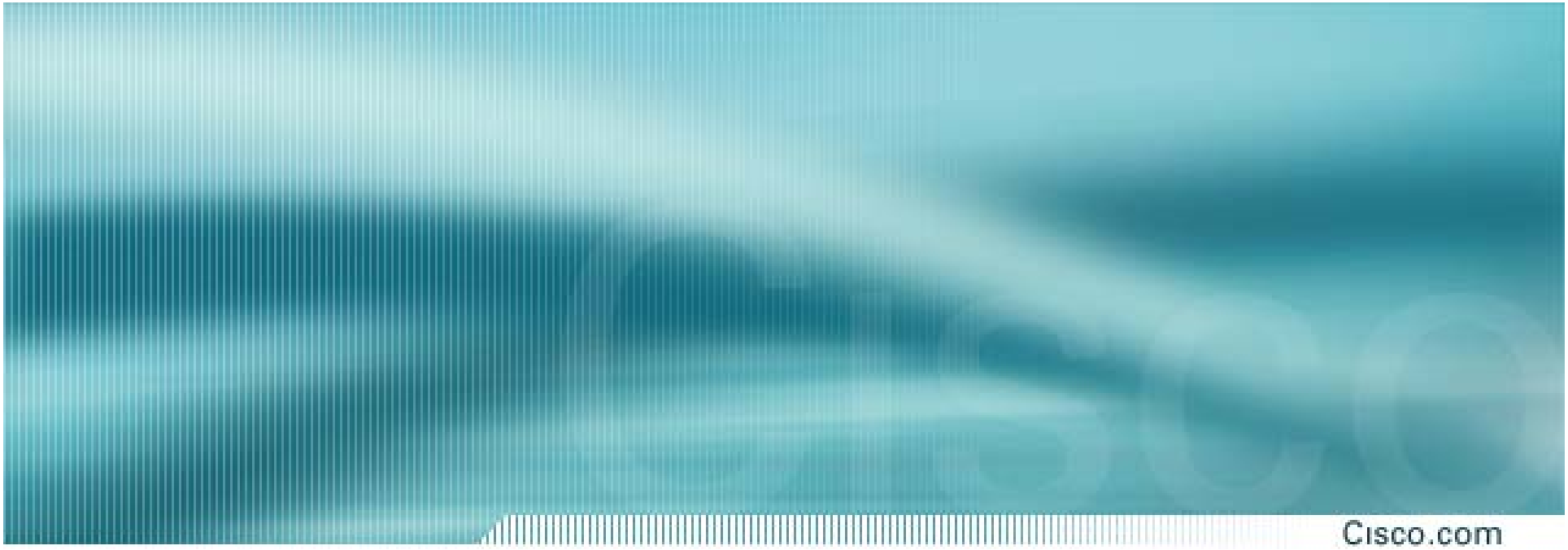


CE Bridge Interoperability

(draft-sajassi-l2vpn-vpls-bridge-interop-00.txt)

Ali Sajassi

L2VPN WG

November 2004

Cisco Systems

Agenda

- **Motivation Behind VPLS**
- **L2VPN Framework Model for VPLS PE**
- **Discussion of Issues**
- **Next Steps**

