



VLAN-XC for Carrier-Grade Ethernet Networks

Nurit Sprecher

May 2006

SIEMENS

Communications

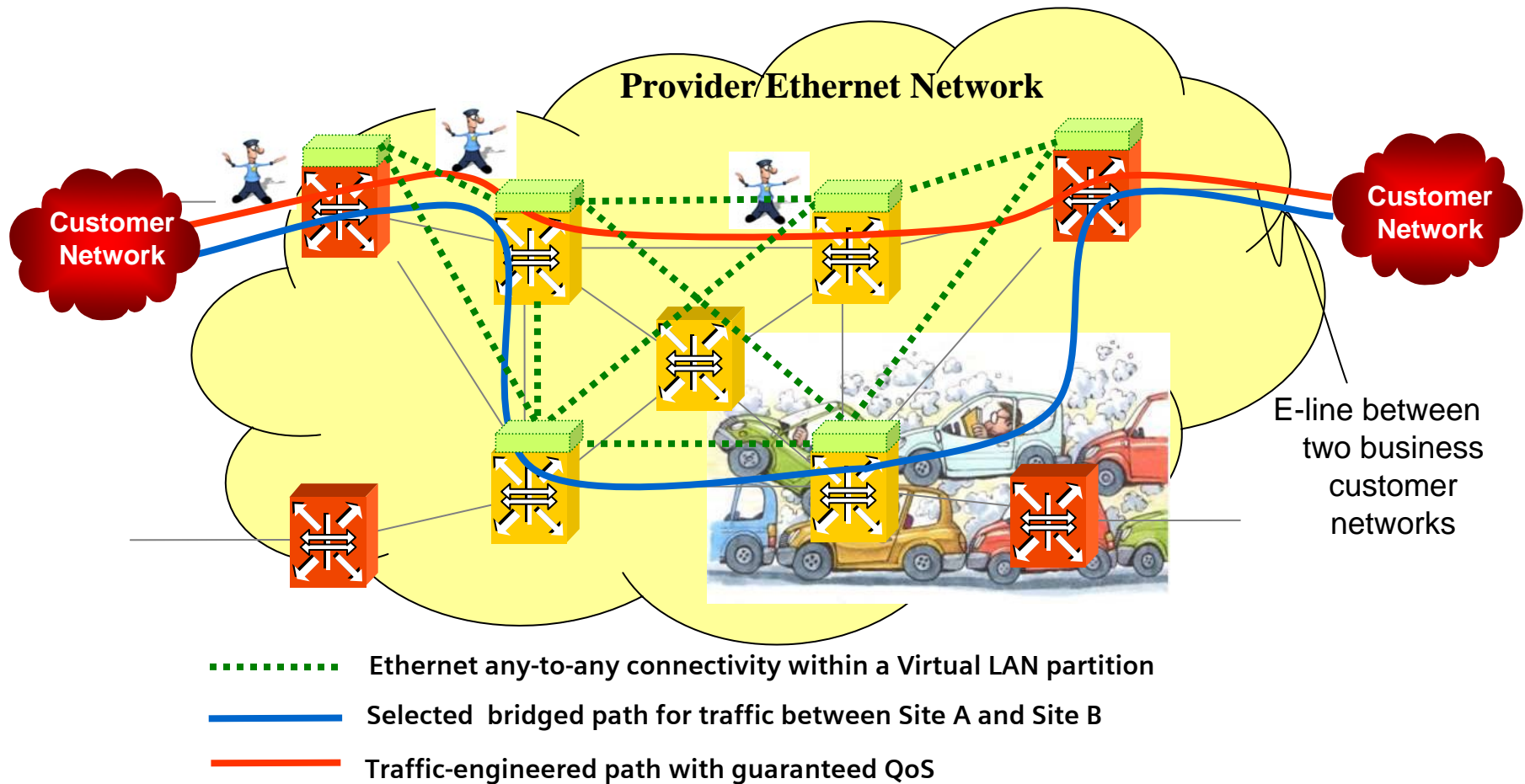
Carrier Requirements for Carrier-grade Ethernet Networks

- Carriers are increasingly searching for mechanisms to enable traffic engineering in carrier-grade Ethernet networks. Their aim is to engineer and provision deterministic, protected and secured trunks and services within their Ethernet networks.
 - Traffic engineering should be enabled.
 - The service model should scale to hundreds of thousands of subscribers with diversity of services in a single Ethernet domain.
 - Bandwidth should be handled using admission control and should be allocated to end-to-end Ethernet Switched Paths (ESPs).
 - Bandwidth should be handled using admission control and should be allocated to end-to-end, pre-provisioned (preferably disjoint) backup ESPs.
 - Full network recovery is required in 50 ms to maintain time-bounded services.
 - The networks and the services should be secured.
 - The network should be kept simple to minimize CAPEX and OPEX.

VLAN-XC in Carrier-grade Ethernet Networks

- VLAN-XC provides a technique for traffic-engineered Ethernet networks.
- VLAN-XC enables a Provider VLAN Transport (PVT) framework that defines mechanisms for carriers to engineer and provision deterministic, protected and secured Connection Oriented trunks and services within the Ethernet network.
 - PVT explicitly enables traffic engineering.
 - The PVT service model scales to hundreds of thousands of subscribers with diversity of services in a single Ethernet domain.
 - PVT allows bandwidth admission control and allocation to end-to-end Ethernet Switched Paths (ESPs).
 - PVT allows bandwidth admission control and allocation to end-to-end, pre-provisioned backup ESPs.
 - PVT provides 50 ms full network recovery.
 - The PVT service model provides secured networks and services.
 - Using PVT, the network is kept simple.

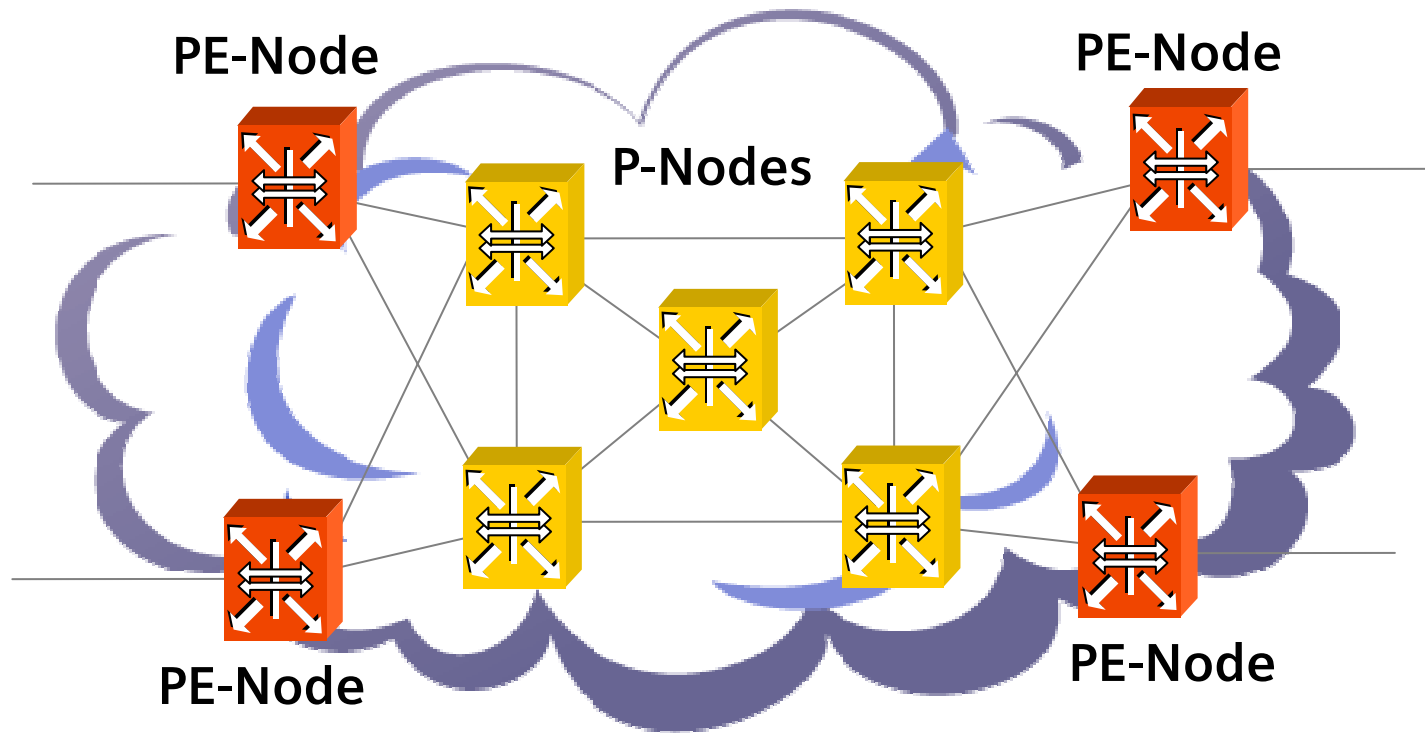
Provider VLAN Transport in Carrier Grade Ethernet Networks



