Carrier Ethernet and Ethernet OAM

Santanu Dasgupta (santanu@cisco.com)

Dhaka, 29th January 2010

House Rules

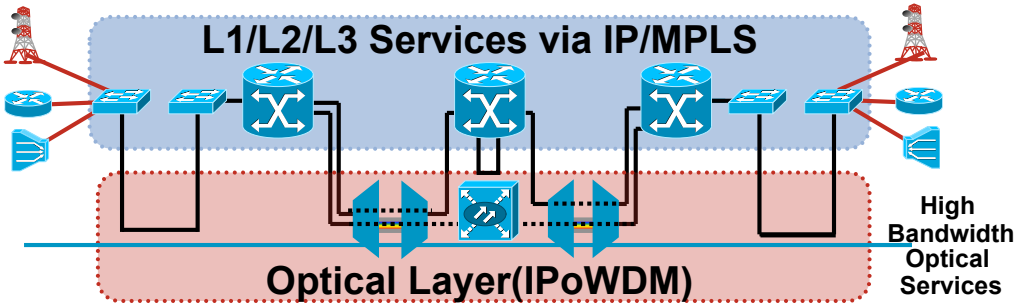
- Please put your mobile phones into silent mode.
- Kindly do not take calls inside of this room while the session is going on.
- Your feedback on the session is extremely important!

Assumptions

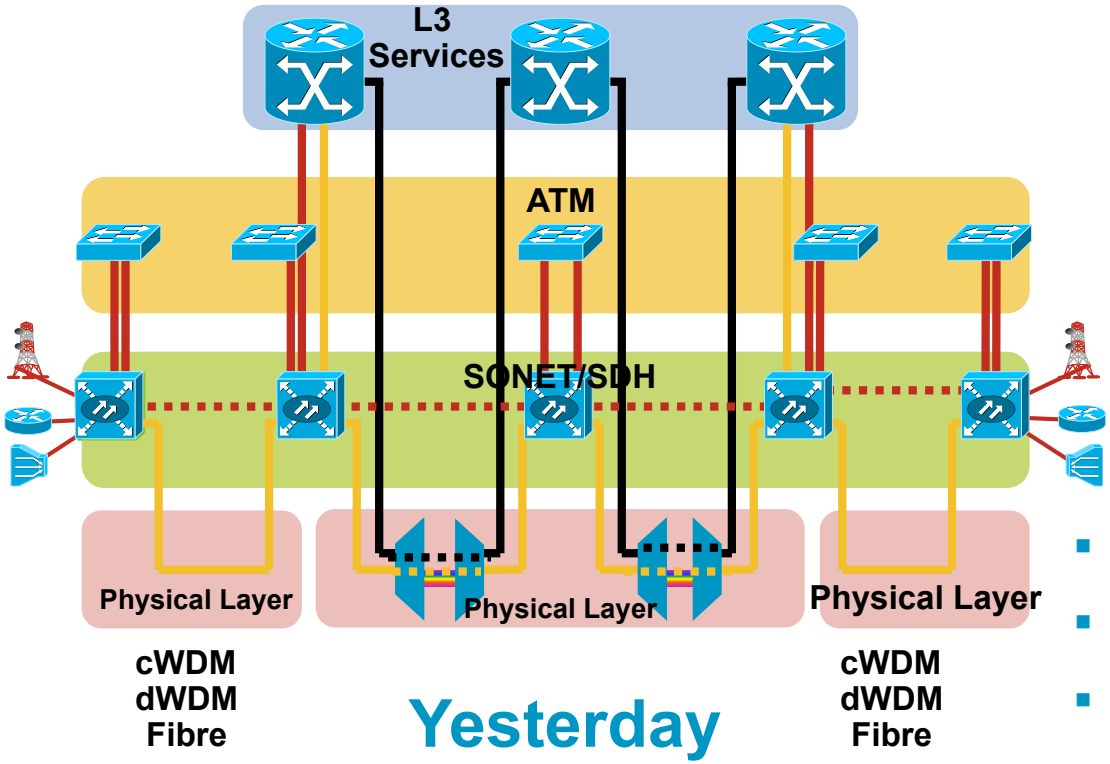
- You have a good understanding Ethernet Switching and some basic understanding of Carrier-E technology
- You have some general understanding of OAM.
- You will be awake throughout the presentation! ☺☺

SP Network Evolution

- Historic Growth
- Not built for packet initially
- Diff. Departments
- High OPEX due to layering



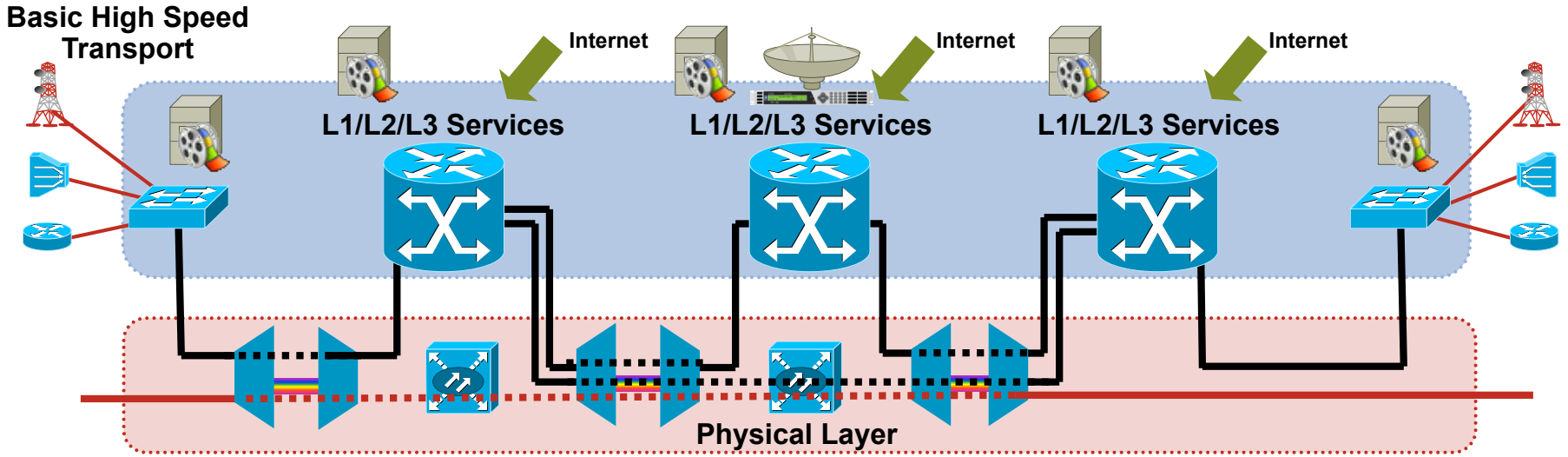
Tomorrow



Yesterday

- Evolution not revolution
- Minimal Layering
- Similar control plane in aggregation and core

IP NGN: Converged Topology



- 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
  - Based on an end to end IP/MPLS control plane
  - Concurrent support of L1, L2, L3 services
  - MPLS for 'Connection oriented' properties with Traffic Engineering, Path protection (and Link and Node protection!), P2P AND MP2MP, Superior and absolute QoS (RSVP-TE)
- Flexible injection and service points → Multi-Edge

Carrier Ethernet : Agenda

- Business Connectivity—The Landscape
- Why Ethernet? The Evolution
- Carrier Ethernet— Technology Primer
- Carrier Ethernet Services Flow
- Ethernet OAM

Once Upon a Long Ago…

- 1972
  Dr Robert Metcalfe implemented the Alto Aloha Network at Xerox Parc
- 1976
  The name Ethernet was first used

Business Connectivity – The Landscape

Business Connectivity

The Landscape

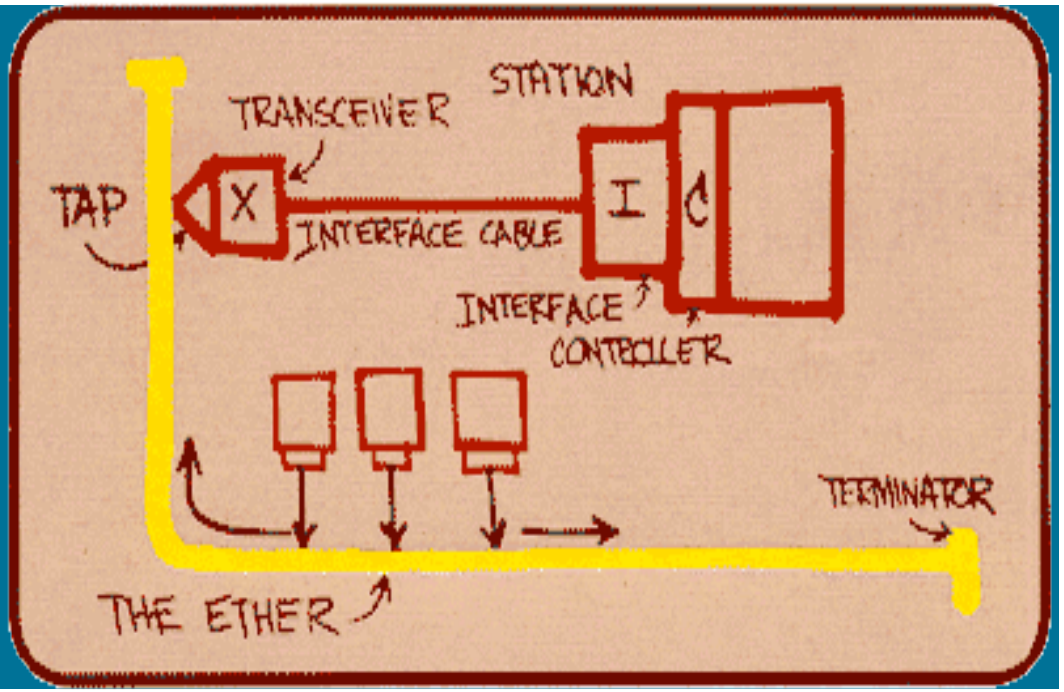
- Geographically diverse business locations
- Distributed applications require LAN extension
- Multiple customers over a single infrastructure
- Killer applications driving next generation Layer 2 VPNs
- Active/Active or Active/Backup resiliency configurations

Site-to-Site Connectivity

The Answer: Carrier Ethernet

- L2VPNs must evolve
- Ethernet: The next step
- Ethernet provides
  - More bandwidth than traditional L2VPNs
  - True LAN extension between remote areas
- Customer Ethernet connected via SP Ethernet
- BFD with MPLS Fast ReRoute can minimize downtime
- Multiple redundancy models can be deployed

Why Ethernet?



The Evolution

Why Ethernet?

The Basics

1. Mature and Widely Deployed

Long history of deployment

De-facto LAN technology

2. Resilient and Versatile

CSMA/CD has withstood the test of time

Can terminate fiber and copper effectively

3. Cost Effective

Not as expensive as other WAN technologies

IT staff already trained in Ethernet

4. Constantly Evolving

Ethernet has came a long way since its early days

Why Ethernet?

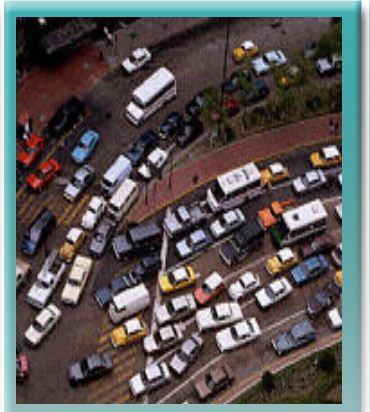
The Evolution

Higher Bandwidth

Started as 10 mbps Ethernet

Evolved to 100 Mbps and 1Gbps

Now available as 10Gbps Ethernet



Quality of Service

QoS mechanisms

IP Prec/DSCP

802.1P (CoS)

MPLS EXP LLQ

Congestion avoidance

Scheduling

LAN Extension

Port-based services

Transparent connectivity

L2 protocol tunneling

Access agnostic

Economics

Lower per port cost

OPEX/CapEx reduction

IT staff already trained

No expensive upgrades

Resiliency

No single point of failure

Quick failure recovery

Provides link and node failure protection

The Result: Carrier Ethernet Network

Carrier Ethernet

An Overview

Carrier Ethernet

Terminology

E-Line	Ethernet Line; refers to point-to-point services
E-LAN	Ethernet LAN; refers to multipoint services
EPL	Ethernet Private Line
EVPL	Ethernet Virtual Private Line
EPLAN	Ethernet Private LAN
EVPLAN	Ethernet Virtual Private LAN
U-PE	User Provider Edge
PE-Agg	Provider Edge Aggregation
N-PE	Network Provider Edge
CPE	Customer Premises Equipment
UNI	User Network Interface
NNI	Network to Network Interface

Carrier Ethernet Cooks— Who Does What?

Focus on the User-Perspective: Ethernet Services, UNI, Traffic Engineering, E-LMI, ...

Building Ethernet-Access (and beyond) Networks: Provider Bridges (802.1ad); Connectivity Management – OAM: 802.1ag, 802.1ah Backbone Bridges, 802.1ak Multiple Registration Protocol, 802.1aj Media Converters, 802.1aq Shortest Path Bridging, etc.

L2VPN, PWE3 WG – Building the Network Core: VPWS, VPLS

SG15/Q12, SG13/Q3; Architecture of Ethernet Layer Networks, Services etc. – from a Transport perspective. E2E OAM.

Ethernet to Frame-Relay/ATM Service Interworking

DSL related architecture & transport aspects (TR-101): BRAS-requirements, Ethernet Aggregation / TR-59 evolution, subscriber session handling, …

Carrier Ethernet

The Basics

- Metro Ethernet Forum driving Carrier Ethernet services and acceleration of adaptation
- Over 110* Service Providers and equipment suppliers part of Metro Ethernet Forum
- MEF certifications verify product feature support

So What Exactly Is Carrier Ethernet?

*Source: www.metroethernetforum.org

"Carrier Ethernet is a ubiquitous, standardized, carrier-class *SERVICE* defined by five attributes that distinguish Carrier Ethernet from familiar LAN based Ethernet."

Carrier Ethernet

Service Attributes

- Standardized Services
  - Point-to-point (E-LINE) and multipoint (E-LAN) services
  - Does not require any changes to customer LAN equipment
- Scalability
  - Bandwidth scalability from 1mbps up to 10gbps
  - Large number of customers over a common infrastructure
- Reliability
  - Failure detection and recovery without customer impact
  - 50msec or less convergence for sensitive traffic

Carrier Ethernet

Service Attributes

- Quality of Service
  - Provide a range of Bandwidth and Quality of Service options
  - Multiple classes of traffic with guaranteed Service Level Agreements (SLA)
- Service Management
  - Central monitoring and management stations
  - User friendly service provisioning

Carrier Ethernet

Service Provider Perspective

- Network convergence
  - IP over Ethernet as enabling technologies for “One” Network
  - CAPEX and OPEX reductions
- Flexible Service Offerings
  - Customized solutions
  - Flexible mix of services and data rates (EPL, EVPL, E-LAN)
- Ubiquitous Access
  - Access networks that leverage Ethernet
  - PON, Wimax, IP DSLAMs, Ethernet over Fiber, Ethernet over Copper, etc.

Carrier Ethernet

Service Provider Perspective

- Standardization
  - Products must go through certification
  - MEF certification tests are conducted to meet service requirements
- Box-Level Economics
  - Ethernet equipment is already widely deployed
  - Less expensive than ATM or SONET/SDH

Carrier Ethernet

Enterprise Customer Perspective

- Network Convergence
  - One network for all Business applications
  - Cost reductions
- Virtualization
  - High speed, low latency VPNs
  - Extend LAN–MAN–WAN without protocol conversion
- Operational Benefits
  - Ethernet is very familiar to IT staffs

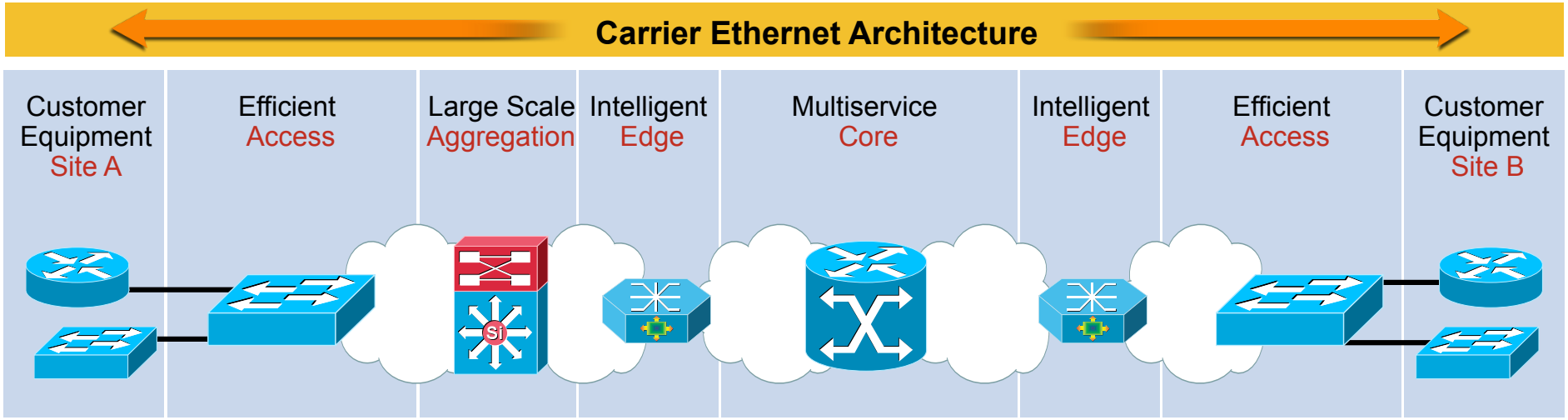
Carrier Ethernet

Enterprise Customer Perspective

- Simple Upgrades
  - Ethernet delivers bandwidth up to 10 Gbps (and beyond)
  - Easier Incremental bandwidth upgrades
- Standardization
  - User-to-Network Interface (UNI) everywhere in the networks
  - Reduced spares inventories, training, management and testing tools

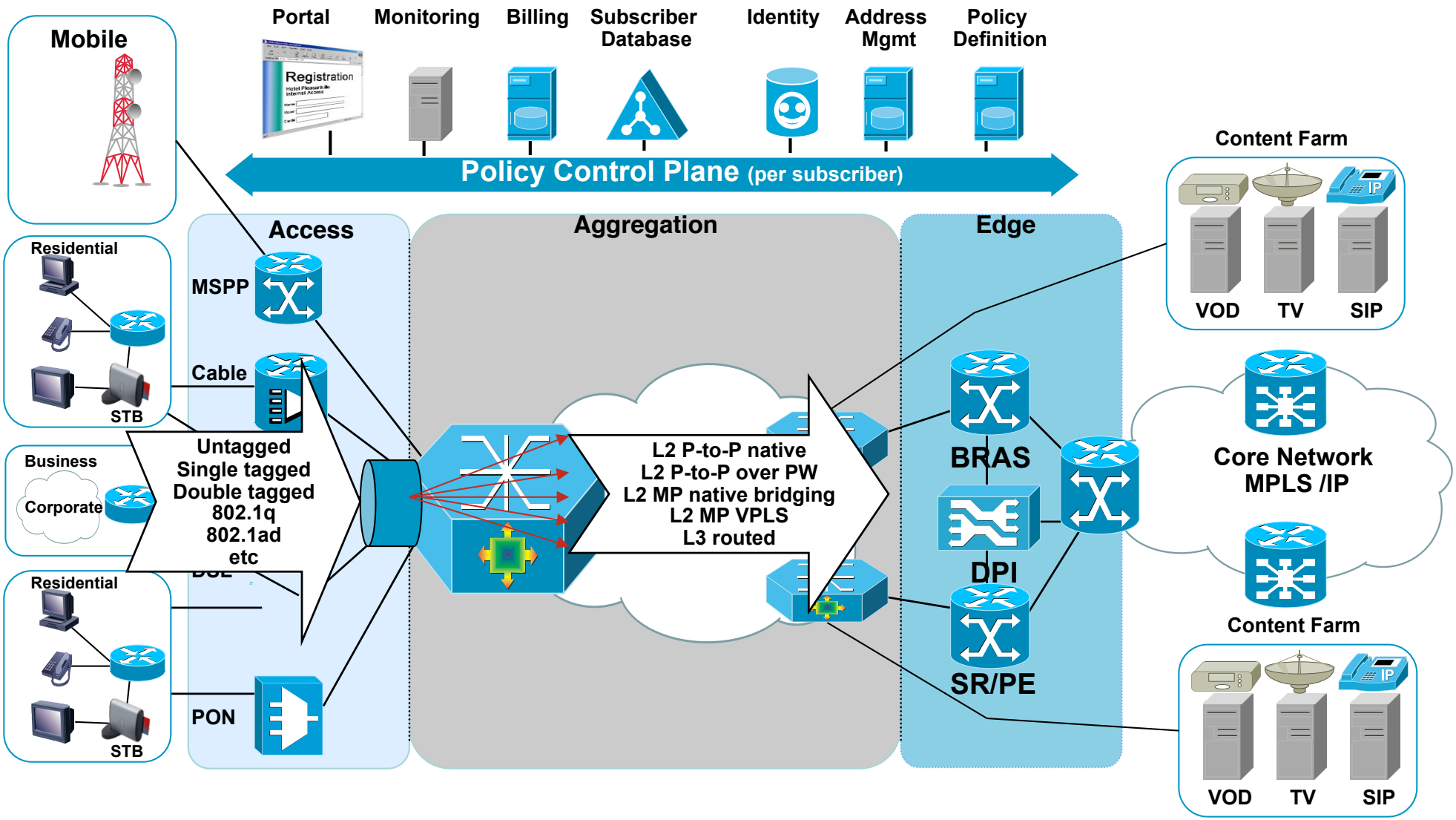
Carrier Ethernet

The Architecture



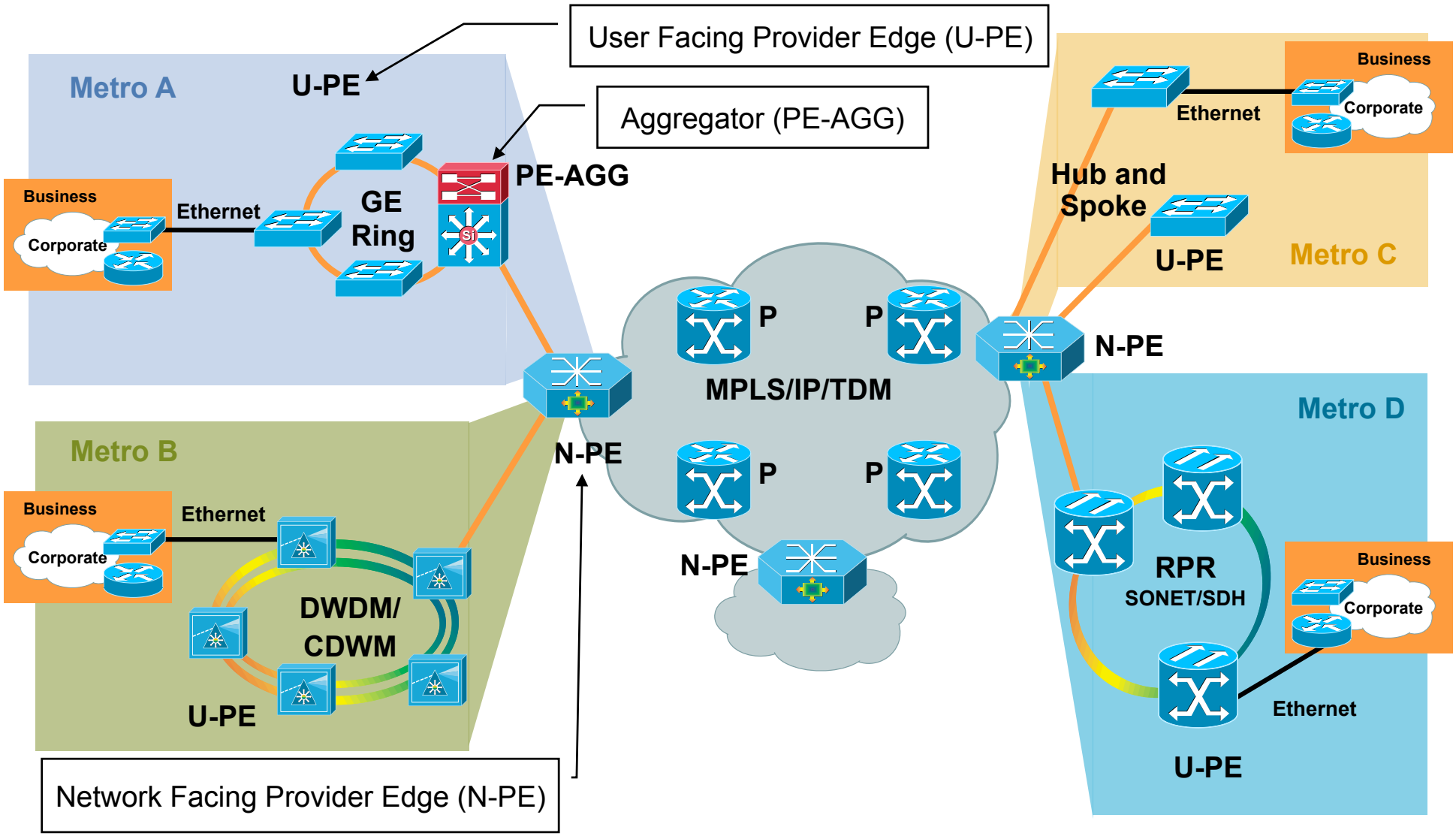
Access U-PE	Aggregation PE-AGG	Edge N-PE	Core P
Admission control, Security Policy Enforcement, Classification, Policing and Marking, Queuing and scheduling	Traffic aggregation, Congestion management, L2 wholesale handoff, Service insertion	MPLS, L2TPv3,EoMPLS H-VPLS, L3VPN, Internet Access, Service Gateway, Value Added Services (Security, Voice,…)	Fast Packet Forwarding (IP/MPLS), Sophisticated Traffic Engineering and Congestion management

Flexible Ethernet Edge

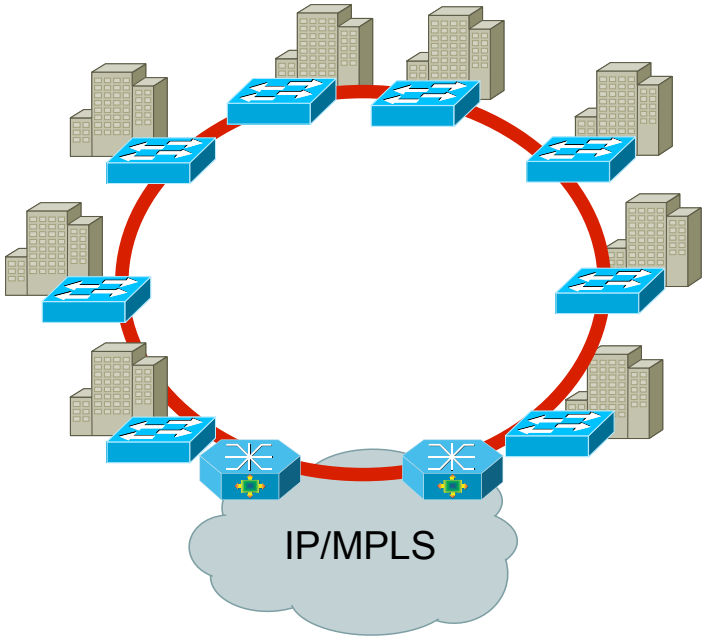


Carrier Ethernet

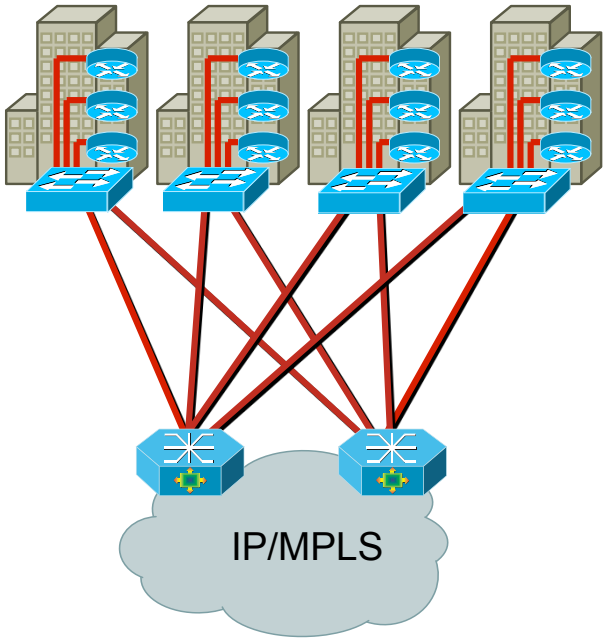
Sample Deployments



Ethernet Access Topologies



- Ethernet access rings → multiple spanning tree
- Convergence dependant on VLANs/MAC-addresses
- Often non-deterministic
- No support for per VLAN STP
- STP being replaced by ring optimized protocols



- Hub and spoke → FlexLink or link aggregation
- Fast convergence independent of VLANs/MAC-addresses

Resilient Ethernet Protocol

Problem Statement

- Large spanning-tree domain
- Carrier Ethernet trend
  - Fast convergence requirements
  - Spanning tree not perceived as carrier-class
- Complexity of management and troubleshooting of STP
- REP addresses these issues

What Is REP?

- A new protocol designed to provide a solution for fast and predicable Layer 2 convergence for carrier Ethernet networks
- Fast and predictable convergence
  - Convergence time: 50 to 250 ms
  - Fast failure notification even in large rings
- Limit the scope of spanning tree
  - STP is deactivated on REP interfaces
- Allows VLAN load balancing for optimal bandwidth utilization
- Cisco proprietary (so far, future alignment with ITU-T G.8032)

Carrier Ethernet Services

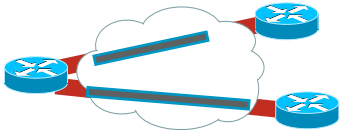
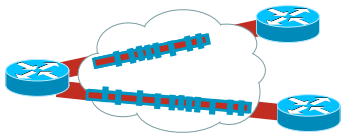
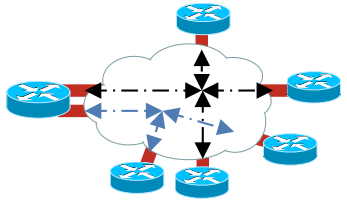
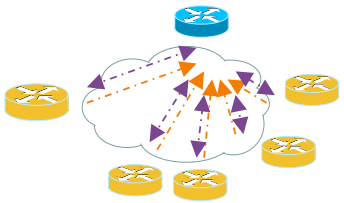
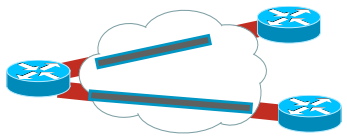
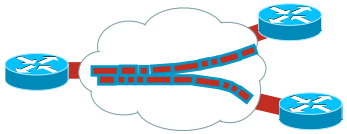
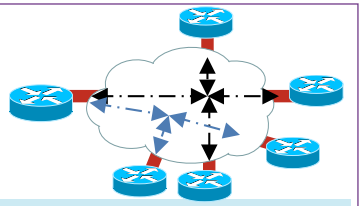
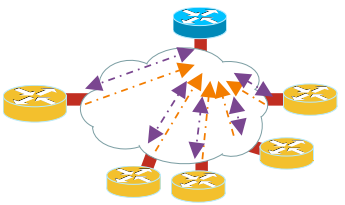
Carrier Ethernet Services

The Basics

- Business connectivity provided using MEF services
- SP may offer point-to-point or multipoint services
- Point-to-point services called E-Line
  - Ethernet Private Line (EPL)
  - Ethernet Virtual Private Line (EVPL)
- Multipoint services called E-LAN
  - Ethernet Private LAN (EPLAN)
  - Ethernet Virtual Private LAN (EVPLAN)
- Classification dependent upon access features

Services Standards Map

Summary

	Point-to-Point EVC		Multipoint EVC	Rooted MP EVC
	Dedicated Service Layer	Shared Service Layer		
Port-Based EVC Identification (Un-Mux'ed UNI)	 ITU-EPL Type 1 (GFP-T) ITU-EPL Type 2 (GFP-F)	 ITU-EVPL Type 2	 ITU: SG 15/11 Work…	
	MEF-EPL** (with QoS: 3C2R or 2C1R)		MEF: EP-LAN*	MEF: EP-Tree*
VLAN-Based EVC Identification (Mux'ed UNI)	 ITU-EVPL Type 1	 ITU-EVPL Type 3	 ITU: SG 15/11 Work…	
	MEF EVPL*** (with QoS: 3C2R or 2C1R)		MEF: EVP-LAN*	MEF: EVP-Tree*
	MEF E-Line		MEF E-LAN	MEF E-Tree*
	IETF: VPWS		IETF: VPLS	IETF: Work Started…

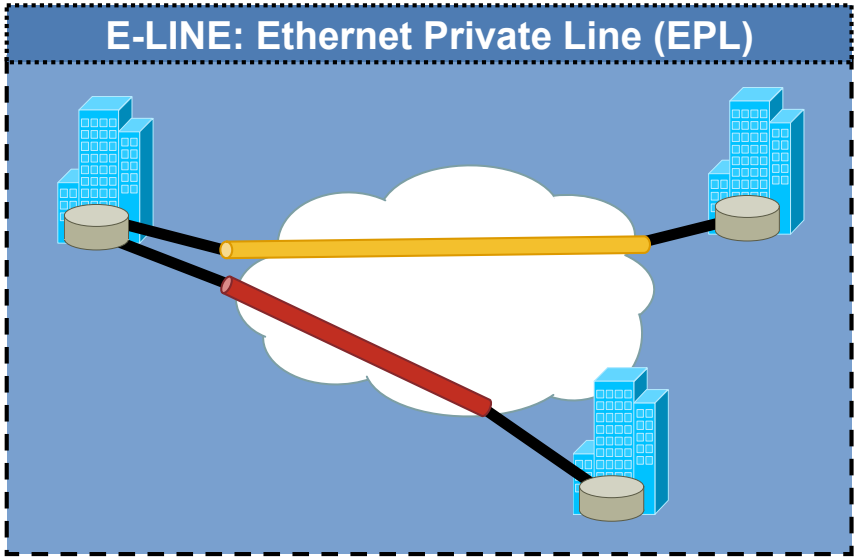
* Phase Two Specs Stable, Document in Letter Ballot (Revised Specs Will Be MEF 6.1 and MEF 10.1)

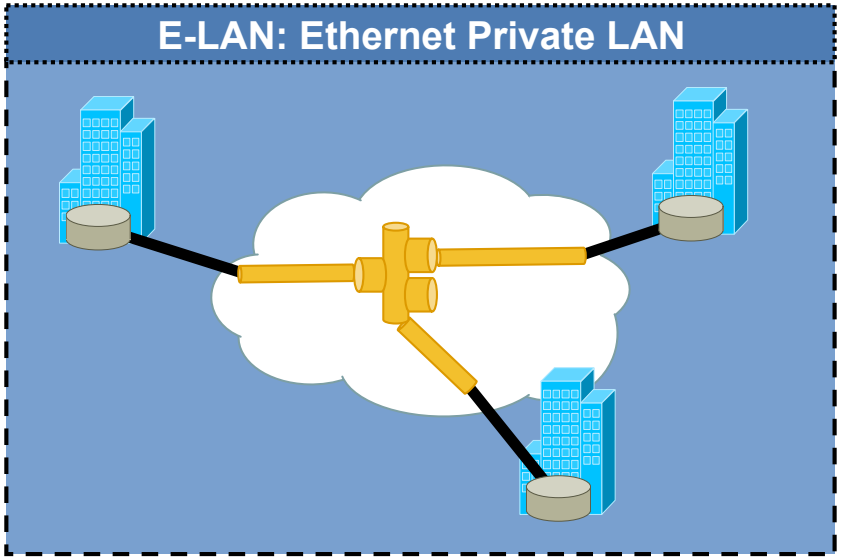
** E-Private-Line, Phase 2 Similar to MEF6 EPL, but with Expanded Scope (Including Multiple Classes of Service and 2R3C Policing)

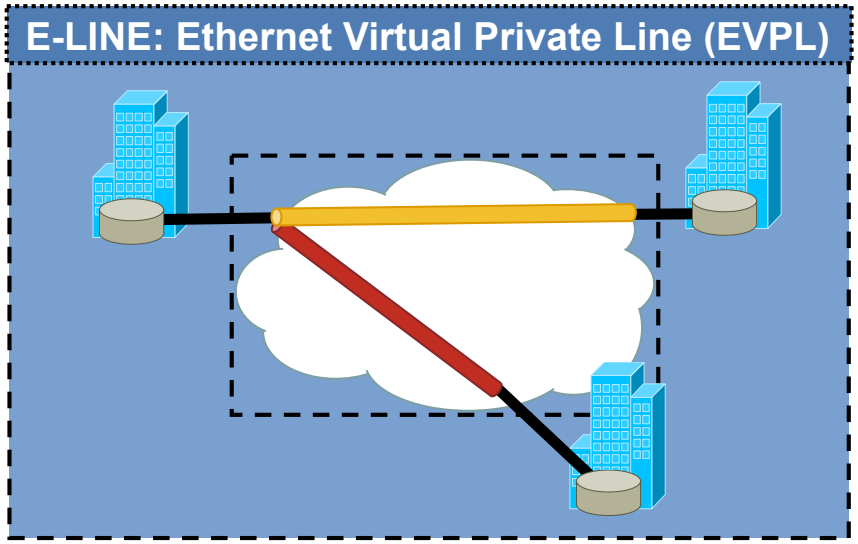
*** E-Virtual-Private-Line (Phase 2), Similar to MEF6 EVPL; Phase 2 Service Definition Is More Restricted than EVPL Phase 1; EVPL Has to Be VLAN-Based (Port-Based No Longer Allowed)

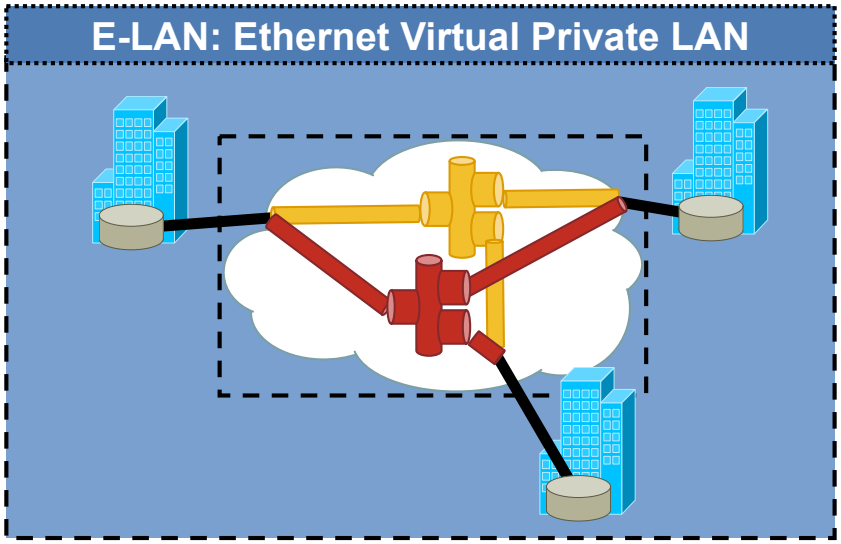
Carrier Ethernet Services

Service Visualization







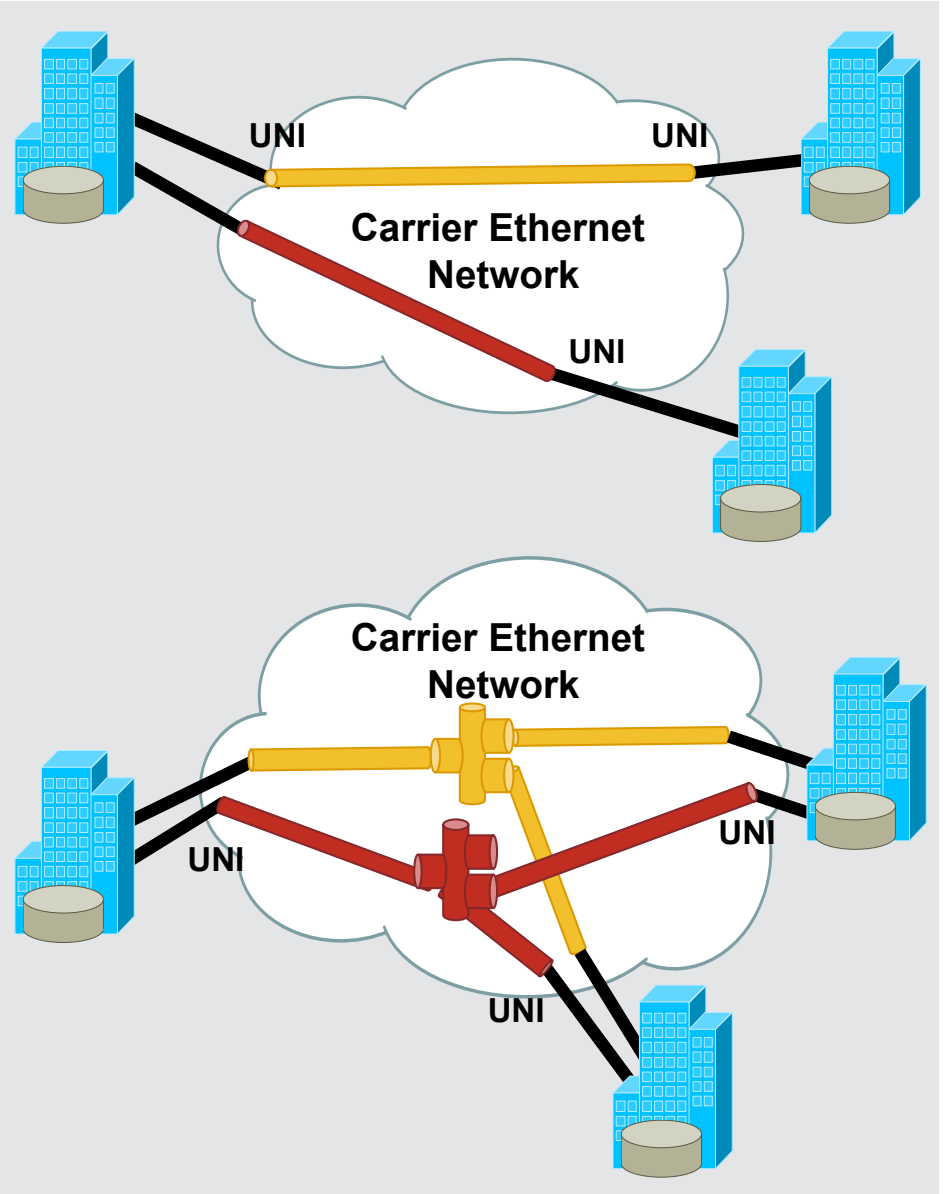


Carrier Ethernet Services

EPL/EPLAN*

Service Features

- Port-based service
- H-VPLS/EoMPLS in the core
- L2PDU tunneling support
- High degree of transparency
- Multiple classes of service
- Router or switch as CPE