Motivations Behind VPLS

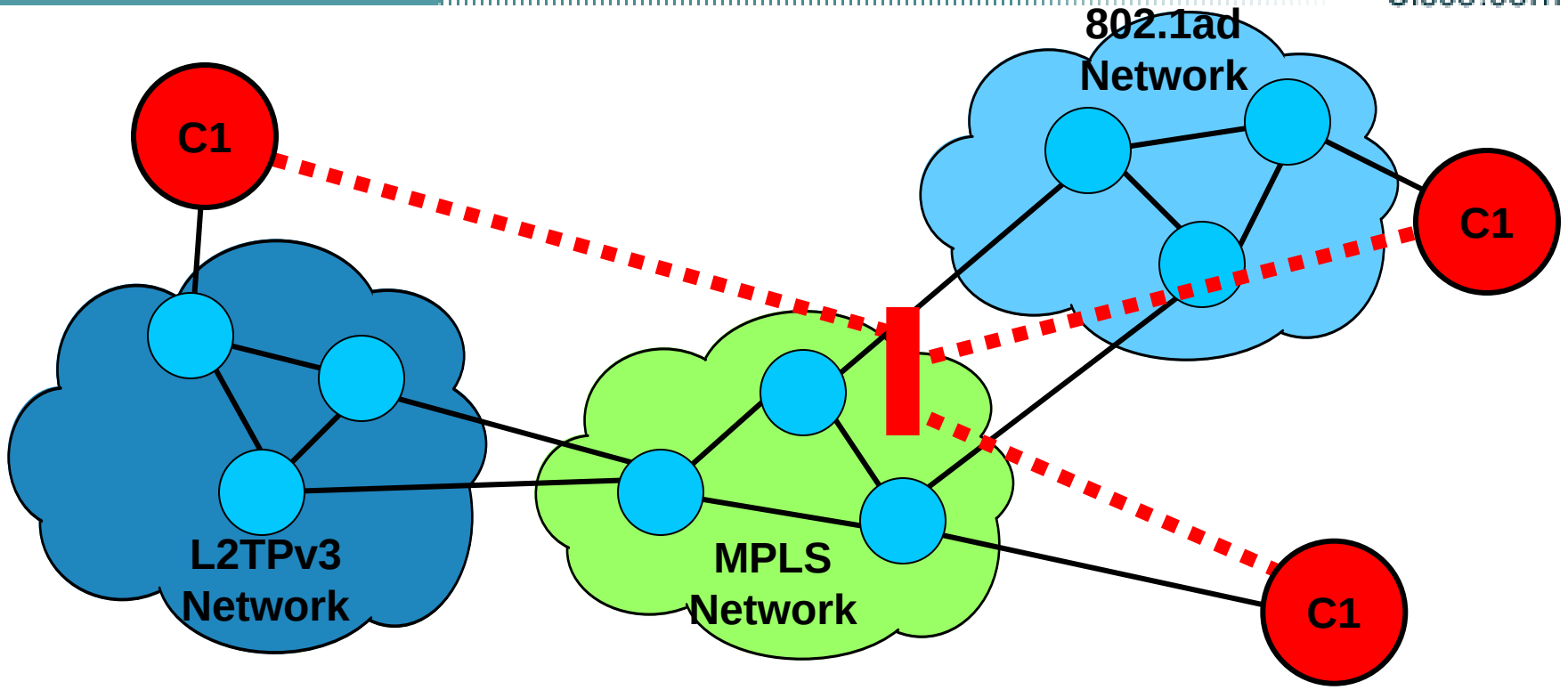
- **It can support CE bridges as well as**
- **It can support CE non-Bridges (e.g., routers/hosts)**
- **If CE devices were only limited to IP routers/hosts, then IPLS could be used**

- **=> So if one of the fundamental premise behind VPLS is the support of CE bridges, then we'd better make sure it can do it right !!**

Motivations Behind VPLS - Continue

- VPLS (as service) is a bridged LAN service
- There are a number of bridging issues that need to be discussed and addressed
- Many of previous discussions have been centered around signaling & auto-discovery
- We need to pay attention to bridging issues if we want to offer proper multipoint Ethernet service

