AGG-2024

Layer-2 Business VPN Services

Technologies, Architectures and Deployment

Dr. Frank Brockners

Recuerde siempre:

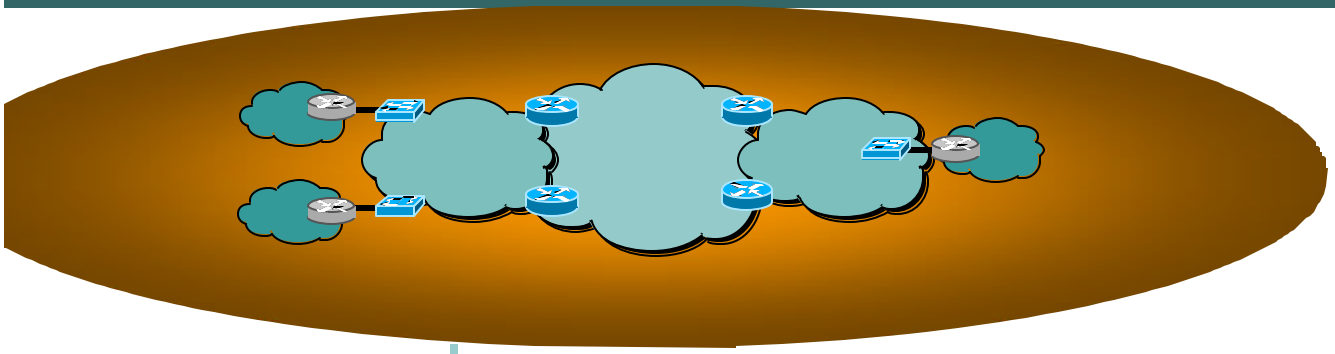
- **Apagar su teléfono móvil/pager, o usar el modo “silencioso”.**

- **Completar la evaluación de esta sesión y entregarla a los asistentes de sala.**

- **Ser puntual para asistir a todas las actividades de entrenamiento, almuerzos y eventos sociales para un desarrollo óptimo de la agenda.**

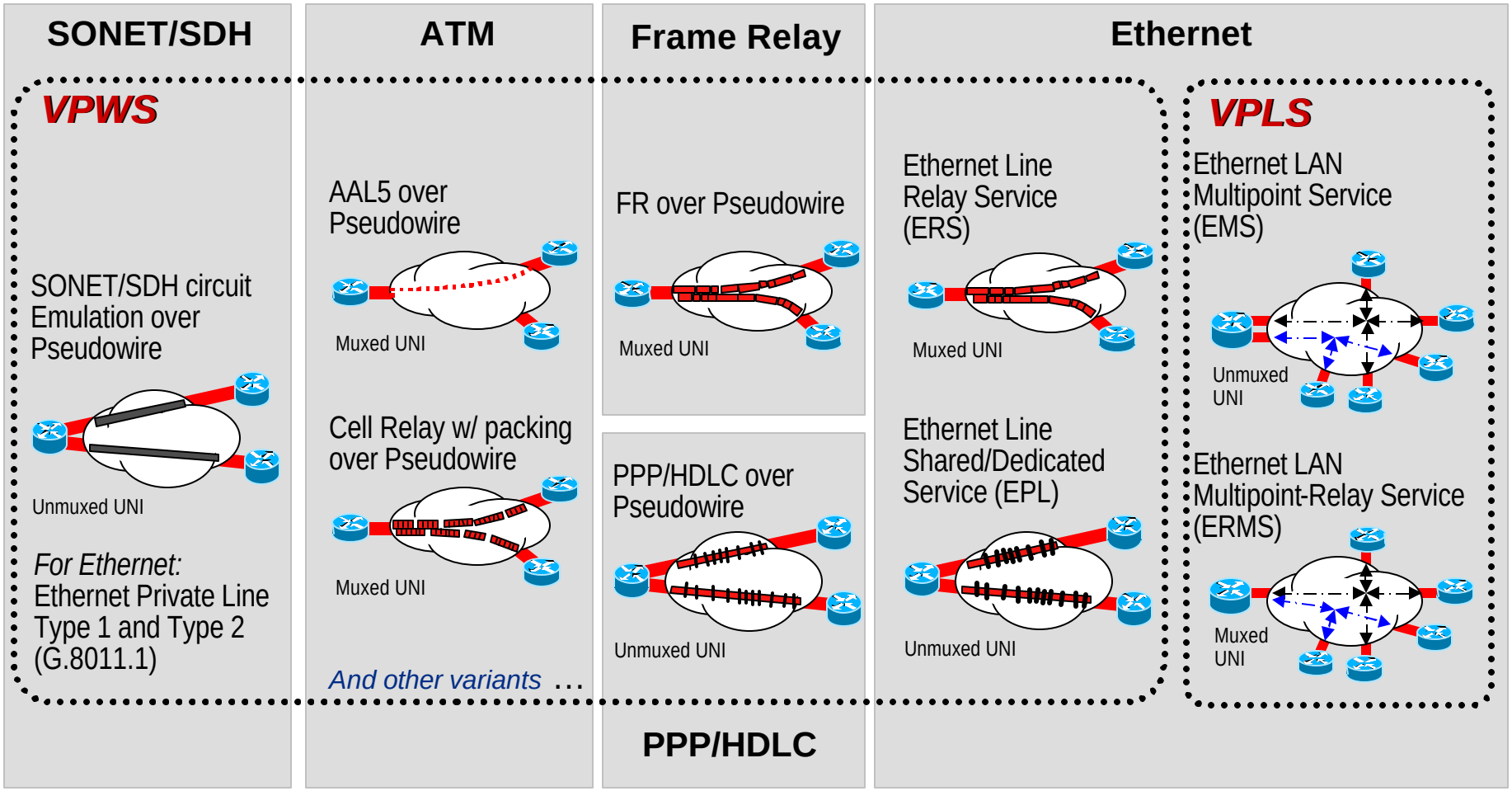
- **Completar la evaluación general incluida en su mochila y entregarla el miércoles 8 de Junio en los mostradores de registración. Al entregarla recibirá un regalo recordatorio del evento.**

Agenda



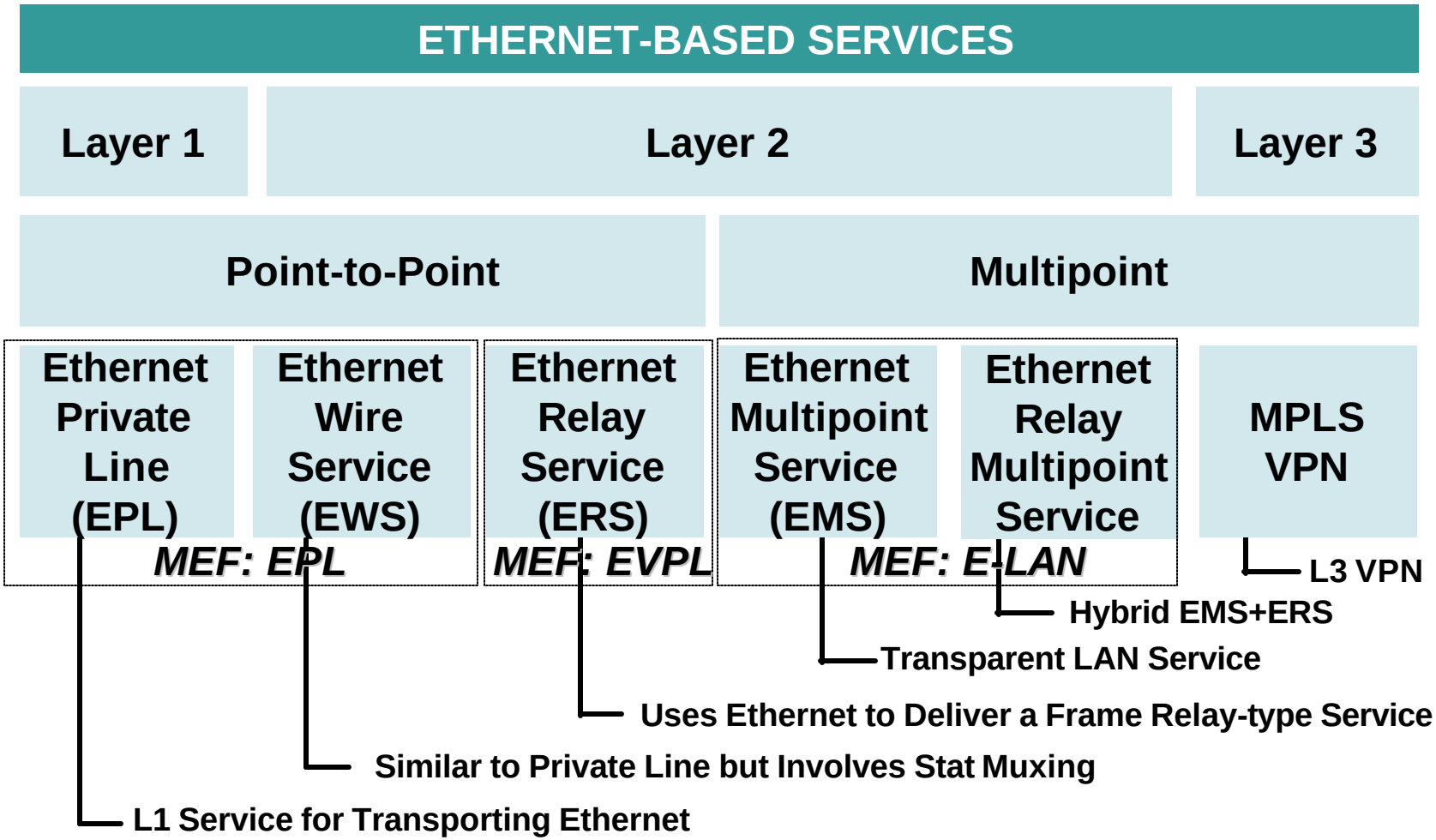
- Introduction to L2VPNs & L2VPN Service Classification
- Point-to-Point Technologies
  - Any Transport over MPLS (AToM) Overview
  - Layer 2 Tunneling Protocol Version 3 (L2TPv3)
  - Advanced Concepts
    - Layer 2 Interworking, PW Redundancy, PW Switching
- Multipoint Technologies
  - IEEE Provider Bridges (P 802.1ad)
  - Virtual Private LAN Services
- Deployment Aspects
  - Operational Aspects, OAM
  - QoS
  - Security

Service Offerings
L2VPN Transport Services



VPWS: IETF's Virtual Private Wire Service
VPLS: IETF's Virtual Private LAN Service

Overview of Ethernet-Based Services



EPL: Ethernet Private Line, EVPL: Ethernet Virtual Private Line, E-LAN: Ethernet LAN

Layer 3 and Layer 2 VPN Characteristics

LAYER 3 VPNs

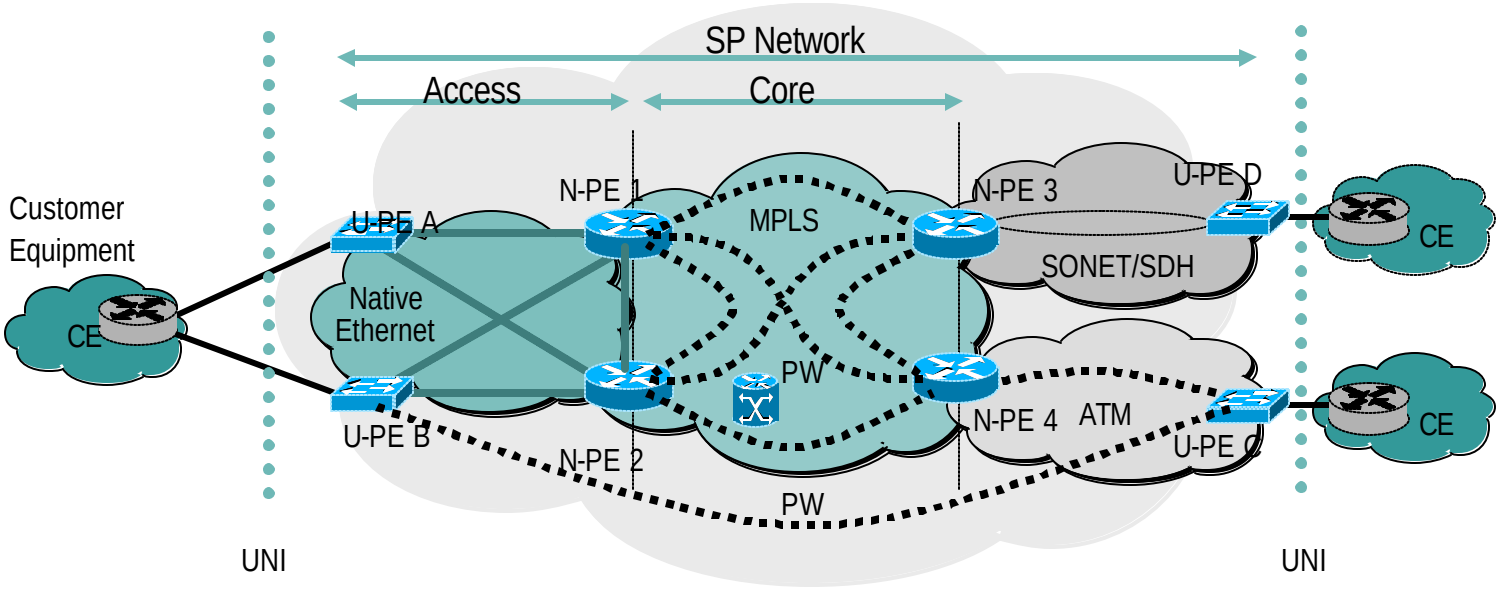
- SP devices forward customer packets based on Layer 3 information (e.g. IP addresses)
- SP is involved in customer IP routing
- Support for any access or backbone technology
- IP specific
- Foundation for L4-7 Services!
- Example: RFC 2547bis VPNs (L3 MPLS-VPN)

LAYER 2 VPNs

- SP devices forward customer frames based on Layer 2 information (e.g. DLCI, VPI/VCI, MAC)
- Enterprise stays in control of L3 policies (Routing, QoS)
- Access technology is determined by the VPN type
- Multiprotocol support
- Example: FR—ATM—Ethernet

The Choice of L2VPN over L3VPN Will Depend on How Much Control the Enterprise Wants to Retain
L2 VPN Services Are Complementary to L3 VPN Services

Building a L2VPN Service Network
Areas to Be Addressed



UNI Definition

- Customer STP and BPDU handling
- 802.1x, 802.3x,802.3ad
- Dual Homing
- Customer's GVRP, GMRP, LLDP,…

How to Build the Ethernet Access

- Minor changes to standard IEEE bridges
- Customer VLAN transp.
- MAC address scalability
- Redundancy
- OAM&P,…

How to Build the Interconnect Media

- MPLS/L2TPv3
- Redundancy address withdrawal
- PW – encap & signal.
- Auto-Discovery
- OAM&P,…

How to Connect the EA & IM Networks

- Redundancy, Interaction w/ PWs
- Dual-Homing
- Backdoor links
- STP & address scaling
- OAM&P, …

L2VPN 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); EFM (802.3ah); Connectivity Management – OAM: 802.1ag; 802.1ah Backbone Bridges, 802.1ak Multiple Registration Protocol, 802.1aj Media Converters,...

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.

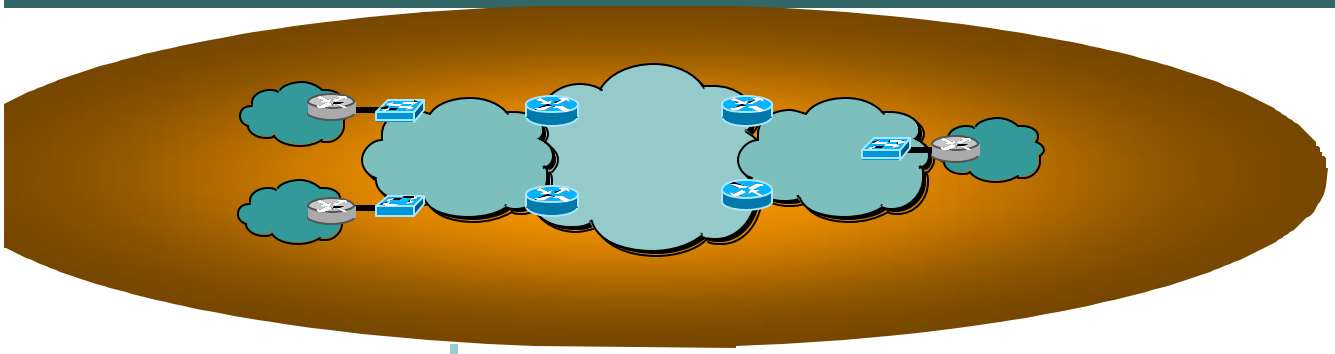
Ethernet to Frame-Relay/ATM Service Interworking

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

L2VPN related IETF Working Groups

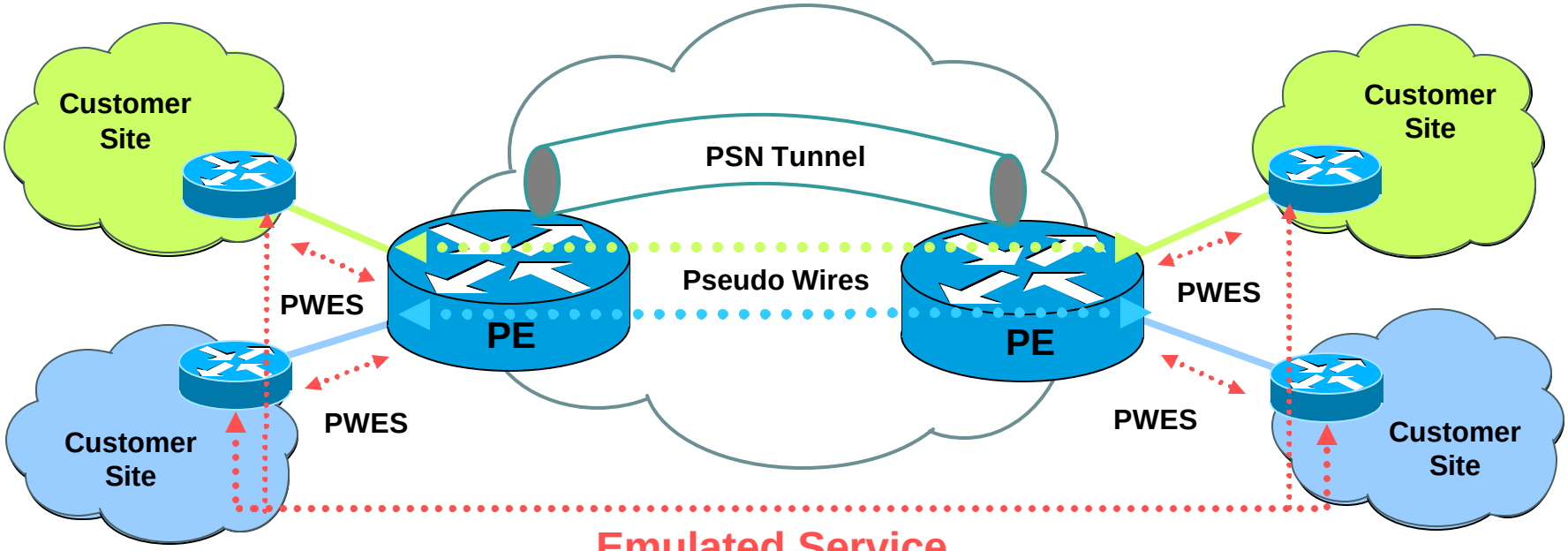
Internet Area		Transport Area
L2TPEXT	**L2VPN**	**PWE3**
L2TP(v2 & v3) • Extensions to RFC2661 • Control Plane Operation • AVPs • Updated data plane • Relevant MIBs	**VPLS, VPWS, IPLS** • Solution Architectures • PE Discovery • Signaling (with PWE3) • L2VPN OAM extensions • Relevant MIBs	**AToM** • PWE3 Architecture • PWE3 Requirements • LDP Control Channel • L2 Service Encap Specifics • TDM, CES, etc. • Relevant MIBs

Agenda



- Introduction to L2VPNs & L2VPN Service Classification
- Point-to-Point Technologies
  - Any Transport over MPLS (AToM) Overview
  - Layer 2 Tunneling Protocol Version 3 (L2TPv3)
  - Advanced Concepts
    - Layer 2 Interworking, PW Redundancy, PW Switching
- Multipoint Technologies
  - IEEE Provider Bridges (P 802.1ad)
  - Virtual Private LAN Services
- Deployment Aspects
  - Operational Aspects, OAM
  - QoS
  - Security

VPWS 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

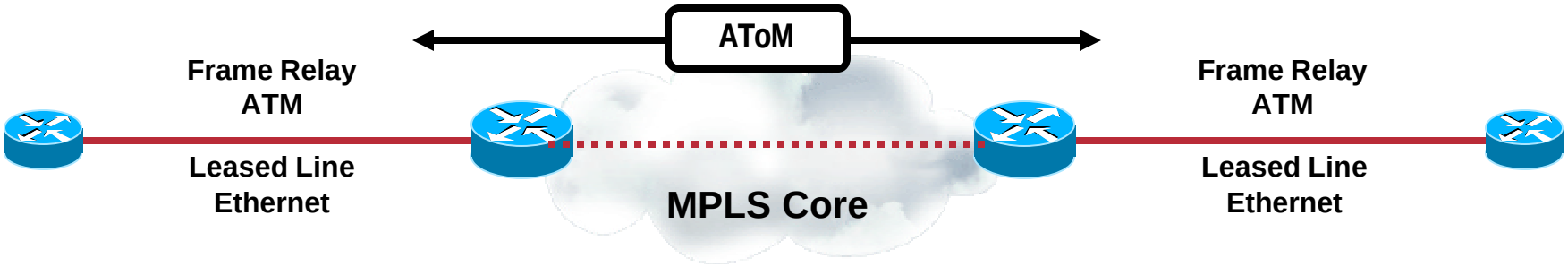
Service Types:

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

PWES

- HDLC
- PPP
- Frame Relay VC

Virtual Private Wire Service (VPWS)
Any Transport over MPLS (AToM)



- AToM is Cisco's implementation of VPWS for MPLS networks
- Provides ability to transport layer 2 traffic such as ATM, FR, Ethernet, PPP and HDLC across MPLS packet-based core networks
- A standards track open architecture allows extensibility to many transport types.
- AToM, combined with Cisco IOS QoS and MPLS Traffic Engineering allows Service Provides to offer "Virtual leased line" types of services
- Service Provider does not participate in customer routing

Layer-2 Transport across MPLS

Control Connection

Directed LDP

Used for VC-Label Negotiation, Withdrawal, Error Notification

Transport Component

Tunnel Header (Tunnel Label)

to get PDU from ingress to egress PE;

MPLS LSP derived through LDP or RSVP-TE

Note: 'Emulated Circuits' have 3 layers of encapsulation

Tunneling Component

Demultiplexer field (VC Label)

to identify individual circuits within a tunnel;

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

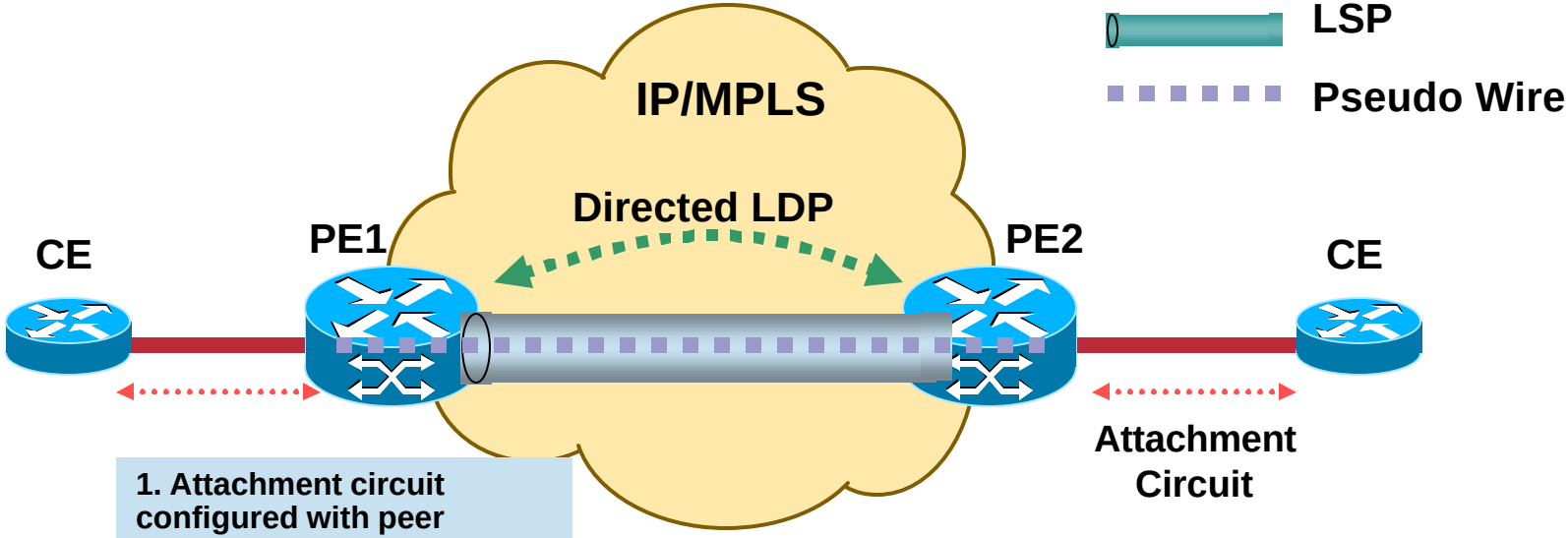
L2 PDU (Emulated)

