PW Control word Type 2: use MPLS router alert label Type 3: manipulate TTL exhaust
Applications	▪ Layer 2 transport over MPLS FRoMPLS, ATMoMPLS, EoMPLS
IETF Standards	RFC 5085 draft-ietf-pwe3-vccv-bfd-01

Pseudowire Status Notification via LDP

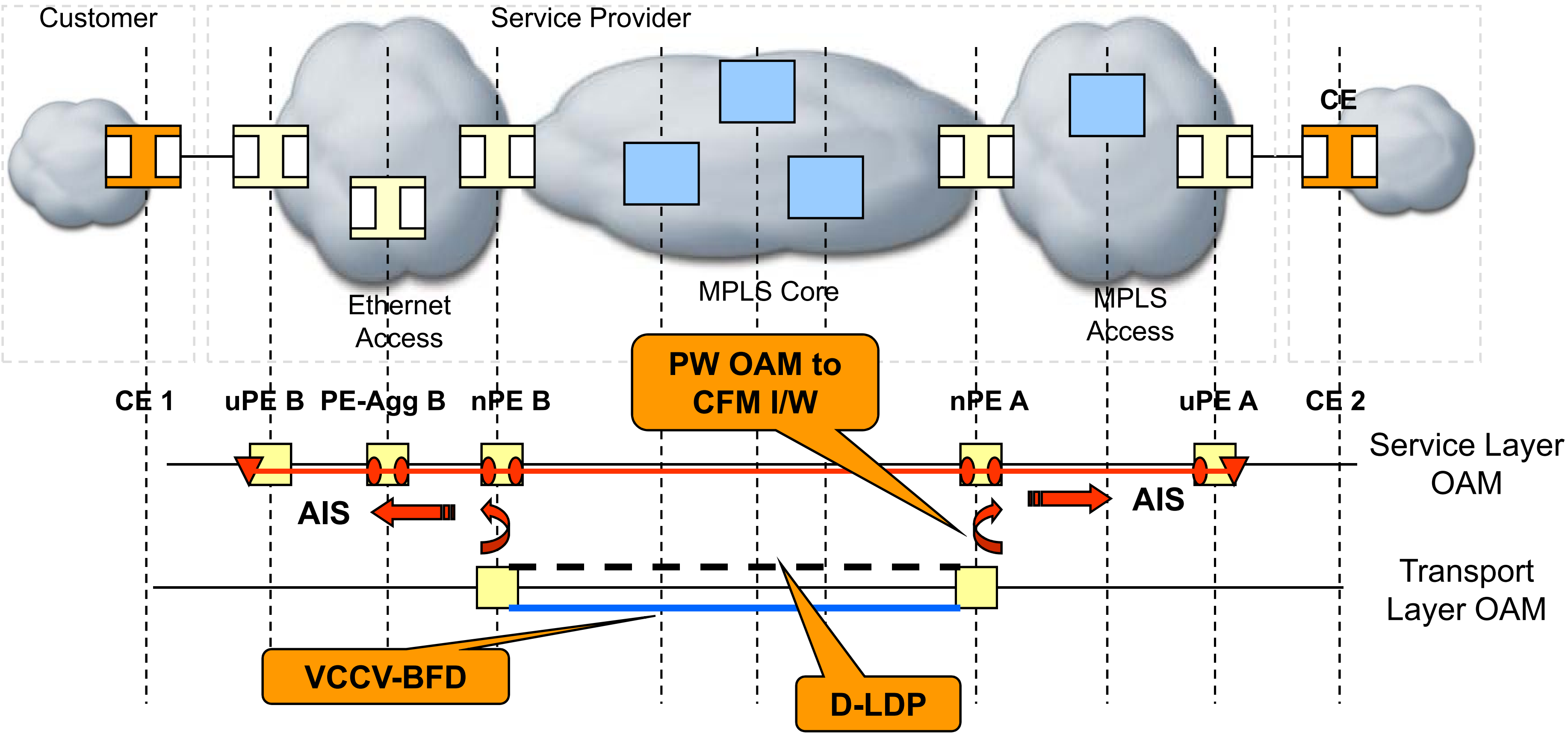


- Pseudowire endpoints negotiate use of status TLV in LDP Notification messages
- Status TLV codes
    - 0x00000000 - Pseudowire forwarding (clear all failures)
    - 0x00000001 - Pseudowire Not Forwarding
    - 0x00000002 - Local Attachment Circuit (ingress) Receive Fault
    - 0x00000004 - Local Attachment Circuit (egress) Transmit Fault
    - 0x00000008 - Local PSN-facing PW (ingress) Receive Fault
    - 0x00000010 - Local PSN-facing PW (egress) Transmit Fault
- Endpoints rely on LDP label withdrawal messages if status TLV not supported

MPLS Performance Management

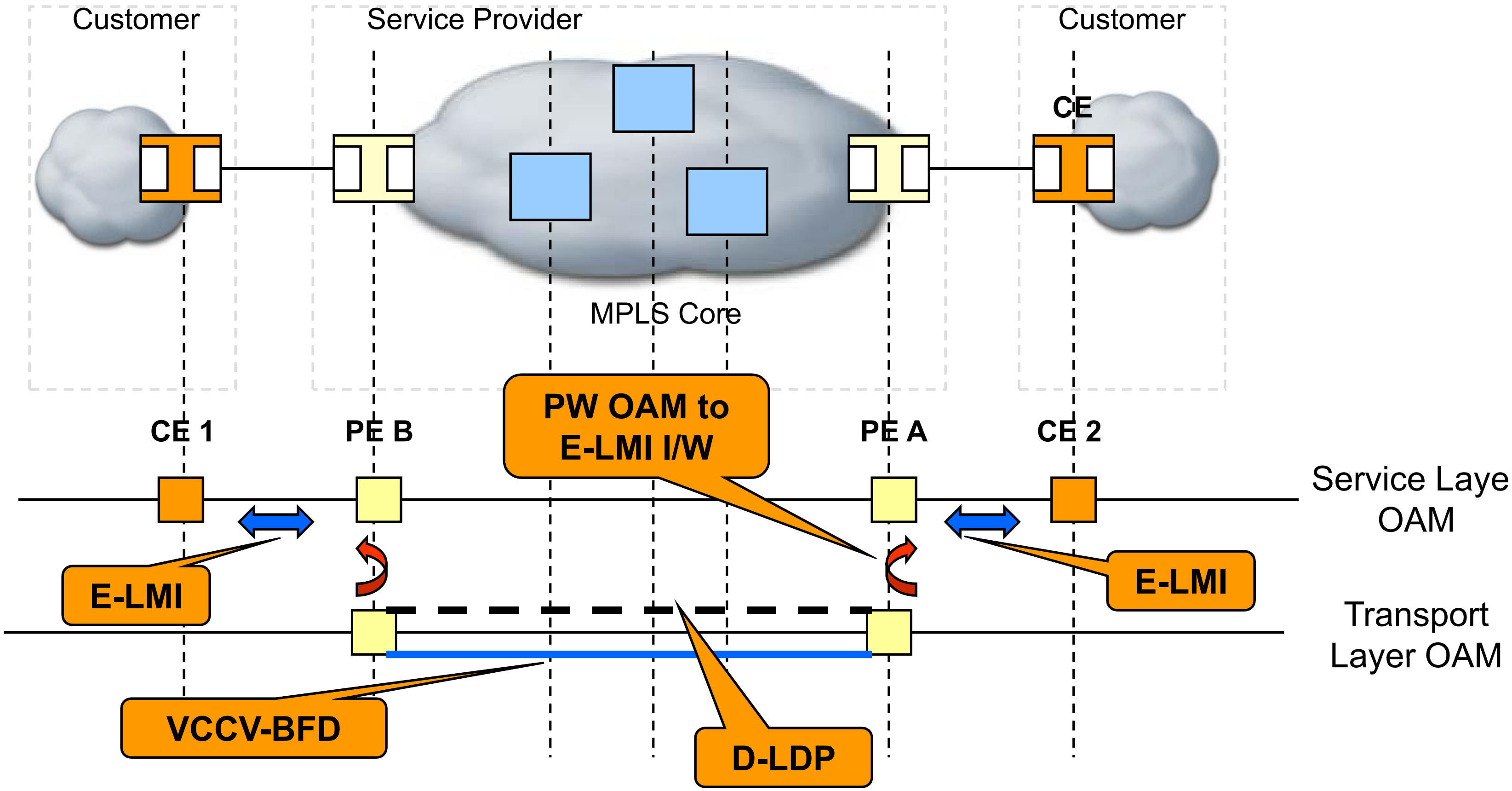
- LSP Ping includes packet timestamp
- LSP Ping can be used to measure packet delay, jitter and loss
- Applies to all different LSP types (P2P, P2MP, MP2P)
- Similar to IP performance management

Inter-working Scenarios: MPLS PW OAM to CFM



- Directed-LDP & VCCV (BFD mode) running between nPEs.
- D-LDP for defect notification, VCCV for defect detection
- Requires CFM AIS/RDI

Inter-working Scenarios: MPLS PW OAM to E-LMI



- Directed-LDP & VCCV (BFD mode) running between PEs.
- D-LDP for defect notification, VCCV for defect detection
- Defects detected/communicated by PW OAM are relayed to E-LMI via I/W function on PE.

Standardization Status for MPLS OAM

- draft-ietf-bfd-base
  Bidirectional Forwarding Detection
- draft-ietf-bfd-mpls
  BFD For MPLS LSPs
- draft-ietf-pwe3-vccv-bfd
  BFD for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)
- RFC 4379 (Standards Track)
  Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
- RFC 5085 (Standards Track)
  Pseudo Wire Virtual Circuit Connectivity Verification (VCCV)
- draft-ietf-mpls-p2mp-lsp-ping (Standards Track)
  Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping
- draft-ietf-mpls-remote-lsp-ping
  Proxy LSP Ping
- draft-ietf-mpls-mcast-cv (Standards Track)
  Connectivity Verification for Multicast Label Switched Paths

Other Packet Transport Proposals

- Provider Backbone Transport / Provider Backbone Bridge – Traffic Engineering
- ITU-T Transport MPLS (T-MPLS)

Provider Backbone Transport

- In a sentence:

  Basically using 802.1ah data-plane functionality with OSS/NMS provisioning in lieu of IEEE control protocols (MSTP, GVRP, etc.) to setup P2P VCs.