ESI v.s. VPLS Instance

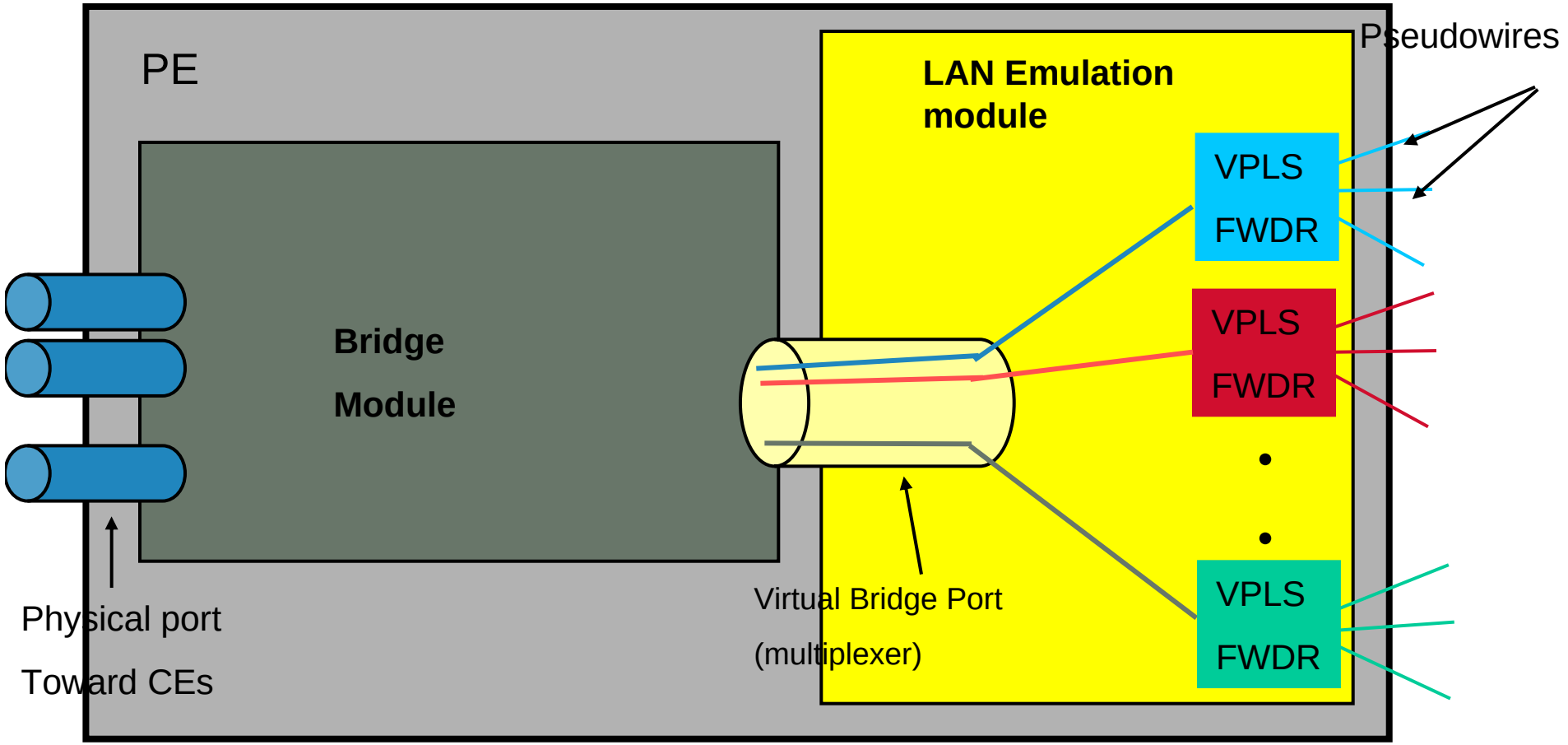


- **ESI – end-to-end service provided to C1**
- **VPLS Instance: LAN Emulation portion of ESI (as defined in L2VPN FRWK)**