Provider VLAN Transport in Carrier Grade Ethernet Networks (Cont.)

- Provider VLAN Transport (PVT) enables the provisioning of p2p and p2mp TE Ethernet Switched Paths (ESPs) across the Provider network.
 - Each TE ESP is uniquely identified by an NMS identifier.
 - The TE ESP is constructed from consecutive VLAN Cross Connects (VLAN-XCs):
 - The Provider Edges Nodes (PE-Nodes), which reside at the boundary of the Provider network, create and terminate the TE ESP.
 - The Provider Internal Nodes (P-Nodes), which reside within the Provider network, perform VLAN Cross Connect switching.
 - Each VLAN-XC has a 12-bit or 24-bit local scope identifier (VLAN-XC Identifier). Local scope identifiers simplify the VLAN-XC domain-wide provisioning task and improve scalability.
- PVT enables the provisioning of client services over the server TE ESPs.
- PVT realizes VLAN stacking to preserve customer information.

Provider VLAN Transport Network Reference Model

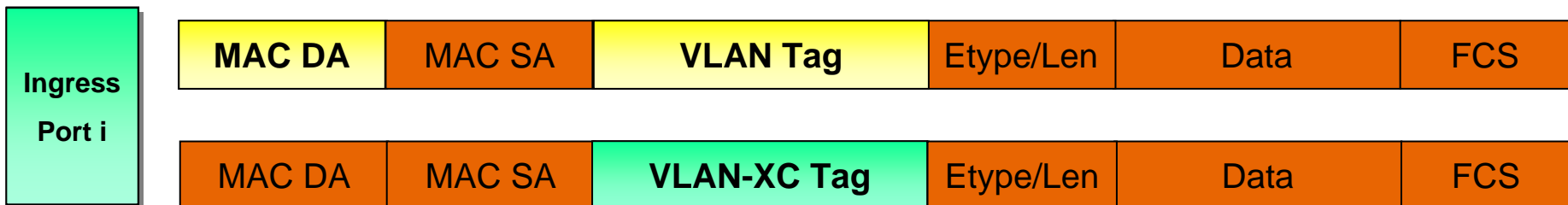


- Provider Edge Nodes (**PE-Nodes**) reside at the boundary of the provider network and create/terminate TE ESPs.
- Provider Internal Nodes (**P-Nodes**) perform VLAN Cross Connect switching.

VLAN-XC Frame Format

- VLAN-XC maintains the standard Ethernet frame (as defined in IEEE 802.1Q , IEEE 802.1ad).
- Once IEEE 802.1ah reaches a stable state, VLAN-XC will also maintain the new Ethernet frame format:
 - **Standard VLAN Bridging:** Switching based on MAC addresses and VLANs
 - **VLAN Cross Connect Switching:** Cross Connect according to the ingress port and the VLAN-XC Tag, **regardless of the MAC addresses**

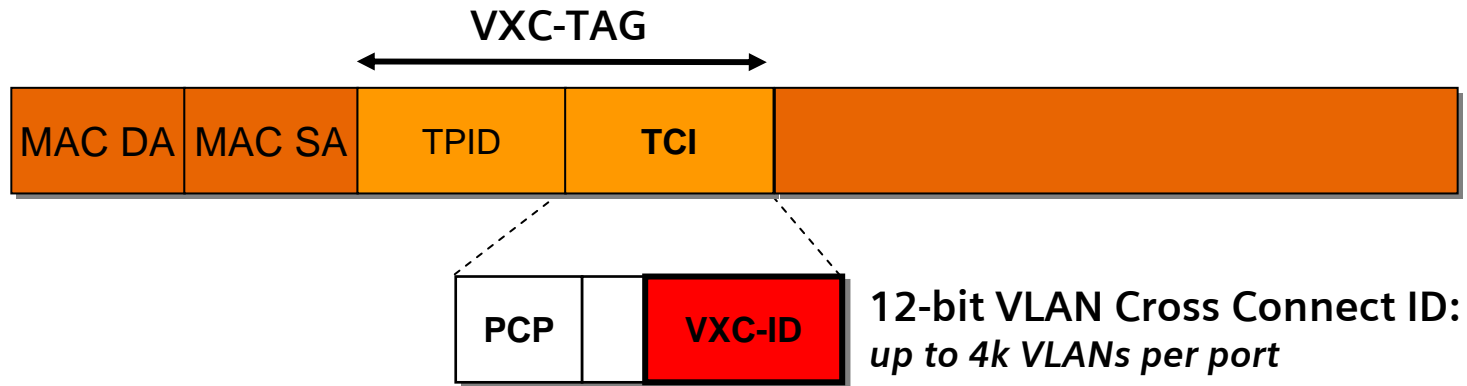
Ingress L2 packet



VLAN-XC Frame Semantic (1)

- Frame format as defined in IEEE 802.1Q
- VLAN Cross Connect tagged frame allows up to 4K VLANs per port

VLAN Cross Connect tagged frame

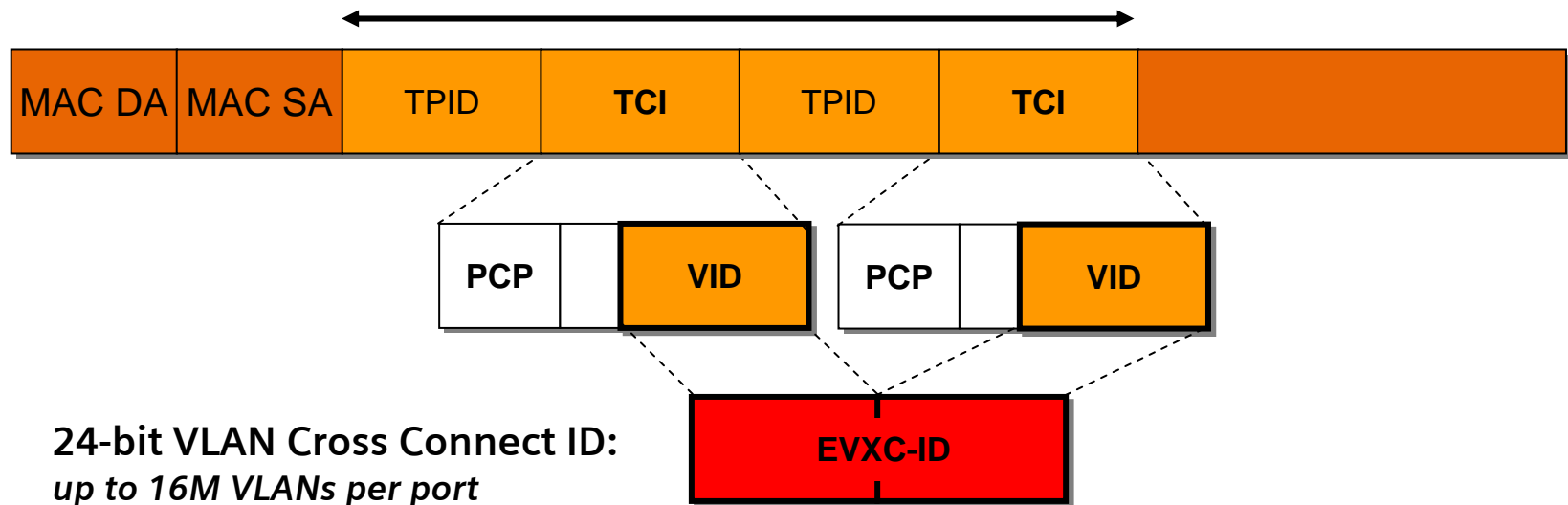


VLAN-XC Frame Semantic (2)