- It Consists of the following three components:

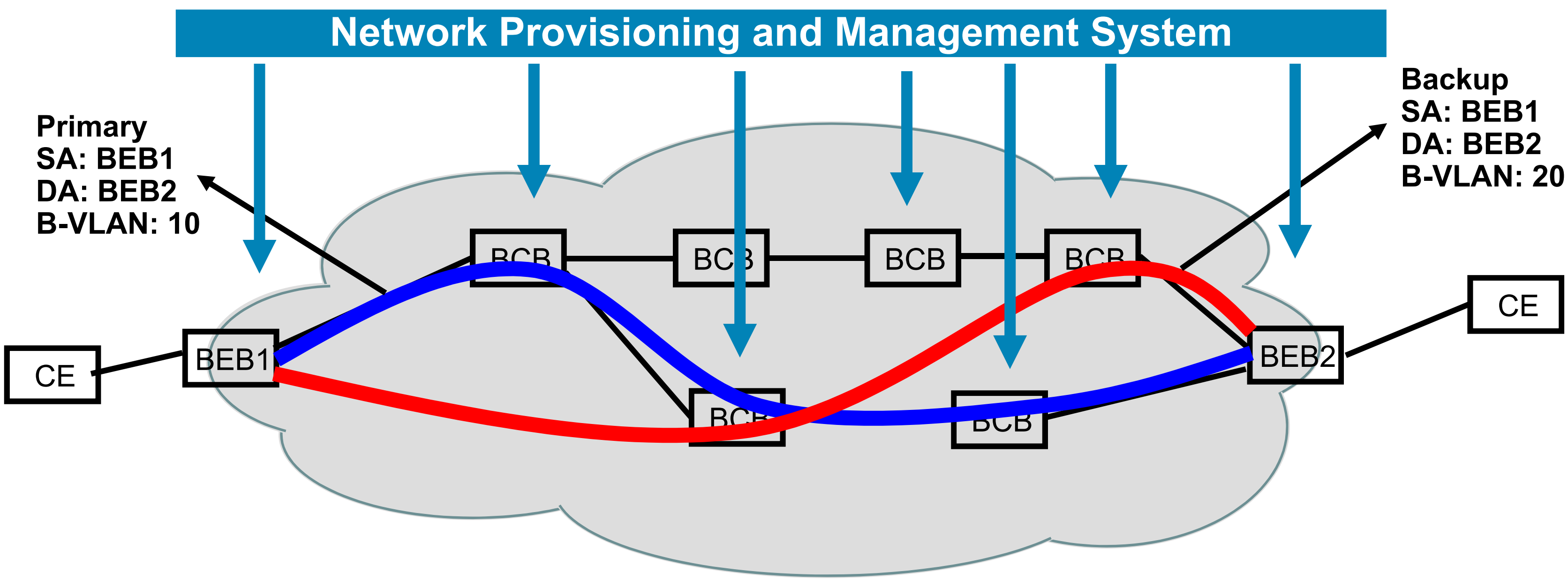
  Data-plane based on 802.1ah

  OAM based on 802.1ag (with modifications)

  A protection switching mechanism similar to MPLS TE Path Protection (protection path switching between two edge switches)

How Does It Work ?

- Use OSS to configure B-MACs and B-VLANs manually in the bridge along both primary and backup paths
- Use CFM Continuity Check Messages to monitor the primary and the backup paths
- Upon failure of the primary path, configure the edge switches (BEB1 & BEB2) to switch to the backup path



BCB: Backbone core bridge   BEB: Backbone Edge bridge

How Does It Work ? (Cont'd)

- Divide the B-VID address space between conventional 802.1ah PBBN (Provider Backbone Bridge Network) B-VLANs and PBT
- Turn off learning and broadcasting on all PBT B-VIDs
- Use bridge MIB to configure the Bridge forwarding tables for PBT B-VIDs
- Each bidirectional PBT circuit is composed of a working and a protection path
- Manage co-routed bundles of PBT backbone circuits using IEEE 802.1ag

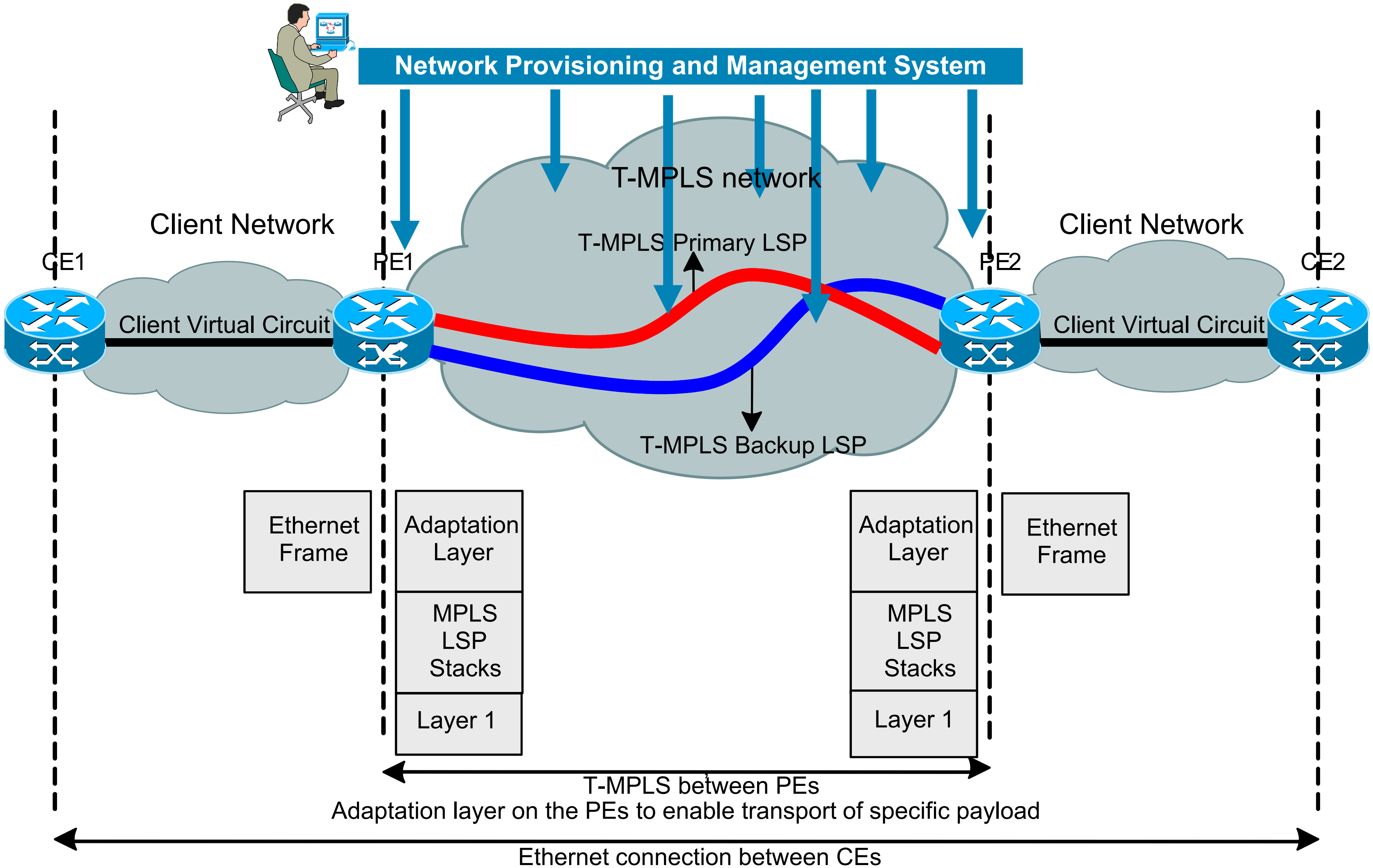
Some Pending Questions Regarding PBT

- What is the applicability?
- Does it satisfy the requirements of a wide range of services?
- If multipoint transport requires 802.1ah, what is the operational complexity of running PBB and PBT simultaneously?
- What is the protection scalability? What are the target restoration times? For how many trunks?
- What are the real benefits compared to other existing Ethernet transport alternatives?

Other Packet Transport Proposals – T-MPLS

- Connection oriented packet switched transport over an optical transport network
  - Architecture based on ITU-T G.805
- Its main characteristics are:
  - Bidirectional point-to-point LSP
  - “Client-server” model
  - No control plane (GMPLS later?)
  - OAM (Y.17tom) derived from ITU-T Ethernet OAM (Y.1731) and ITU-T MPLS OAM (Y.1711) but incompatible with IETF MPLS OAM
  - Protection switching and Survivability based on ITU-T Y.1720/G.8131 (linear protection switching 1+1, 1:1, shared mesh options) and Y.mrps (ring protection switching)
  - Use same data-link protocol ID (e.g. EtherType), frame format and forwarding semantics as defined for MPLS frames
- T-MPLS is another MPLS “pseudowire” with bi-directional traffic engineered paths

How is it Intended to Work?



Note: Adaptation layer functions on PE define the payload to be transported into the T-MPLS LSP
It can possibly be Ethernet, MPLS, TDM…

How Does it Work – as Defined Today?

- Management system (OSS) will configure primary and backup T-MPLS trail (LSP) in every NE along the path

  As T-MPLS uses the same Ethertype as MPLS, they share the same label table

  OSS will need to coordinate with LSRs to ensure that label management is consistent

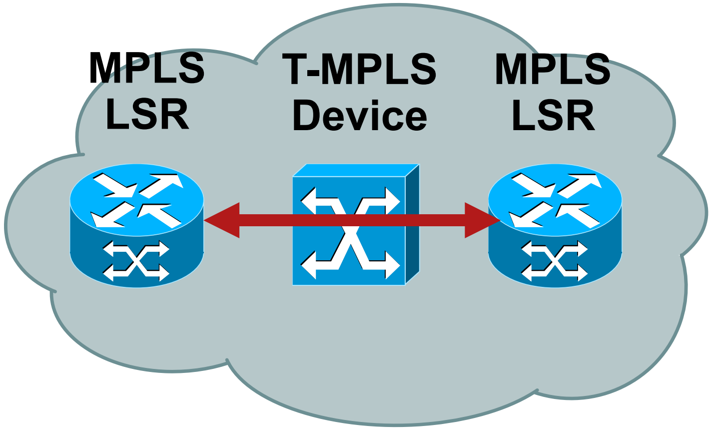
- Y.17tom OAM CV message to monitor primary T-MPLS availability and switch traffic to backup in case of failure
- Adaptation function required at the head-end/tail-end to map client layer to T-MPLS layer trail
- Client layers: L2 (Ethernet), T-MPLS, etc.