Emulated VC encapsulation (Control Word)

information on enclosed Layer-2 PDU;

implemented as a 32-bit control word

VC Label Negotiation with Directed LDP



1. Attachment circuit configured with peer address and VC ID

2. PE1 starts directed LDP session with PE2 if one does not already exist

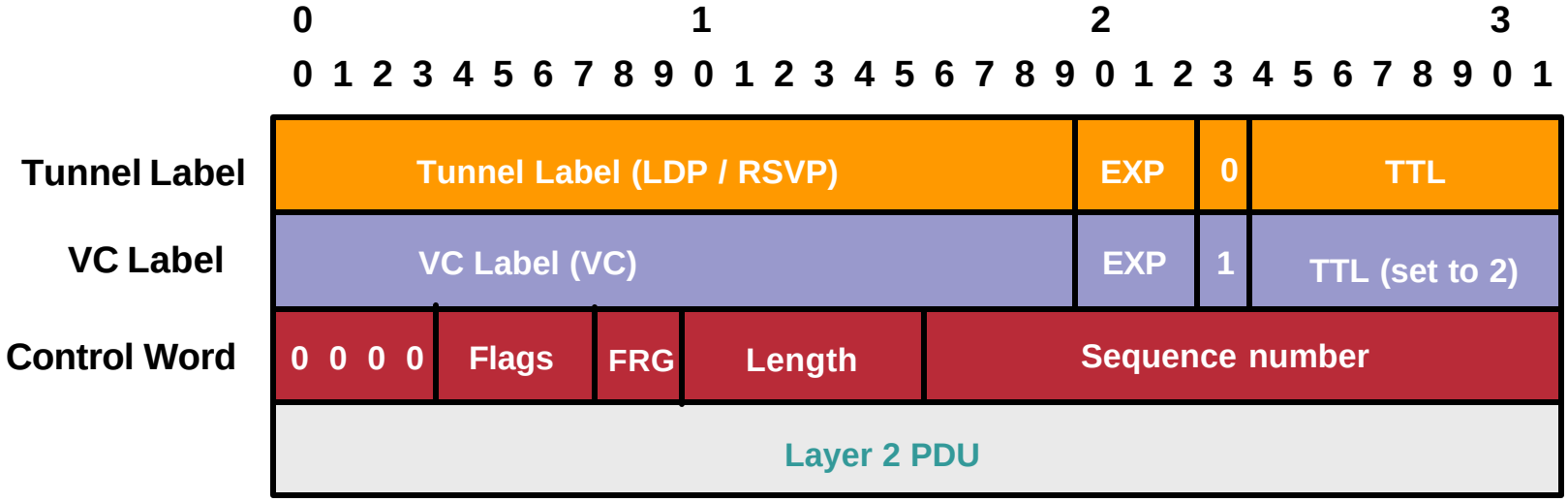
3. PE1 allocates VC label for new circuit & binds to configured VC ID

4. PE1 sends LDP label mapping message containing VC FEC TLV & VC label TLV

5. PE2 receives VC FEC TLV & VC label TLV that matches local VCID

6. PE2 repeats steps 1-5 so that bidirectional label/VCID mappings are established

AToM Traffic Encapsulation



- Three-level encapsulation
- Packets switched between PEs using top (tunnel) label
- VC label identifies PW
- VC label negotiated between PE with directed LDP
- Optional Control Word carries Layer 2 control bits and enables sequencing

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

Frame Relay and ATM Support in AToM

Cisco.com

Frame Relay

- Two main transport modes: Port-to-Port or DLCI-to-DLCI
- LMIs carried transparently for Port-to-Port
- LMIs terminated for DLCI-to-DLCI with remote notifications via LDP
- Multiple FR encapsulation support
- Multiple LMI support

ATM

- Two encapsulations: AAL5 and Cell Relay
- Single or multiple Cell Relay supported
- AAL5 supported in VC mode
- Cell Relay in VC/VP and Port modes
- OAM traffic carried transparently
- AAL5 mode may perform OAM emulation

Ethernet/HDLC/PPP Support in AToM

Cisco.com

Ethernet

- Two main transport modes: VLAN and Port
- VLAN mode requires 802.1q
- VLAN mode supports VLAN Id rewrite
- Support Ethernet Speed of 10/100/1000MBps

PPP/HDLC

- No special restrictions on HDLC Traffic
- PEs do not participate in PPP negotiation
- PPP negotiation requires attachment circuit compatibility

AToM – XConnect CLI Components

ldp enabled

- Defines LDP as label protocol
- Globally defined

Example:

```
mpls label protocol ldp
mpls ldp router-id loopback 0 force
```

pseudowire-class (optional)

- Characteristics template for PWs
- Tunneling mechanism
- Data plane encapsulation type

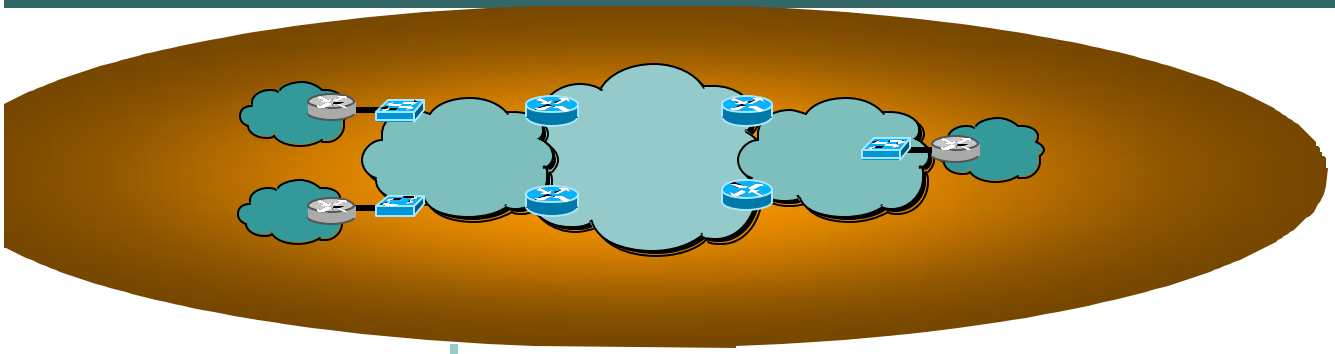
```
pseudowire-class atom_def
 encapsulation mpls
 sequencing both
```

2 Ways to configure:

- xconnect <target PE>
- mpls l2transport route <target PE>

```
interface FastEthernet5/1.500
 encapsulation dot1Q 500
 service-policy input vlan-hi-priority
 xconnect 172.18.255.3 1002 pw-class atom_def
```

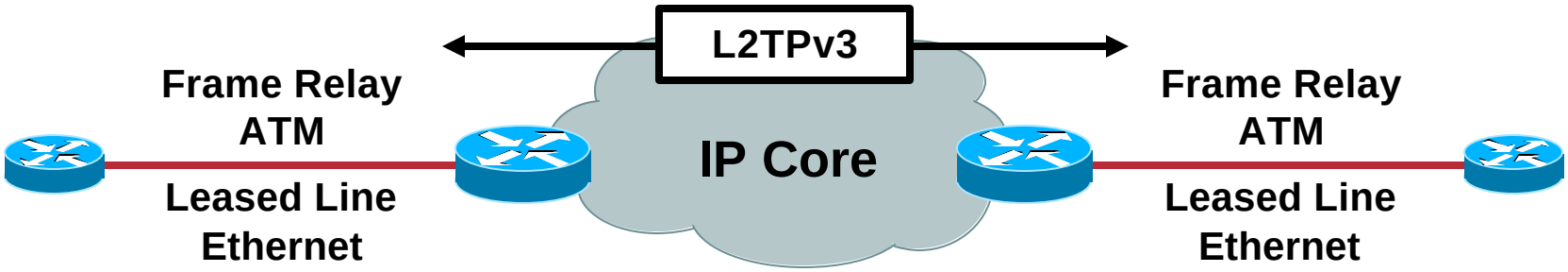
Agenda



- **Introduction to L2VPNs & L2VPN Service Classification**
- **Point-to-Point Technologies**
  - **Any Transport over MPLS (AToM) Overview**
  - **Layer 2 Tunneling Protocol Version 3 (L2TPv3)**
  - **Advanced Concepts**
    - **Layer 2 Interworking, PW Redundancy, PW Switching**
- **Multipoint Technologies**
  - **IEEE Provider Bridges (P 802.1ad)**
  - **Virtual Private LAN Services**
- **Deployment Aspects**
  - **Operational Aspects, OAM**
  - **QoS**
  - **Security**

Layer 2 Tunneling Protocol Version 3:
Point-to-Point Pseudowire Services

Cisco.com



- **L2TPv3 is designed for multiservice tunneling over IP networks**
- **Extends L2TPv2 (RFC 2661), the standard protocol for tunneling PPP**
- **Standards-based architecture allows for extensibility (RFC 3931)**
- **Fixed header allows for high-performance/HW-accelerated decapsulation**
- **Simple edge configuration is all that is required!**

Layer 2 Transport over IP

Control Connection	**L2TP Control Connection—Secure and Reliable Connection Used for Service Negotiation and OAM**
Tunneling Component	**Delivery Header (IPv4 Header)** **Transports an L2 PDU from Ingress to Egress PE; Comprised of IPv4 Loopback Addresses (DA, SA)**
Service Component	**L2TPv3 Header** **Session ID (Service Identifier) and Cookie (Service Integrity Check)**
L2 PDU	**L2 Specific Sublayer + Payload (Layer 2 PDU)** **Sequence Support and L2 Attribute Integrity** **L2 Payloads: ATM, HDLC, PPP, Ethernet and Frame Relay**

Note: 'Emulated Circuits' have 3 layers of encapsulation

L2TPv3: Control Connection Highlights

- **Dynamic sessions**

  L2TP control connection and sessions for each service are created dynamically

- **Service integrity/validation**

  Hello message provides periodic keepalive, dead-peer, and path detection for all services associated with a given control connection

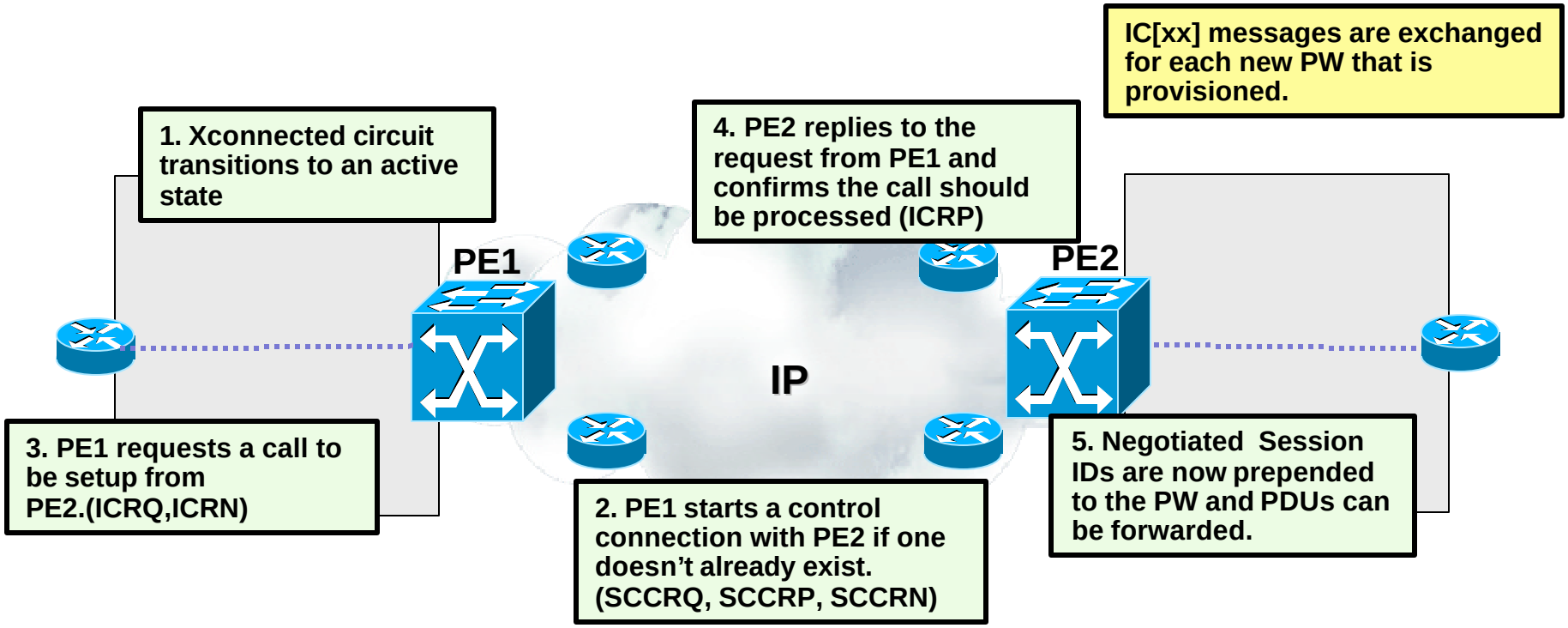
- **Authentication and security**

  Each control message is authenticated; rate limiting of control plane messages is supported

- **LMI/OAM interworking—circuit status**

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

L2TPv3
Control Plane Operation



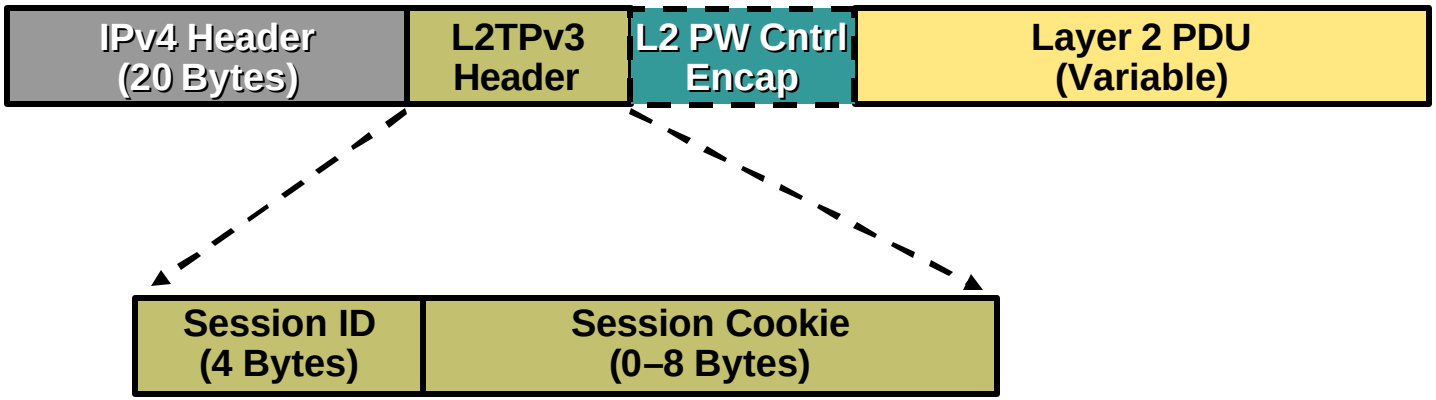
One control connection signals multiple PWs

Provides a dynamic mechanism to interface with UNI signaling

Requires a common VCID to successfully bind ACs together.

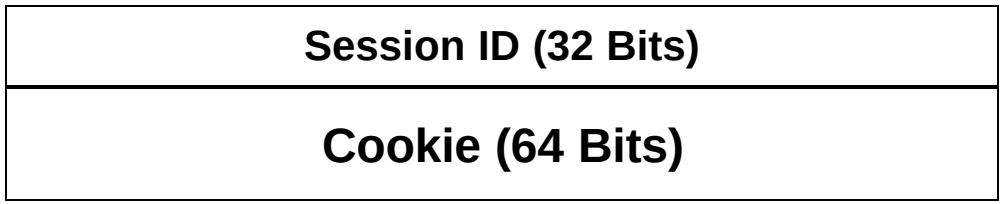
Session IDs are negotiated between peers and are not required to be globally unique

L2TPv3: Data Messages



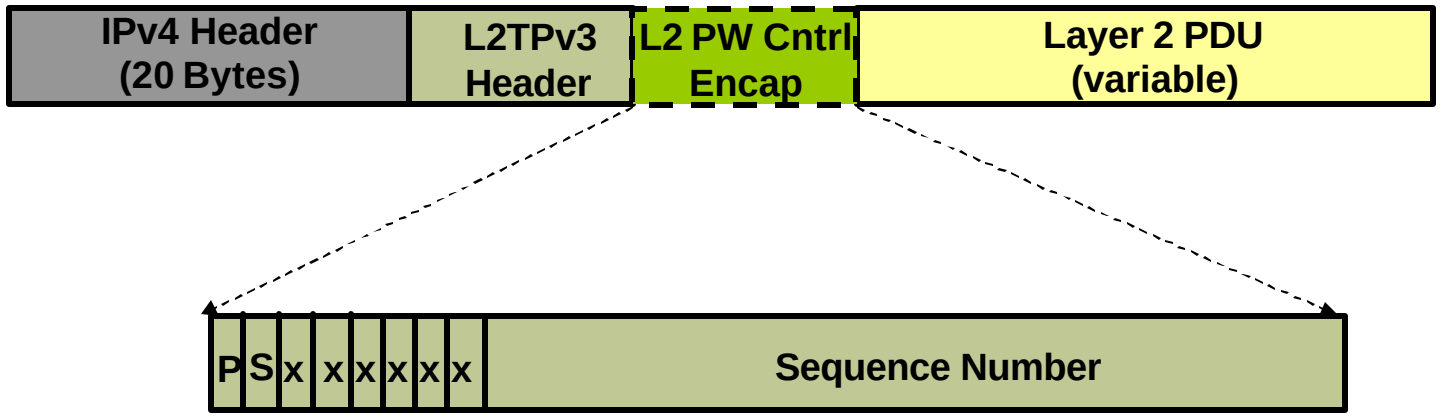
- IPv4 Header—delivery header for the tunnel
- L2TPv3 header—consists of two parts: (1) session ID, which uniquely identifies the correct session on the remote system; (2) cookie, which adds service integrity check to mitigate spoofing attacks
- L2 PW control encapsulation—sequence numbers, priority bits, and 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 to be transported by L2TPv3; typically the entire link-level frame

L2TPv3 Security – What is the L2TPv3 “Cookie”?



- The L2TPv3 Cookie is a 64-bit cryptographically random value, present in each L2TPv3 packet
- Chosen by the receiver, associated with a Session ID, and signaled to the sender
- Cookies in the header must match upon receipt, otherwise the packet is dropped and a global counter incremented
- Provides an additional layer of security at a very important place: before switching packets out of the core and into the customer premises
- Casts a strategic balance for the SP: Stronger than ACLs, but less complex than IPsec encryption and key negotiation

Default Control Encapsulation



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.

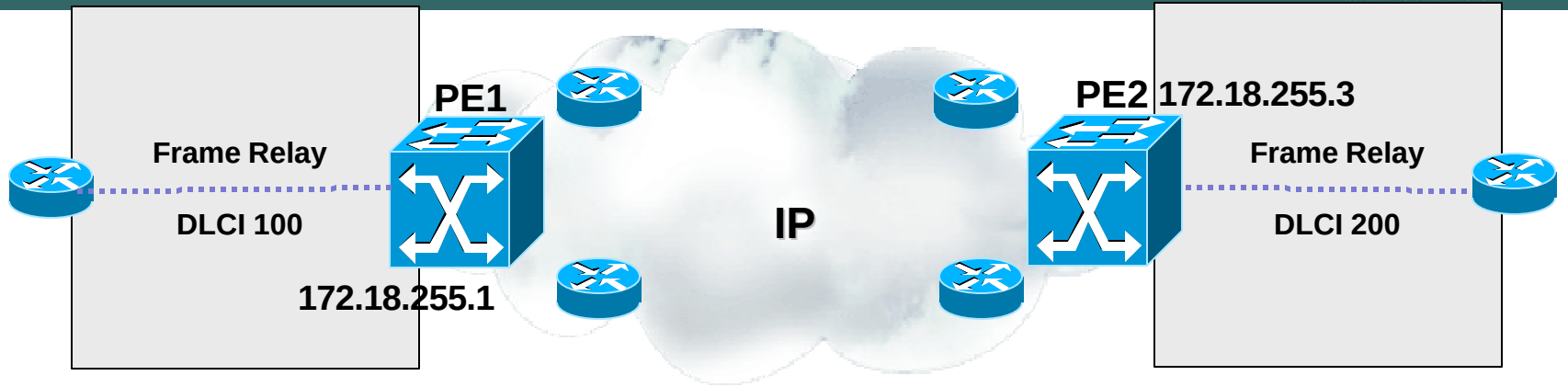
(S)equencing - Indicates the presence of sequence numbers and can be used in services such as ATM / Frame-Relay, etc. (2^24 Looping Counter, includes 0)

(x) – Reserved

L2TPv3: Data Plane Highlights

- **Data plane validation**
  - **Data plane has integrated service integrity checking**
  - **Session ID and cookie values mitigate the success of blind insertion/spoofing attacks**
- **Familiar IP tools for troubleshooting/management**
  - **Traditional tools, such as IP Ping and Traceroute, can be used.**
  - **IP MTU with fragmentation of IP packets prior to entering psuedowire**
- **Hardware support**
  - **Native processing on leading platforms**
- **Enhanced QoS capabilities for SLA management**
  - **Support for IP QoS mechanisms (e.g. traffic shaping, policing, marking)**
  - **May 'reflect' the TOS bits from tunneled IP payloads**

Layer 2 Tunneling Protocol version 3 – *Basic Configuration – Frame Relay Example*



PE1:

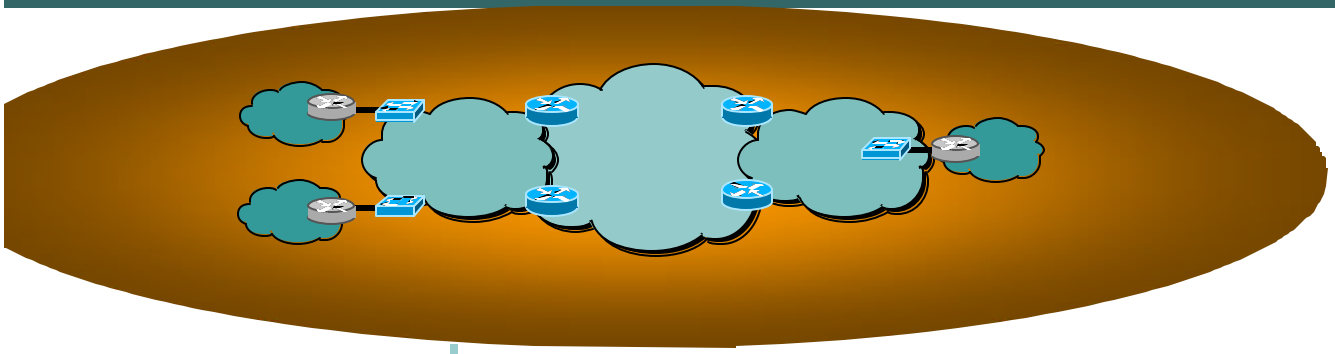
```
frame-relay switching
!
pseudowire-class l2tpv3-default
 encapsulation l2tpv3
 ip local interface loopback 0
!
connect MYFRPW1 Serial2/0 100 l2transport
 xconnect 172.18.255.3 100 pw-class l2tpv3-default
```

PE2:

```
frame-relay switching
!
pseudowire-class l2tpv3-default
 encapsulation l2tpv3
 ip local interface loopback 0
!
connect MYFRPW1 Serial3/0 200 l2transport
 xconnect 172.18.255.1 100 pw-class l2tpv3-default
```

- **Frame-Relay switching enabled globally**
- **Pseudowire class establishes encapsulation type & source interface**
- **Xconnnect starts control connection and negotiates Session IDs between local loopback and targeted PE**