- Extended VLAN Cross Connect frame with a 24-bit VLAN Cross Connect ID:
 - Frame format as defined in IEEE 802.1Q
 - VLAN Cross Connect tagged frame allows up to 16M VLANs per port

Extended VLAN Cross Connect tagged frame

EVXC-TAG



Extended VLAN Cross Connect frame: VLAN Scalability Issues

- In enterprise networks, 4K VLANs are traditionally used to create virtual LANs.
- In provider networks, VLAN deployment is extended to handle new requirements:
 - **User identification** is required for policing, billing and fault isolation purposes.

User identification is required, for example, in wholesale solutions where the network provider is not aware of the IP addresses of its customers.
 - **User isolation** is required to prevent traffic leaking and unauthorized communication between users.
 - **Service separation** is required for traffic engineering purposes.
- Extending the use of VLANs creates VLAN scalability issues.

Extended VLAN Cross Connect frame:

VLAN Scalability Issues (Cont.)

Example of VLAN scalability problems:

For residential services, with hundred of thousands of subscribers, Q-in-Q should be supported:

- In a typical aggregation network, the outer VLAN is used to identify the DSLAM (and optionally, the specific service), while the inner VLAN is used to identify the DSLAM port (i.e. the subscriber).
- In VDSL, the number of DSLAMs in an aggregation domain can easily reach thousands:
 - 4K VLANs are insufficient, especially when more than one service is provided.
 - The number of VLANs left for multipoint services (E-LAN services) is small.

In bridging, there are mechanisms which resolve the scalability issues, such as port isolation, PVLAN, etc. However, although these mechanisms resolve the scalability issues, they do not address the network providers' requirement for user identification.

 A wider VLAN TAG is required to handle the new requirements in provider networks.

Extended VLAN Cross Connect frame: Translation Operation on the Wider VLAN TAG

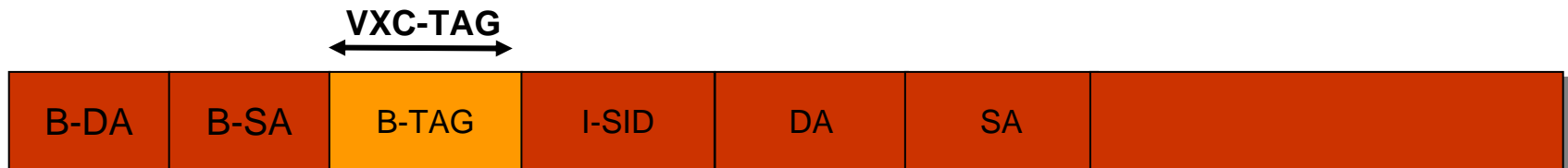
A translation operation is required on the wider VLAN TAG to enable a simple mass provisioning process. Mass provisioning is very common, for example, in residential services:

- The DSLAMs tag the customer's traffic with a VID identical to the DSLAM's port number to which the customer is attached.
- The first-level aggregation nodes stack a frame from a DSLAM with a VID that is identical to the port number to which the DSLAM is attached.
- The 2nd-level aggregator should translate the incoming VID to a unique value when forwarding it via its uplink.

PVT Frame Semantic (3)

- VLAN Cross Connect frame with a 12-bit VLAN Cross Connect ID:
 - Frame format as defined in IEEE 802.1ah
 - VLAN Cross Connect tagged frame allows up to 4K tunnels per port
 - VLAN Cross Connect tagged frame allows up to 16M services per tunnel

VLAN Cross Connect tagged frame

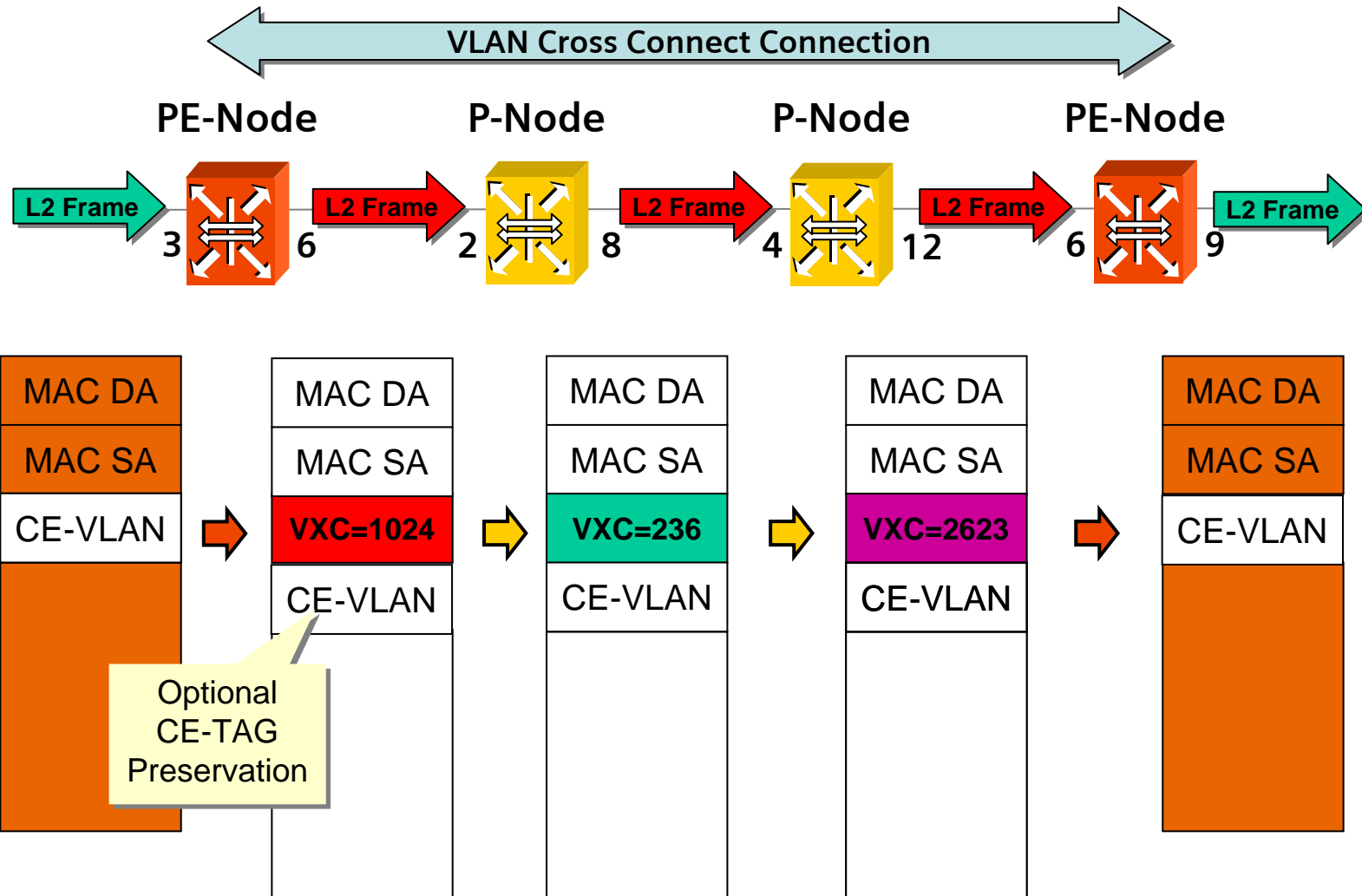


12-bit VLAN Cross Connect ID:
up to 4k tunnels per port
up to 16M services per tunnel

PVT – Forwarding Behavior

- At each P-Node, VLAN-XC frames are forwarded according to the ingress port and the VLAN-XC identifier of the ingress frames. The P-Node may swap the VLAN-XC identifier.
- PVT's forwarding tables are configured using a provisioning/management system or a GMPLS control plane.

