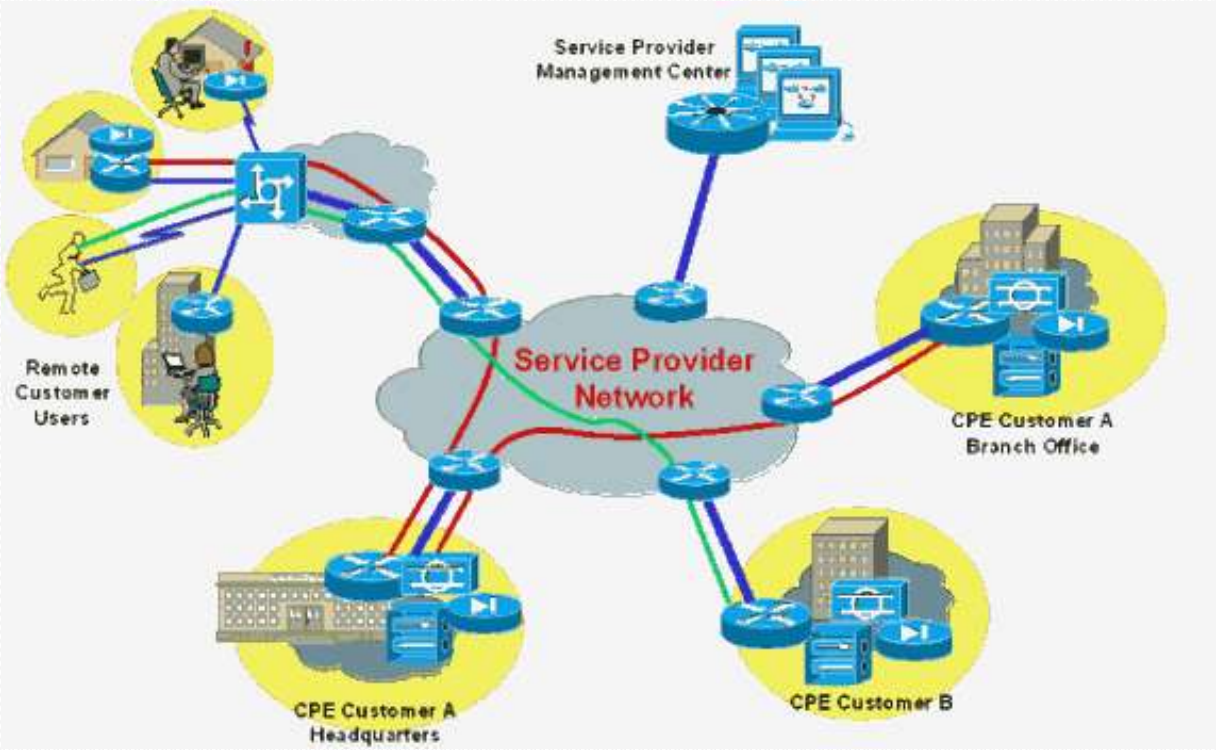
PI-Grau
(Internet Protocols)

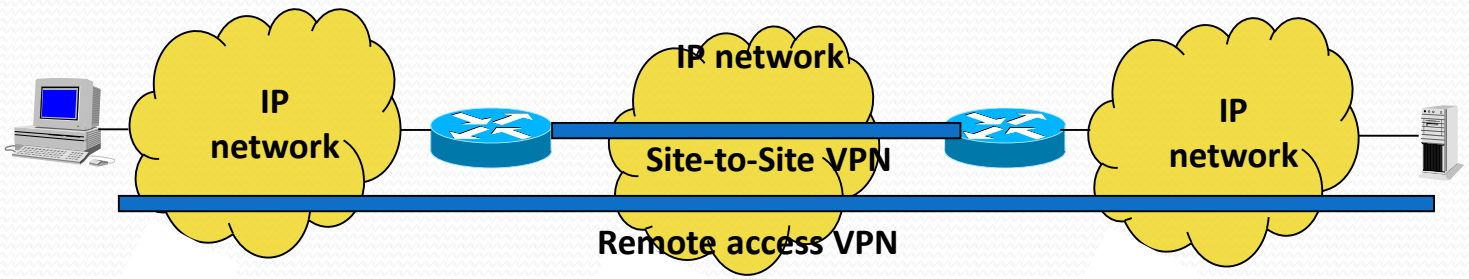
José M. Barceló Ordinas
Departamento de Arquitectura de Computadores (UPC)

- **Topic 5: Corporate Networks revisited: VPN**
  - Objectives
    - Connectivity with **the Remote Sites and between sites**
    - **Virtual Private Networks (VPN)**
      - MPLS-BGP
      - Metro-Ethernet

- **VPN (Virtual Private Networks):**
  - Network provided by ISP's (L3) or Telecom operators (L2) that interconnects the main site with remote sites or with end users (tele-working) in a secure an private manner.

