Introduction To L2 Transport & Tunneling Technologies
(aka L2VPN)

James Moffat

Consulting Systems Engineer

jmoffat@cisco.com

Objectives

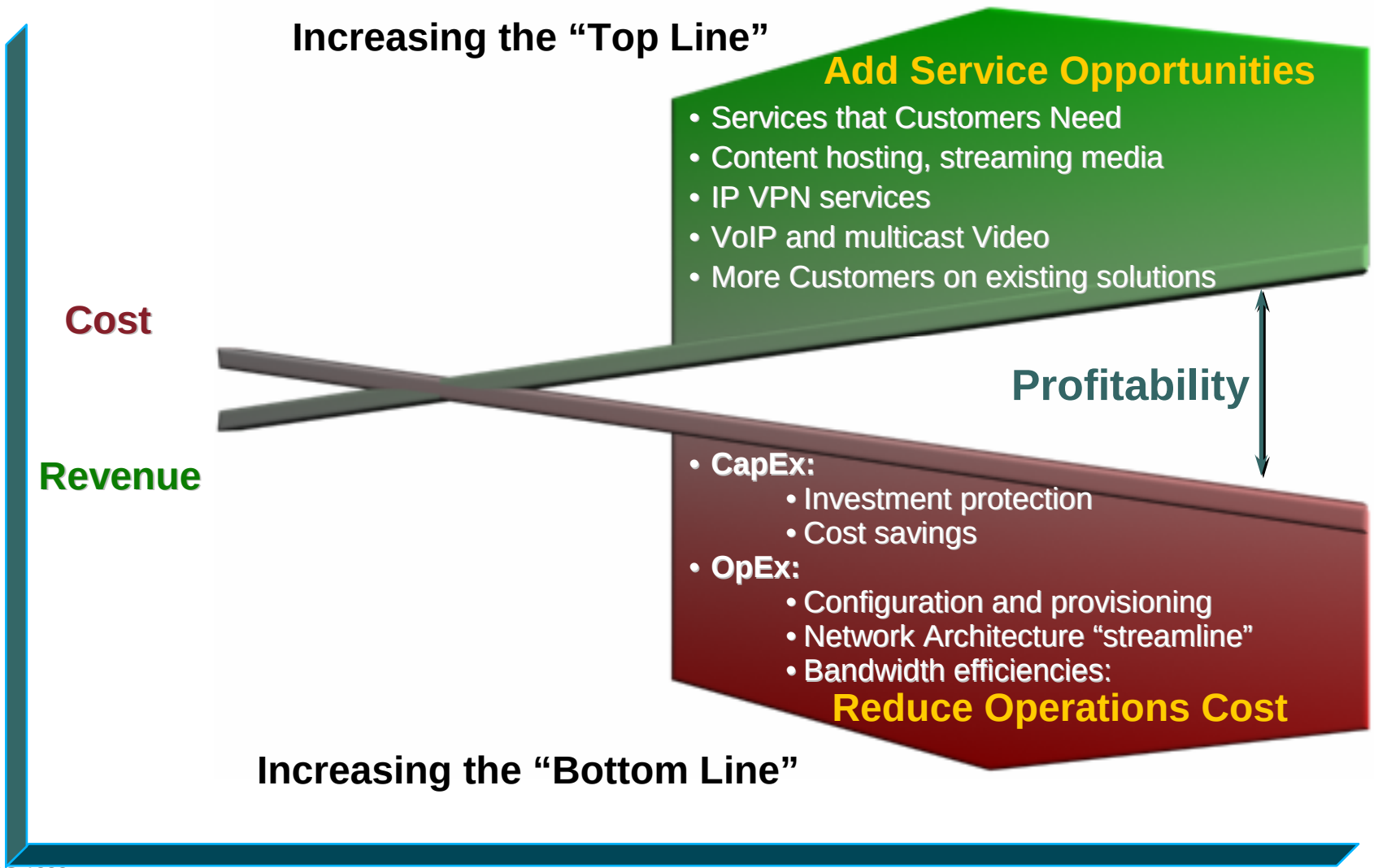
- **Define what the leading drivers for L2VPN over packet switched infrastructure are?**
- **Outline the IETF's role in L2VPN evolution.**
- **Provide a technical review of emerging L2VPN technologies for IP & MPLS cores.**
- **Demonstrate how application of L2VPNs is meeting the challenges of Service Providers.**

Agenda

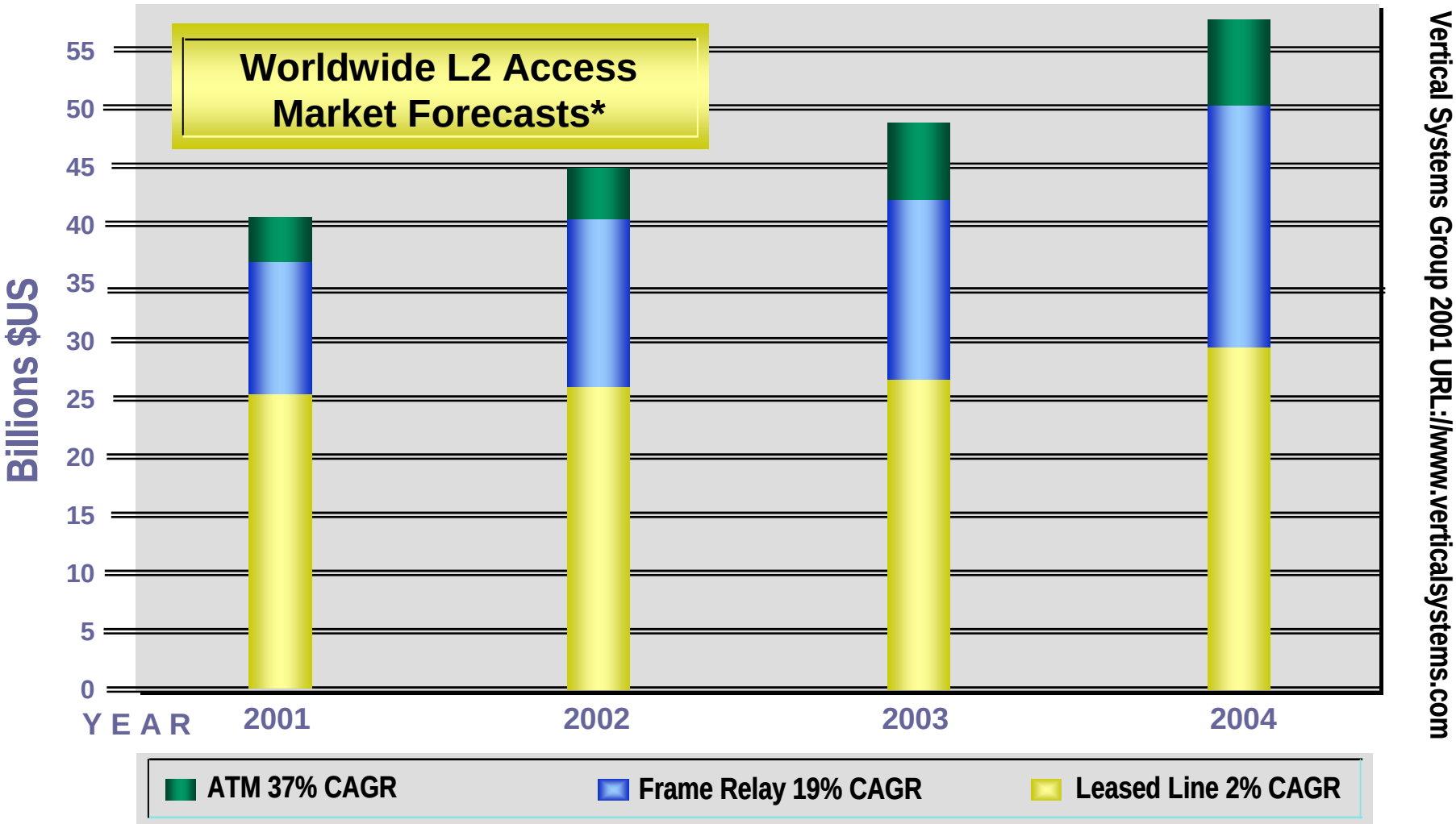
Why L2VPNs ?

- Pseudowire Overview
- Layer 2 Tunneling Protocol (L2TPv3)
- Any Transport over MPLS (AToM)
- Virtual Private LAN Services
- L2VPN Applications

Realizing profitability on IP Networks…

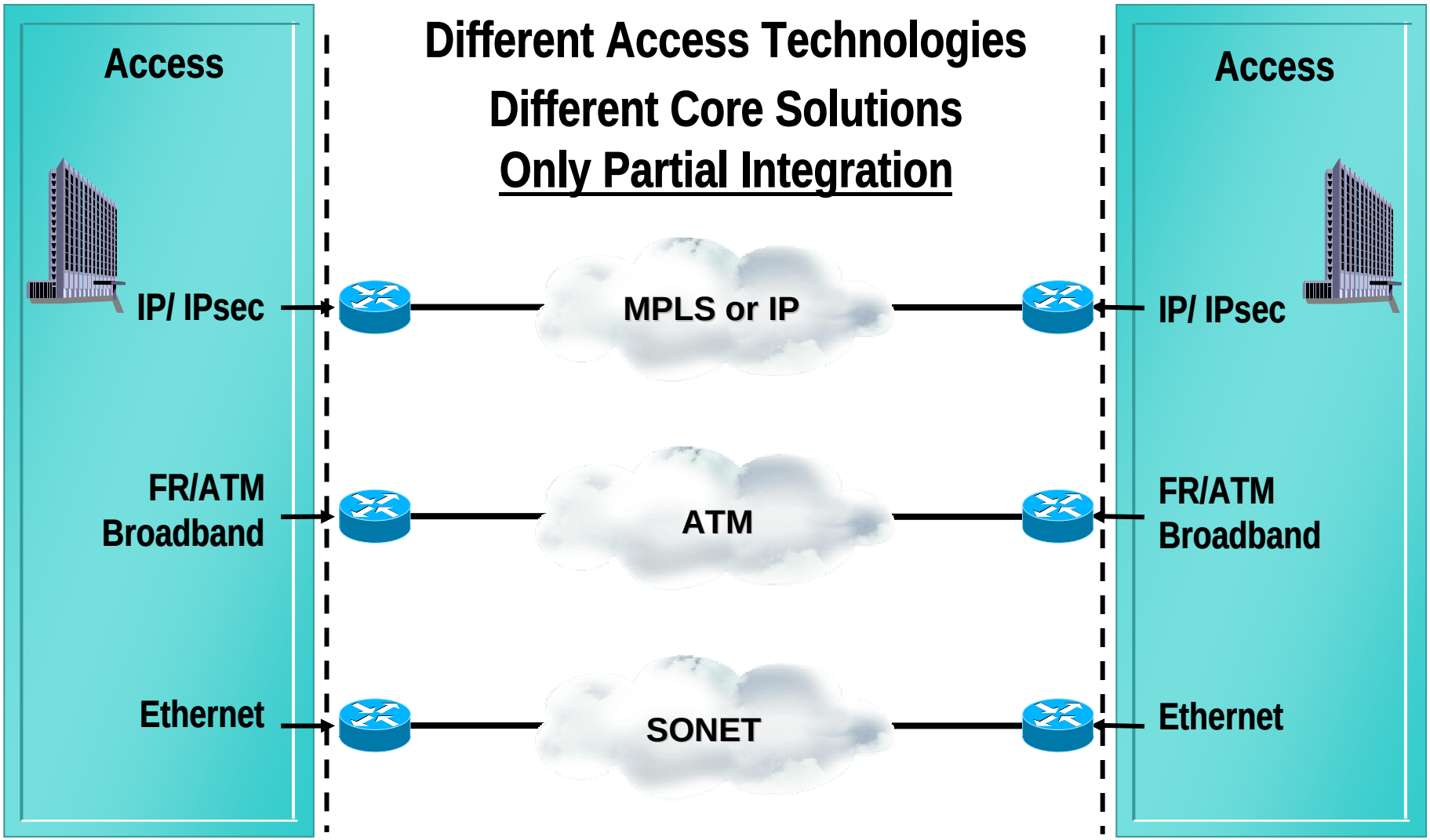


Current Major Access Methods

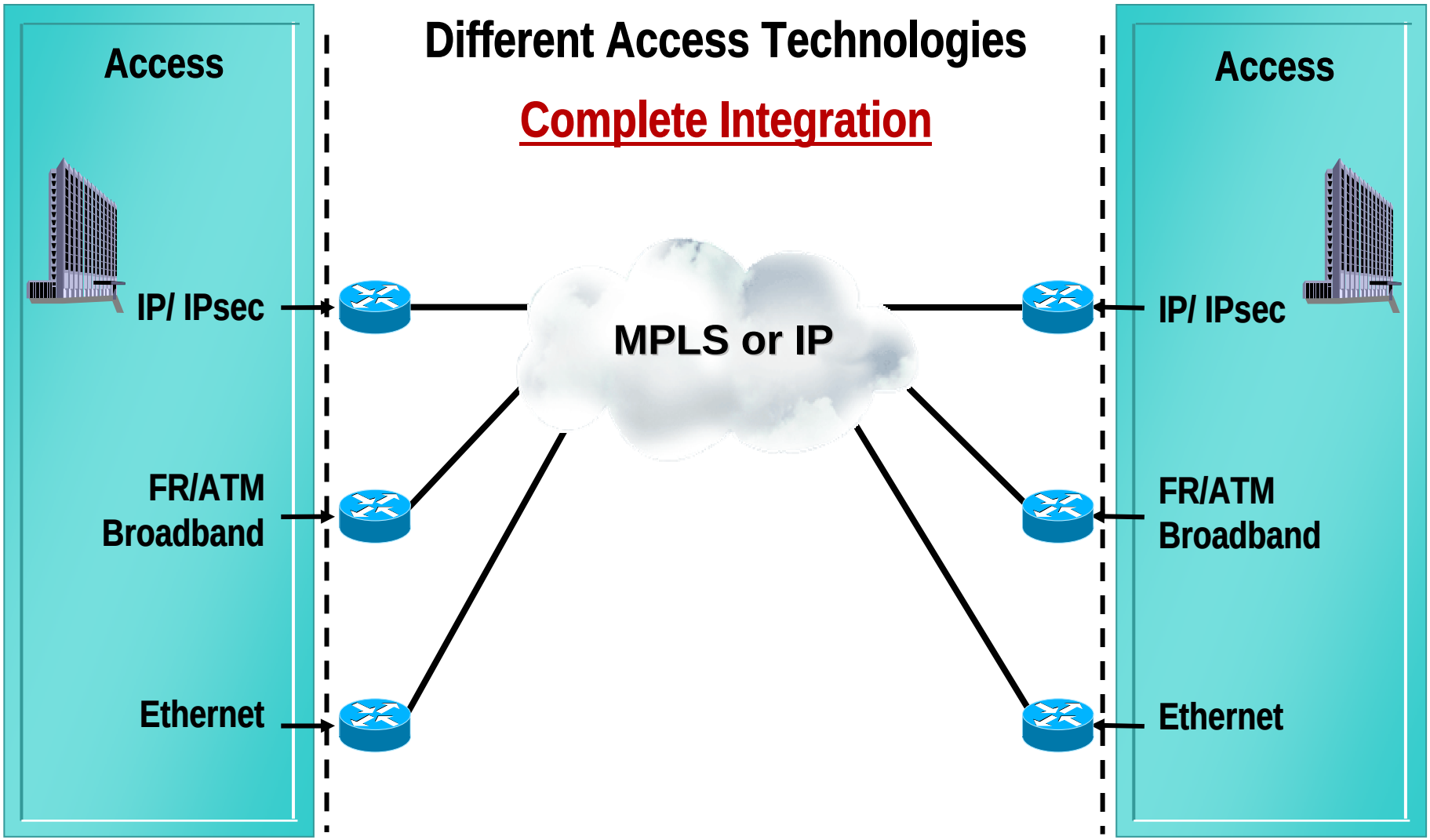


*NB. New and Emerging Access Methods e.g. Metro Ethernet, Broadband Wireless etc. not projected here but supported by Unified VPN

VPN Deployments Today: Technology & VPN Diversity



Consolidated Core – Supports…



Summary of Benefits for L2VPNs

- **New Service Opportunities**
  - **Virtual leased line Service**
  - **Offer “PVC like” Layer 2 based service**
- **Reduced Cost – Consolidate multiple core technologies into a single packet-based infrastructure**
- **Simplify Services - Layer 2 transport provide options for Service Providers who need to provide L2 connectivity and maintain customer autonomy.**
- **Protect Existing Investments - Greenfield networks to extend customer access to existing Layer 2 networks without deploying an old-world infrastructure.**
- **Feature Support – Through the use of IOS features such as IPsec, QoS and Traffic Engineering, L2 transport can be tailored to meet customer requirements**

Agenda

- Why L2VPNs ?
- **Pseudowire Overview**
- Layer 2 Tunneling Protocol (L2TPv3)
- Any Transport over MPLS (AToM)
- Virtual Private LAN Services
- L2VPN Applications

A brief word about L2 / L3 VPNs

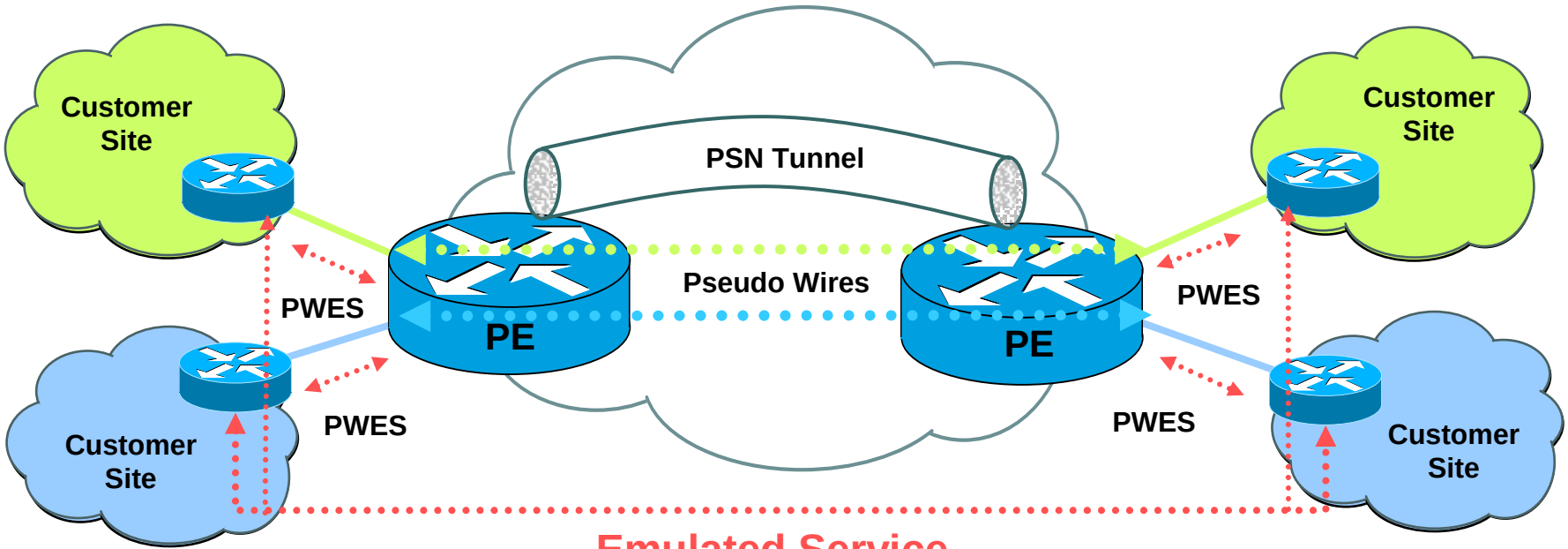
Layer 3 VPNs

- Provider devices forward customer packets based on Layer 3 information (e.g., IP)
- SP involvement in routing
- MPLS/BGP VPNs (RFC 2547), GRE, virtual router approaches

Layer 2 VPNs

- Provider devices forward customer packets based on Layer 2 information
- Tunnels, circuits, LSPs, MAC address
- "pseudo-wire" concept

Pseudo Wire Reference Model



A pseudo-wire (PW) is a connection between two provider edge (PE) devices which connects two pseudo-wire end-services (PWESs) of the same type

Service Types:

- Ethernet
- 802.1Q (VLAN)
- ATM VC or VP

PWES

- HDLC
- PPP
- Frame Relay VC

Pseudo Wire – Basic Building Blocks

Control Connection

Scale through: Session Management, Error Notification, L2 Access management interworking, etc.