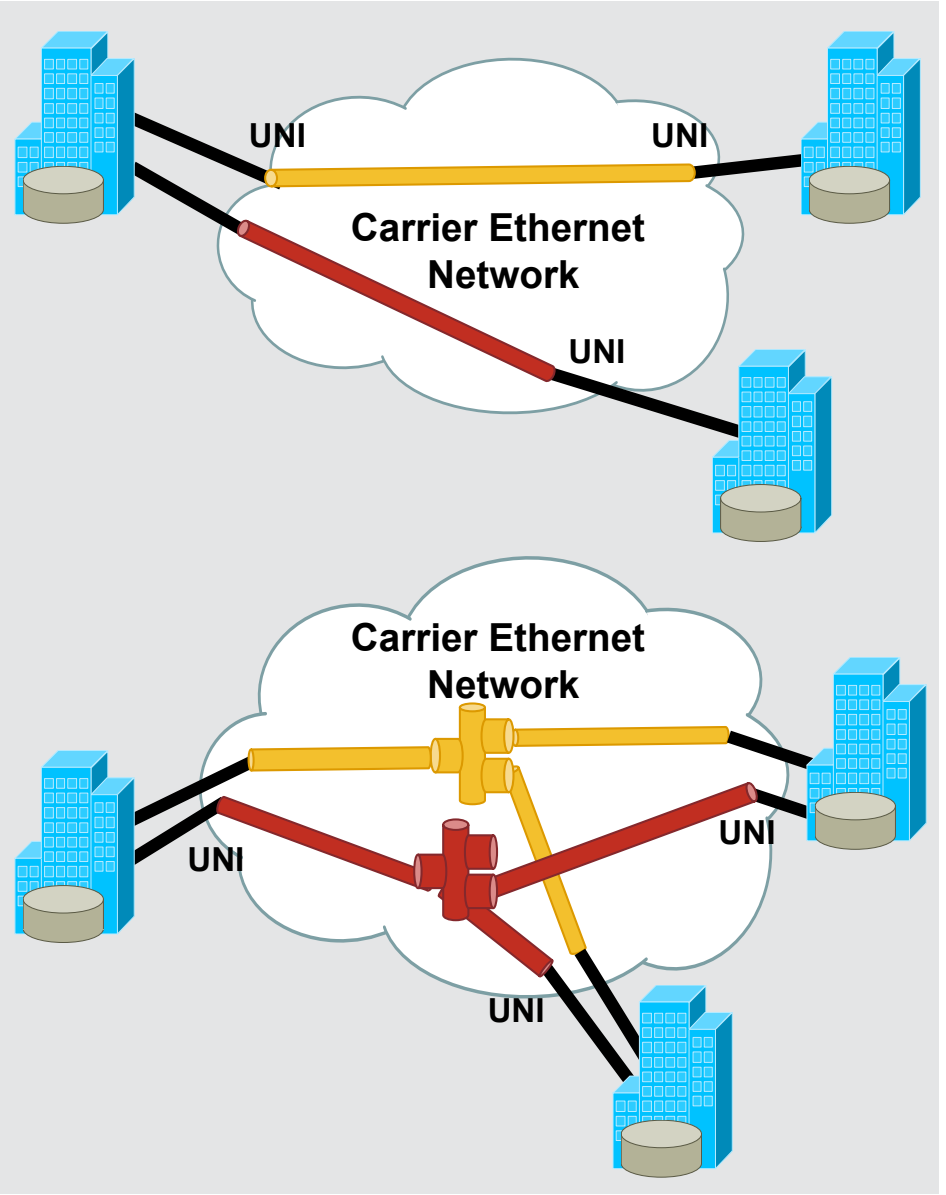
*EPLan—Name not yet adopted by MEF but covered under E-LAN Service Type

Carrier Ethernet Services

EPL/EPLAN*

Sample SP Offering

- Corporate/Campus LAN Extension over WAN
- Business Connectivity
- Data Center
- Network consolidation



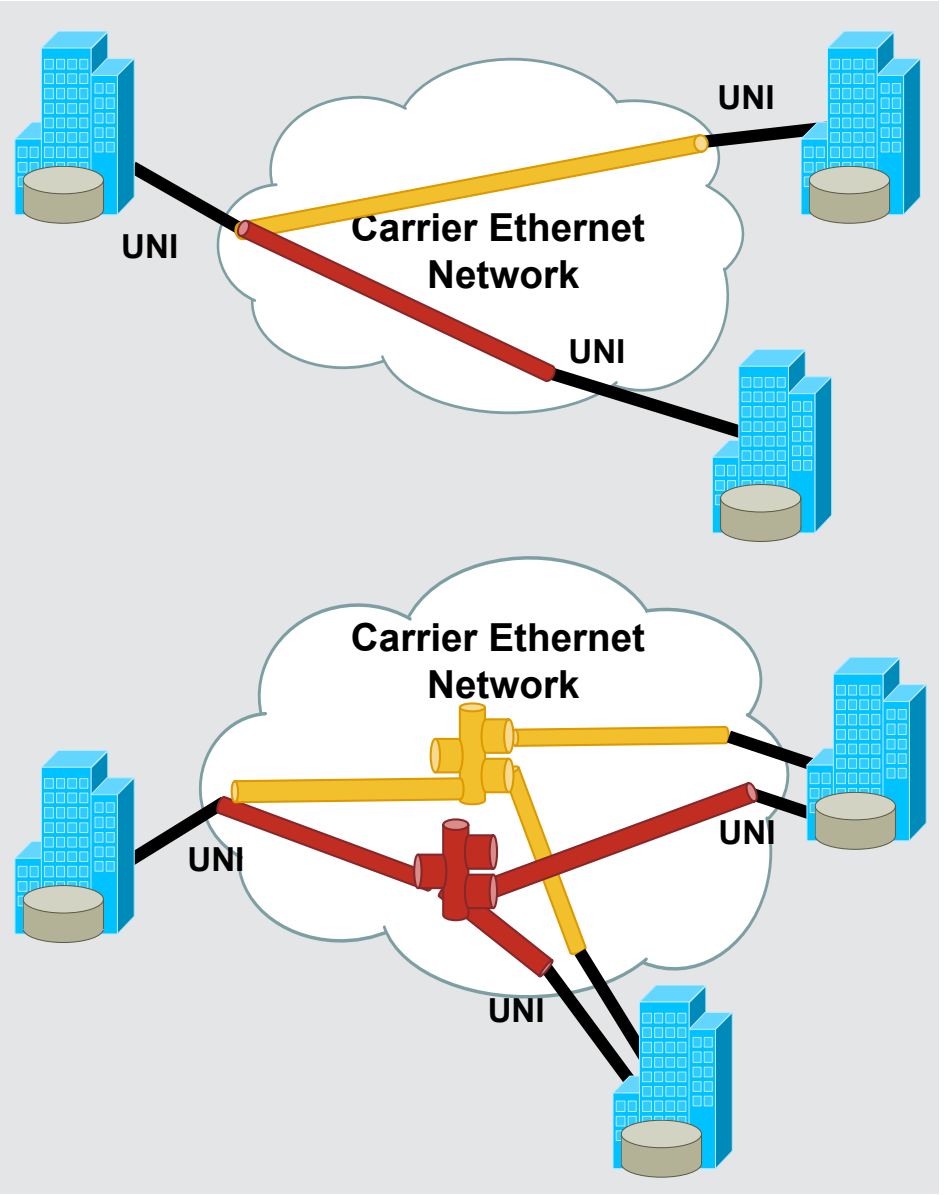
*EPLan—Name not yet adopted by MEF but covered under E-LAN Service Type

Carrier Ethernet Services

EVPL/EVPLAN*

Service Features

- Service multiplexing at UNI
- H-VPLS/EoMPLS in core
- Multiple classes of service
- No support for L2PDU tunneling
- Scalability for larger sites
- Router recommended as CPE



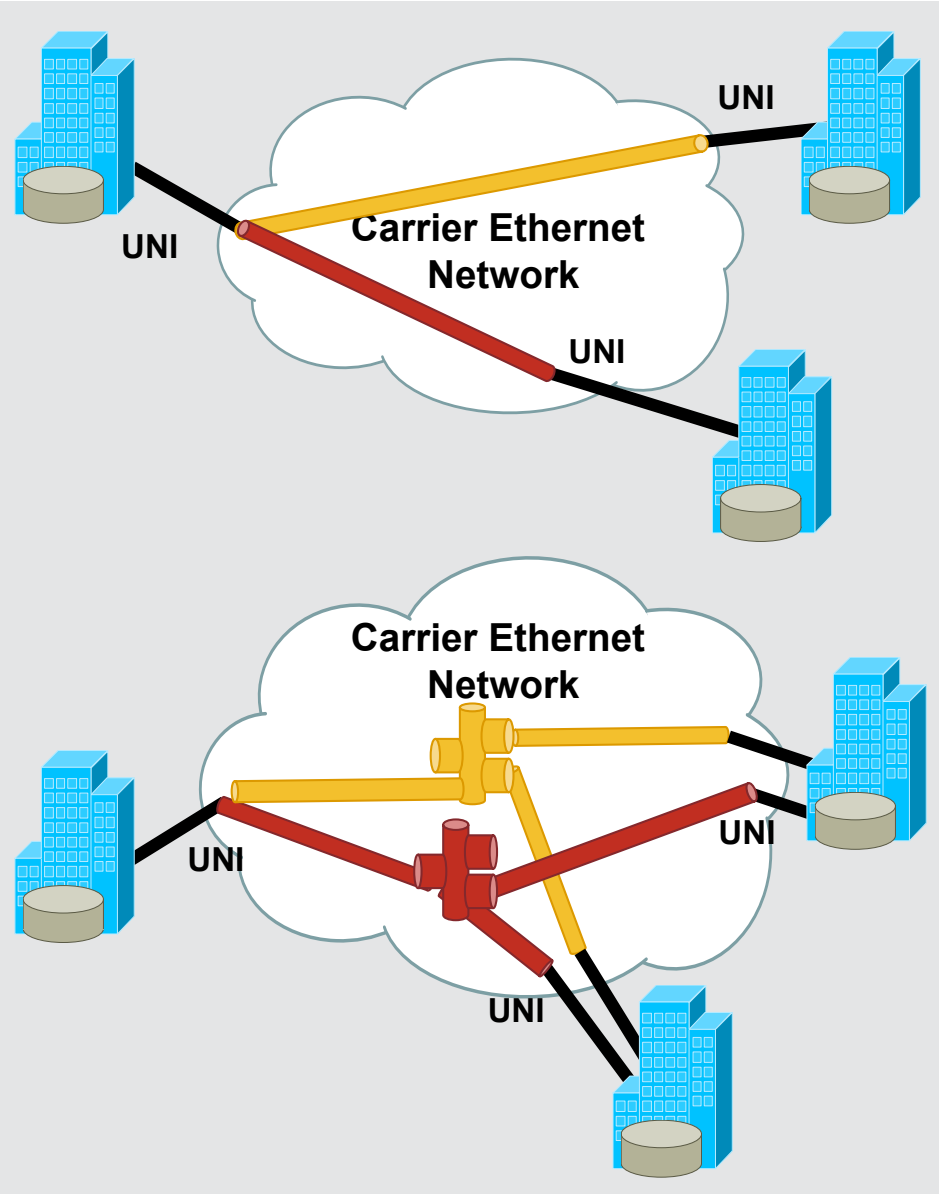
*EVPLan—Name not yet adopted by MEF but covered under E-LAN Service Type

Carrier Ethernet Services

EVPL/EVPLAN*

Sample SP Offering

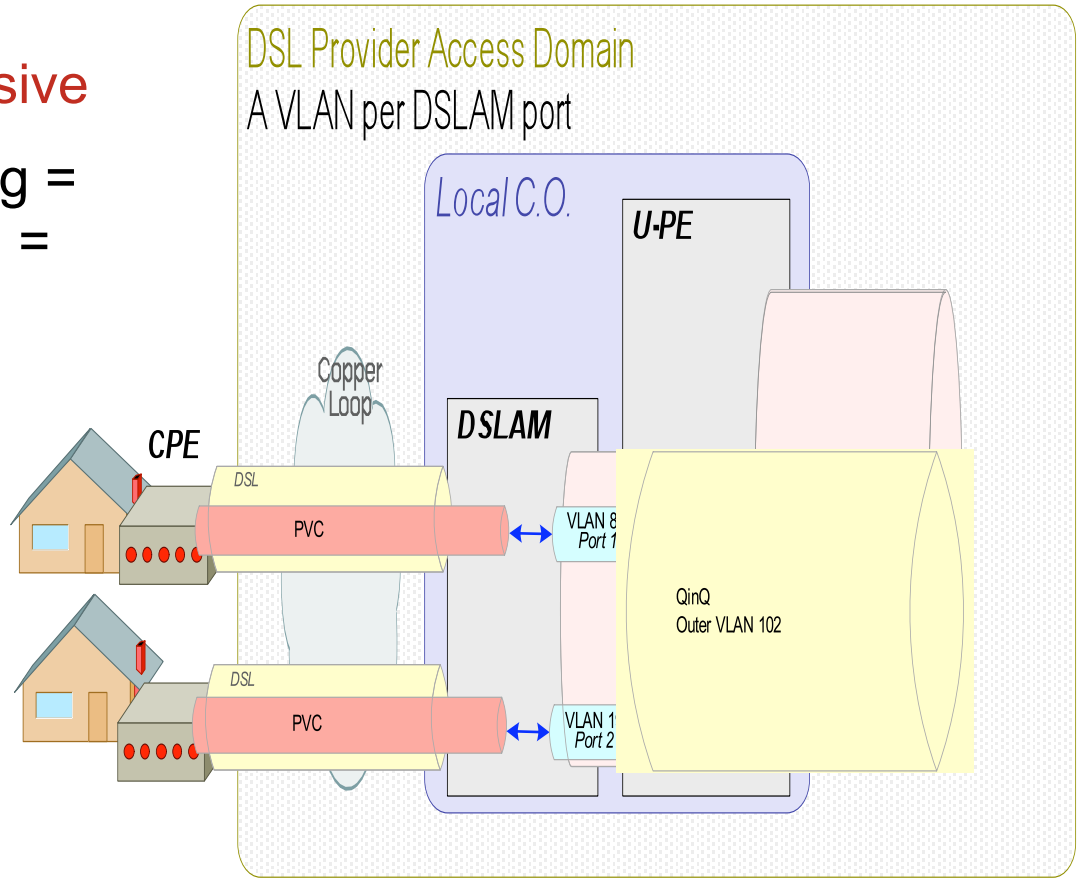
- Branch offices (L2VPN, F/R equivalent)
- IP VPN (L3VPN) access
- Internet (ISP) access
- Disaster Recover



*EVPLan—Name not yet adopted by MEF but covered under E-LAN Service Type

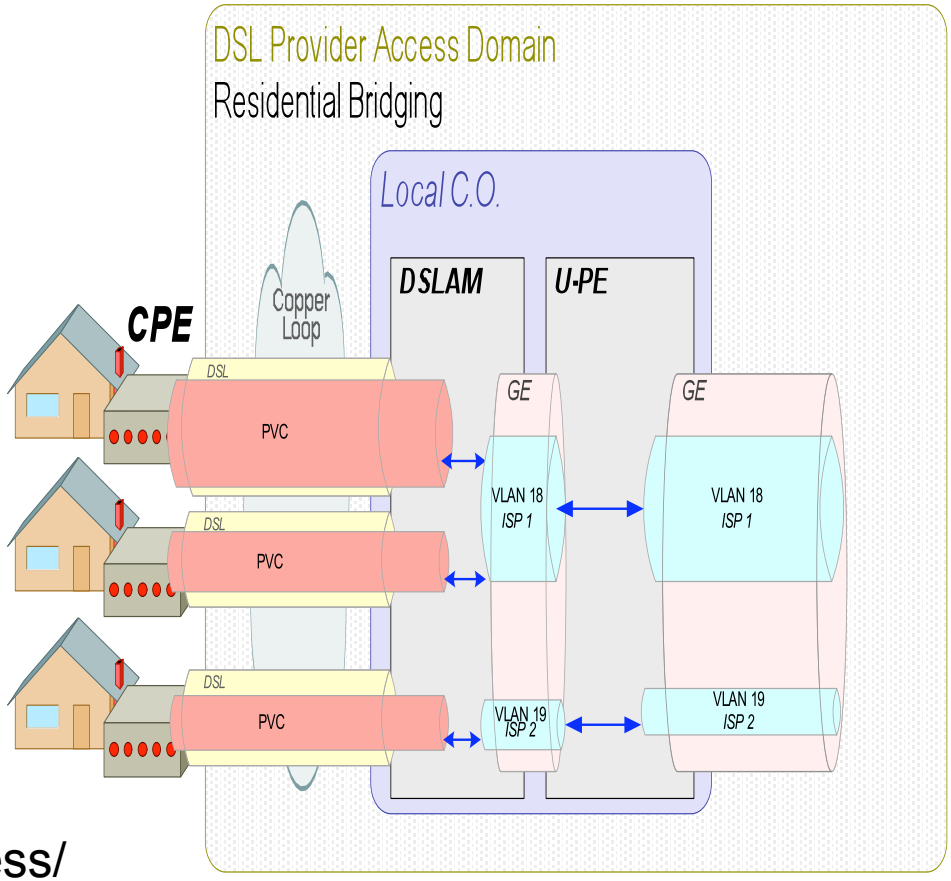
VLAN Architecture: VLAN per User (1:1)

- VLAN use similar to ATM, i.e. connection-oriented, i.e., configuration intensive
- IEEE802.1ad—inner tag = port identifier, outer tag = DSLAM identifier
- Multicast replication inside single BNG, **not** inside Ethernet aggregation network
- Multihoming to two BNGs is complex
- Good for p2p business services; less ideal for triple-play services

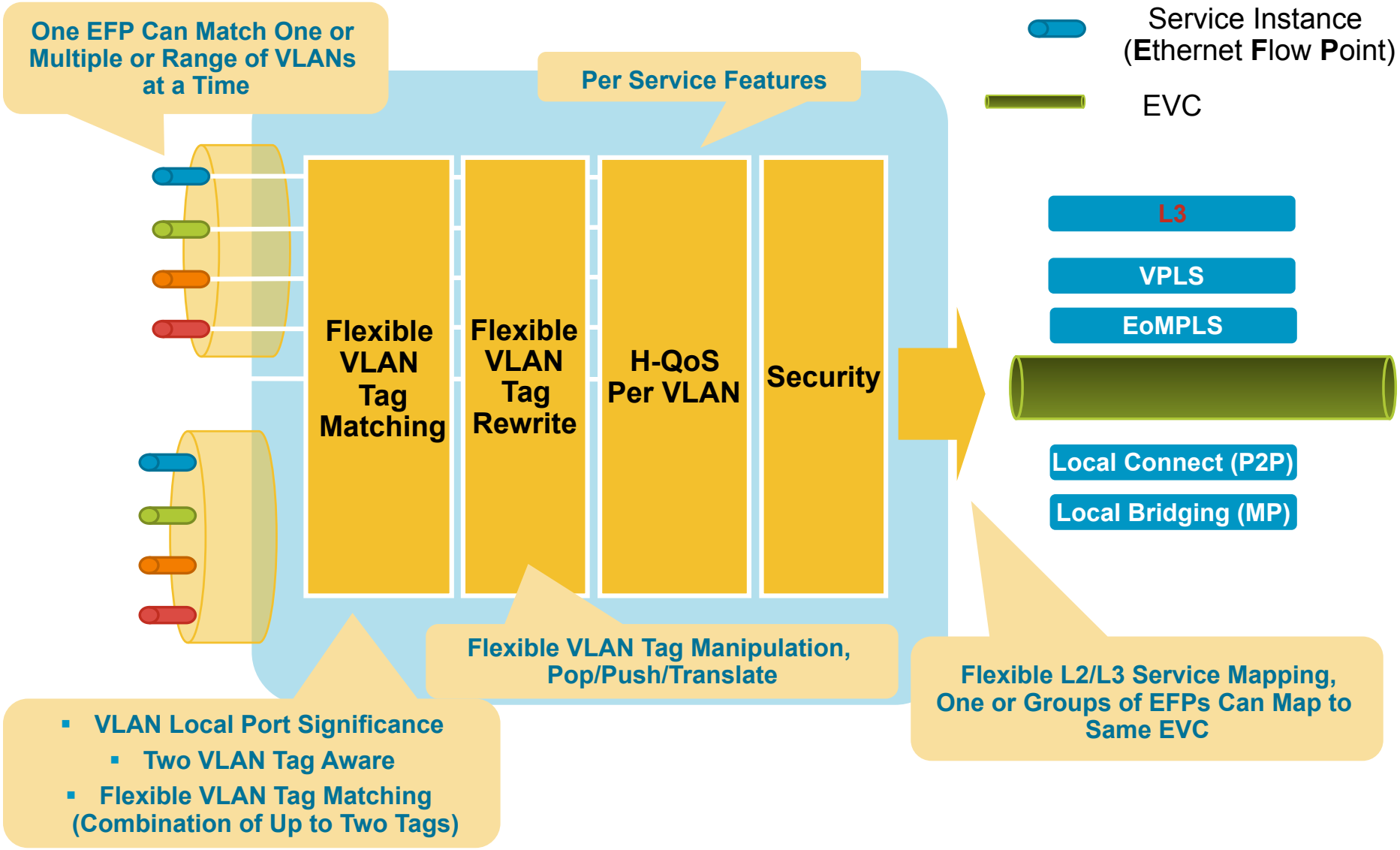


VLAN Architecture: VLAN Per Service/SP (N:1)

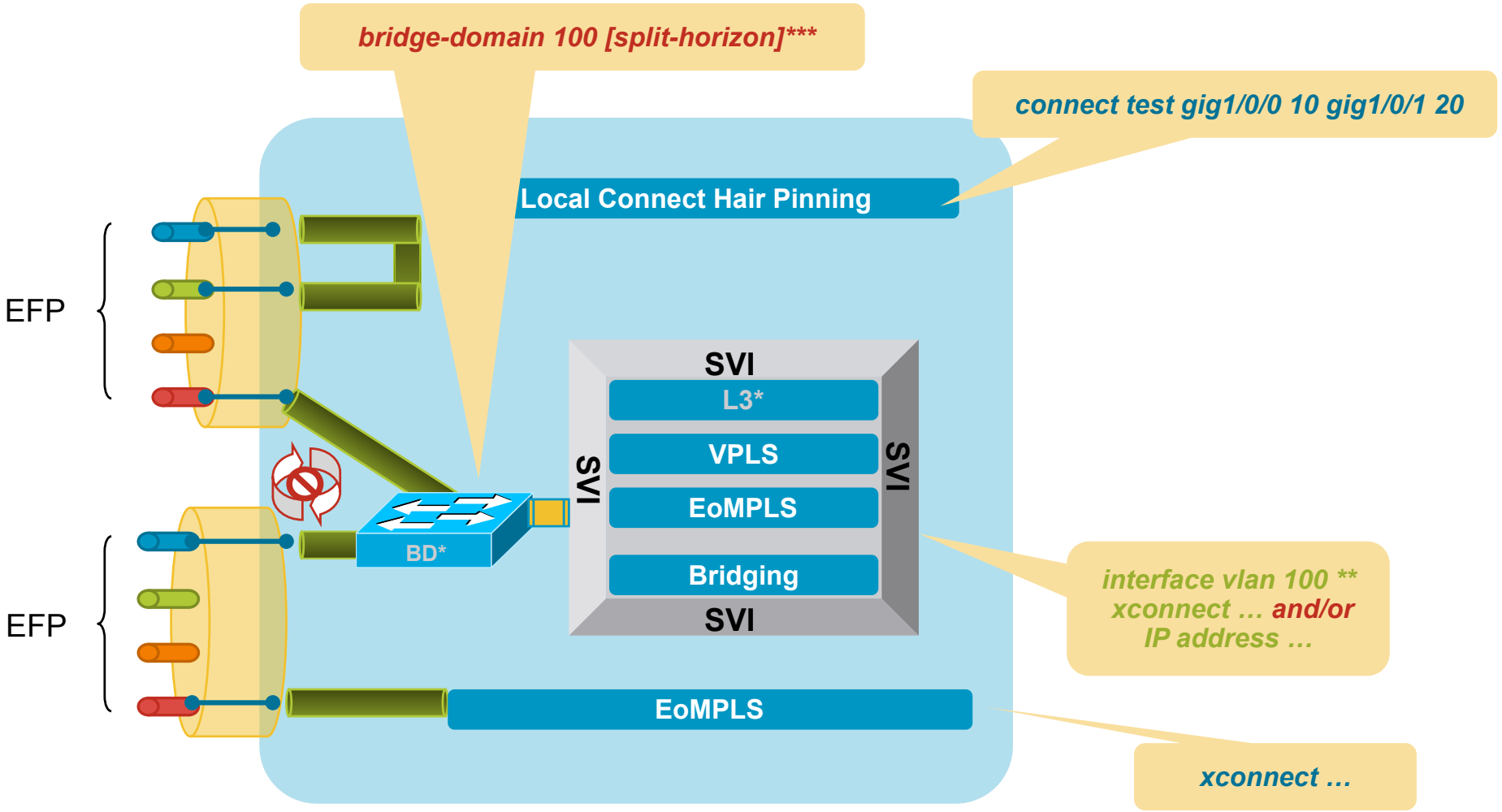
- Single tagged (802.1Q or 802.1ad) VLANs—double tagging not needed
- Connectionless provisioning benefit; access node inserts line ID (DHCP Opt 82 , PPPoE intermediate agent)
- Network elements take care of subscriber MAC isolation through split horizon forwarding
- Multiple injection points per VLAN (BRAS **and** video service router) possible
- Multicast replication within access/ aggregation



Ethernet Virtual Connection (EVC) Overview



EVC: Flexible Service Mapping Summary



*** Multiple EFPs into one global VLAN for L2 bridging; split-horizon option to enable/disable bridging between EFPs

** L2/L3 service associated to bridge-domain (global VLAN)

* L3 termination is done by Switched Virtual Interface (SVI) or by sub-interface

Approaches for implementation

- Control Plane & Forwarding Plane Options

  QinQ (With or without STP)

  Mac-in-Mac (With or without STP)

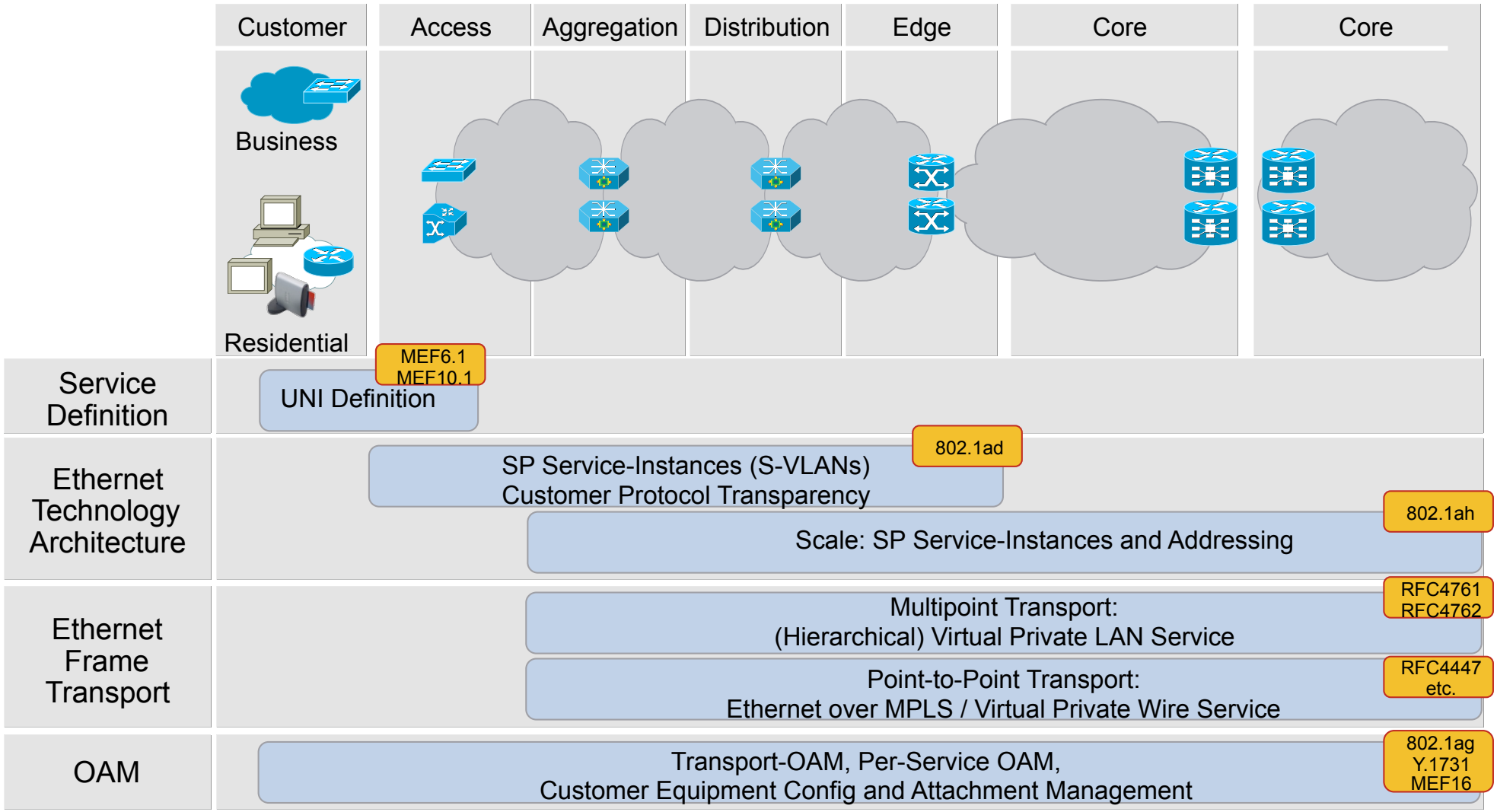
  IP/MPLS

  PBB-TE, T-MPLS, GMPLS …….

- Basic idea is similar across the approach i.e. use the existing technologies to expand the scalability of existing “enterprise or services providers’ technologies” to handle large Ethernet networks

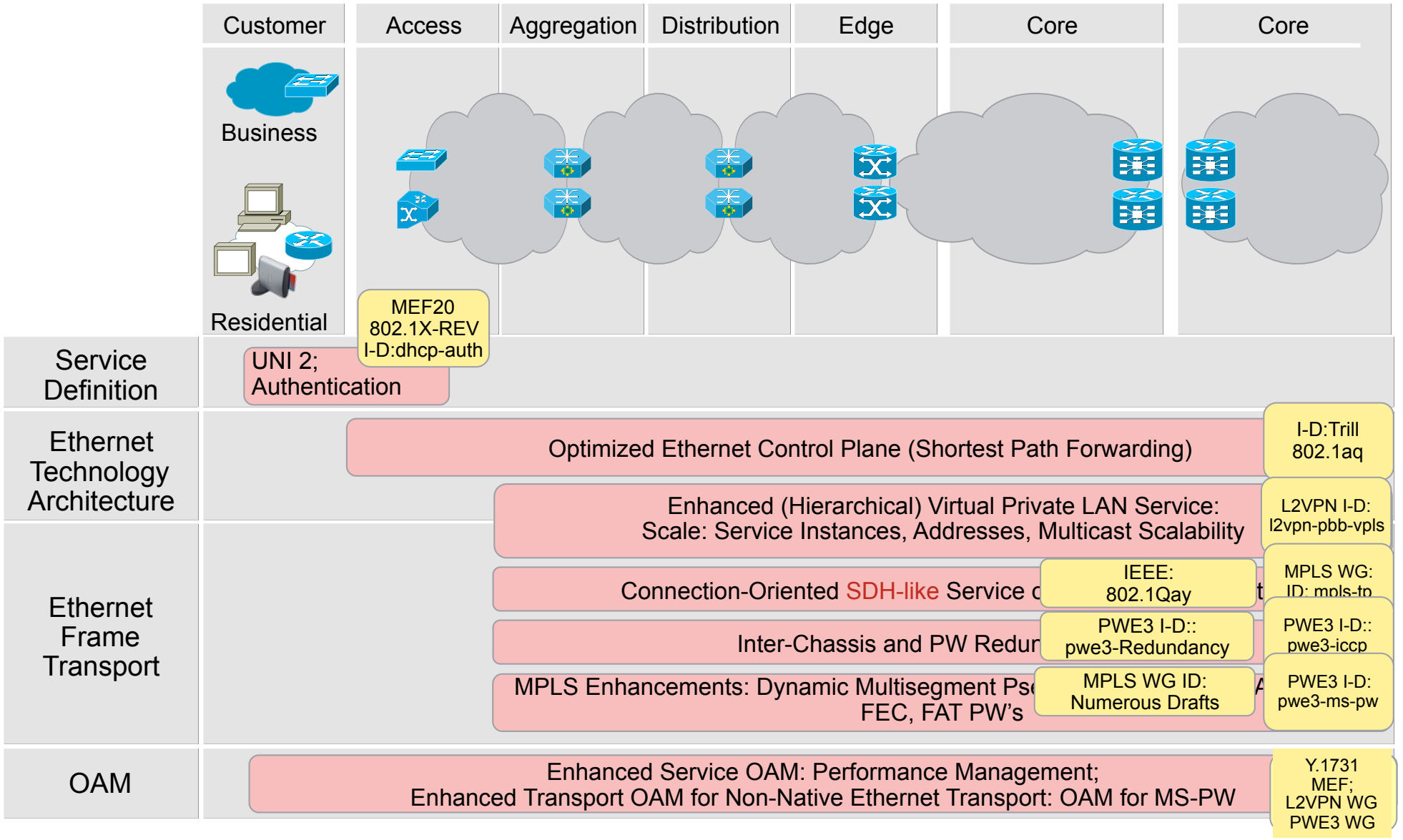
Carrier Ethernet Standards

First Phase

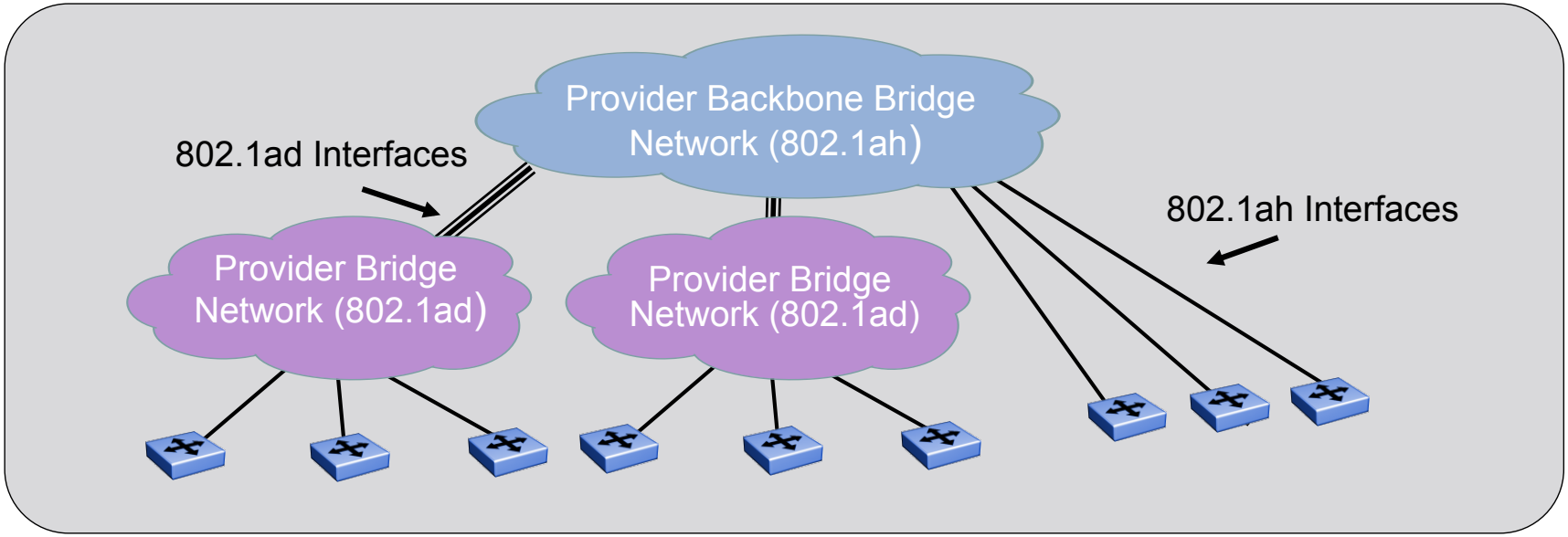


Carrier Ethernet Standards

Second Phase—In Process

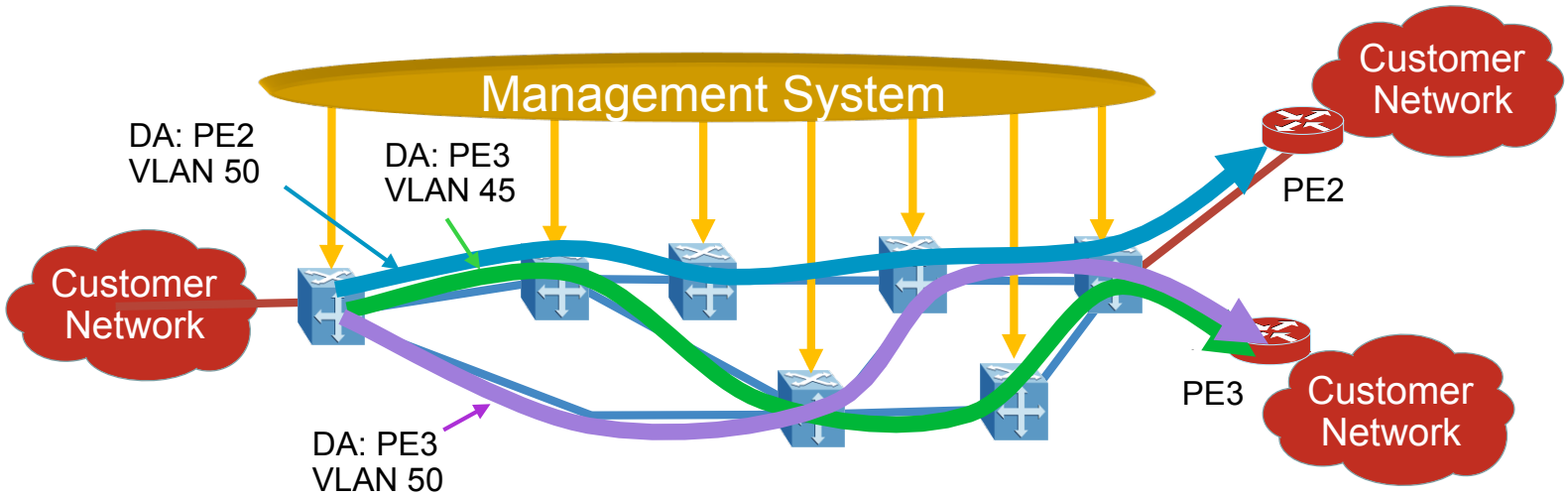


Provider Backbone Bridges (802.1ah)



- IEEE 802.1ah = PBB = MAC in MAC
- Scales multipoint Layer 2 services
- Customer demarcation
- ELAN, ELINE, and ETREE
- 16 million service IDs
- Assumes STP, but could also ‘hide’ topology and make it loopfree by LAN Emulation (VPLS). Future: ISIS (802.1aq)

Provider Backbone Bridges—Traffic Engineering (802.1Qay)

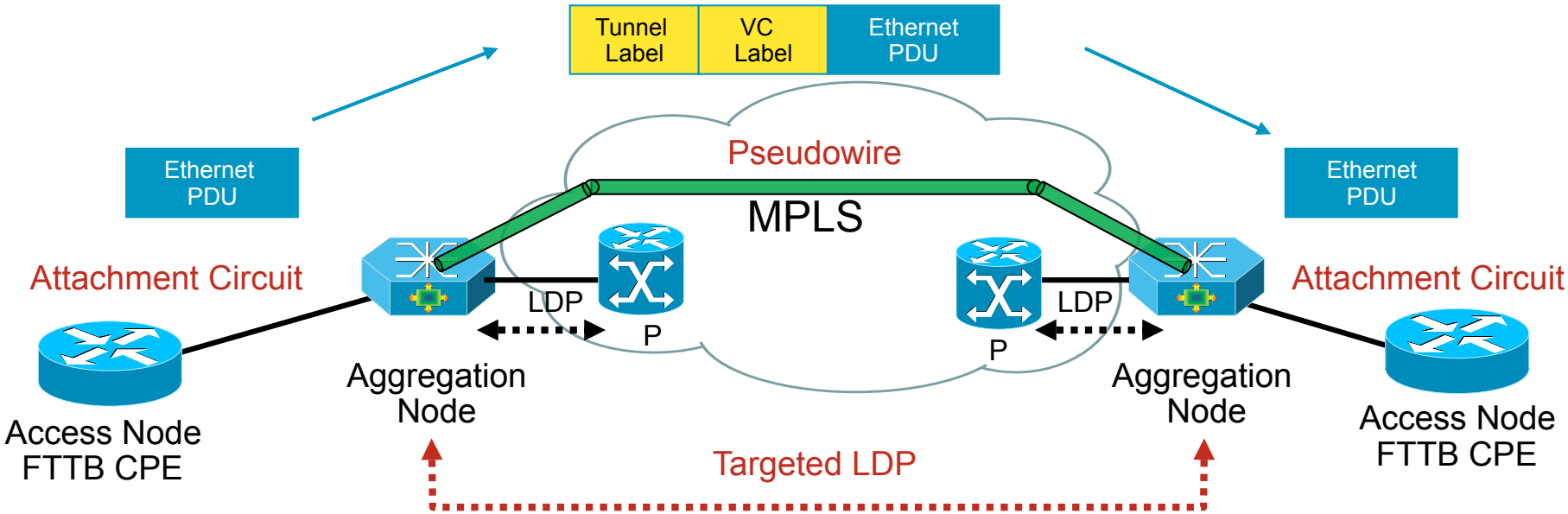


- Static offline control plane
- Long-haul optics MTTR challenge five nines
- Long-haul RTT challenge 50-msec failover
- Scale challenges with end-to-end heartbeats
- Non-trivial backup path selection