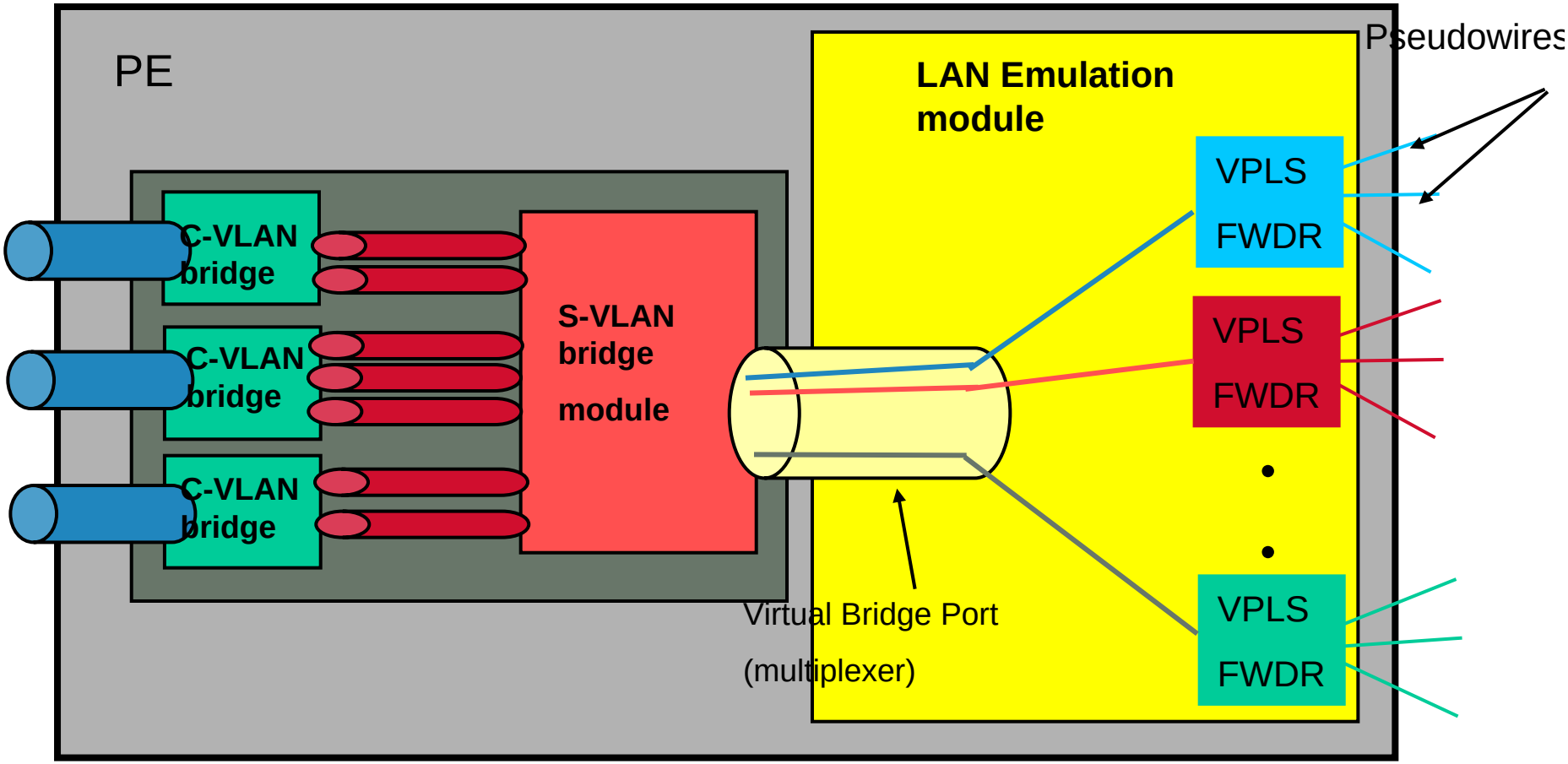
Ethernet Service Types

		Ethernet ACs & Service Mapping			
		Port-based w/ untagged	***Port-based w/ tagged & untagged***	***VLAN mapping***	***VLAN bundling***
Eth ACs & Srv Map	***Port-based w/ untagged traffic***	VPLS Unqualified Learning	N/A	?	N/A
	Port-based w/ tagged & untagged	N/A	VPLS Unqualified Learning	?	?
	VLAN mapping	?	?	VPLS Qualified Learning **!!!**	?
	VLAN bundling	N/A	?	?	?