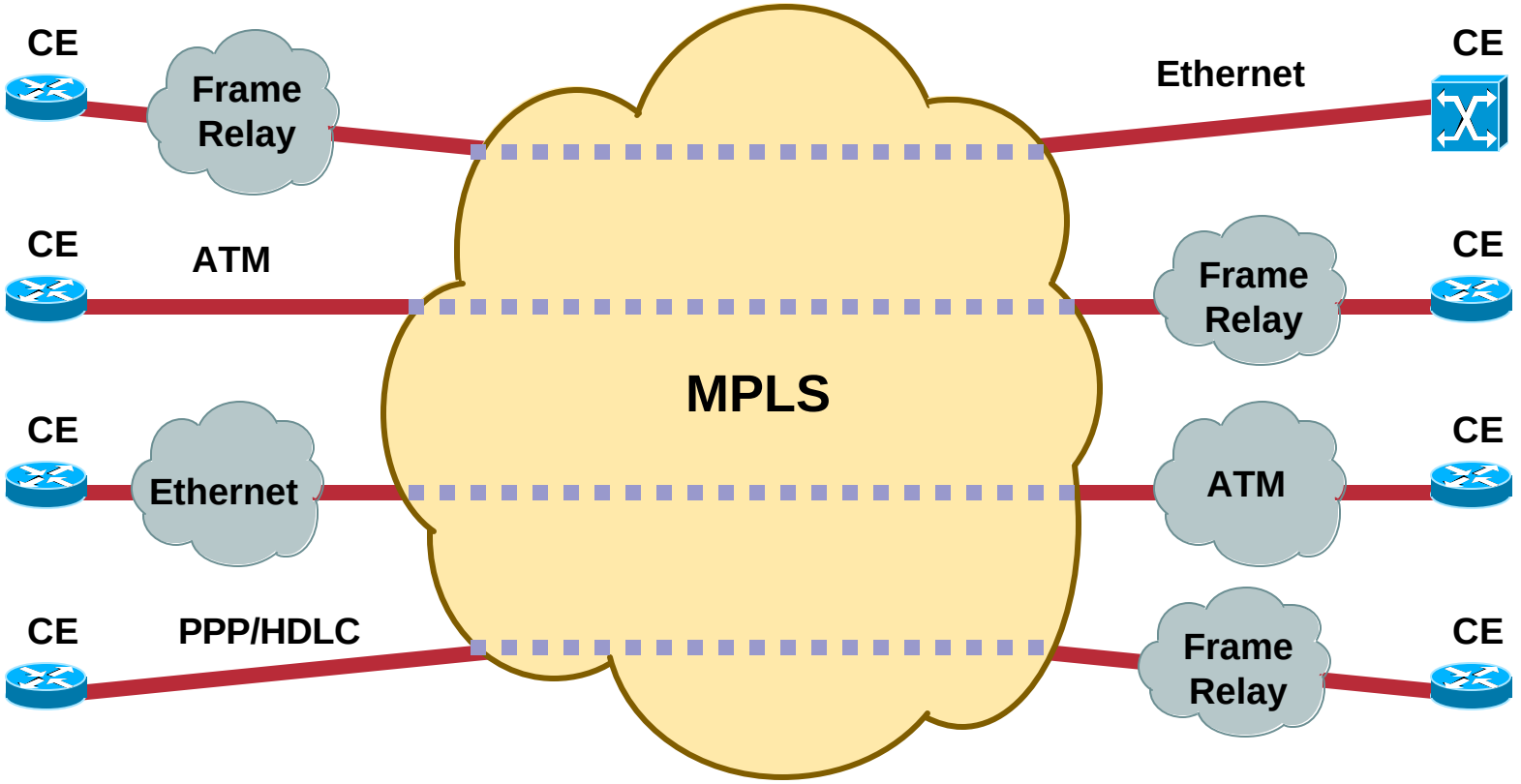
Agenda



- Introduction to L2VPNs & L2VPN Service Classification
- Point-to-Point Technologies
  - Any Transport over MPLS (AToM) Overview
  - Layer 2 Tunneling Protocol Version 3 (L2TPv3)
  - Advanced Concepts
    - Layer 2 Interworking, PW Redundancy, PW Switching
- Multipoint Technologies
  - IEEE Provider Bridges (P 802.1ad)
  - Virtual Private LAN Services
- Deployment Aspects
  - Operational Aspects, OAM
  - QoS
  - Security

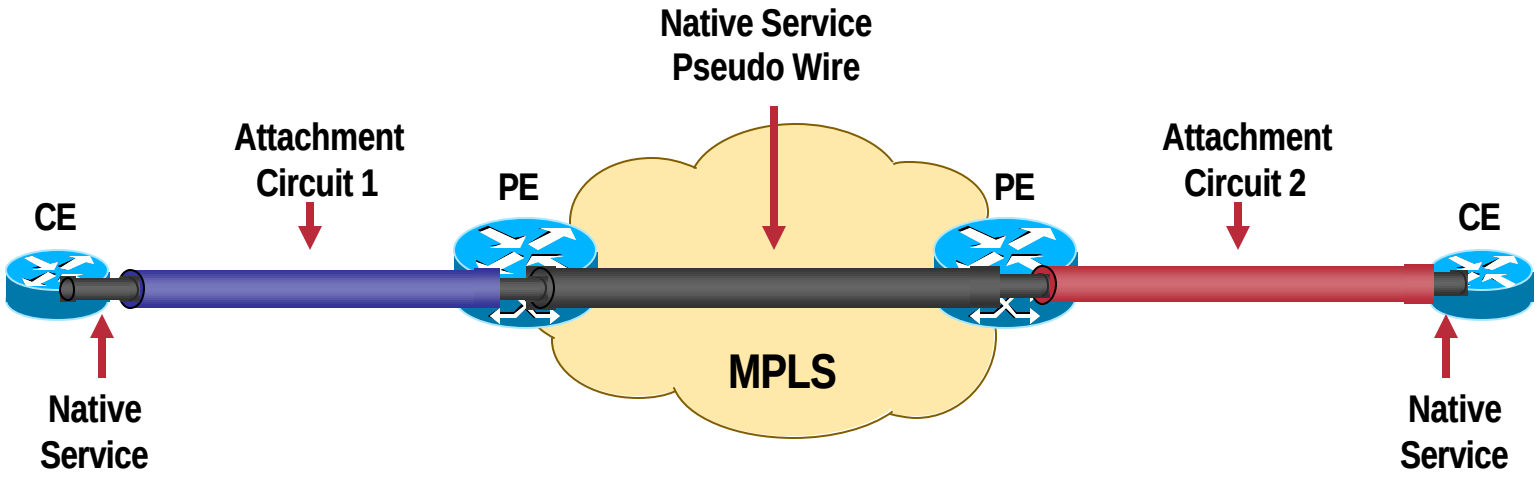
Layer 2 Service Interworking

Cisco.com



Inter-working Function (IWF) terminates the protocol used in one network and translates it to the protocol used in the other network

Layer 2 Interworking



Interworking achieved by common Native Service (e.g. Ethernet) between CEs and local AC termination

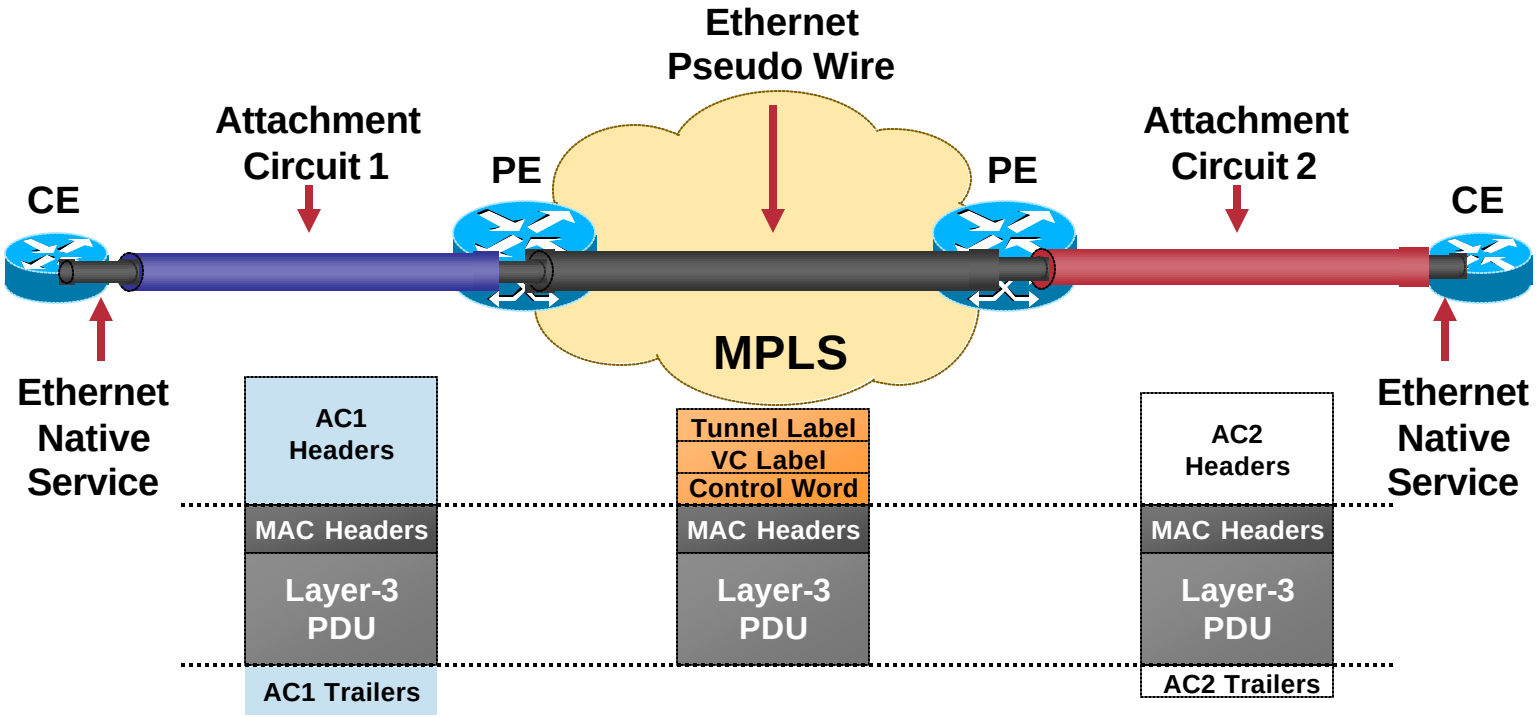
AC has to be able to carry Native Service

Two Native Services available for Interworking

- **Ethernet – (`interworking ethernet`)**
- **IP – (`interworking ip`)**

Based on draft-sajassi-l2vpn-interworking and MFA Interworking draft

Ethernet Interworking

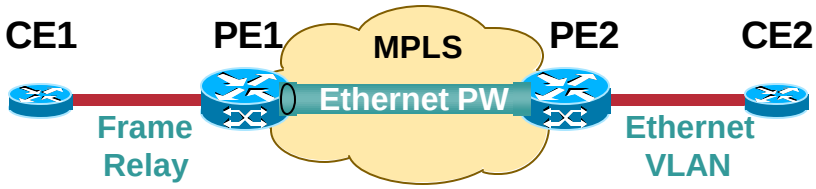


FR, ATM, PPP/HDLC use bridged encapsulation to carry Ethernet frames (ATM: RFC 2684-B, FR: RFC 2427-B, PPP: RFC 2878)

CEs may be required to use bridging (IRB/RBE)

Ethernet Interworking Configuration Example

Cisco.com



CE1

```
!
bridge irb
!
interface Serial1/0:1
 no ip address
 encapsulation frame-relay
!
interface Serial1/0:1.18 point-to-point
 frame-relay interface-dlci 18
 bridge-group 1
!
interface BVI1
 ip address 192.168.5.1 255.255.255.252
!
!
bridge 1 protocol ieee
bridge 1 route ip
!
```

CE2

```
!
interface FastEthernet1/0.4
 encapsulation dot1Q 400
 ip address 192.168.5.2 255.255.255.252
!
```

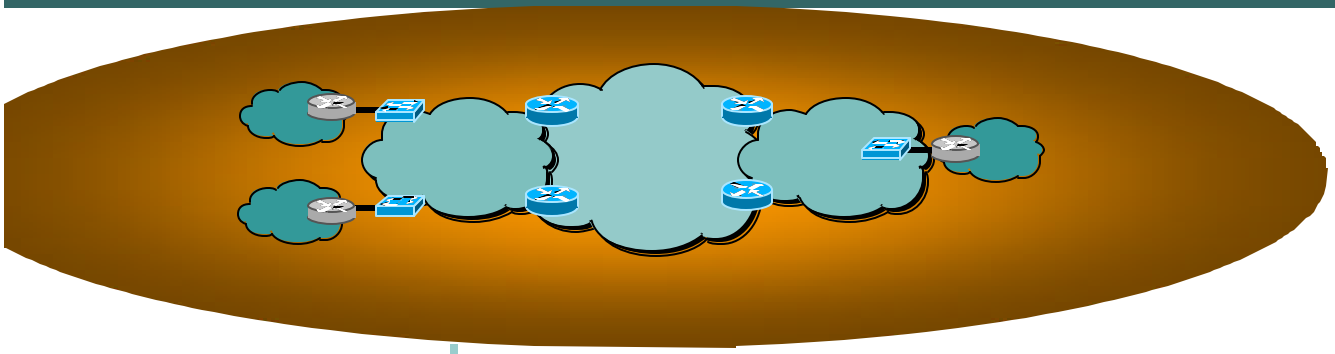
PE1

```
!
frame-relay switching
mpls label protocol ldp
!
pseudowire-class FR-VLAN-PW
 encapsulation mpls
 interworking ethernet
!
interface Serial2/0:1
 no ip address
 no ip directed-broadcast
 encapsulation frame-relay
 frame-relay interface-dlci 18 switched
  class FR-17-20
 frame-relay intf-type dce
!
!
connect FR-18-PE1 Serial2/0:1 18 l2transport
 xconnect 172.16.255.1 118 pw-class FR-VLAN-PW
!
```

PE2

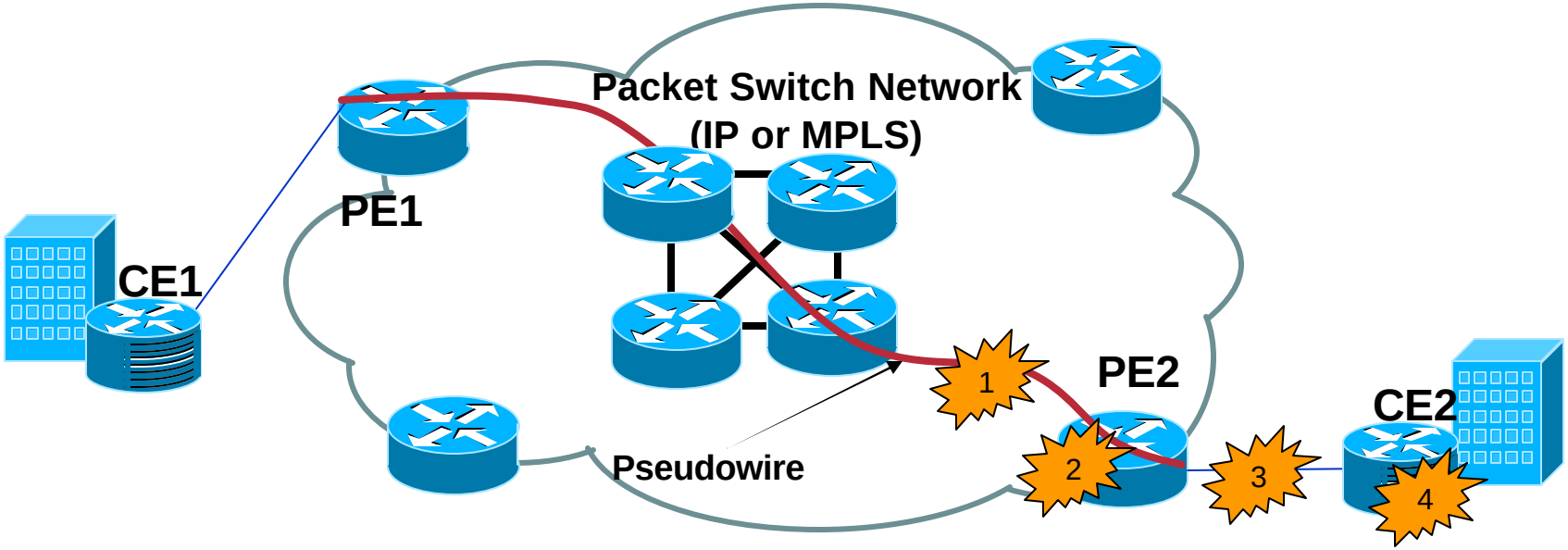
```
!
mpls label protocol ldp
!
pseudowire-class VLAN-FR-PW
 encapsulation mpls
 interworking ethernet
!
interface FastEthernet1/1/1.4
 encapsulation dot1Q 400
 no ip directed-broadcast
 no cdp enable
 xconnect 172.16.255.4 118 pw-class VLAN-FR-PW
!
```

Agenda



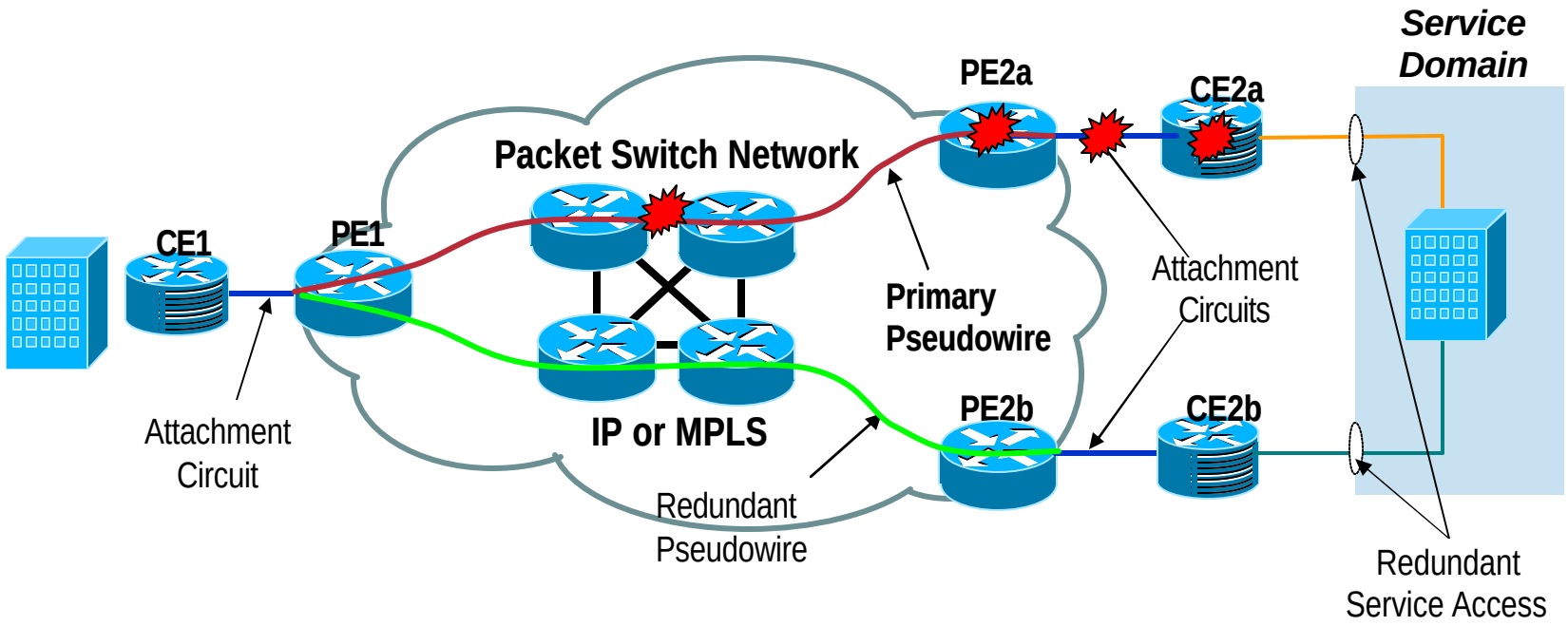
- Introduction to L2VPNs & L2VPN Service Classification
- Point-to-Point Technologies
  - Any Transport over MPLS (AToM) Overview
  - Layer 2 Tunneling Protocol Version 3 (L2TPv3)
  - Advanced Concepts
    - Layer 2 Interworking, PW Redundancy, PW Switching
- Multipoint Technologies
  - IEEE Provider Bridges (P 802.1ad)
  - Virtual Private LAN Services
- Deployment Aspects
  - Operational Aspects, OAM
  - QoS
  - Security

Pseudowire Service Failure Points



1. PSN failure due to end-to-end routing failure
2. PE failure due to HW or SW fault
3. Attachment circuit failure due to line break
4. CE failure due to HW or SW fault

Pseudowire Redundancy - Single Side Full Redundancy



- **Active-Standby Approach to Redundancy**

  Ensure Access to redundant Service Access Points

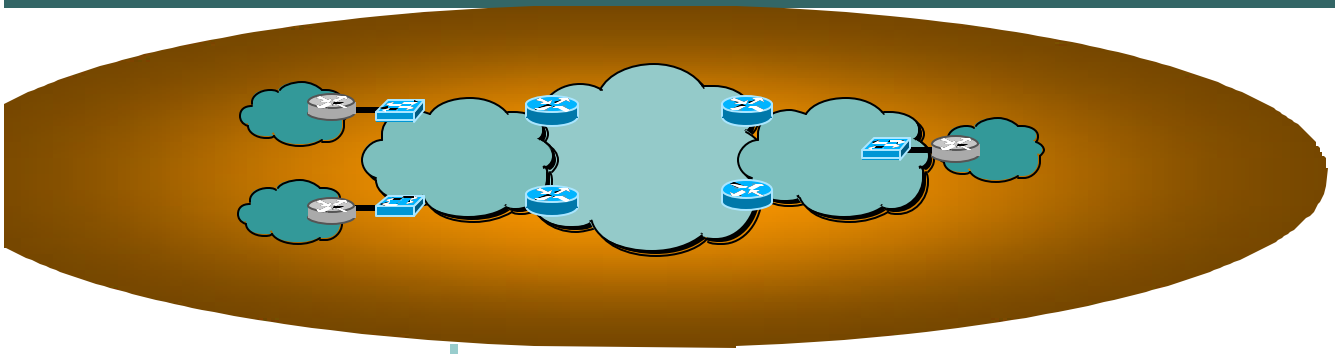
- **PW-Redundancy is End-to-End, can be combined with SSO/NSF and FRR**

PW Redundancy CLI
Active-Standby (similar to dial-backup feature)


```
xconnect <ip-addr> <vcid> pw-class <name>
 backup peer <ip-addr> <vcid> <pw-class <x>> priority <value>
 backup delay <enable-delay> <disable-delay | never>
```

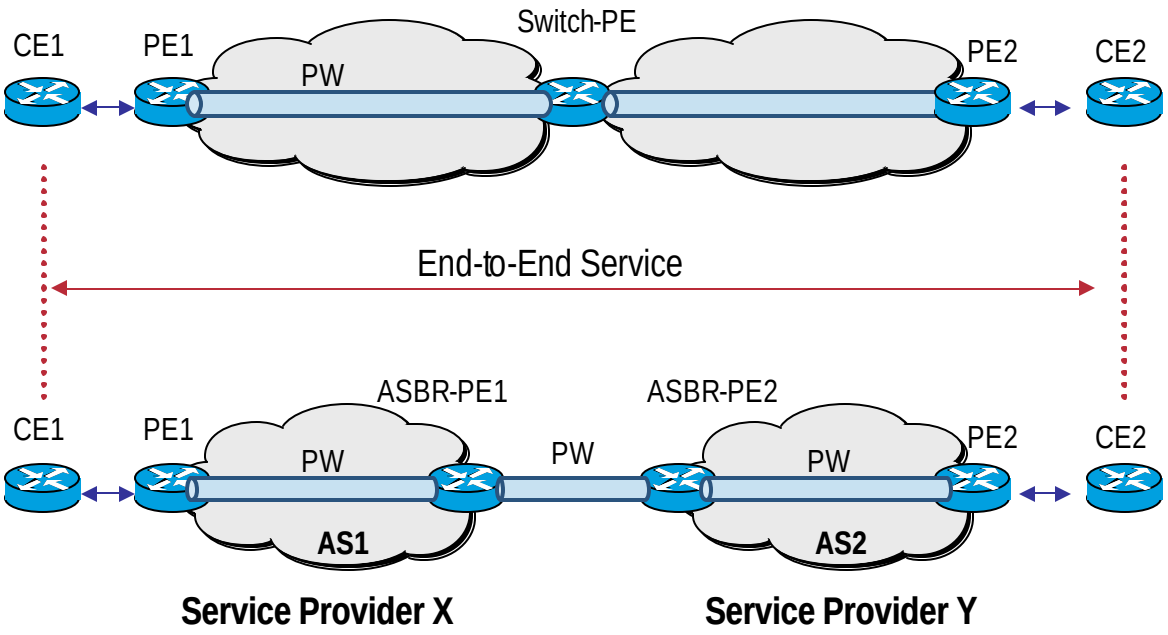
- **Multiple Redundant Peers supported**
- **Revertive Switch-Over Support**
  - **Dampening support to avoid frequent switchover (enable-delay/dis-able delay)**
- **Failure Detection**
  - **Attachment Circuit can be caused by interface condition (up/down/LOS) or integrated LMI notification**
  - **AToM PW failure discovered by LDP timeout**
  - **L2TPv3 PW failure identified by control plane keepalive failure**
- **Forced Switchover Support**
  - Router> xconnect backup force-switchover peer <ip-addr> <vcid>
  - Router> xconnect backup force-switchover interface <ifcname>

Agenda



- Introduction to L2VPNs & L2VPN Service Classification
- Point-to-Point Technologies
  - Any Transport over MPLS (AToM) Overview
  - Layer 2 Tunneling Protocol Version 3 (L2TPv3)
  - Advanced Concepts
    - Layer 2 Interworking, PW Redundancy, PW Switching
- Multipoint Technologies
  - IEEE Provider Bridges (P 802.1ad)
  - Virtual Private LAN Services
- Deployment Aspects
  - Operational Aspects, OAM
  - QoS
  - Security

Intra-AS and Inter-AS Pseudowires



- **Objective: Extend PWs across an Inter-AS boundary or across two separate MPLS networks**
- ***"Inter-provider model"* (PW spans across 2 different service provider domains or AS's)**

  SP will have "no" or "very limited" levels of trust between people managing different AS's – as well as different network policies (QoS, Security).