L2 MPLS Transport

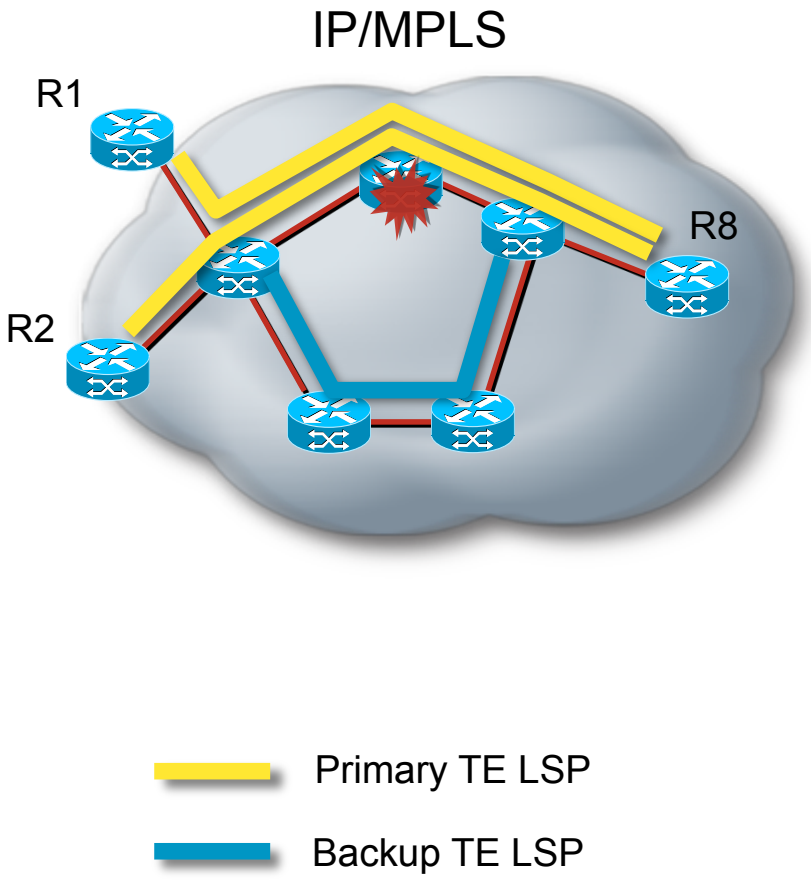
- Two technologies for L2 transport over MPLS:
  - Ethernet over MPLS (EoMPLS)
    - Used for L2 point-to-point link over MPLS cloud
    - No MAC learning involved
  - Virtual Private LAN Services (VPLS)
    - Used for multipoint L2 connections
    - Collection of pseudowires tied together by a Virtual Forwarding Interface (VFI)
    - MAC addresses learned on VFI
    - Traffic forwarding based on destination MAC addresses
    - H-VPLS, an extension of VPLS
- Can co-exist with L3VPNs (MPLS-VPNs/RFC2547bis)
- Both L2 and L3 VPNs can leverage traffic engineering with Fast Reroute (TE-FRR)

EoMPLS Overview



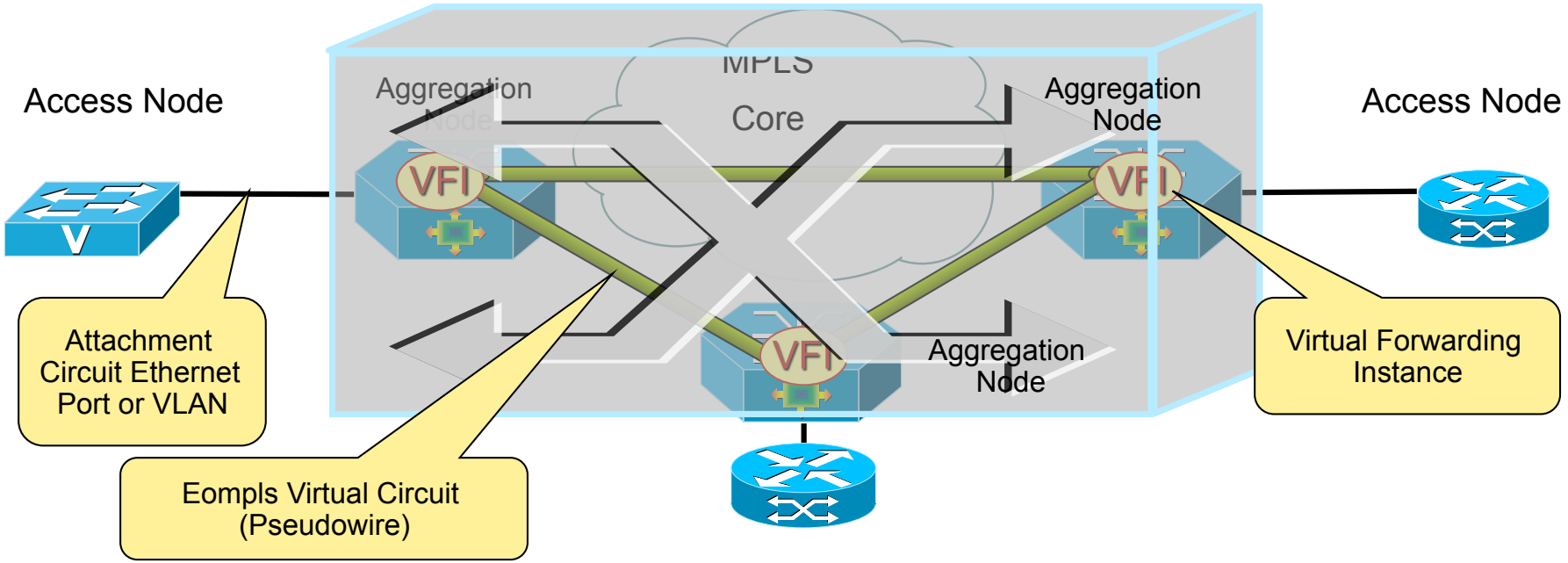
- MPLS in the aggregation network and core
- Targeted LDP session between PEs to exchange VC label
- Tunnel label is used to forward packet from PE to PE
- VC label is used to identify L2VPN circuit
- Attachment Circuit (AC) can be port-based or VLAN-based

MPLS TE Fast Re-Route (FRR)



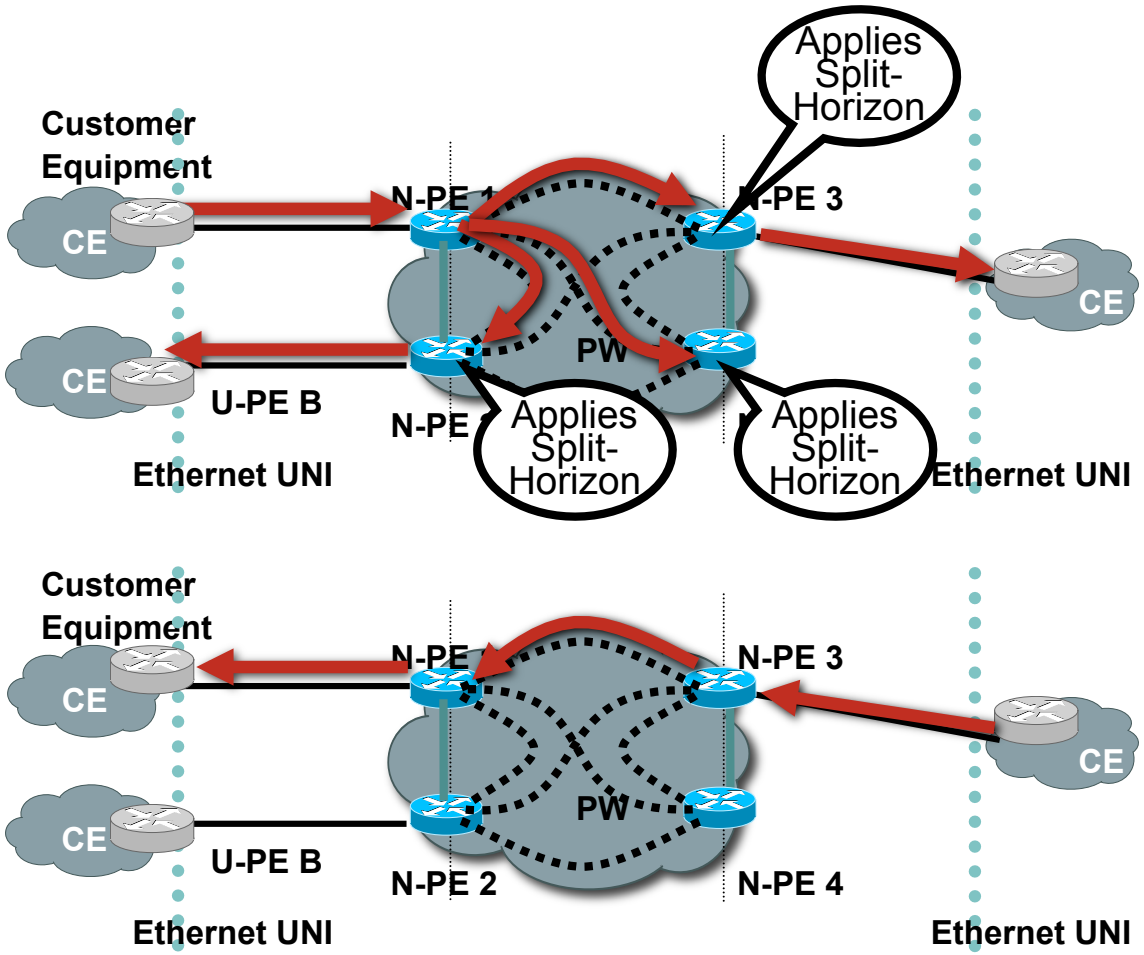
- Subsecond recovery against node/link failures
- Scalable 1:N protection
- Greater protection granularity
- Cost-effective alternative to optical protection
- Bandwidth protection

VPLS (Virtual Private LAN Services)



- Attachment Circuit (AC)—connection to aggregation using an Ethernet VLAN
- Virtual Circuit (Pseudowire)—EoMPLS tunnel between PEs using a full mesh
- Virtual Forwarding Instance (VFI)—A virtual L2 bridge instance that connects ACs to VCs (PWs); VFI=VLAN=broadcast domain

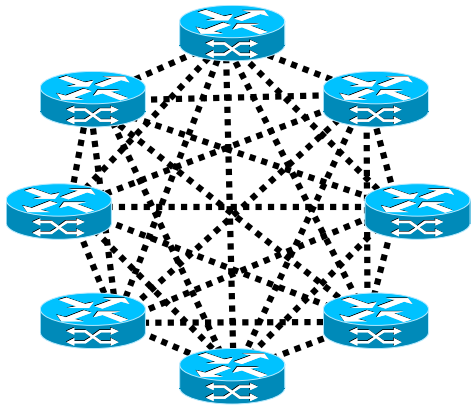
How VPLS Works.
Emulating a Bridge: Flooding, Forwarding,...



- 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

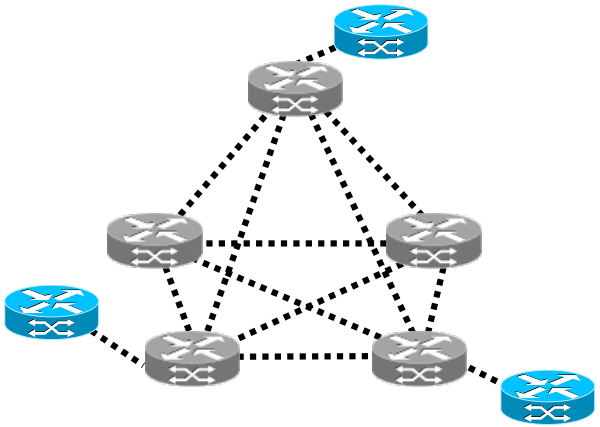
Hierarchical-VPLS: Why?

VPLS



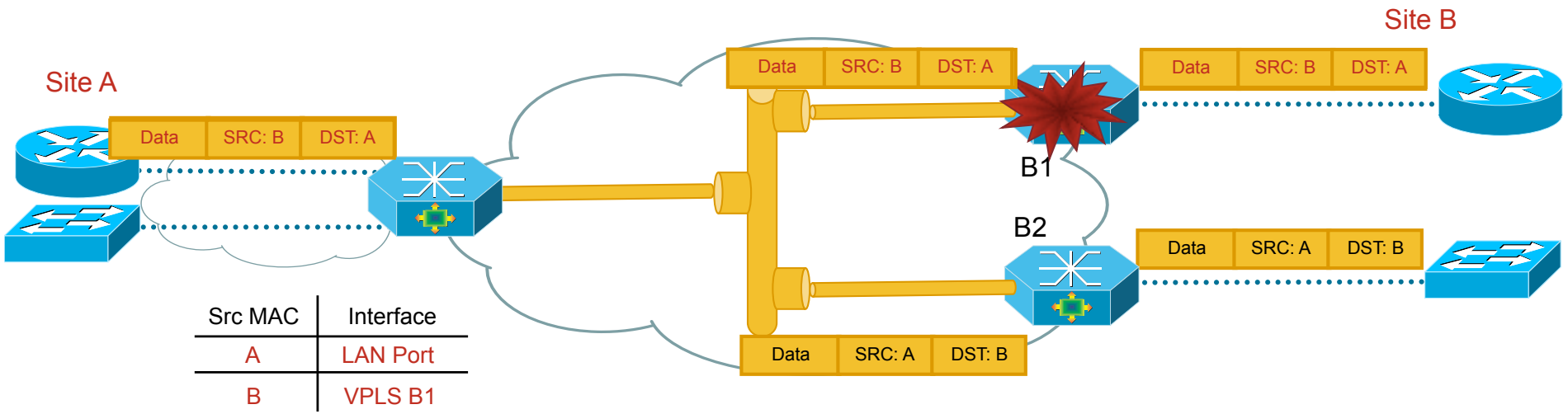
- Potential signaling overhead
- Full PW mesh from the Edge
- Packet replication done at the Edge
- Node Discovery and Provisioning extends end-to-end

H-VPLS



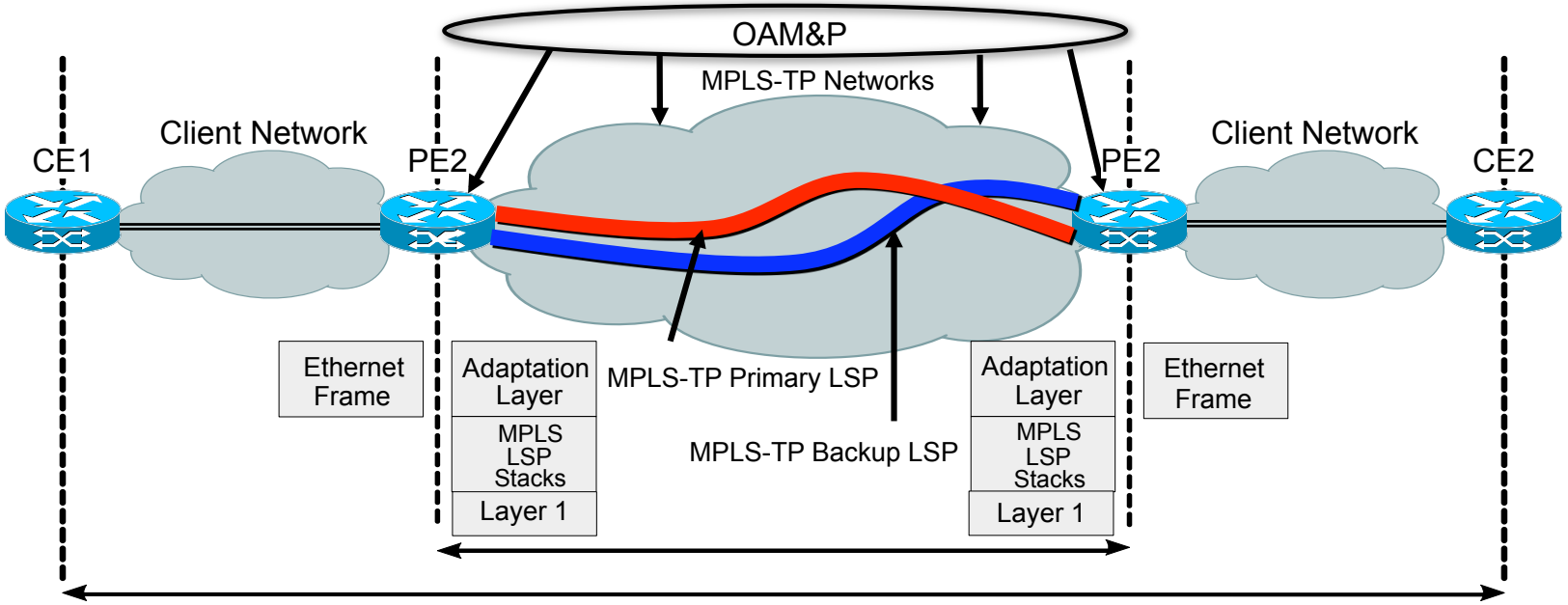
- Minimizes signaling overhead
- Full PW mesh among Core devices only
- Packet replication done the Core only
- Partitions Node Discovery process
- H-VPLS Flavors: H-VPLS with Ethernet Access & H-VPLS with MPLS Access

VPLS Traffic Forwarding Example



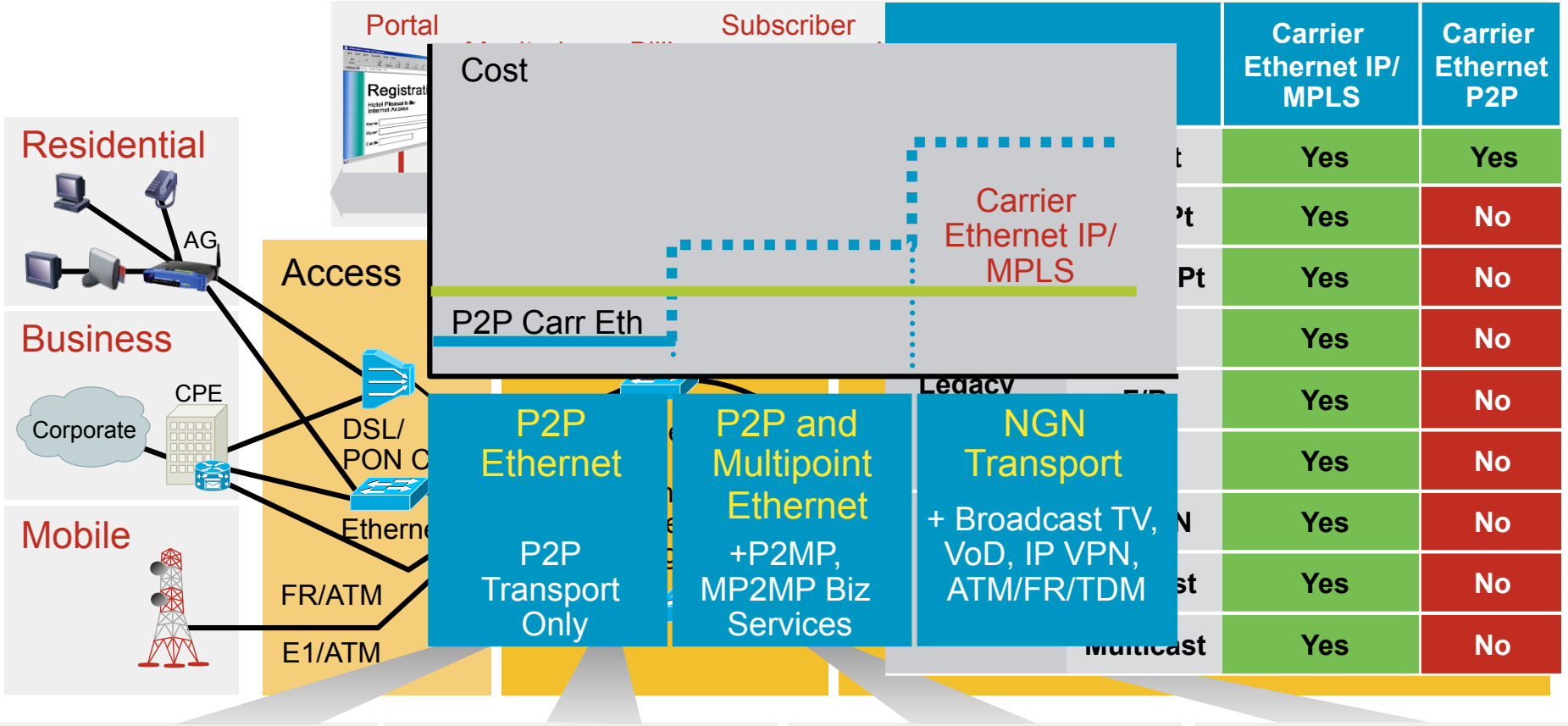
- Initial traffic across all pseudowires; MAC address learned
- Traffic sent to relevant pseudowires
- On N-PE failure, pseudowires goes down, MACs flushed
- MAC learning process again

MPLS-TP Perspective



- MPLS-TP similar solution PBB-TE, except MPLS encapsulation and different OAM
- Same MTTR and RTT issues
- Now aligned with IETF: T-MPLS → MPLS-TP
- OAM might simplify MPLS-based transport

Next-Generation Transport Requirements



	Carrier Ethernet IP/ MPLS	Carrier Ethernet P2P
t	Yes	Yes
Pt	Yes	No
Pt	Yes	No
	Yes	No
	Yes	No
	Yes	No
N	Yes	No
st	Yes	No
Multicast	Yes	No

Ethernet	Legacy Services	NGN Application	Others
Point-to-Point Point-to-MP Multipoint	ATM Frame Relay TDM	Efficient IP Multicast Efficient VoD Delivery Call Admission Control	QoS, OAM&P, TE, and Recovery Fast/Zero-Touch Provisioning

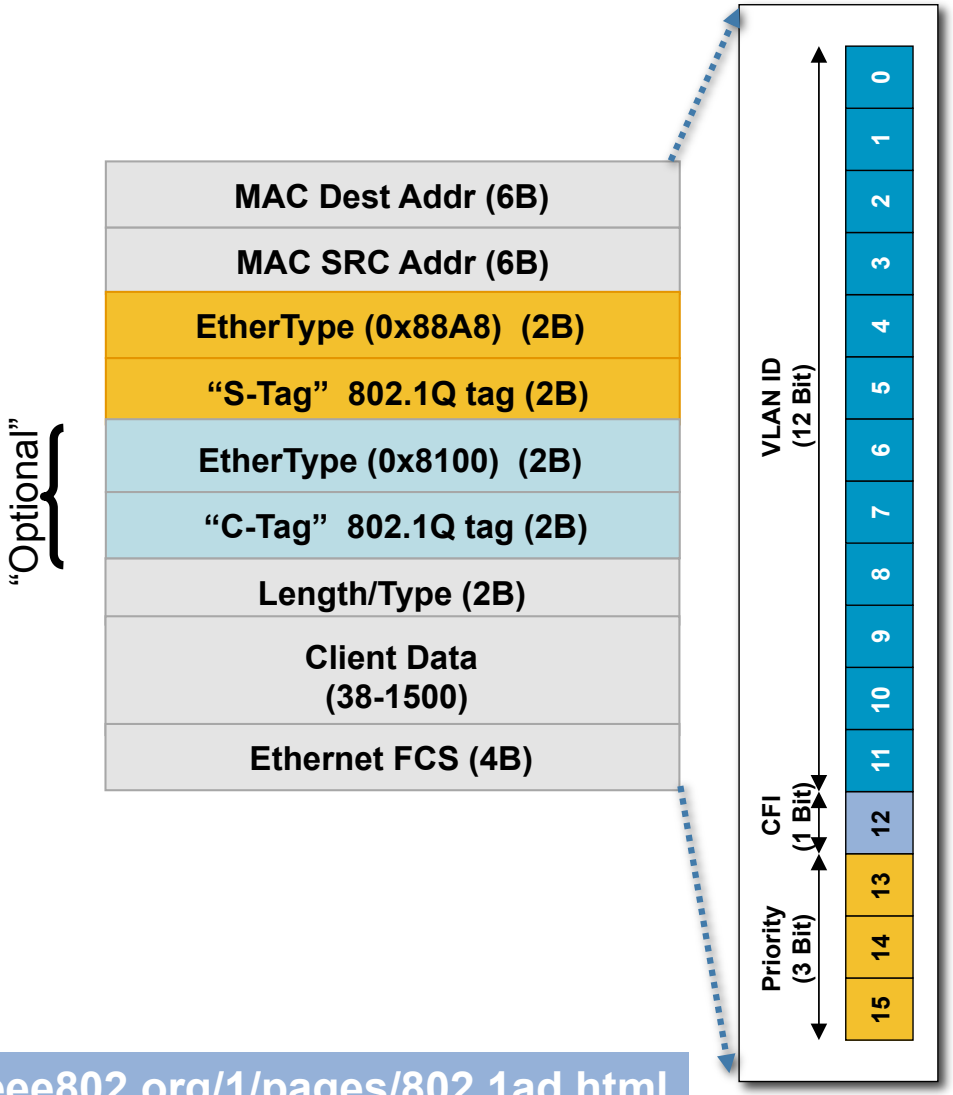
MPLS—Extending Service Spectrum

		L1, L2, L3 Services Pt-Pt, Pt-MPt, MPt-MPt	L1, L2 Services Pt-Pt and Pt-MPt
Node / Link Addressing	IP	IP	Multiple
Tunnel Provisioning	LDP or RSVP-TE	LDP or RSVP-TE External NMS	RSVP-TE External NMS
LSP Creation	Dynamic and static	Dynamic and static	Dynamic and static
Label space	Dynamic only	Split label space (static/dynamic)	Split label space (static/dynamic)
Load Balancing	Mainly ECMP	ECMP and no ECMP	No ECMP
Penultimate Hop Popping	PHP or no PHP	PHP or no PHP	No PHP (PHP TBC)
PW Setup	Static or tLDP	Static or tLDP	Static or tLDP
Recovery	Control Plane and OAM	Control Plane and OAM	Mainly OAM-based

MPLS-TP Enhances Existing MPLS Capabilities and Extends MPLS Applicability

IEEE 802.1ad Provider Bridges

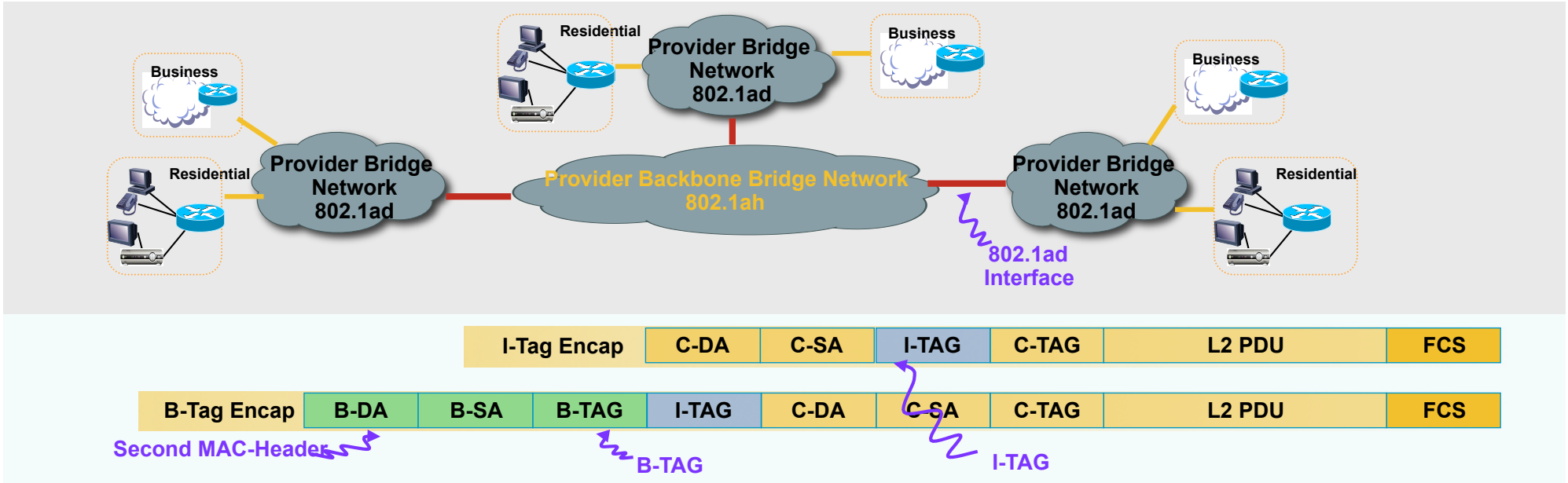
- Customer VLAN Transparency
  - IEEE 802.1ad will provide a standardized version of "QinQ" (Note: Inner .1Q tag is optional)
- Frame Format same as "QinQ"
  - New Ethertype: 0x88A8
- Customer Protocol Transparency
  - Reserve a block of MAC addresses (out of the block of 32) for the operation of customer bridges
  - Describe which of these reserved MAC addresses to be used for peering & how the peering is performed
  - Describe how and where to do discarding customer protocols (filtering action), describes how and where to tunnel them
- Draft Technically complete
  - Currently at Draft 6



http://www.ieee802.org/1/pages/802.1ad.html

IEEE 802.1ah PBB

- Defines an architecture and bridge protocols compatible and interoperable with Provider Bridged Network protocols and equipment
- Allows for services scalability (up to 2^{24} service instances) when interconnection of multiple Provider Bridged Networks by specifying
  - a service instance identifier (I-TAG) and
  - a Backbone VLAN ID (B-TAG) to allow for 2^{24} service instances.
- Allows for MAC address scalability by
  - Encapsulating Customer MAC-frames at the edge of the network into a “Provider MAC-Frame”



Services
Carrier Ethernet System

Market	Services	Access	SLA Type	SLA Example
Residential	Internet Access	Ethernet, PON, DSL, WIMAX	Transport	Dynamic access bandwidth, session/idle timeout, advertisements, post paid/prepaid (time and volume)
	VoIP Telephony	Ethernet, PON, DSL, WIMAX	Application	The number of VoIP appliances, SIP URLs/PST Phone numbers, active calls, VoIP call quality
	VoD	Ethernet,, PON, DSL	Application	The number of STBs, stream quality, content flavours, charging models
	TV	Ethernet, PON, DSL	Application	The number of STBs, type of TV packages, SD vs HD content and delivery quality
Business	L3 VPN MPLS/ Multicast	Ethernet, PON, DSL, WIMAX	Transport	Access bandwidth, differentiated services support, L3 VPN topology, managed services (MPLS/Multicast VPN)
	E-Line	Ethernet, PON, DSL, WIMAX*	Transport	Access bandwidth, differentiated services support, transparency
	E-LAN	Ethernet, PON, DSL, WIMAX*	Transport	Access bandwidth, differentiated services support, multipoint transport, transparency
Wholesale	L3 (P2P, MP)	DSL	Transport	Aggregated bandwidth on ISP level, differentiated services support, with subscriber management at ISP
	L2 (P2P, MP)	DSL	Transport	Aggregated bandwidth on ISP level, differentiated services support, transparent Ethernet transport P2P and MP (multicast optimized)

*** Ethernet Relay Point to Point and Multipoint only**

System Functional Overview
Carrier Ethernet System

Access Network Functions

DSL, Ethernet and Fixed WiMAX Access

- DSL Forum TR-101 functions
- MEF Ethernet services models
- N:1 and 1:1 VLAN Multiplexing Models
- Multi VC, Trunk and Non Trunk UNI options
- ETTX STP Access Rings and Hub and Spoke
- WimAX nodes integrated in the ETTX Access
- DSL Access Nodes with redundant connectivity

Residential, Business, Ethernet Bitstream services

Aggregation Network Functions

Integrates Intelligent Edge for all residential and business retail and wholesale services

- ISG based dynamic subscriber and service control for residential services in retail and L3 handoff wholesale
- EVC based L2 and L3 business VPN and wholesale L2 handoff services

Provides MPLS L2 and L3 transport functions between Access and Core based on the service needs:

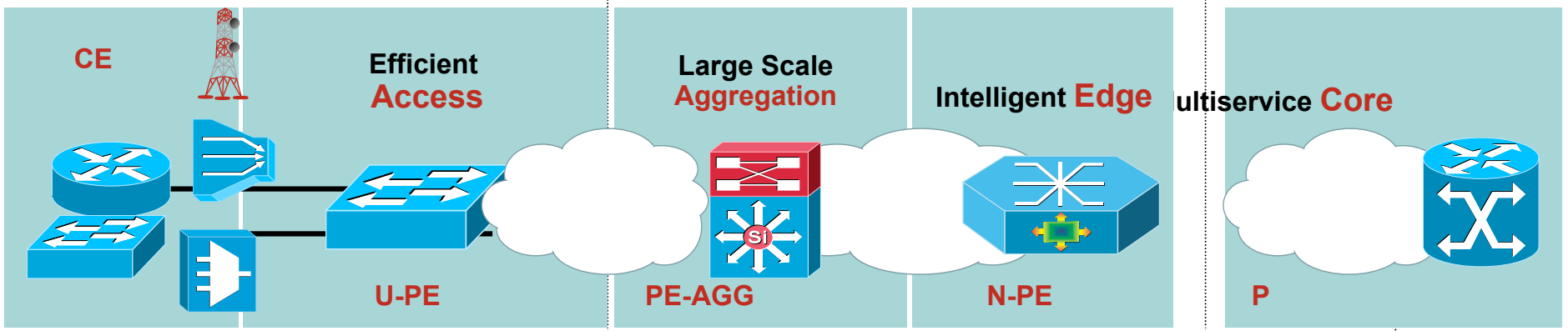
- Combines support for IP unicast/multicast, MPLS and Multicast VPNs, EoMPLS and H-VPLS
- The L2/L3 MPLS/IP transport layer provides flexibility scalability, transparency, virtualization and service awareness when required

Edge Nodes Functions

Optional L3 VPN PE

- L3 VPN Edge functions and SLA enforcement

This network layer may be already present and may be considered for CAPEX optimization reasons



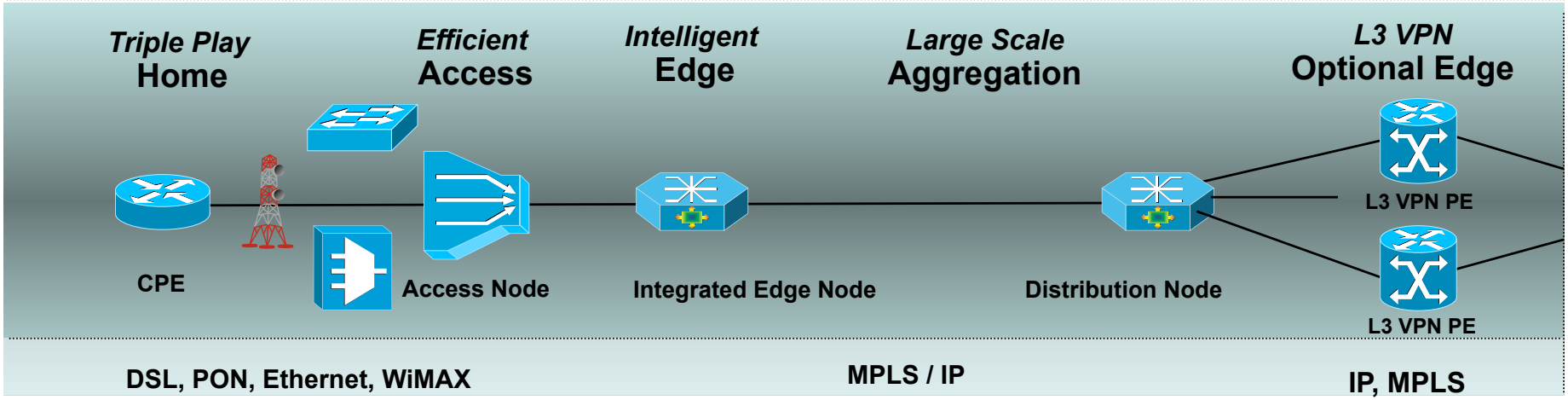
Residential CPE Functions
Carrier Ethernet System

Routed Non Trunk UNI CPE

- CPE interfaces:
  - 802.3, 802.11a/b/gn, MoCA, HPNA, Home Plug LAN interface
  - ADSL/2+, VDSL, 802.3 WAN interface with Non Trunk UNI (Single VC or Ethernet priority tagged)
- NAT/PAT forwarding function for unicast services :
  - Local DHCP server for the LAN interface
  - PPPoE or DHCP client on the WAN interface with default route
  - Triple Play Functions: SIP and RSTP ALG (NAT traversal)
- IGMP proxy routing forwarding function for multicast services:
  - IGMP fast leave
  - Individual host tracking
  - IGMP queries are encapsulated as IPoE (and PPPoE)
- QOS support on the WAN interface
  - DSCP, Home Device Classification (MAC, 802.1P COS, DSCP, Op 60) with 802.1p marking and class based scheduling

Routed Trunk UNI (Multi VC) CPE

- CPE interfaces:
  - 802.3, 802.11a/b/gn, MoCA, HPNA, Home Plug LAN interface
  - ADSL/2+, VDSL, 802.3 WAN interface with Trunk UNI (Multi VC or Ethernet 802.1q tagged)
- NAT/PAT forwarding function for unicast services on the Unicast WAN VC/VLAN:
  - Local DHCP server for the LAN interface
  - PPPoE or DHCP client on the WAN interface with default route
  - Triple Play Functions: SIP and RSTP ALG (NAT traversal)
- IGMP proxy or snooping forwarding function for multicast service on the bridged Multicast VC/VLAN WAN interface:
  - IGMP fast leave
  - Individual host tracking
- QOS support on the WAN DSL interface
  - DSCP, Home Device Classification (MAC, 802.1P COS, DSCP, Op 60) and ATM COS or 802.1P scheduling (with marking)



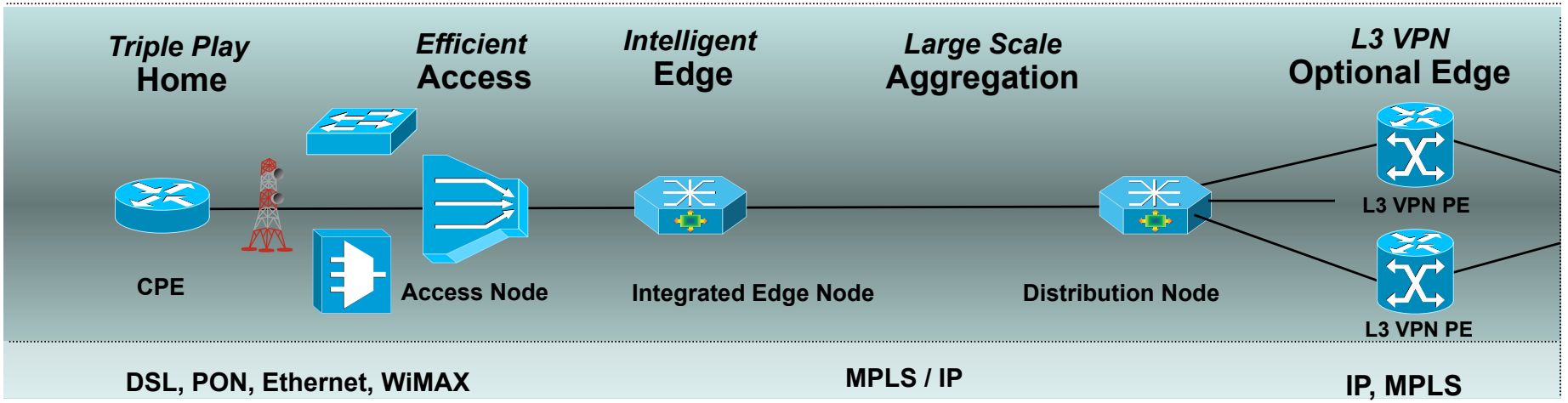
Business CPE Functions
Carrier Ethernet System

Routed CPE

- CPE interfaces:
  - LAN: 802.3, 802.11a/b/g, others
  - WAN: ADS/2+, SHDSL, 802.3 interface with Non Trunk UNI (single VC) or multiple Non Trunk UNI interfaces
- IP Routing Forwarding function:
  - IP unicast and multicast
  - IPoE encapsulations on the WAN
  - Dynamic routing RIP, OSPF, E-BGP and PIM
- QOS support on the WAN interface
  - DSCP classification and ATM COS or 802.1P scheduling, 802.1p marking

Bridged CPE

- CPE interfaces:
  - LAN: 802.3, with 802.1Q support
  - WAN: 802.3, WiMAX with 802.1Q support
- 802.1Q Bridging Forwarding function:
  - Spanning Tree Protocol (not on WiMAX)
- QOS support on the WAN DSL/Ethernet interface
  - 802.1p classification and scheduling