Provider VLAN Transport Example (with CE-VLAN Preservation)

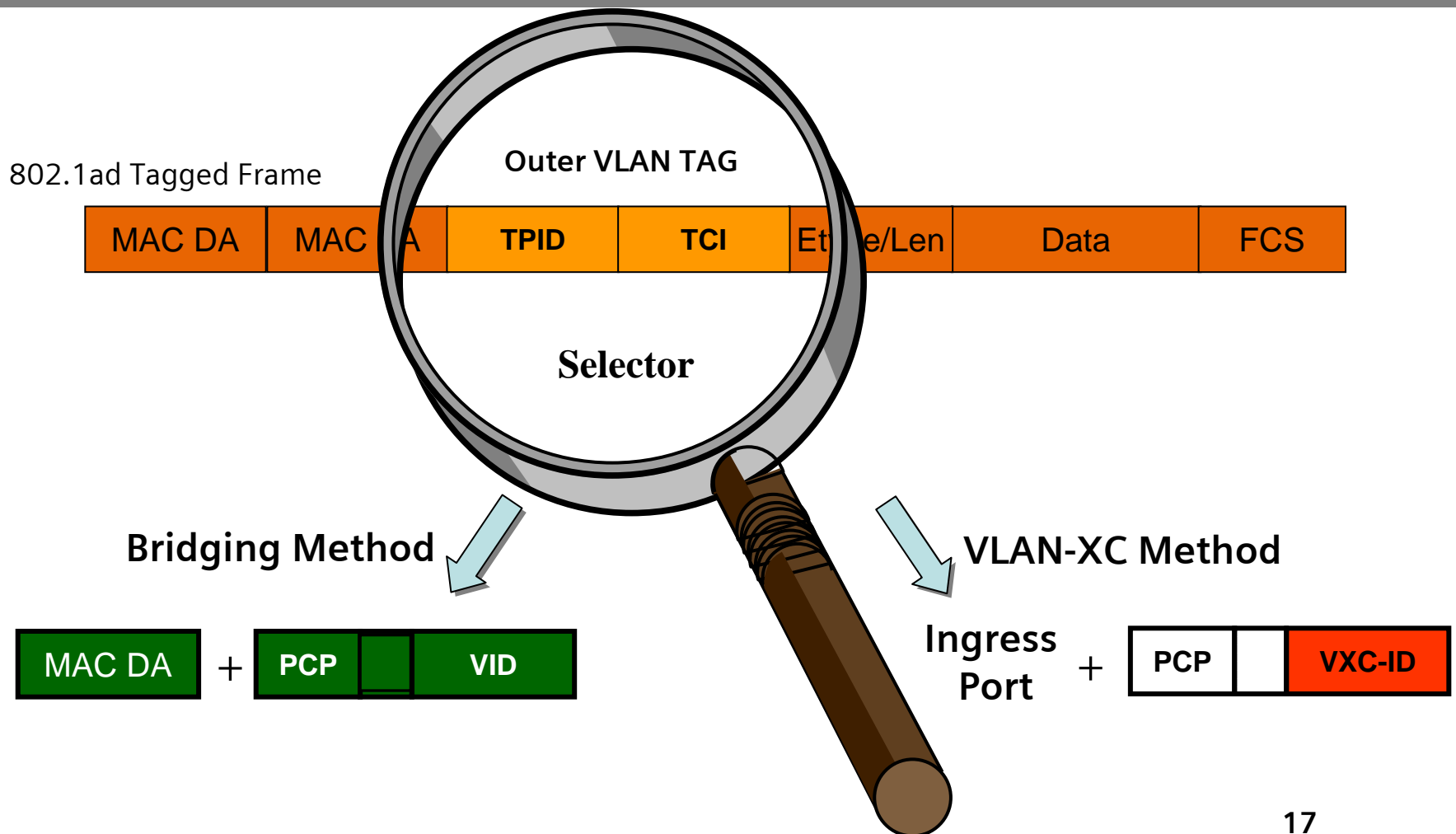


Provider VLAN Transport – How it Works

- The VID address space is pre-divided between conventional bridging and PVT:
 - MAC learning is disabled on all VLAN-XC VIDs:
 - Unknown frames are discarded.
 - Multicast and broadcast frames are forwarded.
 - PVT has complete freedom to configure routes. There is no need to disable blocking.
- A separate management or control plane is used to:
 - Set up ESPs:
 - May use any route algorithm which assures loop-free paths
 - Load may be calculated for each ESP and allocated to each physical link
 - Populate the forwarding table
 - Set up protection ESPs
- VLAN-XC layer co-exists with standard VLAN bridging layer, even on the same port.

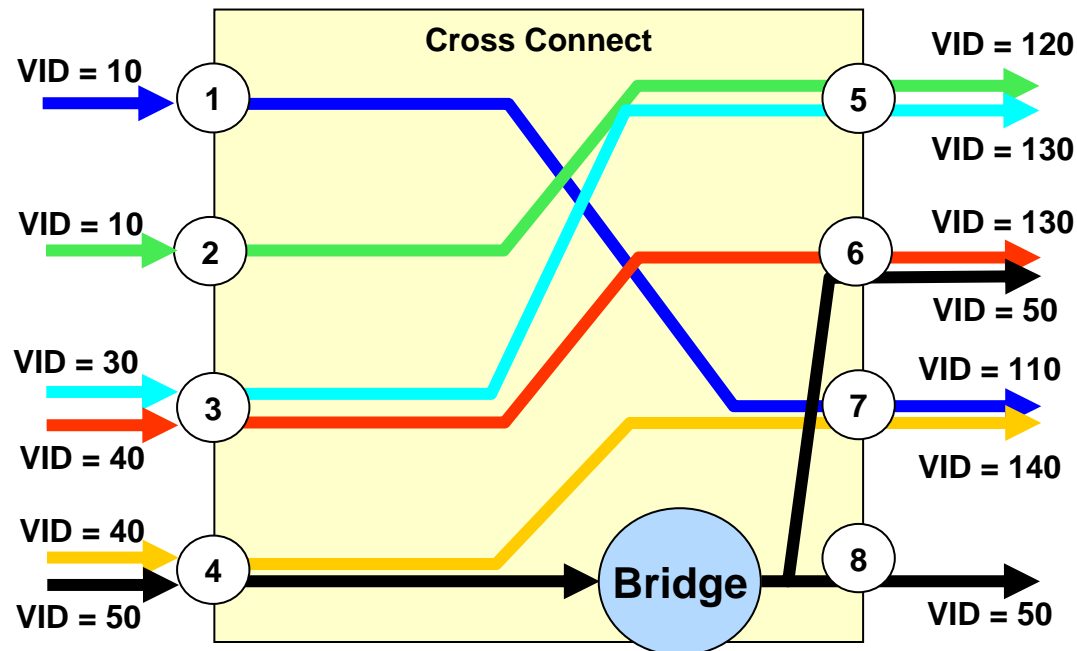
VLAN-XC / Bridging Selector

The outer VLAN Tag acts as the method selector (TBD whether VID space, new TPID).