3 Models

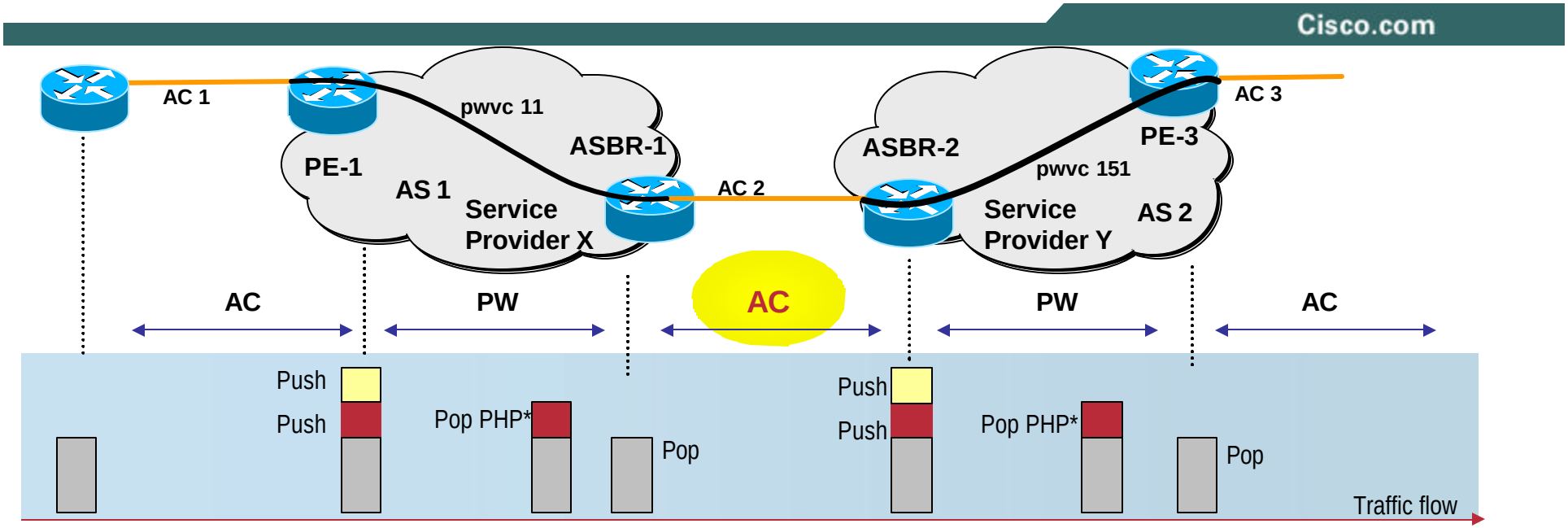
Attached Circuit model
RFC2547bis*, section 10a like

Pseudo-wire Switching Model
RFC2547bis*, section 10b like

Multi-AS tunnel LSP Model
RFC2547bis*, section 10c like

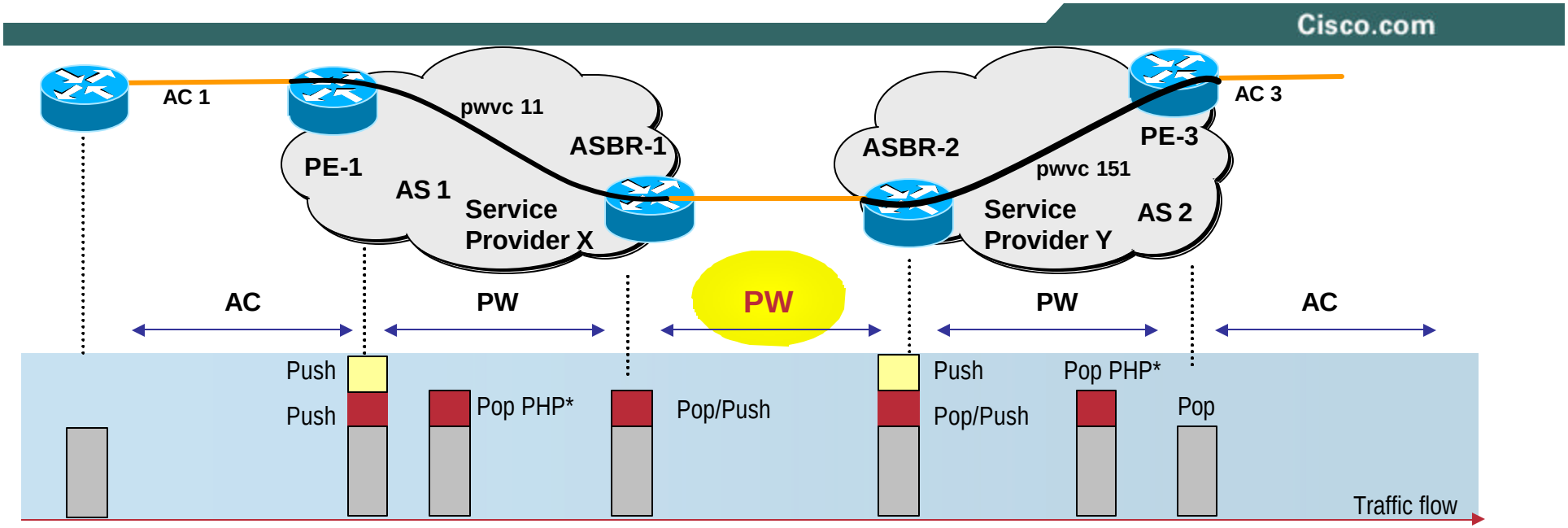
* draft-ietf-l3vpn-rfc2547bis-03.txt

Attached Circuit between ASBR's Model



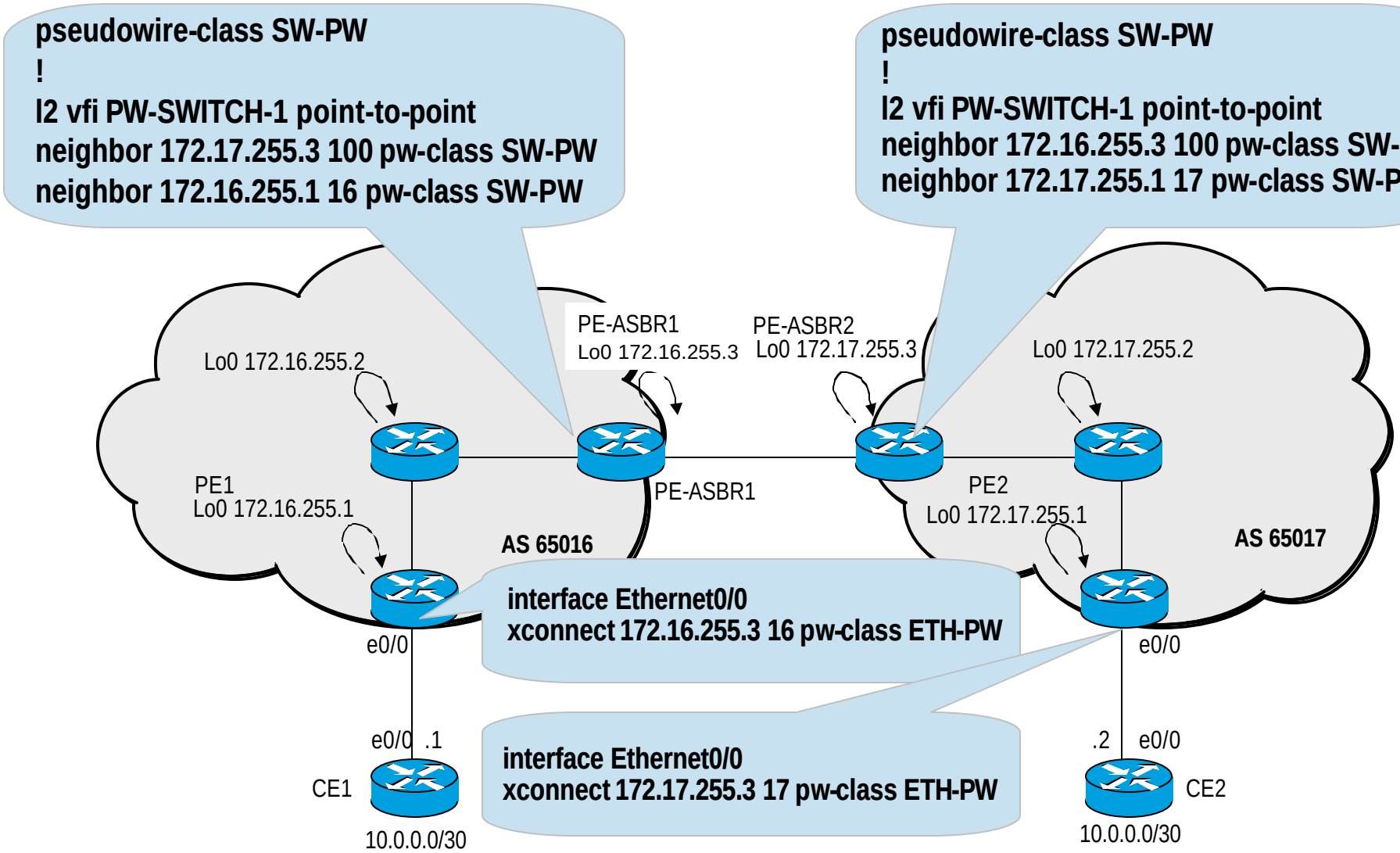
- **Simple, well-known solution, since already utilised by ATM/FR SP's.**
- **Security model: Trusted (auto-discovery, LDP, IGP is local to AS)**
- **QoS model: Independent**
- **Complex Provisioning (Lot's of ACs to be configured between ASBRs)**
- **Link between both ASBR's has to be same type or interworking function has to be involved as per attached circuit**

Pseudo-Wire Switching Model
PW between ASBRs

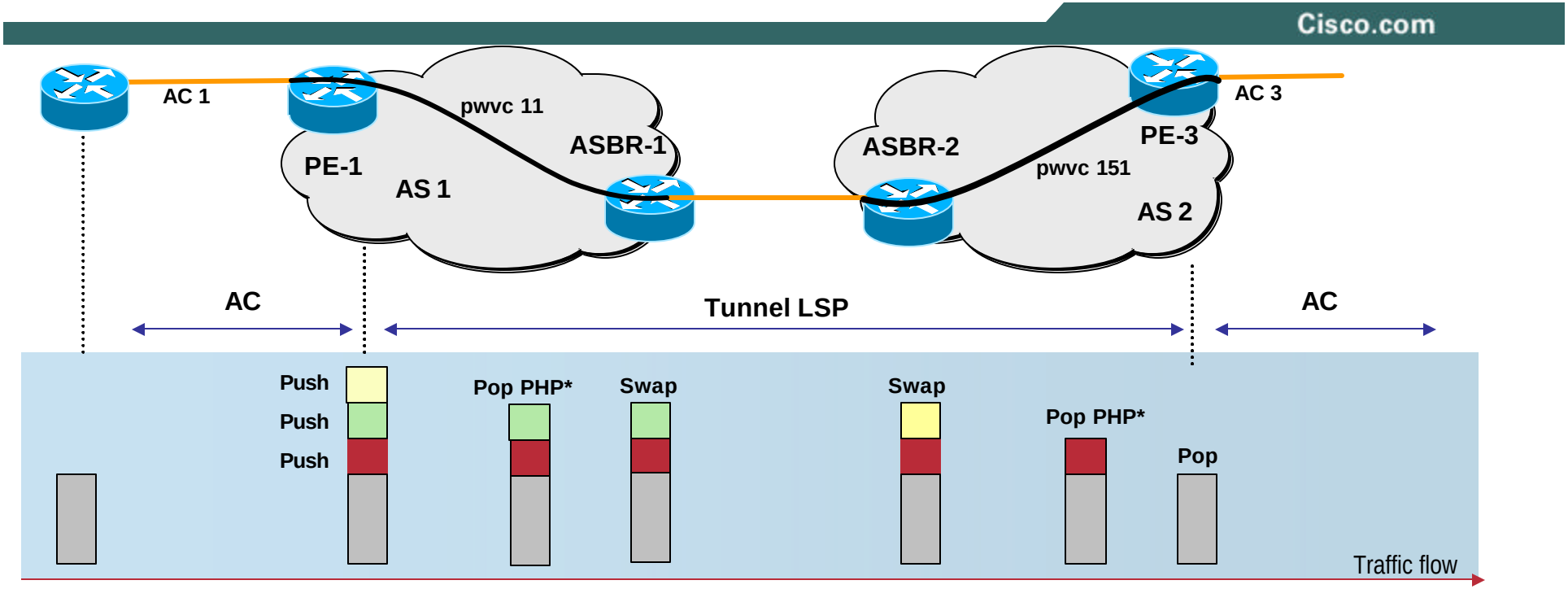


- **Security model: Almost Trusted (LDP, IGP cross boundary of SP's but is limited to neighbour ASBR), IP-Addr of PE-3 unknown to SP X**
- **QoS model: Independent**
- **Simplified Provisioning**
- **No Interworking on ASBR-ABSR link required:**
  Link between ASBR's is independent of attached-circuit media

Pseudowire-Switching
Configuration Example (12.0(31)S)

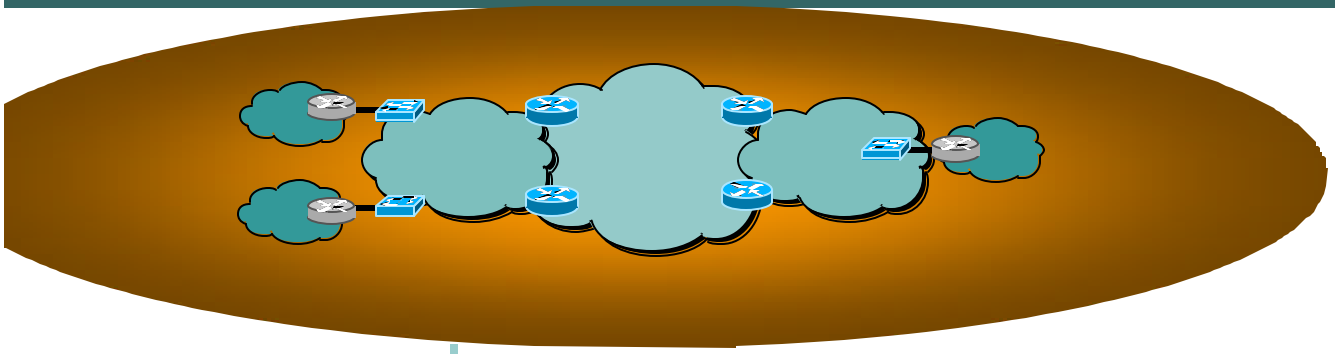


Multi-AS tunnel LSP model



- **Re-utilize RFC2547bis Multi-AS 10c or Multi-AS TE to build end-end tunnel LSP and end-to-end PW VCs**
- **Link between ASBR's is independent of attached-circuit media, on same link, we could have ATM, FR, Ethernet PW, and/or other services (IP, MPLS-VPN, …)**

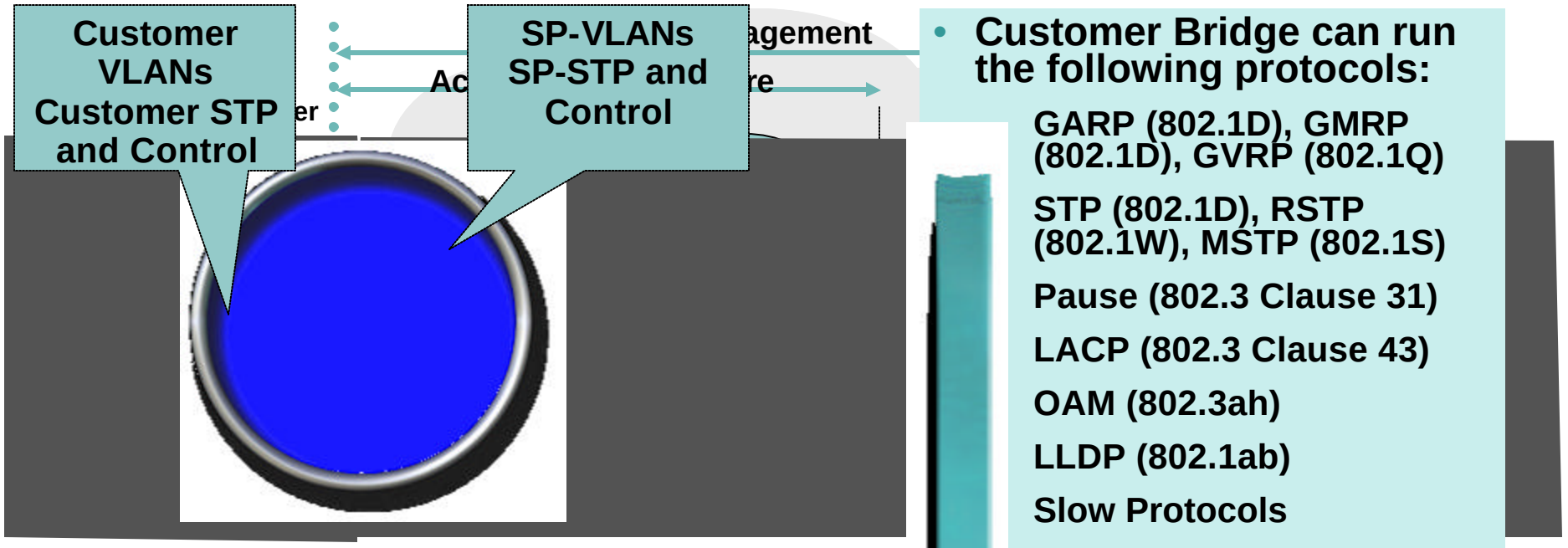
Agenda



- **Introduction to L2VPNs & L2VPN Service Classification**
- **Point-to-Point Technologies**
  - **Any Transport over MPLS (AToM) Overview**
  - **Layer 2 Tunneling Protocol Version 3 (L2TPv3)**
  - **Advanced Concepts**
    - **Layer 2 Interworking, PW Redundancy, PW Switching**
- **Multipoint Technologies**
  - **IEEE Provider Bridges (P 802.1ad)**
  - **Virtual Private LAN Services**
- **Deployment Aspects**
  - **Operational Aspects, OAM**
  - **QoS**
  - **Security**

Connecting Customers to Provider Domain

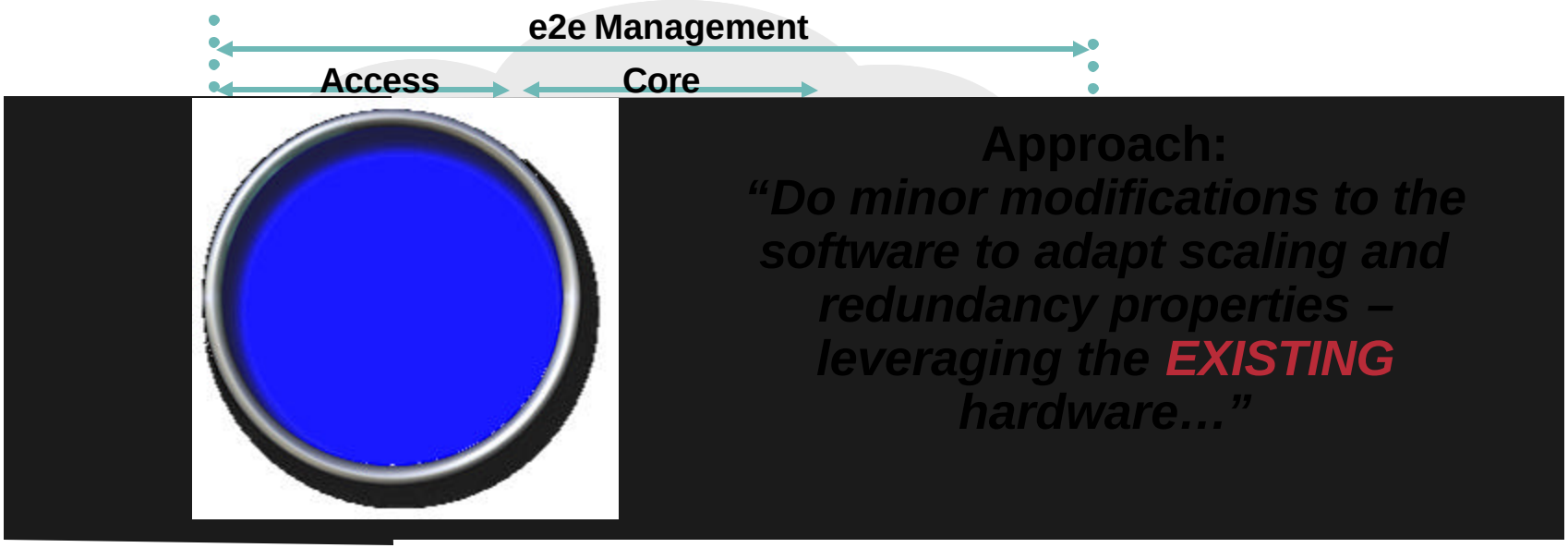
Cisco.com



- Provide an Ethernet Service to Customers (with or without VLANs)
  - Service should be transparent to the customer

- Customer Bridge can run the following protocols:
  - GARP (802.1D), GMRP (802.1D), GVRP (802.1Q)
  - STP (802.1D), RSTP (802.1W), MSTP (802.1S)
  - Pause (802.3 Clause 31)
  - LACP (802.3 Clause 43)
  - OAM (802.3ah)
  - LLDP (802.1ab)
  - Slow Protocols
  - Port-based Network Access Control (802.1X)
- AC dependent
  - Operate transparently
  - Discard them
  - Peer with them
  - Snoop them

Building Access Networks
IEEE 802.1ad Provider Bridges Approach



- **IEEE P802.1ad Provider Bridges**
  - **Reserves a block of MAC addresses (out of the block of 32) for the operation of customer bridges**
  - **Describes which of these reserved MAC addresses to be used for peering & how the peering is performed**
  - **Describes how & where to do discarding customer protocols (filtering action), describes how & where to tunnel them**

Allocation of Addresses
(as per Mar/05 802.1 meeting)

Cisco.com

Address	802.1Q Bridge	Provider Bridge
01:80:C2:00:00:00	BPDUs	Treat as Data
01:80:C2:00:00:01	802.3 Pause	802.3 Pause
01:80:C2:00:00:02	Slow Protocols	.3ah OAM, .3ad LACP / Slow Protocols
01:80:C2:00:00:03	802.1X	Providers' .1ab LLDP
01:80:C2:00:00:04	LLDP	Treat as Data
01:80:C2:00:00:05	Reserved: Do not pass through	Reserved
01:80:C2:00:00:06		Reserved
01:80:C2:00:00:07		Reserved
01:80:C2:00:00:08		.1ad Provider BPDU
01:80:C2:00:00:09		Reserved
01:80:C2:00:00:0A		Reserved
01:80:C2:00:00:0B		Reserved
01:80:C2:00:00:0C		Reserved
01:80:C2:00:00:0D		.1ad GVRP
01:80:C2:00:00:0E		Customers' .1X, LACP
01:80:C2:00:00:0F		Reserved

Building Provider Ethernet Access Networks
IEEE 802.1ad Provider Bridges

- **Customer VLAN Transparency**

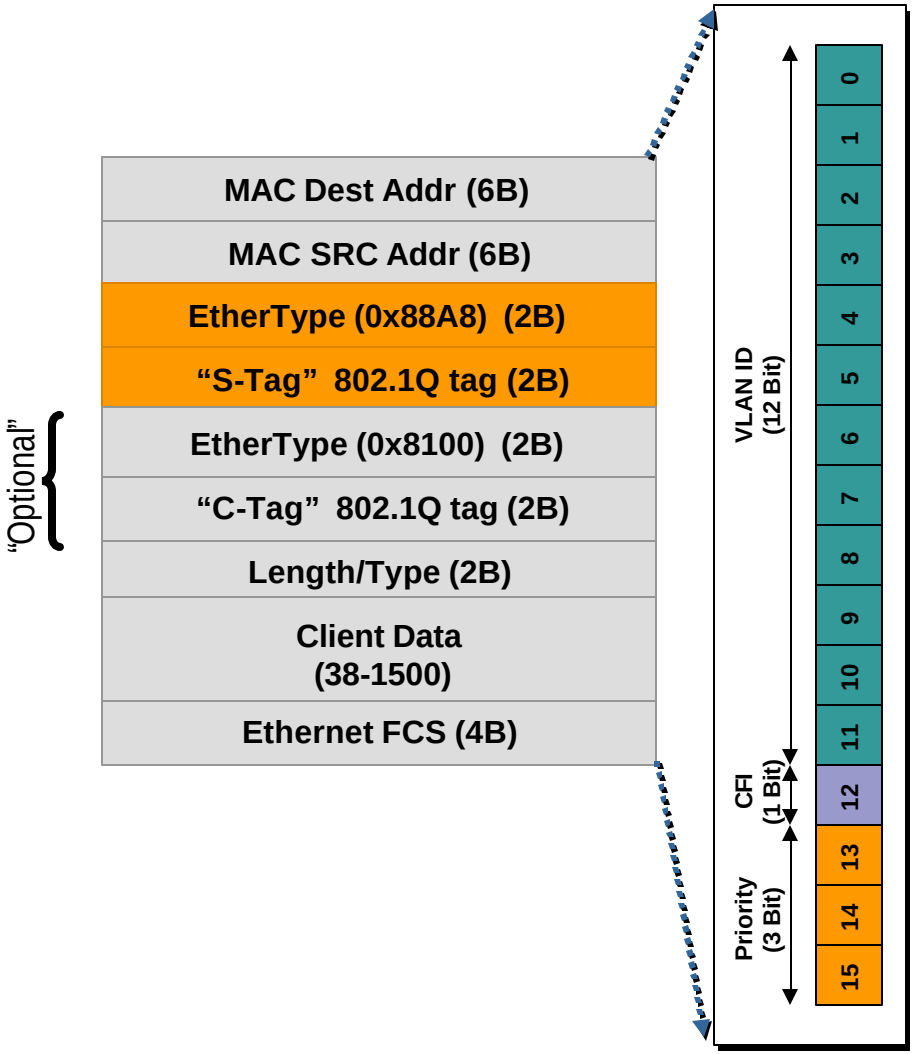
  IEEE 802.1ad Provider Bridges will provide a standardized version of "QinQ" (Note: Inner .1Q tag is optional)