Required Components

Transport Component

This is the delivery header of the encapsulated packet. This can be a Label (MPLS) or an IP Header. (Typically the IP address of the Loopback interface on Provider Edge (PE) routers.

Tunneling Component

A Unique identifier used to identify a particular circuit / port on a given PE. (VC Label or VC ID)

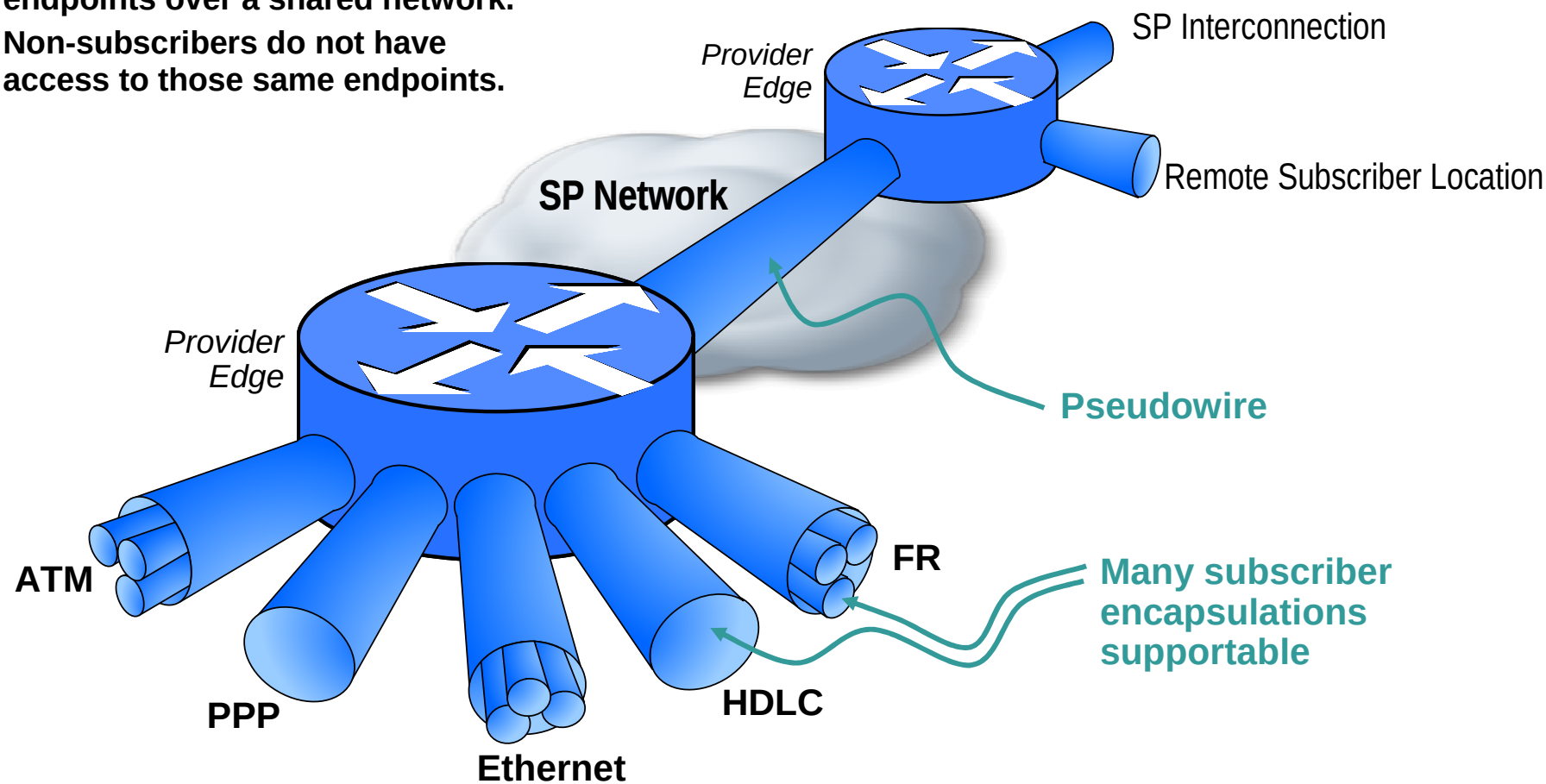
L2 PDU

The Layer 2 PDU that is the subject of transport (I.e. traffic received from the Customer Edge router, typically Ethernet, Frame Relay, HDLC frames,..etc.)

"Connectivity between PEs assumed; verified through ICMP or LSP ping."

What is an L2VPN?
IETF's L2VPN Logical Context

- **An L2VPN is comprised of switched connections between subscriber endpoints over a shared network.**
  Non-subscribers do not have access to those same endpoints.

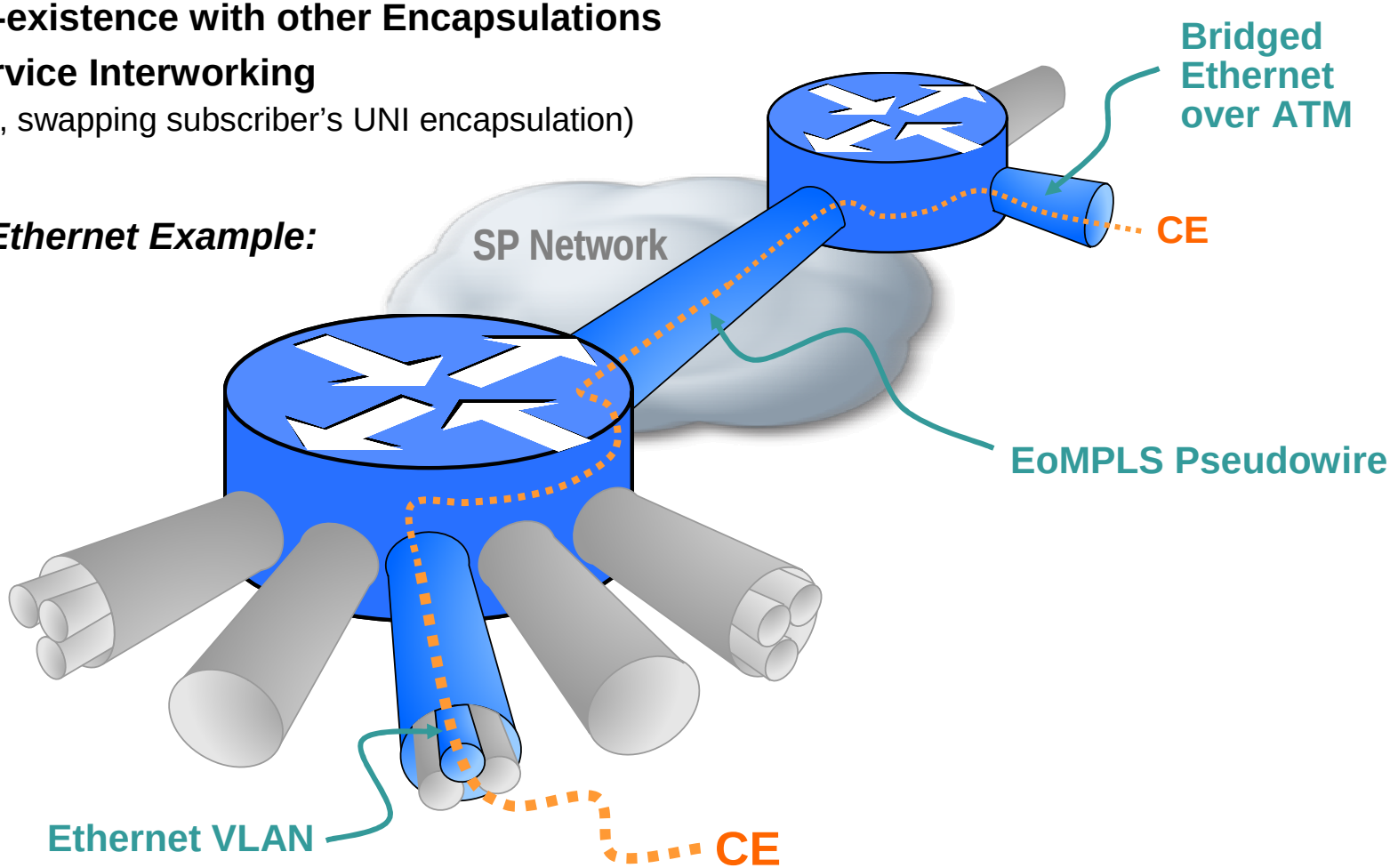


Some L1 frame encapsulations are transportable under the framework of L2VPN. This is acceptable since (unlike native L1) Frames can be dropped due to congestion.

What is an L2VPN?
Pseudowire Abstraction Enables…

- **Transport over non-Native Backbones**
- **Co-existence with other Encapsulations**
- **Service Interworking**
  (i.e., swapping subscriber's UNI encapsulation)

One Ethernet Example:



Pseudo Wire – IETF Working Groups

L2TP(v2 & v3):
- Extensions to RFC2661
- Control Plane Operation
- AVPs
- Updated data plane
- Relevant MIBs

VPLS, VPWS, IPLS:
- Solution Architectures
- PE Discovery
- Signaling (with PWE3)
- L2VPN OAM extensions
- Relevant MIBs

AToM:
- PWE3 Architecture
- PWE3 Requirements
- LDP Control Channel
- L2 Service Encap Specifics
- TDM, CES, etc.
- Relevant MIBs

IETF Standardization Activity

- **IETF working group PWE3**

  ‘Pseudo Wire Emulation Edge to Edge’;

  Requirements detailed in

  - *draft-ietf-pwe3-requirements*
  - *draft-ietf-pwe3-framework*

- **Develop standards for the encapsulation & service emulation of “pseudo wires”**

  Across a packet switched backbone

- **Focused on Point-to-Point circuit emulation**

  PSN tunnel -> GRE, MPLS, L2TP

  Service -> Ethernet, ATM, PPP, FR, HDLC and so on ..

Pseudo Wire – Cisco IETF Technology Adoption

- **Layer 2 Transport**
  - **L2TPv3**
    - *draft-ietf-l2tpext-l2tp-base*
  - **MPLS (P2P, formerly draft-martini)**
    - *draft-ietf-pwe3-control-protocol*
    - *draft-ietf-pwe3-[atm, frame-relay, ethernet, etc.]*
- **Layer 2 VPN (VPLS)**
  - *draft-ietf-l2vpn-vpls-ldp*
  - *No VPLS draft for native IP*
- **Auto-Provisioning**
  - *draft-ietf-l2vpn-signaling (BGP auto-discovery)*

Service Offerings
L2VPN Transport Services

Cisco.com

ATM

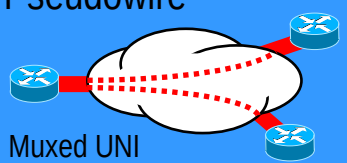
Frame Relay

Ethernet

VPWS

VPLS

AAL5 over Pseudowire



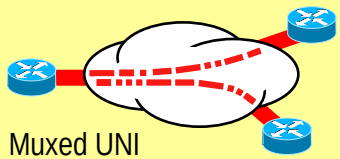
Muxed UNI

Cell Relay w/ packing over Pseudowire

Muxed UNI

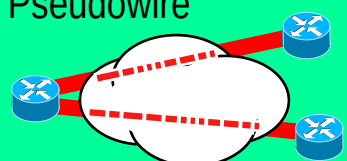
Other variants …

FR over Pseudowire



Muxed UNI

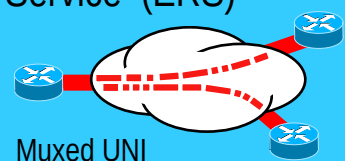
PPP/HDLC over Pseudowire



Unmuxed UNI

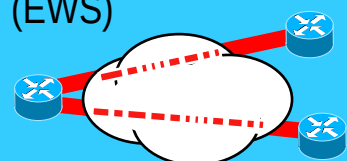
PPP/HDLC

Ethernet Relay Service (ERS)



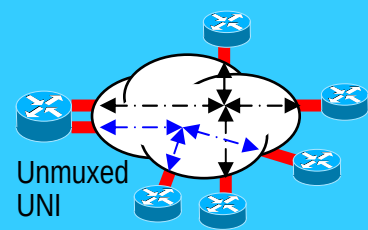
Muxed UNI

Ethernet Wire Service (EWS)



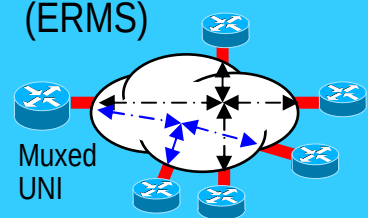
Unmuxed UNI

Ethernet Multipoint Service (EMS)



Unmuxed UNI

Ethernet Relay Multipoint Service (ERMS)

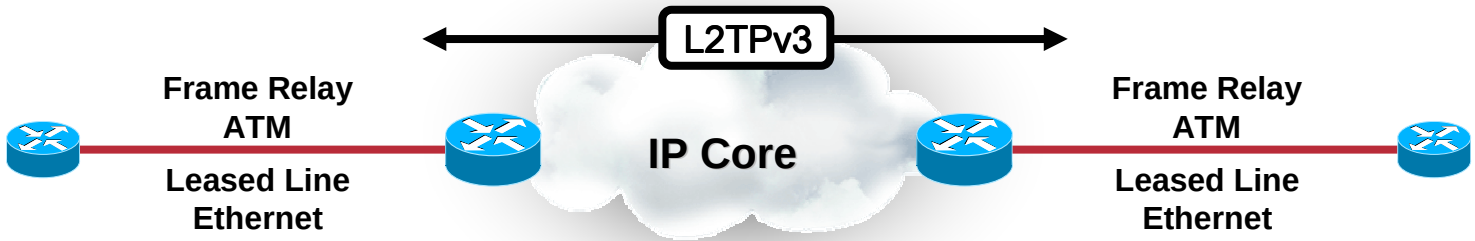


Muxed UNI

Agenda

- Why L2VPNs ?
- Pseudowire Overview
- **Layer 2 Tunneling Protocol (L2TPv3)**
- Any Transport over MPLS (AToM)
- Virtual Private LAN Services
- L2VPN Applications

Layer 2 Tunneling Protocol version 3



- L2TPv3 for customers that prefer a native IP network
- Provides ability to transport layer 2 traffic across IP packet-based core networks
- Based on a well-established lineage of protocols:
- L2TPv2 and pre-standards Cisco innovation – Universal Transport Interface (UTI)

- A standards track open architecture allows extensibility to many transport types
- Efficient header for high performance decapsulation
- Configuration on the edge routers (PEs) only!

Layer-2 Transport over IP

Control Connection

L2TP Control Connection

Used for Session ID Negotiation, Withdrawal, Error Notification

'Emulated Circuits' have 3 layers of encapsulation

Transport Component

Delivery Header (IPv4 Header)

to transport an L2 PDU from ingress to egress PE;

Comprised of IPv4 loopback addresses (DA, SA)

Tunneling Component

Demultiplexer field (L2TPv3 Header)

to identify individual circuits within a tunnel;

(4 byte Session ID + Optional 8 byte Cookie)

L2 PDU

L2 Specific Sublayer + Payload (Layer 2 PDU)

Basic Priority & Sequence Support

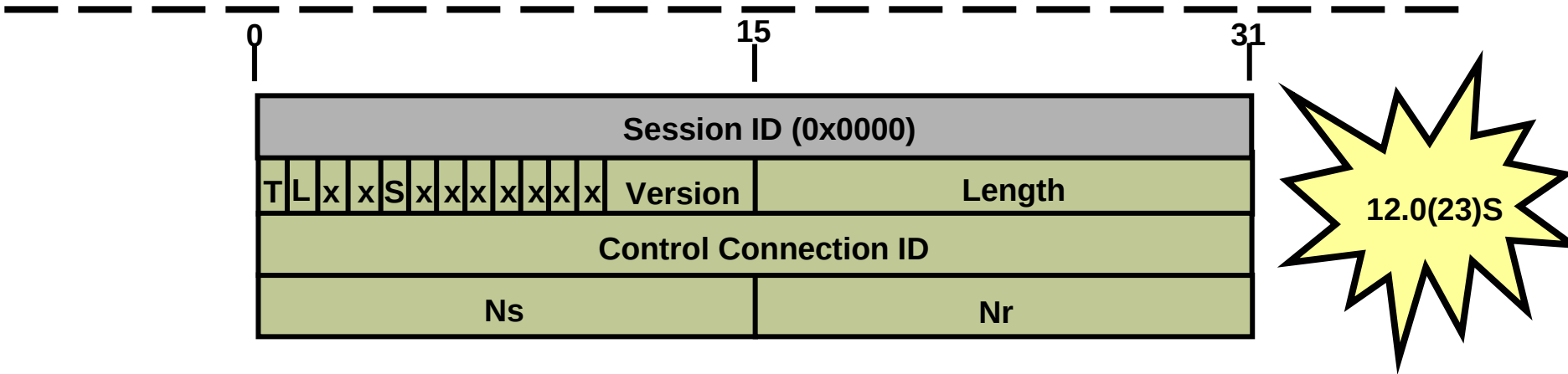
L2 Payload:ATM, HDLC, PPP, Ethernet, Frame Relay, etc.