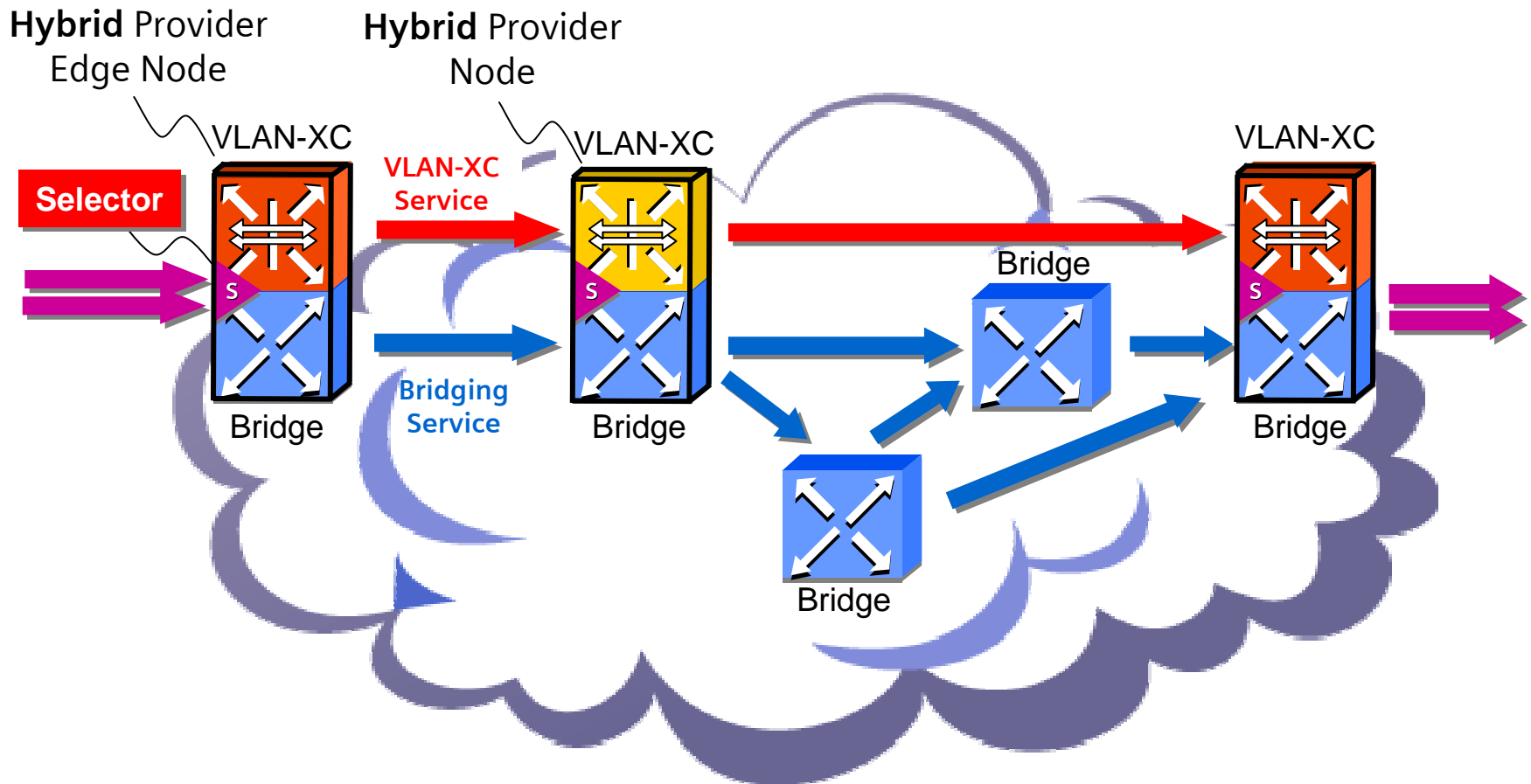
PVT VLAN Cross Connect Switching Process Example

| In Port | Ingress VLAN | Out Port | Egress VLAN |
|---------|--------------|----------|-------------|
| 1 | 10 | 7 | 110 |
| 2 | 10 | 5 | 120 |
| 3 | 30 | 5 | 130 |
| 3 | 40 | 6 | 130 |



Hybrid VLAN-XC & Bridging Network

VLAN-XC and Bridging layers co-exist in the same provider network.



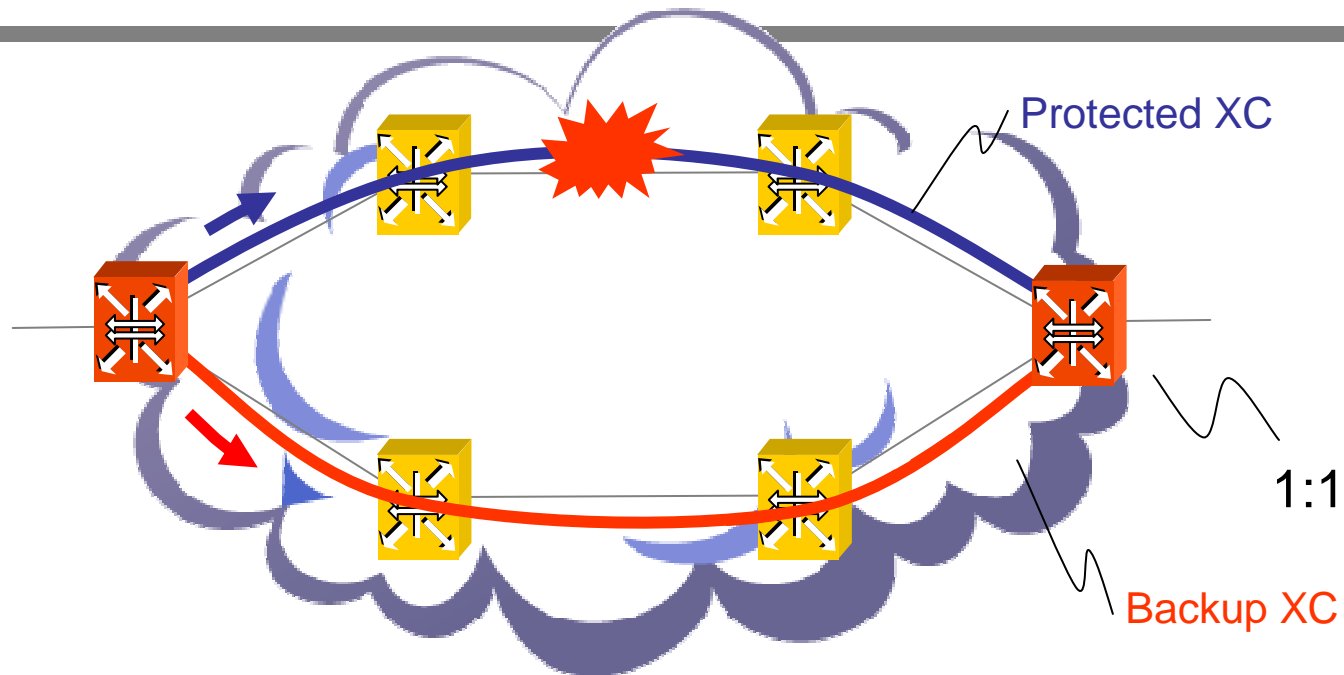
Hybrid VLAN-XC & Bridging Network (Cont.)