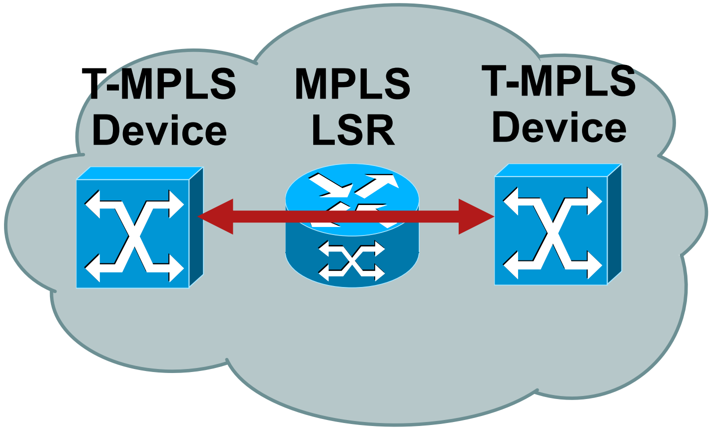
T-MPLS Challenges

- Interoperability with MPLS
- Additional layer of complexity to deploy and manage converged MPLS networks
- MPLS PW already provides similar capabilities

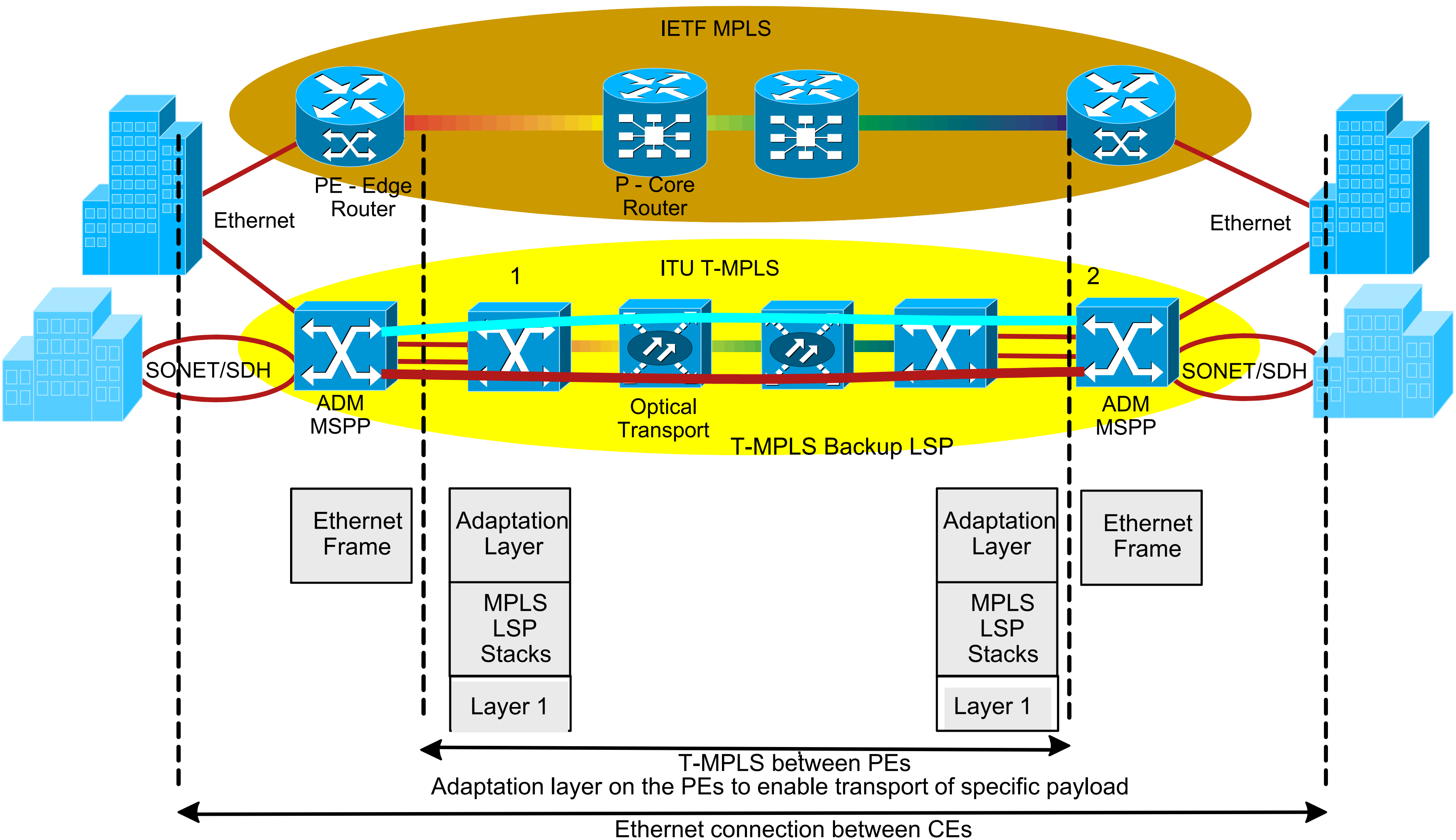
T-MPLS – MPLS Interoperability Challenge

- T-MPLS claims to be a subset of MPLS
  - Equipment co-existence within network?
  - Interoperability if T-MPLS LSP crossing an MPLS device (vice-versa)?
- Interoperability between T-MPLS PW and MPLS PW
  - Different signaling protocols
  - Different OAMs