VPLS PE Model as Defined in L2VPN Framework

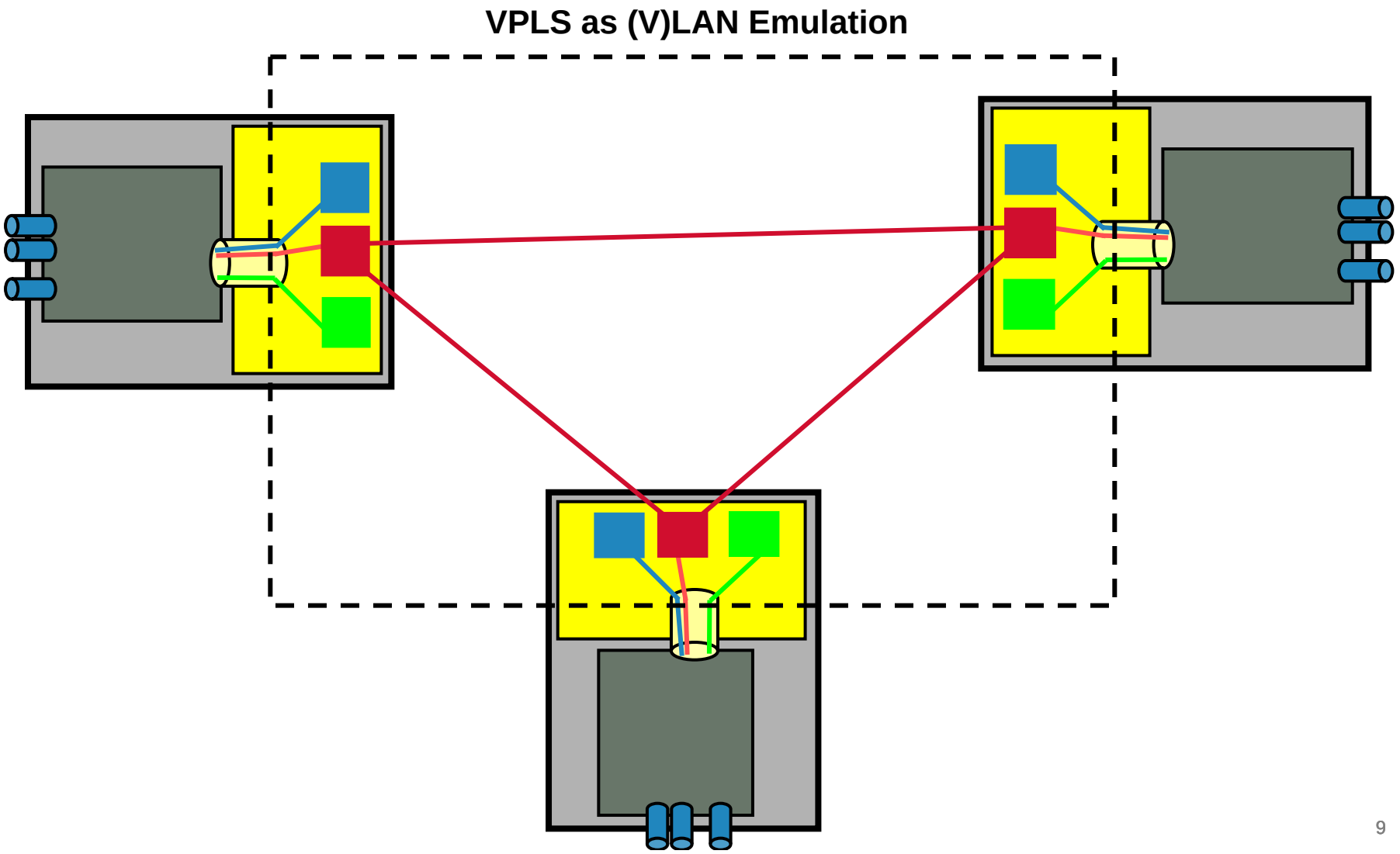


VPLS PE Model as Defined in L2VPN Framework – Continue

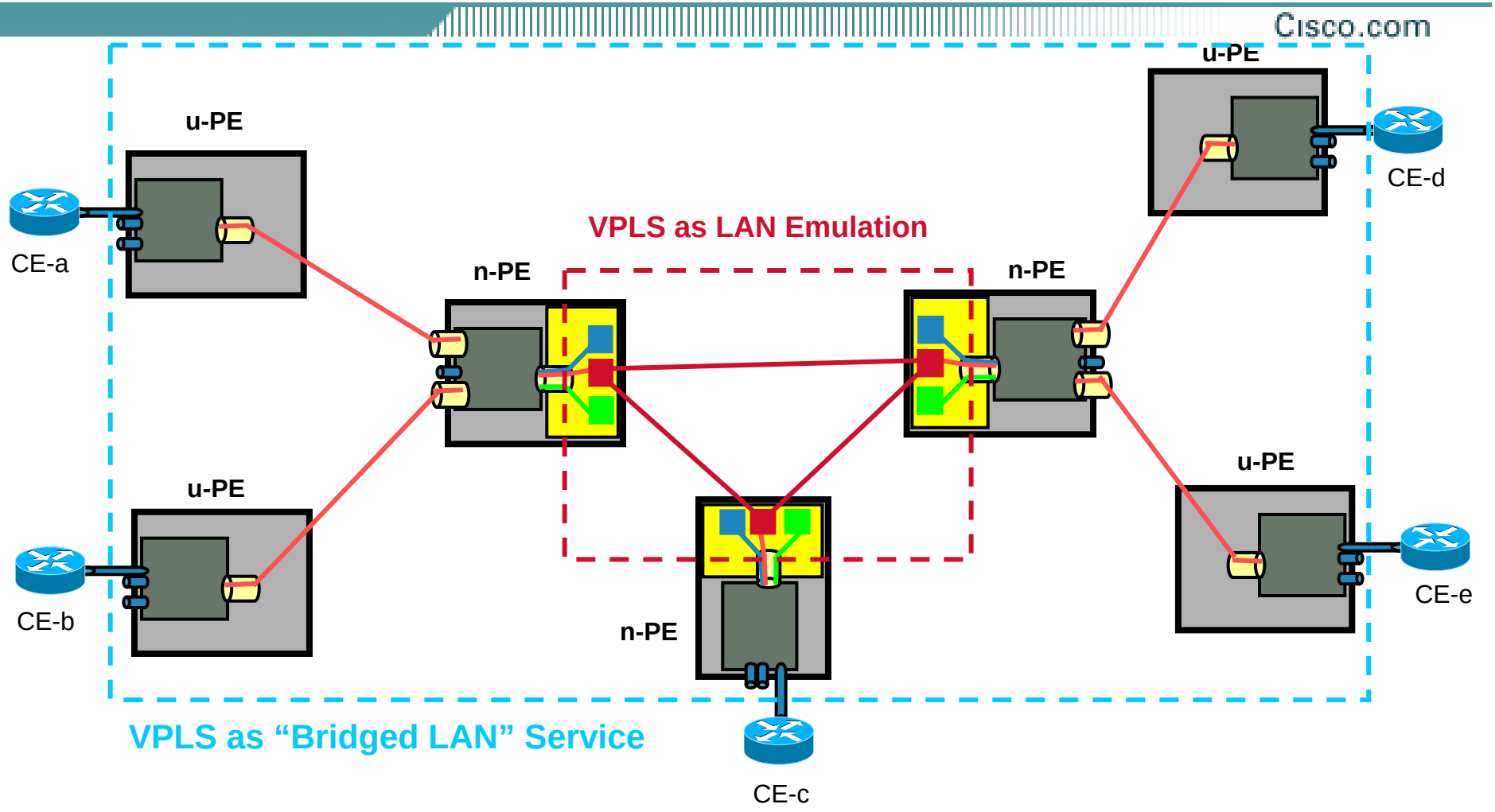


If a PE is modeled as such, then it can handled all of the previously mentioned services