- VLAN-XC should be implemented in conjunction with connectionless bridging with the aim of providing the optimum method per service:
 - Bridging is appropriate for the following services:
 - IPTV
Requires tens of channels (DA MACs) and a few TV servers (SA MACs)
 - Business multipoint VPN (E-LAN):
 - Provided for large enterprises
 - Small enterprises use point-to-point VPNs (optionally using the hub-and-spoke topology).
 - Network management
Requires a small number of MAC addresses (i.e. number of network elements) and only one VLAN
 - VLAN-XC is appropriate for business-critical services with an associated SLA, and for services that consume a large number of MAC addresses and VLANs:
 - Residential services
 - High speed Internet service
 - Voice services
 - Video-on-demand
 - Business services
 - Point-to-point VPN (E-LINE)
 - Multipoint VPN (hub-and-spoke based E-LAN)
 - Voice services
 - Wholesale services

PVT - Service Resiliency

PVT provides 50 ms full network recovery to maintain time-bounded services, even when thousands of services are simultaneously affected by a failure:

- 1:1 global protection with extra traffic, including pre-provisioned end-to-end backup paths
- Fast error detection using IEEE 802.1ag OAM messages
- 50 ms switchover following failure
- Revertive or non-revertive modes when the failure is eliminated



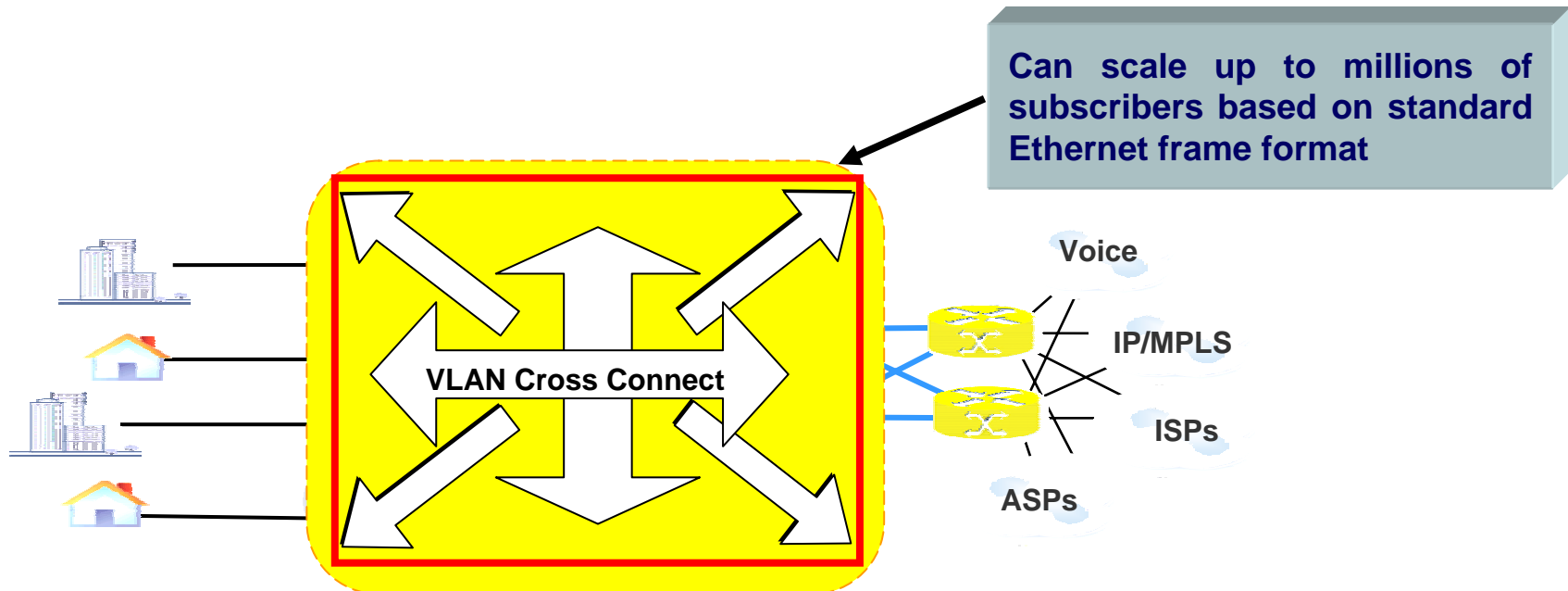
PVT – OAM Messages

Using PVT, OAM frames are transmitted within the ESP towards the destination.

CC OAM messages are sent to detect misconnectivity and connection breaks to enable fast recovery in the event of a failure in the network.

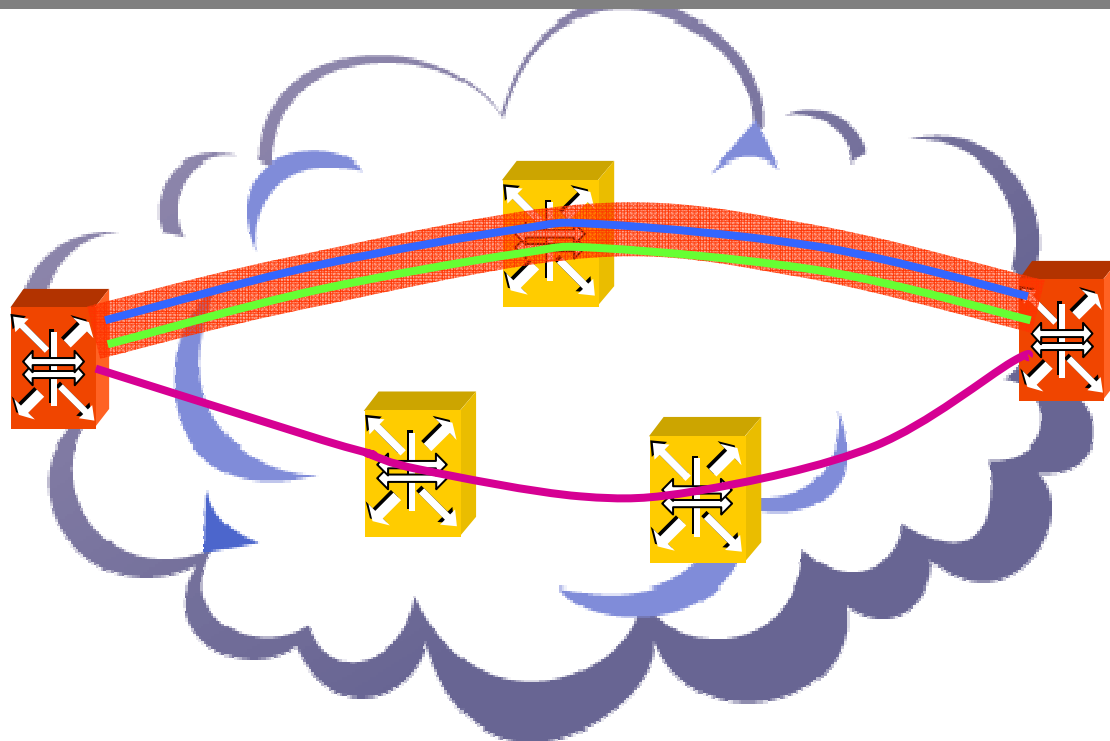
PVT - Scalability

- VLAN Cross Connect is MAC agnostic, hence the MAC scalability issue is inherently eliminated.
- VLAN Cross Connect eliminates VLAN scalability issues.
 - In a VLAN Cross Connect, the VLANs have local port scope.
 - Users are inherently identified and isolated by the end-to-end connection.