Layer-2 Transport over IP

Control Connection

L2TP Control Channel

Session ID Negotiation, Circuit/Session Status, Error Notification, etc.



T – Set to 1, indicates this is a control message

L, S – For a control message, this must be set to 1 indicating the presence of Length & Sequence fields

x – Reserved for future extensions.

Ver – Indicates which version of L2TP is in use. This field must be set to 3.

Length – Indicates the total size of the control message in octets, starting with the T bit.

Control Connection ID – A locally significant ID, it is the peer's ID not it's own.

L2TP Control Connection Highlights

- **Dynamic Sessions**

  L2TP Control Connection and sessions for each Pseudowire are setup and torn down dynamically, no need to configure each individually.

- **"In band" Data and Control Plane**

  If the Control Connection is active, the "IP path" between L2TP Connection endpoints is likely good.

- **Keepalive**

  Hello message provides periodic keepalive, dead-peer and path detection for all sessions associated with a given Control Connection.

- **Tunnel Authentication**

  Shared-secret tunnel authentication for Control Connection

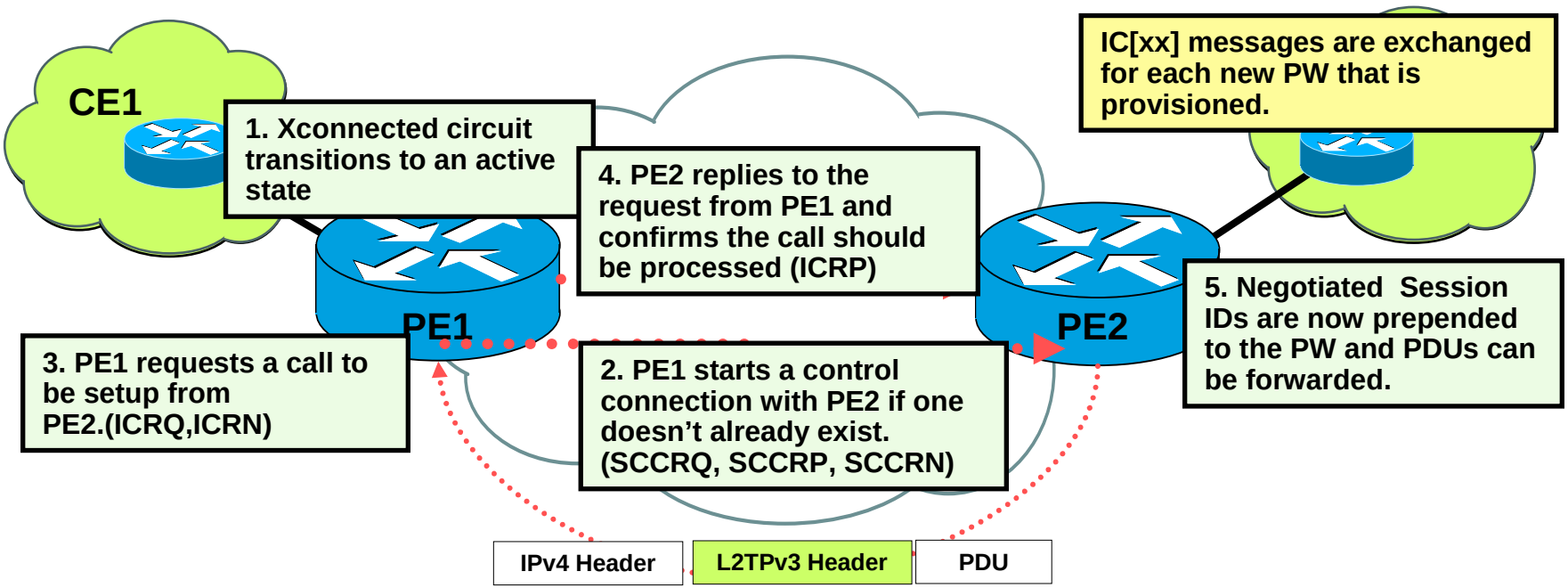
- **LMI Interworking - Circuit Status**

  Integration with various circuit LMI to provide circuit status updates without tearing down L2TP session.

Negotiating Circuit Identification – VC Information Exchange

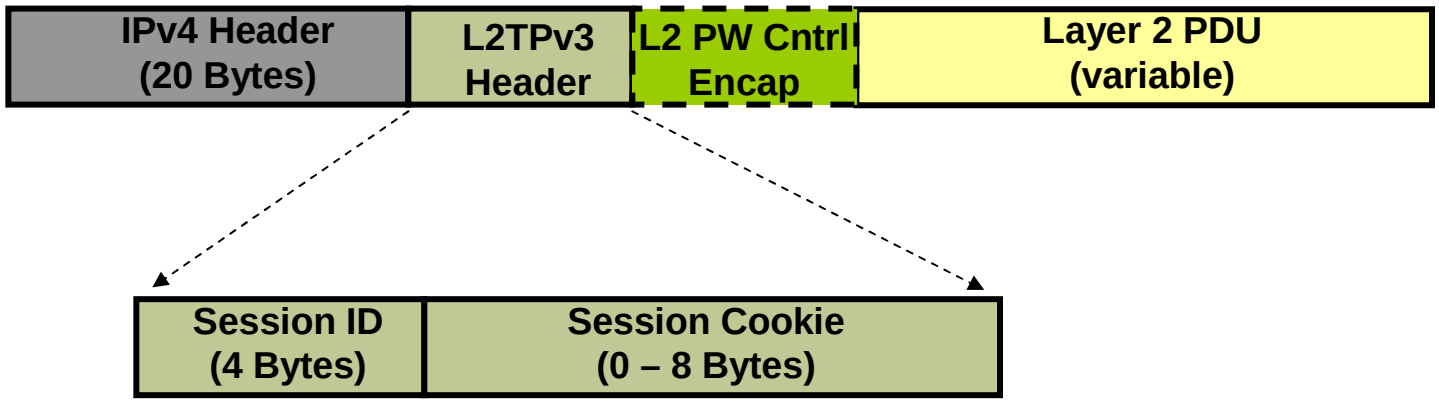
- **Optional Control Connection provides scalable session negotiation and reliable VC management**
  - Keepalive (Hellos)
  - Tunnel authentication
- **Session IDs are negotiated between L2TP Endpoints**
  - Negotiated in L2TPv3 Control Messages (ICRQ, ICRP, ICCN), and applied to L2TPv3 Data Messages
- **Attribute Value Pairs (AVPs) are used to describe the session and provide optional parameters**
  - Described in draft-ietf-l2tpext-l2tp-base-10.txt

L2TPv3 – Session Negotiation



Bi-directional Session ID exchange initiated by one of the LCCEs

L2TPv3 – Data Messages



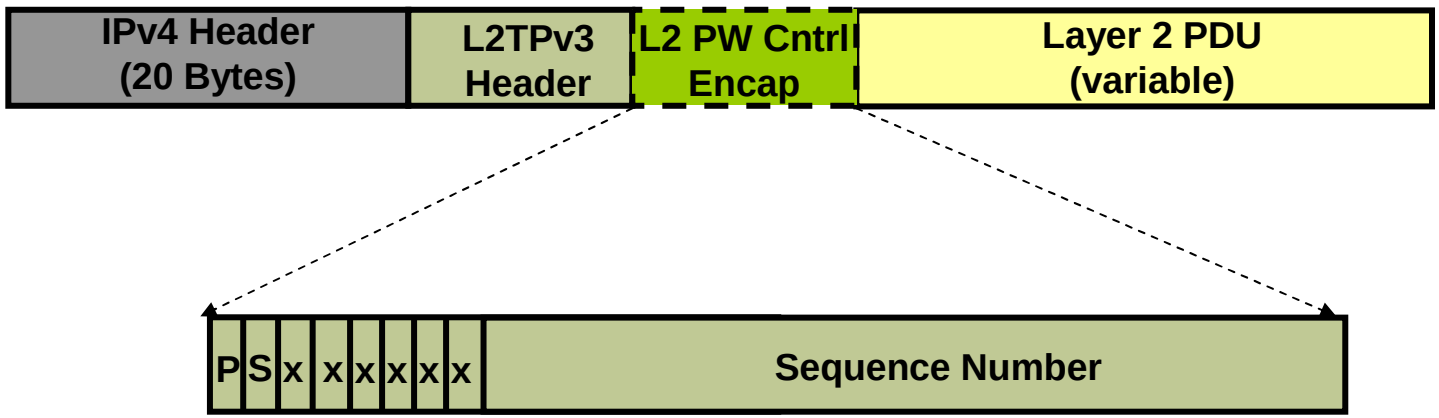
IPv4 Header - The delivery header for the Tunnel. Always destined for an LCCE.

L2TPv3 header – Consists of two parts; (1) **Session ID** used to uniquely identify the correct Session on the Remote system, and (2) the **Cookie** used as an added measure of session integrity between peers.

L2 PW Control Encapsulation - Sequence numbers, priority bits, and any additional flags needed to support the L2 emulation for the given PW type. There is a default defined in the L2TPv3 base specification, though this may vary among PW types if necessary.

Payload - Payload to be transported by L2TPv3. Typically the entire link-level frame.

Default L2-Specific Sublayer



PW emulation enhancements (optional):

(P)riority – Used to give higher priority to PW packets that shouldn't be dropped during congestion. This is not a hop-by-hop QoS bit. Per-hop QoS should utilize IP ToS (DSCP) settings.

(S)equencing - Indicates the presence of sequence numbers and can be used in services such as ATM / Frame-Relay, etc. (2^24 Looping Counter, includes 0)

(x) – Reserved

L2TPv3 – Highlights of IP Data Plane

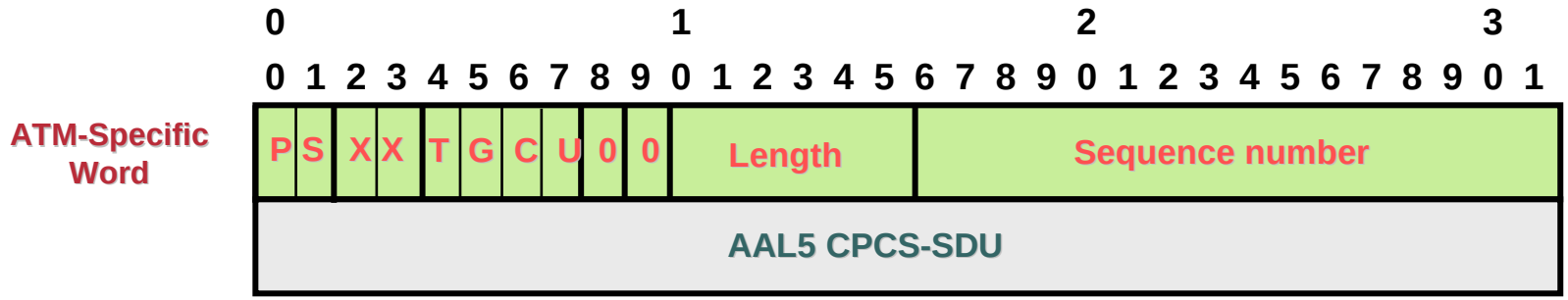
- **ICMP Data Plane Validation**
  - Simple Ping validates data path (no T-LSP validation required)
- **Path MTU**
  - Leverage the Control Plane to communicate the data plane MTU between LCCEs
  - Fragment IP packets before entering PW
- **Time-to-Live**
  - Control the scope of routable space for the L2TPv3 packets
- **Type-of-Service (DSCP)**
  - Set the Precedence bits of the encapsulating header
  - May ‘reflect’ the TOS bits from framed and tunneled IP payloads

ATM Transport over L2TPv3

- **Two main requirements for the transport of ATM across an MPLS backbone**
  - **AAL5 encapsulated frames (RFC1483)**
  - **ATM cells (cell relay)**
- **Multiple modes of operation**
  - **AAL5 Transport – VC Mode**
  - **ATM Cell Relay – VC, VP, Port Mode**
  - **Cell Packing – VC / VP / Port Mode**

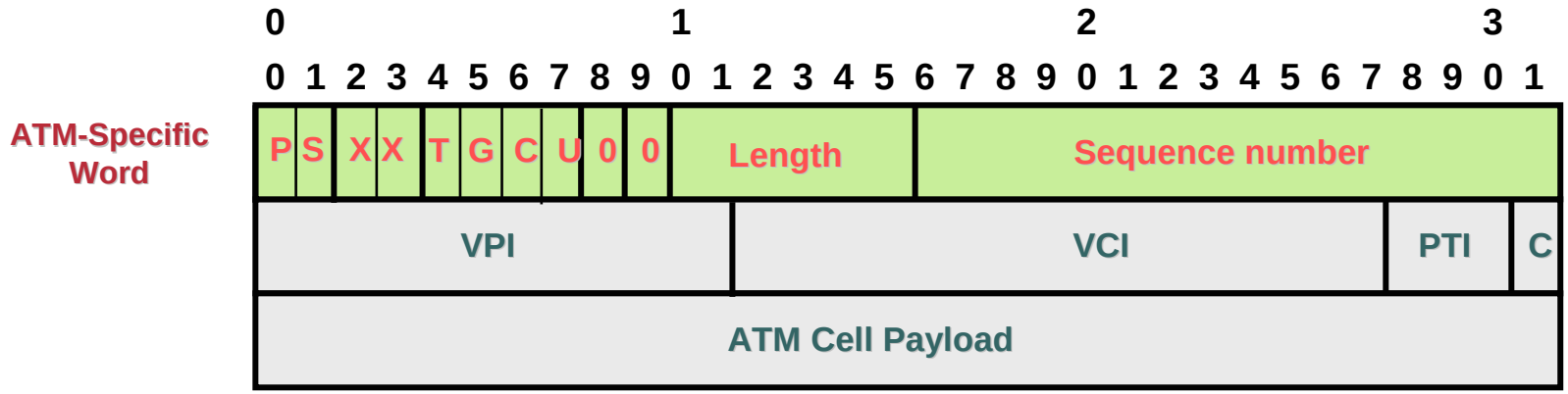
Note: Check L2VPN Roadmap for specific feature & platform support

AAL5 Encapsulation Details



- **Support AAL5 SDU Mode:**
  - Ingress port discards PAD and CPCS-PDU trailer
  - Egress port rebuilds PAD and AAL5 trailer
- **ATM-Specific Sublayer is Required (Similar to AToM)**
- **Control word flags encapsulate transport type, EFCI, CLP, C/R bit**
- **OAM emulation and transparency**
  - Emulation terminates at the local PE
  - Transparent passes OAM cells across the pseudowire

Virtual Path – Cell Relay Encapsulation Details



- Each ATM VP maps to a single L2TPv3 Session
- Support for any ATM Adaptation Layer
- F4 / F5 OAM Cells are transported transparently
- ATM-Specific Sublayer and Sequence Number
- Cell Packing Capable

ATM Transport over L2TPv3 OAM Cell Support and ILMI

- OAM emulation signaled via AVP (AAL5-SDU only)
- Pass (Transport) through supported for AAL5/CR/CP
- Emulation possible for AAL5-SDU only
- Emulation provides periodic loopback cells, AIS/RDI generation

ILMI:

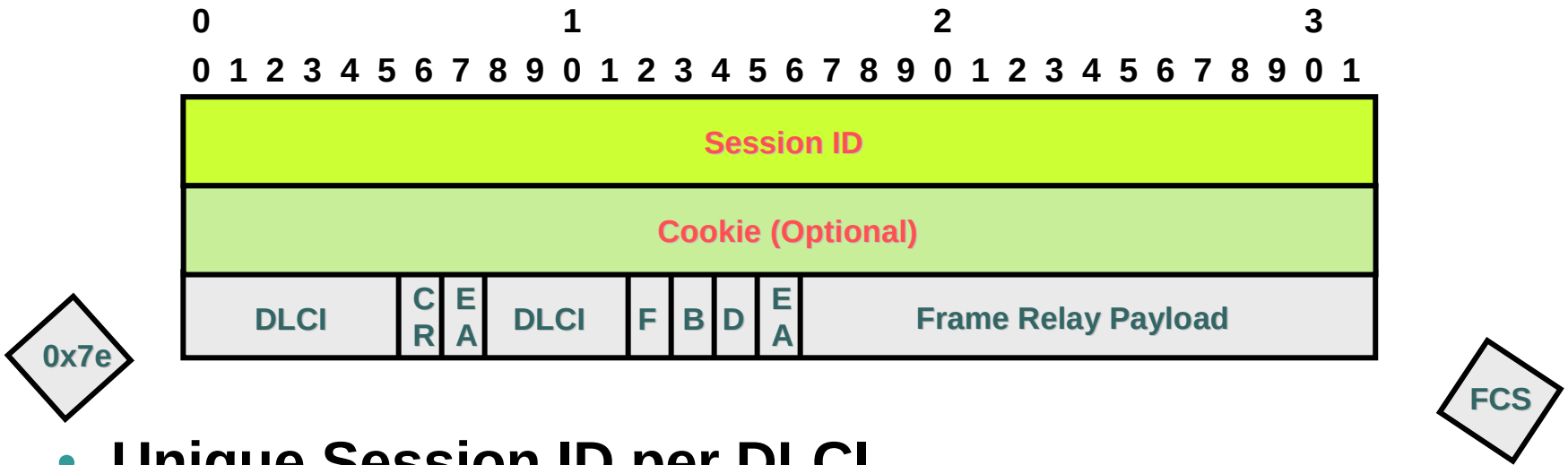
- Label withdrawal initiated if PVC goes down
- Remote CE notified via ILMI after label withdrawal

Frame Relay Transport over L2TPv3

- **Frame Relay Connection Types**
  - Port Trunking (HDLC encap, like encaps req.)
  - DLCI-to-DLCI Switching
- **Encapsulation Support**
  - Cisco, IETF (RFC1490)
  - Does not require like encaps on both sides
- **LMI Support**
  - Cisco, ANSI, Q933a
    - DLCI-to-DLCI, LMI types can differ
    - Port-to-Port, LMI must be the same