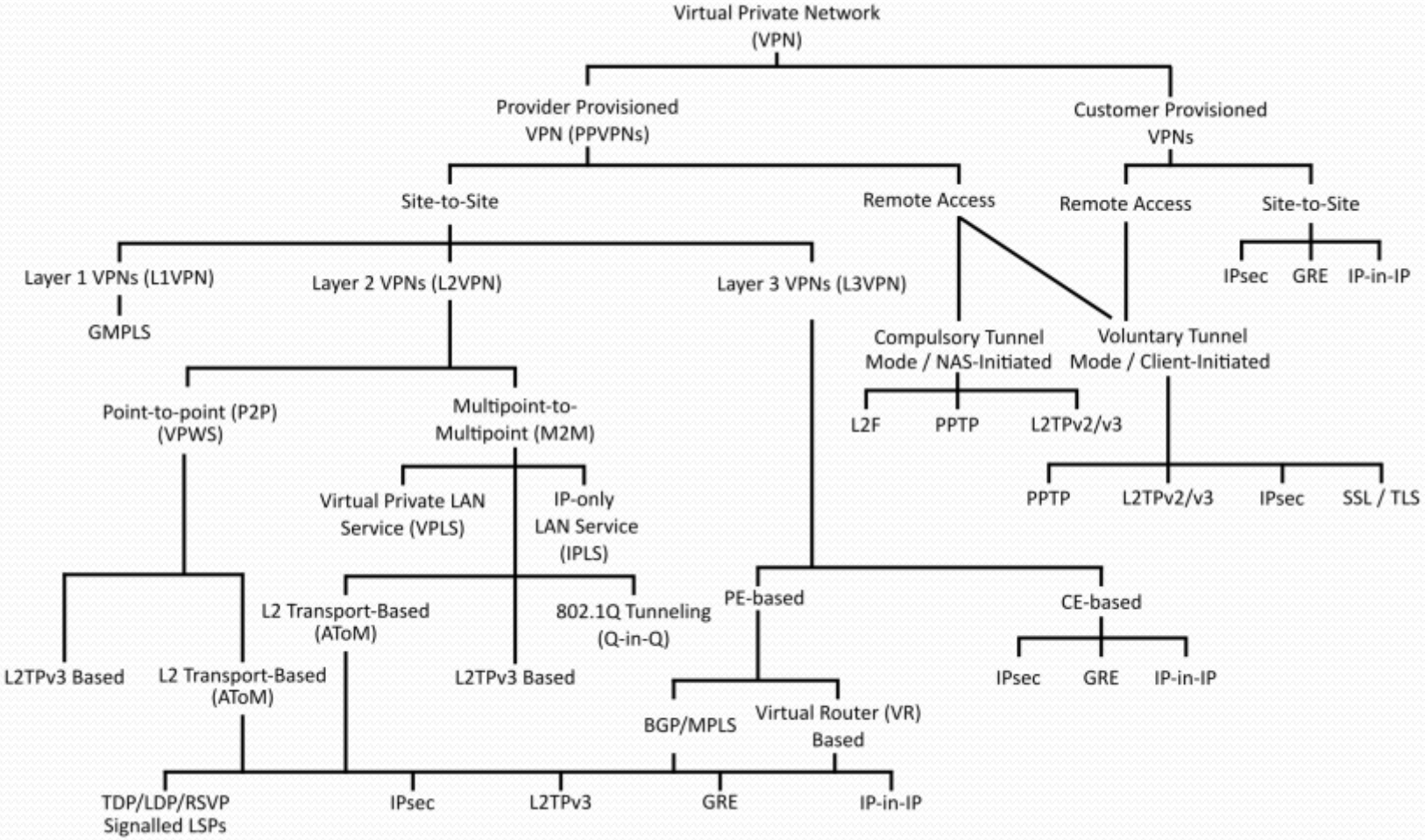


- **VPN (Virtual Private Networks):**
  - Connection between two network points using tunnel techniques that may include QoS negotiation, security, …
  - Used to connect the Main Site with the Remote Site
    - **Site-to-Site VPN**: connects two networks (sites), thus implying gateway-to-gateway tunnels. The main example is a remote office connection to the main company quarters.
    - **Remote access VPN**: connects a user to a network, thus implying a host-to-gateway or host-to-host tunnel. The main example is a worker that remotely access to the office.