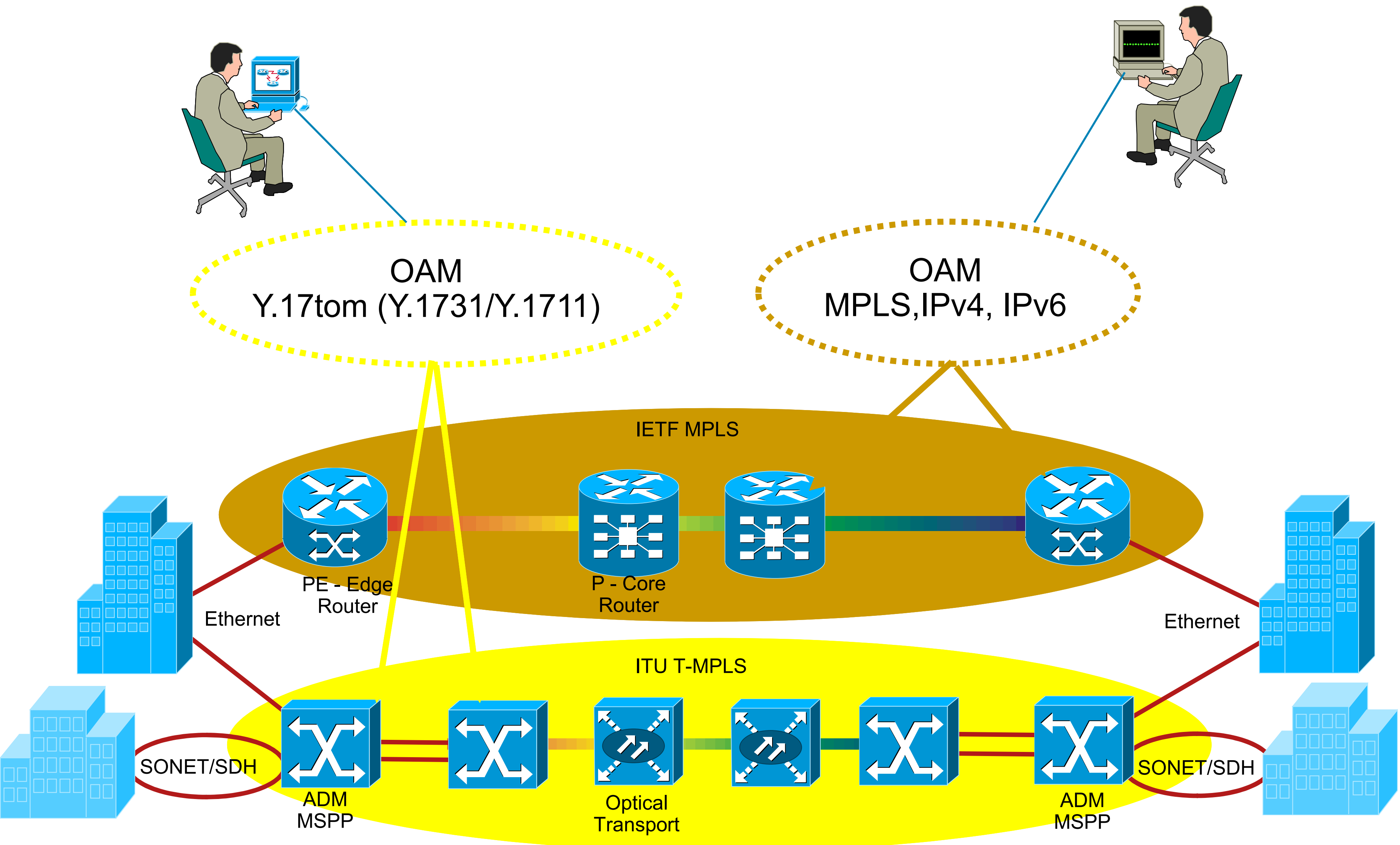




ITU T-MPLS : Another Packet Aware Technology



ITU T-MPLS : Separate FCAPS & OAM



Application of Pseudowires to MPLS Transport Networks

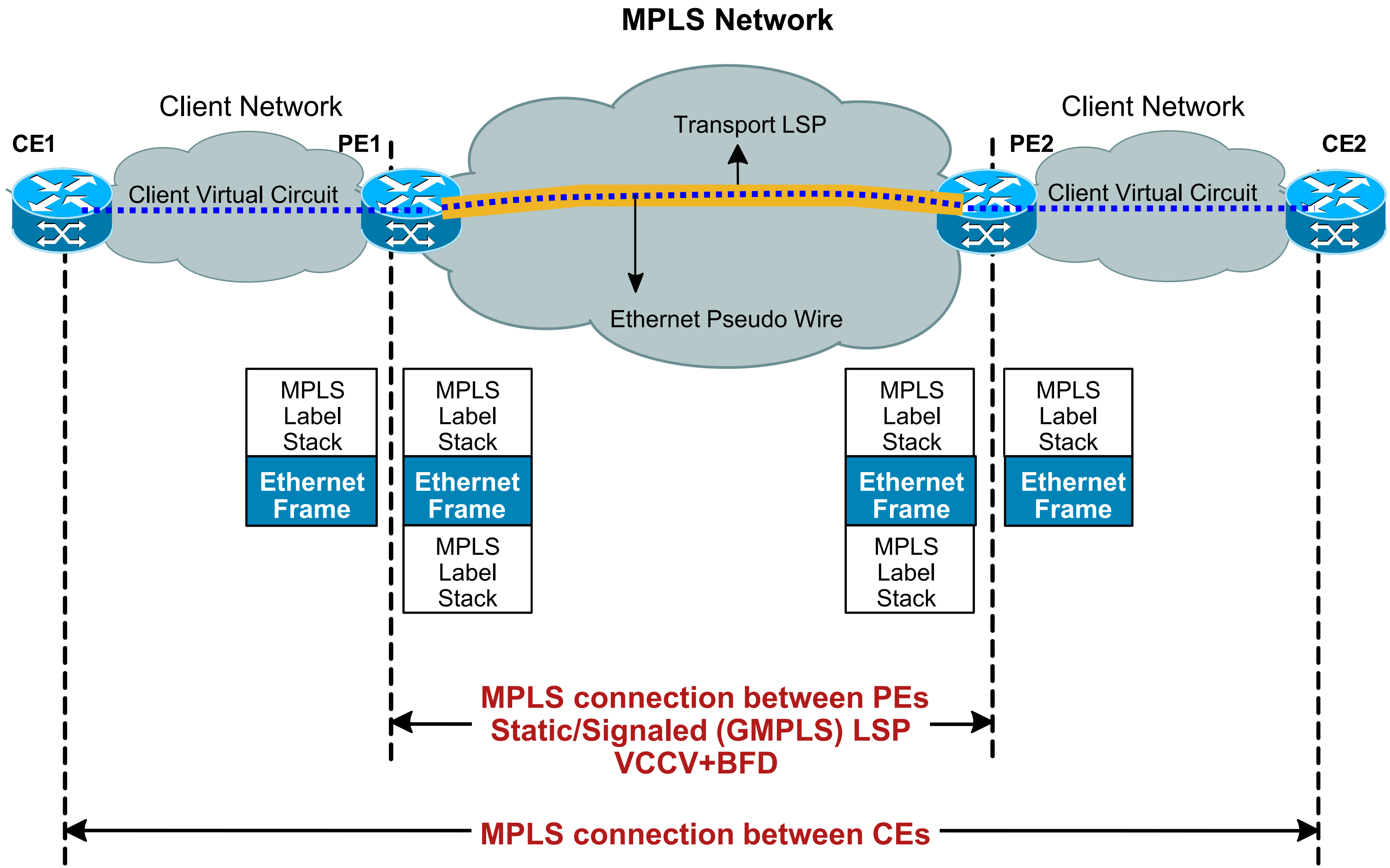
- Requirement: Strong isolation when LSP *A* carries LSP *B* (client-server network relationship)
- Solution: Leverage (Ethernet) pseudowire to separate two MPLS networks
- Restrictions on transport/server LSP (based on ITU requirements)
  - Symmetrical routing of bi-directional LSPs
  - No equal cost multi-path load balancing
  - No LSP merging (unless FRR used)
  - No penultimate hop popping
  - No support for DiffServ uniform mode

OAM and Configuration Options

- Strict subset of MPLS specifications to meet transport requirements (i.e. no PHP, load balancing, etc)
- Two VCCV profiles for OAM
  - BFD without IP/UDP headers
  - BFD with IP/UDP headers
- Two configuration methods
  - External/Static configuration
  - Dynamic control plane (GMPLS)

draft-ietf-pwe3-mpls-transport-02

MPLS Transport Example



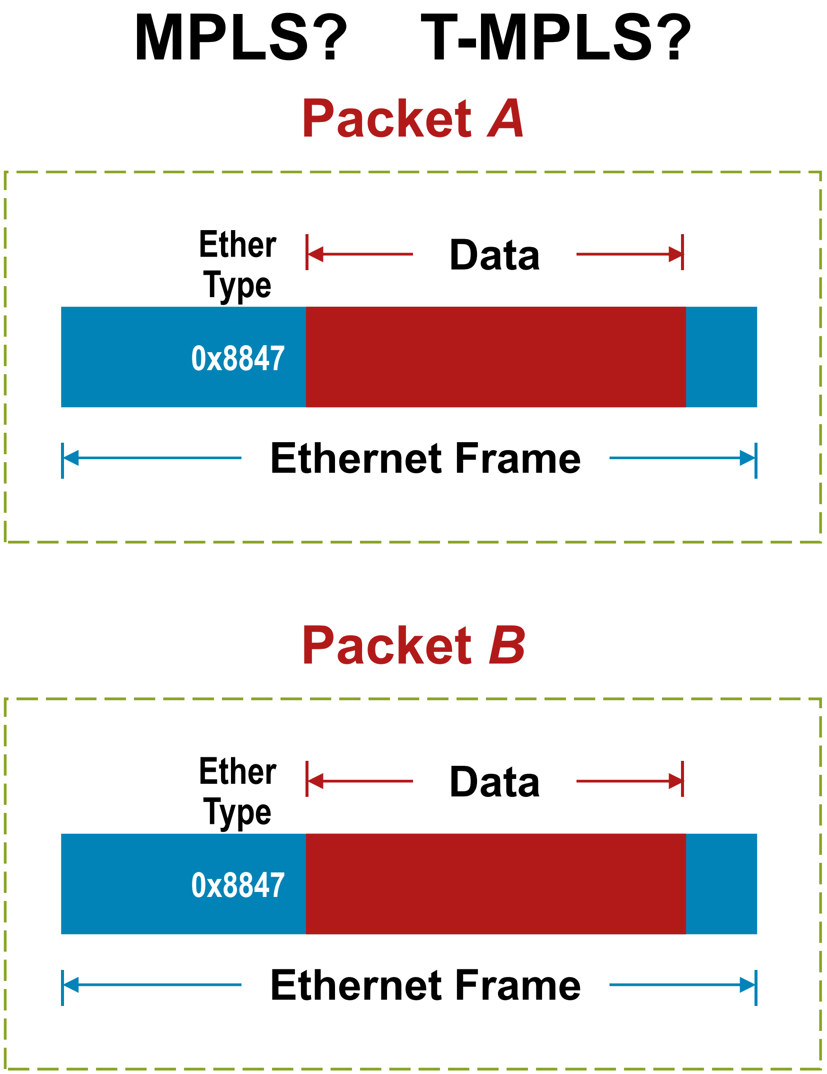
ITU-T Standardization Status for T-MPLS

Standardization on hold until harmonization with or separation from IETF MPLS resolved

- G.8101: Terms and definitions for transport MPLS
- G.8110: MPLS layer network architecture
- G.8110.1: Architecture of Transport MPLS (T-MPLS) layer network
- G.8112: Interfaces for the Transport MPLS (T-MPLS) hierarchy
- G.8121: Characteristics of Transport MPLS equipment functional blocks
- G.8131: Linear protection switching for Transport MPLS (T-MPLS) networks
- G.8151: Management aspects of the T-MPLS network element

T-MPLS Standardization Assumptions

- T-MPLS reuses MPLS Ethernet Type and protocol identifiers
- ITU-T T-MPLS not intended ultimately as a profile of IETF MPLS
- Implicit expectation that T-MPLS and MPLS networks will be disjoint
- Technology separation relies on careful network planning and design
- Disaster waiting to happen?



IETF / ITU-T Ad Hoc group on T-MPLS

- Joint working team (JWT) involving ITU-T and IETF experts created Feb 2008
- JWT will recommend one of two options and define work plan
  - Extend MPLS through IETF to meet transport requirements
  - Separate technologies completely (new Ether type and name for T-MPLS)
- Areas of focus
  - Forwarding plane
  - OAM
  - Control plane
  - Network survivability
  - Network management
- JWT expected to end by Sep 2009

Questions Regarding T-MPLS

Is T-MPLS necessary since existing MPLS PW technology delivers similar capabilities….