DSL/PON Access Node Functions
Carrier Ethernet System

Residential Services

Access Node interfaces

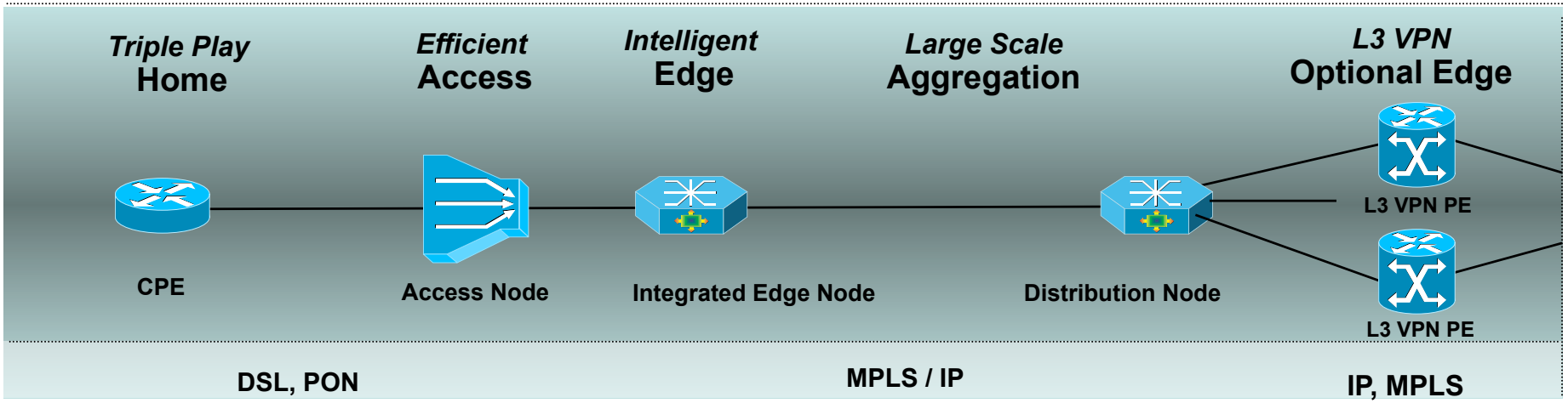
- NNI: 802.1q (uplink and subtending)
- UNI: ADSL/2+, VDSL with Non Trunk UNI (single VC or priority tagged UNI), Trunk UNI (multi VC or 802.1Q)

Access Node Functions with Residential Services support

- 1:1 and N:1 VLAN connectivity
- Subscriber isolation function in N:1 VLANs
- DHCP OP82 and PPPoE Line ID tag support
- ARP, MAC and IP spoofing prevention on Access UNI ports
- IGMP snooping, w/ proxy reporting IGMP filters, IGMP fast leave
- MAC limit on port and broadcast rate limit on upstream direction
- Active/Standby and Active/Active redundant Access Node uplinks
- ATM COS and IEEE 802.1p classification and prioritization on UNI interface, policing upstream

Business Services

- Access Node interfaces
  - NNI: 802.1q (uplink and subtending)
  - UNI: ADS/2+, VDSL, G.SHDSL with Non Trunk UNI (single VC or priority tagged UNI), Trunk UNI (multi VC or 802.1Q)
- Access Node Functions with Business services support
  - 1:1, N:1 VLAN connectivity
  - MAC limits, ACLs, BPDU filters on Access UNI ports (bridge domain)
  - MST, Active/Standby and Active/Active redundant Access Node uplinks
  - IEEE 802.1p classification, marking and prioritization on the UNI interface, policing upstream



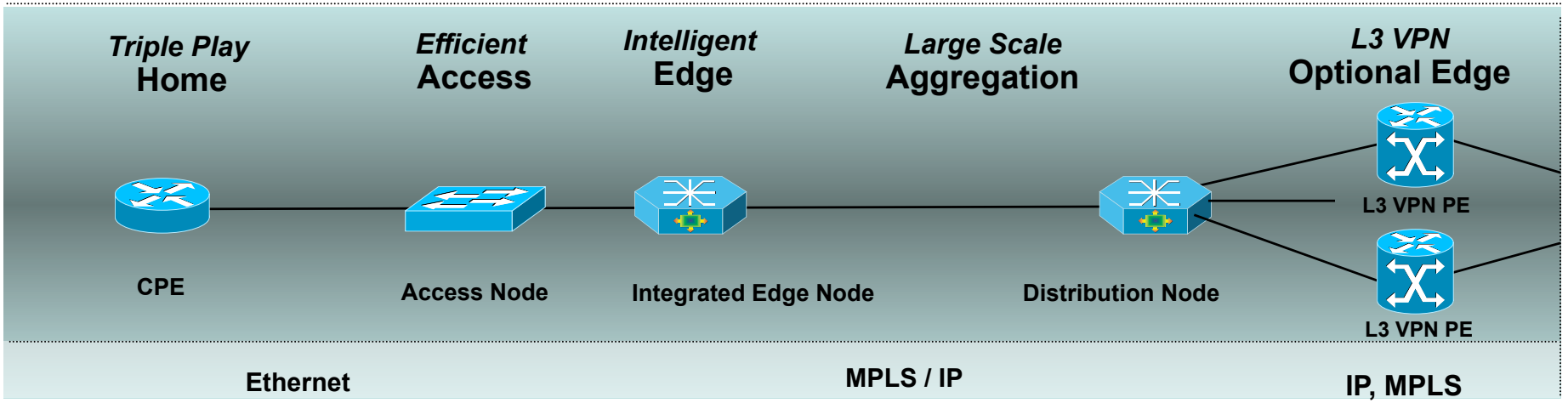
Ethernet Access Node Functions
Carrier Ethernet System

Residential Services

- Access Node interfaces
  - NNI: 802.1q (uplink and subtending)
  - UNI: Ethernet, Non Trunk UNI and Trunks UNI
- Access Node Functions with Residential Services support
  - 802.1Q bridging
  - 1:1 and N:1 VLAN connectivity
  - DHCP snooping OP82 Line Identity
  - ARP, MAC and IP spoofing prevention (DAI, IPSG)
  - Port Security (MAC limit and unicast/multicast flood limit)
  - IGMP snooping, w/ proxy reporting, IGMP filters, fast leave
  - Private VLAN (with community and isolated VLAN support) and MVR IEEE 802.1p/DSCP classification, marking and prioritization on the UNI interface, policing per service class upstream

Business Services

- Access Node interfaces
  - NNI: 802.1q (uplink and subtending)
  - UNI: Ethernet, Non Trunk UNI and Trunks UNI
- Access Node Functions with Residential and Business services support
  - 802.1Q with STP(MST) support
  - 802.1Q tunneling per port or access node
  - L2PT (Layer 2 Protocol Tunneling) and COS mutation
  - MAC limits, ACLs, BPDU filters on UNI ports and bridge domain)
  - IEEE 802.1p/DSCP classification, marking and prioritization on the UNI interface, policing upstream
  - STP security (BPDU guard, Root guard), fast convergence (RST), control plane policing



WiMAX Access Node Functions
Carrier Ethernet System

Residential Services

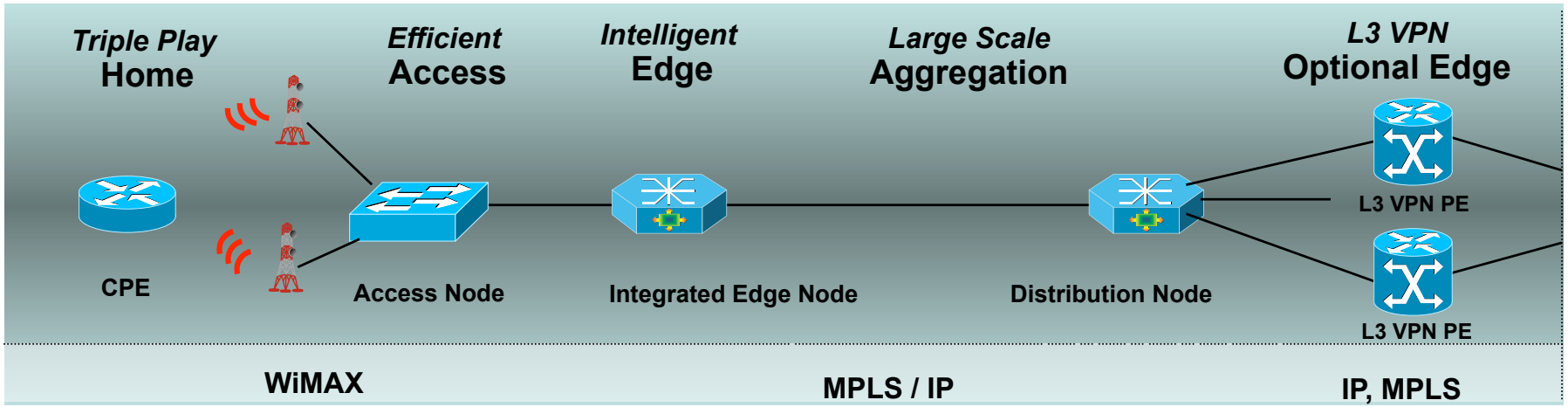
- Access Node interfaces
  - NNI: Ethernet 802.1Q transparent bridge
  - UNI: Fixed WiMAX 802.16-2004 P2P and P2MP
- Access Node Functions with Residential Services support
  - DHCP OP82 Line Identity support
  - Multipoint bridging with split horizon
  - IEEE 802.1p classification and mapping to the WiMAX service flows, which provides per subscriber endpoint per service class scheduling
- Usually there are 6xWiMAX sector controllers deployed per site that will be connected in an Ethernet Access Node that complements the functions required for residential and business services support

Note the VLAN tags are initiated by the CPE

Business Services

- Access Node interfaces
  - NNI: Ethernet 802.1Q transparent bridge
  - UNI: Fixed WiMAX 802.16-2004 P2P and P2MP
- Access Node Functions with Residential Services support
  - P2P and MP bridging with no split horizon
  - IEEE 802.1p classification and mapping to the WiMAX service flows, which provides per subscriber endpoint per service class scheduling
- Usually there are 6xWiMAX sector controllers deployed per site that will be connected in an Ethernet Access Node that complements the functions required for residential and business services support

Note the VLAN tags are initiated by the CPE



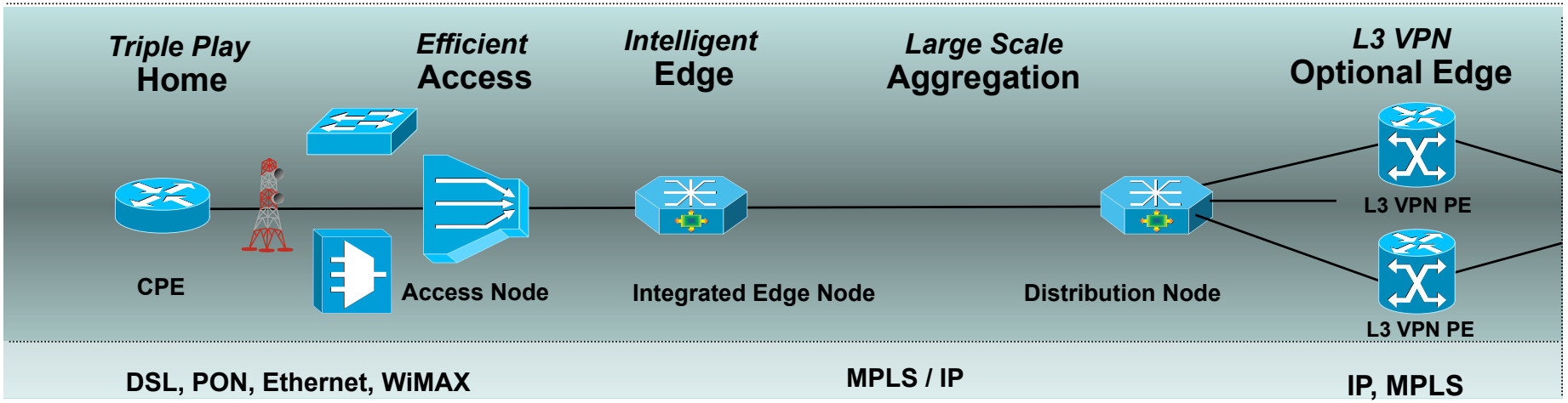
Aggregation Network Functions
Carrier Ethernet System

Integrated Edge Node

- Intelligent Service Gateway for residential and wholesale L3 services
  - IP and PPPoE sessions with AAA (RADIUS COA)
  - Dynamic policy control (RADIUS COA) for: access policies (QOS, ACLs), session control policies (session/idle timeouts) network forwarding policies (MPLS VPN mapping)
  - IP and MPLS (multicast) VPN ISG session forwarding
- Flexible Ethernet UNI for business and wholesale L2 services
  - Classification: port, 1Q, range 1Q, QinQ, untagged traffic
  - Translation and Rewrites: push and pop tags
  - H-QOS (parent shaper child queuing)
- Carrier Ethernet Transport functions (also concurrent):
  - EoMPLS Pseudowire and VPLS VFI x-connect
  - Bridge domains with split horizon, IGMP snooping
  - IP unicast and multicast routing with Multicast CAC and RSVP receiver proxy; MPLS(IP over MPLS and IP multicast over EoMPLS PW) and Multicast VPN support

Distribution Node

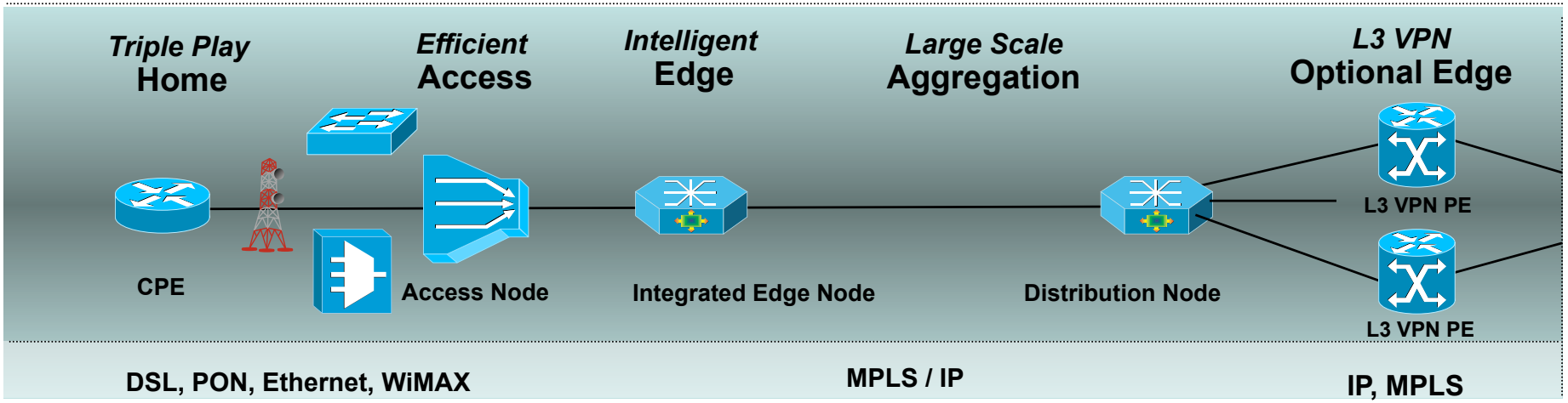
- May include Integrated Edge Node function
- Flexible Ethernet UNI functions (L3VPN PE interface):
  - Classification: QinQ
  - Translation and Rewrites: push and pop tags
- Carrier Ethernet Forwarding functions (also concurrent):
  - H-VPLS
  - EoMPLS Pseudowire switch function
  - IP unicast and multicast routing; MPLS (IP over MPLS and IP multicast over EoMPLS PWs) and MPLS/Multicast VPN
  - MPLS NNI function between Aggregation Network and Core



L3 VPN PE Functions
Carrier Ethernet System

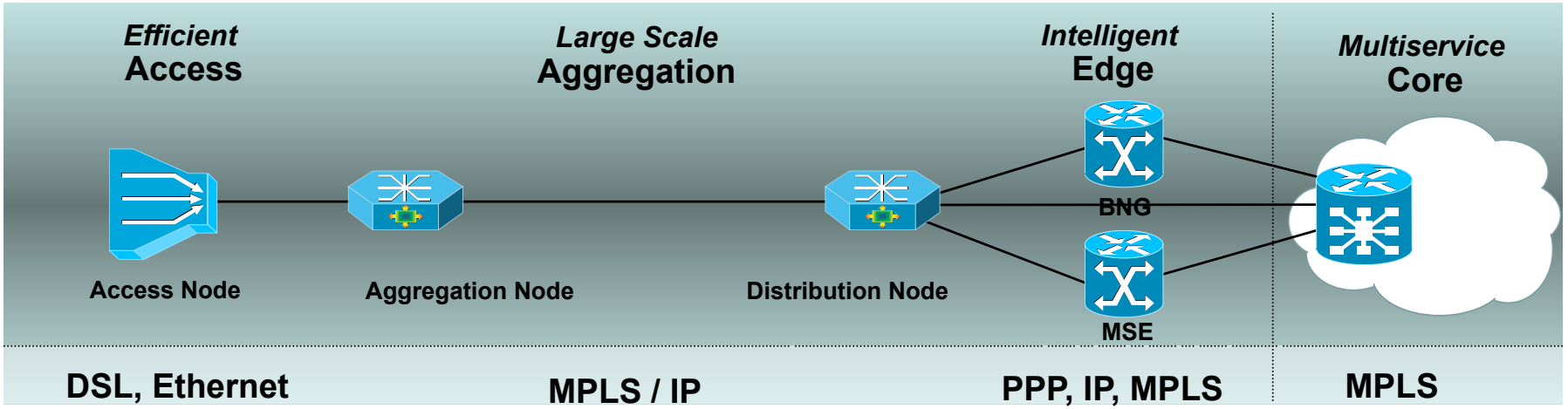
L3 VPN PE

- 802.1Q and QinQ Access Interfaces
- Business Service MPLS PE function:
  - MPLS (multicast) VPN
  - VPLS support for E-LAN services
  - EoMPLS pseudowire support for E-Line services
- Advanced network access control on the access interfaces:
  - ACLs
  - MAC Limits
  - BPDU filters and L2TP
  - Ingress and Egress H-QOS

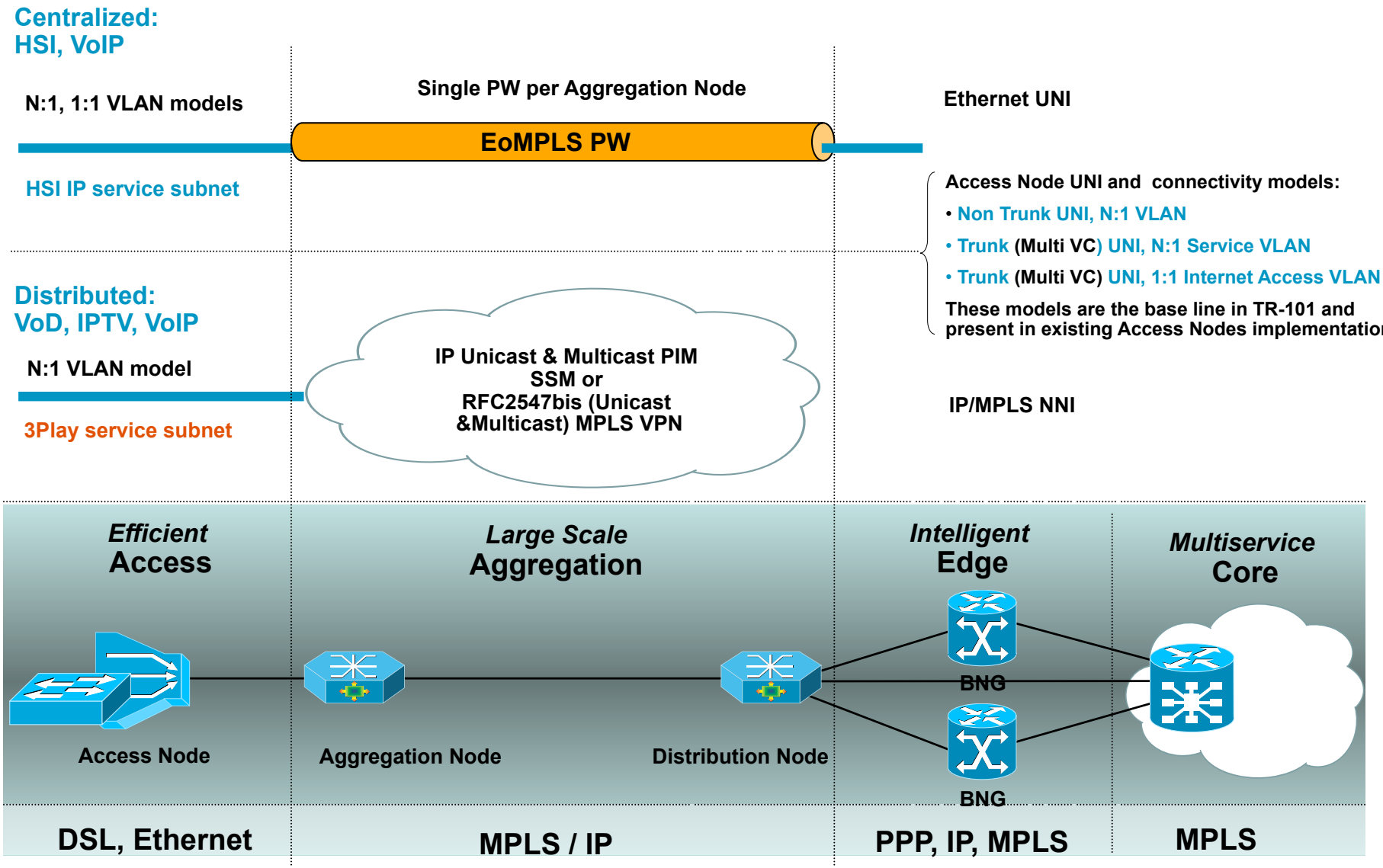


Service Delivery Models

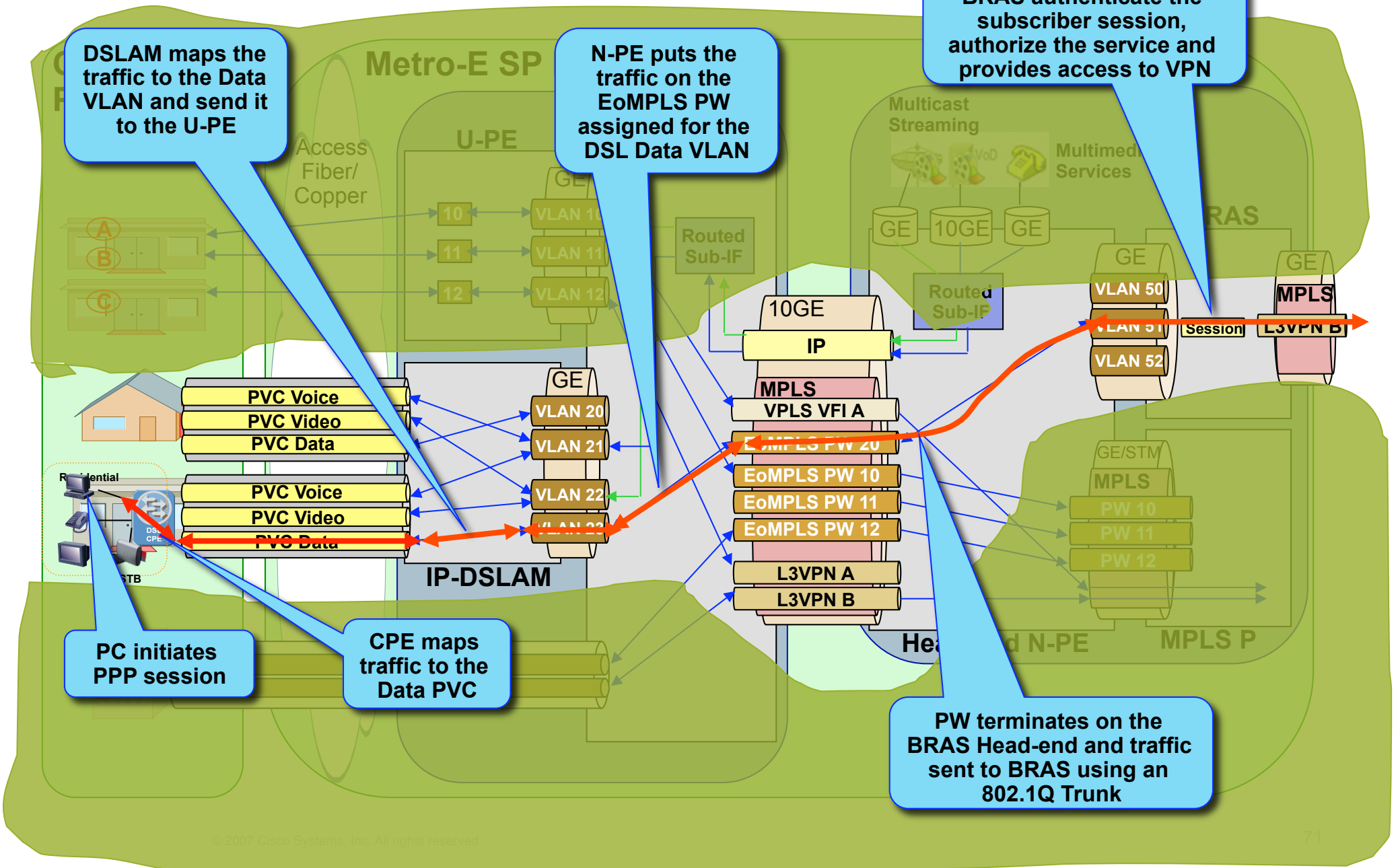
- Service Aggregation Models
  - Residential, Business, Wholesale
- Access Node and CPE UNI Models
  - ETTH Access Rings and xDSL Access
- IP and Ethernet Services Edge Models



Retail Residential Services Architecture

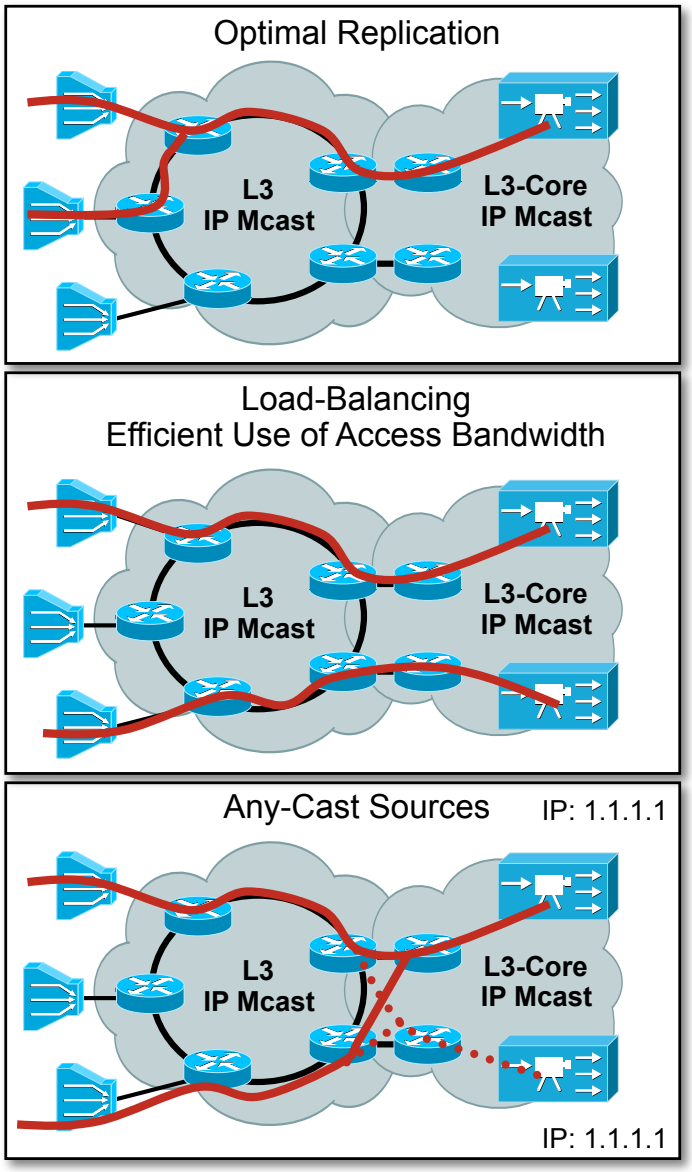


Residential HSI Service on DSL on PPPoE



IP for Video and IP/TV Service Delivery Key Characteristics and Benefits

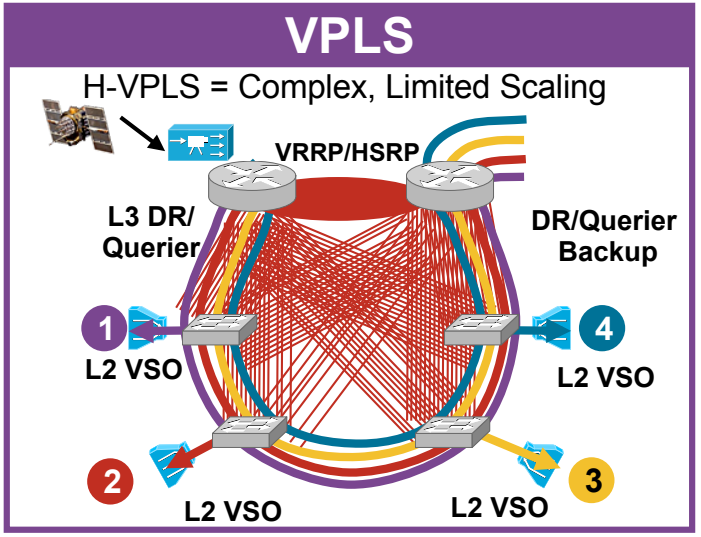
- Simplified Operations
  - IGMP/PIM only required, no snooping necessary in Aggregation network; snooping contained in DSLAM
  - Single point of L3 termination for IP/TV (no VRRP required)
- Optimal and Scalable Forwarding
  - SSM multicast distribution model for optimal tree creation under all conditions
  - Dynamic load balancing on equal cost paths(!!)
  - Optimized ARP and IGMP tables through distribution
  - Flexible content injection, including localized content
  - Scales in terms of network nodes and subscribers in any topology due to distributed L3
  - Allows for on-path CAC
- Resiliency
  - Consistent convergence in all failure cases: Source-, Node-, Link-Failure.
  - Anycast-Source model for enhanced redundancy
  - SSM security and address-space efficiency proven architecture in many 3Play production networks today
- Future Ready
  - Possibility to add/distribute video monitoring and error concealment techniques easily

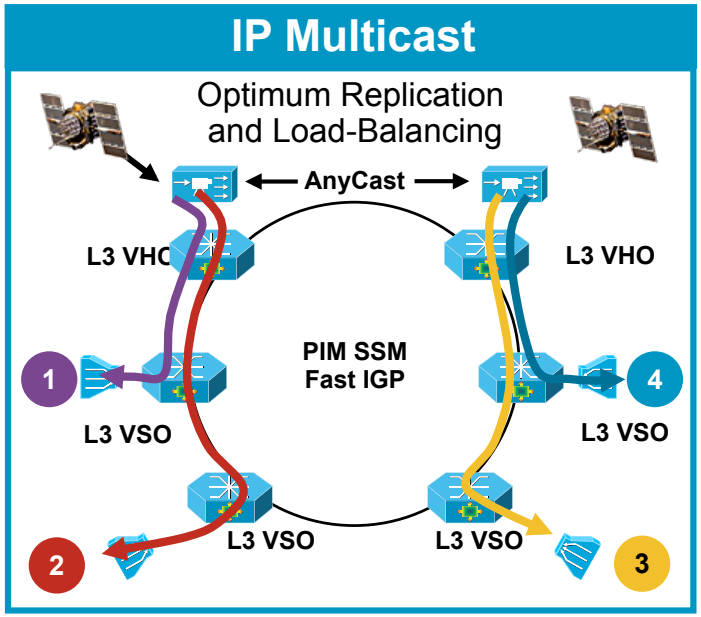


H-VPLS for Video and IP/TV

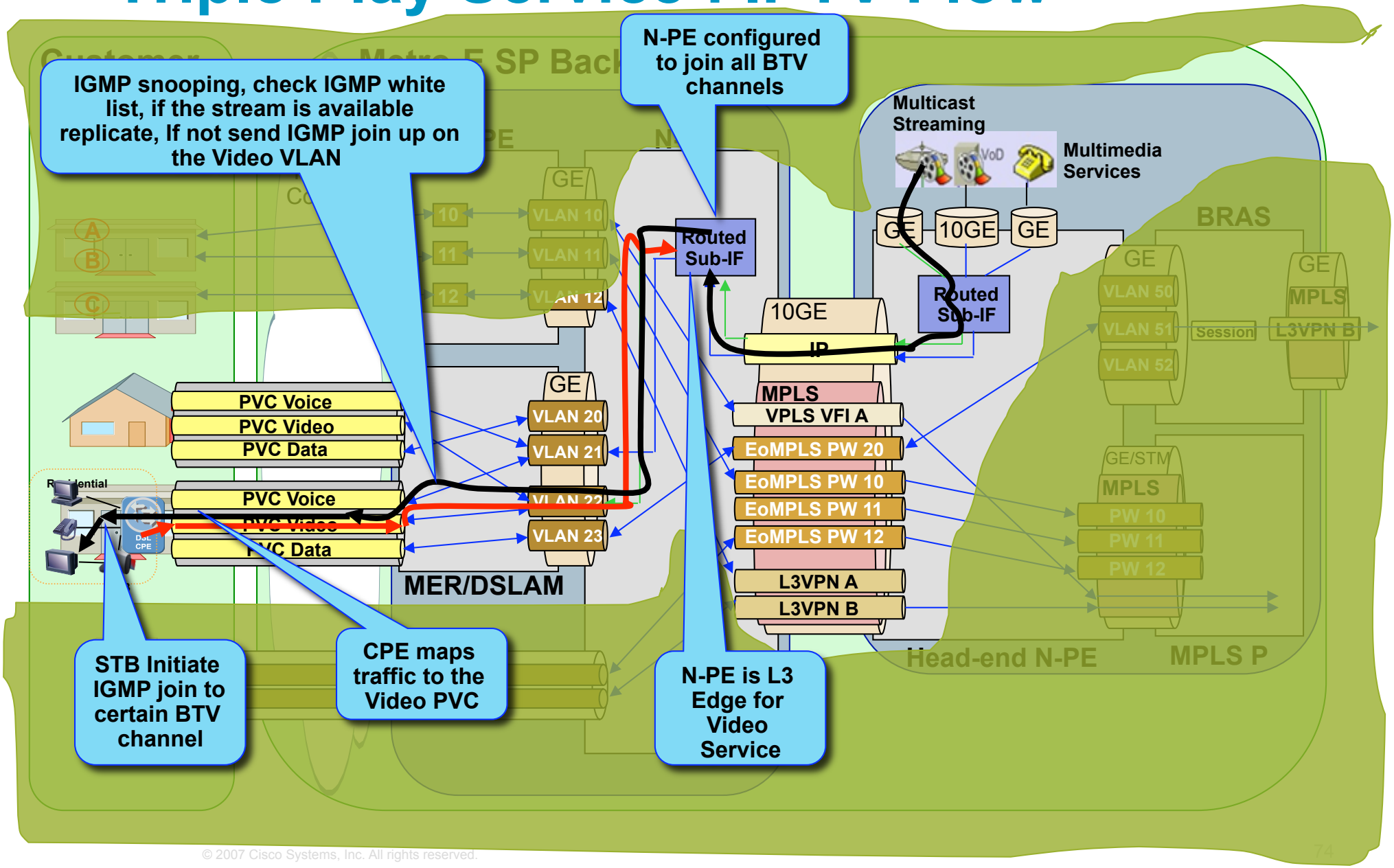
Key Characteristics and Issues

- Complex Operations
  - Complex H-VPLS mesh
  - Troubleshooting challenges due to complexity of L3/L2/VPLS/ PWE3 multi-layer solution
  - **Different** unicast versus multicast topologies!
  - IGMP snooping across all Aggregation network
  - VRRP for redundancy
- Sub-Optimal Forwarding
  - Static distribution tree with sub-optimal forwarding in link failure conditions
  - Per link load-balancing with 802.3ad
  - Scale issues with centralized ARP and IGMP tables
  - Restricted scalability in terms of network nodes and subscribers
  - No on-path CAC possible
- Resiliency
  - No source redundancy
  - H-VPLS L2 ring approach requires L3 GW to recover from node failures, while all users are affected)
  - Higher security risk due to large L2 domain with snooping-based forwarding

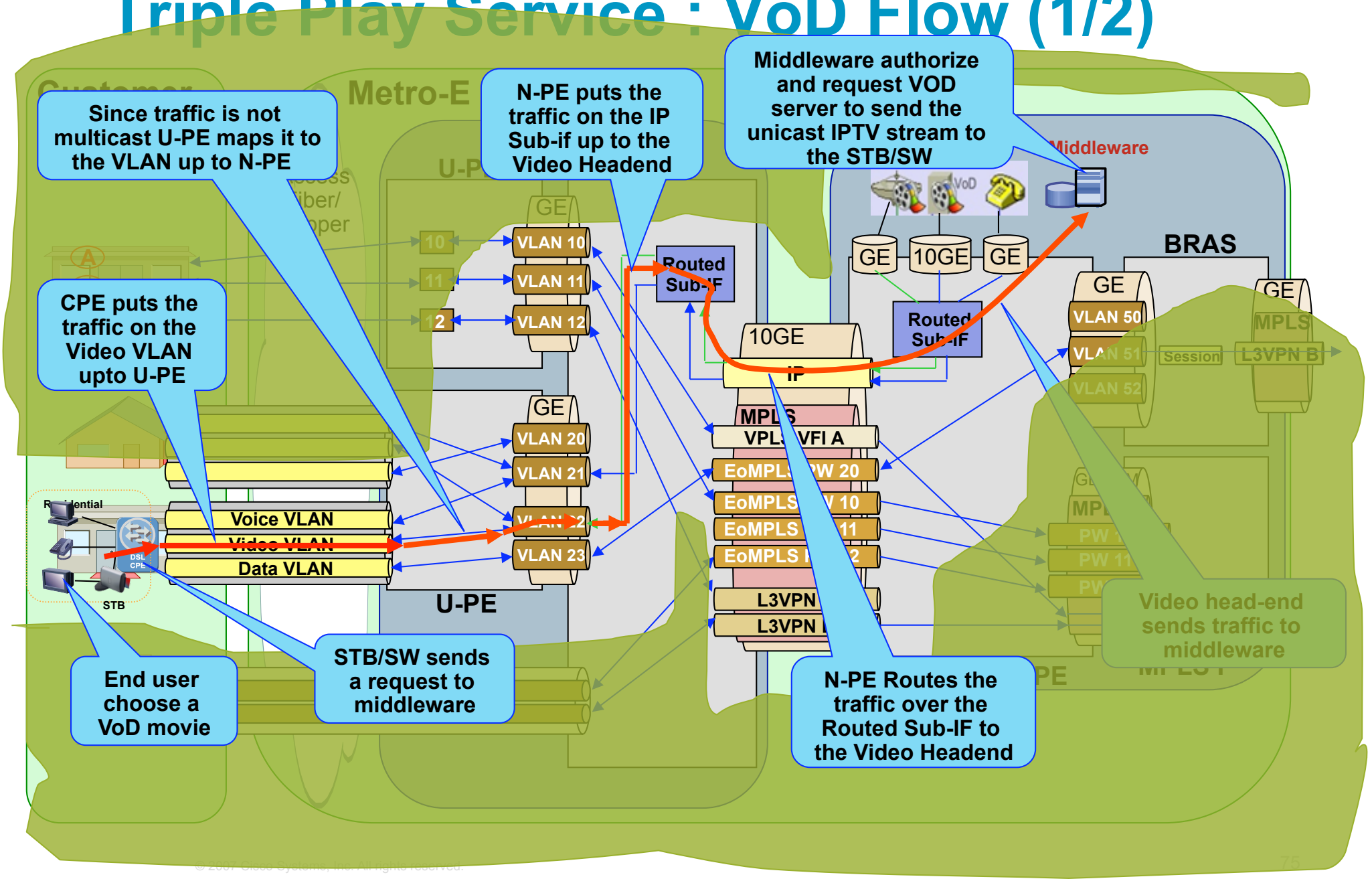




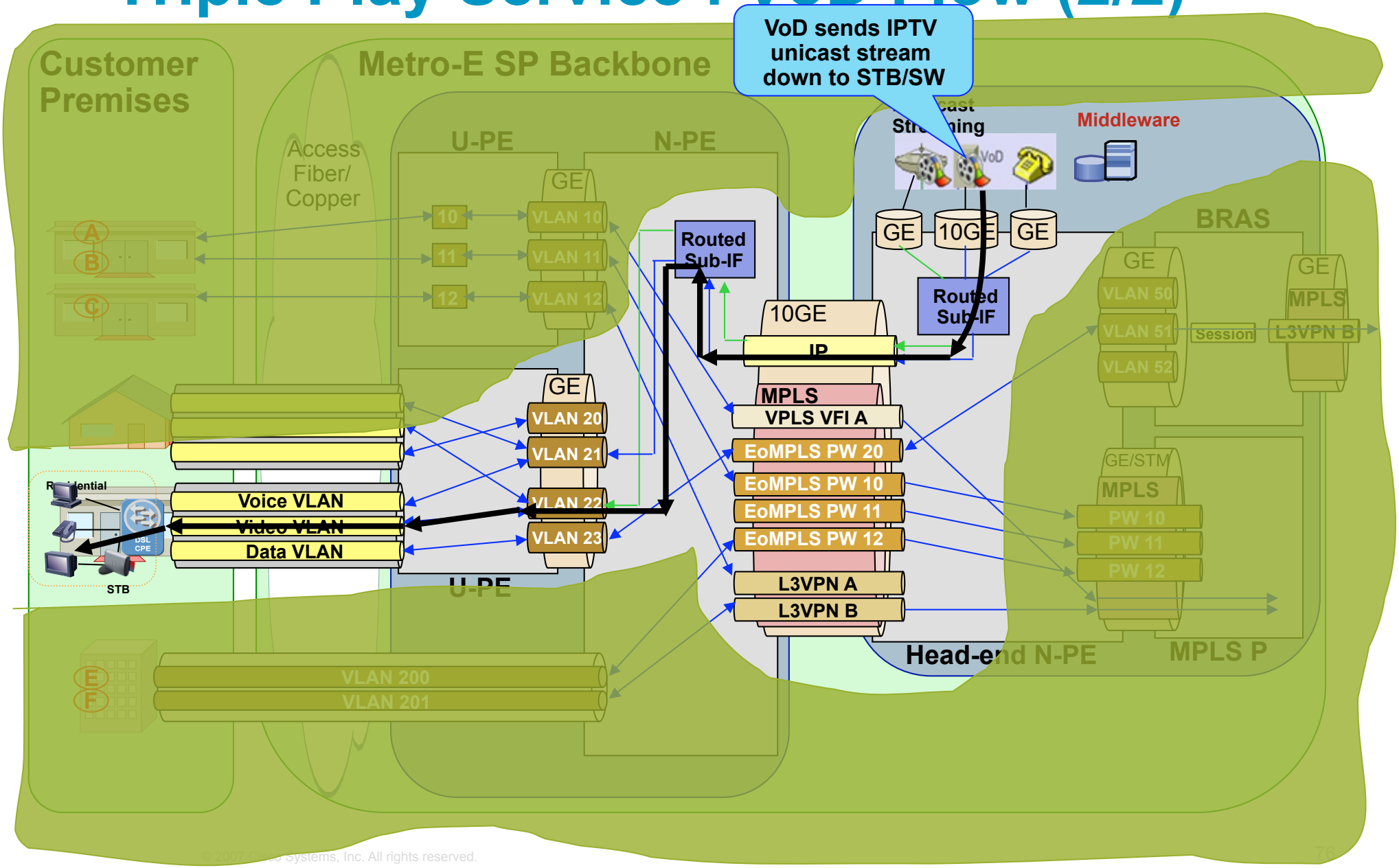
Triple Play Service : IPTV Flow



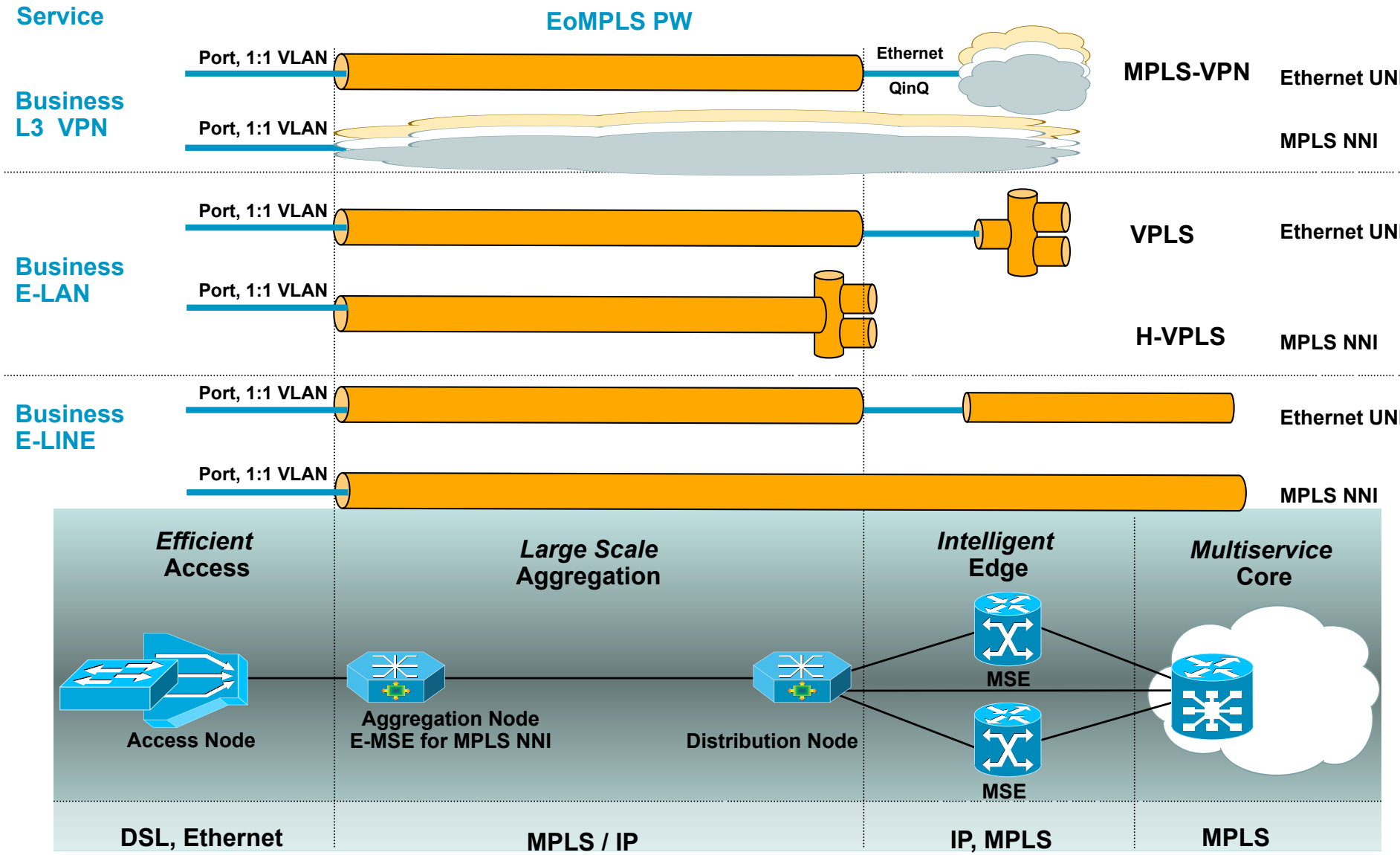
Triple Play Service : VoD Flow (1/2)