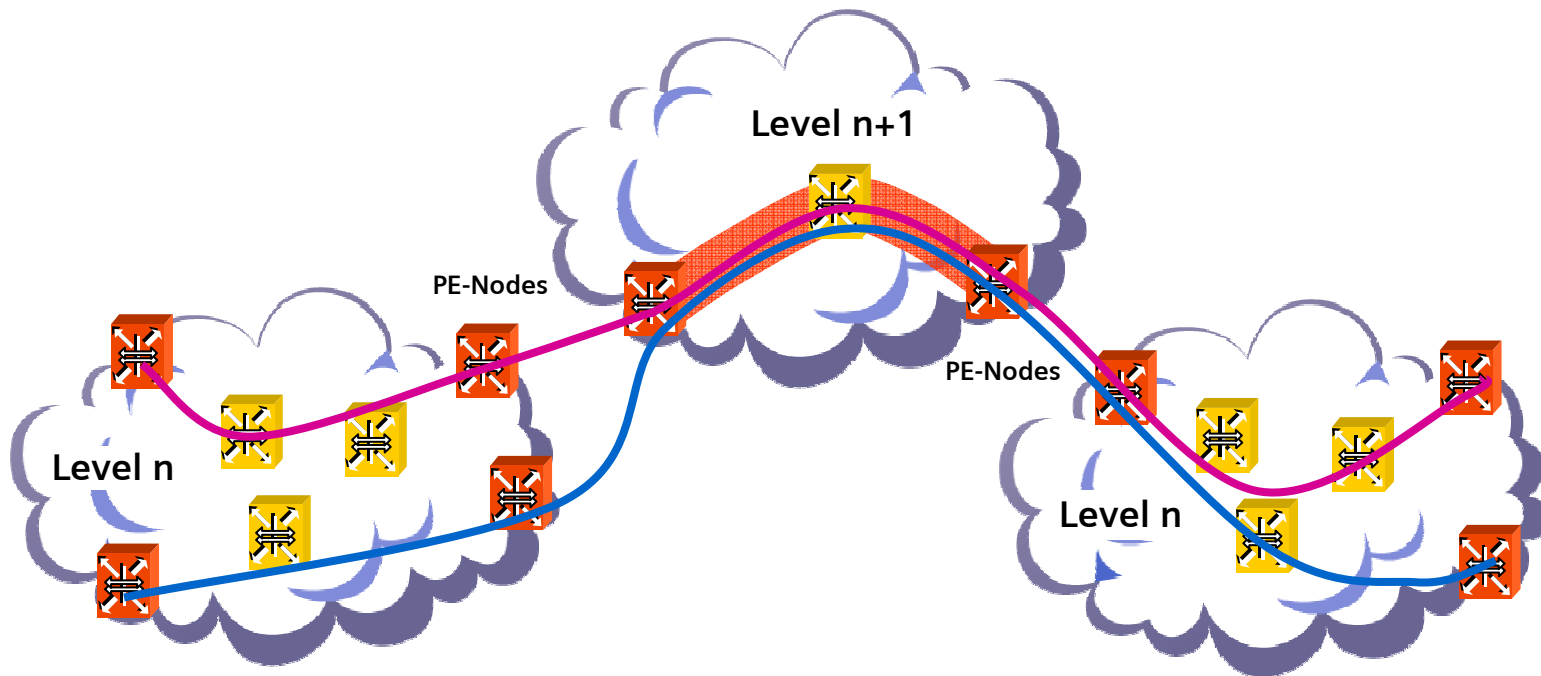
PVT – Scalability (Cont.)

- An ESP can be used as a service transport or as a tunnel. Many combinations may be considered:
 - Services with 12 or 24-bit identifiers
 - Tunnels with a 12-bit identifier. Services within the tunnel may have a 12-bit or 24-bit identifier.



PVT – Scalability (Cont.)

- End-to-end services between two level n domains can be delivered via level n+1 tunnels (using VLAN Stacking).



In a VLAN Cross Connect, security issues are inherently eliminated for the following reasons:

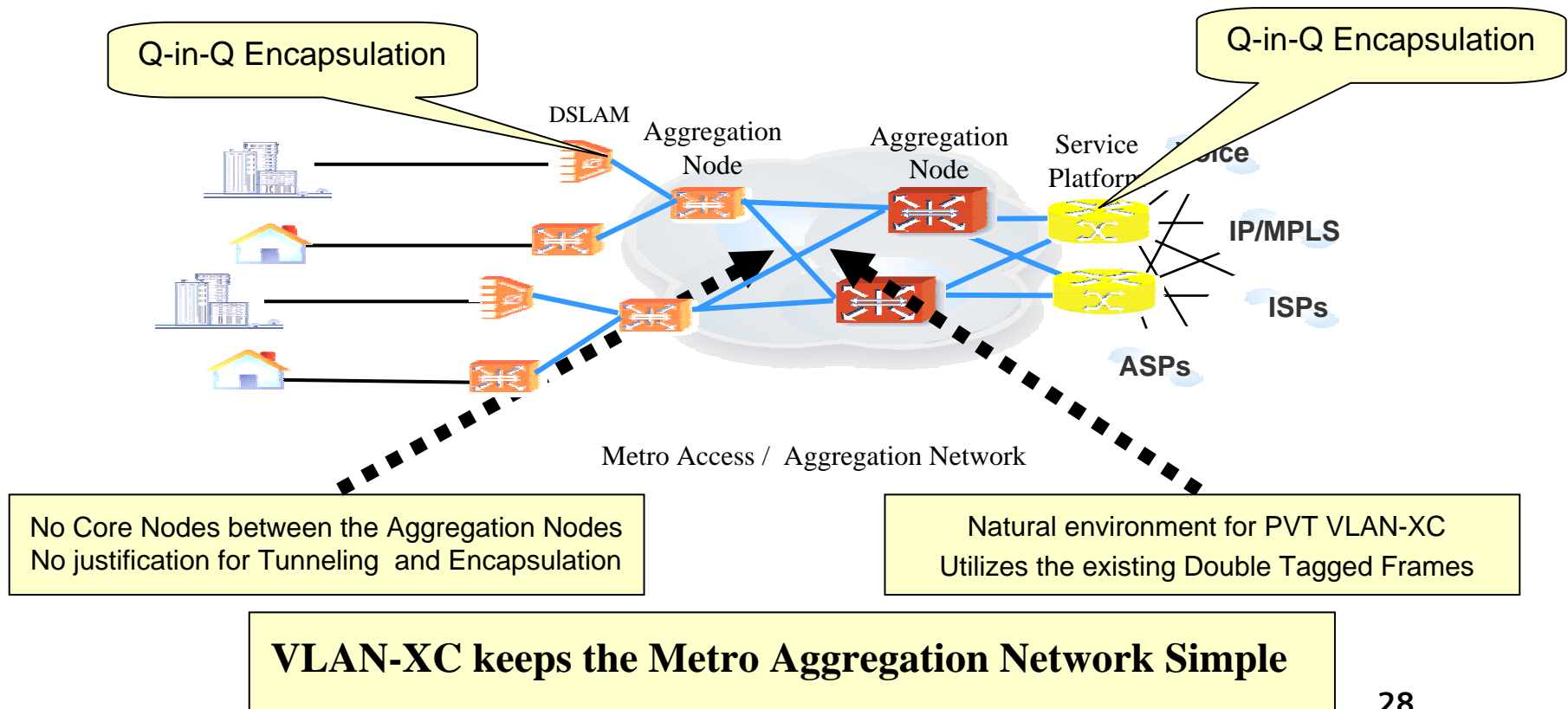
- It is MAC agnostic, hence there is no danger of MAC attacks and MAC spoofing.
- Traffic flows are transmitted via a pre-provisioned, end-to-end connection and there is no flooding, hence:
 - Traffic leaking is eliminated.
 - Communication between unauthorized users is eliminated.

PVT – Client Services

- A client service is mapped to ESP(s) according to the port on which the frame has been received and the frame's outer VID.
- Client service adaptation: PVT is capable of providing any service that is supported by standard Ethernet (such as IP, Ethernet MAC frame, TDM, etc.).
 - PVT adapts Ethernet traffic per 802.1ad. Non-Ethernet traffic is adapted using standard Ethernet encapsulation: TDMoE, etc.
 - PVT uses encapsulation and multiplexing to adapt client services over 802.1ah trunks.