Static PW combined with static LSP and VCCV+ BFD

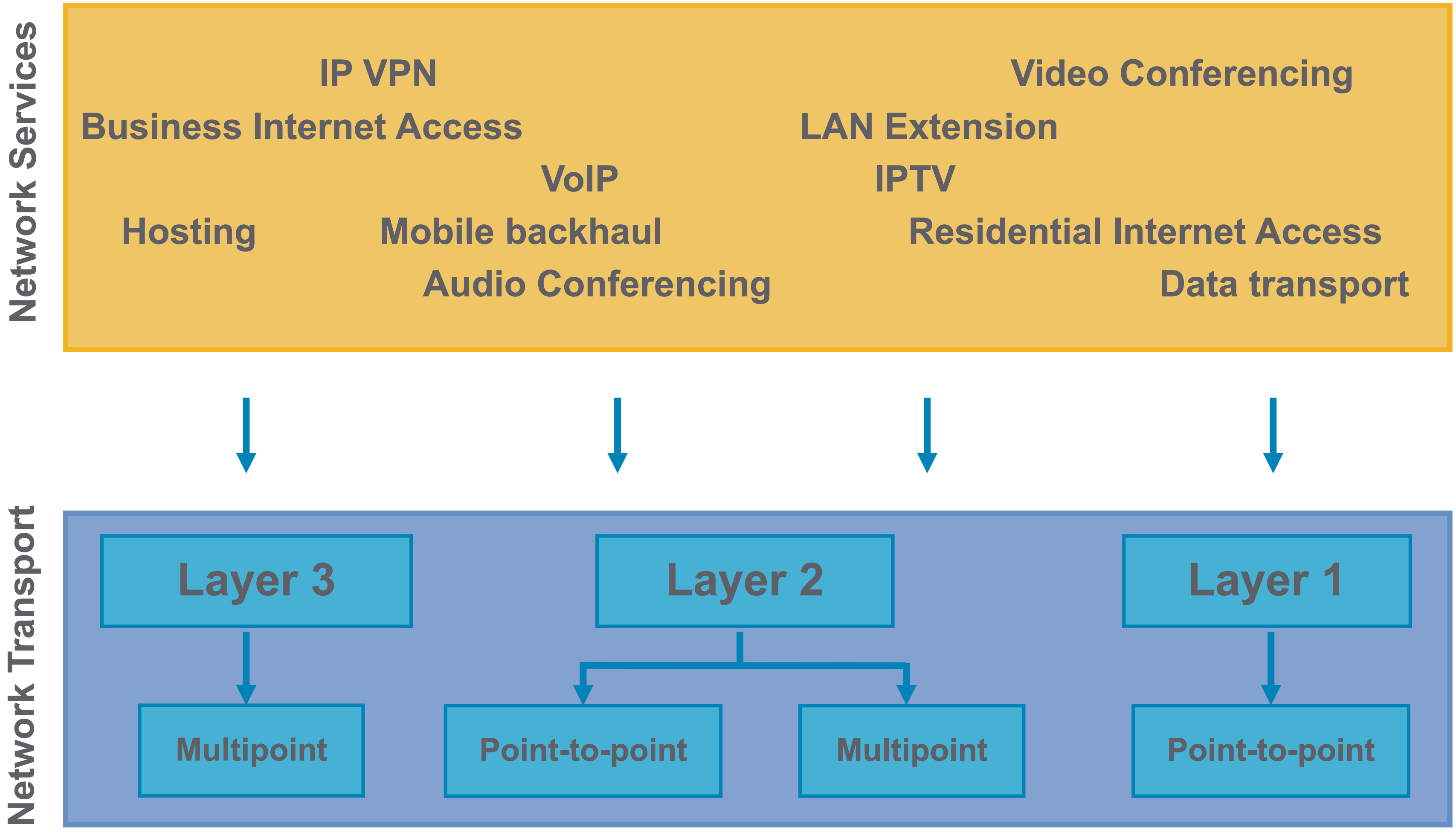
Therefore

Reinventing the wheel ?

- Use approved standards
- Use technology already deployed
- Leverage knowledge that already exists
- Extend existing standards if needed

Service Mapping and Applicability

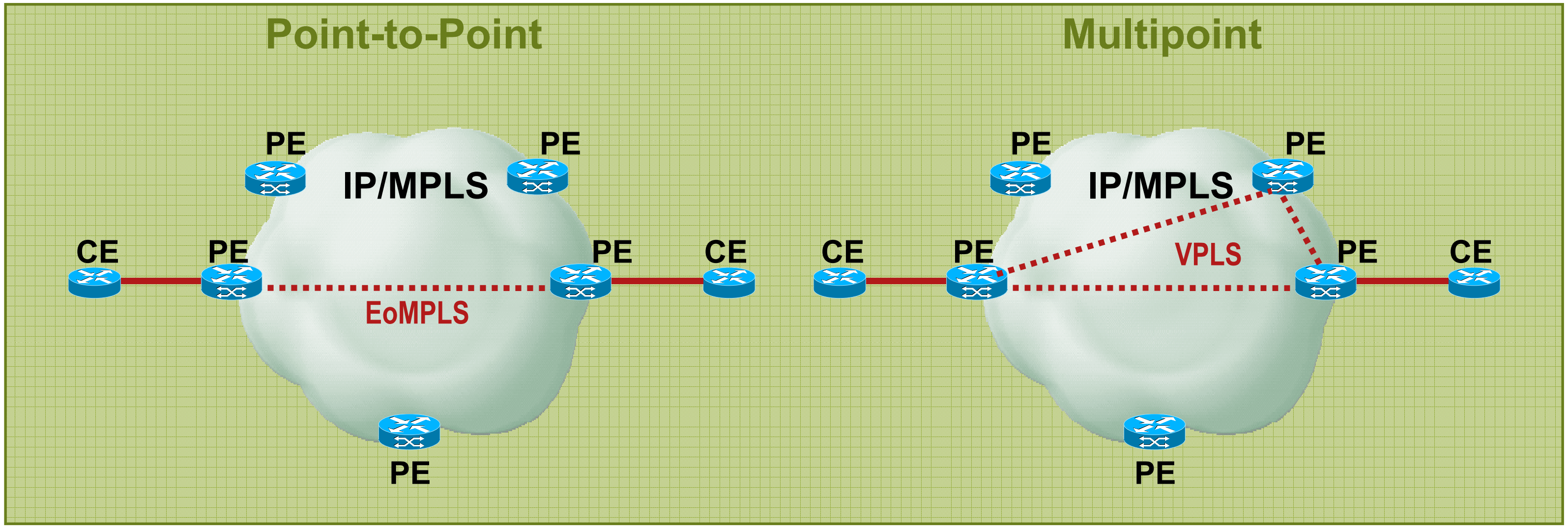
Network Service Portfolio



Building Network Services

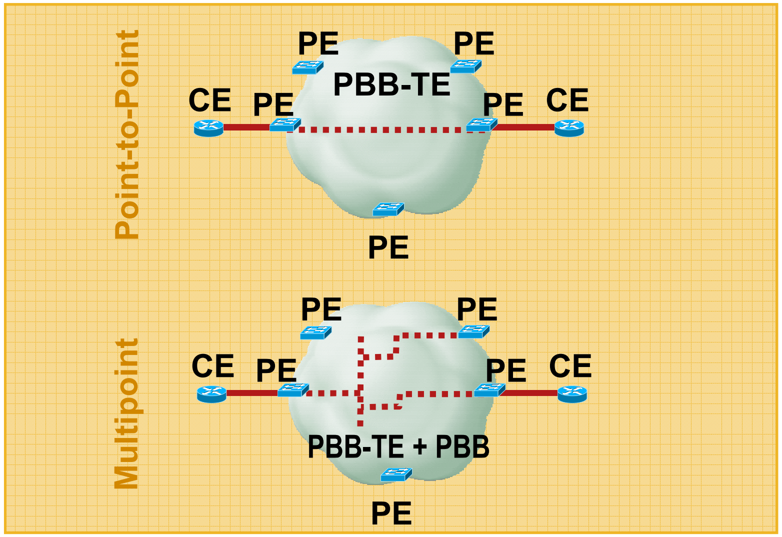
- What are the important services ?
- What are the transport requirements?
  – Point to Point Transport
  – Multipoint Transport
  – Multicast for Video Delivery
  – Legacy Integration & TDM Circuit Emulation

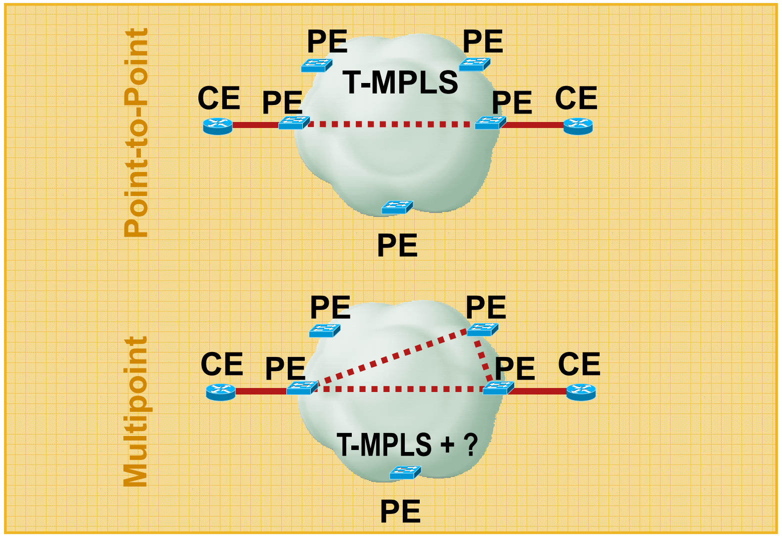
Ethernet over MPLS Transport



- Ethernet pseudowire for point-to-point services
- VPLS for multipoint services
- Leverages protection, traffic engineering, QoS and OAM capabilities of MPLS
- Established specifications and implementations
- Deployment experience