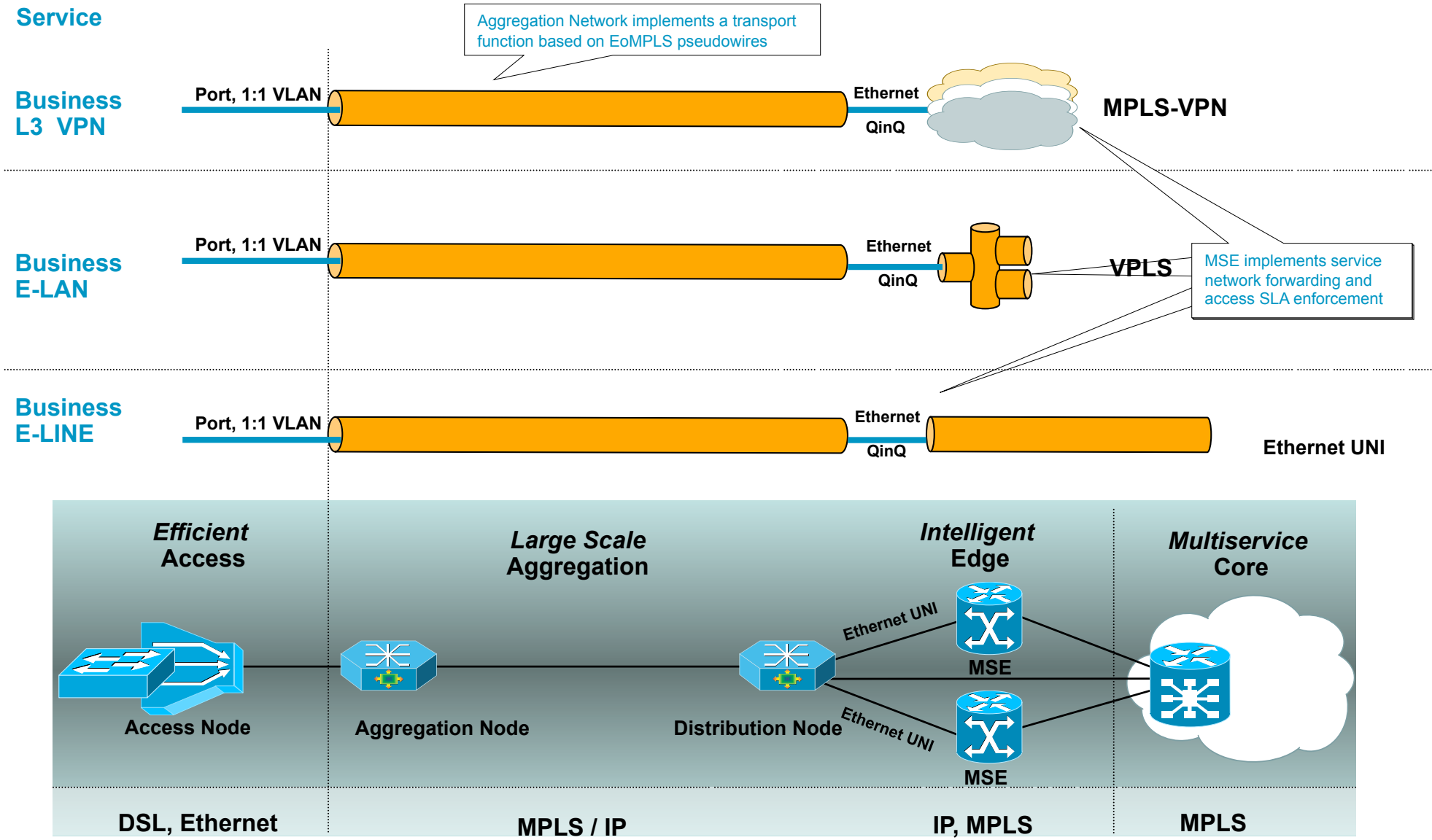
Triple Play Service : VoD Flow (2/2)



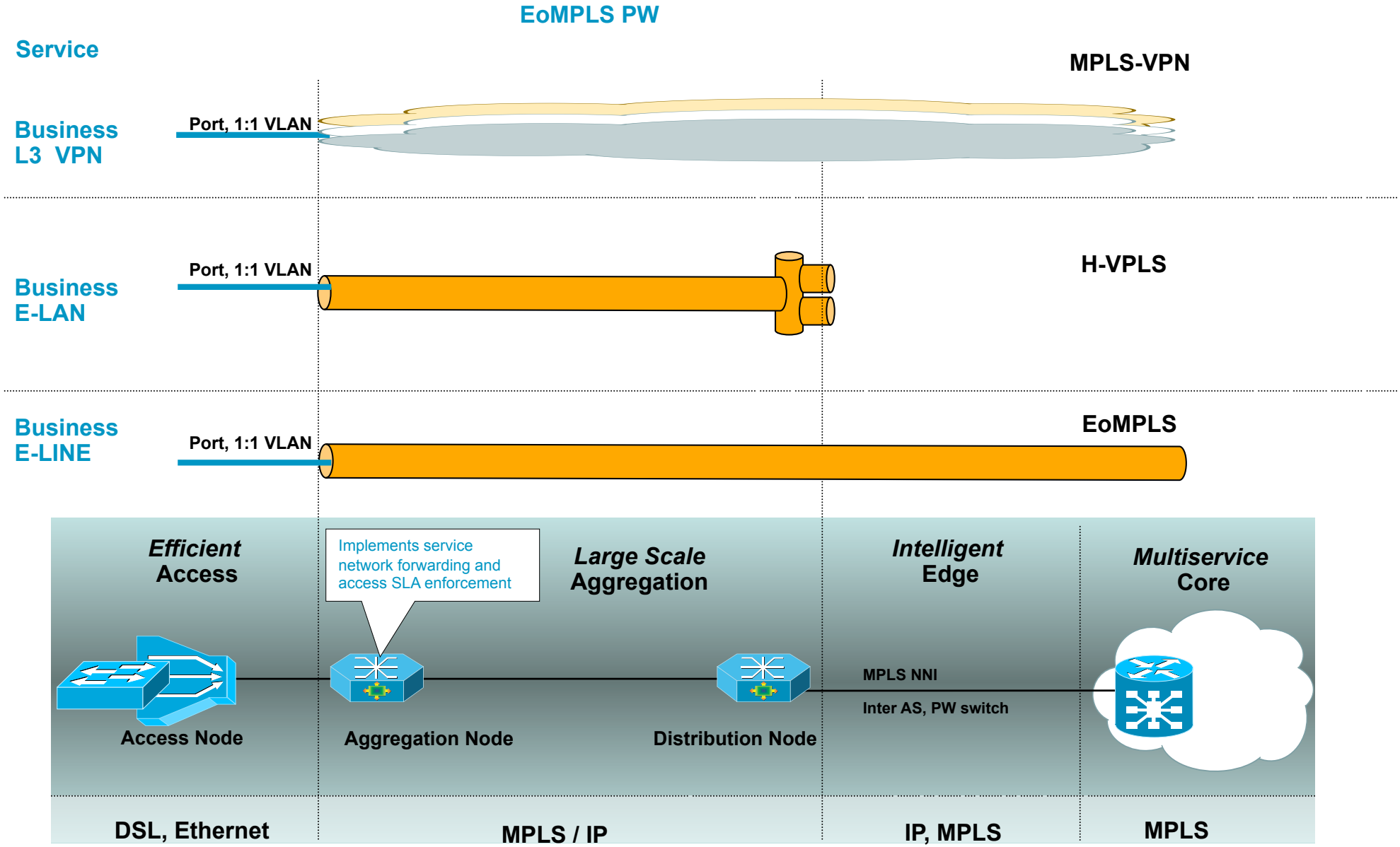
Business Ethernet Services Architecture



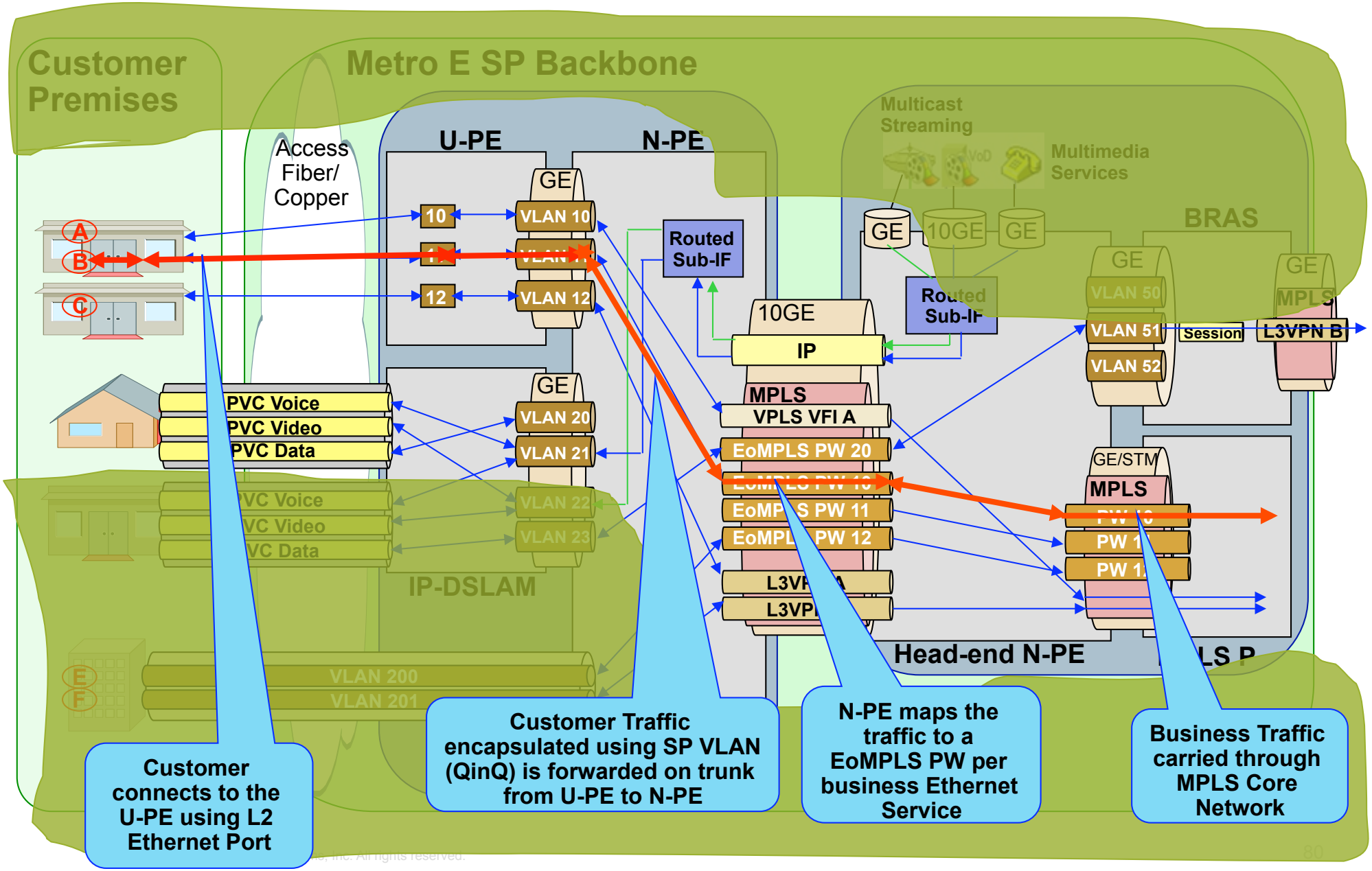
MSE Service Edge
Business Ethernet Services Architecture



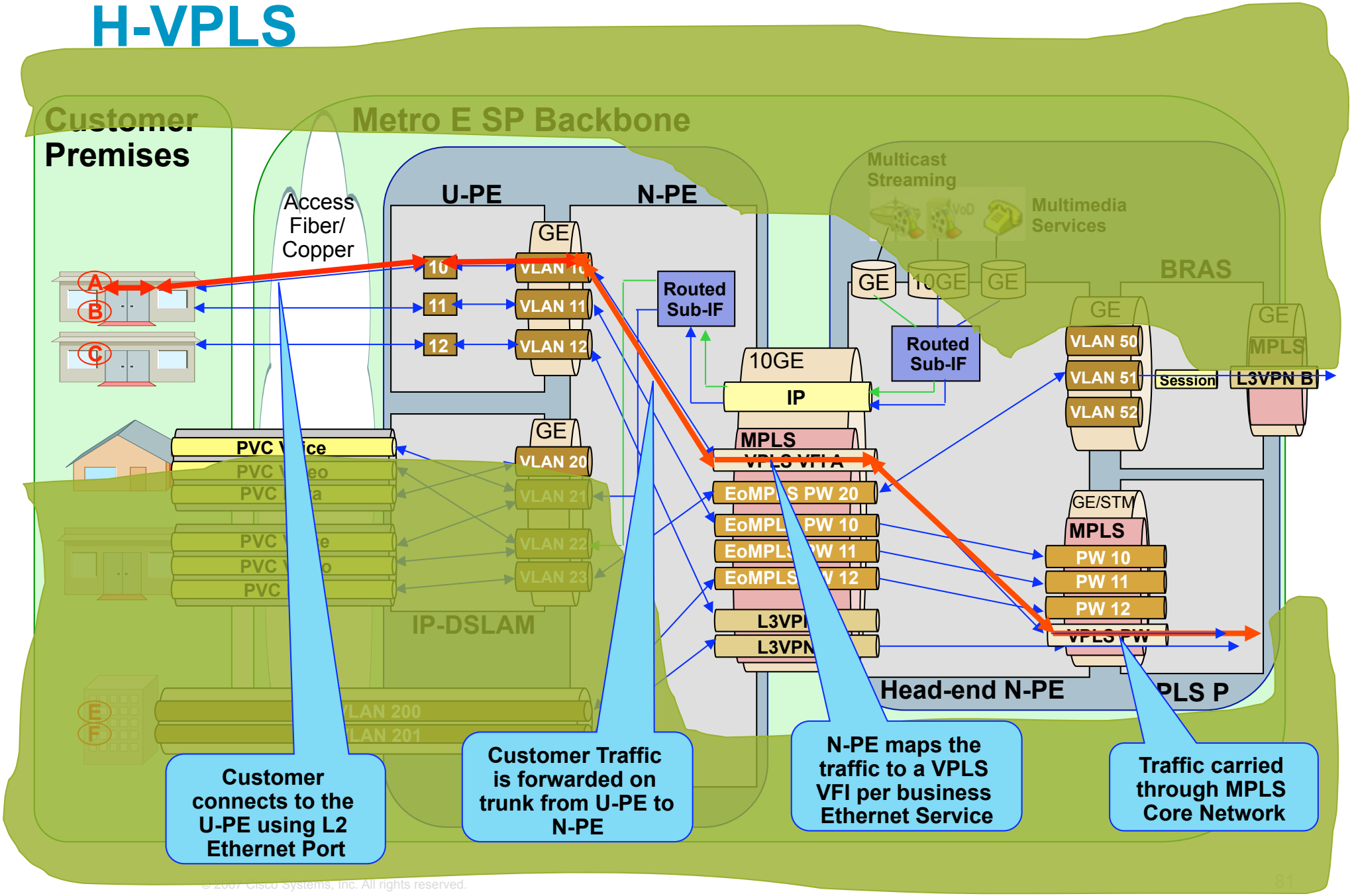
Aggregation Network Service Edge
Business Ethernet Services Architecture



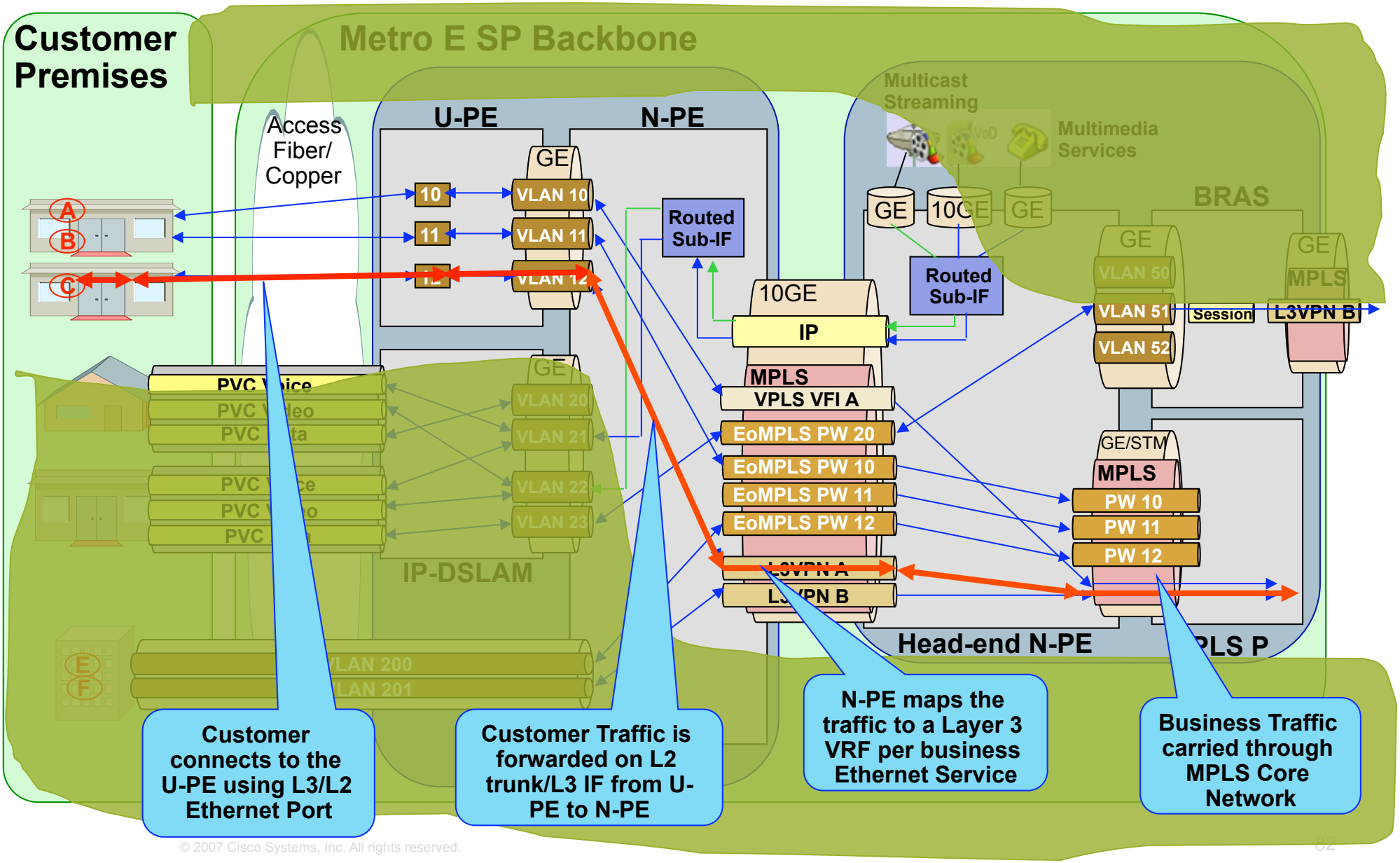
L2VPN P2P Business Services – EPL/EVPL



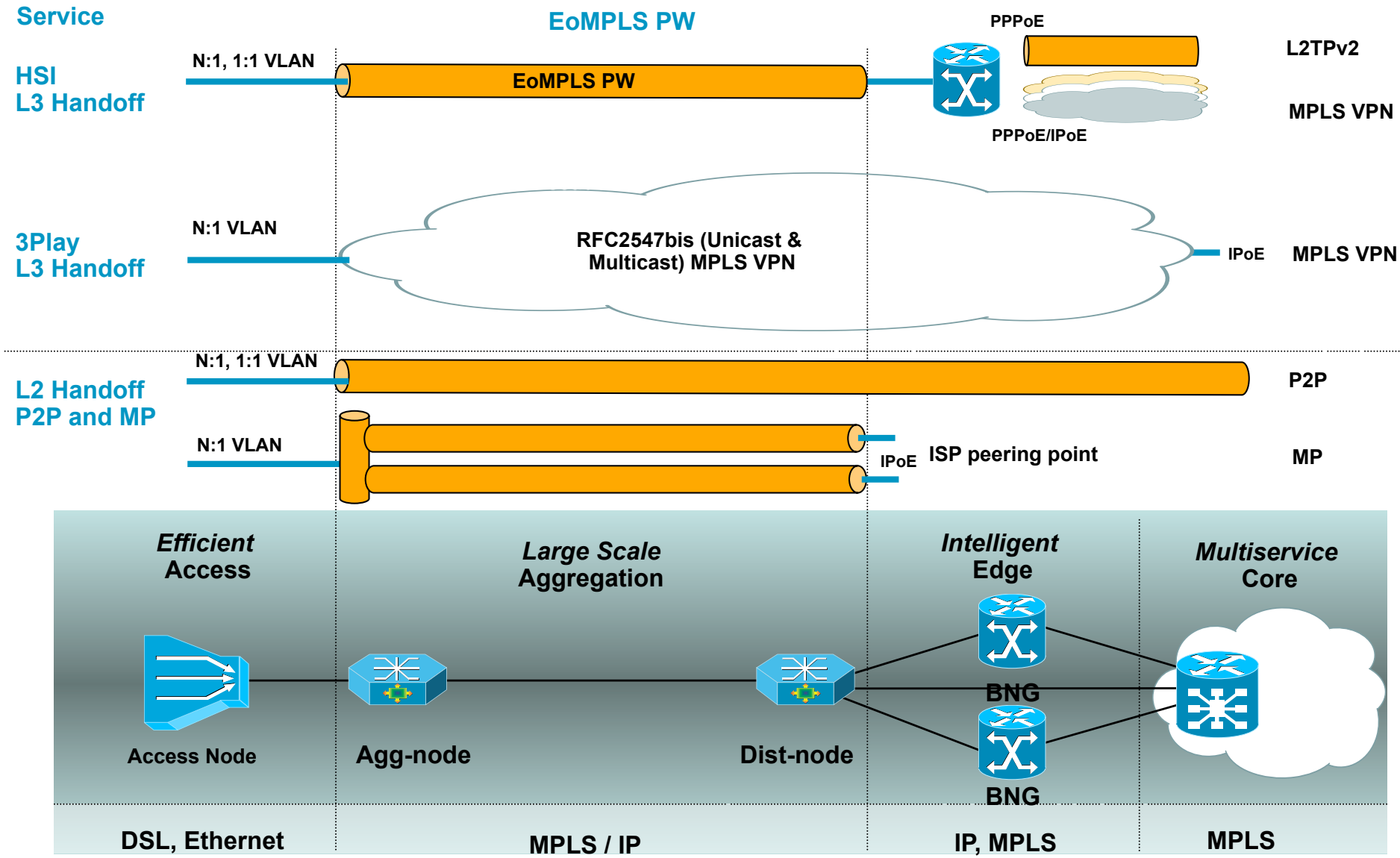
L2VPN Multipoint Business Services : H-VPLS



L3VPN Multipoint Business Services



Wholesale Services Architecture



Summary

- You have an understanding of Metro Ethernet technology and its services now.
- You have the fundamental understanding of how different services work in a Metro-E network.
- You have the basic knowledge of different control & data plane technology options for building a Metro-E network.

Questions ?

Time for a Quick Break!

Ethernet OAM

Agenda

- Review - OAM In General
- Ethernet OAM Protocol Overview
  - IEEE 802.1ag – CFM
  - ITU Y.1731
  - IEEE 802.3ah (clause 57) – Link OAM (EFM)
  - MEF E-LMI
- Ethernet OAM Fault Management
- Fault Management Scenarios
- Summary

Review: OAM in General

OAM Basics

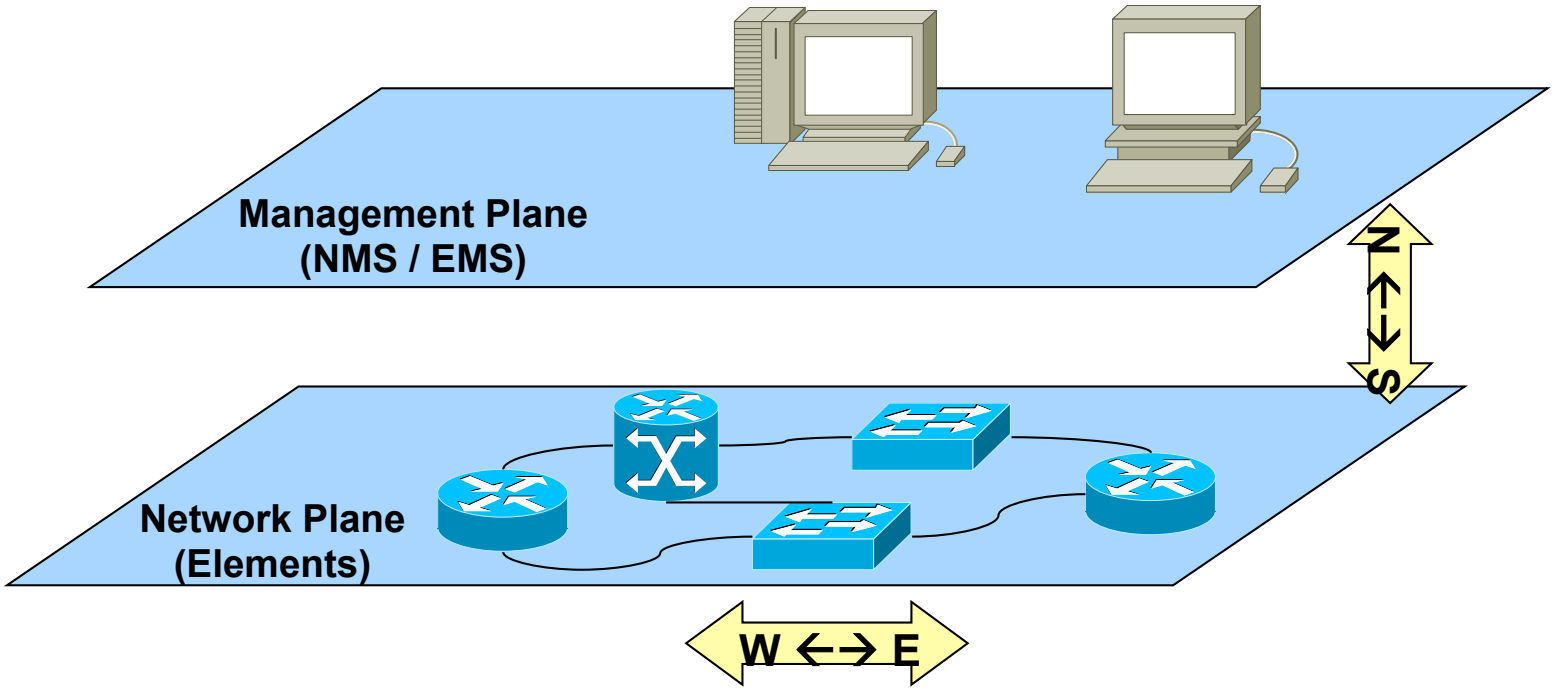
- **F** – Fault Management
- **C** – Configuration Management
- **A** – Accounting
- **P** – Performance Management
- **S** – Security Management

OAM Protocols and Mechanisms helps operator to achieve some of the FCAPS functionality.

OAM capability is one of the key differentiator to make a network “Carrier Class”.

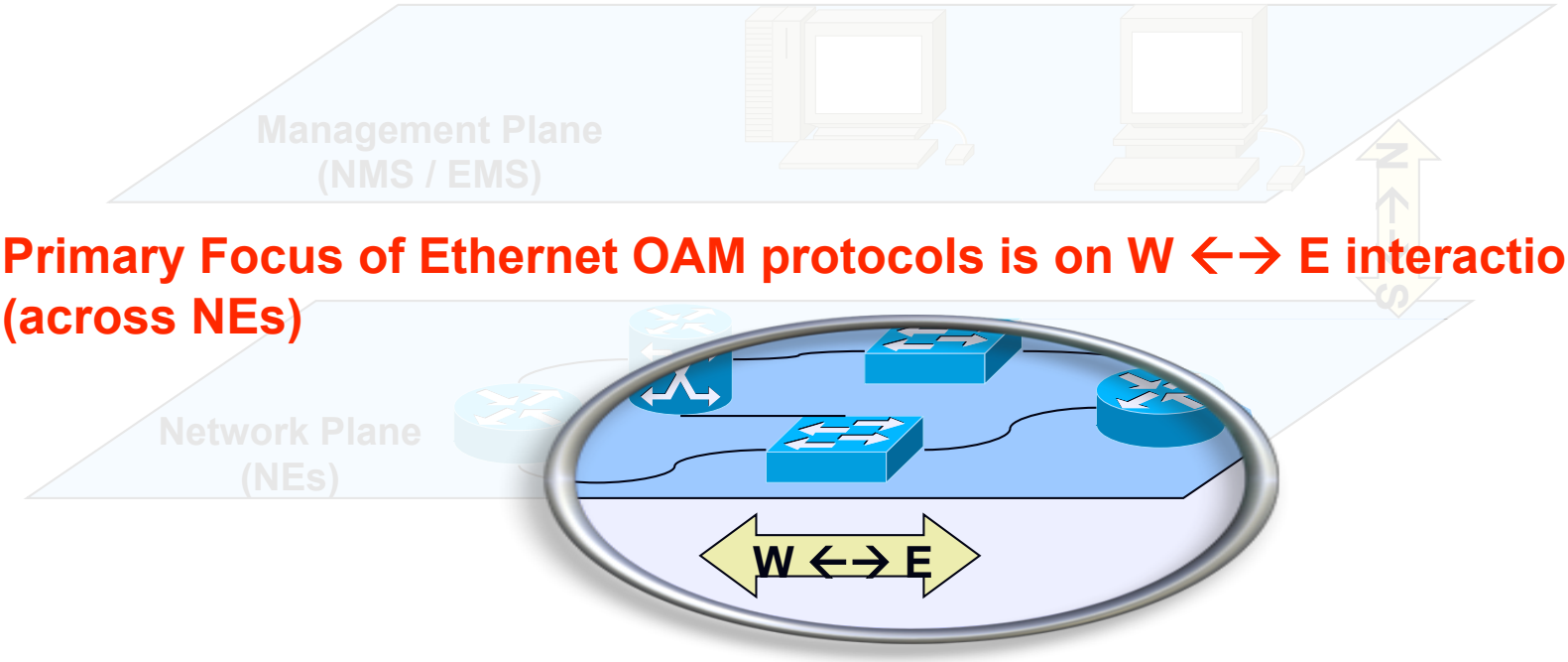
OAM &P: The Concept

- Operations, Administration, Maintenance & Provisioning:
  - fault indication
  - performance monitoring
  - security management
  - diagnostic functions
  - configuration & service provisioning
- OAM covers both N←→ S and W←→E interfaces



OAM &P: The Concept

- Operations, Administration, Maintenance & Provisioning:
  - fault indication
  - performance monitoring
  - security management
  - diagnostic functions
  - configuration & service provisioning
- OAM covers both N←→ S and W←→E interfaces



Primary Focus of Ethernet OAM protocols is on W ←→ E interactions (across NEs)

Ethernet OAM Protocol Overview

Drivers for Ethernet OAM

- OAM benchmarks

  Set by TDM and existing legacy WAN technologies

- Increase Operational Efficiency

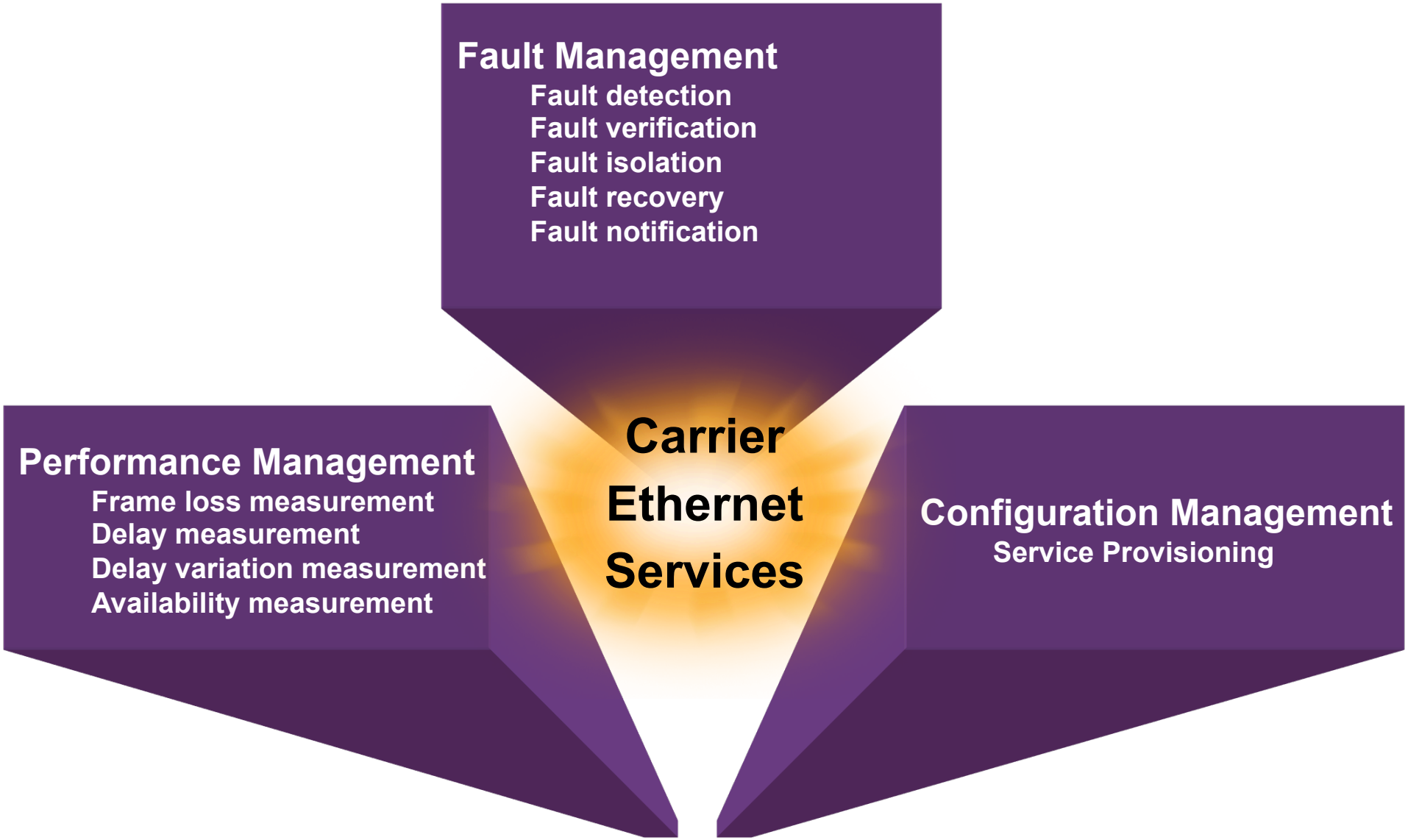
  Reduce OPEX, downtime & cost

- Simplify Management Complexity

  Large Span Networks

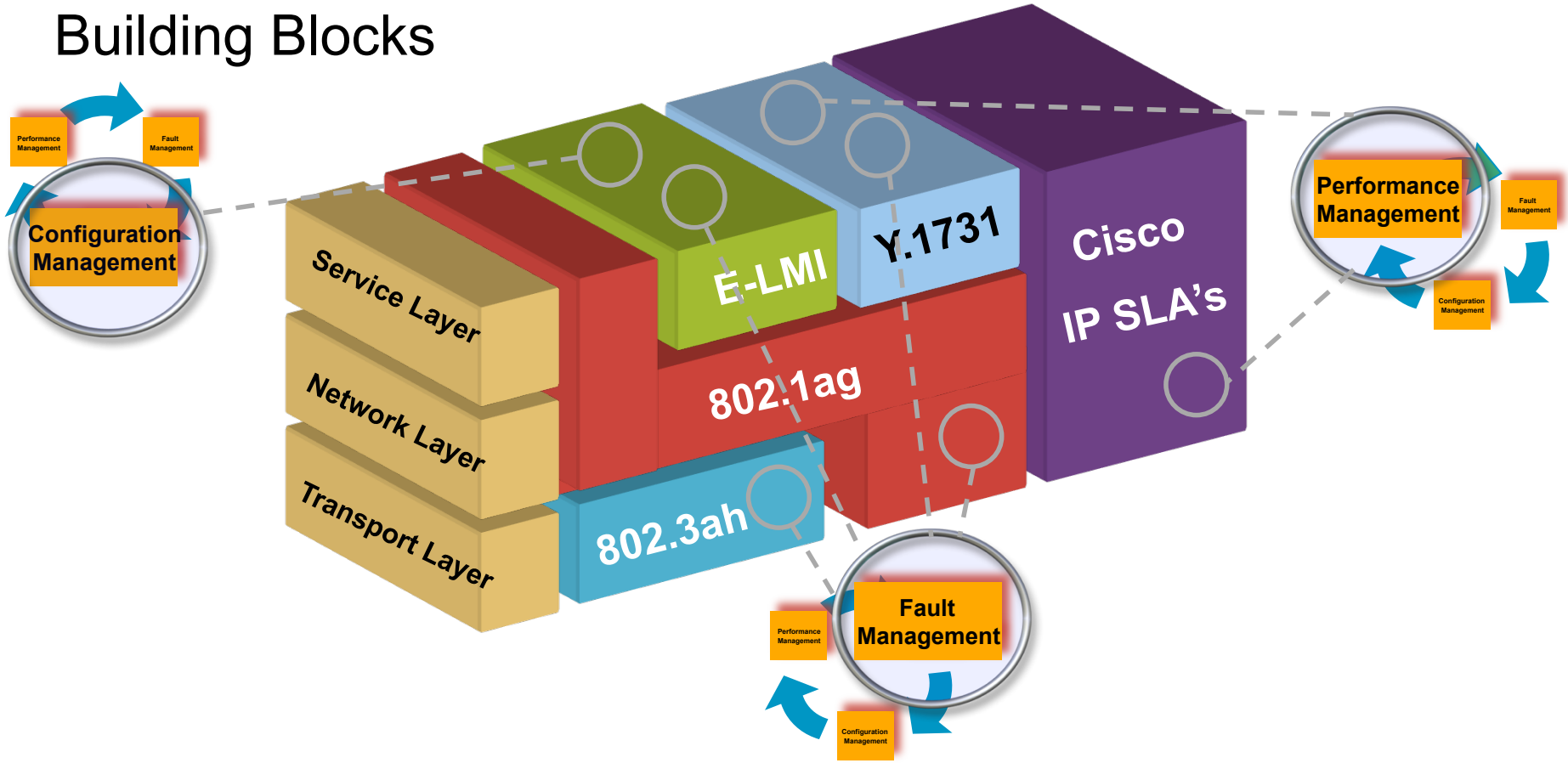
  Multiple constituent networks belong to disparate organizations/ companies