  Standard will include additional enhancements

- **Frame Format same "QinQ"**

  New Ethertype: 0x88A8

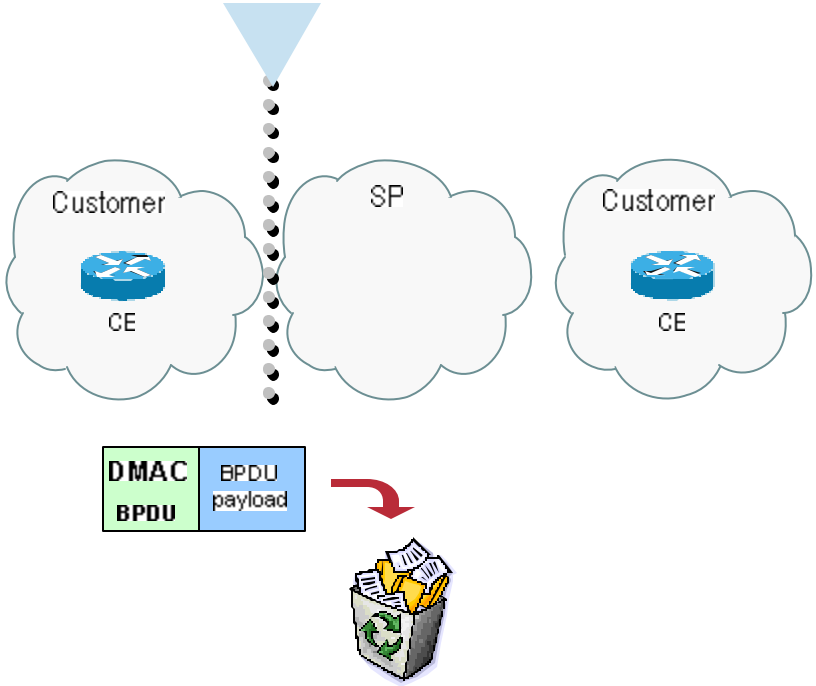
- **Draft Technically complete**



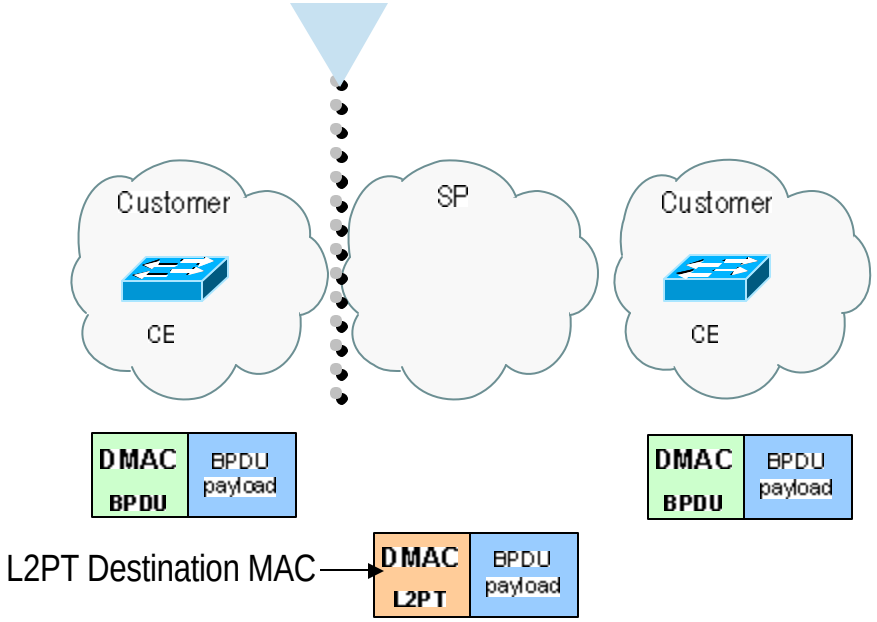
- **http://www.ieee802.org/1/pages/802.1ad.html**

L2 Control Processing Implementation

Behavior: "Discard"
Feature: MAC Access Lists

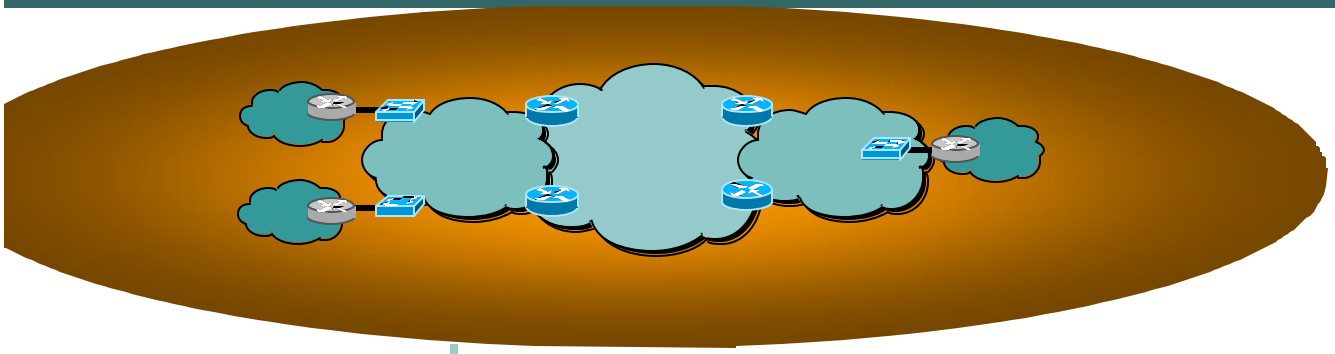


Behavior: "Tunnel"
Feature: L2 Protocol Tunneling (L2PT)



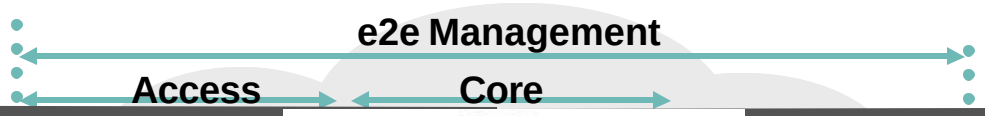
- **Pre-Standard P802.1ad solution across Catalyst LAN switches and the Cisco 7600 in hardware**
- **Configurable L2 Control Protocol parameters that allows a Provider to selectively peer, tunnel or drop**

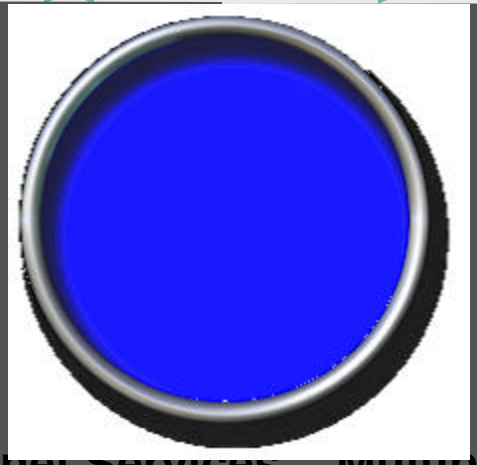
Agenda



- **Introduction to L2VPNs & L2VPN Service Classification**
- **Point-to-Point Technologies**
  - **Any Transport over MPLS (AToM) Overview**
  - **Layer 2 Tunneling Protocol Version 3 (L2TPv3)**
  - **Advanced Concepts**
    - **Layer 2 Interworking, PW Redundancy, PW Switching**
- **Multipoint Technologies**
  - **IEEE Provider Bridges (P 802.1ad)**
  - **Virtual Private LAN Services**
- **Deployment Aspects**
  - **Operational Aspects, OAM**
  - **QoS**
  - **Security**

IETF's Way to multipoint L2 Service: VPLS





- **Provide Layer-2 Ethernet Services – Multipoint capable**

  A service which looks, smells and behaves like a bridge when experienced by a customer

- **CE devices can be**

  Hosts, Bridges, Routers (if CE devices would be limited to routers only, IPLS would be a consideration)

- **IETF L2VPN WG: Virtual Private LAN Services (VPLS)**

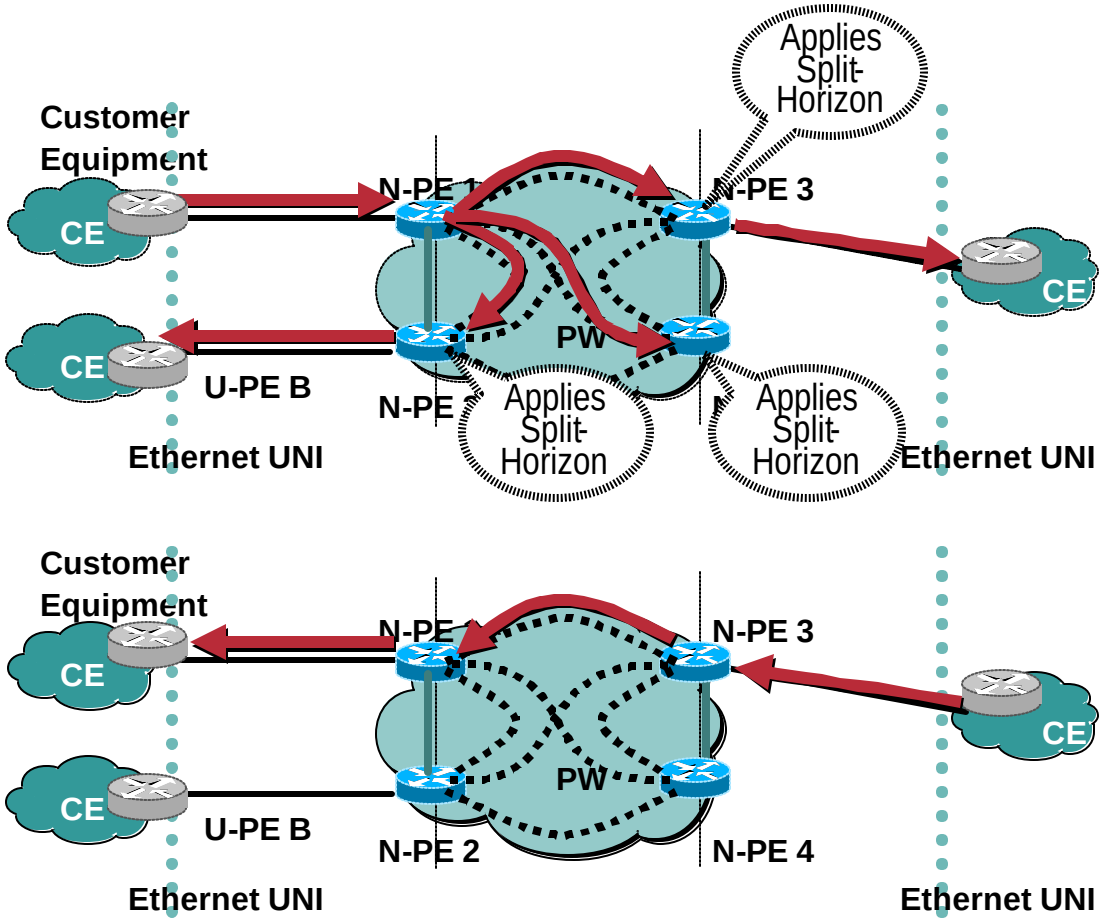
  Emulate a big-fat virtual Layer-2 Switch

  draft-ietf-l2vpn-vpls-ldp-06.txt (various + Cisco)

  draft-ietf-l2vpn-vpls-bgp-05.txt

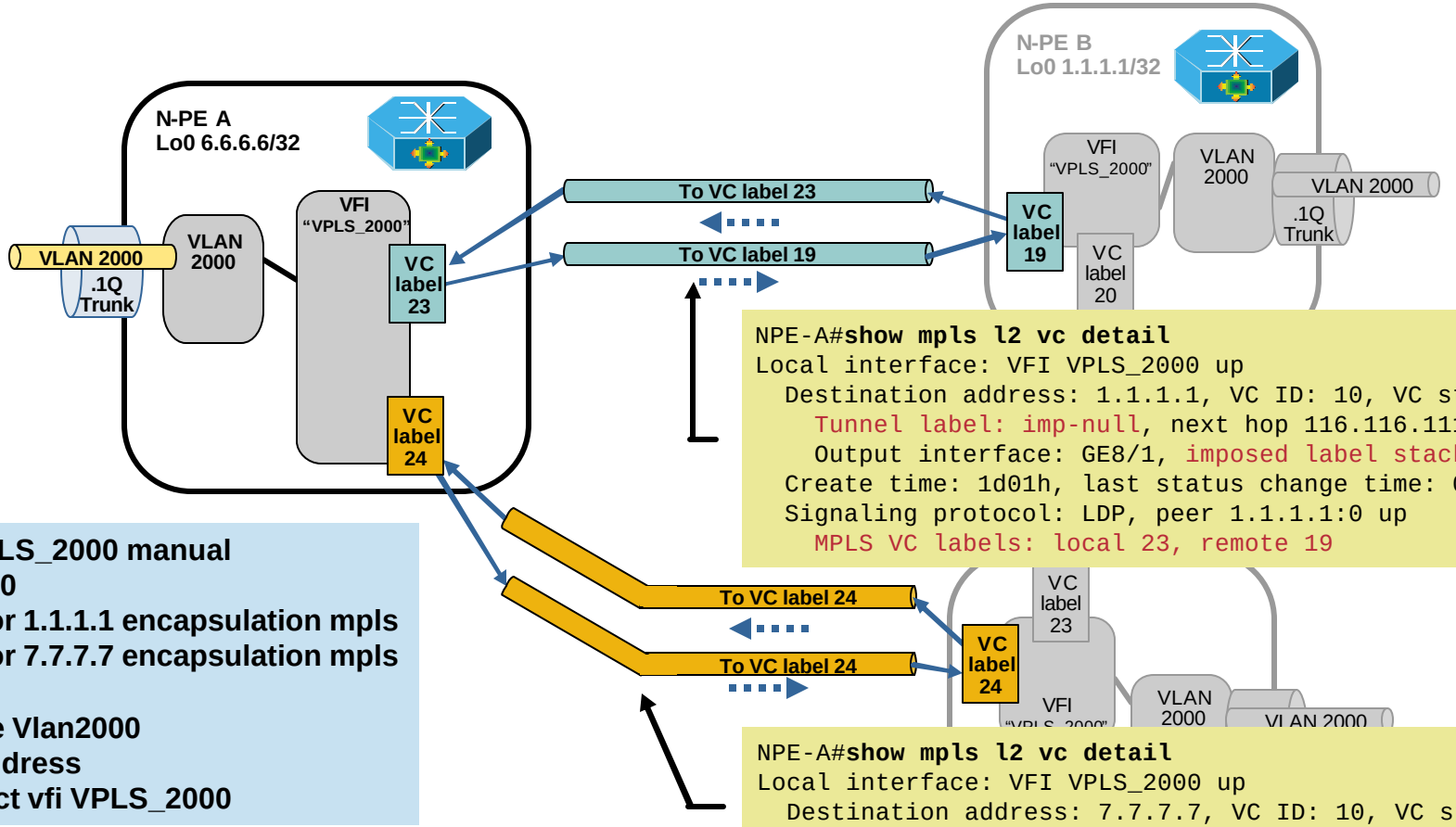
How VPLS works...

(Almost) 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**

VPLS Configuration/Verification



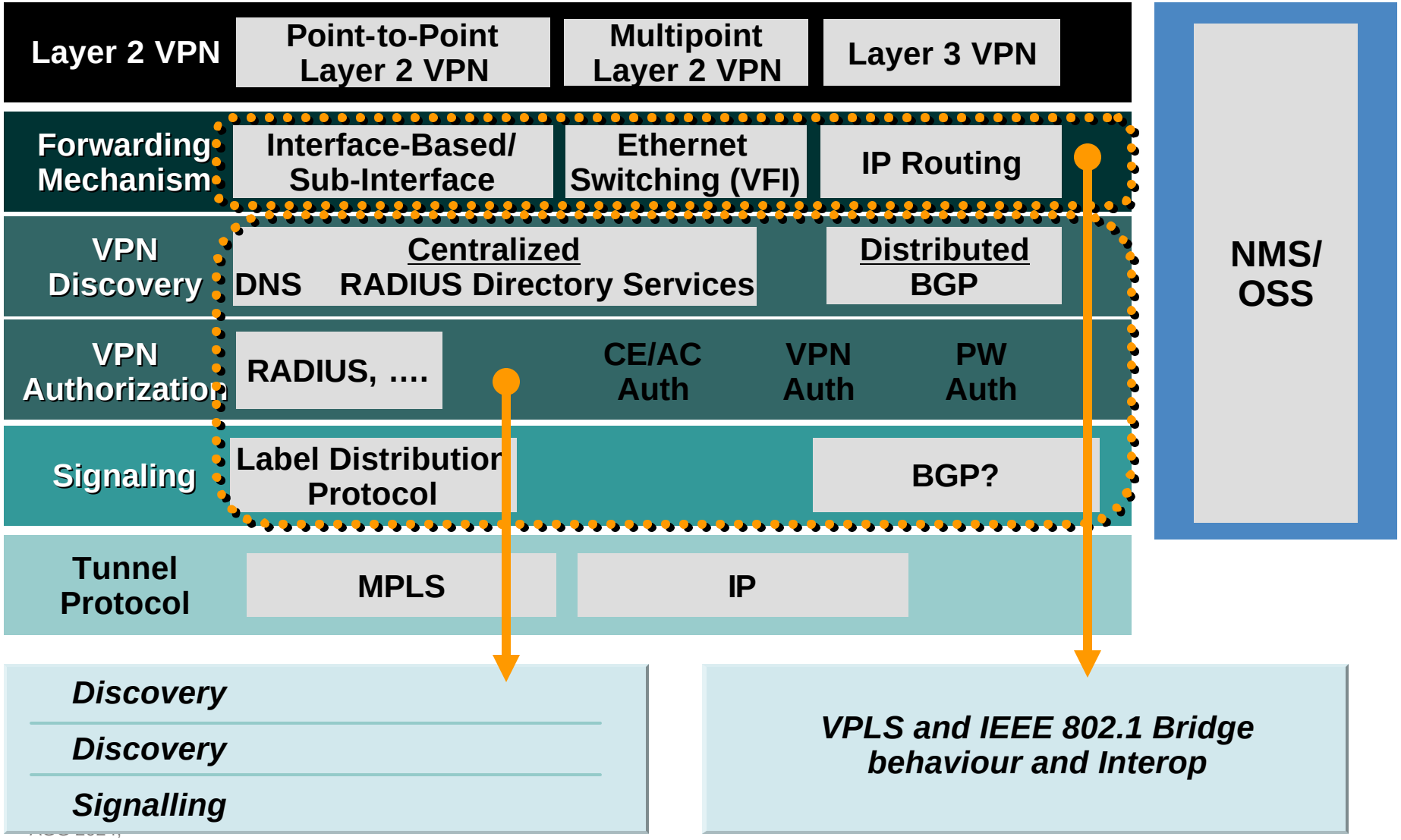

```
l2 vfi VPLS_2000 manual
 vpn id 10
 neighbor 1.1.1.1 encapsulation mpls
 neighbor 7.7.7.7 encapsulation mpls

interface Vlan2000
 no ip address
 xconnect vfi VPLS_2000
```

```
NPE-A#show mpls l2 vc detail
Local interface: VFI VPLS_2000 up
  Destination address: 1.1.1.1, VC ID: 10, VC status: up
    Tunnel label: imp-null, next hop 116.116.111.1
    Output interface: GE8/1, imposed label stack {19}
  Create time: 1d01h, last status change time: 00:40:16
  Signaling protocol: LDP, peer 1.1.1.1:0 up
    MPLS VC labels: local 23, remote 19
```

```
NPE-A#show mpls l2 vc detail
Local interface: VFI VPLS_2000 up
  Destination address: 7.7.7.7, VC ID: 10, VC status: up
    Tunnel label: imp-null, next hop 167.167.222.7
    Output interface: GE8/4, imposed label stack {24}
  Create time: 1d01h, last status change time: 1d00h
  Signaling protocol: LDP, peer 7.7.7.7:0 up
    MPLS VC labels: local 24, remote 24
```

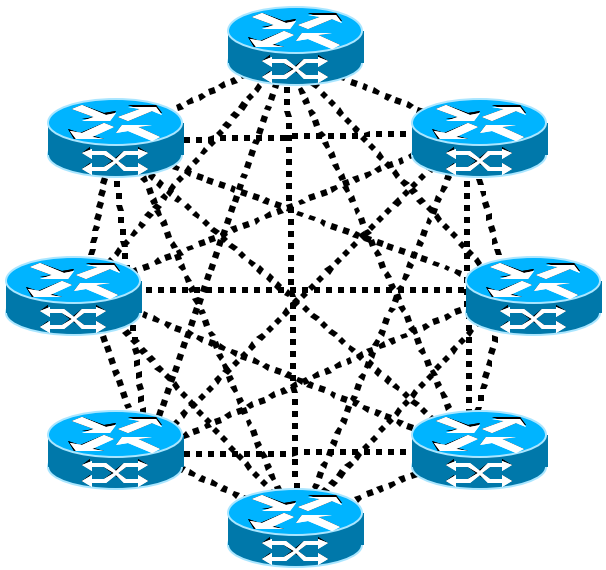
```
NPE-A#show mpls l2 vc
Local intf     Local circuit Dest address  VC ID  Status
-------------  ------------- ------------- ------ ------
VFI VPLS_2000  VFI           1.1.1.1       10     UP
VFI VPLS_2000  VFI           7.7.7.7       10     UP
```

VPLS Building Blocks & Major Work Areas



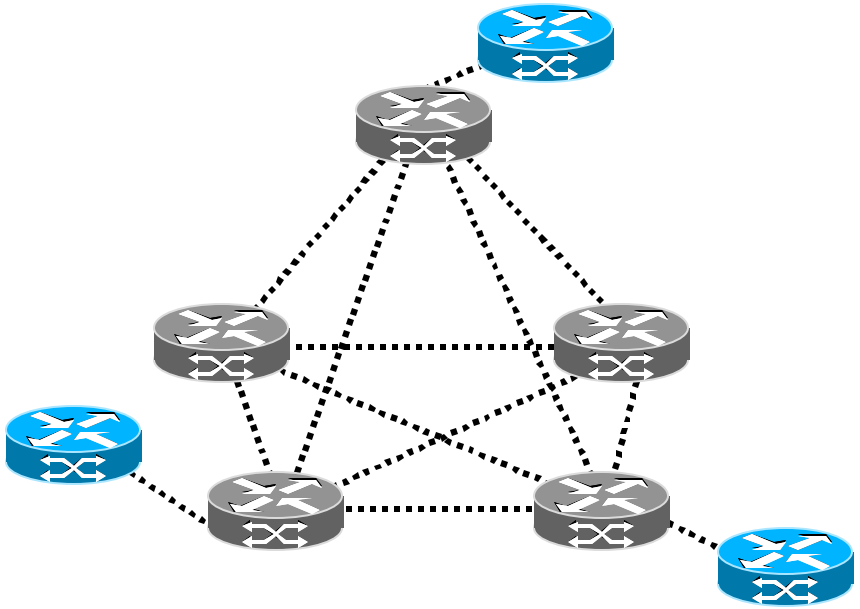
Hierarchical-VPLS: Why?