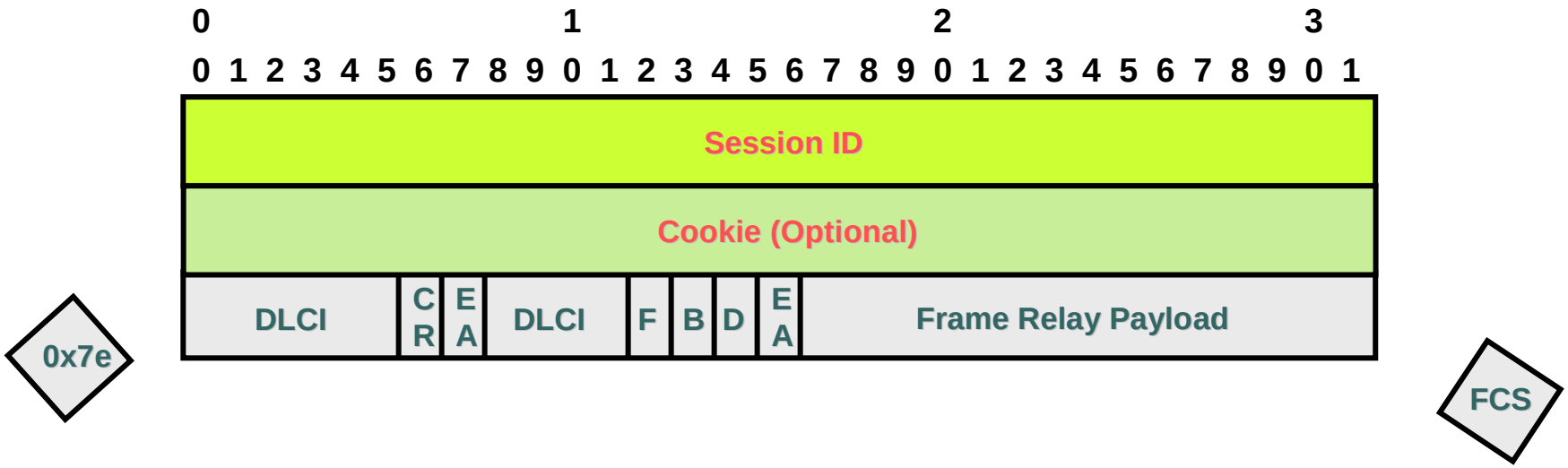
Note: Check L2VPN Roadmap for specific feature & platform support

Frame Relay Encapsulation Details DLCI to DLCI



- Unique Session ID per DLCI
- Frame Relay PDUs are transported without the start flag and Frame Check Sequence (FCS)
- Default L2-Specific sub-layer is optional
- BECN, FECN, DE & C/R bits are carried within the original frame
- DLCI value is re-written, if necessary, on egress port

Frame Relay Encapsulation Details Port Mode



- Used to trunk between switches carrying multiple PVCs
- All DLCIs on the port use the same Session ID
- VCs are not individually visible
- The L2-Specific sub-layer is optional

Frame Relay over MPLS Link Management Interface

- **For DLCI-to-DLCI mode:**

  PVC Status is conveyed with Set Link Info (SLI) messages (Active, Inactive, Deleted)

  Remote CE notified via LMI after label withdrawal

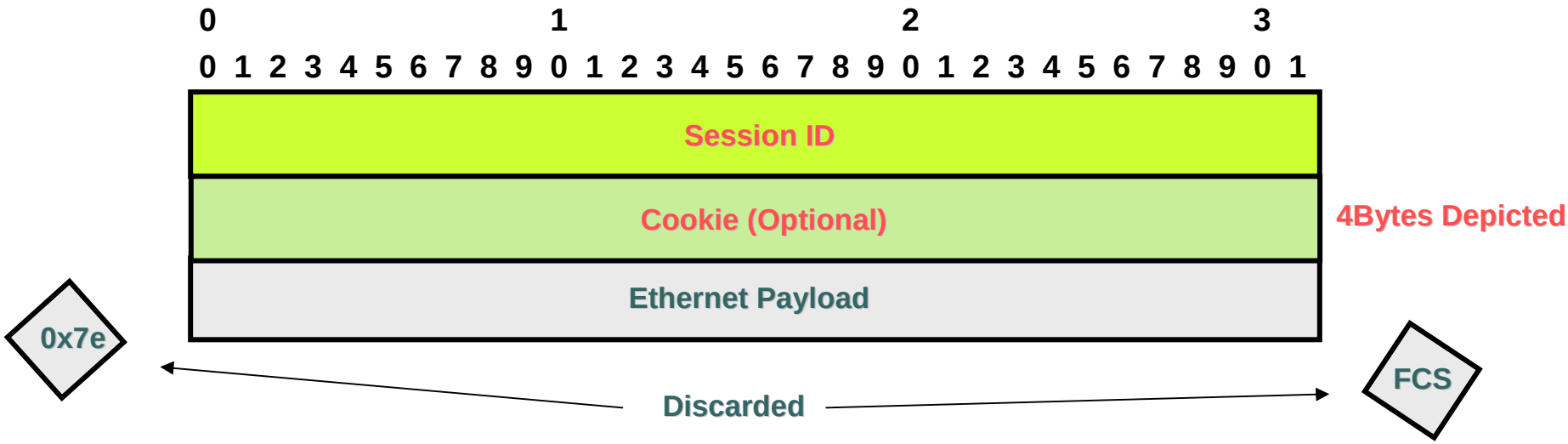
- **LMI frames transported transparently for port mode**

Ethernet Transport over L2TPv3

- **Two modes of operation**
  - **Port**
  - **VLAN**
- **Point-to-Point configuration**
- **ISL not supported**

Note: Check L2VPN Roadmap for specific feature & platform support

Ethernet Encapsulation Details



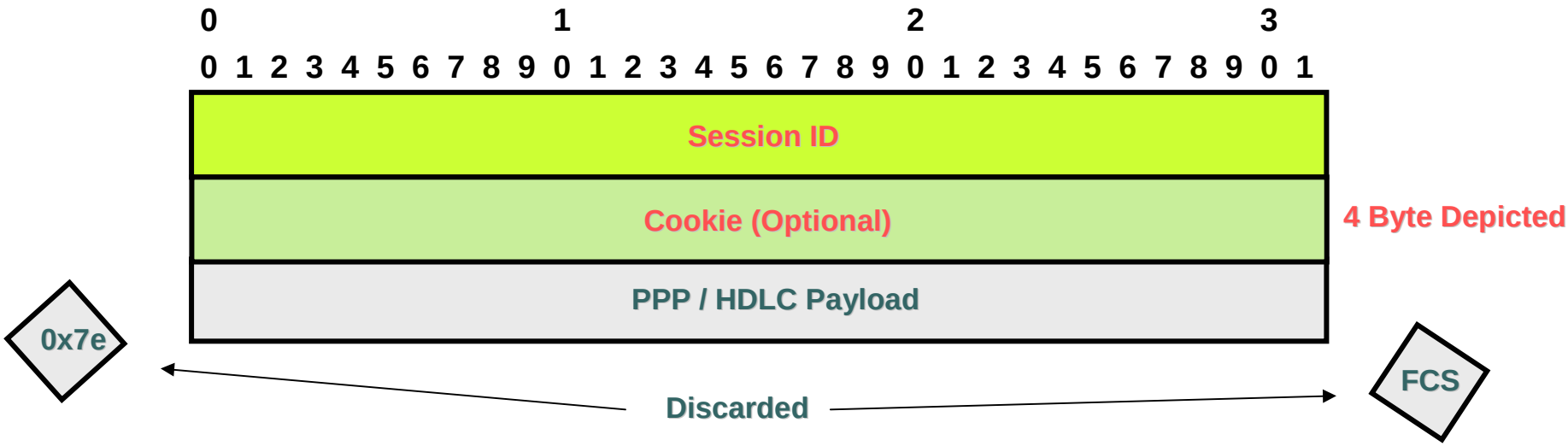
- Frame are transported without preamble and FCS
- L2-Specific sub-layer is not required
- 802.1Q tag may be rewritten in VLAN mode
- PE port requires promiscuous mode for proper operation

PPP/HDLC Transport over L2TPv3

Cisco.com

- **Simplest PW model (transparent frame pass-through)**
- **PEs do not participate in PPP negotiation**
- **ACs must have similar physical characteristics (e.g. sync / async, PPP Multilink)**

PPP/HDLC Encapsulation Details



- HDLC frames transported without frame flags and FCS
- PPP frames transported without frame flags, media-specific framing info and FCS
- The L2-Specific sub-layer is optional, may be used to ensure out-of-sequence detection

L2TPv3 – CLI Example

802.1Q VLAN over IP

```
pseudowire-class vlan-hi-priority
 encapsulation l2tpv3
 ip local interface Loopback0
 ip pmtu
 ip tos value 5
!
interface loopback 0
 ip address 172.18.255.1 255.255.255.255
!
interface FastEthernet5/1.150
 encapsulation dot1Q 150
 xconnect 172.18.255.3 150150 pw-class vlan-hi-priority
```

L2TPv3 – Summary

- L2TPv3 is used for the point to point transparent transport of Layer 2 PDUs across and native IP cores.
- L2TPv3 uses control messages (ICRQ, ICRP, etc.) to negotiate Session IDs and session specific AVPs
- L2TPv3 can use an optional L2-Specific sub-layer to preserve ensure out-of-sequence detection and discard
- L2TPv3 provides interworking with native service management protocols to maintain VC status via SLI messages (ex. LMI, ILMI, etc.)

Agenda

- Why L2VPNs ?
- Pseudowire Overview
- Layer 2 Tunneling Protocol (L2TPv3)
- **Any Transport over MPLS (AToM)**
- Virtual Private LAN Services
- L2VPN Applications

AToM
Any Transport Over MPLS

Layer 2 Transport for MPLS Networks

HDLC/PPP

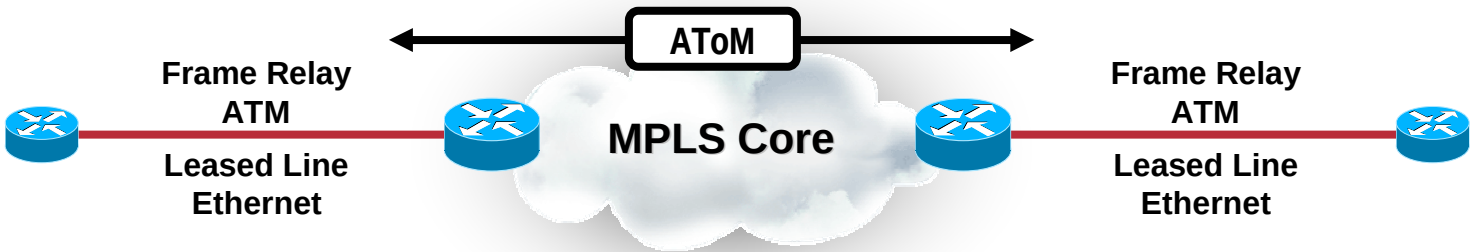
Frame Relay

Ethernet

802.1Q

ATM AAL5 & Cell Relay

Any Transport over MPLS (AToM)



- Provides ability to transport layer 2 traffic across MPLS packet-based core networks, extending the richness of MPLS capabilities to L2 VPNs
- A scalable architecture that supports the multiplexing of subscriber connections
- A standards track open architecture allows extensibility to many transport types
- Designed for Any-to-Any connectivity
- Service Provider does not participate in customer routing
- Allows Service Providers to combine with Cisco IOS QoS and MPLS Traffic Engineering to provide “Virtual leased line” like services

Layer-2 Transport across MPLS

- **Two relevant drafts by Luca Martini**
  - ***draft-ietf-pwe3-control-protocol***

    describes label distribution mechanisms for VC labels
    - *draft-ietf-pwe3-atm-encap, draft-martini-ppp-hdlc-encap-mpls*
    - *draft-ietf-pwe3-ethernet-encap, draft-ietf-pwe3-frame-encap, etc.*

    describes emulated VC encapsulation mechanisms

Control Plane

Data Plane

- **Layer 2 Transport Options:**
  - **Frame Relay**
  - **ATM AAL5 & ATM Cell Relay**
  - **Ethernet, 802.1q (VLAN)**
  - **POS**
  - **TDM, Cisco HDLC & PPP**

Layer-2 Transport across MPLS

Control Connection

Directed LDP

Used for VC-Label Negotiation, Withdrawal, Error Notification

'Emulated Circuits' have 3 layers of encapsulation

Transport Component

Tunnel Header (Tunnel Label)

to get PDU from ingress to egress PE;

MPLS LSP derived through LDP or RSVP-TE

Tunneling Component

Demultiplexer field (VC Label)

to identify individual circuits within a tunnel;

could be an MPLS label, L2TPv3 header, GRE Key, etc.

L2 PDU (Emulated)

Emulated VC encapsulation (Control Word)

information on enclosed Layer-2 PDU;

implemented as a 32-bit control word

AToM Control Connection Highlights

- **Dynamic Sessions**
  - Directed LDP control connection negotiates VC-Labels dynamically
  - Pseudowire are setup and torn down dynamically
- **Reliable Control Plane**
  - TCP based control connection allows for guaranteed, sequenced delivery of control messages
  - LDP Hellos used for dead peer detection (targeted is a 45sec holdtime)
- **LMI Interworking - Circuit Status**
  - Integration with native service circuit management provides a means for circuit status updates without tearing down AToM pseudowire.

Negotiating Circuit Identification – VC Information Exchange

- **VC labels are exchanged across a directed LDP session between PE routers**

  Carried in Generic Label TLV within LDP Label Mapping Message (RFC3036 -LDP)

- **New LDP FEC element defined to carry VC information**

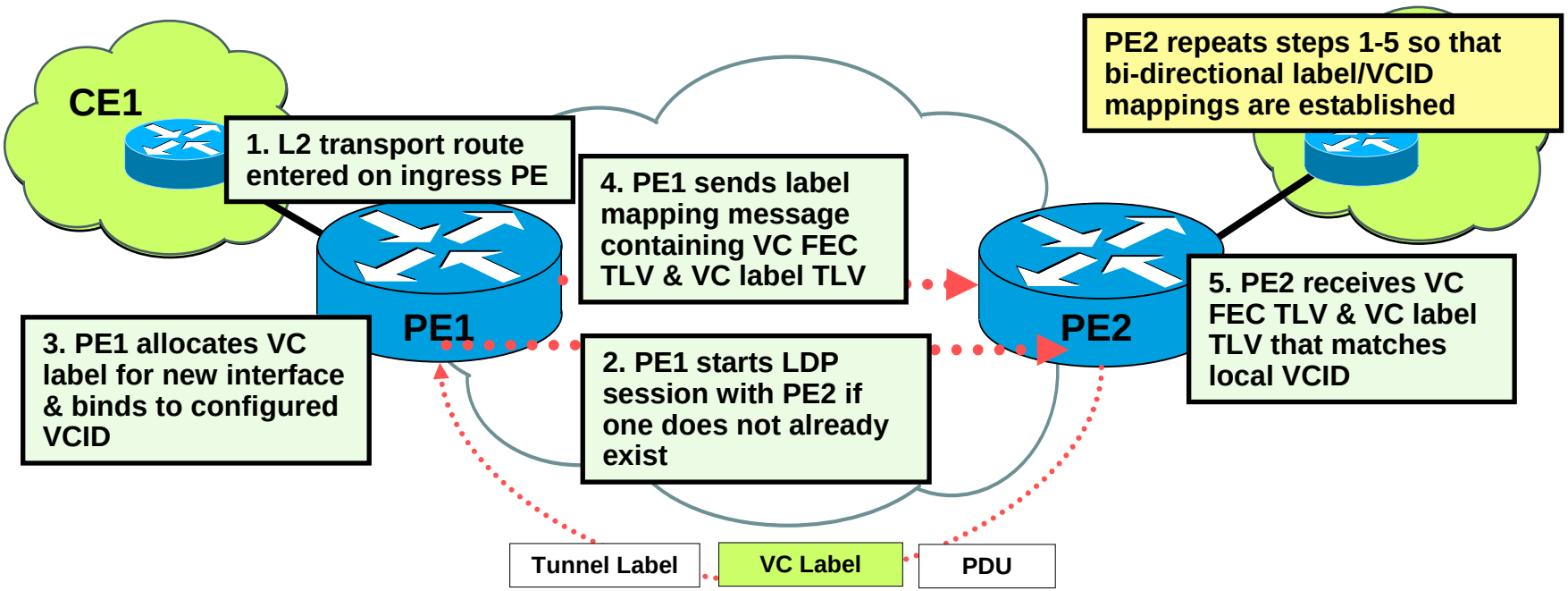
  FEC element type ‘128 – Virtual Circuit FEC Element’;

  Carried within LDP Label Mapping Message

- **VC information exchanged using Downstream Unsolicited label distribution procedures**

  Described in draft-martini-l2circuit-trans-mpls

AToM – Label Mapping Exchange



Bi-directional Label / VCID mapping exchange

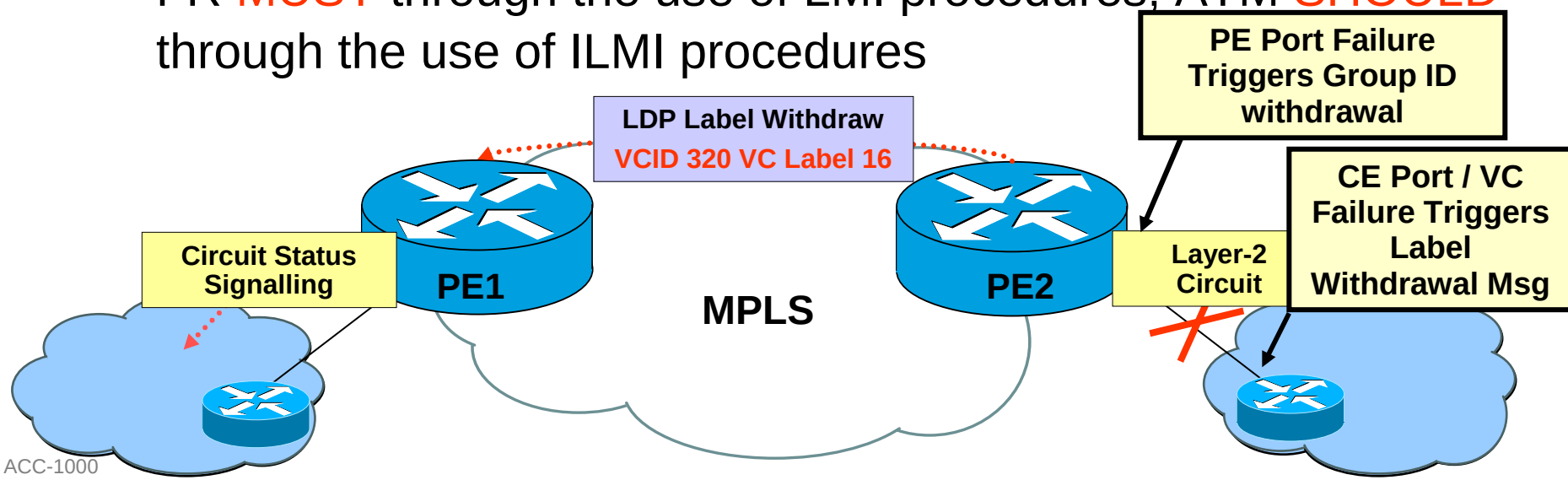
VC Label Withdrawal Procedures

- **If a PE router detects a condition that affects normal service it MUST withdraw the corresponding VC label**