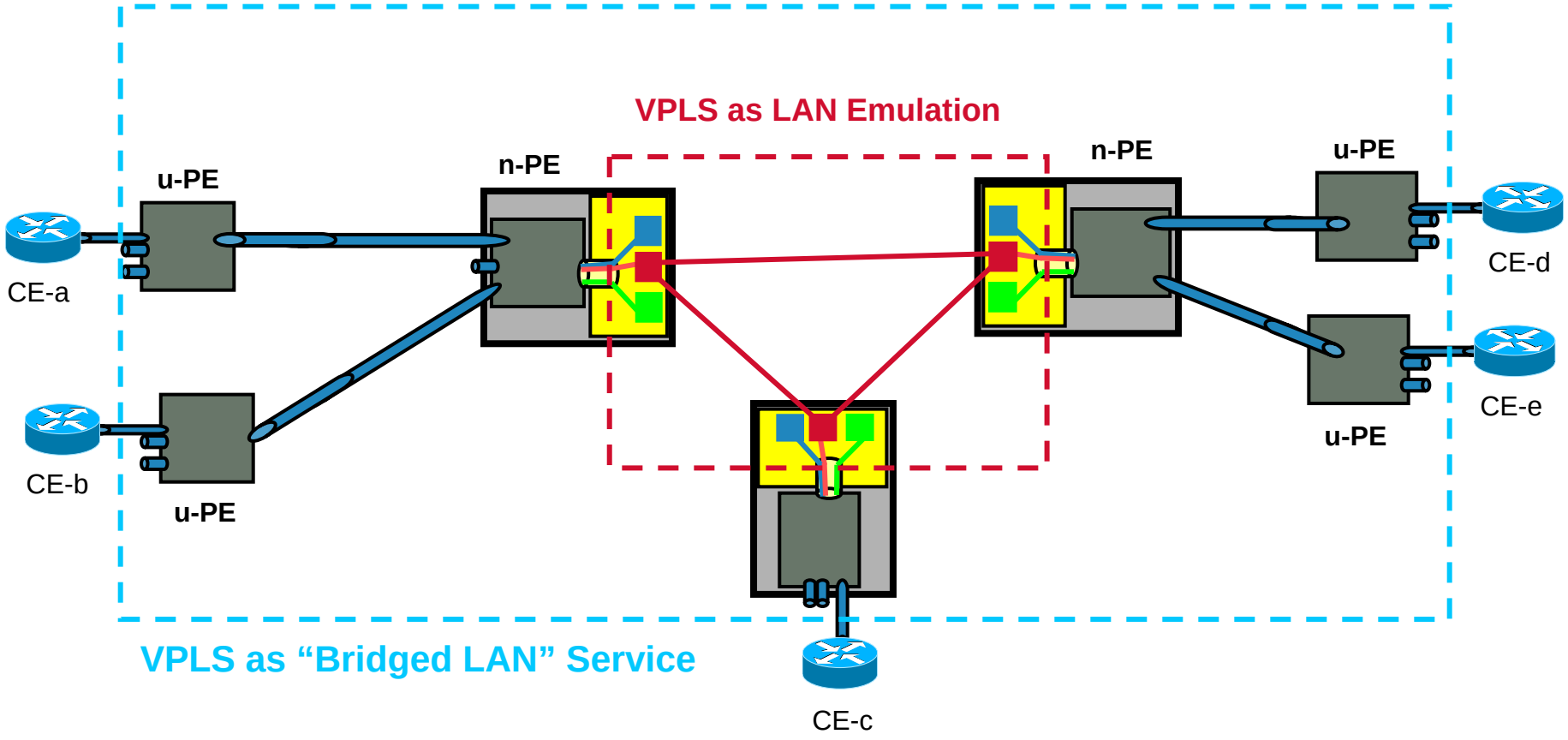
VPLS as LAN (VLAN) Emulation



H-VPLS with MPLS Access



H-VPLS with QinQ Access



Bridge Interoperability Issues

1. CE Bridge Protocol Handling
2. Customer Network Topology Changes
3. Redundancy
4. MAC Address Scalability
5. Partial-mesh PWs
6. Multicast Traffic
7. Inter-operability with 802.1ad Provider Bridges