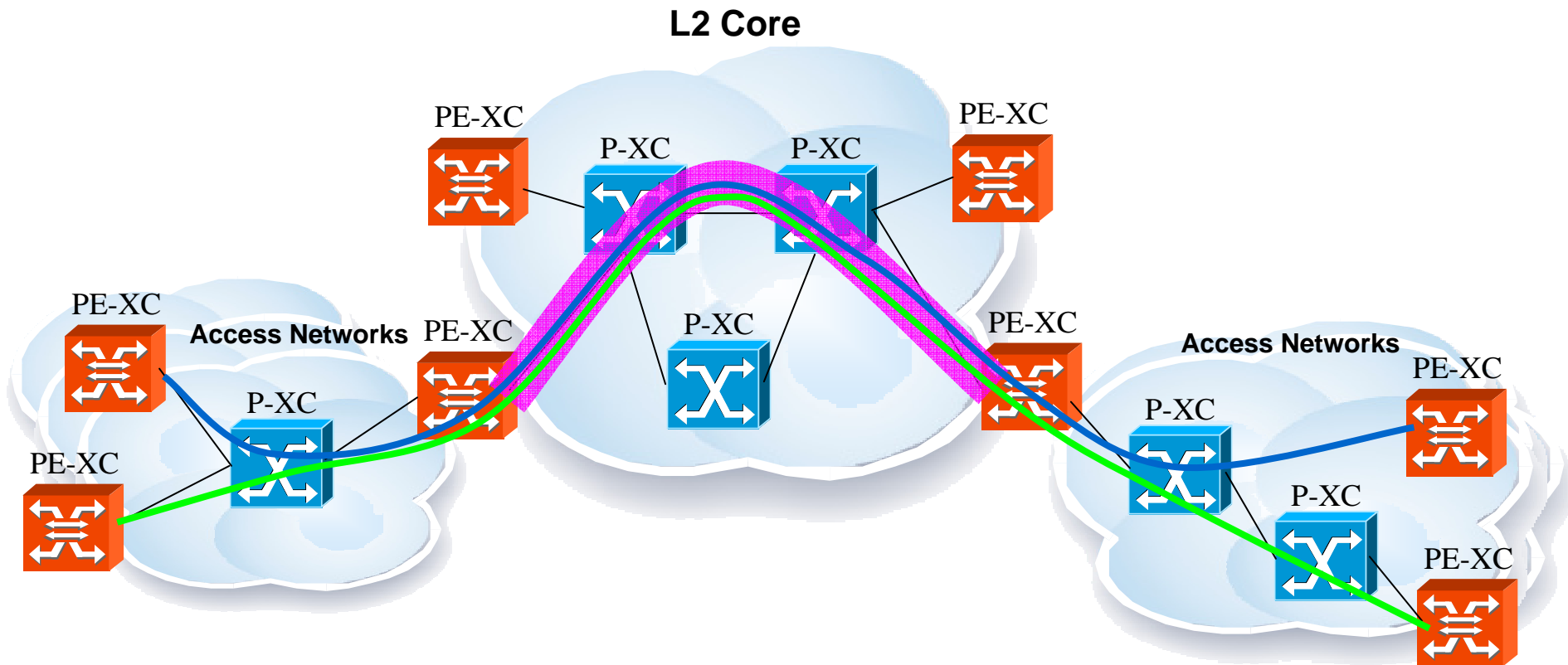
PVT in Metro-Access Networks

PVT is naturally appropriate for the delivery of residential and broadband services in Metro Access and Metro Aggregation networks.



PVT for Ethernet Services in Access and Core Networks

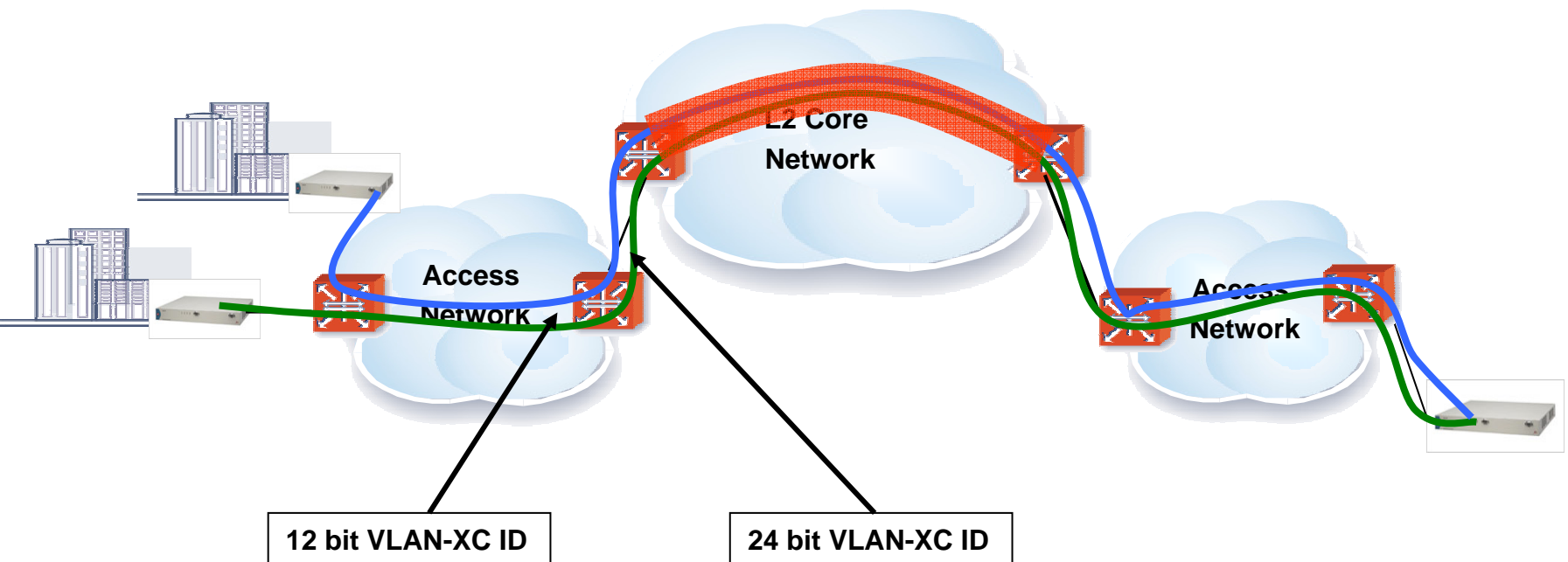
- PVT is appropriate for the delivery of p2p and p2mp services in Metro Core and Core networks. It provides ESPs with tunneling mechanisms.



PVT from CPE Site

PVT can start from the CPE site without imposing any scalability problems.

- The VLAN has local port scope.
- Can scale up to millions of subscribers per network.



PVT Advantages

- Realizes a proven cross connect technology.
- Uses a simple method for TE p2p and p2mp ESPs.
- Utilizes a simple adaptation function for Ethernet services in edge nodes.
- Defines a simple multiplexing method.
- Can easily be extended to work with 802.1ah.
- May start from the CPE site without imposing any scalability problems.
- Provides a natural solution for residential and broadband services in aggregation networks.
- Can be naturally used to deliver p2p and p2mp services across L2 core and transport networks.
- Co-exists with Ethernet bridging.
- Provides a solution for both E-LSP and L-LSP.
- Has no impact on Layer 3 protocols.
- All GMPLS functions can naturally be applied (e.g. inter-domain connectivity, FRR, segment and local protections, p2mp connectivity, etc.).

Conclusion

- Provider VLAN Transport (PVT) is a framework that utilizes VLAN-XC as a technique for Traffic Engineered Ethernet Network.
- Provider VLAN Transport (PVT) is appropriate for delivering Ethernet services across Metro and Core networks. PVT can start from the CPE site.
- We think it is important to standardize the Provider VLAN Transport (PVT) with its VLAN-XC technique.
- We encourage participants who are interested in Provider VLAN Transport to contact us and discuss the concept with us.



Thank You!