VPLS



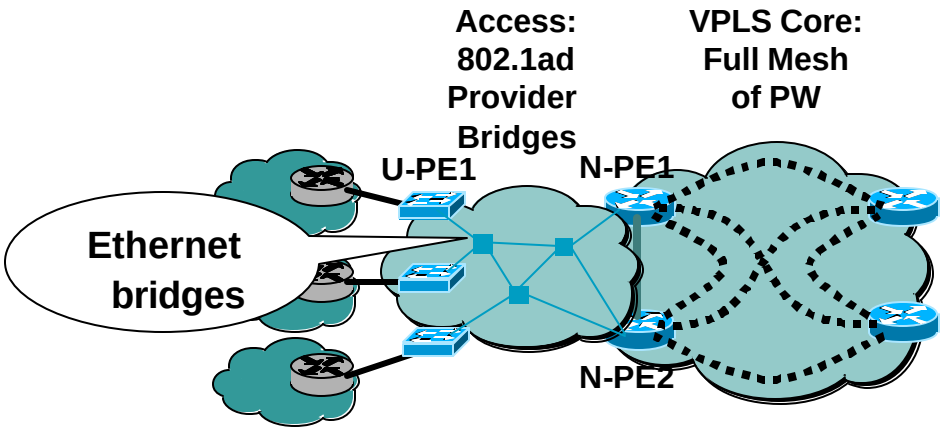
- Potential signaling overhead
- Full PW mesh from the Edge
- Packet replication done at the Edge
- Node Discovery and Provisioning extends end-to-end

H-VPLS

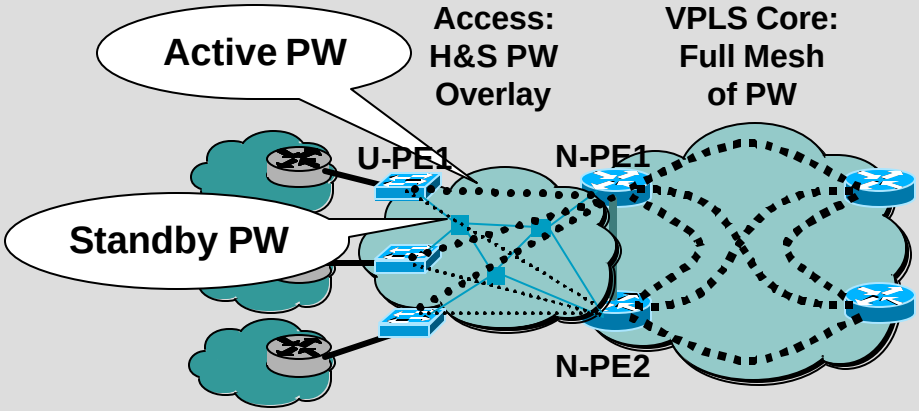


- Minimizes signaling overhead
- Full PW mesh among Core devices only
- Packet replication done the Core only
- Partitions Node Discovery process

H-VPLS flavors



"H-VPLS"
w/ Ethernet
Access



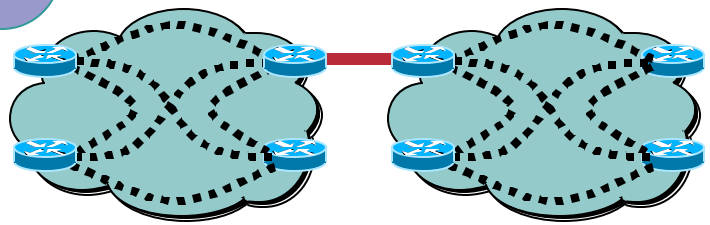
"H-VPLS"
w/ MPLS
to the edge

- IEEE 802.1ad Provider Bridges in the Access running 802.1s/w MSTP/RSTP, VPLS core (full-mesh of PW w/ split-horizon for loop-avoidance

- MPLS edge and core
  - Full-mesh of PW in core, split-horizon
  - Hub & Spoke access PW for access. Only one PW per U-PE (per service instance) active at a time

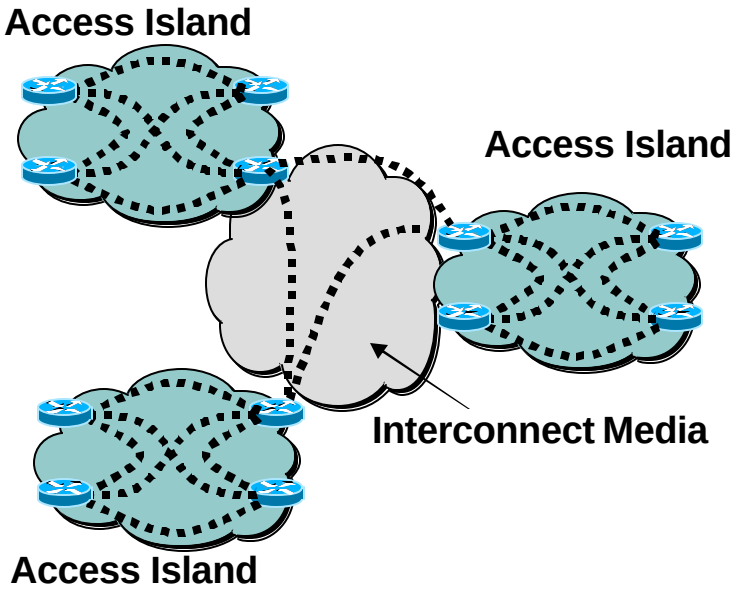
VPLS: Full Mesh at the Edge?

A



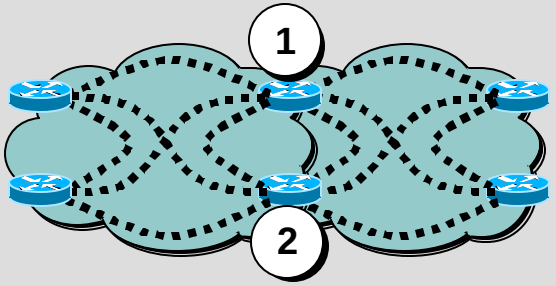
Works, but no redundancy…

B



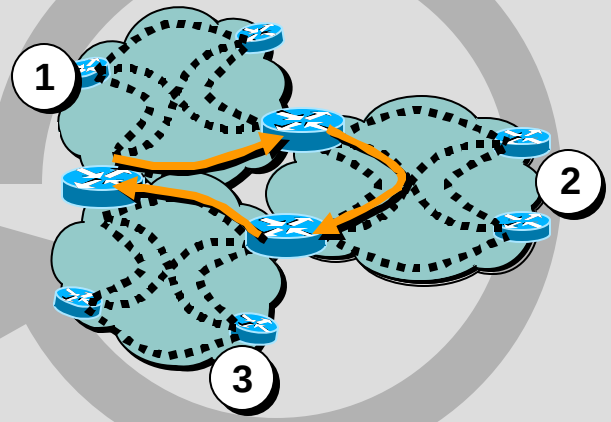
Works, but no redundancy…

C



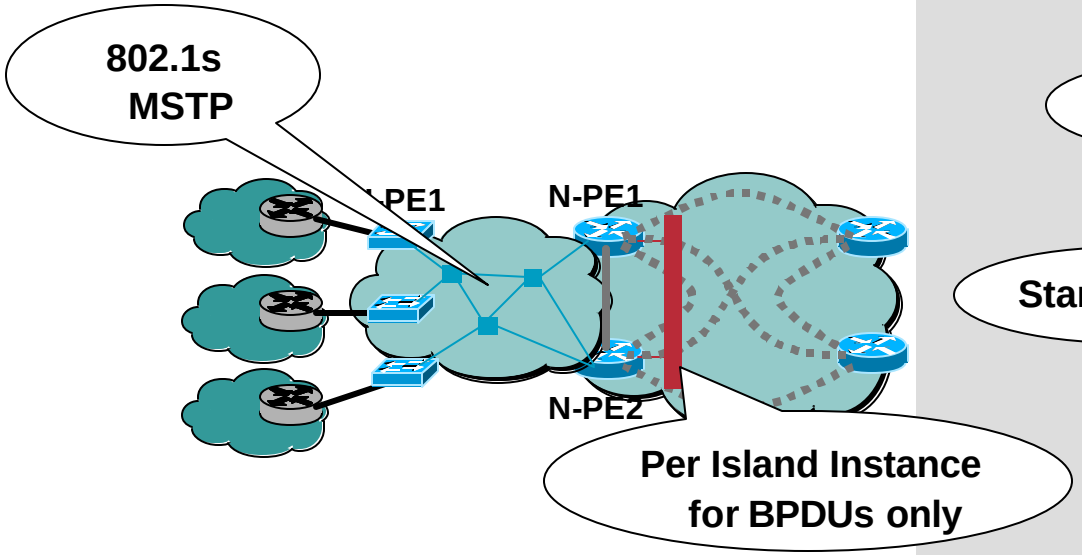
Does not work straight away – requires a protocol between (1) and (2)

D

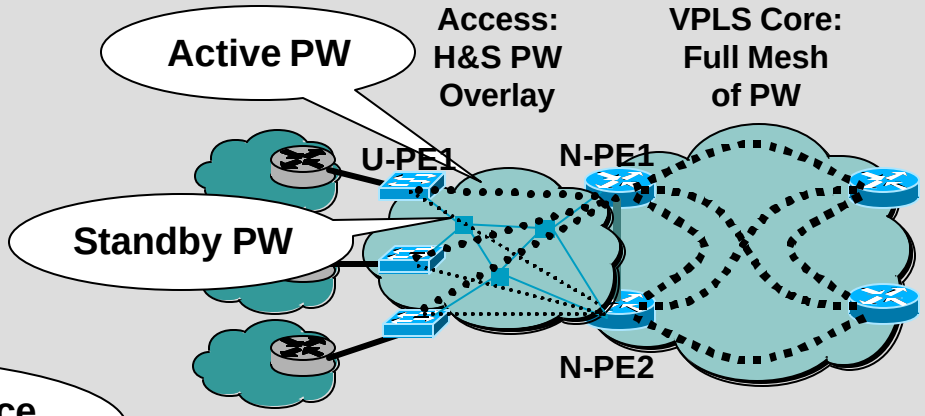


Does not work – loops – even if (c) is solved. Only way is a CENTRAL Interconnect media (like (B) – similar to Cisco's way)

H-VPLS: Redundant Access to Core

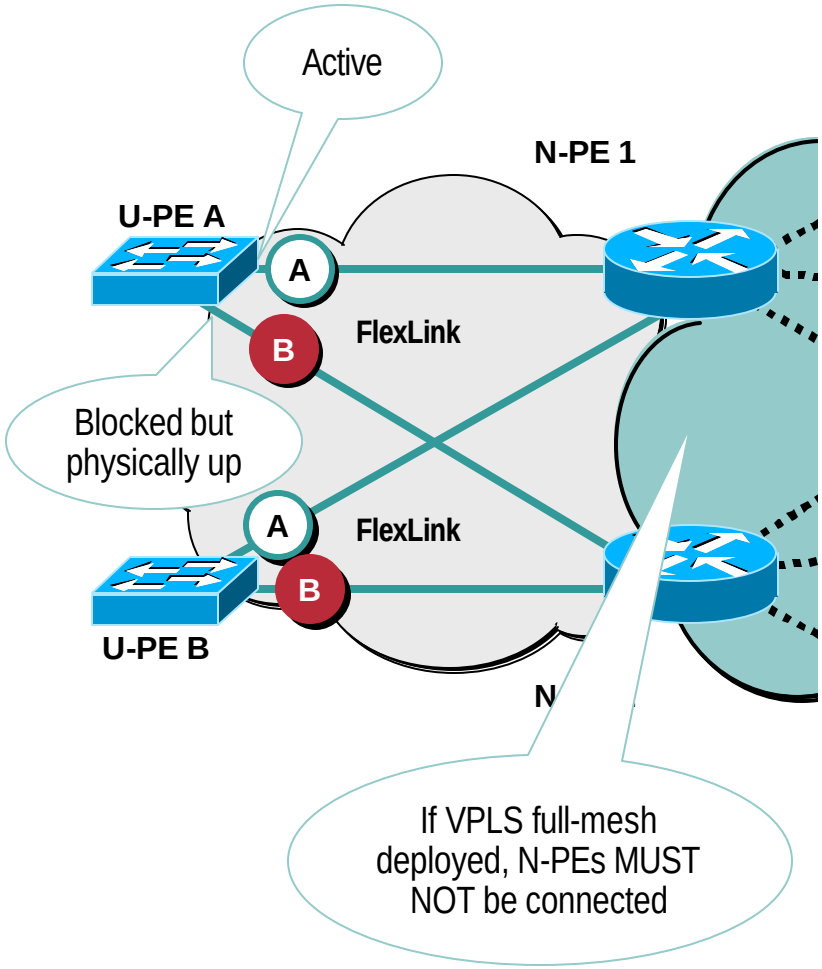


- Standard 802.1s
- Per Access Island "BPDU Instance"
- Constrained topology



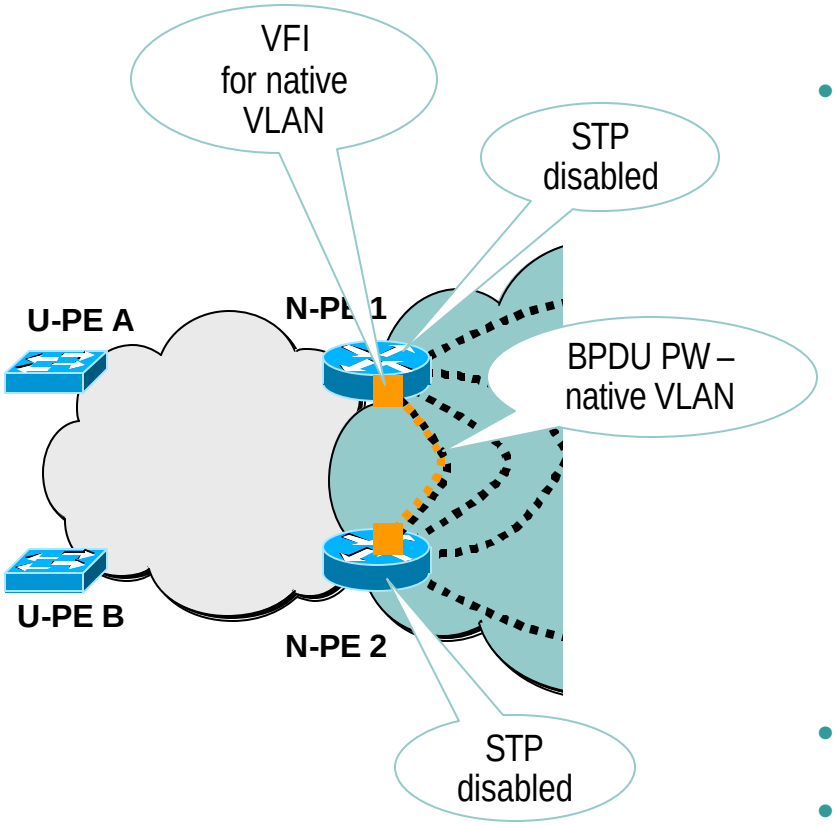
- Hub & Spoke access with only a single Attachment-Circuit active per Service Instance
- Constrained Topology

Redundancy between Core and Access
An Option: FlexLink



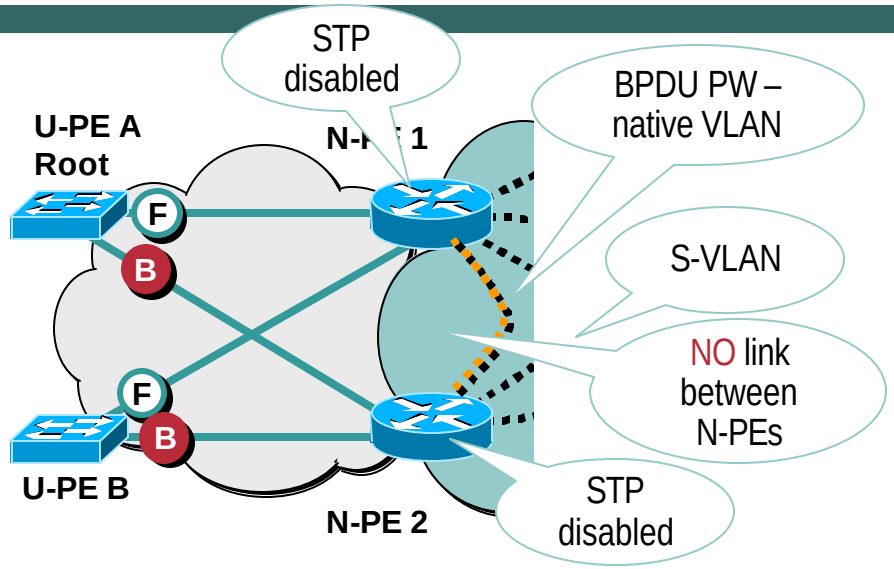
- U-PE dual-homed to N-PEs
- Convergence time = link failure detection time (optimized to sub 100ms on 3750); non-revertible
- Pros:
  - Simple (no STP)
  - N-PE is transparent
  - Faster convergence than STP
  - No Flooding during convergence; less volatile
- Cons:
  - No load sharing
  - Direct PE link w/o repeater or media converter (need UDLD, 802.3ah)
  - Hub&spoke access topology only

Redundancy between Core and Access
(Option 2) MST in the access island, no STP on N-PE

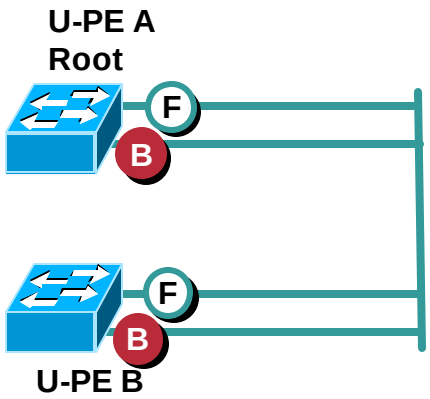


- **Assumptions**
  - **Each U-PE can reach MPLS core by a pair of N-PEs for a VPLS instance**
  - **Both N-PEs support the protected VPLS instance**
  - **Provide N-PE redundancy for path protection between U-PEs**
  - **MPLS core is protected; PWs are stable**
  - **MSTP is used for path selection in local L2 island**
- **N-PEs do not run STP**
- **One extra PW per VFI between pair of N-PE if local bridge is required between U-PEs**
- **A PW is provisioned to relay BPDU per MSTP: "BDPU PW"**

Redundancy between Core and Access
(Option 2) N-PE does not run STP, H&S access

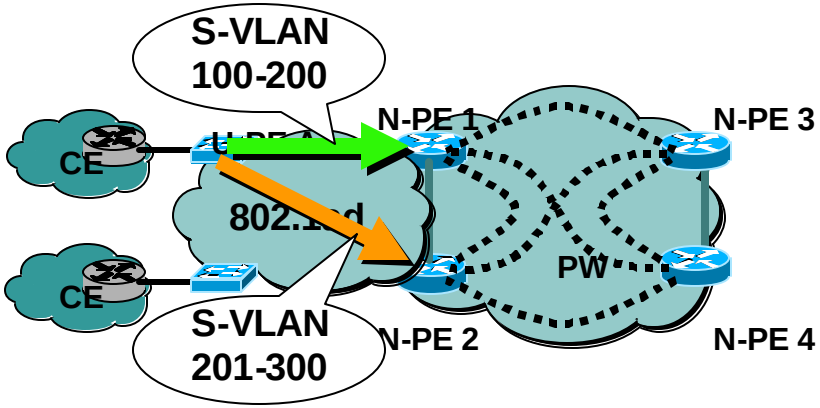


Logical view: Shared media



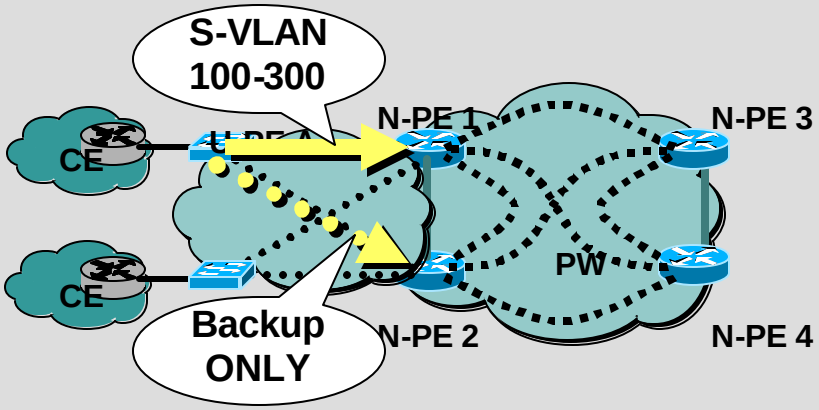
- **MSTP on U-PE**
- **Disable PE VLAN STP on N-PE**
- **Provision one PE VLAN as native VLAN for BPDU transport from U-PE**
- **Add one PW for the PE VLAN (native VLAN) between pair of N-PEs to transport MSTP BPDU**
- **Convergence time = MSTP convergence time (2 fw delay + 3 BPDU hello)**
- **May support load sharing per MSTP instance**
- **MSTP can be configured on U-PE independently**

Comparing H-VPLS: Load Sharing



**"H-VPLS"
w/ Ethernet
Access**

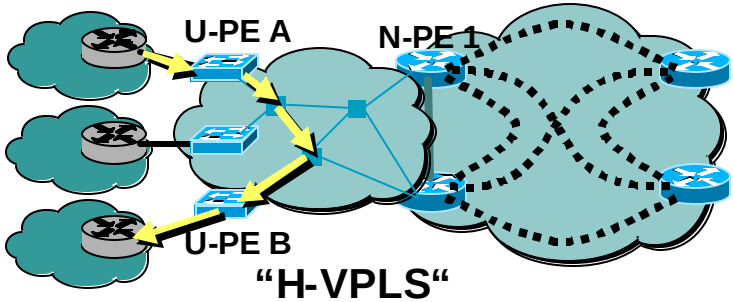
- **802.1s MSTP allows to map different vlans to different links and PEs (both PE active)**
- **Optimized use of bandwidth and PE resources**



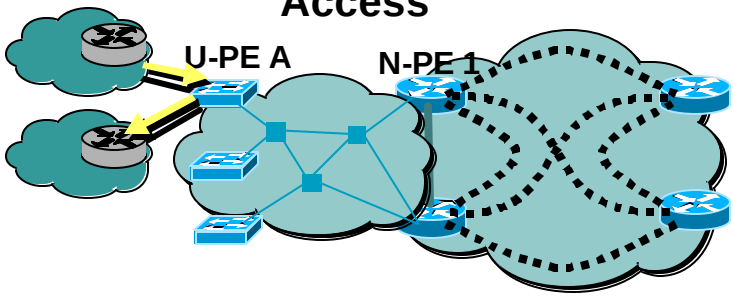
**"H-VPLS"
w/ MPLS
to the Edge**

- **Some Implementations**
  - **Only ONE active link from U-PE to N-PE, other link backup only**
  - **Second N-PE just standby / not used; Non optimal use of resources**

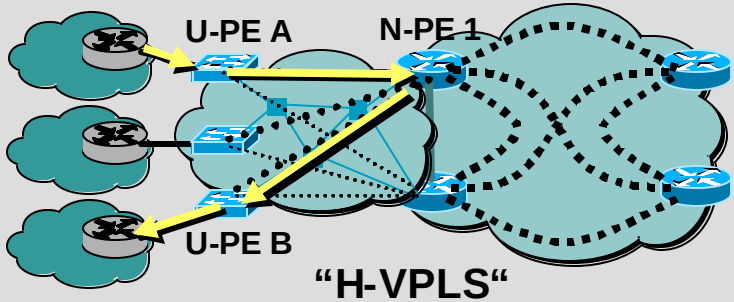
Comparing H-VPLS: Local Switching



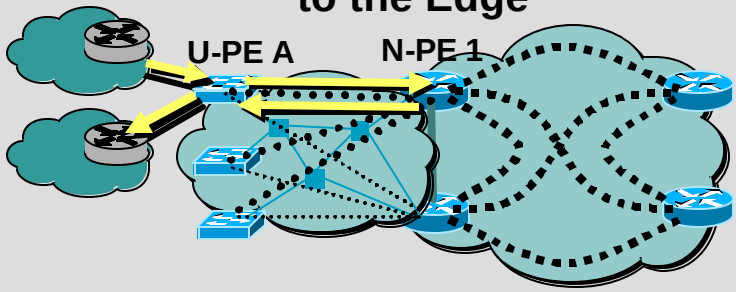
"H-VPLS" w/ Ethernet Access



- Local Switching within the access domain: Optimal traffic flow, PE not involved
- Remember: Metro 80/20 rule: 80% of the traffic stays local…

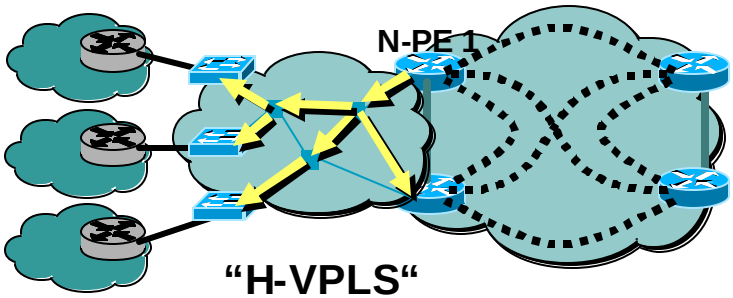


"H-VPLS" w/ MPLS to the Edge



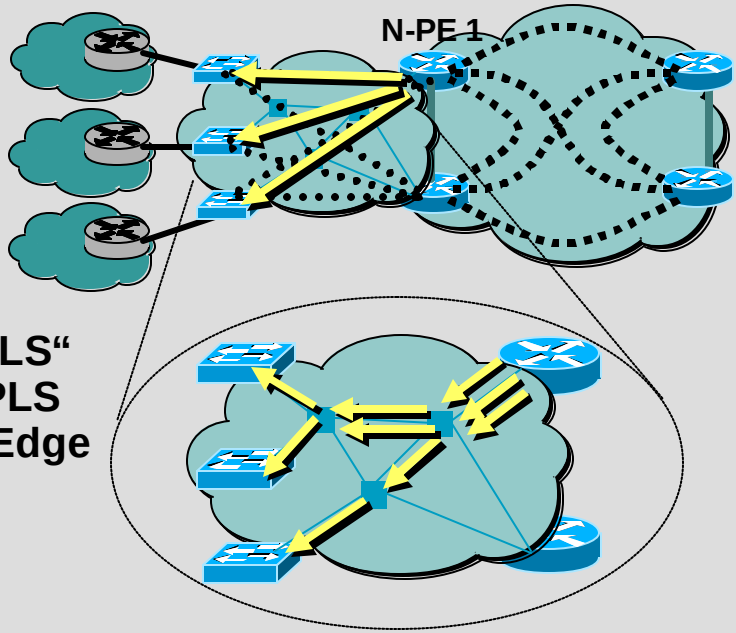
- Traffic always first passed from U-PE to N-PE, even if traffic destined for other U-PE in same access network or even the same U-PE