1) Protocol Handling of CE Bridge

- **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)**

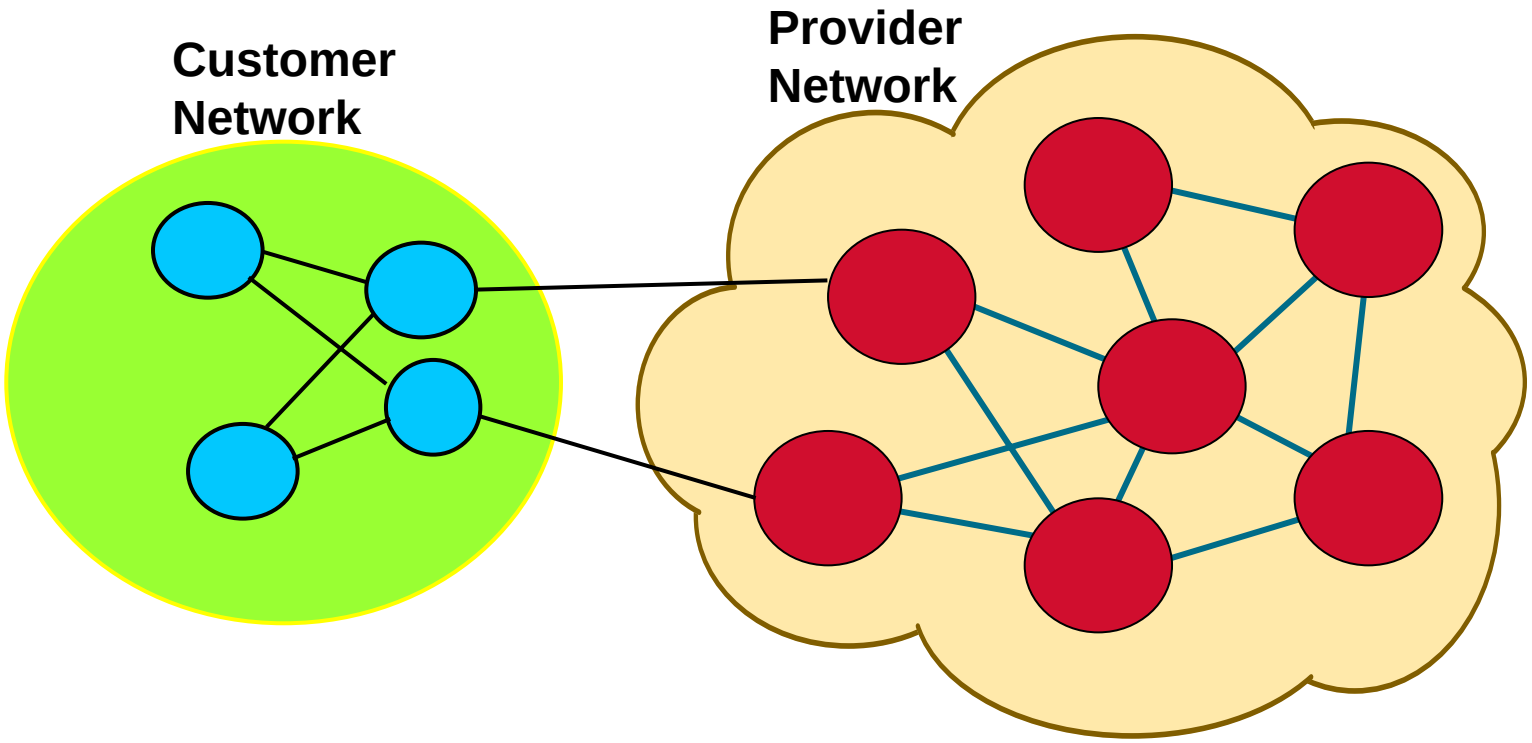
1) Protocol Handling of CE Bridge – cont.

- **Depending on the type of AC, the PE needs to do one of the following with respect to each customer protocol:**
  - **Operate transparently**
  - **Discard them**
  - **Peer with them**
  - **Snoop them**

1) Protocol Handling of CE Bridge – cont.

- **IEEE 802.1ad**
  - **reserves a block of 16 MAC addresses 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**
- **IEEE 802.1ad bridge model facilitates all these operation**