Problem Taxonomy
FCAPS Buckets that Ethernet OAM will Address



Ethernet OAM

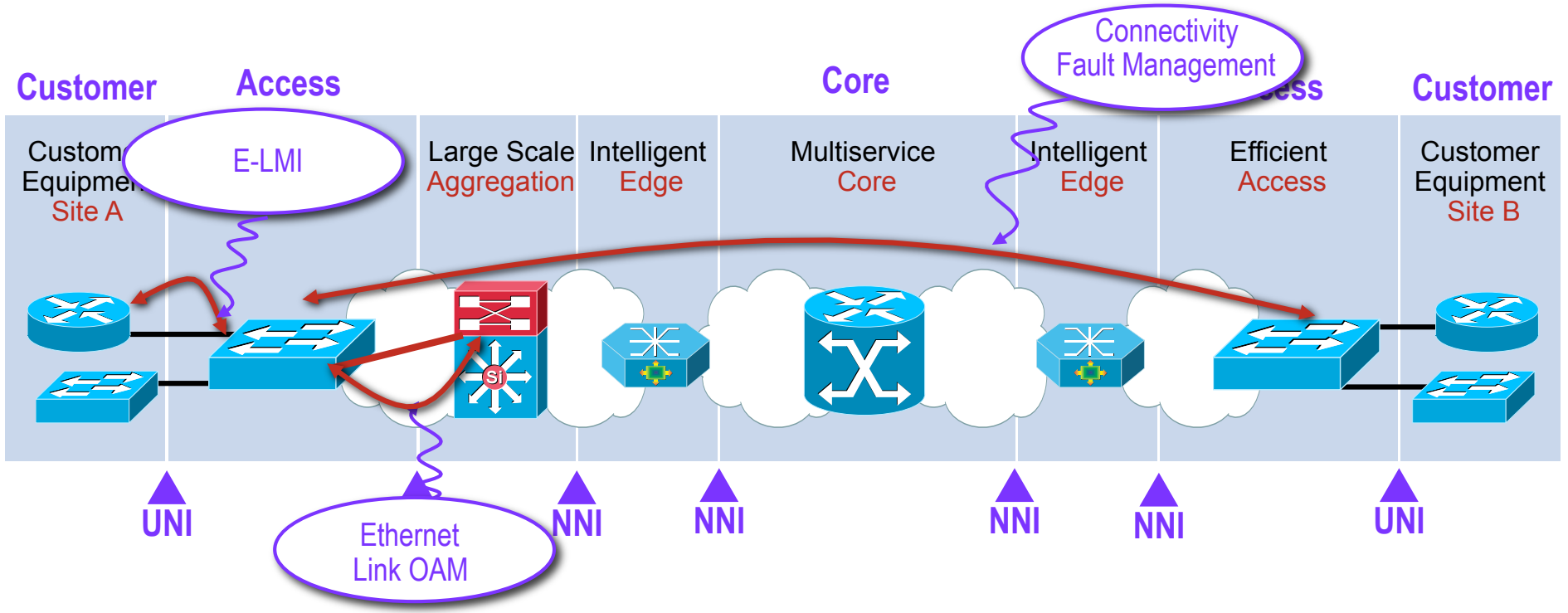
Building Blocks



- IEEE 802.1ag: Connectivity Fault Management (CFM)
- IEEE 802.3ah: Ethernet Link OAM (EFM OAM)
- ITU-T Y.1731: OAM functions and mechanisms for Ethernet based networks
- MEF E-LMI: Ethernet Local Management Interface
- Cisco IP SLA's: Performance Management using CFM and Y.1731 mechanisms

Ethernet OAM

Protocol Positioning



- E-LMI: User to Network Interface (UNI)
- Link OAM: Any point-point 802.3 link
- CFM: End-to-End Ethernet virtual connection

IEEE 802.1ag Connectivity Fault Management (CFM)

Connectivity Fault Management (CFM)

Overview

- Family of protocols that provides capabilities to detect, verify, isolate and report ethernet connectivity faults
- Employs regular Ethernet frames that travel in-band with the customer traffic

  Devices that cannot interpret CFM Messages forward them as normal data frames

- Under standardization by IEEE (P802.1ag)

  Now at Sponsor Ballot stage (expected ratification 2HCY07)

As of 09/26/07, CFM is now standard (IEEE std. 802.1ag-2007)
Draft 8.1 was the final draft

CFM Overview (Cont.)

- Key CFM mechanisms include:

  Nested **Maintenance Domains** (MDs) that break up the responsibilities for network administration of a given end-to-end service

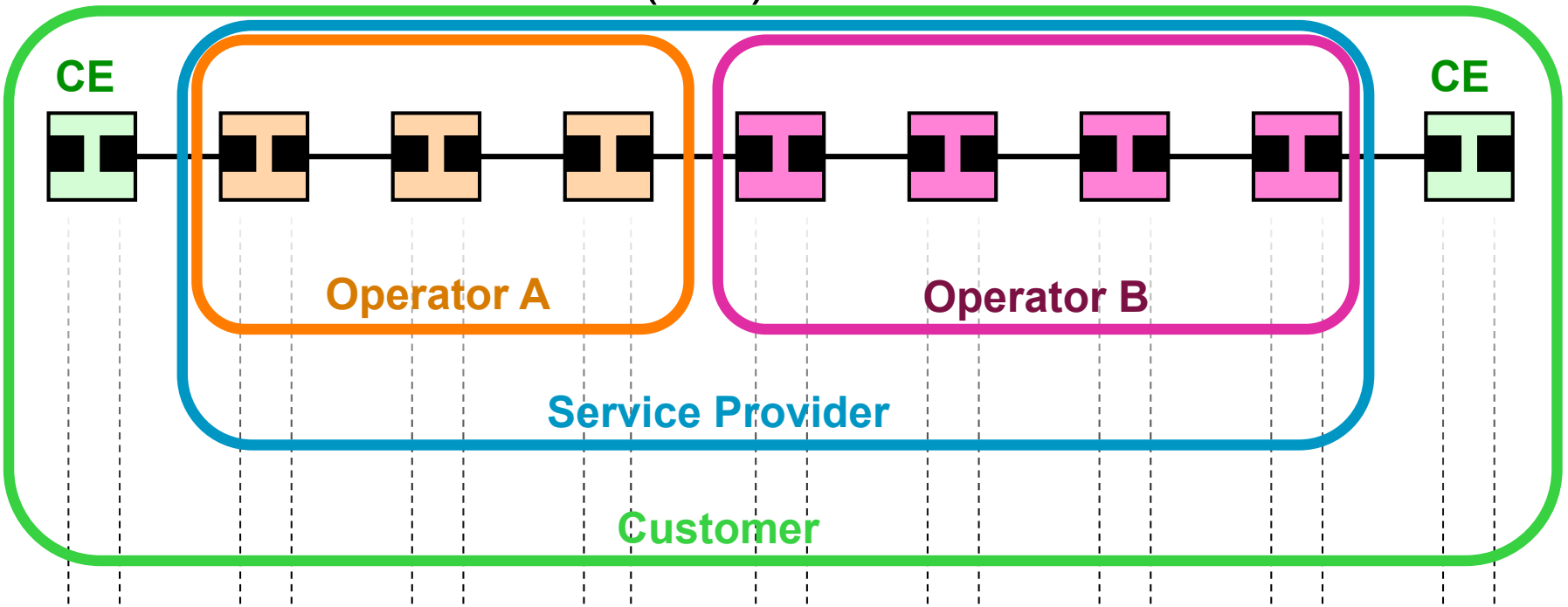
  Maintenance Associations (MAs) that monitor service instances under a given MD

  Maintenance Points (MPs) that generate and respond to CFM PDUs

  Protocols (Continuity Check, Loopback and Linktrace) used for Fault Management activities

CFM Concepts

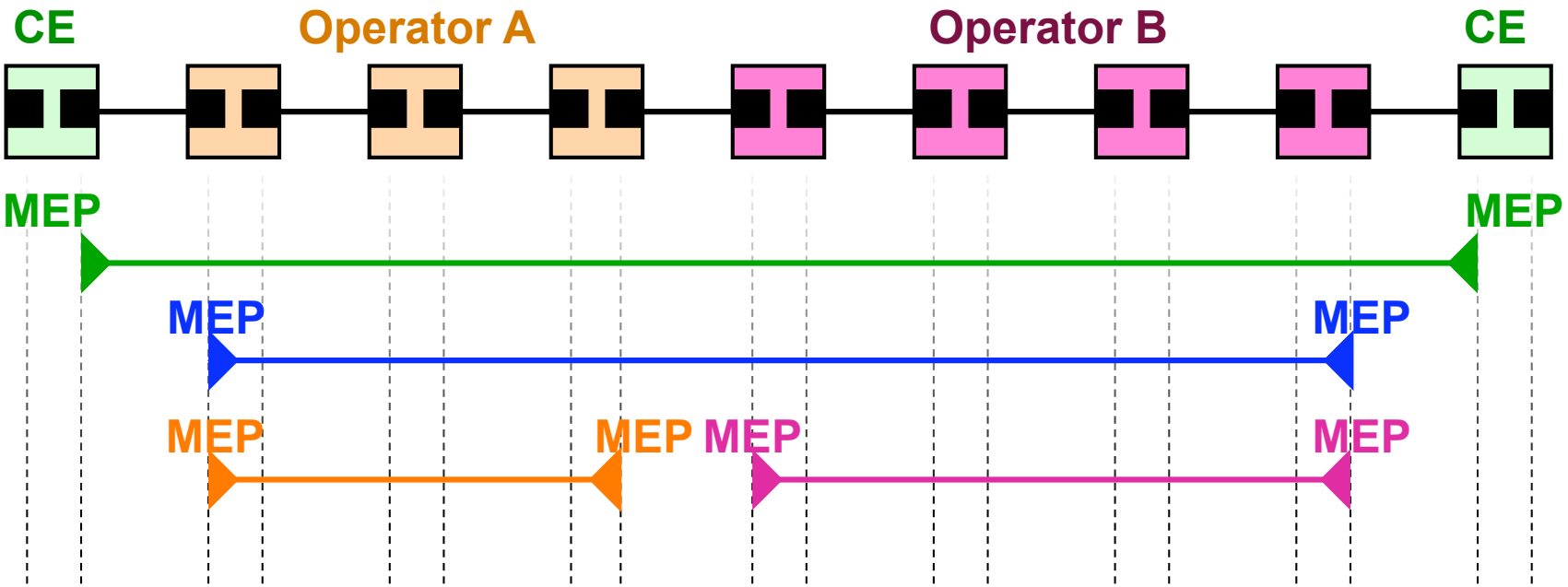
Maintenance Domain (MD)



- Defined by Operational/Contractual Boundaries
  - e.g. Customer / Service Provider / Operator
- MD may nest and touch, but never intersect
- Up to 8 levels of “nesting”: MD Level (0..7)
  - The higher the level, the broader its reach

CFM Concepts

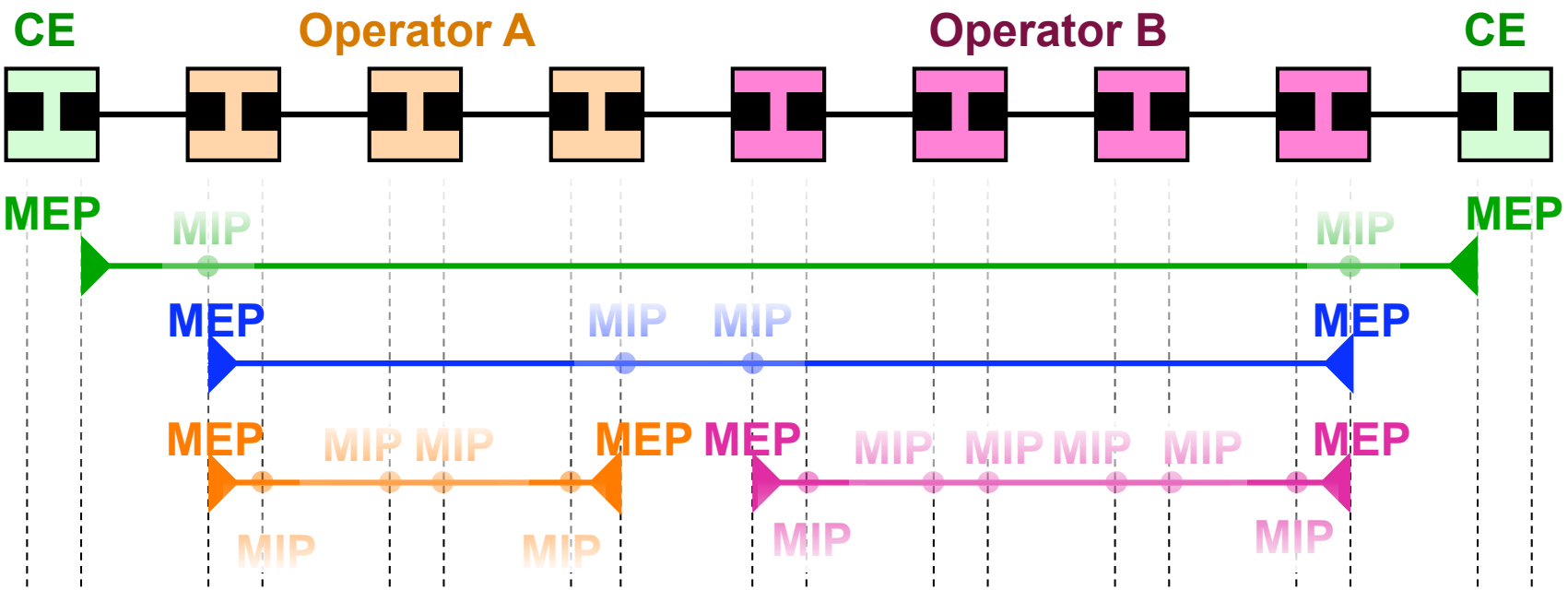
Maintenance Association (MA)



- Monitors connectivity of a particular service instance in a given MD (e.g. 1 service traversing 4 MDs = 4 MAs)
- Defined by a set of Maintenance End Points (MEP) at the edge of a domain
- Identified by MAID == “Short MA” Name + MD Name

CFM Concepts

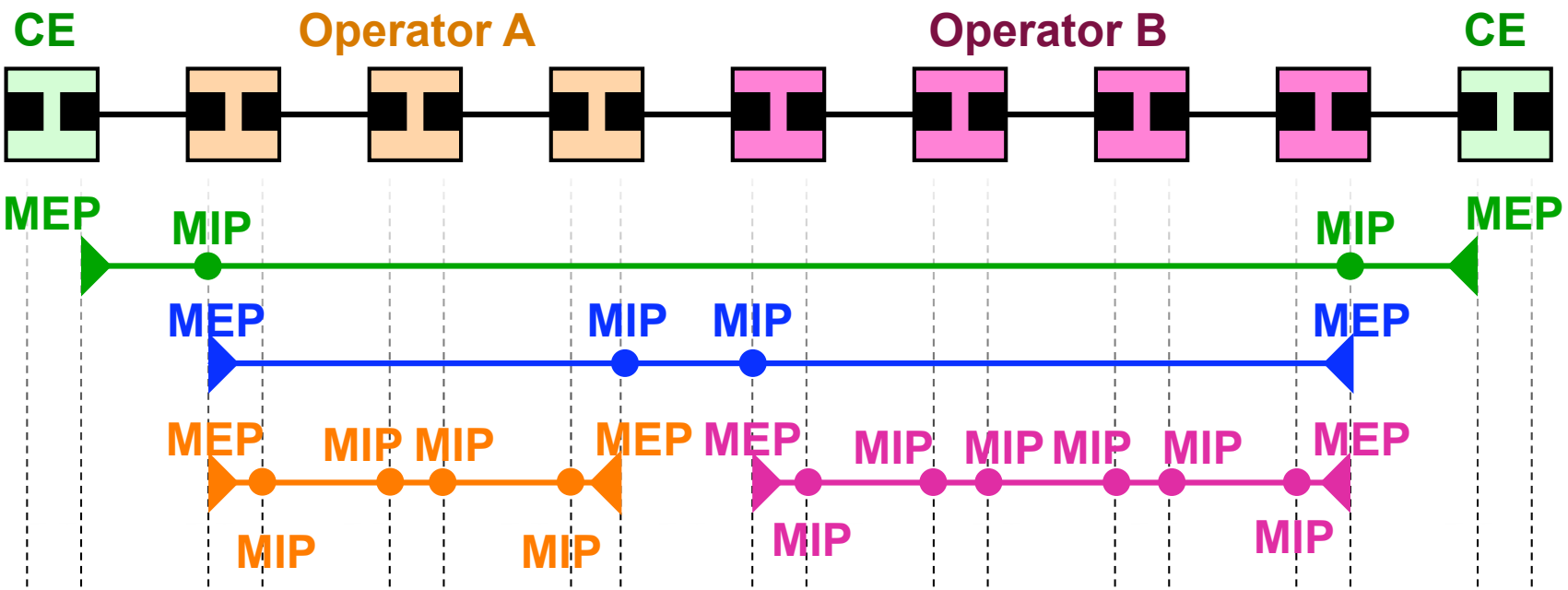
Maintenance Point (MP)—MEP



- Maintenance Association End Point (MEP)
- Define the boundaries of a MD
- Support the detection of connectivity failures between any pair of MEPs in an MA
- Associated per MA and identified by a MEPID **(1-8191)**
- Can initiate and respond to CFM PDUs

CFM Concepts

Maintenance Point (MP)—MIP

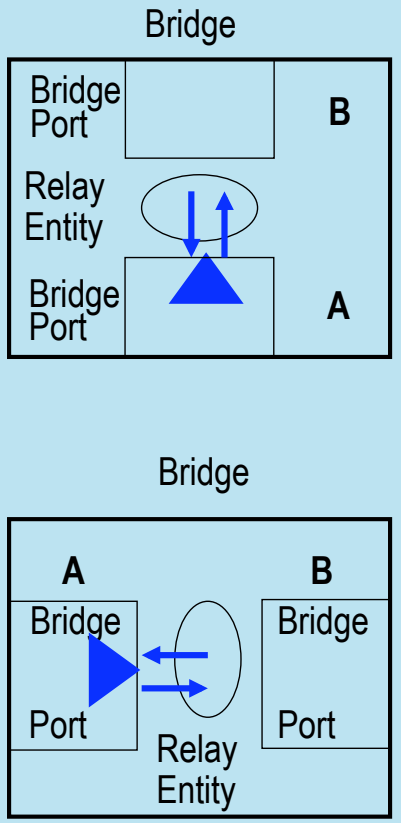


- Maintenance Domain Intermediate Point (MIP)
- Support the discovery of paths among MEPs and location of faults along those paths
- Can be associated per MD, rather than per MA
- Can add, check and respond to received CFM PDUs

CFM Concepts

UP MEP

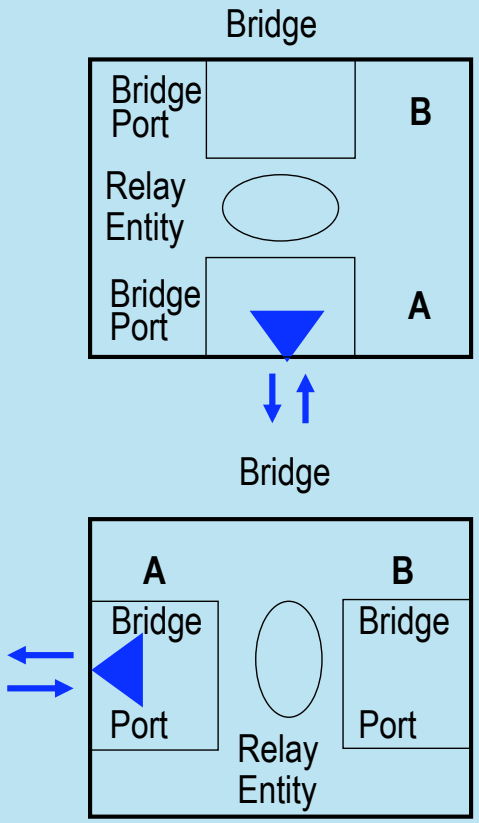
- CFM PDUs generated by the MEP are sent towards the Bridge's Relay Function and not via the wire connected to the port where the MEP is configured
- CFM PDUs to be responded by the MEP are expected to arrive via the Bridge's Relay Function
- Applicable to switches



- Top half depicts a vertical port view that triggered the name UP MEP in the standard
- Bottom half is identical to previous but with a horizontal port view

CFM Concepts
DOWN MEP

- CFM PDUs generated by the MEP are sent via the wire connected to the port where the MEP is configured
- CFM PDUs to be responded by the MEP are expected to arrive via the wire connected to the port where the MEP is configured
- Applicable to routers and switches



- Top half depicts a vertical port view that triggered the name DOWN MEP in the standard
- Bottom half is identical to previous but with a horizontal port view

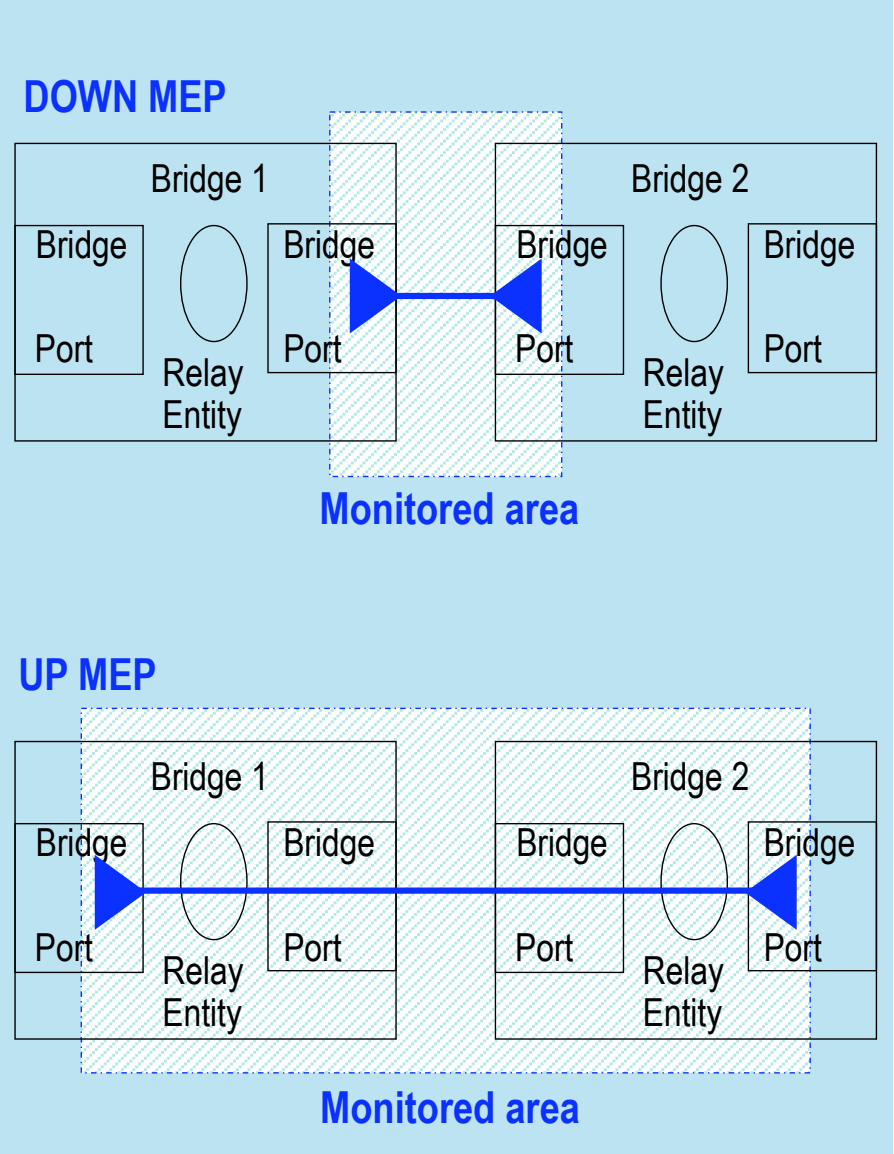
CFM Concepts

MAs and UP/DOWN MEPs

- Applicability of UP/DOWN MEPs in switches:

  DOWN MEPs are typically used for MAs spanning a single link

  UP MEPs are commonly used for MAs with a wider reach (e.g. end-to-end, beyond a single link

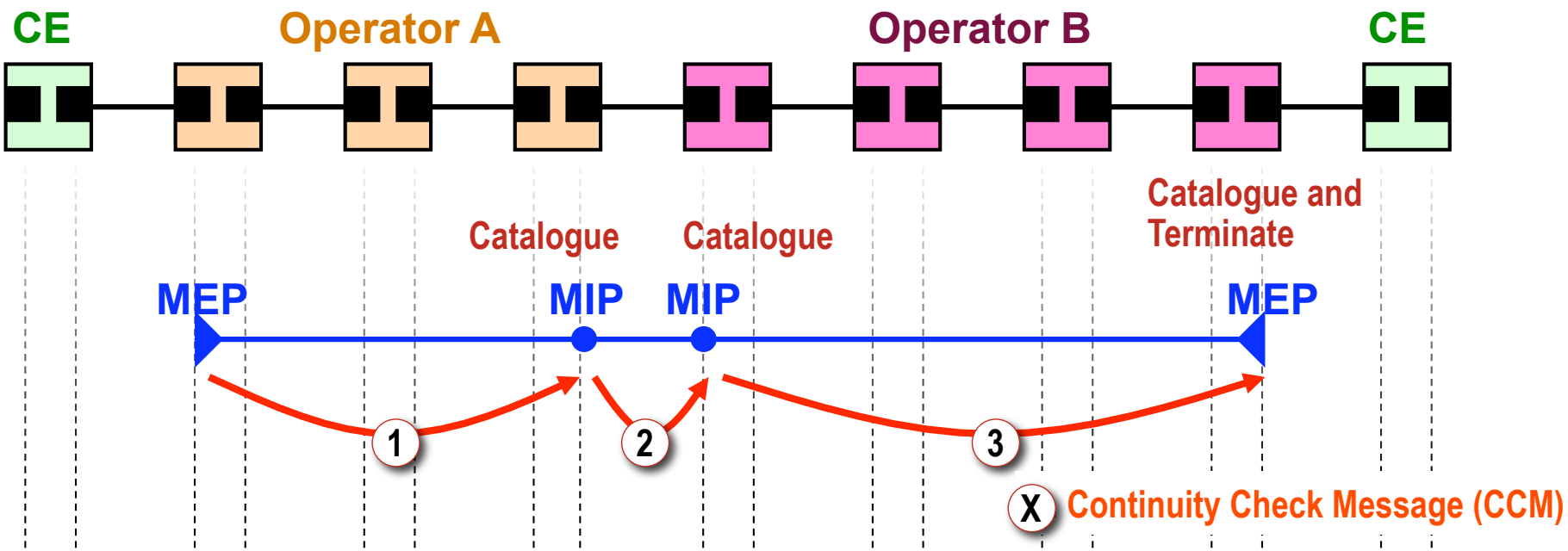


CFM Protocols

- There are three protocols defined by CFM
- Continuity Check Protocol (heart-beat)
  - Fault Detection
  - Fault Notification
- Loopback Protocol
  - Fault Verification
- Linktrace Protocol
  - Fault Isolation

CFM Protocols

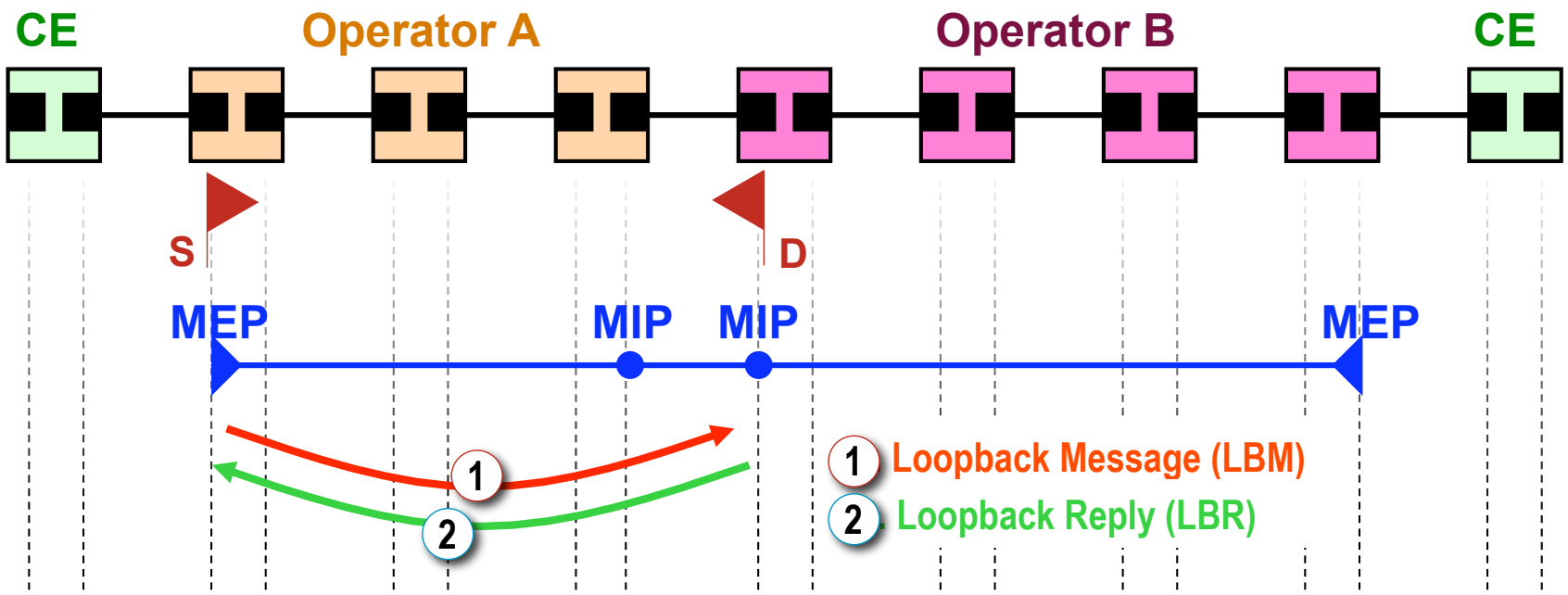
Continuity Check Protocol (CCM)



- Used for Fault Detection and Notification
- Per-Maintenance Association multicast “heart-beat” messages
  - **Carries status of port on which MEP is configured**
  - **Uni-directional (no response required)**
  - **Transmitted at a configurable periodic interval by MEPs**
- Catalogued by MIPs at the same MD-Level, Terminated by remote MEPs in the same MA

CFM Protocols

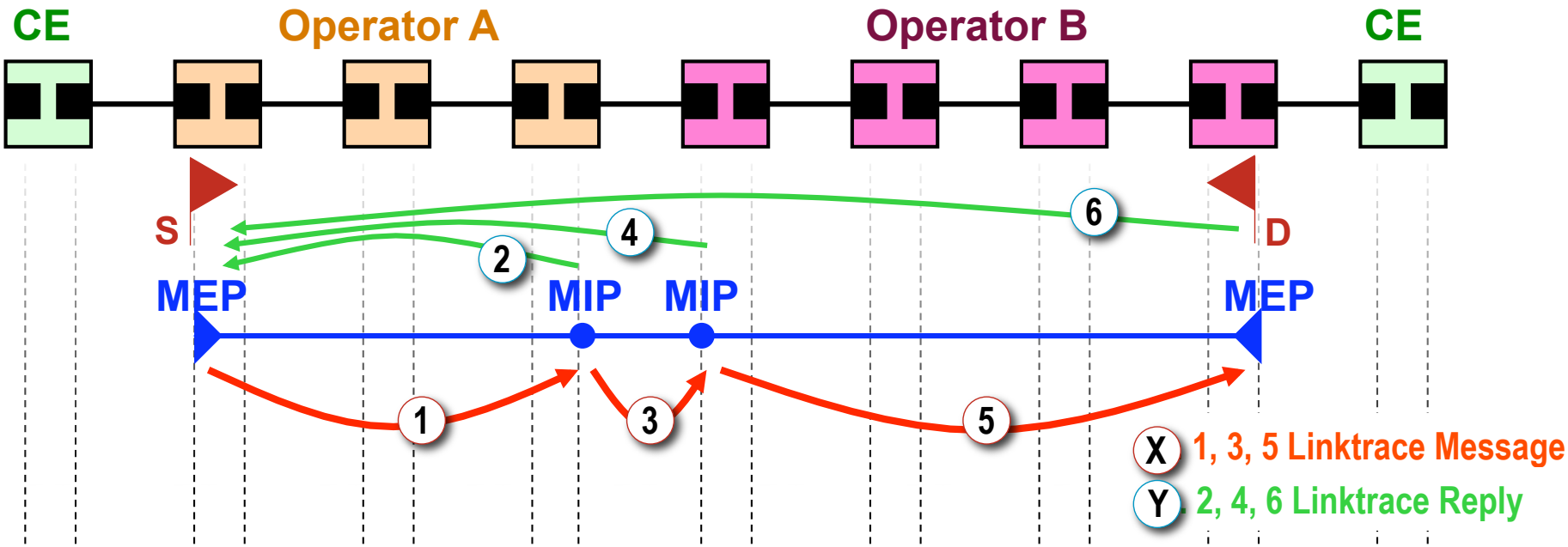
Loopback Protocol (LBM, LBR)



- Used for Fault Verification – Ethernet Ping
- MEP can transmit a unicast LBM to a MEP or MIP in the same MA
- Receiving MP responds by transforming the LBM into a unicast LBR sent back to the originating MEP

CFM Protocols

Linktrace Protocol (LTM, LTR)



- Used for Path Discovery and Fault Isolation – Ethernet Traceroute
- MEP can transmit a multicast message (LTM) in order to discover the MPs and path to a MIP or MEP in the same MA
- Each MIP along the path and the terminating MP return a unicast LTR to originating MEP

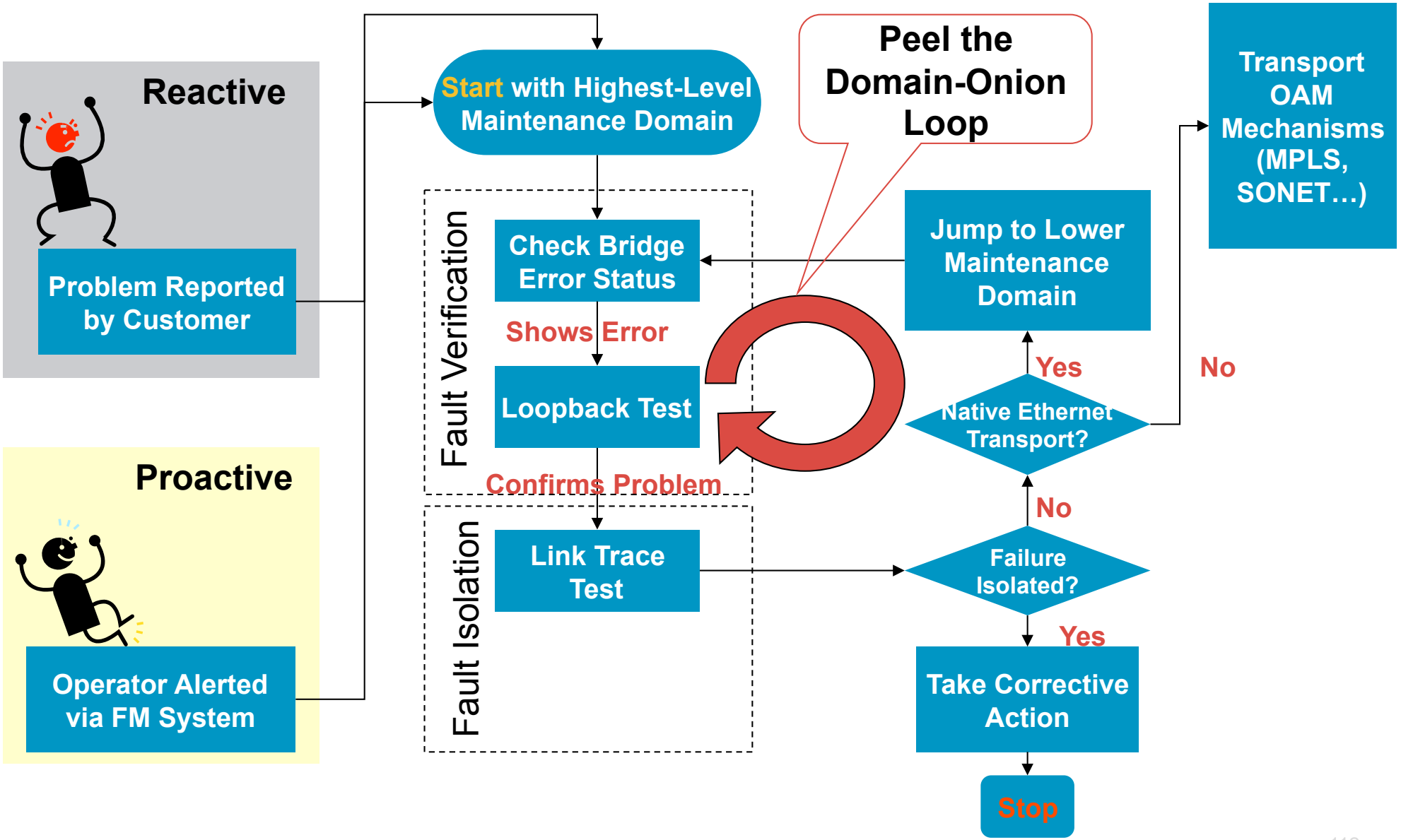
CFM Protocols

CFM PDU Summary

- Summary of CFM PDUs defined per protocol and type of frame used

CFM Protocol	CFM PDU	Destination MAC address
Continuity Check	Continuity Check Message (**CCM**)	Multicast
Loopback	Loopback Message (**LBM**)	Unicast
	Loopback Reply (**LBR**)	Unicast
Linktrace	Linktrace Message (**LTM**)	Multicast
	Linktrace Reply (**LTR**)	Unicast

Troubleshooting: The Workflow



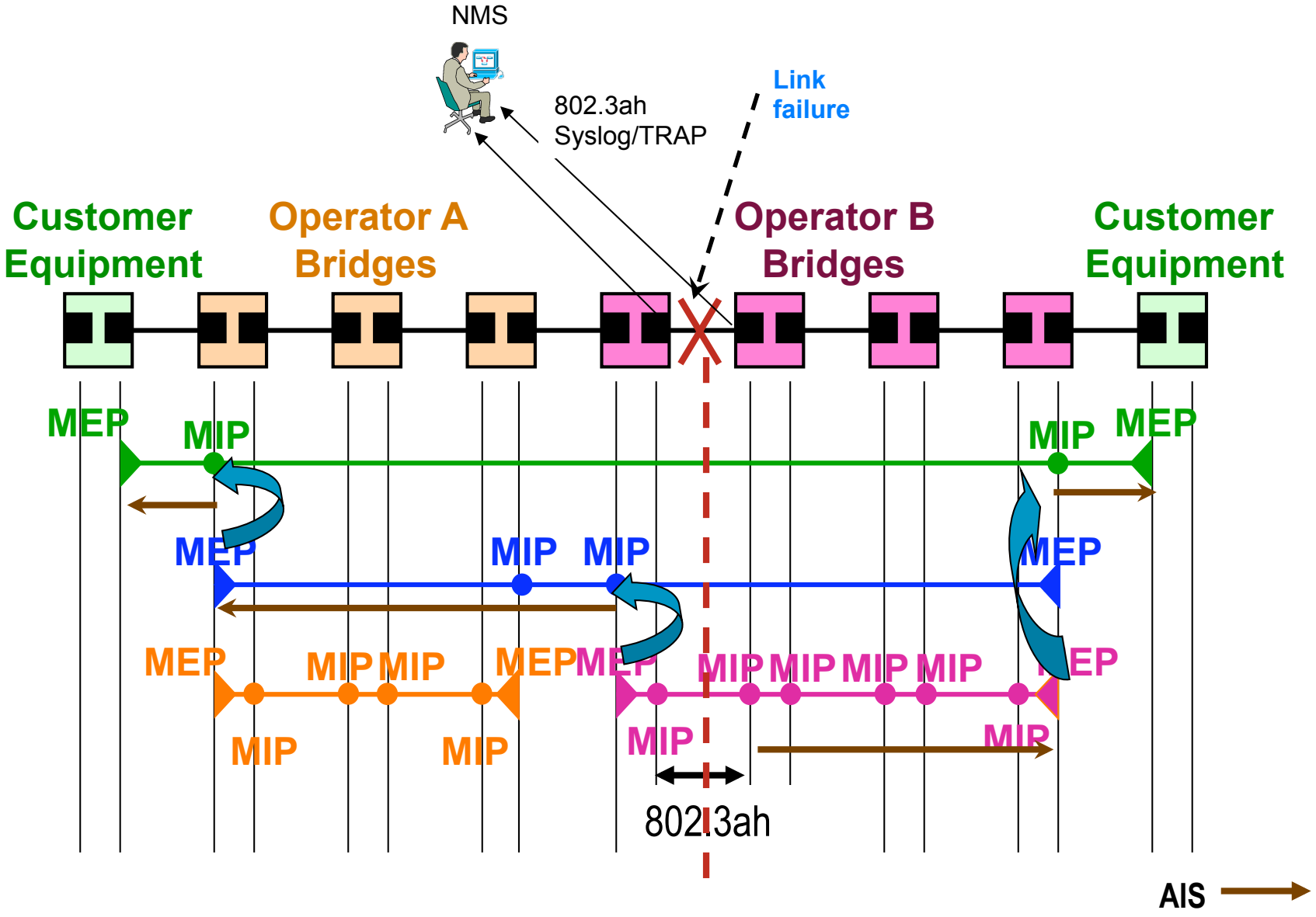
ITU Y.1731 OAM Functions and Mechanisms for Ethernet-Based Networks

ITU-T Y.1731

- ITU Recommendation that provide mechanisms for user-plane OAM functionality in Ethernet networks
- Compatible extension of IEEE CFM. It adds capabilities such as:
  - Ethernet Locked Signal (ETH-LCK)
  - Ethernet Test Signal (ETH-Test)
  - Multicast Loopback
  - Alarm Indication Signal (ETH-AIS)
  - Ethernet Maintenance Communication Channel (ETH-MCC)
  - Ethernet Experimental OAM (ETH-EXP)
  - **Performance Management**
    - Frame Loss Measurement (ETH-LM)
    - Frame Delay Measurement (ETH-DM)
    - Throughput Measurement
- Approved on May 2006 by ITU-T SG 13

ITU Y.1731

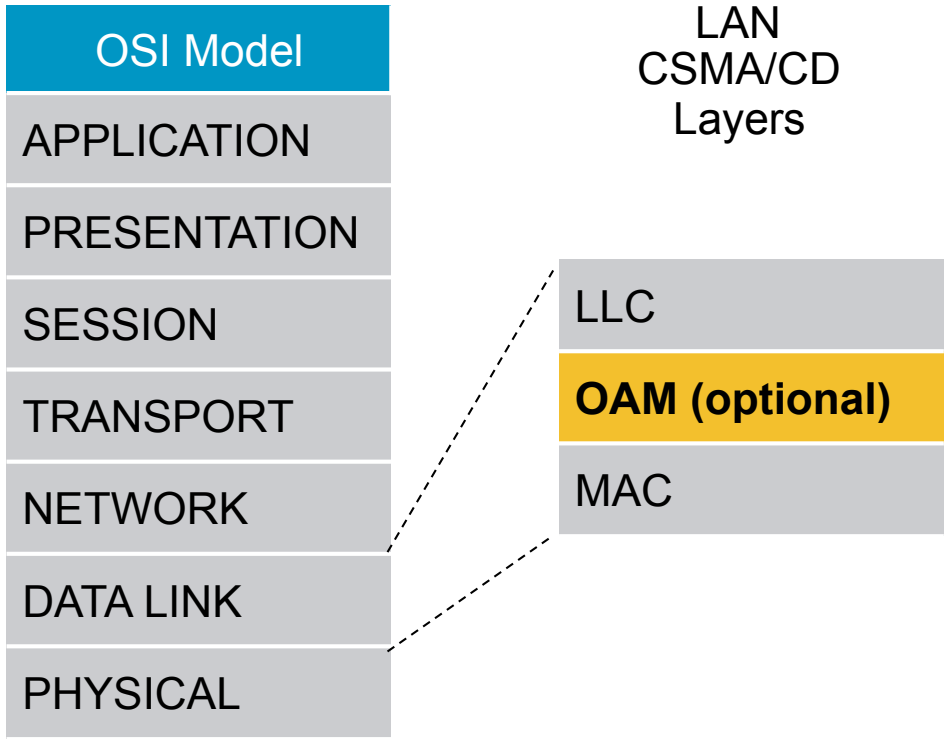
Alarm Indication Signal (ETH-AIS) (cont.)