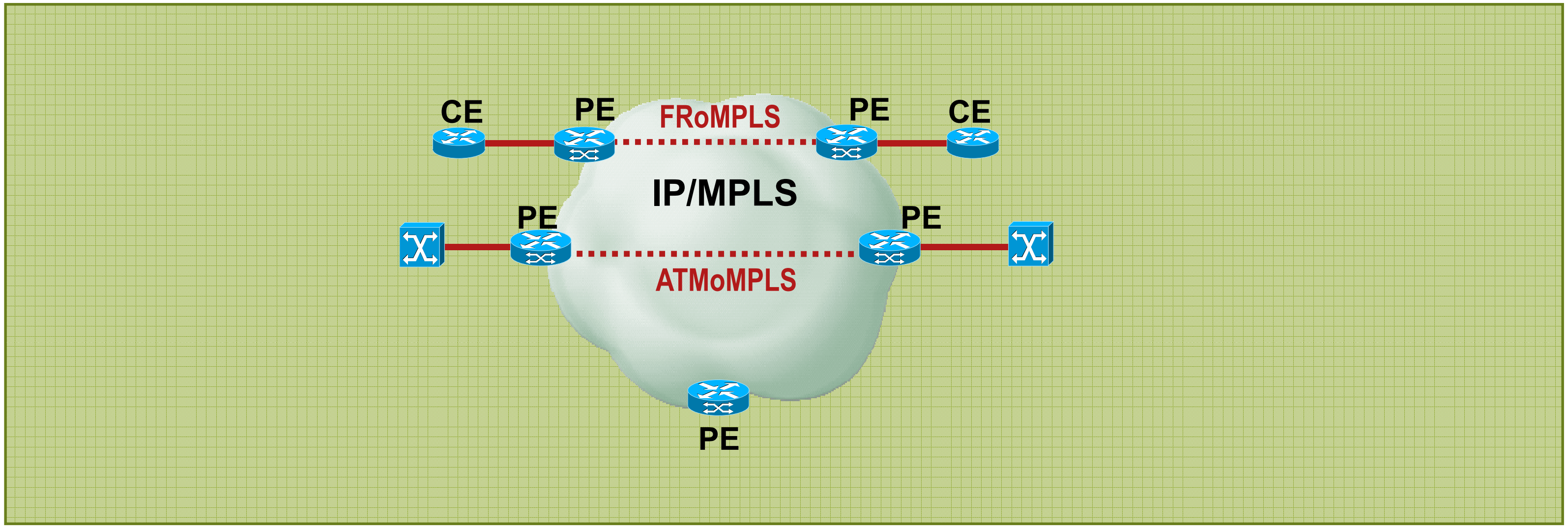
Ethernet over Other Packet Transport





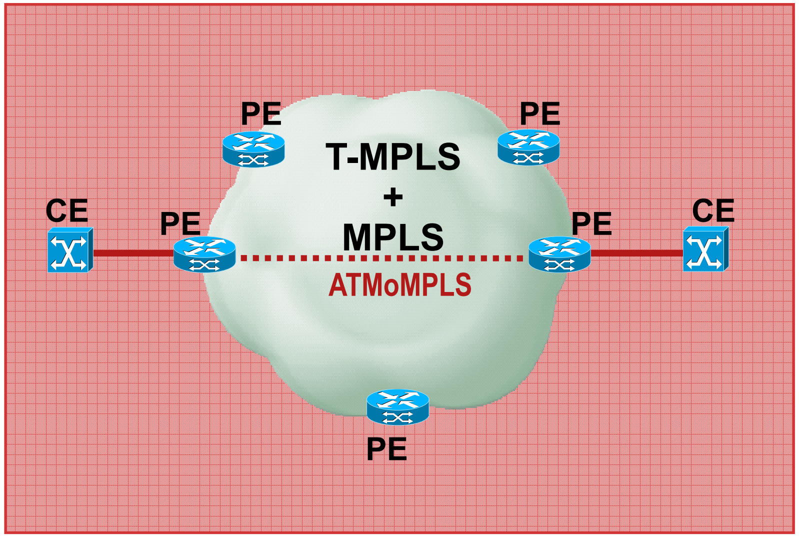
- Native support for point-to-point services
- No native support for multipoint services
- PBB-TE requires PBB for multipoint services
- T-MPLS requires overlay technology for multipoint services
- No/partial standardization
- No support for layer-1 and other layer-2 technologies

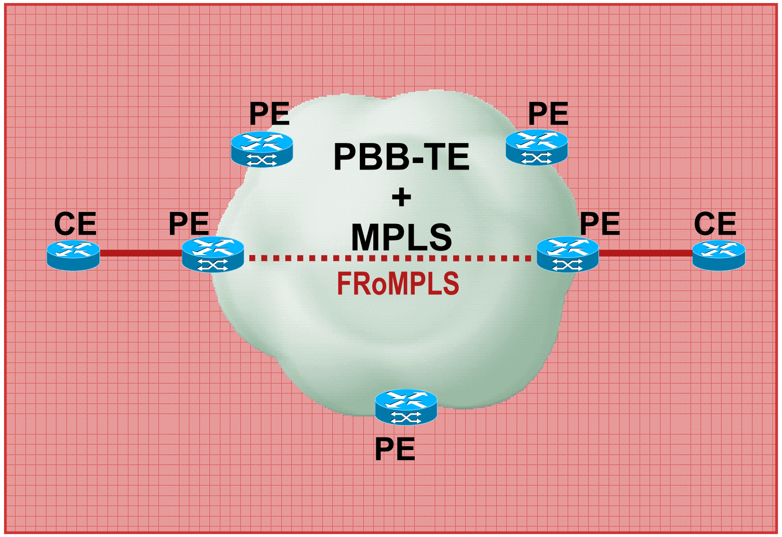
Other Layer-2 Service over MPLS Transport



- Mature specifications to transport Frame Relay, ATM, PPP/HDLC
- Leverages protection, traffic engineering, QoS and OAM capabilities of MPLS
- Deployment experience

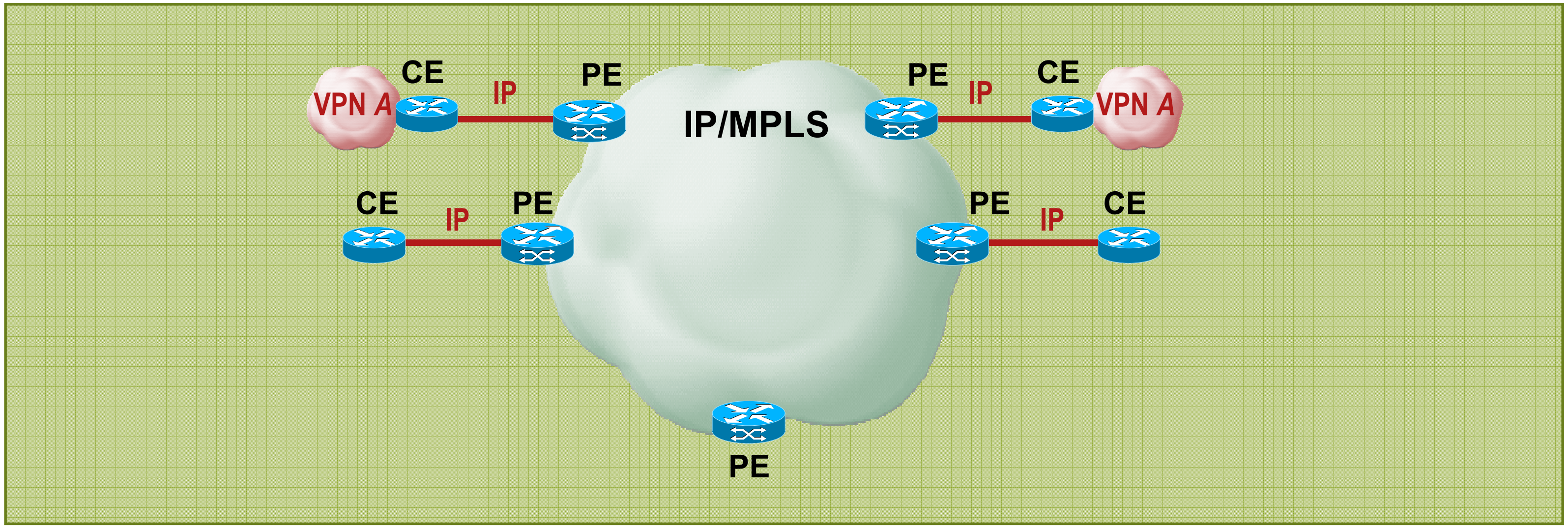
Other Layer-2 Service over Other Packet Transport





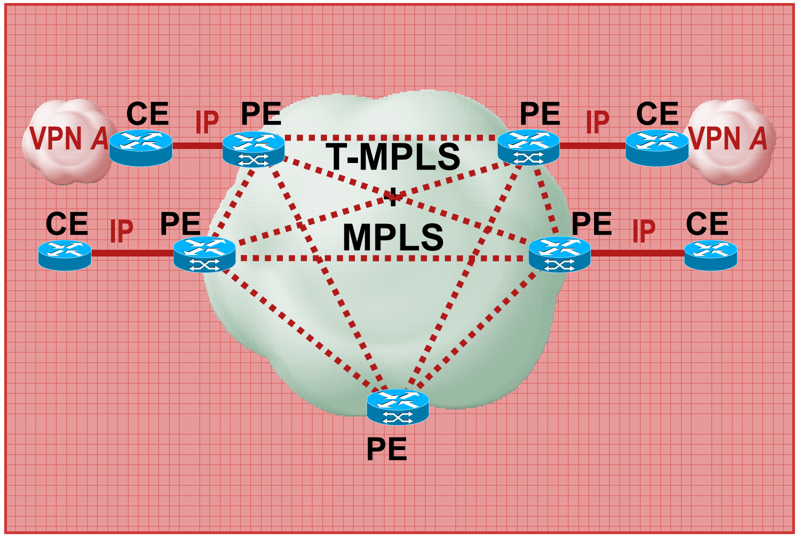
- Neither T-MPLS nor PBB-TE are multiservice
- MPLS still required to transport ATM, FR, PPP, etc.
- Edge devices need interface and MPLS pseudowire support for other layer-2 services

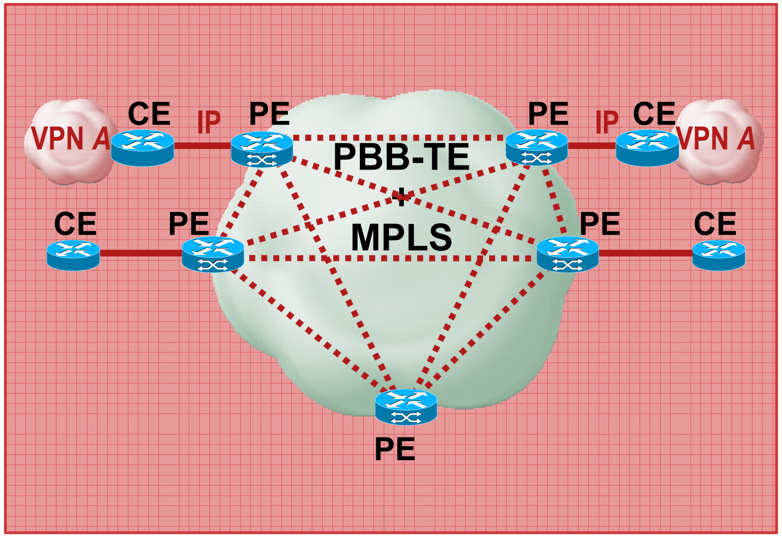
Unicast Layer-3 Service over MPLS Transport