Comparing H-VPLS: Multicast Distribution



“H-VPLS“ w/ Ethernet Access

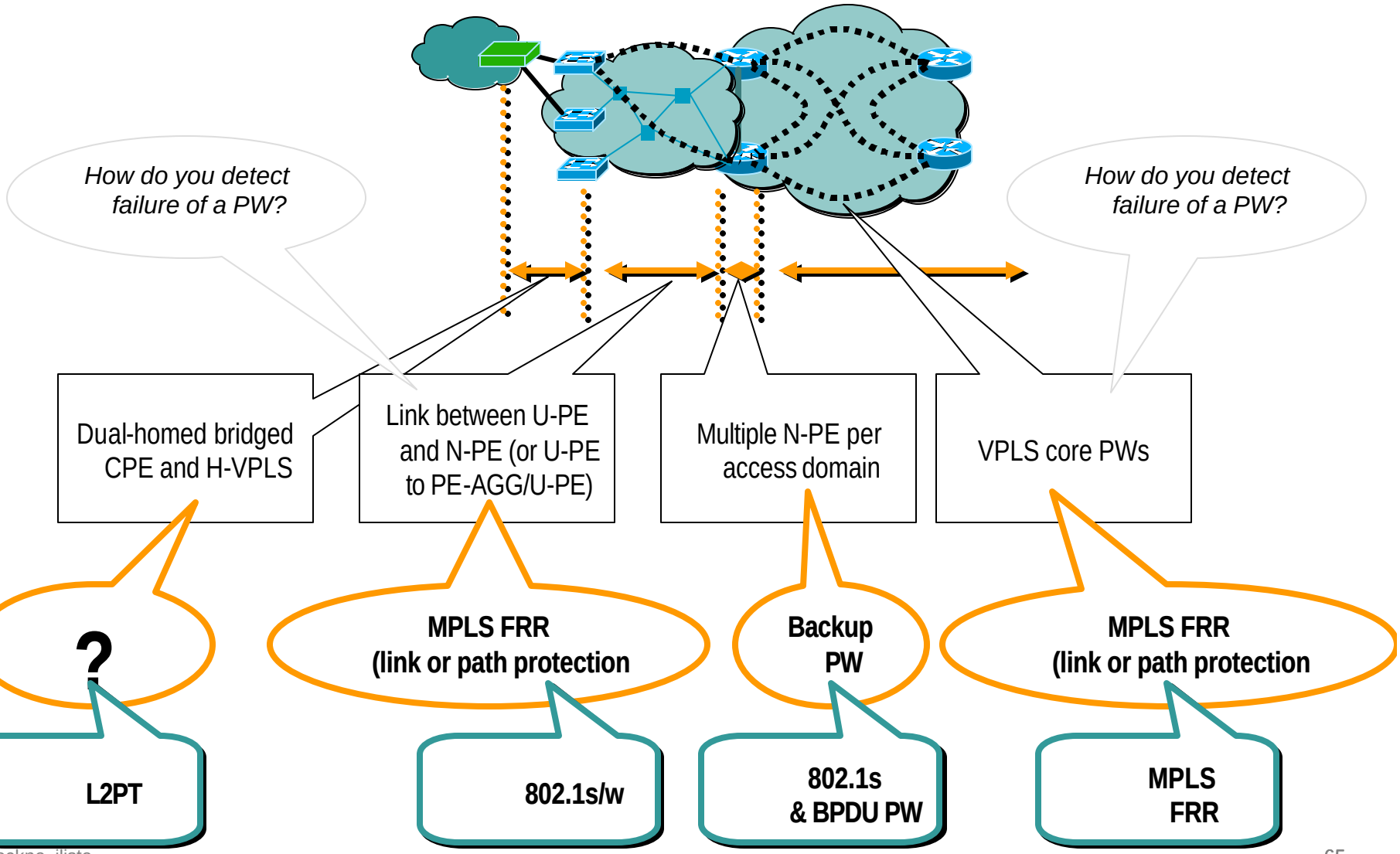
- **Efficient Broadcast/ Multicast distribution—native Ethernet. Distributed replication**



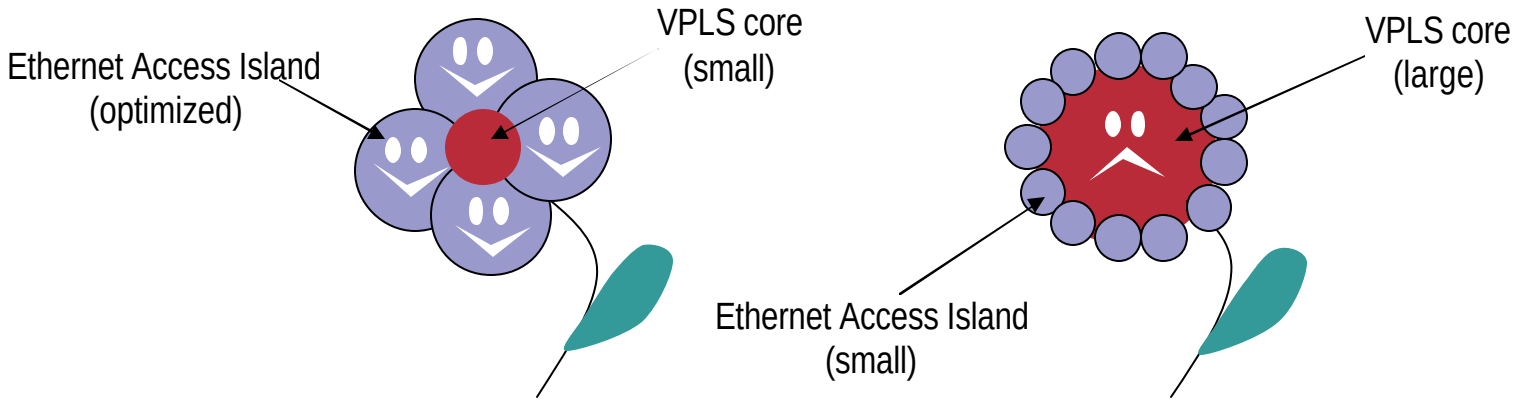
“H-VPLS“ w/ MPLS to the Edge

- **All Multicast/Broadcast traffic replicated only by the N-PE and sent to all attachment PW in the access: Significant load on the N-PE (which also does replication towards the core)**

MPLS Edge versus QinQ-Edge – Protection & Failure domains

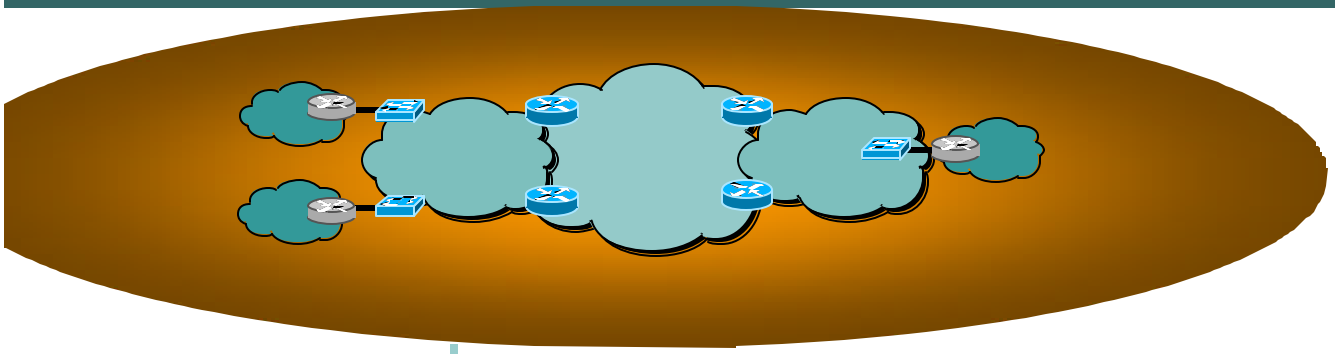


VPLS Best Practice Design Recommendations for Network Architecture



- **Optimize size of Q-in-Q domain instead of VPLS**
- **Optimizes additional Memory & CPU requirements of VPLS**
- **Leverages Ethernet Bridging Beauties (Multicast, Cost, …)**

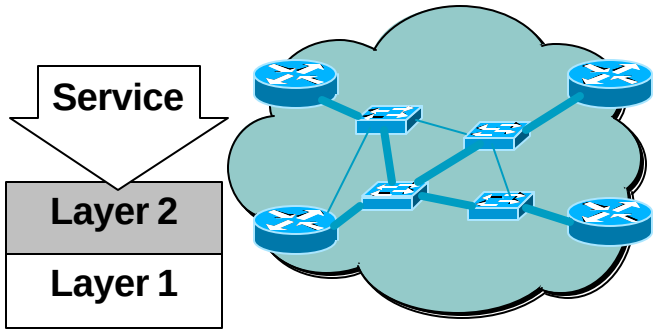
Agenda



- **Introduction to L2VPNs & L2VPN Service Classification**
- **Point-to-Point Technologies**
  - **Any Transport over MPLS (AToM) Overview**
  - **Layer 2 Tunneling Protocol Version 3 (L2TPv3)**
  - **Advanced Concepts**
    - **Layer 2 Interworking, PW Redundancy, PW Switching**
- **Multipoint Technologies**
  - **IEEE Provider Bridges (P 802.1ad)**
  - **Virtual Private LAN Services**
- **Deployment Aspects**
  - **Operational Aspects, OAM**
  - **QoS**
  - **Security**

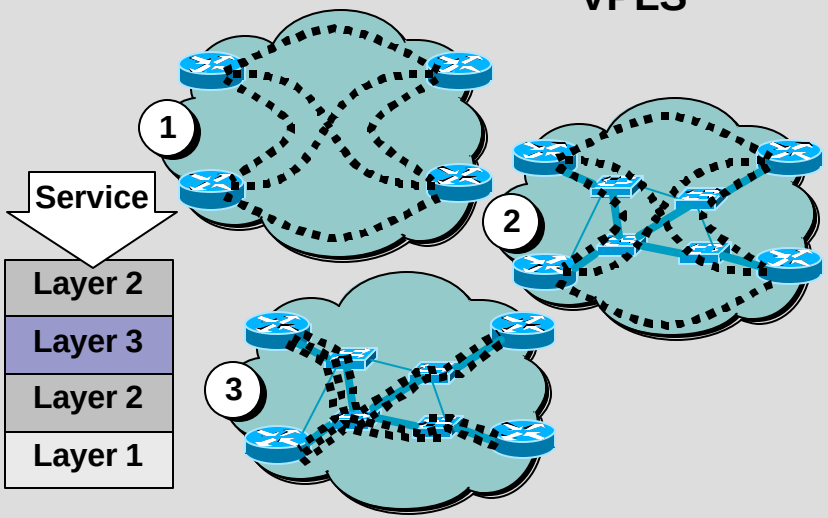
VPLS & Ethernet Bridges
Operational Perspectives

Ethernet Bridges/Provider Bridges



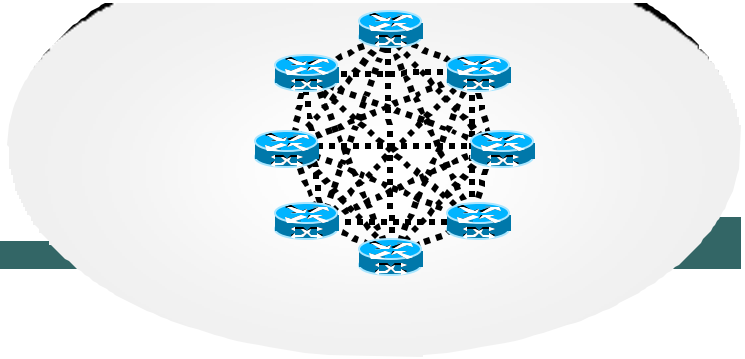
- Native Ethernet in the Access – Layer-1 topology is visible. Fault-detection can leverage L1. No overlay topology.
- Traffic engineering via STP

VPLS

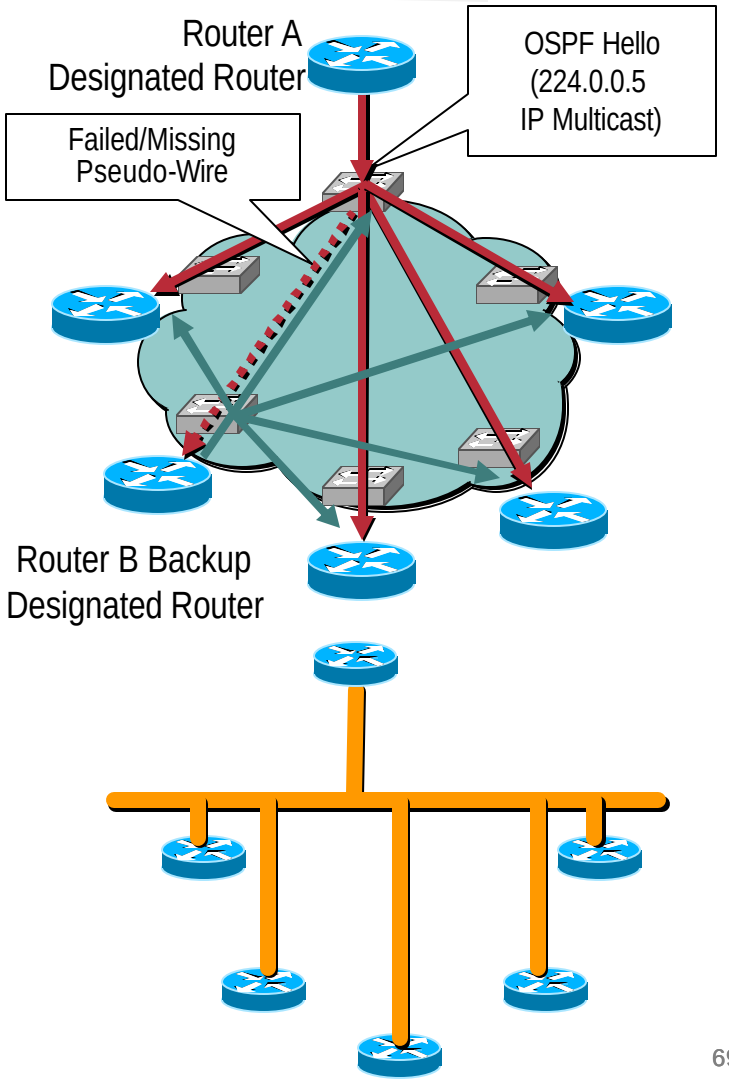


- Virtual Topology – Mapping of PW to physical topology not visible in VPLS
  - Can Traffic-Engineer underlying layers – MPLS, …
- VPLS needs full-mesh monitoring to ensure proper operation!

VPLS:
Partial Mesh Connectivity

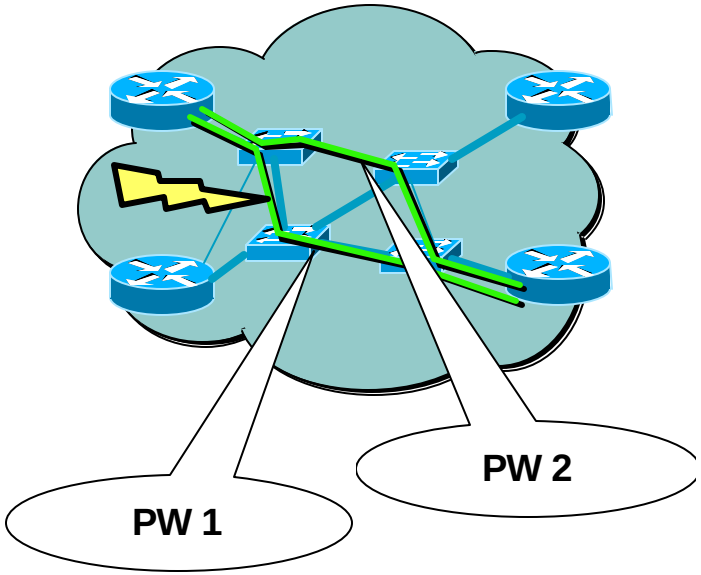


- **Partial Mesh can be caused due to:**
  - **– failure in discovery mechanism**
  - **– PW fails to come up from the start**
  - **– PW failure occurs due to HW or SW failure**
  - **– Node or Link failure along the path (including PEs)**
- **Failure to detect PW failure can result in (see: draft-rosen-l2vpn-mesh-failure)**
  - **– L3 control and routing protocols to misbehave**
  - **– broadcast storm in the customer and provider network**
  - **– multiple copies of a single frame to be received by CE and/or PEs**



VPLS-LDP draft approach to PW Failure detection

- **PW failure detection**
  - **Connection check based**
    - **VPLS-LDP draft advocates LDP-Hellos for this. LDP-Hello might not follow the same path as data-PW**
    - **Per PW monitoring required – e.g. VCCV. Scalability?**
  - **Interface down – Physical failure/LOS**
- **ECMP: Equal Cost Multiple Path in an MPLS/IP network results in load balancing of PWs across different paths**
  (see also draft-swallow-mpls-ecmp-bcp-00.txt)
  - **LDP-Hellos might not be able to detect failure in one of the paths**



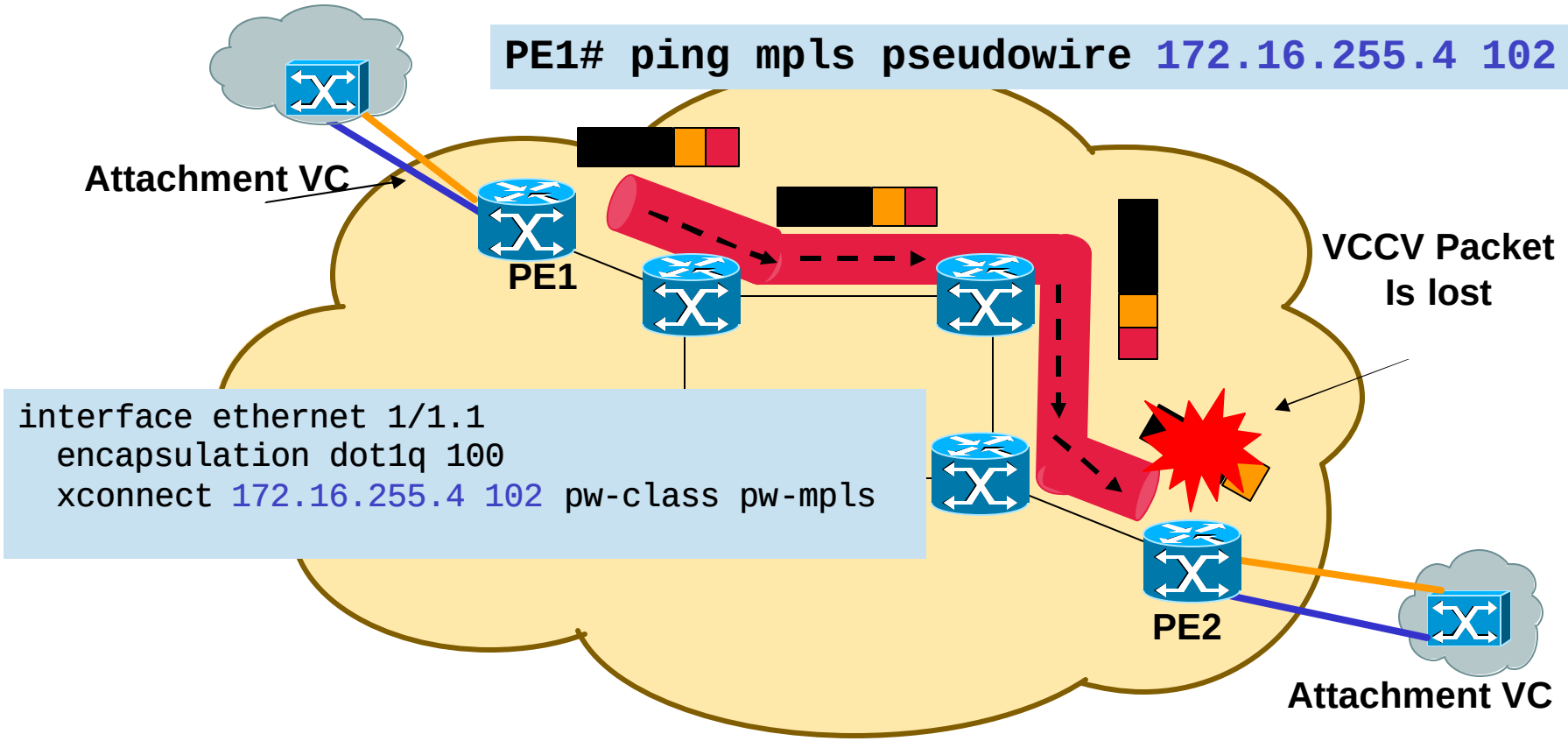
How do you manage the Pseudo-Wire?
VC Connection Verification (VCCV)

- **VCCV goal is to verify aliveness, integrity of defined pseudowire**
- **VCCV capability is negotiated when the AToM tunnel is brought up**
- **A new pseudowire interface parameter is defined**
- **2 data plane methods defined**

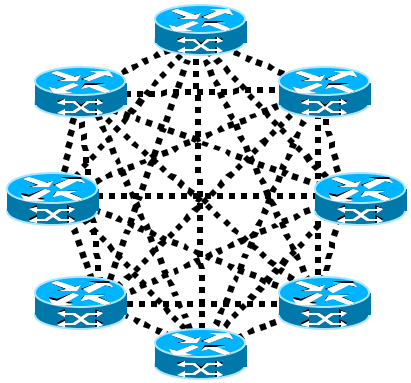
  1.Inband : One bit from pseudowire Control-Word is defined VCCV bit, egress PE are going to intercept all packets with VCCV bit set 1

  2.outband : An additional VCCV label is defined, egress PE are going to intercept all packets with this label.

Connectivity Trace Using VCCV



IEEE 802.1ag Connectivity Fault Management *"Per VLAN OAM"*



- **Networks which leverage VPLS transport require mechanisms like any native Ethernet Transport Network**

  Fault detection, Fault verification, Fault isolation, Fault notification, Fault recovery

- **IEEE 802.1ag addresses this issue comprehensively and introduces the following concepts and mechanisms:**

  Concepts: Domain, Domain Level, Maintenance Entity, Maintenance End Point, Maintenance Intermediate Point

  4 central Tools defined by IEEE P802.1ag:

  (1) L2 Connectivity Check
  (2) L2 Traceroute
  (3) Loopback/L2-Ping
  (4) Alarm Indication Signal (AIS)

- **IETF L2VPN WG to adopt IEEE P802.1ag concepts**

Operational Advantages: References

- **Latest operational features of the Cisco 7600:**
- **Time Domain Reflectometer (TDR) on Copper Ports**

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/intrface.htm#wp1066783

```
R10-7600-1#sh cable-diagnostics tdr interface gig4/37
TDR test last run on: April 15 02:47:34
Interface Speed Pair Cable length        Distance to fault   Channel Pair status
--------- ----- ---- ------------------- ------------------- ------- ---------
Gi4/37    100   1-2  8    +/- 6  m       N/A                 Pair A  Terminated
                3-4  8    +/- 6  m       N/A                 Pair B  Terminated
                5-6  N/A                 9    +/- 6  m       Invalid Short
                7-8  N/A                 8    +/- 6  m       Invalid Short
```