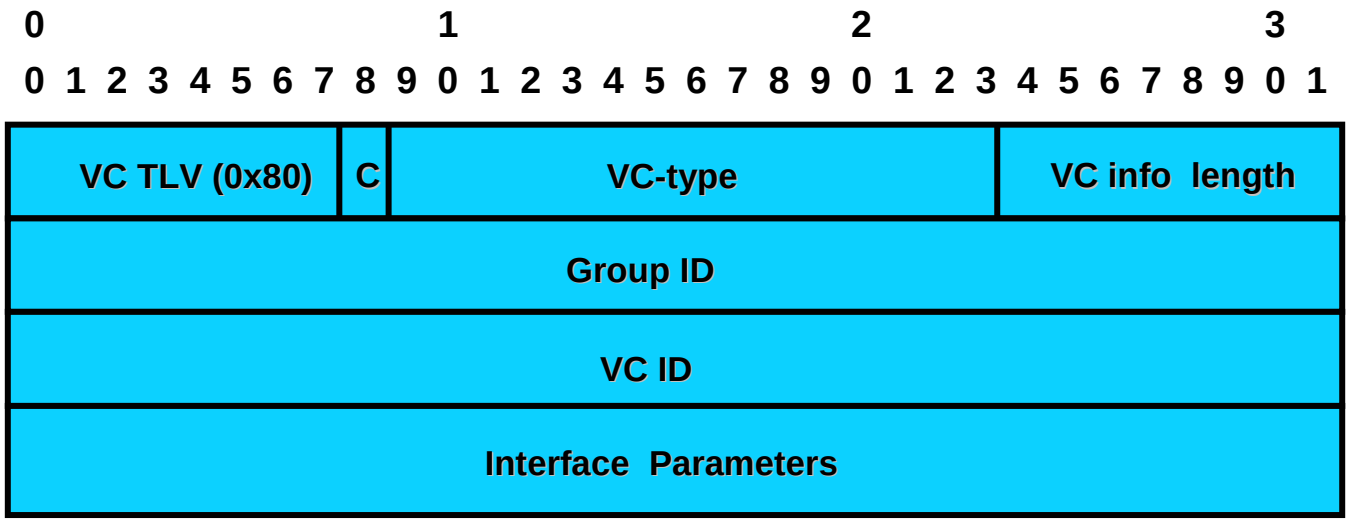
  Through the use of LDP signalling

- **A PE router may provide circuit status signalling**

  FR MUST through the use of LMI procedures; ATM SHOULD through the use of ILMI procedures



Virtual Circuit FEC Element



C: Control Word (1 bit) – Control word present if bit set

VC-type (15 bits) - Type of VC e.g FR, ATM, VLAN, Ethernet, PPP, HDLC

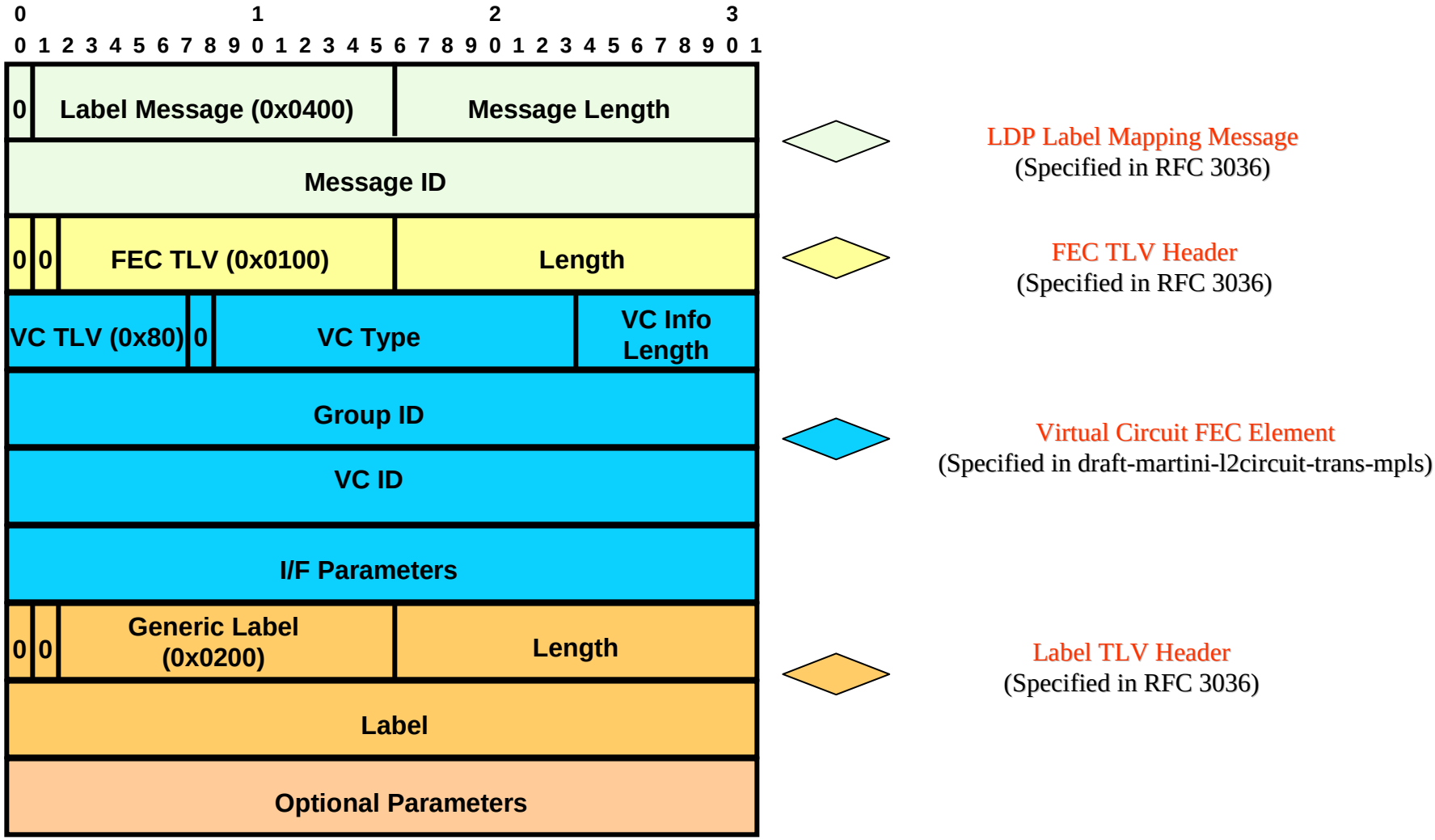
VC info length (8 bits) – Length of VCID field and interface parameters

Group ID (32 bits) – Represents a groups of VCs. Can be used for mass label withdrawal

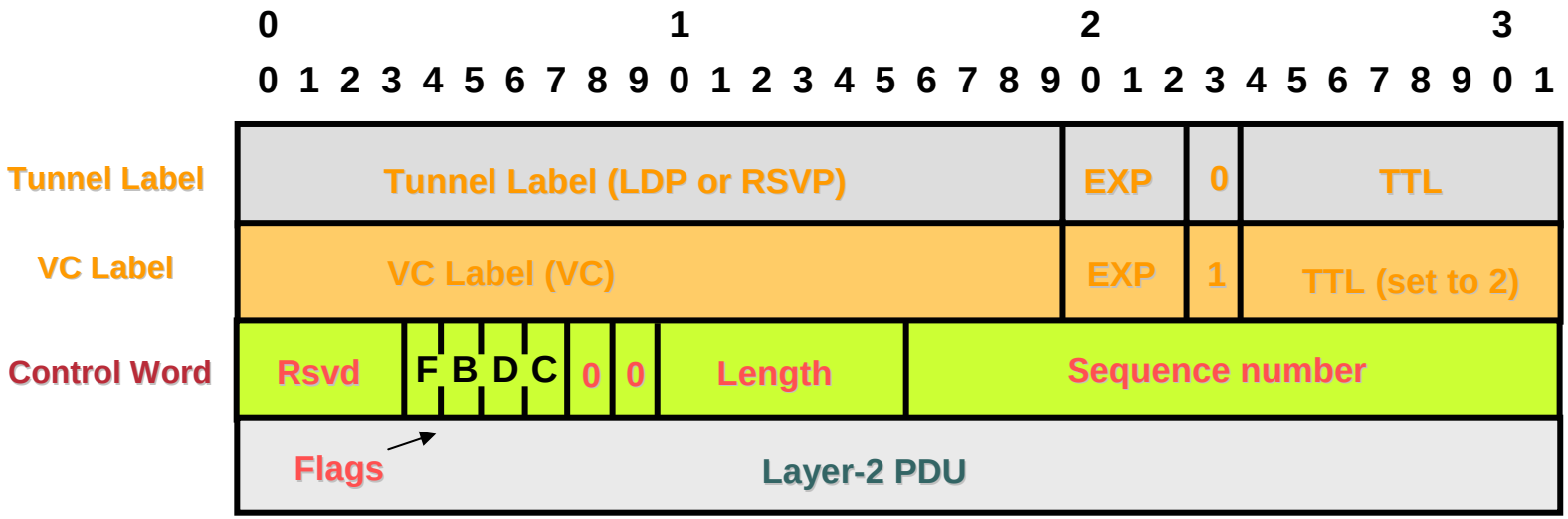
VC ID (32 bits) – Connection identifier used in conjunction with the VC-type to identify a particular VC

Interface Parameters (Variable) – Edge facing interface parameters, such as MTU

VC Label Mapping – Composition



Layer-2 Transport Control Word



When transporting layer-2 protocols over an IP or MPLS backbone:

- The sequence of the packets may need to be preserved;
- Small packets may need to be padded if the minimum MTU of the medium is larger than actual packet size;
- Control bits carried in header of Layer-2 frame may need to be transported

Control Word	
Encap.	Required
CR	No
AAL5	Yes
Eth	No
FR	Yes
HDLC	No
PPP	No

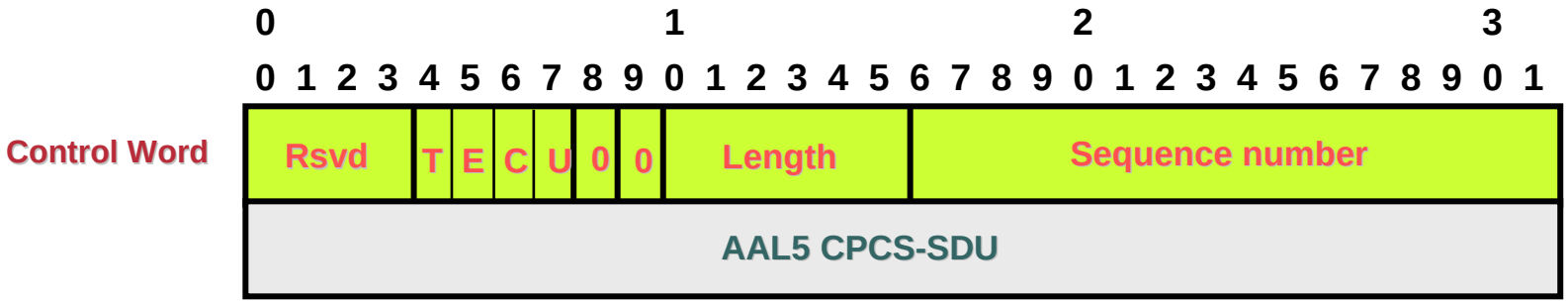
Highlights of AToM Data Plane

- **MPLS-QoS**
  - **Offer service differentiation through multi-class policies**
  - **Set EXP bits in VC & Tunnel Labels based on ingress IP DSCP, 802.1p, FR-DE, ATM-CLP, etc.**
- **MPLS-TE**
  - **Use MPLS-TE for bandwidth protection and enable “tight SLA”**
  - **Use tunnel selection to choose which path traffic will traverse**
  - **Fast Reroute (FRR) allows link and node protection for pseudowires providing quick recovery times around network failures**

ATM Transport over MPLS

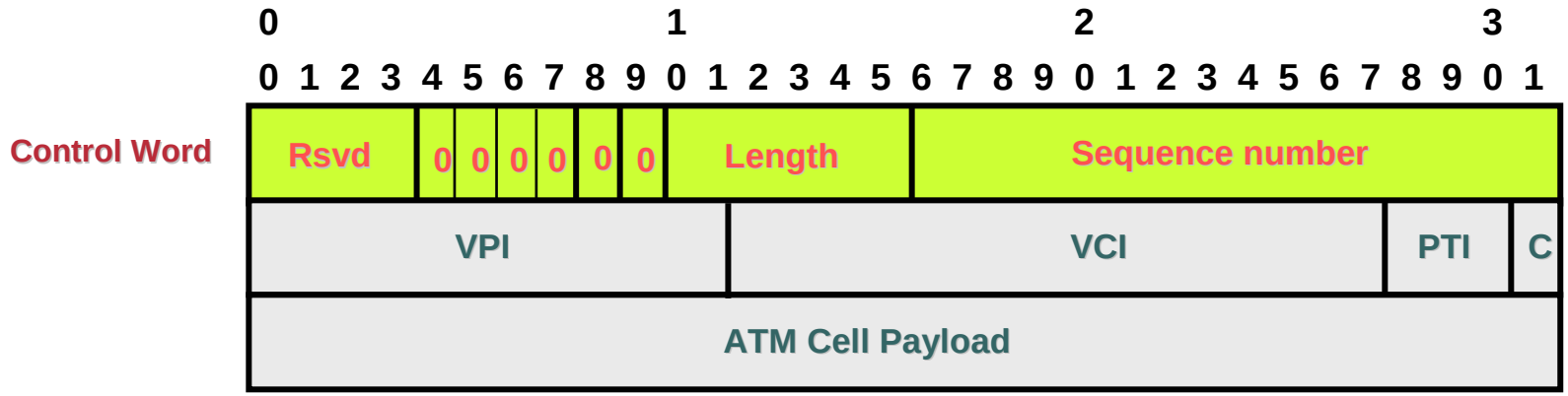
- **Two main requirements for the transport of ATM across an MPLS backbone**
  - **AAL5 encapsulated frames (RFC1483)**
  - **ATM cells (cell relay)**
- **Multiple modes of operation**
  - **AAL5 Transport – VC Mode**
  - **Cell Relay – VC / VP / Port Mode**
  - **Cell Packing – VC / VP Mode**

AAL5 Encapsulation Details



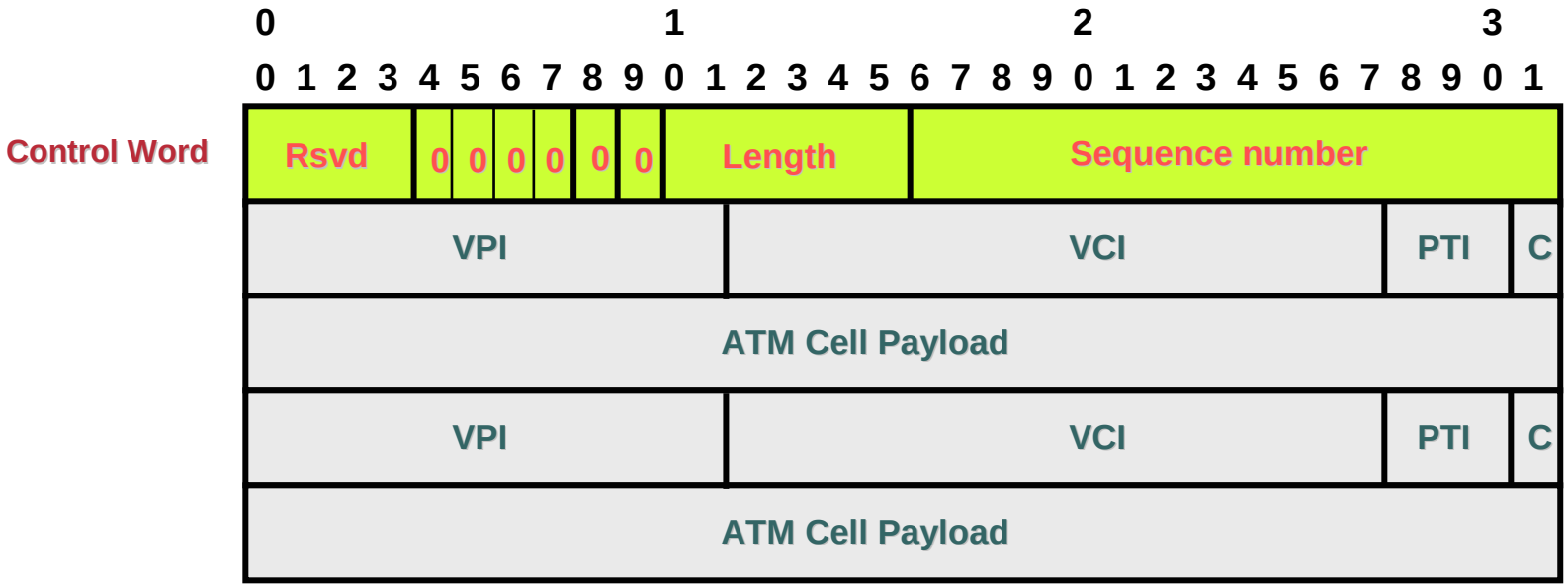
- AAL5 SDUs are encapsulated
- Control word is required
- Control word flags encapsulate transport type, EFCI, CLP, C/R bit
- Service allows transport of OAM and RM cells

Cell Relay Encapsulation Details



- **Single cell is encapsulated**
- **Control word is optional**
- **Control word flags should be set to zero and ignored**

Cell Packing Encapsulation Details



- Multiple cells are packed per MPLS packet
- All cells must belong to the same VC / VP
- Packing controlled by max number of cells and timer
- Control word is optional

ATM Transport over MPLS
OAM Cell Support and ILMI

- Transport supported for AAL5/CR/CP
- Always encapsulated in single packet
- Emulation possible for AAL5 transport
- Emulation provides periodic loopback cells, AIS/RDI generation
- Label withdrawal initiated if PVC goes down
- Remote CE notified via LMI after label withdrawal

Frame Relay Transport over MPLS

Frame Relay Connection Types:

- **Port to Port Switching (HDLC encap)**
- **DLCI-to-DLCI Switching**

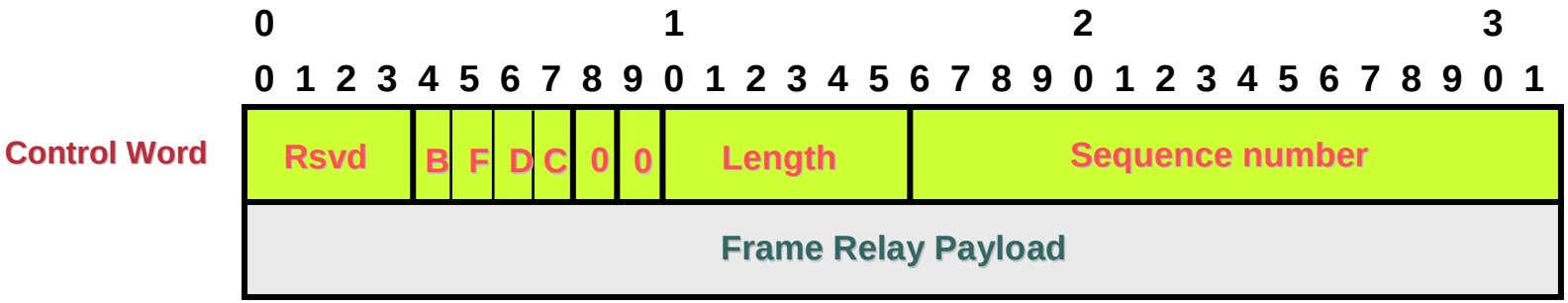
Encapsulation Support:

- **Cisco, IETF (RFC1490)**
- **Does not require like encaps on both sides**

LMI Support:

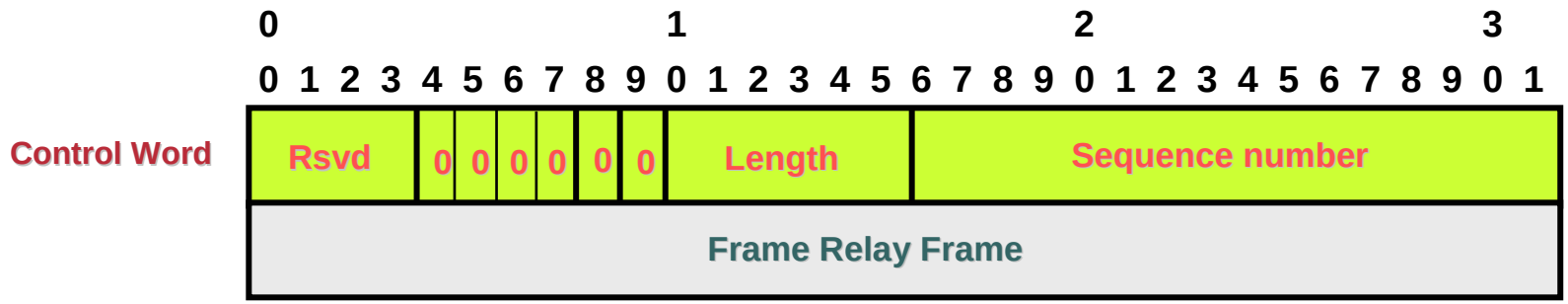
- **Cisco, ANSI, Q933a**
  - **DLCI-to-DLCI, LMI types can differ**
  - **Port-to-Port, LMI must be the same**

Frame Relay Encapsulation Details DLCI to DLCI



- Frame Relay PDUs are transported without header and FCS
- The control word is required
- BECN, FECN, DE & C/R bits are carried within the control word

Frame Relay Encapsulation Details Port Mode



- **Frame Relay frames transported without frame flags and FCS**
- **VCs are not individually visible**
- **The control word is optional**
- **Control word flags should be set to zero and ignored**

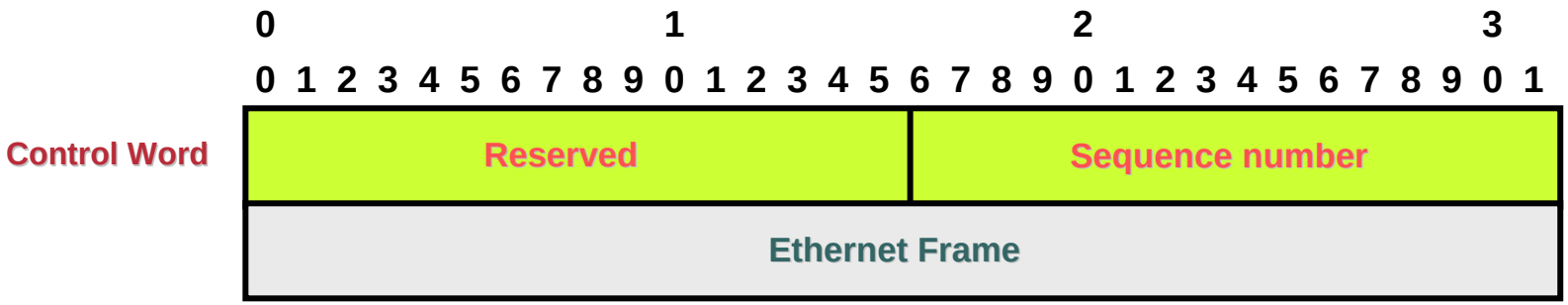
Frame Relay over MPLS Link Management Interface

- **For DLCI-to-DLCI mode:**
  - **Label withdrawal initiated if PVC goes down**
  - **Remote CE notified via LMI after label withdrawal**
- **LMI frames transported transparently for port mode**

Ethernet Transport over MPLS

- **Two modes of operation**
  - **Port**
  - **VLAN**
- **ISL not supported**

Ethernet Encapsulation Details



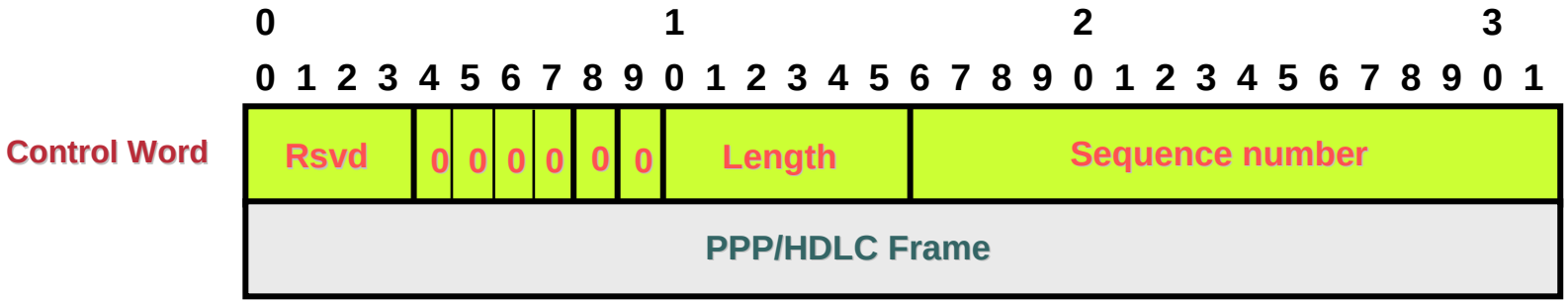
- **Ethernet frames transported without preamble and FCS**
- **Control word is optional**
- **802.1Q tag may be rewritten in VLAN mode**

PPP/HDLC Transport over MPLS

Cisco.com

- **Simplest PW model (transparent frame pass-through)**
- **PEs do not participate in PPP negotiation**
- **ACs must have similar physical characteristics (e.g. sync /async, PPP Multilink)**

PPP/HDLC Encapsulation Details



- HDLC frames transported without frame flags and FCS
- PPP frames transported without frame flags, media-specific framing info and FCS
- The control word is optional
- Control word flags should be set to zero and ignored

AToM – CLI Example in 12.0(25)S

ATM Cell Relay over MPLS: VC Mode

```
mpls label protocol ldp
 mpls ldp router-id loopback0 force
!
interface loopback 0
 ip address 172.18.255.1 255.255.255.255
!
interface atm1/0
pvc 100/1 l2transport
encapsulation aal0 ← raw cell mode, no SAR
xconnect 172.18.255.3 100 encapsulation mpls
```

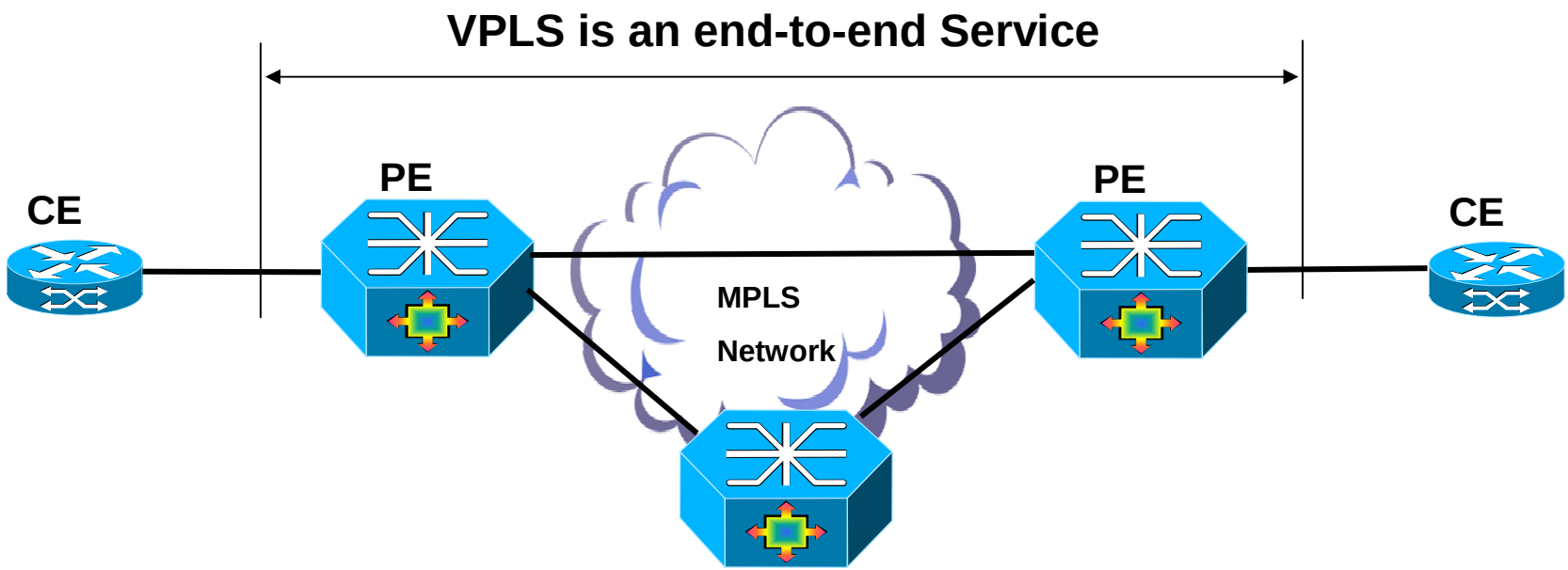
AToM – Summary

- AToM is used for the point-to-point transport of Layer 2 PDUs across an MPLS enabled cores.
- AToM uses Directed LDP sessions to negotiate VC Labels between participating peers
- AToM can use a Control Word to preserve relevant information in transported PDUs (ex: BECN, FECN, DE, C/R bits, etc.)
- AToM can interwork with native service management protocols such as ILMI / LMI to indicate local circuit status to remote peers

Agenda

- Why L2VPNs ?
- Pseudowire Overview
- Layer 2 Tunneling Protocol (L2TPv3)
- Any Transport over MPLS (AToM)
- Virtual Private LAN Services
- L2VPN Applications

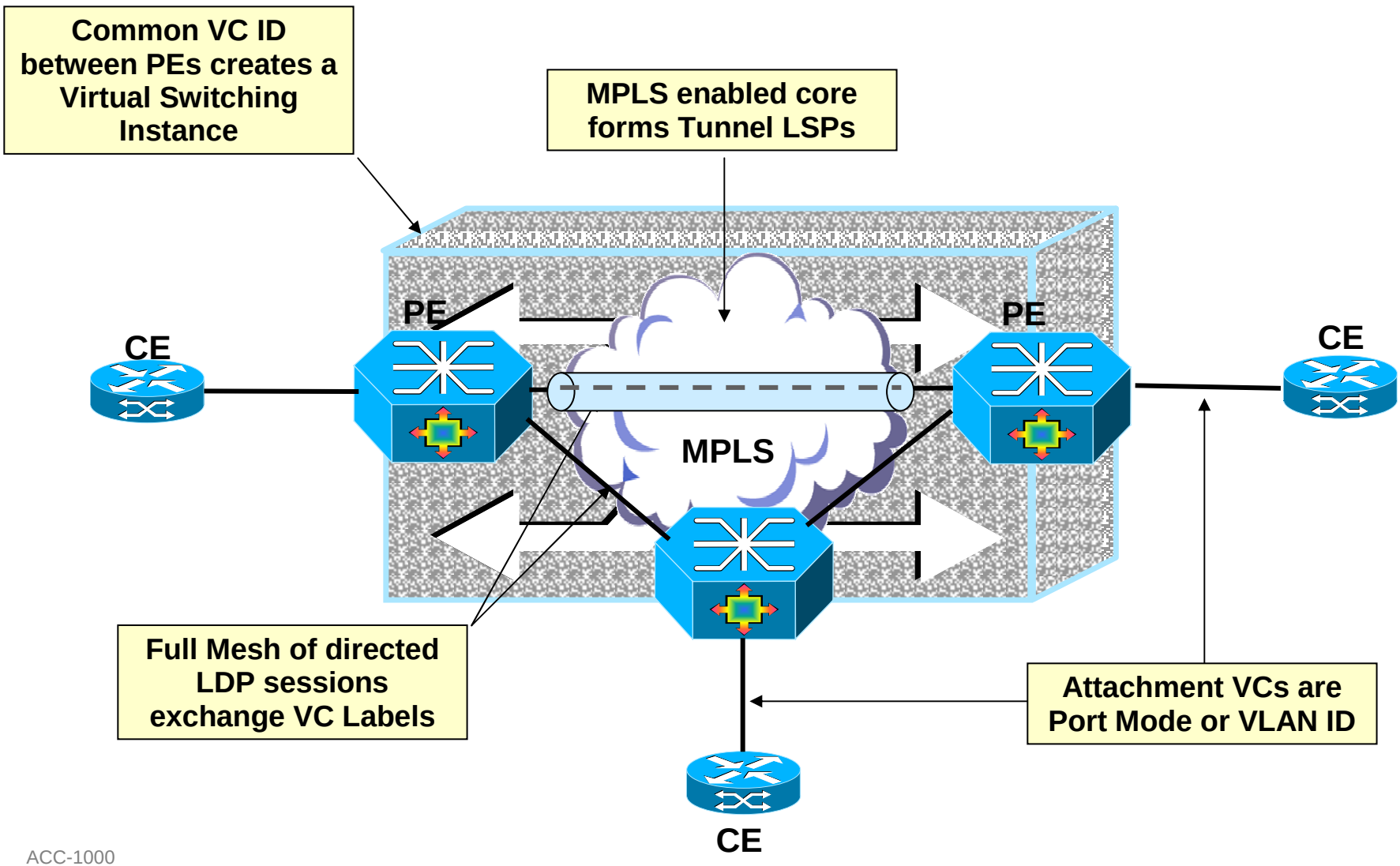
What is VPLS ? Service or Architecture



Initial IETF drafts:

- **treat PWs a logical ports of a switch**
- **do MAC address learning/forwarding on that logical port**
- **Run split horizon among the PWs to avoid STP over core**

VPLS Overview – Building Blocks



VPLS – L2 Forwarding Instance

- **Requirements for this solution**

  MAC table instances per customer and per customer VLAN (L2-VRF idea) for each PE

  VSI will participate in learning, forwarding process

  Create partial or full-mesh of EoMPLS VCs per VPLS

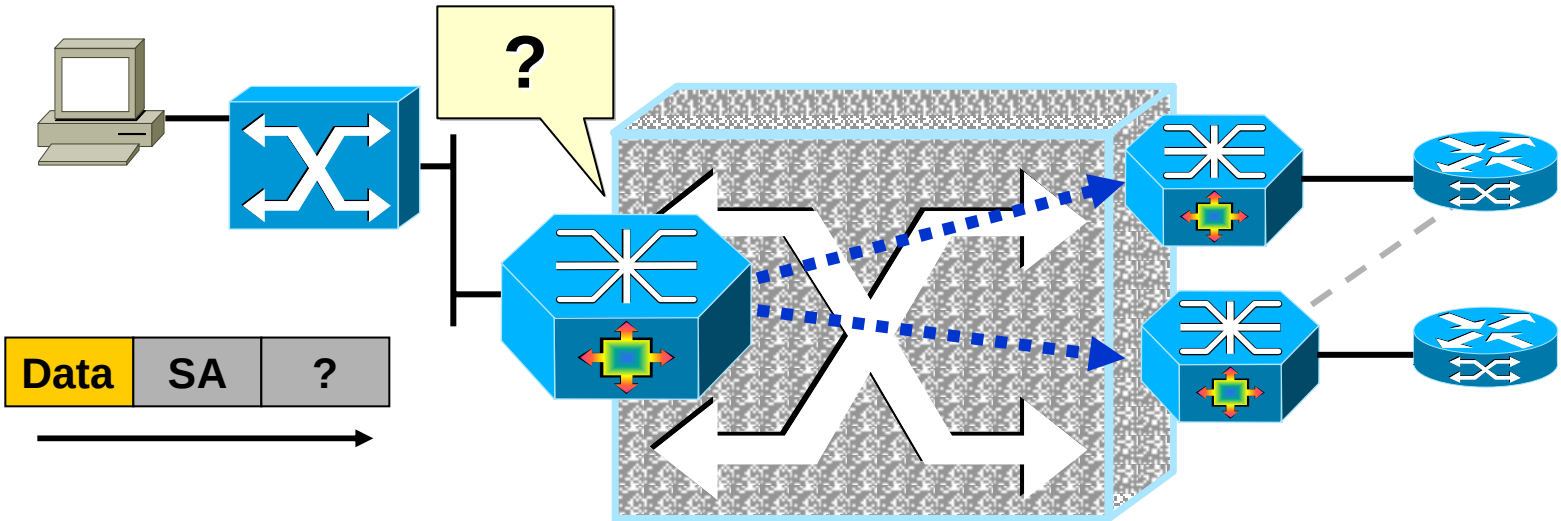
  Usage of network "split horizon" to prevent loops