VPN (Virtual Private Networks):

- **Tunnels:** Logic interface that allows packet encapsulation in several formats (L4, L3 or L2). Examples of L2/L3 tunnels are PPTP, L2TP, IP-in-IP Encapsulation, Minimal Encapsulation, Generic Routing Encapsulation, IPsec, MPLS, …



Provider-provisioned VPN (PPVPN):

- PPVPN are L3 tunnels (sometimes are L2) that provide connectivity site-to-site (including many-to-many sites) guaranteeing QoS and security (authentication and encryption) across an ISP,
- They allow to create a super-imposed network topology over the ISP, meaning that the owner of the sites can create a:
  - **Point-to-point topology:** connectivity between two sites,
  - **Point-to-multipoint topology:** connectivity between one site and many sites,
  - **Multipoint-to-multipoint topology:** connectivity between many sites and many sites.
- Examples:
  - **MPLS-BGPv4** that creates tunnels using BGPv4 to signal and create the tunnel and MPLS to route traffic,
  - **VPLS (Virtual Private LAN Service)** that creates VPN's using VLAN (and thus is a emulating a L2 VVPN). The example is **MetroEthernet**.
- In general, VPN's does not support broadcasting services, but there are variants (normally based in VPLS technologies) that overcome this limitation.

Traffic Parameters

- **CIR (Committed Information Rate)**
  - Average data rate (b/s) associated to a service or flow (not an instantaneous data rate)
- **EIR (Excess Information Rate)**
  - Average data rate (b/s) in excess with respect CIR → be careful, sometimes it is specified a PIR (**Peak Information Rate**) and PIR=CIR+EIR → EIR=PIR-CIR (an excess !!!)
- **CBS (Committed Burst Size)**
  - Size in Bytes of the transmitted information. Amount of bytes that can be sent over a period of time T when congestion occurs. Normally is the **packet size**.
- **EBS (Excess Burst Size)**
  - Excess in size in Bytes of the transmitted information. Amount of extra bytes that can sent by a router over the time T when no congestion occurs. Then, if EBS>0 → you can send traffic exceeding the CIR.

- **Traffic Parameters**
  - Example: Capacity of 10 Mb/s with a CIR of 5 Mb/s and a CBS of 1 packet of 1500 Bytes, with an EIR=0 and EBS=0:

The same, but with an EIR=0 and EBS=1

The same, but with an EIR=0 and EBS=2

  - Capacity of 10 Mb/s with a CIR of 5 Mb/s and a CBS of 1 packet of 1500 Bytes, with a EBS=1 and an EIR = 1 Mb/s (1 packet of every 10):

Traffic Parameters: examples

- **Maximum CIR → CIR ≤ C (Line capacity)**
  - The CIR can not exceed the capacity line (It is logical !!!)
- **Best-effort → CIR=0, CBS=0, EBS >0**
  - Means that you want a best-effort contract, that means that the ISP does whatever he can do to transfer your data but it is not assuring you that the traffic is sent → ideal for a low cost contract
- **CIR enforcement: rate ≤ CIR**
  - The ISP enforces that the traffic is never higher than the CIR
- **CIR Contract: CIR>0, EIR>0, CBS>0, EBS>0**
  - The customer is guaranteed at least a CIR (under congestion conditions) if he sends his CBS. However, if there is no congestion he can achieved CIR+EIR sending EBS bytes of excess during periods of time.

Performance or QoS parameters

- **Packet Delay**
  - Delay in seconds of a packet from the time it leaves from a point to the time it arrives to other point
  - Important in real-time applications (e.g., voiceIP, multimedia) with QoS
- **Jitter**
  - Delay variation of a packet
  - Important in real-time applications (e.g., voiceIP, multimedia) with QoS
  - Normally it is calculated as the difference between the average delay and the minimum delay of packets
- **Packet Losses**
  - 1 less the ratio of delivered packets with respect transmitted packets
  - Important for applications such as VoiceIP (3% of lost packets results in an inacceptable quality reception value)

MPLS (Multi-Protocol Label Switching)