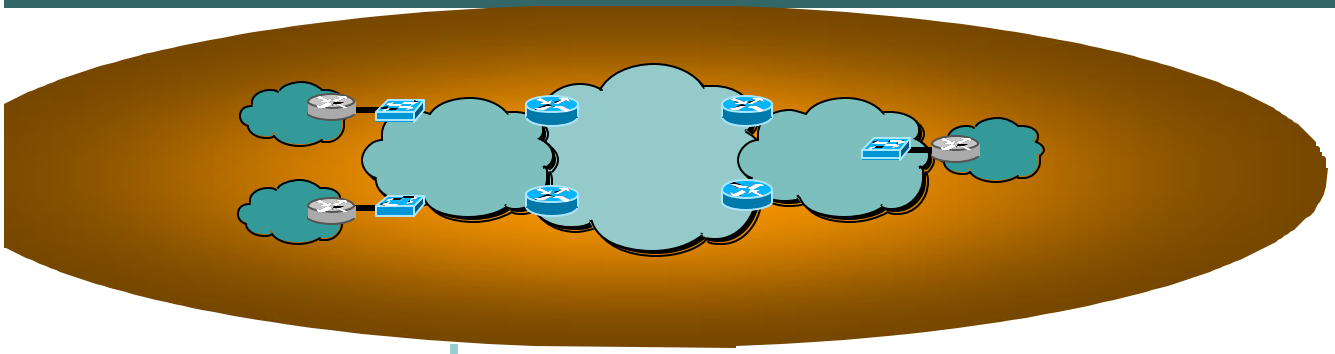
- **L2 Traceroute**

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/l2trace.htm

- **MPLS LSP Ping/Traceroute and AToM VCCV**

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/sx_lsppt.htm

Agenda

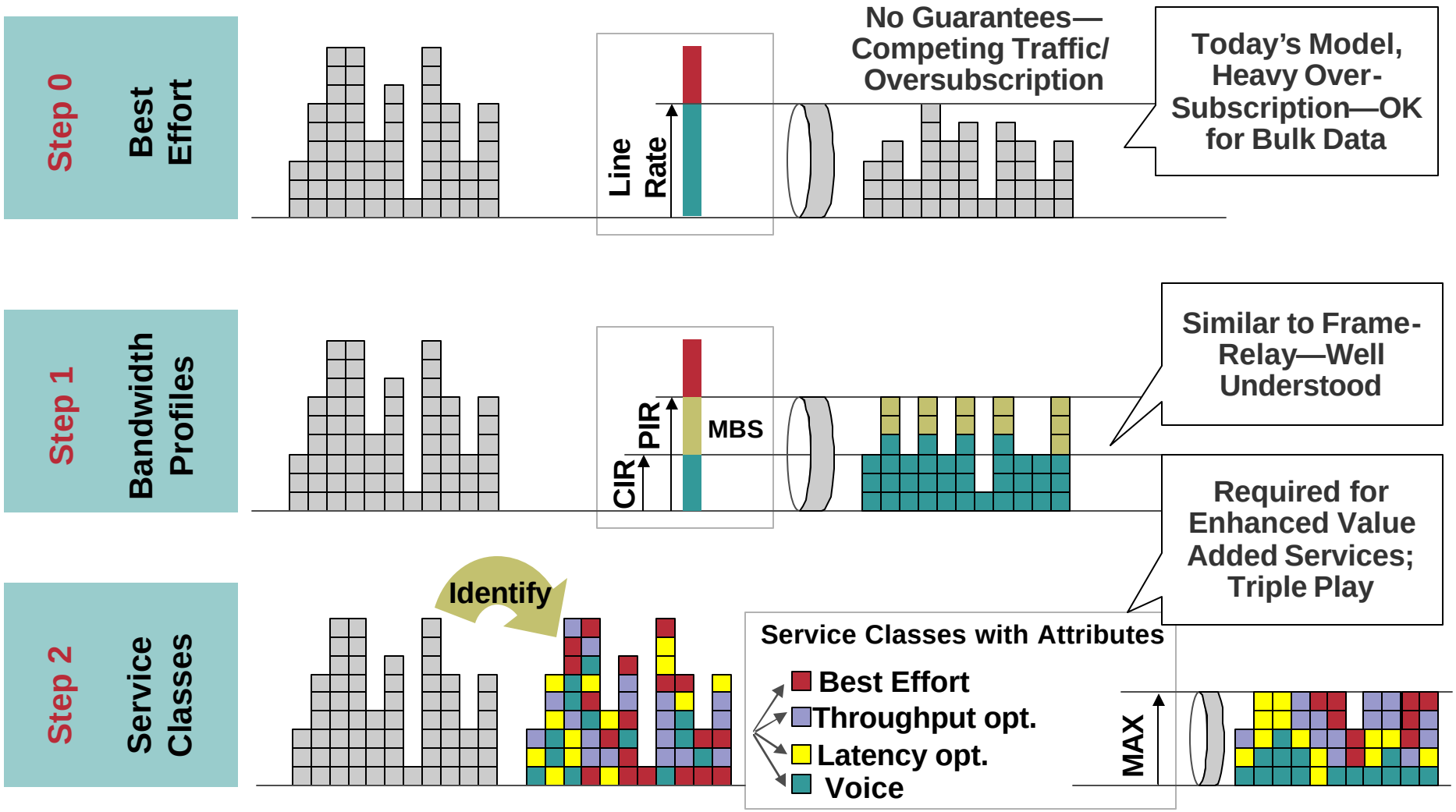


- **Introduction to L2VPNs & L2VPN Service Classification**
- **Point-to-Point Technologies**
  - **Any Transport over MPLS (AToM) Overview**
  - **Layer 2 Tunneling Protocol Version 3 (L2TPv3)**
  - **Advanced Concepts**
    - **Layer 2 Interworking, PW Redundancy, PW Switching**
- **Multipoint Technologies**
  - **IEEE Provider Bridges (P 802.1ad)**
  - **Virtual Private LAN Services**
- **Deployment Aspects**
  - **Operational Aspects, OAM**
  - **QoS**
  - **Security**

Metro Ethernet End-to-End QoS

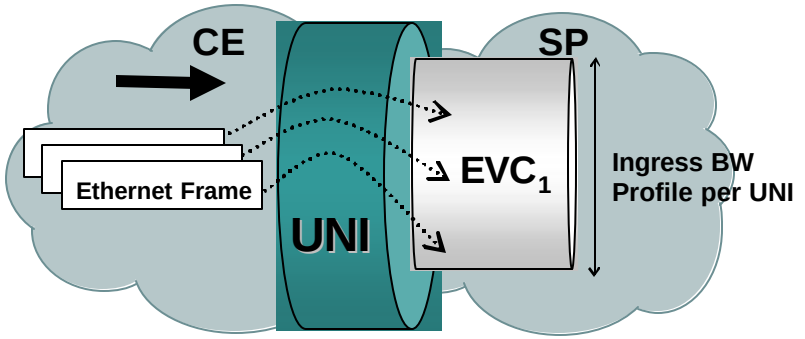
- Allows efficient utilization of links that carry voice, video and data
- SP differentiator between service offerings with SLAs
- Customer contracts to an aggregate that contains specific traffic classes with drop, delay and jitter attributes
- Sample QoS classes—Real Time (voice/interactive video), Business and Best effort
- Customer pays for traffic engineered bandwidth not just the access pipe

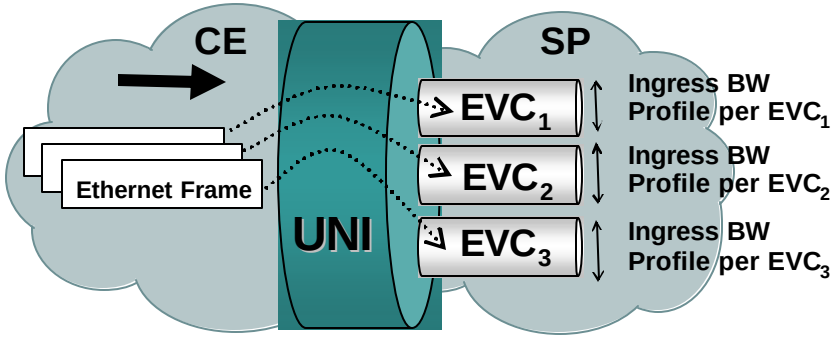
Ethernet SLA Approaches

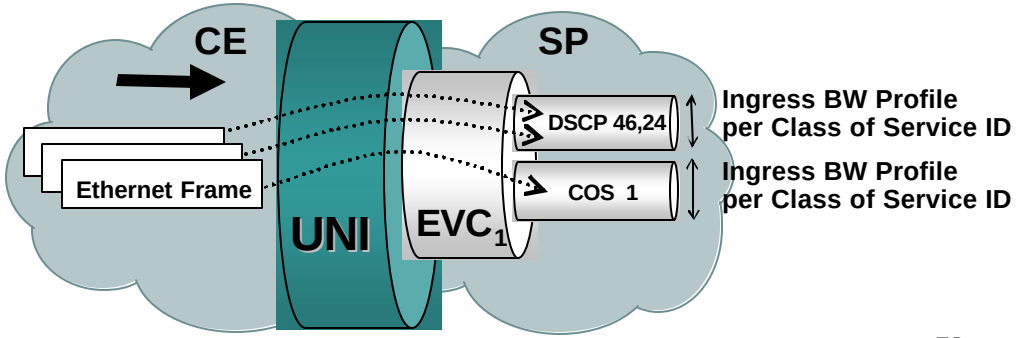


Classes of Service - Implementation

- **Class of Service Instance identified by:**
  - **UNI**
  - **Ethernet Virtual Circuit (EVC)**
  - **or**
  - **EVC and "User Priority" (L2 CoS/L3 DSCP)**
- **A Class of Service is defined by Performance Objectives**
  - **Frame Delay**
  - **Frame Delay Variation**
  - **Frame Loss Ratio**

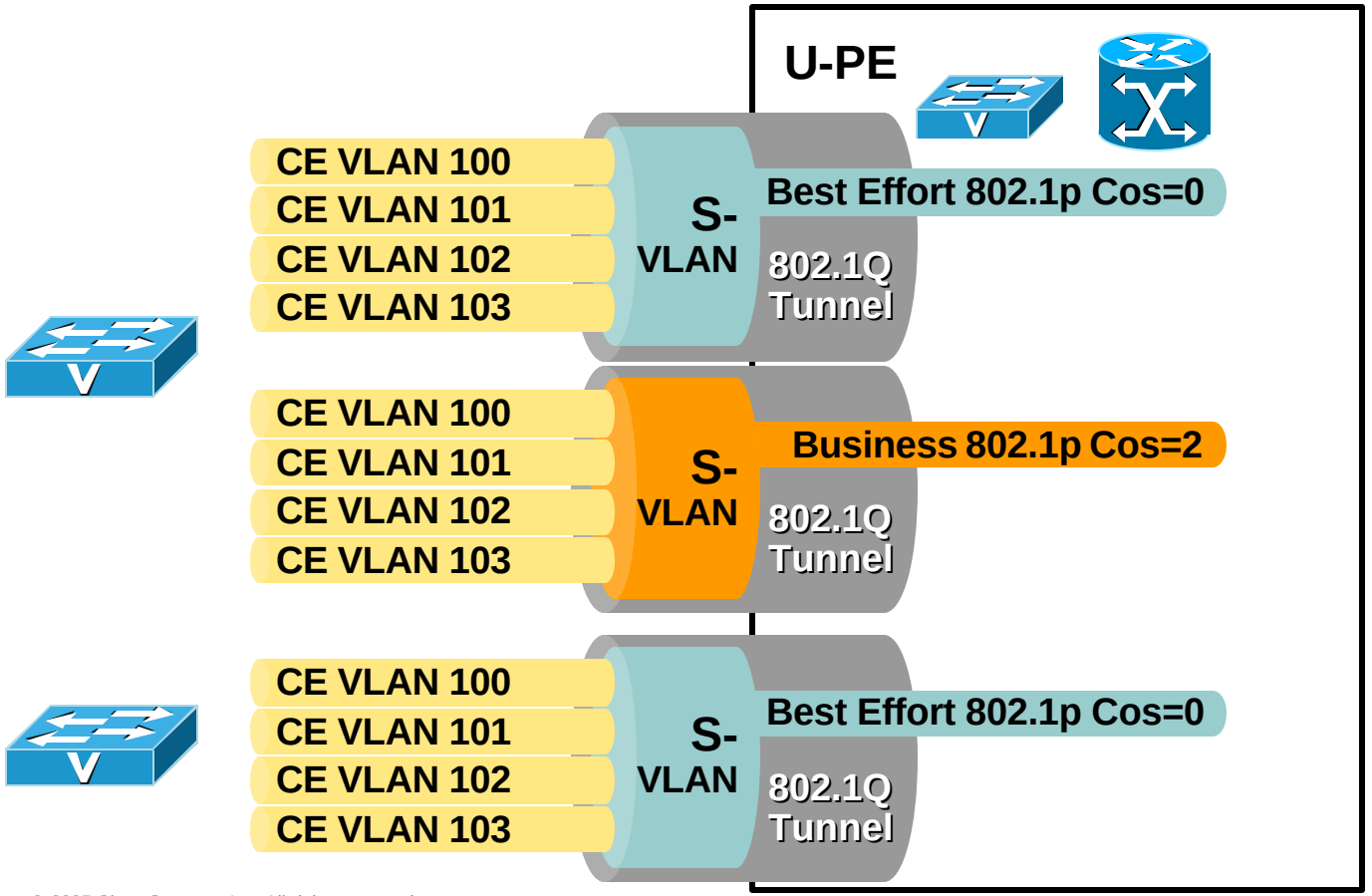






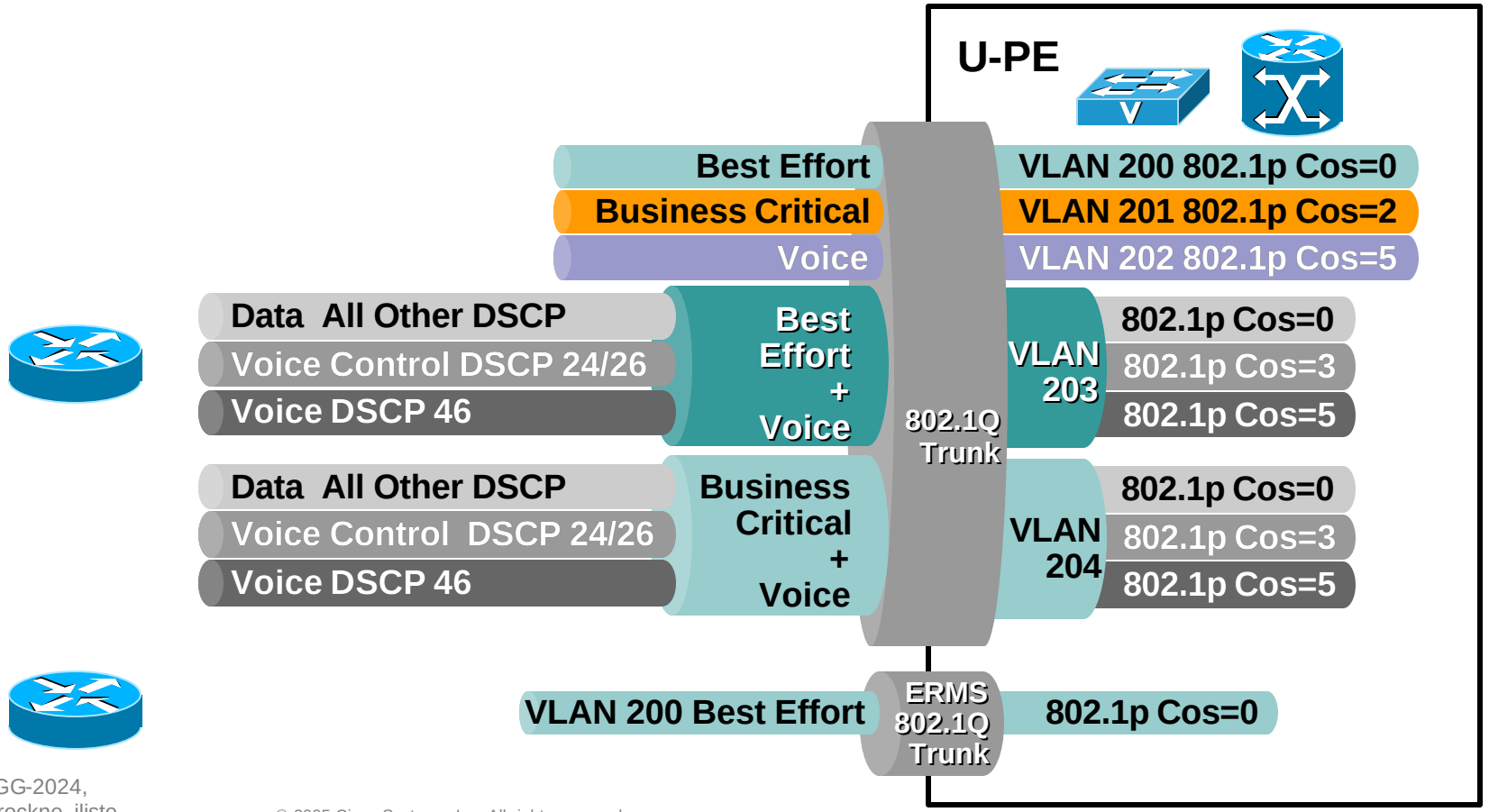
Classes of Service - Implementation

- **Ingress BW profile per UNI:**
  Best effort, Business, or Real-Time on a per-port basis



Classes of Service - Implementation

- **Ingress BW profile per EVC: Best effort, Business or Real-Time on a VLAN basis**
- **Ingress BW profile per Class of Service ID: Best effort, Business or Real-Time on a class basis (e.g. based on CE-VLAN CoS, IP ToS/DSCP)**



Metro Ethernet End-to-End QoS

- **Ethernet QoS similar to ATM/FR model**

  CIR/PIR is well accepted today

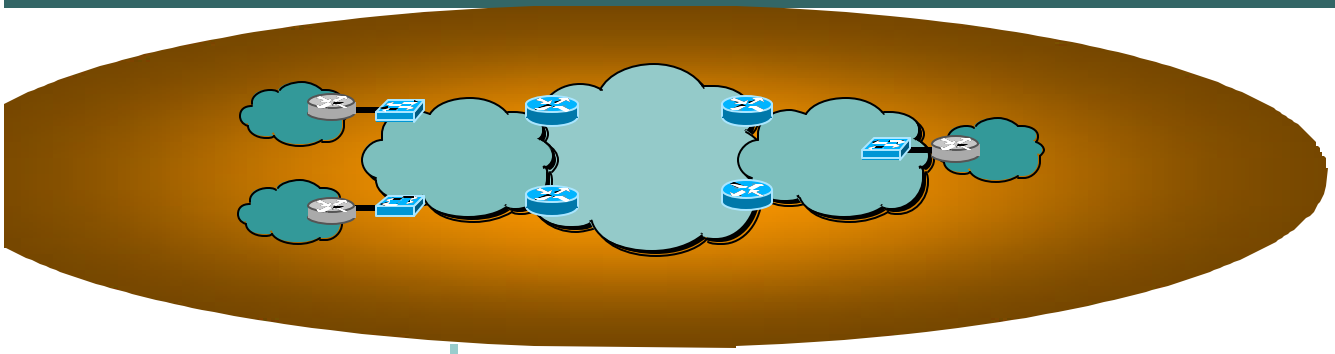
- **Migration to DSCP-like model that can be applied to Layer 2 and Layer 3 services**

  CIR/PIR can be extended to other QoS models allowing for tiered bandwidth rates, i.e. Voice, Business and Best Effort traffic classes

- **Consistent QoS model for L2 and L3 VPNs**
- **Support for mapping of customer's dot1p to SP dot1p (QinQ based services).**

For More Information on End-to-End QoS, Please refer to Cisco Quality of Service Overview at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/qcfintro.pdf

Agenda

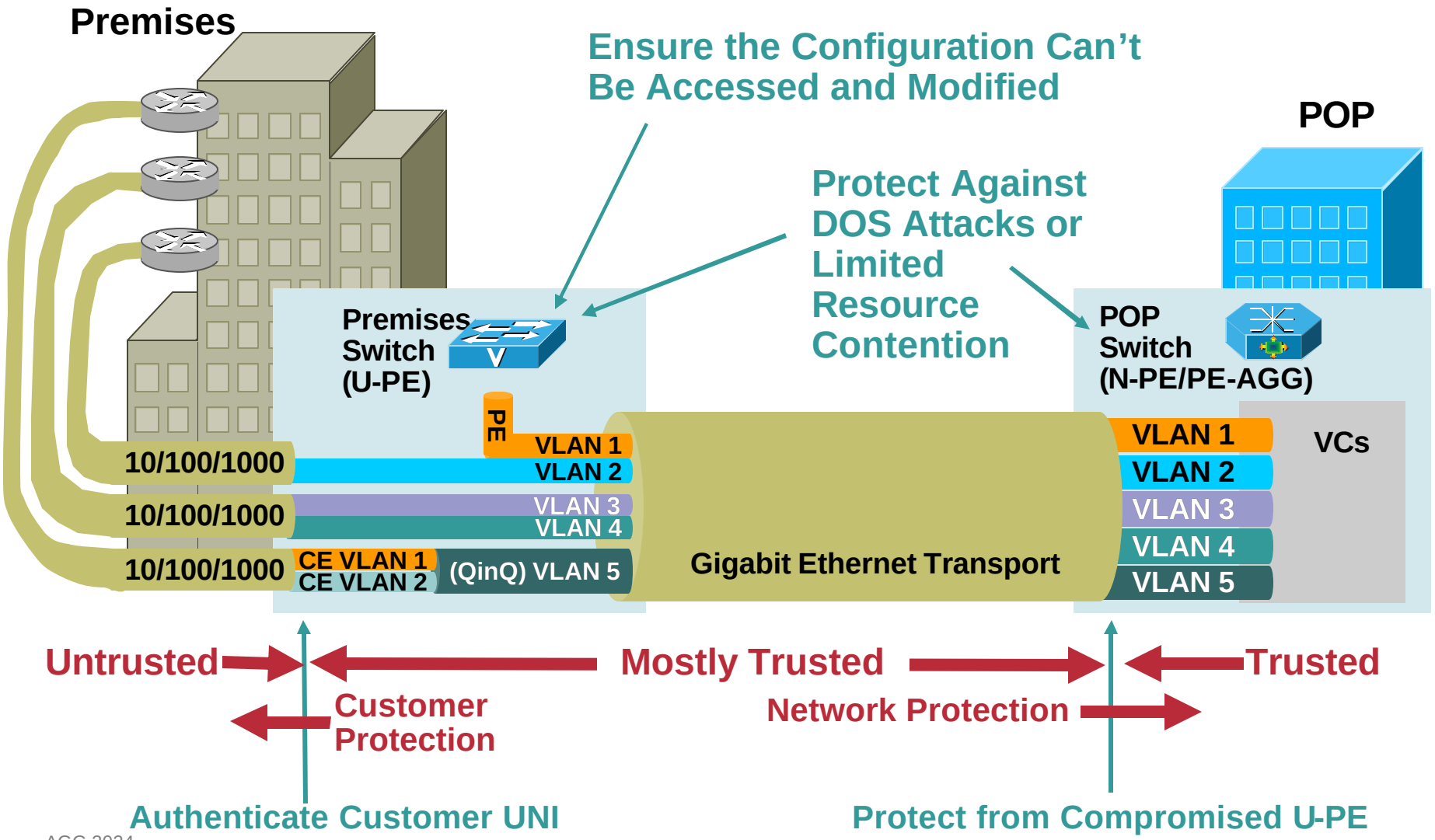


- **Introduction to L2VPNs & L2VPN Service Classification**
- **Point-to-Point Technologies**
  - **Any Transport over MPLS (AToM) Overview**
  - **Layer 2 Tunneling Protocol Version 3 (L2TPv3)**
  - **Advanced Concepts**
    - **Layer 2 Interworking, PW Redundancy, PW Switching**
- **Multipoint Technologies**
  - **IEEE Provider Bridges (P 802.1ad)**
  - **Virtual Private LAN Services**
- **Deployment Aspects**
  - **Operational Aspects, OAM**
  - **QoS**
  - **Security**

Metro Ethernet Security

- **Security is a prime consideration within any public switched network**
  - **One user should not affect any other user**
- **Due to the "Plug and Play" nature of Ethernet, networks have to be designed with caution to provide the necessary degree of security**
- **Precautions need to made to secure the network against Denial of Service (DoS) attacks, as well as, unintentional misconfigurations**

Metro Ethernet Trust Model



Attacks and Defensive Features/Actions

Cisco.com

Attack	Defensive Features/Actions
MAC Attacks (CAM Table Overflow)	Port Security, Per VLAN MAC Limiting
Broadcast/Multicast Storm Attacks	Storm Control
VLAN Hopping, DTP Attacks	Careful Configuration (Disable Auto-trunking, Used Dedicated VLAN-ID for Trunk Ports, Set User Ports to Non-trunking, VLAN 1 Minimization, Disable Unused Ports,…)
Spanning Tree Attacks	BPDU Guard, Root Guard, MD5 VTP Authentication
DHCP Rogue Server Attack	DHCP Snooping (Differentiate Trusted and Untrusted Ports)
Hijack Management Access	Secure Variants of Management Access Protocols (Not Telnet etc., but SSH,… and out of Band Management), Disable Password Recovery, Encrypted Passwords
Pro-Active Defence	Deploy MAC Level Port Security, Wire-Speed ACLs, 802.1x

Security Features and Roles Mapping

Customer Premise CPE	Provider Access U-PE	Provider Aggregation PE-AGG	Provider Edge N-PE	Provider Core P

Roles	Generic	Metro Ethernet Services	
		EVPL/EVPLan	EPL/EPLan
U-PE	Disable Password Recovery Encrypted Password Secure Access Protocol (SSH, ..) SNMPv2 with MD5 encryption VTP Mode Transparent	VLAN 1 Minimization L2 PDUs and Potential DOS Attacks Filters BPDU Filter Disable CDP on the UNI Port Security / Per VLAN MAC Limiting Broadcast Storm Control	L2PT Thresholds Potential DOS Attacks Filters BPDU Filter Disable CDP on the UNI Port Security / Per VLAN MAC Limiting Broadcast Storm Control
PE-AGG	Encrypted Password Secure Access Protocol (SSH, ..) SNMPv2 with MD5 encryption VTP Mode Transparent STP Root Guard	Per VLAN MAC Limiting	Per VLAN MAC Limiting

Security Features and Roles Mapping (cont.)

Cisco.com

Customer Premise CPE	Provider Access U-PE	Provider Aggregation PE-AGG	Provider Edge N-PE	Provider Core P

Roles	Generic	Metro Ethernet Services	
		EVPL/EVPLan	EPL/EPLan
Network-Facing Provider Edge	Encrypted Password Secure Access Protocol (SSH, ..) SNMPv2 with MD5 encryption VTP Mode Transparent STP Root Guard	Per VLAN MAC Limiting	Per VLAN MAC Limiting

Summary

- **L2 VPN services are complementary to L3 VPN services**

  New Packet Transport-Service Opportunities, complementing L3VPN transport Services and L3+ Value-Added Services

  Ethernet is the next natural evolution of customer UNI connection for both L2VPN or L3VPN

  Point-to-Point L2VPN allow for Core-Consolidation, Service-Transport Simplification while ensuring investment protection

- **Ethernet is getting ready to become a core technology**

  Emerging standards on IEEE provider bridges (802.1ad), Connectivity Management (802.1ag), IETF VPWS and VPLS (PWE3, L2VPN WG) and ITU SG 13, 15

Please Complete Your Session Evaluation Form

Cisco.com

Muchas Gracias por asistir a esta sesión.

Por favor, complete y entregue a la salida la evaluación suministrada.

¡Gracias!

Complete Your Online Session Evaluation!

Muchas Gracias por asistir a esta sesión.

Por favor, complete el formulario de evaluación.

¡Muchas gracias!

Session ID: AGG-2024

“Layer-2 Business VPN Services: Technologies, Architectures and Deployment”