IEEE 802.3ah (Clause 57) Link OAM

Link OAM (IEEE 802.3ah, Clause 57)

- Provides mechanisms useful for “monitoring link operation”, such as:
  - Link Monitoring
  - Remote Failure Indication
  - Remote Loopback Control
- Defines an optional OAM sublayer
- Intended for single point-to-point IEEE 802.3 links
- Uses “Slow Protocol”[1] frames called OAMPDUs which are never forwarded by MAC clients
- Standardized: IEEE 802.3ah, clause 57



(1) No More than 10 Frames Transmitted in Any One-Second Period

IEEE 802.3ah

Key Functions

- OAM Discovery

  Discover OAM support and capabilities per device

- Link monitoring

  Basic error definitions for Ethernet so entities can detect failed and degraded connections

- Fault Signaling

  mechanisms for one entity to signal another that it has detected an error

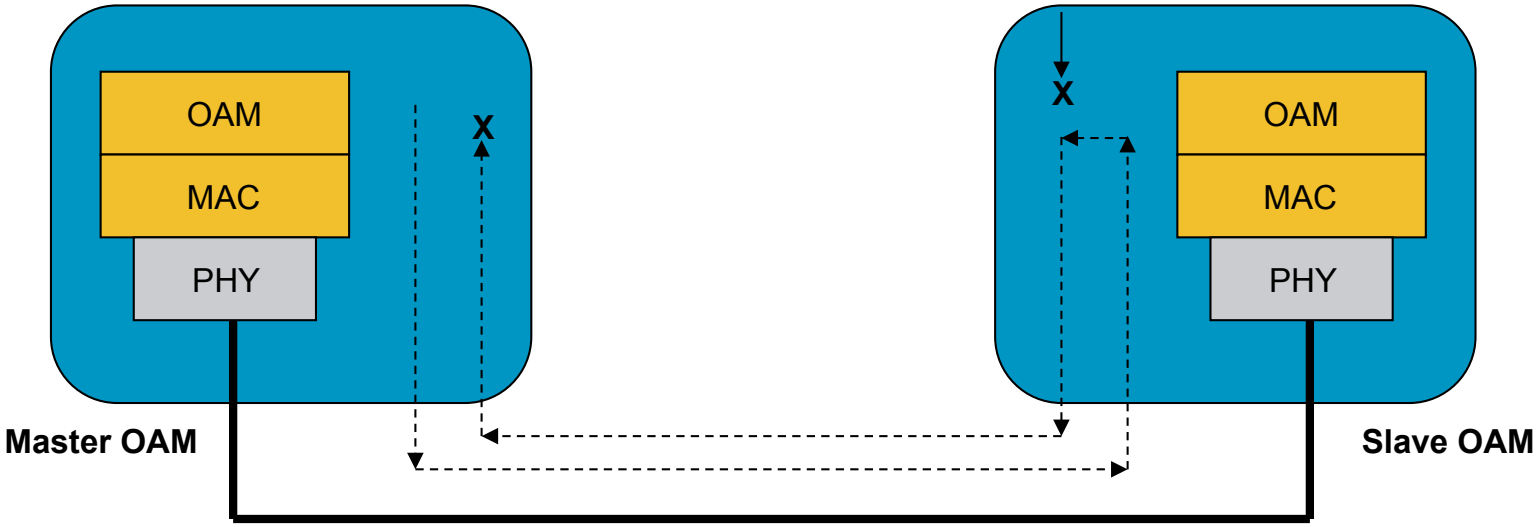
- Remote loopback

  used to troubleshoot networks, allows one station to put the other station into a state whereby all inbound traffic is immediately reflected back onto the link

IEEE 802.3ah

Remote Loopback

- Fault localization and link performance testing
- Loopback Control OAMPDU is used to control a remote OAM client.
- Traffic sent from master loopback port is loopback by slave port, except Pause and OAMPDU

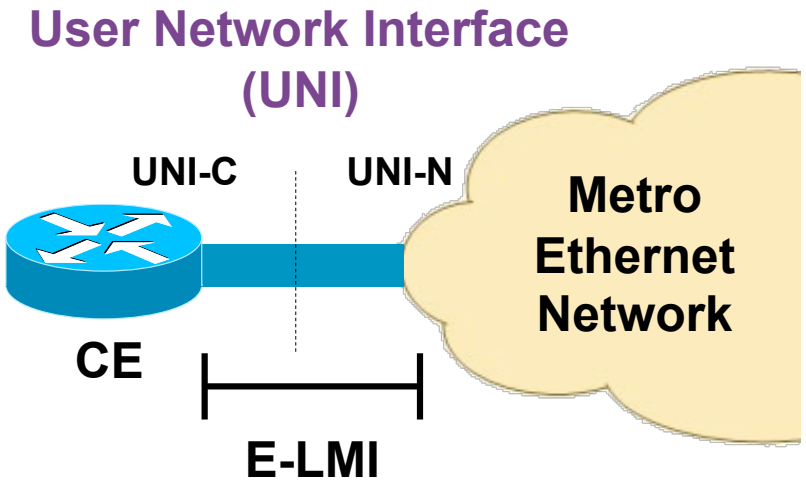


MEF Ethernet Local Management Interface (E-LMI)

Ethernet LMI

Overview

- Provides protocol and mechanisms used for:
  - **Notification of Remote UNI status to CE**
  - **Notification of EVC addition, deletion or status (Active, Not Active, Partially Active) to CE**
  - **Communication of UNI and EVC attributes to CE (e.g. CE-VLAN to EVC map)**
  - **CE auto-configuration**
- Asymmetric protocol based on Frame Relay LMI, mainly applicable to the UNI (UNI-C and UNI-N)
- Specification completed by MEF: http://www.metroethernetforum.org/PDFs/Standards/MEF16.doc

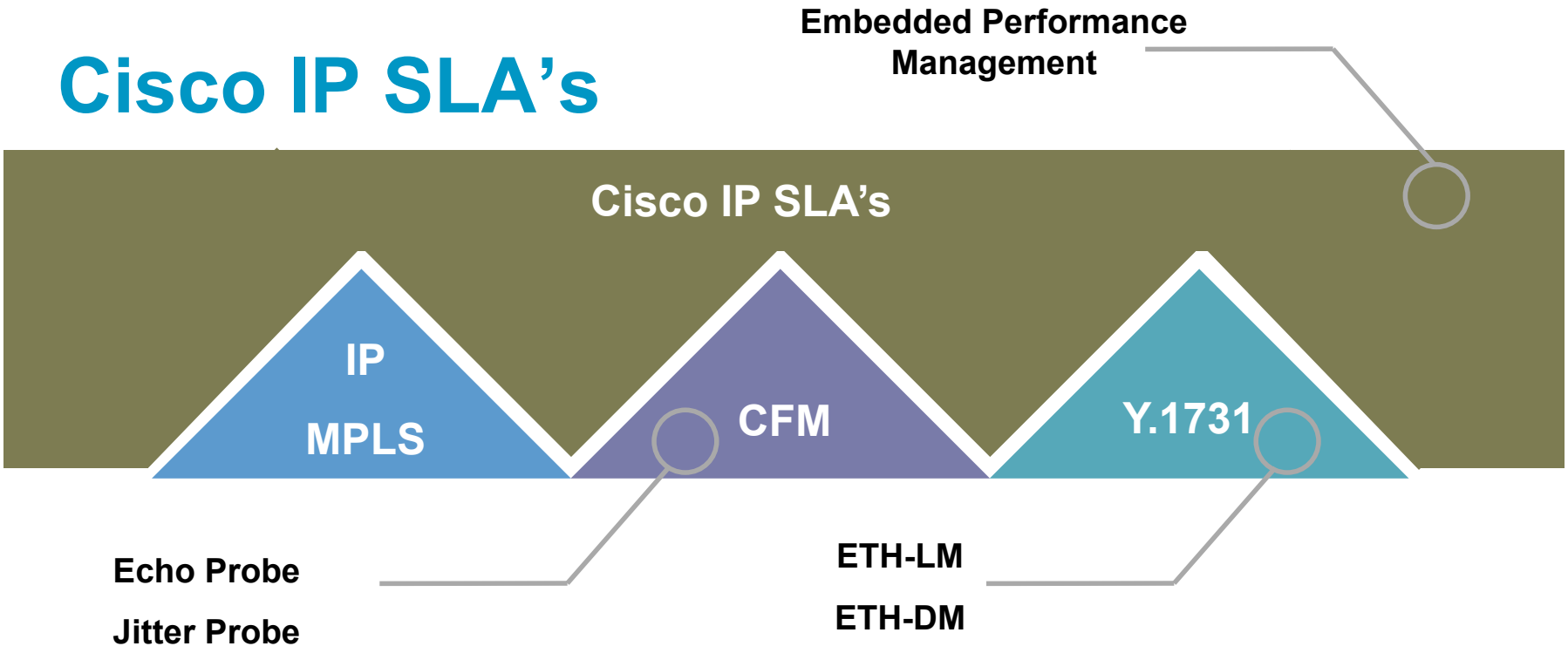


Cisco’s IP SLA

Ethernet Performance Management

Protocol	Mechanism	Capability
Cisco IP SLA for Metro Ethernet	Echo Probe	Per service, ethernet probe Uses CFM LBM/LBR PDUs Measures RTT
	Jitter Probe	Per service, ethernet probe Uses proprietary CFM messages Measures uni-directional packet loss, jitter and latency
Cisco IP SLA with Y.1731 PM	Frame Delay Measurement (ETH-DM) Frame Loss Measurement (ETH-LM)	Measurement of performance parameters for P2P services Frame Loss Ratio Frame Delay Frame Delay Variation Throughput

Cisco IP SLA's



- **Cisco IP SLA's Embedded Policy Management**
  - **Scheduling Automation**
  - **Policy Alerts**
  - **Data Collection / Statistics**
- **CFM and Y.1731 provide underlying 'wire procedures' to collect SLA metrics:**
  - **Frame Formats**
  - **Transmission/reception procedures**

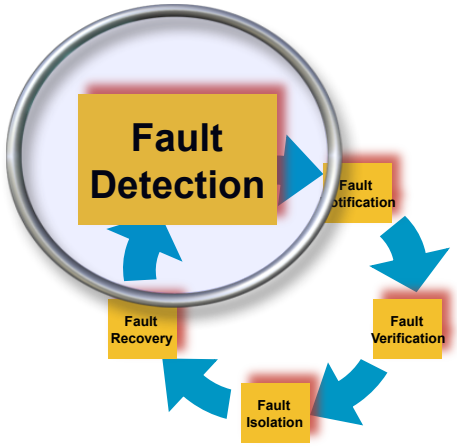
Cisco IP SLA for Metro Ethernet

Highlights

- In-band Performance Management Tool for Ethernet
  - Use native Ethernet frames
  - IP not required
- Built on CFM principles
  - Use Ethernet CFM frames to collect statistics
  - Probes performed in context of a VLAN and a CFM Maintenance Domain
  - CFM MEPs define probe endpoints
- Automatic Discovery of Probe Endpoints
  - Rely on CFM Continuity Check Database (CCDB) to automatically discover Probe Endpoints
  - EVC and Maintenance Domain based
  - Support ‘static’ probes and exclusions

Ethernet OAM and Fault Management

E-OAM Mechanisms for Fault Management (1 of 5)



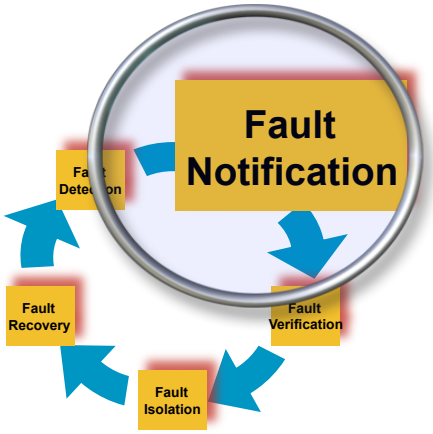
Fault Detection

	Mechanism	Detectable Faults
802.1ag (CFM)	Continuity Check (CC)	• Unintended connectivity/service leaks • Unexpected sites • Loss of connectivity to a site • Link Connectivity failure • Device failure (soft & hard) • Forwarding plane loops • CFM Configuration Errors
802.3ah	Link Monitoring	• Unidirectional Link • Slowly deteriorating link quality (Frame/Symbol Errors)

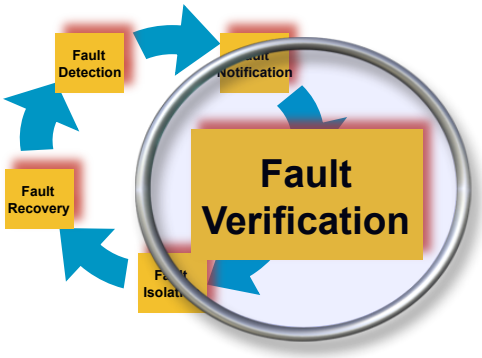
E-OAM Mechanisms for Fault Management (2 of 5)

Fault Notification

	Mechanism	Triggers
Y.1731	Alarm Indication Signal (AIS)	• Loss of CFM Continuity Check • Indication from Server Layer OAM • Indication from lower ME Level CFM Domain
802.1ag (CFM)	Remote Defect Indication (RDI)	• Unidirectional service Connectivity (p2p) • Partial service connectivity (mp)
802.3ah	Remote Failure Indication (RFI)	• Link Fault (receive path) • Critical Event, e.g. when operator shutting down an interface.
	Event Notification	• Error thresholds exceeded (frames/symbols per interval)
E-LMI	Status Message	• EVC Status Change • Remote UNI(s) Status Change



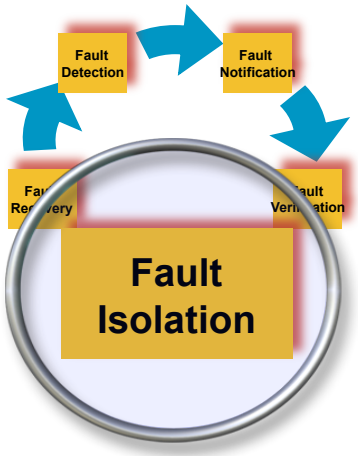
E-OAM Mechanisms for Fault Management (3 of 5)



Fault Verification

	Mechanism	Capability
802.1ag (CFM)	Loopback	• Per EVC MAC Ping (source to single destination) • Verify bidirectional connectivity between two CFM Maintenance Points (for varied frame sizes)
Y.1731	Multicast Loopback	• Per EVC MAC Ping (source to all destinations) • Verify bidirectional connectivity between one CFM Maintenance End Point and all other End Points of a service (for varied frame sizes)

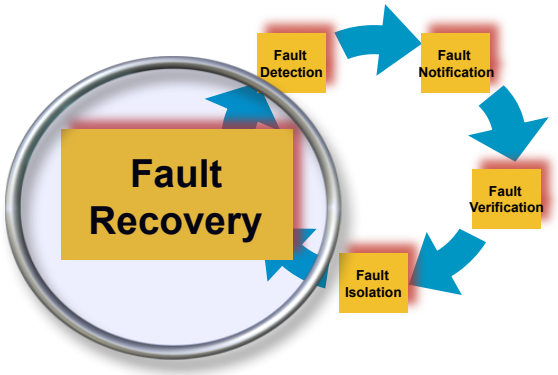
E-OAM Mechanisms for Fault Management (4 of 5)



Fault Isolation

	Mechanism	Capability
802.1ag (CFM)	Link Trace	• Per EVC MAC Traceroute • Discover Maintenance Intermediate Points on path from source End Point to destination End Point • Report Ingress Action, Relay Action, Egress Action hop by hop. • Report encountered ACLs or STP-blocked ports

E-OAM Mechanisms for Fault Management (5 of 5)



Fault Recovery

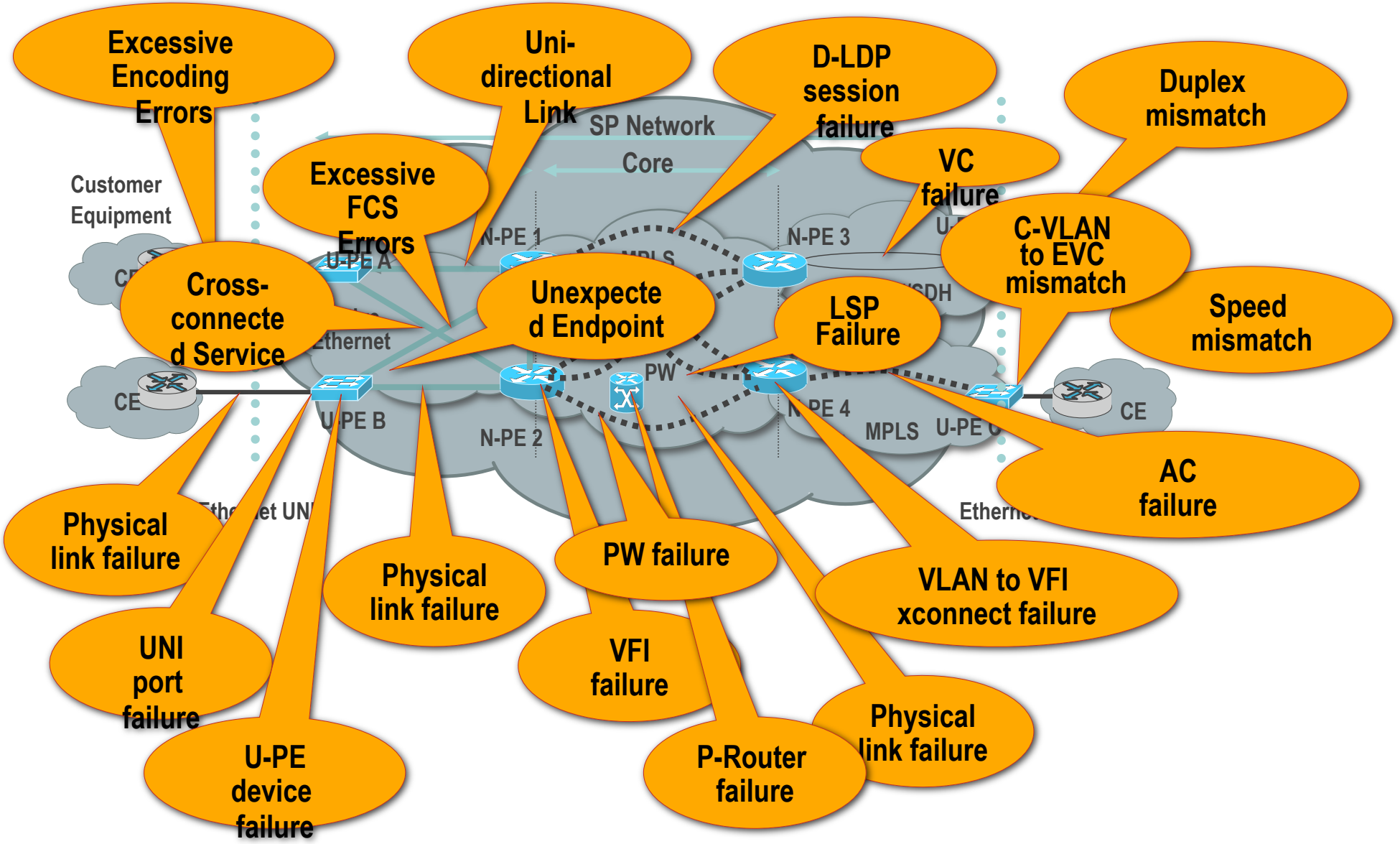
	Mechanism	Capability
G.8031	ETH-APS	• Use CFM mechanisms for monitoring redundant paths (order of msec)
Non-OAM Mechanisms	STP/RSTP	

Inter-working Scenarios
Main Examples

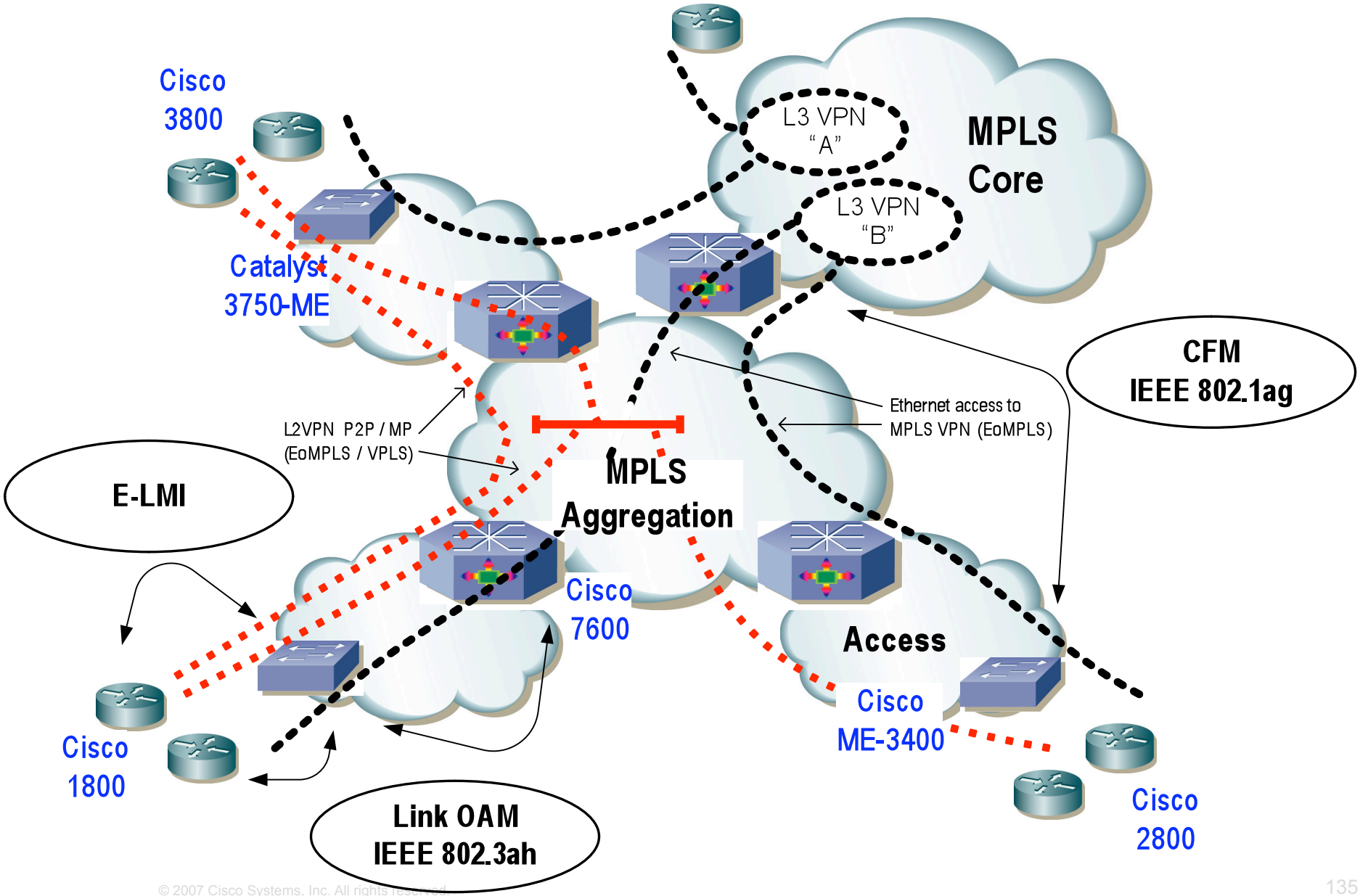
Server Layer		Client Layer
Connectivity Fault Management (CFM)	→	Ethernet LMI (E-LMI)
Link OAM (802.3ah)	→	Connectivity Fault Management (CFM)
MPLS PW OAM	→	Ethernet LMI (E-LMI)
MPLS PW OAM	→	Connectivity Fault Management (CFM)

Ethernet OAM
Fault Management Scenarios

Problem Scope
A few possible scenarios



High Level Topology



Fault Management Scenarios

Number	Description
1	End-to-End Service/Path Verification Fault Verification/Isolation
2	Using E-OAM for Ethernet Access to L3VPN
3	E2E CPE Fault Notification & CPE Corrective Action using Ethernet OAM Interworking
4	Ethernet OAM and MPLS OAM Interworking

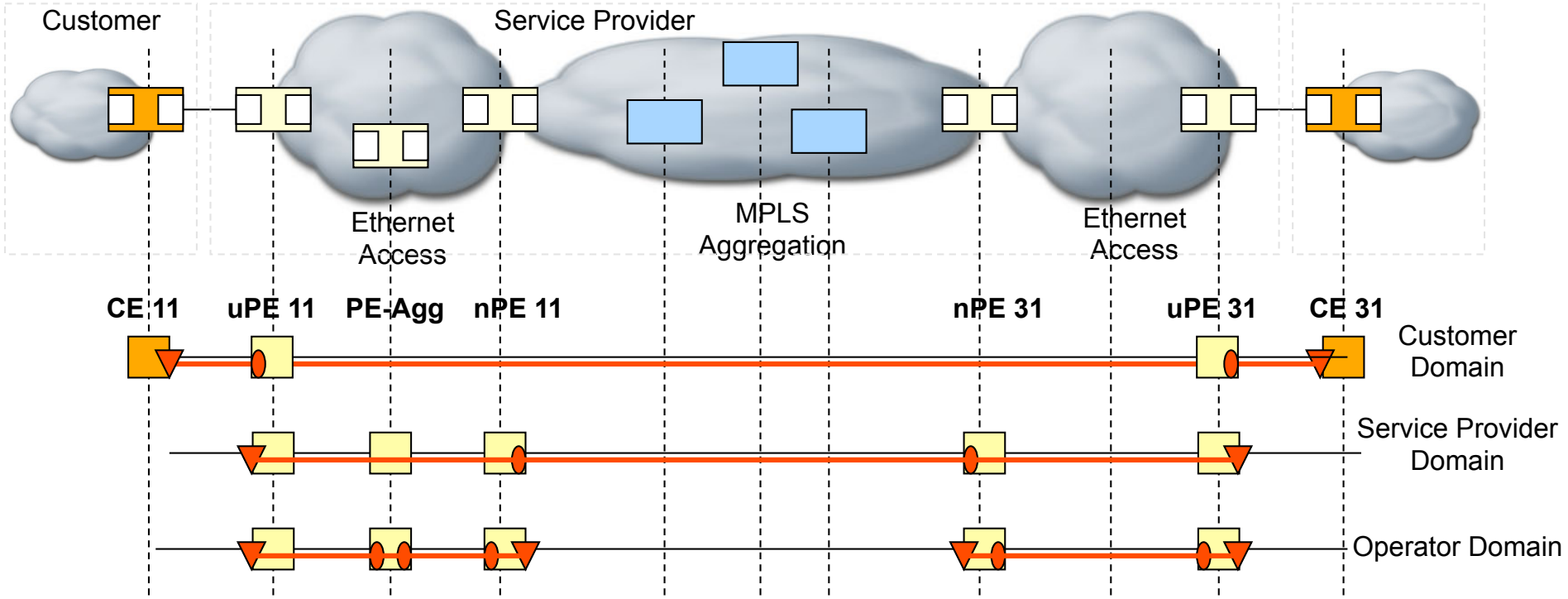
Operational Scenario 1

- Problem Statement

  Fault Verification and Fault Isolation of ethernet connectivity issues

- Problem Solution

  IEEE 802.1ag (CFM) Ping and Traceroute utilities for reactive troubleshooting of service connectivity issues



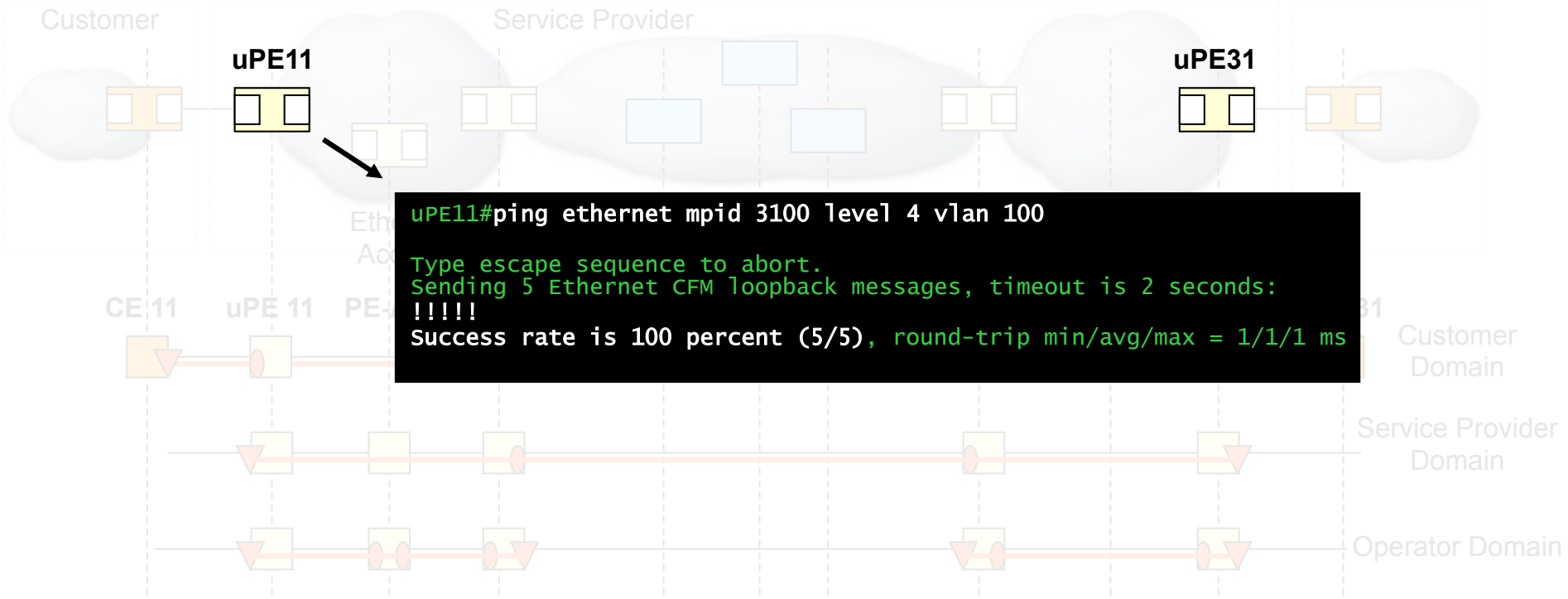
Operational Scenario 1 (cont.)

- Problem Statement

  Fault Verification and Fault Isolation of ethernet connectivity issues

- Problem Solution

  IEEE 802.1ag (CFM) Ping and Traceroute utilities for reactive troubleshooting of service connectivity issues



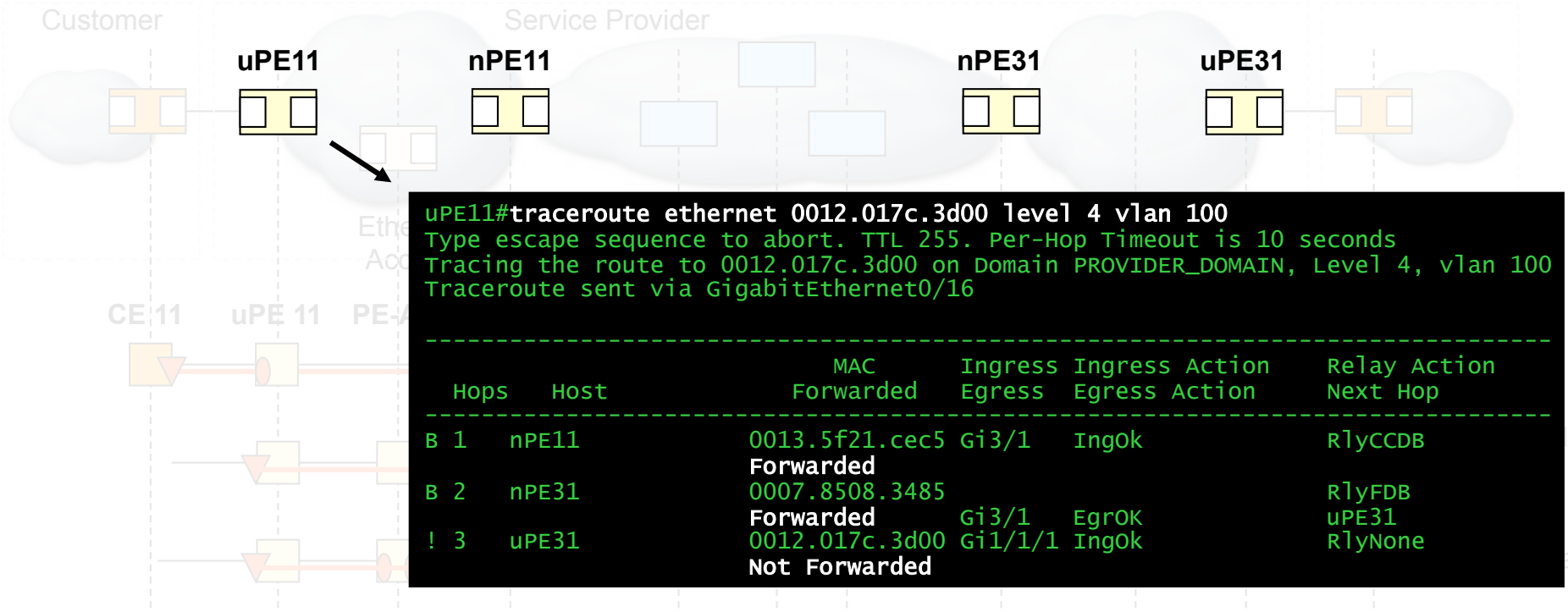
Operational Scenario 1 (cont.)

- Problem Statement

  Fault Verification and Fault Isolation of ethernet connectivity issues

- Problem Solution

  IEEE 802.1ag (CFM) Ping and Traceroute utilities for reactive troubleshooting of service connectivity issues




```
uPE11#traceroute ethernet 0012.017c.3d00 level 4 vlan 100
Type escape sequence to abort. TTL 255. Per-Hop Timeout is 10 seconds
Tracing the route to 0012.017c.3d00 on Domain PROVIDER_DOMAIN, Level 4, vlan 100
Traceroute sent via GigabitEthernet0/16

-------------------------------------------------------------------------------
                                MAC      Ingress Ingress Action    Relay Action
  Hops   Host                 Forwarded  Egress  Egress Action     Next Hop
-------------------------------------------------------------------------------
B 1   nPE11             0013.5f21.cec5 Gi3/1   IngOk             RlyCCDB
                        Forwarded
B 2   nPE31             0007.8508.3485                           RlyFDB
                        Forwarded      Gi3/1   EgrOK             uPE31
! 3   uPE31             0012.017c.3d00 Gi1/1/1 IngOk             RlyNone
                        Not Forwarded
```

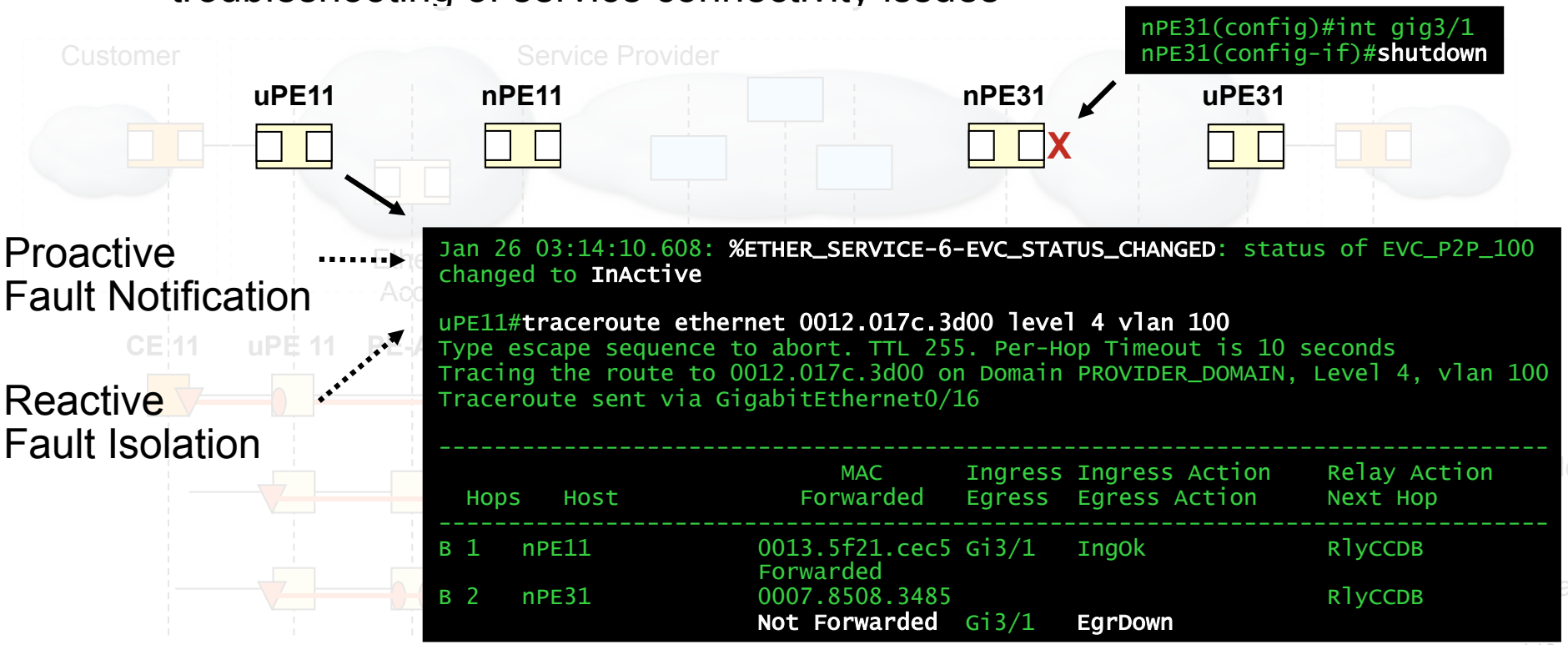
Operational Scenario 1 (cont.)