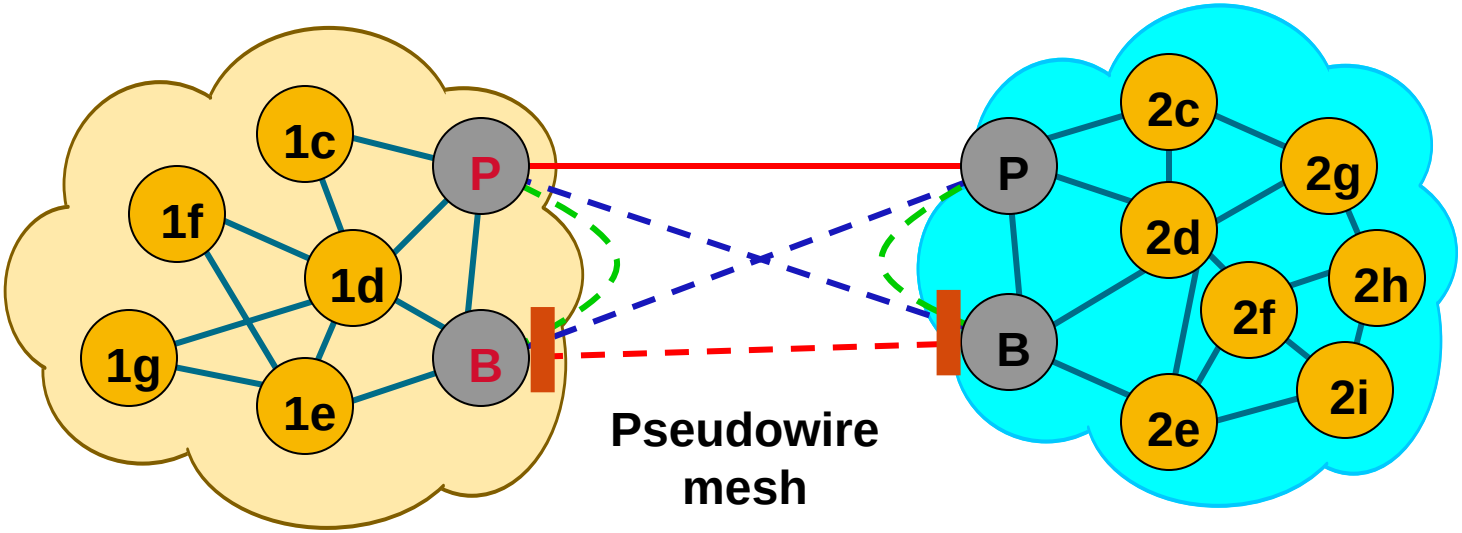
2) Customer Topology Change



2) Customer Topology Change – Cont.

- If There is a Customer Topology Change, then
  - Customer activates its backup link for a subset of its VLANs (e.g., each link can be used for a subset of VLANs for load sharing)
  - Customer sends a Topology Change Notification (TCN) over this newly activated link
  - PE needs to understand and flush its MAC addresses
  - Receiving PE needs to propagate it to all other PEs
  - If any PE along the path doesn't take any action, then customer frames will be black holed
- IEEE 802.1ad snoops the customer TCN and generates Customer Change Notification (CCN) message
- CCN message must be per Provider VLAN (S-VLAN) – e.g., it must be per VPLS instance such that only MAC addresses associated with that VPLS instance is flushed
- IEEE 802.1ai is planned to be used for aggregating all TCN messages from different customers
- It is easier to directly process these in-band CCN than converting them into out-of-band messages (LDP MAC address withdrawal)

3) Redundancy & Inefficient Replication



- There is a full-mesh of PWs (for a given service instance) among the four PEs of the two island
- Even though there are 6 PWs, only a single one (shown in solid line) is needed for that service instance but instead 3 PWs are used
- Because when a Primary PE is selected, then all its PWs are selected

4) MAC Address Learning

- **If customer use bridges instead of routers, then service providers can expect large number of customer MAC addresses**
- **If each customer uses 1000 MAC addresses, then for a 1000 such customers, there will be 1M MAC addresses in the provider network (or even a PE)**

4) MAC Address Learning – Cont.

- **IEEE 802.1 suggests two mechanism to deal with this issue:**
  - **Don’t learn MAC addresses unless you have to (as described in 802.1ad)**
  - **Encapsulate customer MAC addresses using 802.1ah**

5) Partial Mesh Connectivity

- **Partial Mesh can be caused due to:**
  - **A failure in discovery mechanism – e.g., a PE doesn't get a full membership list**
  - **A PW fails to come up from the start**
  - **A PW failure occurs due to hw or sw failure (soft failure)**
  - **Node or Link failure along the path (including PEs)**

5) Partial Mesh Connectivity – Cont.

- **Failure to detect PW failure can result in**
  - **L3 control and routing protocols to misbehave [rosen-mesh-failure]**
  - **broadcast storm in the customer and provider network**
  - **multiple copies of a single frame to be received by CE and/or PEs**
- **Need to detect partial mesh failure**
- **Need to recover from partial mesh failure**
- **draft-rosen-l2vpn-mesh-failure suggests a mechanism for partial mesh detection**
- **no other proposal is on the table**

Issues 6 & 7

- **6) Handling of CE multicast**
  - **bridge control protocols**
  - **bridge data (non-IP)**
  - **bridge data (IP)**
- **7) Inter-operability between IEEE 802.1ad Bridges and VPLS PEs**

8) Fault Management

- **Service Providers need to be able to check the integrity of the service offered to their customers (from ACs to ACs)**
  - **Fault detection**
  - **Fault verification**
  - **Fault isolation**
  - **Fault notification (& alarm suppression)**
  - **Fault recovery**

8) Fault Management – Cont.

- **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**
  - **Mechanisms: Connectivity Check, Tracepath, Loopback, AIS**

Next Step

- Have more discussions on these issues to ensure that they are clear to everyone
- Have compliancy matrix on the bridge interop features listed in this draft
- Adopt this draft as WG document

Thank you!

sajassi@cisco.com