  New additional VC-Type to draft-martini-trans

  Announce EoMPLS VPLS VC tunnels

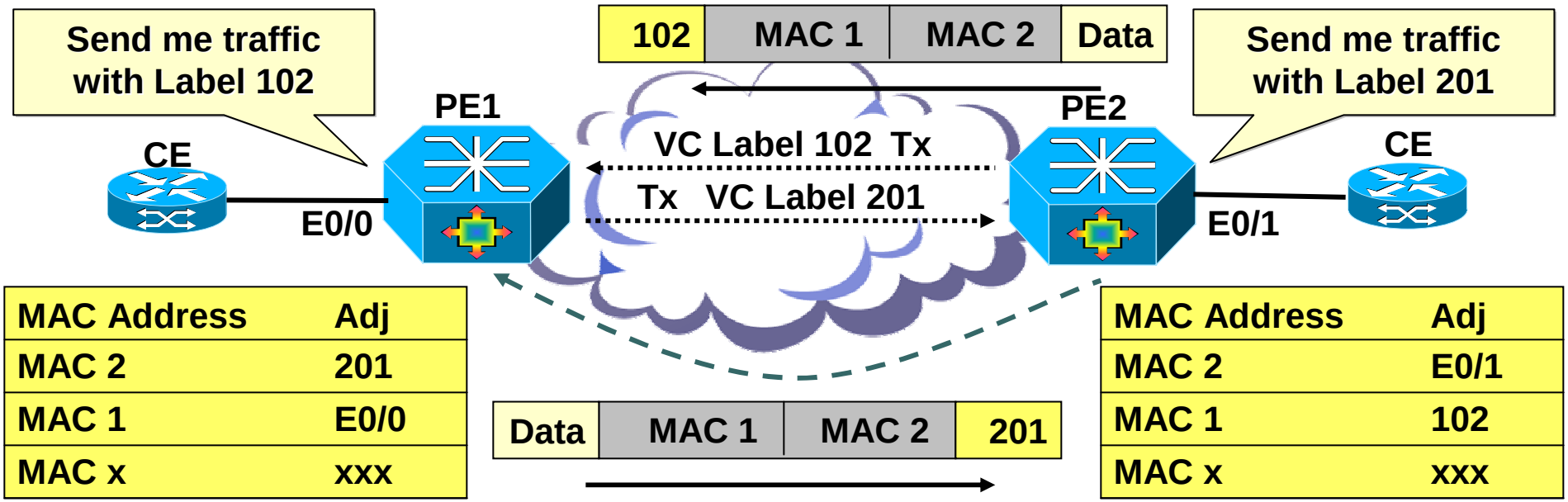
  New additional MAC TLV to LDP

VPLS Overview – Flooding & Forwarding



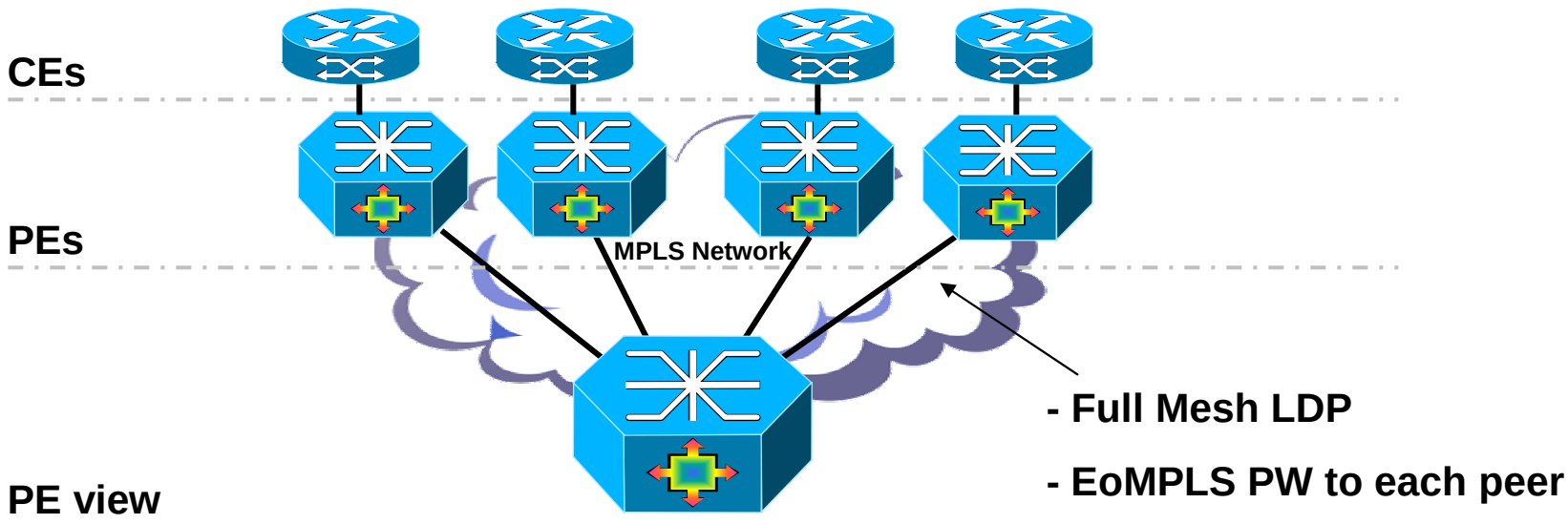
- Flooding (Broadcast, Multicast, Unknown Unicast)
- Dynamic learning of MAC addresses on PHY and VCs
- Forwarding:
  - Physical Port
  - Virtual Circuit

VPLS Overview – MAC Address Learning



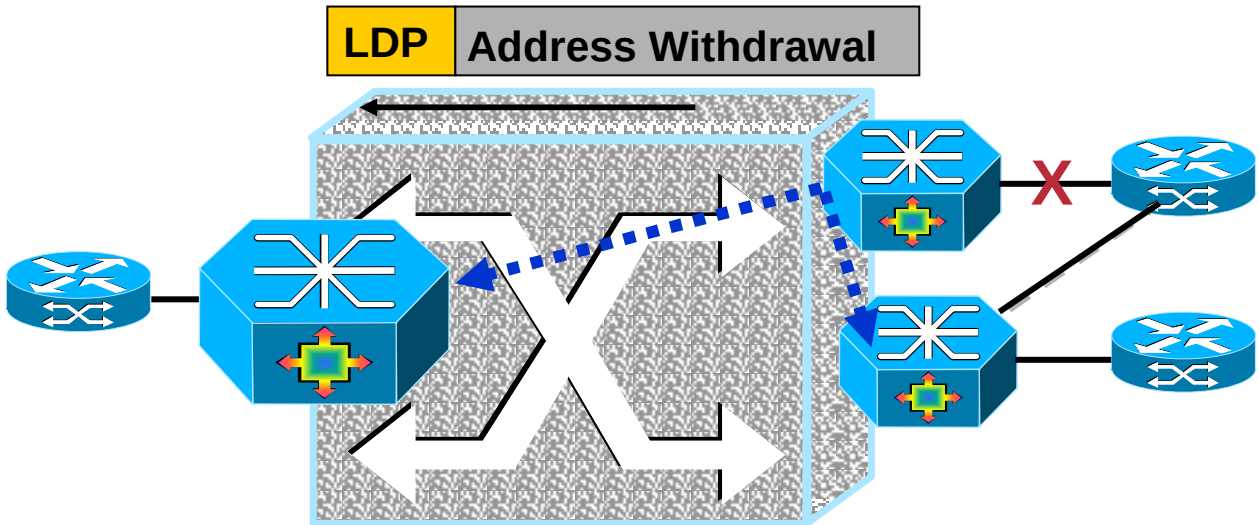
- Broadcast, Multicast, and unknown Unicast are learned via the received label associations
- 2 LSPs associated with an VC (Tx & Rx)
- If inbound or outbound LSP is down the entire circuit is considered down

VPLS Overview – L2 VPN Topology



- Each PE has a P2MP view of all other PEs it sees it self as a root bridge, split horizon loop protection
- Full mesh topology obviates STP requirements in the service provider network
- Customer STP is transparent to the SP / Customer BPDUs are forwarded transparently

VPLS Overview – MAC Address Withdrawal



- Primary link failure triggers Notification Message
- PE removes any locally learned MAC addresses and send LDP Address Withdrawal (RFC3036) to remote PEs in VPLS
- New MAC TLV is used

Agenda

- Why L2VPNs ?
- Pseudowire Overview
- Layer 2 Tunneling Protocol (L2TPv3)
- Any Transport over MPLS (AToM)
- Virtual Private LAN Services
- L2VPN Applications

L2VPN Application – Objectives

- **Illustrate How L2VPNs are being utilized:**
  - **Operational Simplification through Network Consolidation**
  - **Creative Cost Reduction for managed Services**
  - **Leveraging the PSN for New Services**

L2VPNs – Network Consolidation

Provider Profile:

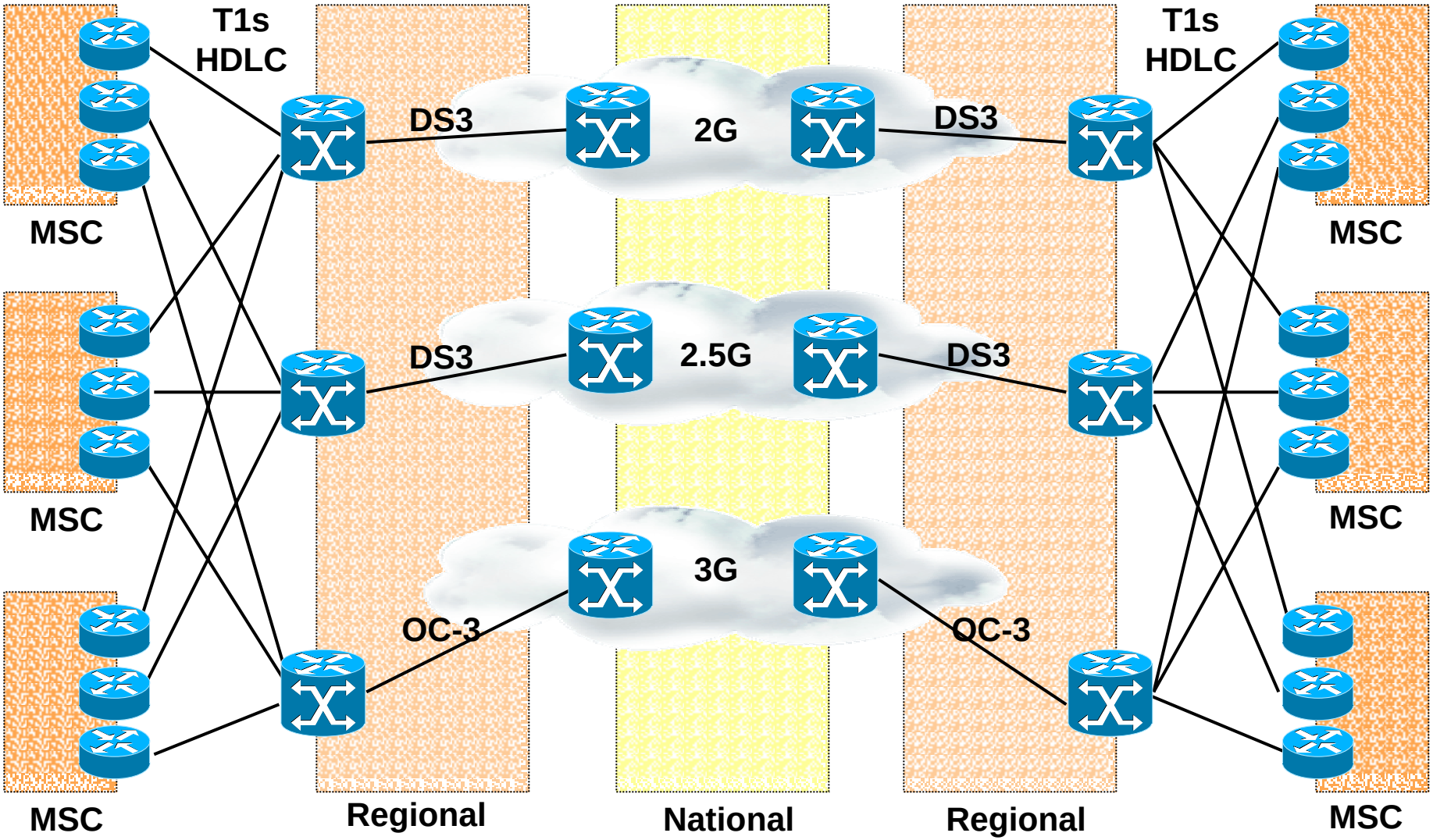
- **Wireless services, updating internal infrastructure, no new service creation**

Problem:

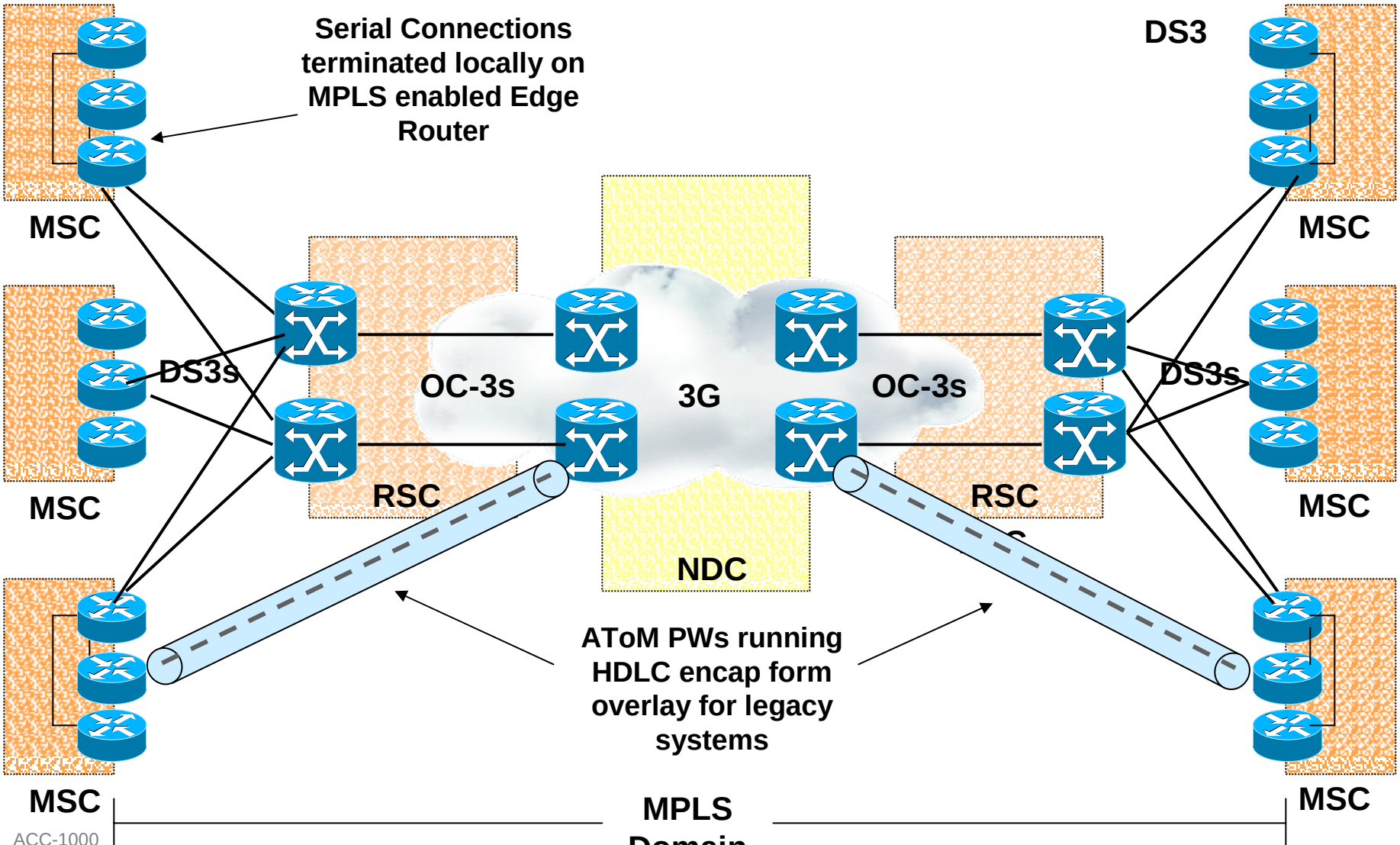
- **Next generation technology required build-out of new network infrastructure**
- **Legacy services left too many overlapping networks to support, maintain and operate.**
- **New high-speed network is underutilized**

Q: How can the Service Provider consolidate legacy systems by utilizing L2VPN technology?

L2VPNs – Pre - Network Consolidation



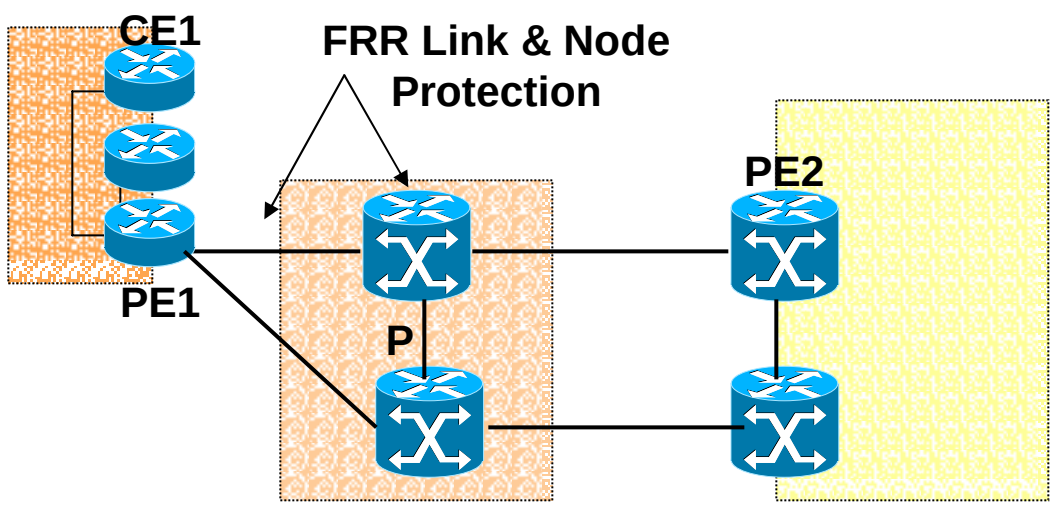
L2VPNs – Post - Network Consolidation



Consolidation – Migration Steps

- **Establish base MPLS infrastructure**
  - **Enable on P, PE routers**
- **Incorporate enhanced MPLS services**
  - **Add MPLS TE Tunnels**
  - **Add relevant QoS configurations**
- **Upgrade links & design**
  - **Redundancy Considerations**
  - **Capacity**
- **Migrate the MSCs to main uplinks**
  - **Configure overlay network with AToM PWs**

Consolidation – FRR Resiliency



Note: Only pw-class reference to MPLS-FRR is depicted here.