- Problem Statement

  Fault Verification and Fault Isolation of ethernet connectivity issues

- Problem Solution

  IEEE 802.1ag (CFM) Ping and Traceroute utilities for reactive troubleshooting of service connectivity issues



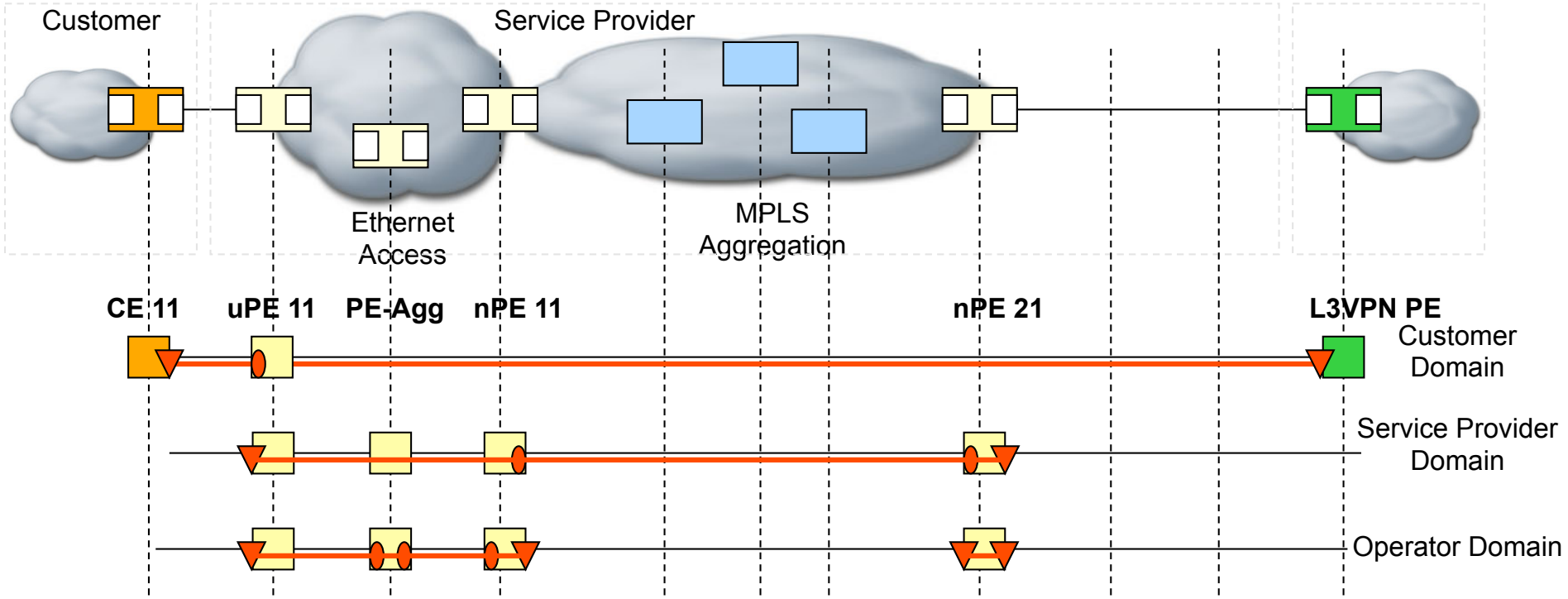
Operational Scenario 2

- Problem Statement

  Troubleshooting Ethernet access connectivity problems by L3VPN PE

- Problem Solution

  IEEE 802.1ag CFM with Outward-facing / Down MEPs at L3VPN PE



Operational Scenario 2 (cont.)

- Problem Statement

  Troubleshooting Ethernet access connectivity problems by L3VPN PE

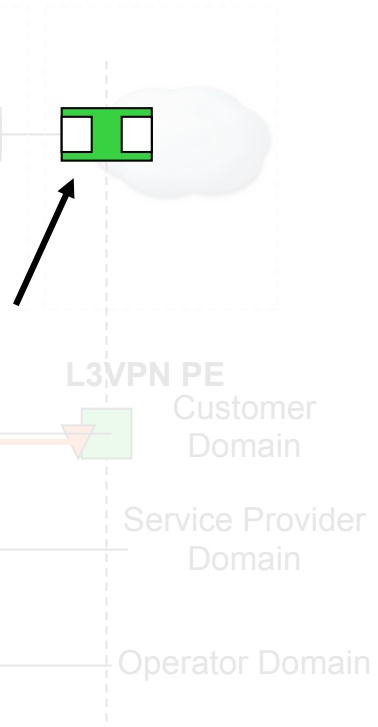
- Problem Solution

  IEEE 802.1ag CFM with Outward-facing / Down MEPs at L3VPN PE

```
L3VPN-PE#show running-config | begin GigabitEthernet3/0/0
interface GigabitEthernet3/0/0
 description L3VPN PE to nPE21 gig3/3
 ethernet cfm mep level 4 outward domain PROVIDER_DOMAIN mpid 2450 vlan 450
 ethernet cfm mep level 4 outward domain PROVIDER_DOMAIN mpid 2350 vlan 350
!
interface GigabitEthernet3/0/0.350
 description To CE31
 encapsulation dot1Q 350
 ip vrf forwarding BLUE
 ip address 1.1.1.1 255.255.255.0
!
interface GigabitEthernet3/0/0.450
 description To CE21
 encapsulation dot1Q 450
 ip vrf forwarding RED
 ip address 1.1.1.1 255.255.255.0


L3VPN-PE#show ethernet cfm maintenance-points remote
Can only Ping/Traceroute to remote MEPs marked with *

MPID  Level Mac Address    Vlan PortState InGressPort     Age(sec) Service ID
3350* 4     0012.017c.3d00 350  UP        Gi3/0/0.350     20       customer_350_provider
2451* 4     0019.552c.0b80 450  UP        Gi3/0/0.450     23       customer_450_provider
```



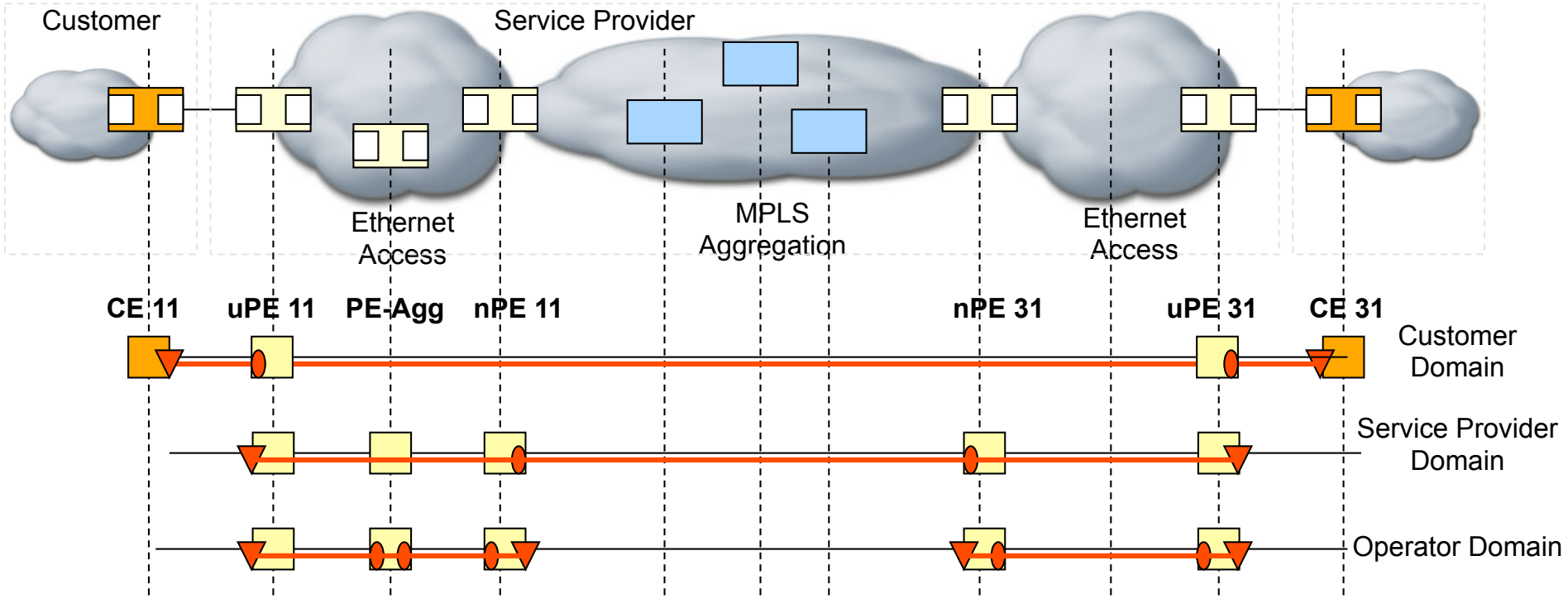
Operational Scenario 3

- Problem Statement

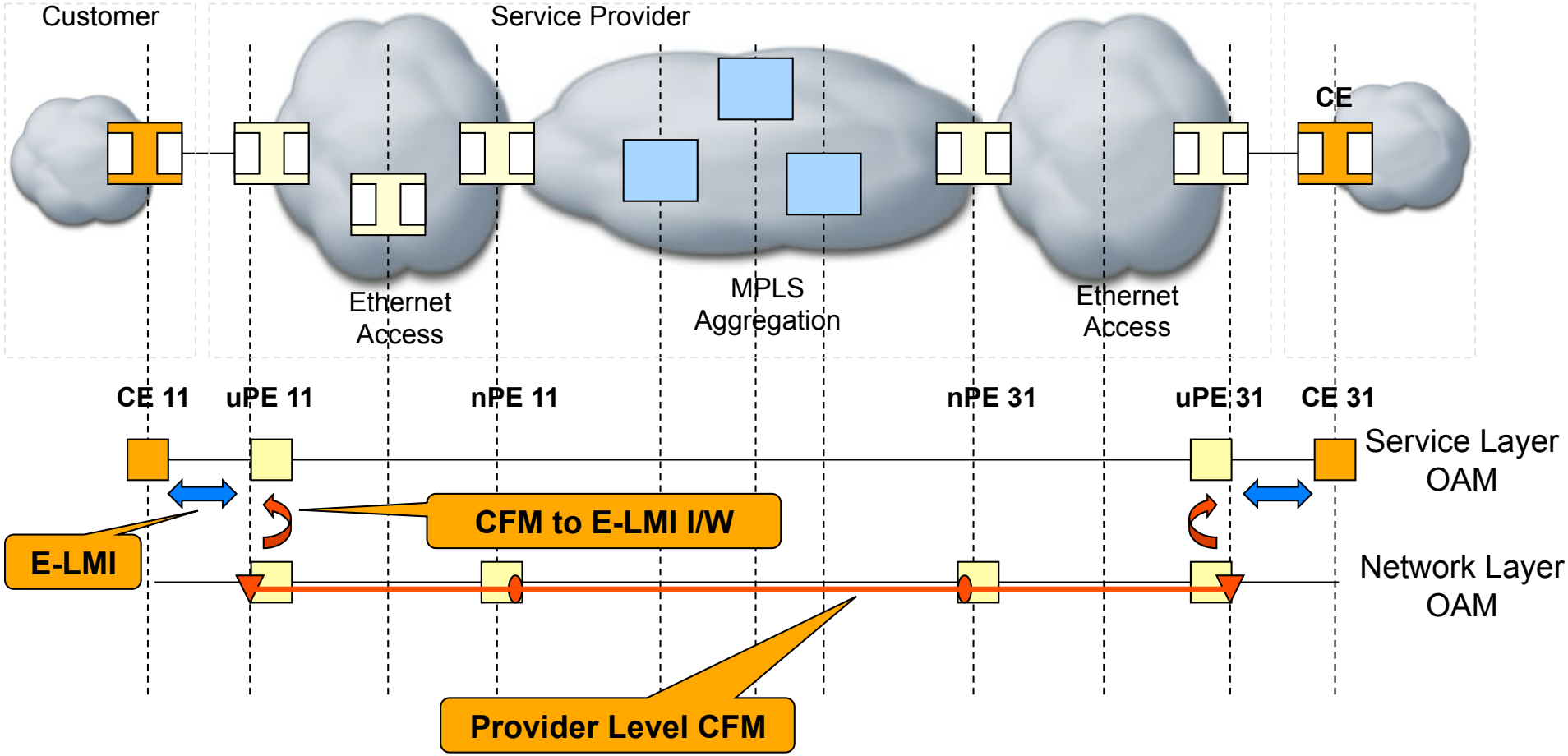
  End to End Fault Notification of service status to Customer Equipment

- Problem Solution

  IEEE 802.3ah to IEEE 802.1ag (CFM) Inter-Working (IW) for propagation of EVC status and CFM to E-LMI IW for notification to CE



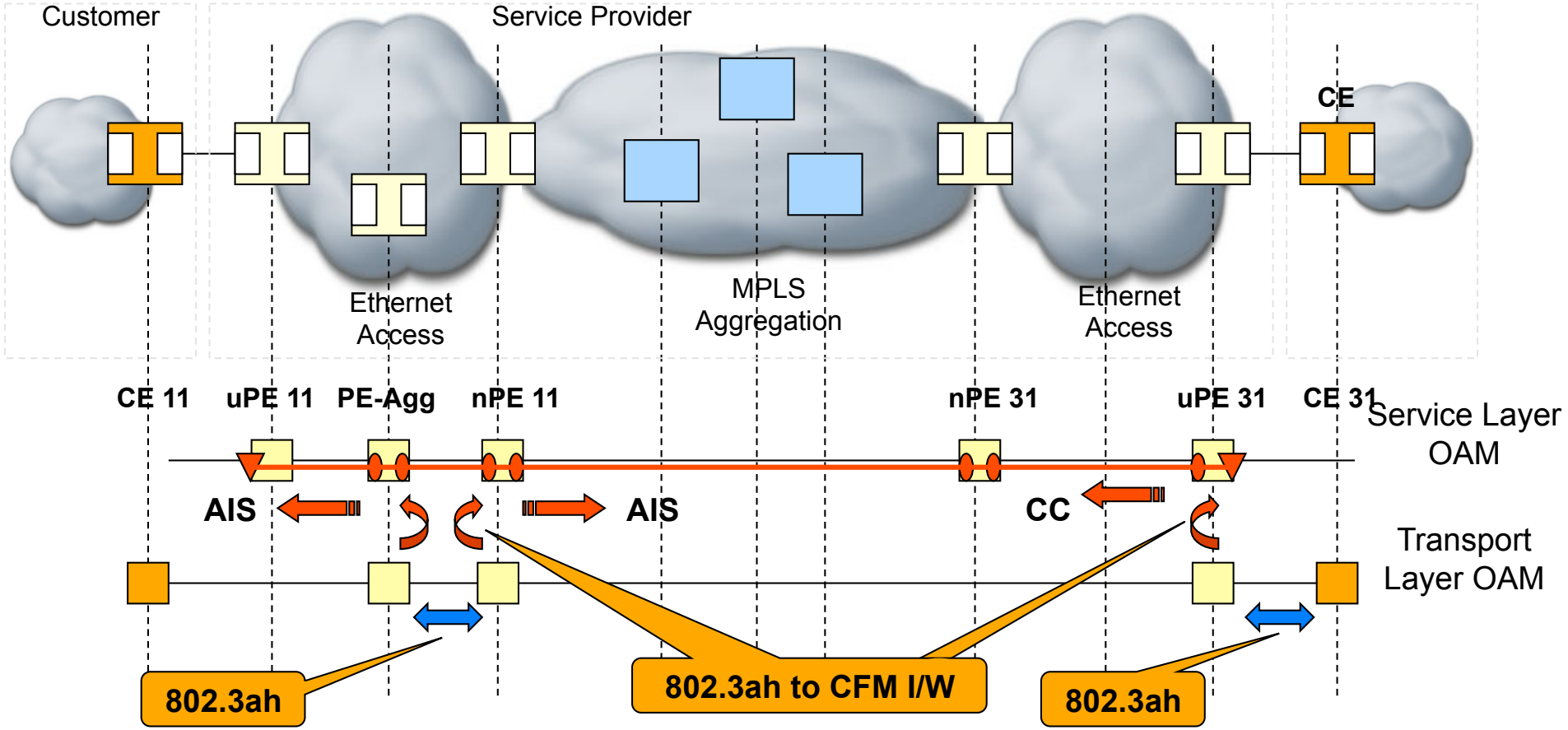
Inter-working Scenarios: CFM to E-LMI



CFM @ Provider Level acts as MEN OAM: provides EVC Status and Remote UNI Status/Name to E-LMI

- Port State TLV of CC Messages carry remote UNI status
- MEP Name TLV of CC Messages carry remote UNI name
- Status of remote MEP in CCDB indicates EVC State

Inter-working Scenarios: 802.3ah to CFM



- Link Layer Defects detected by 802.3ah, relayed to CFM on same device.
- CFM notifies remote devices of localized fault.
- Two variants:
  - CC based (802.3ah on edge of domain)
  - AIS based (802.3ah within domain)

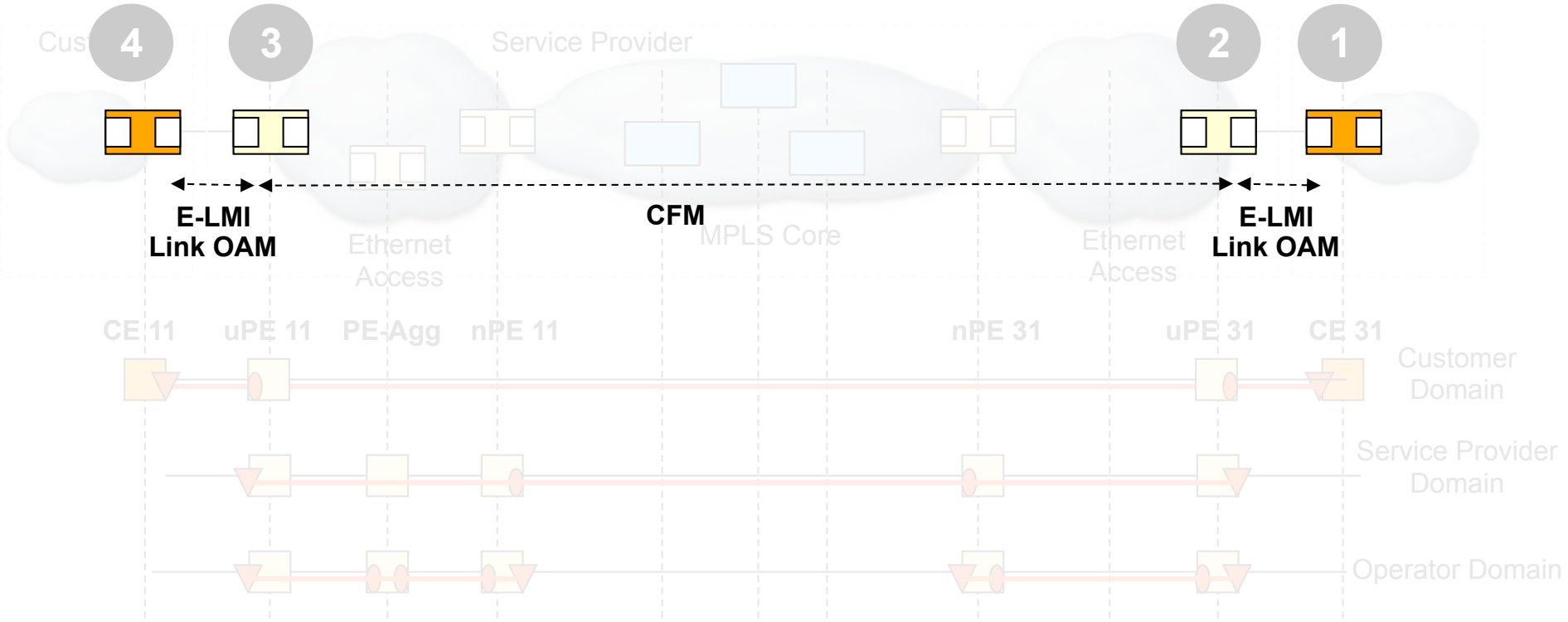
Operational Scenario 3 (cont.)

- Problem Statement

  End to End Fault Notification of service status to Customer Equipment

- Problem Solution

  IEEE 802.3ah to IEEE 802.1ag (CFM) Inter-Working (IW) for propagation of EVC status and CFM to E-LMI IW for notification to CE



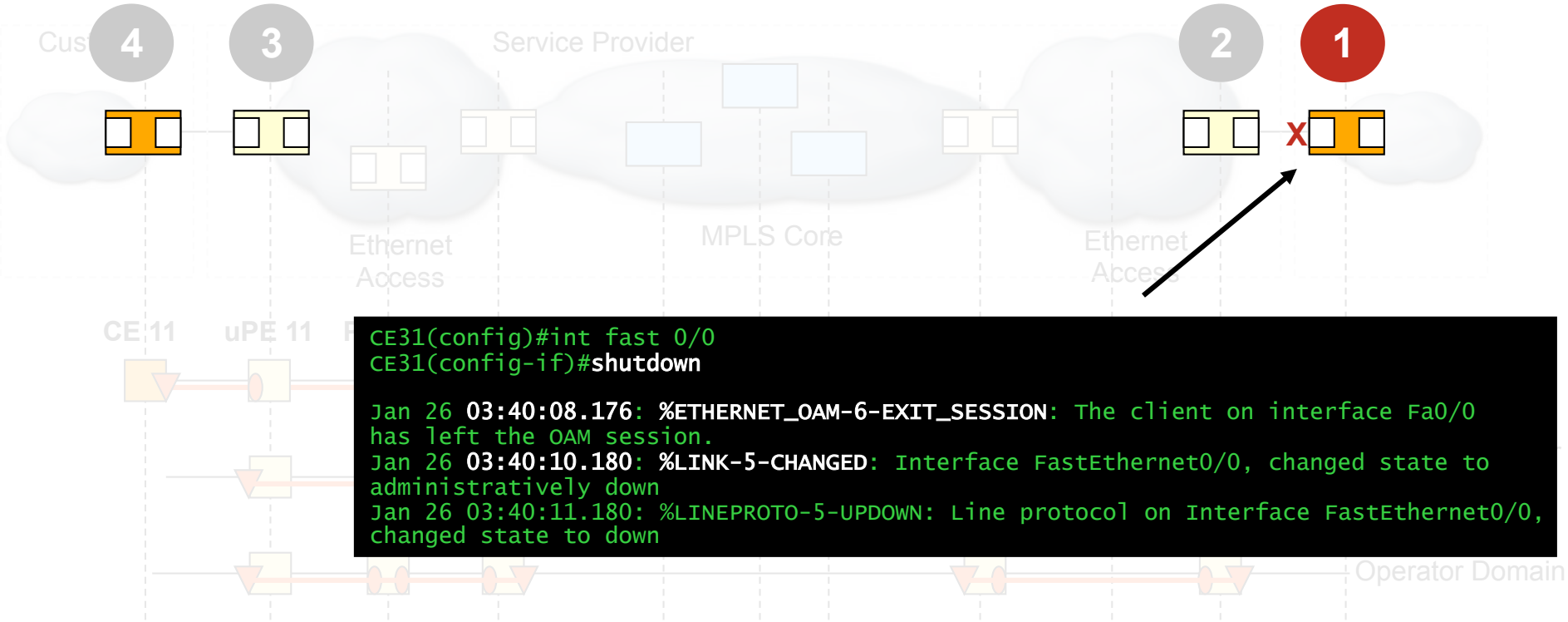
Operational Scenario 3 (cont.)

- Problem Statement

  End to End Fault Notification of service status to Customer Equipment

- Problem Solution

  IEEE 802.3ah to IEEE 802.1ag (CFM) Inter-Working (IW) for propagation of EVC status and CFM to E-LMI IW for notification to CE




```
CE31(config)#int fast 0/0
CE31(config-if)#shutdown

Jan 26 03:40:08.176: %ETHERNET_OAM-6-EXIT_SESSION: The client on interface Fa0/0
has left the OAM session.
Jan 26 03:40:10.180: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
Jan 26 03:40:11.180: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
```

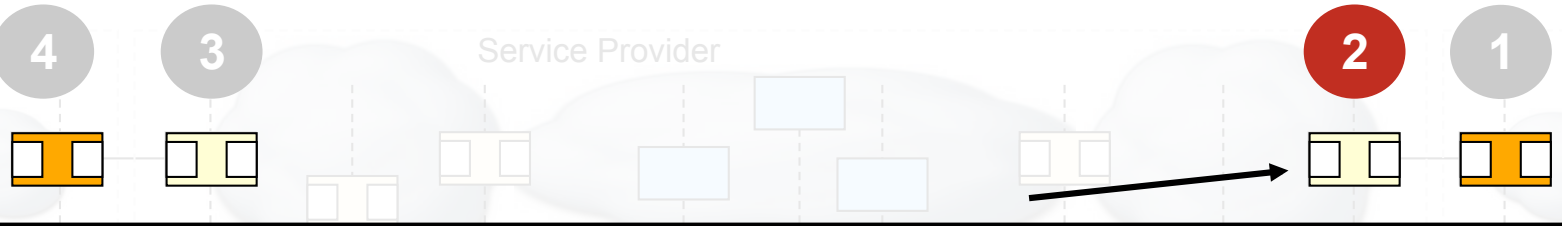
Operational Scenario 3 (cont.)

- Problem Statement

  End to End Fault Notification of service status to Customer Equipment

- Problem Solution

  IEEE 802.3ah to IEEE 802.1ag (CFM) Inter-Working (IW) for propagation of EVC status and CFM to E-LMI IW for notification to CE




```
Jan 26 03:40:08.176: %ETHERNET_OAM-6-RFI: The client on interface Fa1/0/1 has received a remote failure
Indication from its remote peer (failure reason = remote client administratively turned off)

Jan 26 03:40:08.184: %ETHER_SERVICE-6-EVC_STATUS_CHANGED: status of EVC_P2P_100 changed to InActive
Jan 26 03:40:09.191: %ETHERNET_OAM-6-EXIT_SESSION: The client on interface Fa1/0/1 has left the OAM session.

uPE31#show ethernet service evc
Identifier                    Type  Act-UNI-cnt Status
EVC_P2P_100                   P-P       1       InActive

uPE31#show ethernet lmi evc
UNI Id: CE31_UNI
St  Evc Id                                CE-VLAN
--- ------------------------------------ --------------------------------
 ?I EVC_P2P_100                           100

Key: St=Status, A=Active, P=Partially Active, I=Inactive, *=Default EVC, ?=Link Down
```

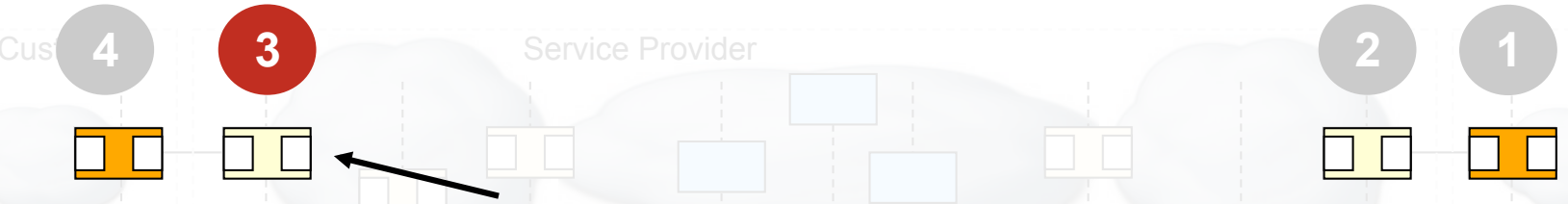
Operational Scenario 3 (cont.)

- Problem Statement

  End to End Fault Notification of service status to Customer Equipment

- Problem Solution

  IEEE 802.3ah to IEEE 802.1ag (CFM) Inter-Working (IW) for propagation of EVC status and CFM to E-LMI IW for notification to CE




```
Jan 26 03:40:36.093: %ETHER_SERVICE-6-EVC_STATUS_CHANGED: status of EVC_P2P_100 changed to InActive

uPE11#show ethernet cfm maintenance-point remote
MPID Level Mac Address    Vlan PortState InGressPort     Age(sec) Service ID
3100 4     0012.017c.3d00 100  DOWN      Gi0/16          21       customer_100_provider

uPE11#show ethernet service evc
Identifier                     Type  Act-UNI-cnt Status
EVC_P2P_100                    P-P       1       InActive

uPE11#show ethernet lmi evc
UNI Id: CE11_UNI
St  Evc Id                                 CE-VLAN
--- ------------------------------------- ---------------------------------
  I EVC_P2P_100                            100

Key: St=Status, A=Active, P=Partially Active, I=Inactive, *=Default EVC, ?=Link Down
```

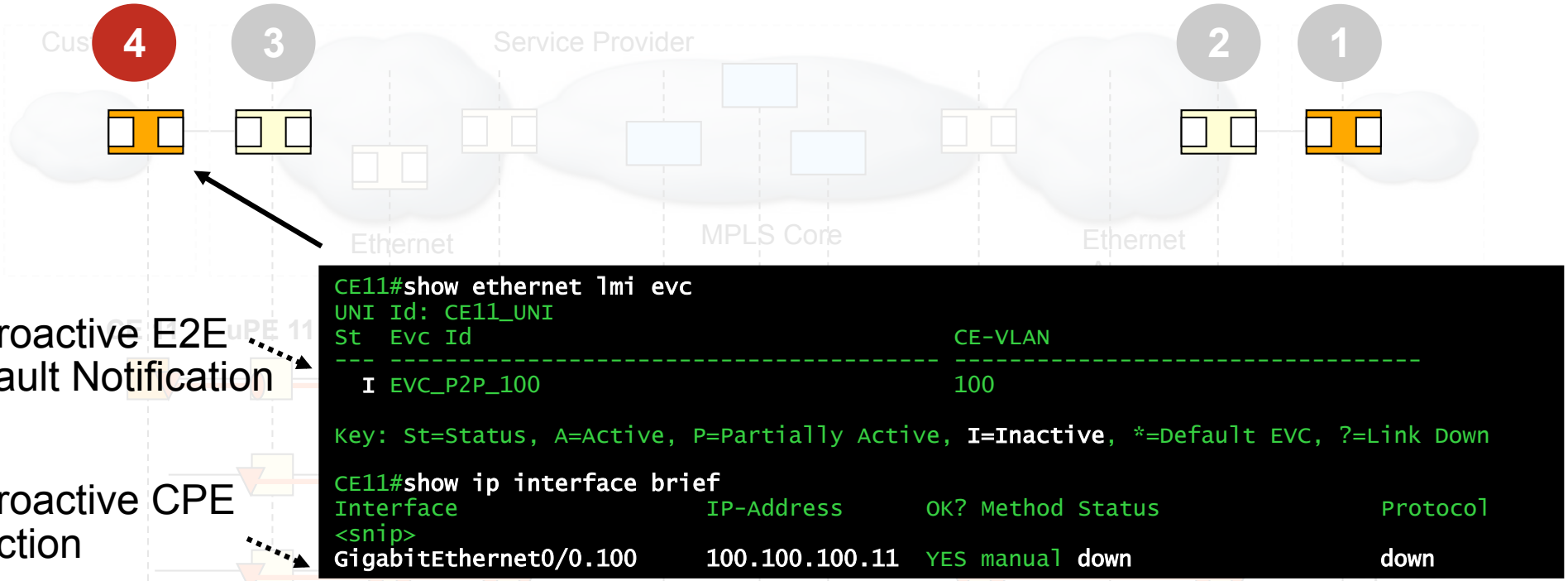
Operational Scenario 3 (cont.)

- Problem Statement

  End to End Fault Notification of service status to Customer Equipment

- Problem Solution

  IEEE 802.3ah to IEEE 802.1ag (CFM) Inter-Working (IW) for propagation of EVC status and CFM to E-LMI IW for notification to CE



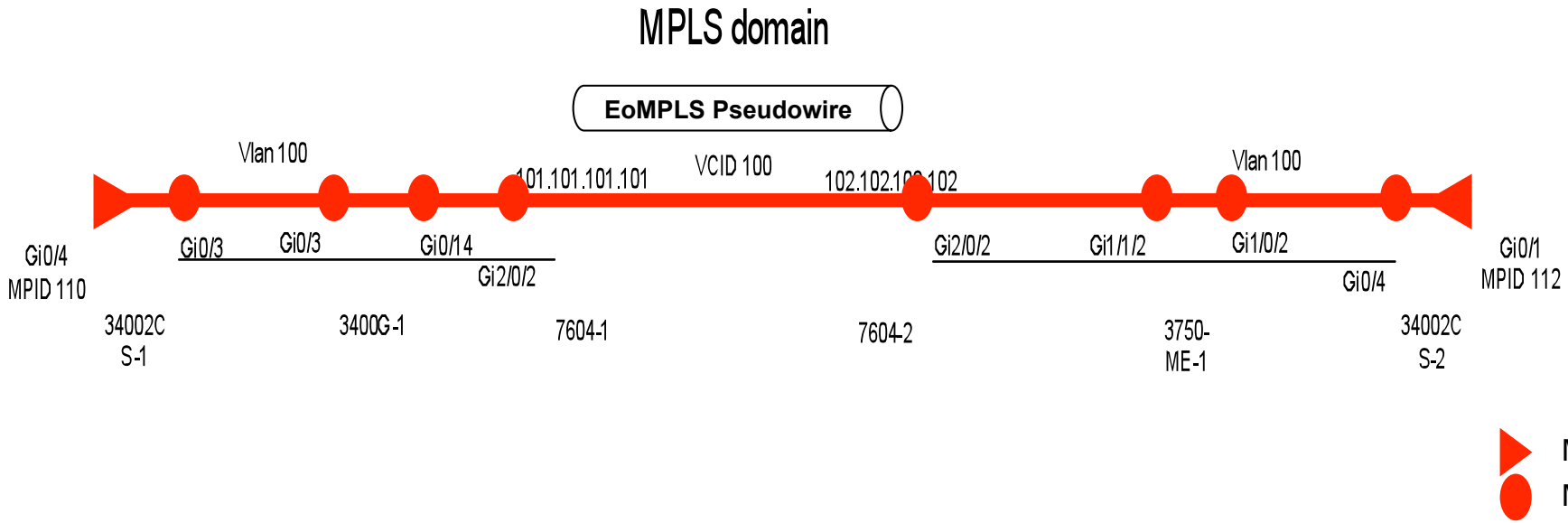
Operational Scenario 4
Ethernet and MPLS OAM

- Problem Statement

  Troubleshooting Ethernet services over MPLS

- Problem Solution

  CFM for detection, CFM and MPLS OAM for verification and isolation



MPLS OAM Summary

Testing the Pseudo-Wire

```
R1#ping mpls pseudowire <IPv4 peer addr> <VC ID>
```

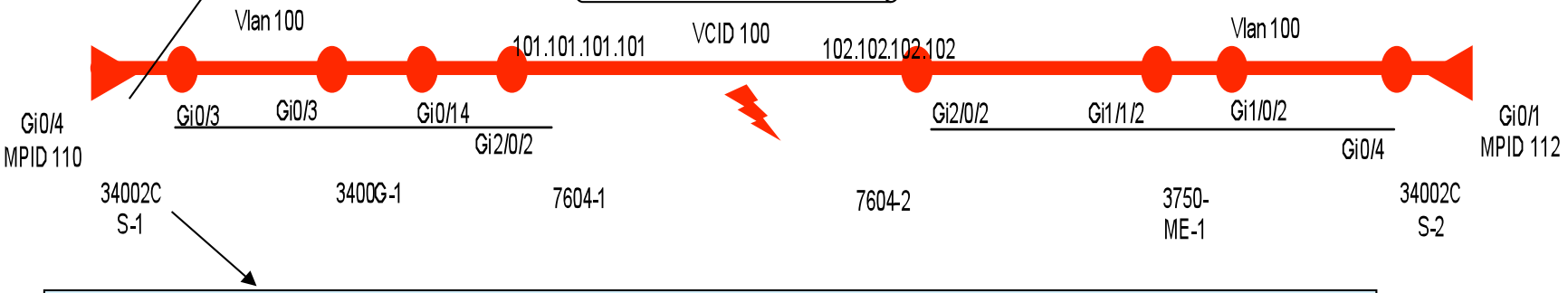
Testing the Transport LSP

```
R3#ping mpls ipv4 <IPv4 peer adr>
```

Operational Scenario 4 …Cont

Ethernet and MPLS OAM

```
Received SNMPv2c Trap:
Community: TEST
From: 127.0.0.1
sysUpTimeInstance = 668615
snmpTrapOID.0 = cEtherCfmCcMepDown
cEtherCfmEventServiceId.1.3.40 = john-p2p
cEtherCfmEventLclMacAddress.1.3.40 = 00 19 30 c0 bb 00
cEtherCfmEventLclMepCount.1.3.40 = 1
cEtherCfmEventLclIfCount.1.3.40 = 1
cEtherCfmEventRmtMepid.1.3.40 = 112
cEtherCfmEventRmtMacAddress.1.3.40 = 00 19 30 c0 ad 80
cEtherCfmEventCode.1.3.40 = 5
```




```
ME3400G-2CS-1#show ethernet cfm errors
Level Vlan MPID Remote MAC     Reason                 Service ID
5     100  112  0019.30c0.ad80 Lifetime Timer Expir john-p2p
```

Operational Scenario 4 …Cont

Ethernet and MPLS OAM

```
ME3400G-2CS-1#ping ethernet 0019.30c0.ad80 level 5 vlan 100

Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

```
ME3400G-2CS-1#traceroute ethernet 0019.30c0.ad80 level 5 vlan 100
Type escape sequence to abort. TTL 255. Per-Hop Timeout is 10 seconds
Tracing the route to 0019.30c0.ad80 on Domain TEST-jose, Level 5, vlan 100
Traceroute sent via GigabitEthernet0/3

------------------------------------------------------------------------------
                              MAC       Ingress Ingress Action    Relay Action
  Hops    Host              Forwarded   Egress  Egress Action     Next Hop
------------------------------------------------------------------------------
B 1    ME3400G-1         0019.552b.df00 Gi0/3   IngOk             RlyFDB
                         Forwarded      Gi0/14  EgrOK             7604-1
B 2    7604-1            0016.9c6e.7985 Gi2/0/2 IngOk             RlyCCDB
                         Forwarded
*
*
*
```

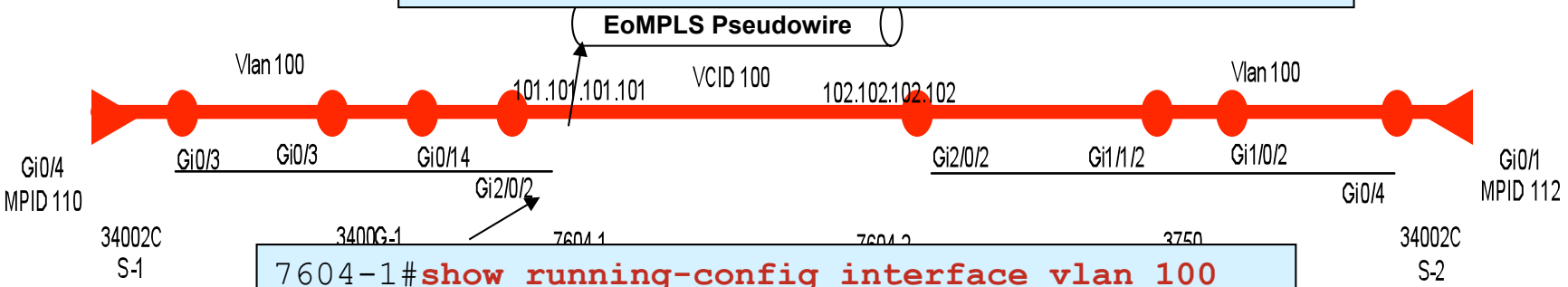
12

Operational Scenario 4 …Cont

Ethernet and MPLS OAM

```
7604-1#show running-config interface gi2/0/2
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet2/0/2
 switchport
 switchport trunk allowed vlan 100
 switchport mode trunk
 ethernet cfm mip level 5
end
```




```
7604-1#show running-config interface vlan 100
Building configuration...

Current configuration : 111 bytes
!
interface Vlan100
 ip address 10.10.10.3 255.255.255.0
 xconnect 102.102.102.102 100 encapsulation mpls
end
```

Operational Scenario 4 …Cont

Ethernet and MPLS OAM

```
7604-1#ping mpls pseudowire 102.102.102.102 100
Sending 5, 100-byte MPLS Echos to 102.102.102.102,
     timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
QQQQQ
Success rate is 0 percent (0/5)
```

Operational Scenario 4 …Cont

Ethernet and MPLS OAM

```
7604-1#ping mpls pseudowire 102.102.102.102 100
Sending 5, 100-byte MPLS Echos to 102.102.102.102,
     timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
```

```
7604-1#ping mpls ipv4 102.102.102.102/32
Sending 5, 100-byte MPLS Echos to 102.102.102.102/32,
     timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
QQQQQ
Success rate is 0 percent (0/5)
```

Summary

- You have an understanding of Ethernet OAM Protocols including CFM, Link OAM (802.3ah), Y.1731 & E-LMI
- You have the fundamental understanding of Ethernet OAM Interworking.
- You have seen how Ethernet OAM and OAM Interworking can be used to handle some common fault scenario!

Questions?

Thanks for your time & attention!

Enjoy the rest of the Program!