- Optimal bandwidth use (shortest path, constraint-based routing, load balancing)
- High resiliency using MPLS TE FRR or IGP fast convergence
- Leverages time-proven IP scalability
- Ethernet may still be used as access technology and data-link encapsulation
- Numerous IP VPN implementations and extensive deployment experience

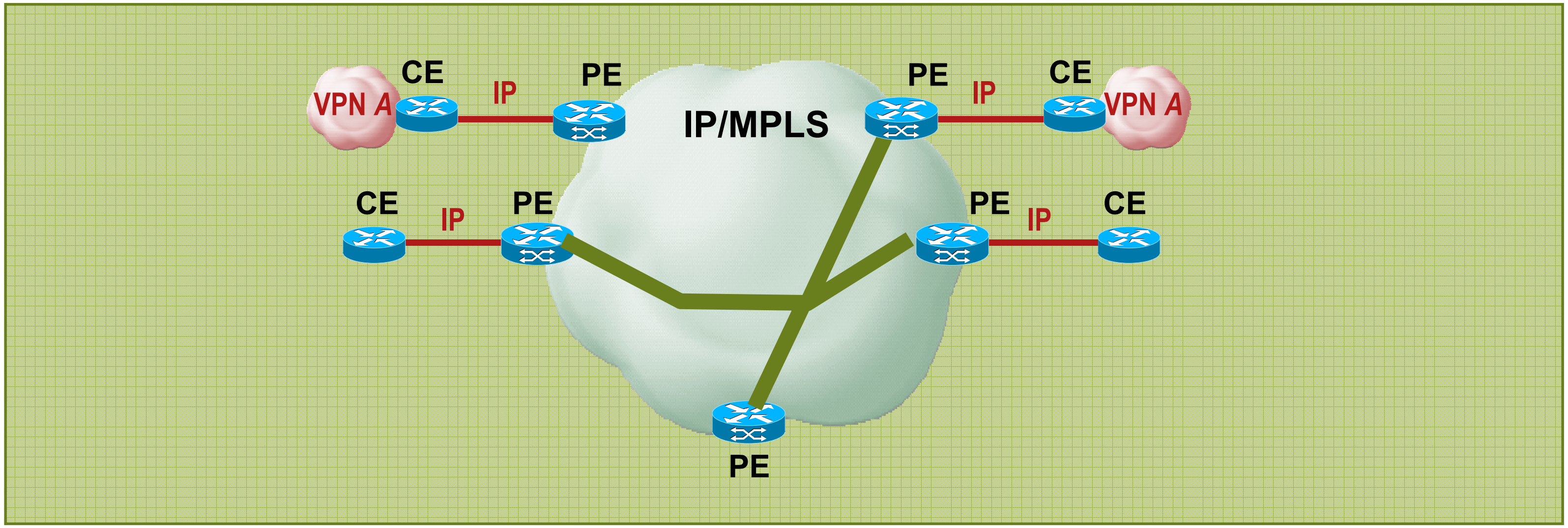
Unicast Layer-3 Service over Other Packet Transport





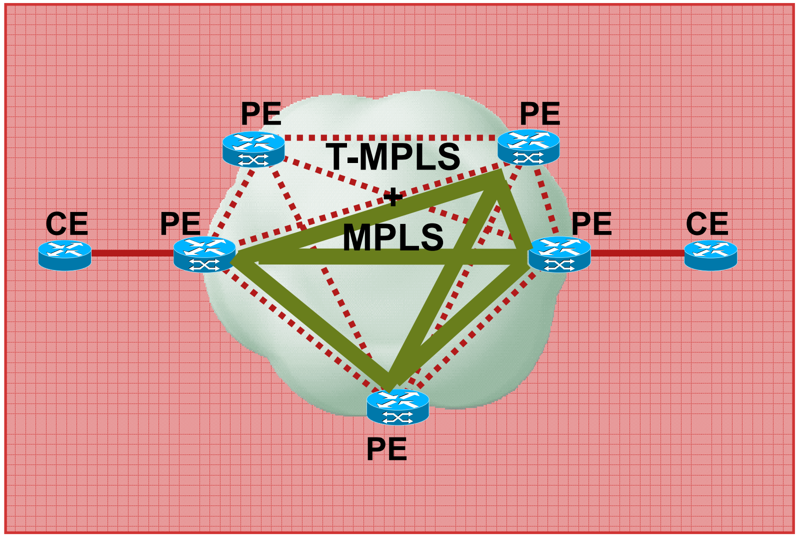
- Operational complexity in full mesh configuration (planning, management)
- May result in sub-optimal bandwidth use (shortest path, load balancing) in partial mesh configuration
- MPLS still required for VPN services
- Impacts IP scalability (IGP adjacencies on PEs)
- Resembles challenges with IP over ATM in 90s

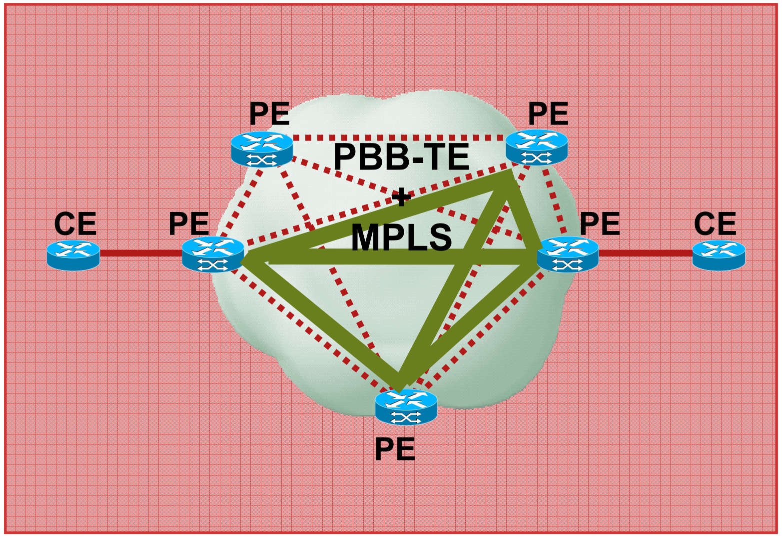
Multicast Layer-3 Service over MPLS Transport



- Point-to-multipoint (mLDP/RSVP-TE) and multipoint-to-multipoint (mLDP)
- Scalable (distributed) packet replication
- Optimal bandwidth use (constraint-based routing, shortest path, load balancing)
- High resiliency using MPLS TE FRR or IGP fast convergence
- Support for receiver or sender initiated trees
- Numerous IP VPN implementations and extensive deployment experience

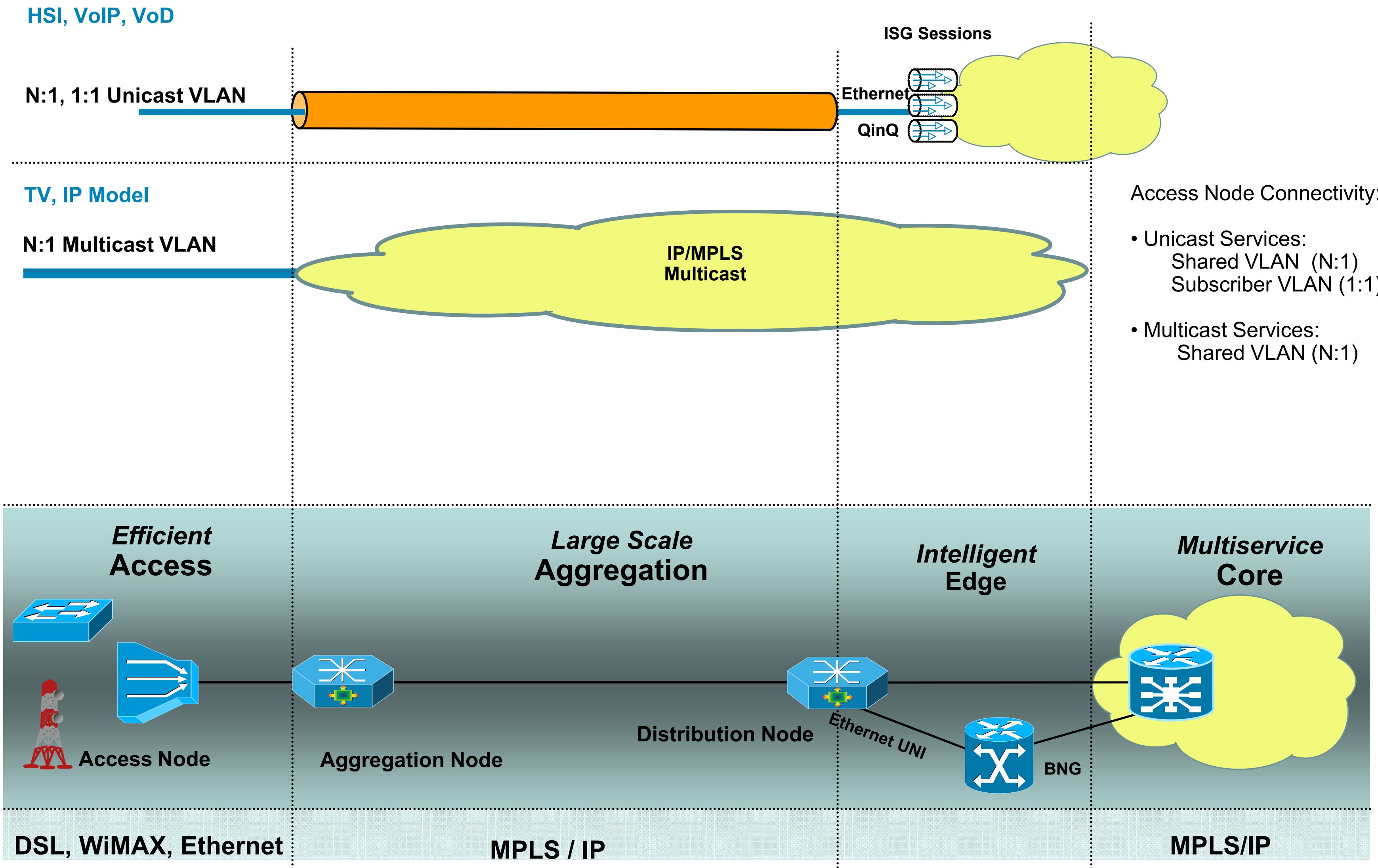
Multicast Layer-3 Service over Other Packet Transport