PE1(Configuration):

```
pseudowire-class HDLC_CEs
 encapsulation mpls
 preferred-path interface Tunnel10 disable-..
Serial1/0
 encapsulation hdlc
 xconnect 1.0.0.1 100 pw-class HDLC_CEs
```

PE2(Configuration):

```
pseudowire-class HDLC_CEs
 encapsulation mpls
 preferred-path interface Tunnel10 disable-..
Serial1/0.
 encapsulation hdlc
 xconnect 1.0.0.1 100 pw-class HDLC_CEs
```

Consolidation – Benefit Summary

- Leveraged new high speed network
- Reduced OPEX for multi-network infrastructure
- Migration path for future L2 & L3 services to external client base
- Enabled hardware migration for next generation wireless gear

L2VPNs – Recurring Cost Reduction

Provider Profile:

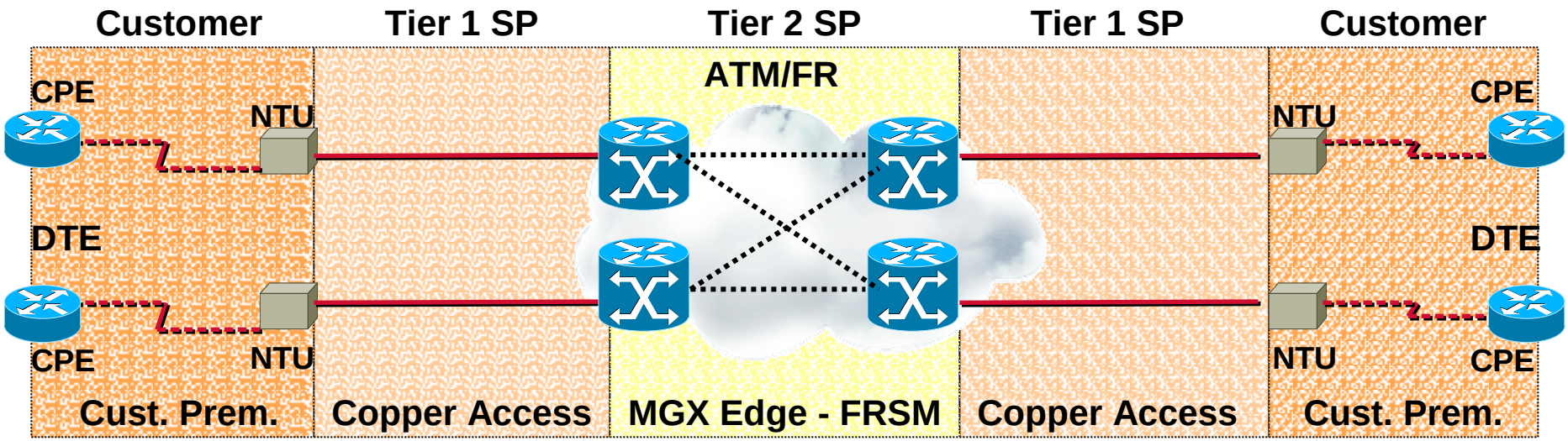
- **Tier 2 Service Provider, regulatory limitation prevents owning copper last mile; ILEC leased. Providing Frame Relay, Leased Line services**

Problem:

- **Recurring costs from ILEC make aggressive competition impossible.**
- **Wireless bypass alone doesn't allow existing customer's service protection**
- **Limited ability to expand.**

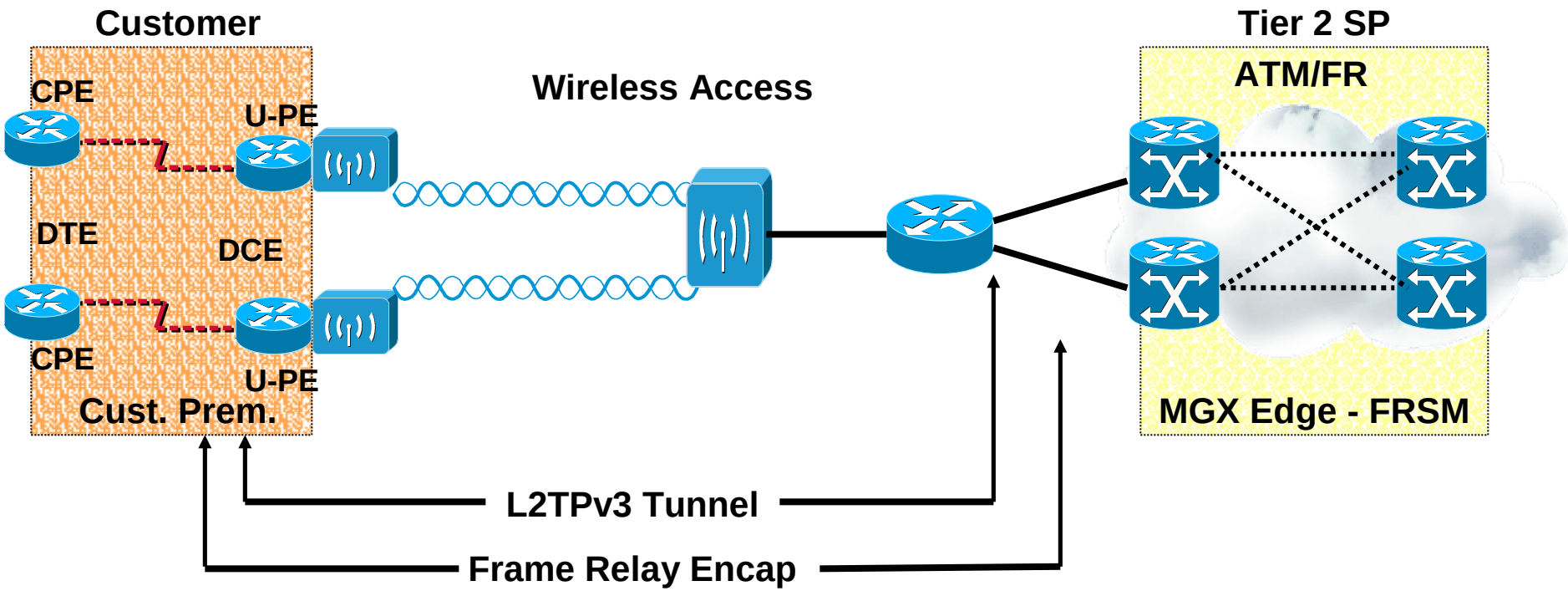
Q: How can the Service Provider save local loop costs without service disruption to existing customers?

L2VPNs – PRE - Recurring Cost Reduction



- Nx64 TDM access provided from the ILEC
- Frame Relay encapsulation from the CPE to the MGX
- Frame Relay VCs mapped through Tier 2 SPs ATM Core

L2VPNs – Recurring Cost Reduction

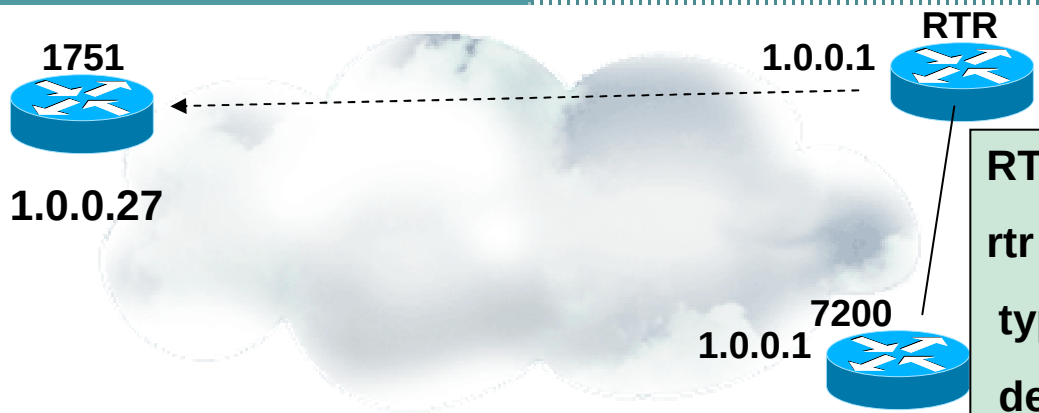


- L2TPv3 enables transparent Frame Relay service
- Simplifies management and reduces overhead
- Seamless ‘no-touch’ migration for the customer

Cost Reduction – Migration Steps

- **IP enabled wireless access network deployed (out of L2TPv3 scope)**
- **Swap SP1 NTUs for Cisco 1751 CPEs**
  - **Clock Serial Interface for desired access speed**
  - **Configure L2TPv3 FR trunking overlay on CPE**
  - **Configure SAA responder to monitor access network**
- **Configure 7200 head end for PWs**
  - **Configure channel-groups relevant to access speeds**
  - **Configure L2TPv3 for FR trunking**
- **Configure SAA head end probe to Access network response time monitoring**

Cost Reduction – Configuration Example




```
RTR#
rtr 1
 type jitter dest-ipaddr 1.0.0.27  /
 dest-port 2020  request-data-size 1000
rtr schedule 1 life forever start-time now
```

```
1751(Configuration):
pseudowire-class l2tpv3_1
 encapsulation l2tpv3
 ip pmtu
 sequencing
Serial1/0
 encapsulation hdlc
 xconnect 1.0.0.1 100 pw-class l2tpv3_1
rtr responder
```

```
7200(Configuration):
pseudowire-class l2tpv3_1
 encapsulation l2tpv3
 ip pmtu
 sequencing
Serial1/0
 encapsulation hdlc
 xconnect 1.0.0.1 100 pw-class l2tpv3_1
```

Cost Reduction – Benefit Summary

- **Bypass the ILEC and reduce monthly recurring tail circuit lease costs**
  - **Leads to competitive pricing for Enterprise**
- **Enables transparent layer 2 service that supports frame relay plus other WAN protocols, ie HDLC,PPP,802.1q etc**
  - **No change to customer's network required**
  - **Frame relay flow control features still work ie FECN, BECN**
  - **Supports both managed and unmanaged service**
  - **Option to convert customer to ethernet without need for additional router**

L2VPNs – New Service Offering

Provider Profile:

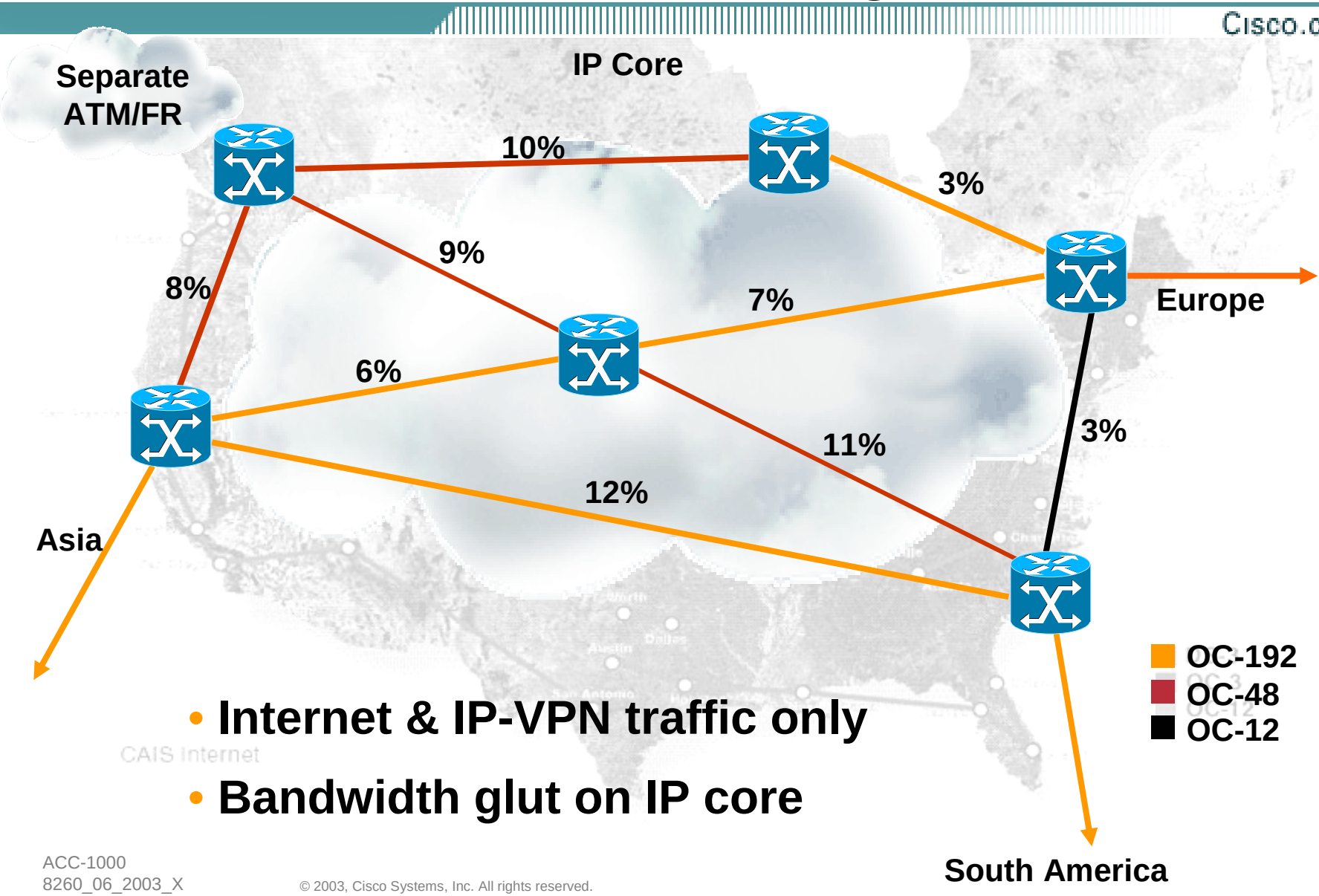
- **Tier 1 Service Provider with traditional voice & data services.**

Problem:

- **Existing L3 data network is massively underutilized**
- **Upgrading legacy L2 ATM/FR network with switches is undesirable.**
- **Would like to offer more competitive L2 options.**
- **Possibly migrate FR switches to IP backbone.**

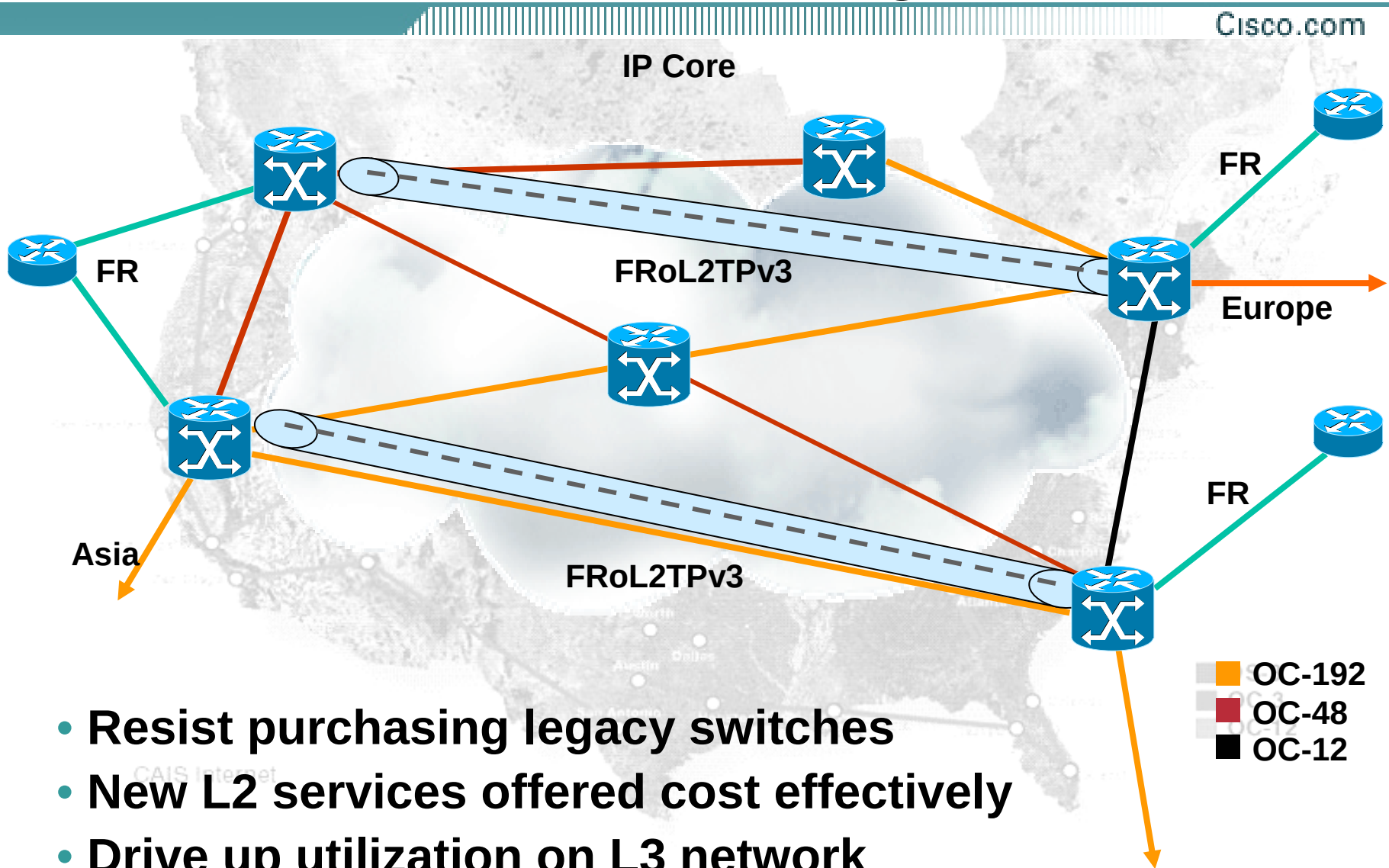
Q: How can the Service Provider take advantage of the unused bandwidth on their existing L3 packet infrastructure?

L2VPNs – PRE - New Service Offering



- Internet & IP-VPN traffic only
- Bandwidth glut on IP core

L2VPNs – POST - New Service Offering



- Resist purchasing legacy switches
- New L2 services offered cost effectively
- Drive up utilization on L3 network

New Service – Preparation

- Global IP Infrastructure was Already Operational
- Update PE software to support L2TPv3 based services (Frame Relay, Ethernet, HDLC/PPP)
- Configure QoS policies to reflect service strategy
  - Configured for FR service models w / egress policing
  - Subrate services for virtual leased line, TLS
- Start configuring L2TPv3 based L2VPN Services
  - Configured PW classes with relevant ToS, Sequencing and Path MTU discovery

New Service – QoS Configuration

7507

```
class-map match-all dlci200
    match fr-dlci 200
policy-map vlan-hi-priority
    class class-default
    set ip precedence 5
policy-map Serial2-1-in
   class dlci200
   police cir 256000 bc 128000 be 256000 conform-action set-prec-transmit  5 exceed- /
action set-prec-transmit 0 violate-action drop
interface Serial2/0
   frame-relay intf-type dce
   service-policy input Serial2-1-in
```

Consolidation – Benefit Summary

- Leverage existing packet infrastructure to offer new source of revenue
  - $8M to Date
  - 50+ Customers Online
- Utilize well-known native IP infrastructure
  - Minimal OPEX expenditure for support
- Enterprise benefits:
  - Reduces monthly WAN recurring costs
  - Maintain well known Layer 2 service
  - Future Layer 3 service opportunity

L2VPN – Summary

- **Established why L2VPN technologies are emerging as the new VPN options for PSNs**
- **Introduced IETF backed solutions for addressing L2VPN market requirements**
- **Introduced some innovative ways Service Providers are taking advantage of L2VPN technologies.**

Useful Links

Cisco.com

CCO:

AToM:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fsatom26.htm

L2TPv3:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s25/l2tpv325.htm

L2VPN Interworking:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fsinterw.htm