- Limited scalability (PE packet replication)
- Suboptimal bandwidth use (premature replication)
- MPLS still required for VPN services

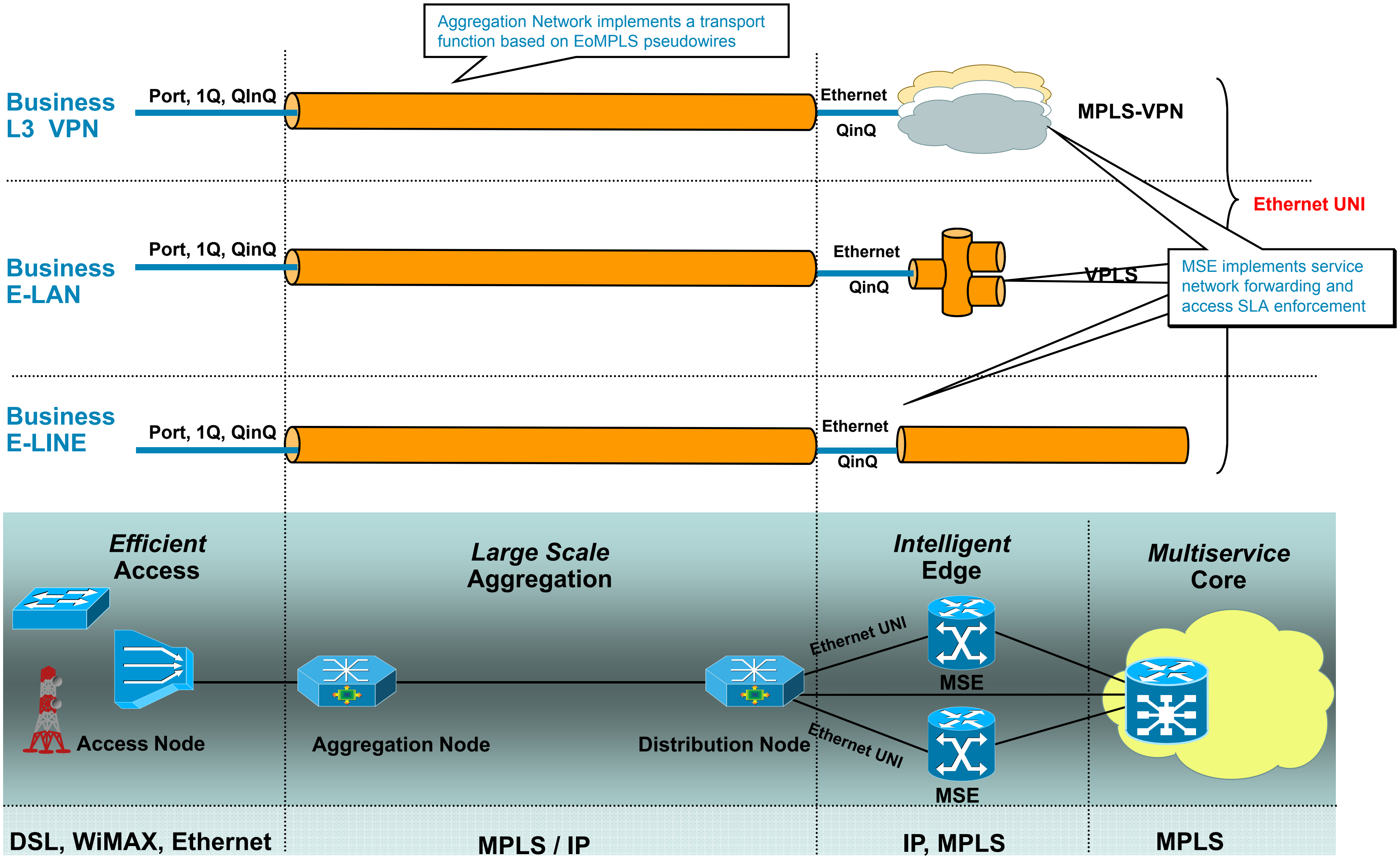
Retail Residential Services Architecture



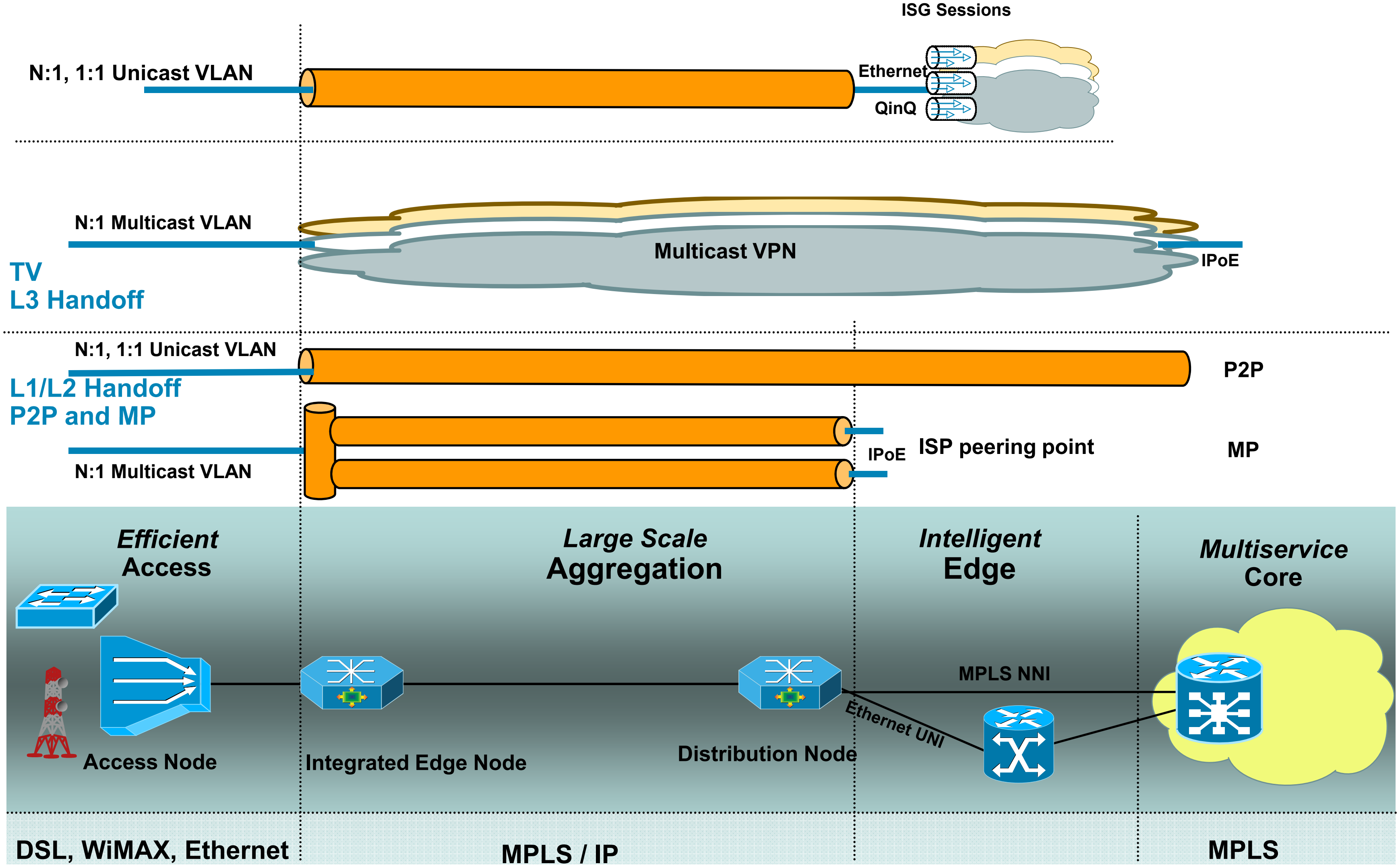
Access Node Connectivity:

- Unicast Services:
  Shared VLAN (N:1)
  Subscriber VLAN (1:1)
- Multicast Services:
  Shared VLAN (N:1)

Business Ethernet Services Architecture



IP Wholesale Services Architecture



Multi-vendor Interoperability

- Multi-Vendor Interoperability is key to ensure
  - No Proprietary Implementation is Deployed
  - No vendor Lock-in
  - Investment protection
- Crucial to test Multi-vendor interoperability for critical services/requirements of the network to ensure right selection of technology
  - Traffic protection
  - Services : Point-to-Point, Multipoint-to-Multipoint, Multicast
  - Legacy Integration (e.g. ATM Transport)
  - Quality of Service
  - OAM

Some Historical Background of Layer 3 vs. Layer 2

- At least 2 major attempts in past 10 years to "revolutionize" networking by introducing a Layer 2 approach

  End-to-End Pure Layer 2 Switching

  ATM LAN Emulation

- Layer 3 deemed as either unnecessary, more complex and more expensive
- Both attempts failed miserably with time!
- IP/MPLS is revolutionary in a way since it unites the benefits of both Layer 2 and Layer 3 together!

Is a Layer 2 Based Solution Cheaper than a Layer 3 Based Solution ?

Some considerations:

- Cost of overlay networks required for legacy integration
- Cost of network management system
- Cost of overlay network/intelligence required for supporting Multicast and Video
- Cost of manual provisioning & management since network doesn’t have intelligent control plane
- Cost of adding Intelligence (GMPLS) to the solution that has no control plane
- Cost of important features on network elements like Hierarchical-QoS (H-QoS), ISSU etc

Summary

Summary

Key Points to Consider Before Selecting Technology for Building your Next Generation Ethernet Network

- Technology state: standardization, maturity, deployment experience, future roadmap
- Network Intelligence: Integrated Control Plane or Proprietary NMS Control Plane
- Transport dependency: Is selected technology agnostic of transport protocols so that it allows you to migrate smoothly?
- Multiservice support: Can all required services be offered by the Technology or basic services require workarounds?
- Interoperability: Is technology multi-mendor and interoperable
- Last but not the least, cost: combined capital and operational cost; converged or separate networks