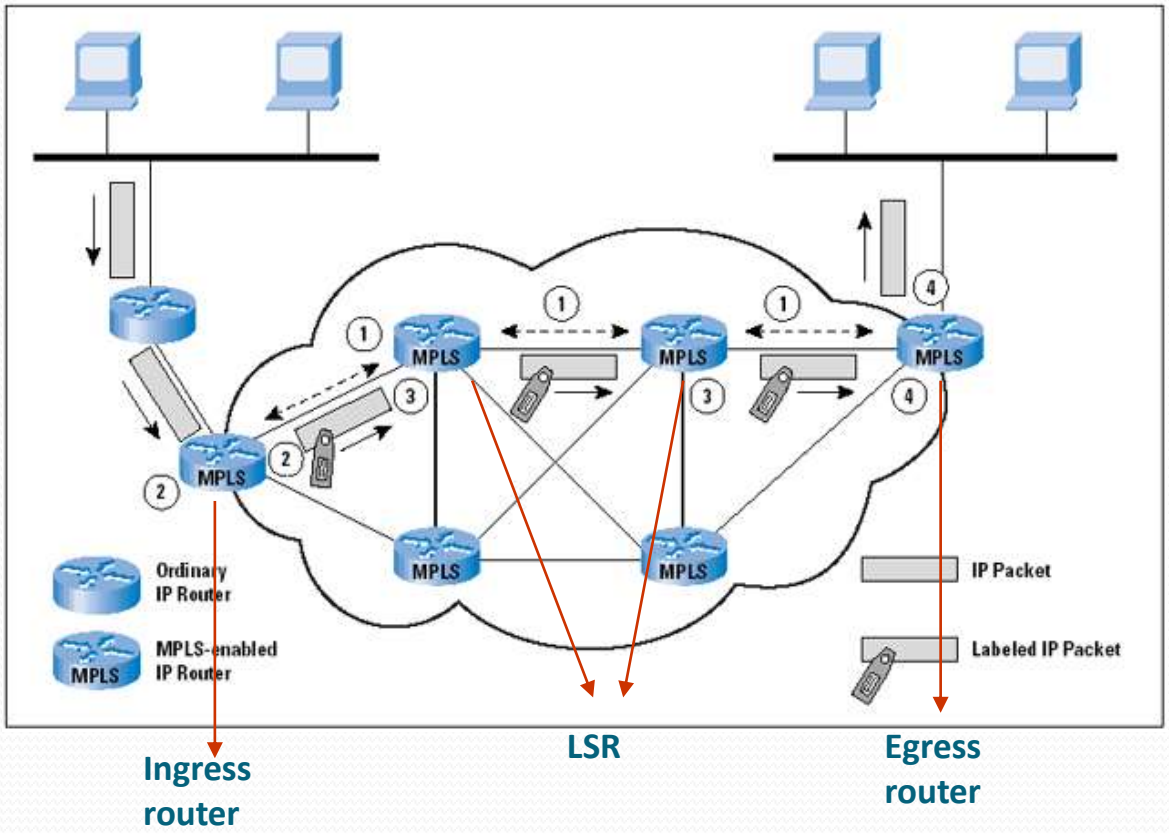
- L3 protocol that forwards packets using labels instead of IP addresses and that allows:

  - **QoS**
    - Guarantee certain capacity to real-time services and guarantee certain packet delay, jitter control and packet losses values → voice and video
  - **VPN services**
    - Support packet segregation in Internet
    - Used jointly with BGP (MPLS-BGP as a VPN)
  - **Traffic Engineering**
    - Optimize network resources from user demand traffic parameters (CIR, EIR, CBS, EBS)
  - **Multi-Protocol support**
    - Independent of the technology (e.g. Frame Relay, ATM, …)

MPLS (Multi-Protocol Label Switching)

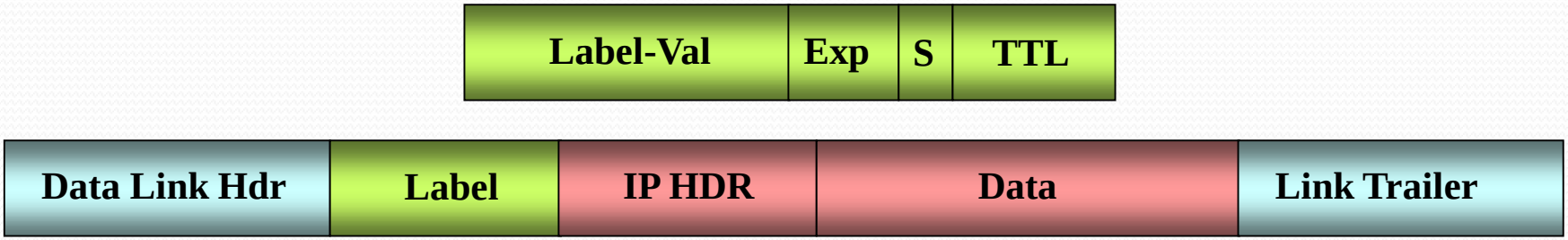
- L3 Basic Functionality: packet labeling and packet labeled switching

Figure 1: MPLS Operation



- **LSR (Label Switched Routers):** routers that switch packets based on labels carried by packets and that identify flows between end points
- **FEC (Forwarding Equivalence Class):** describes a set of flows that will receive the same treatment (same label) and that correspond to an LSP
- **LSP (Label Switched Path):** a path in a MPLS network
- **LDP (Label Distribution Protocol):** protocol for label distribution

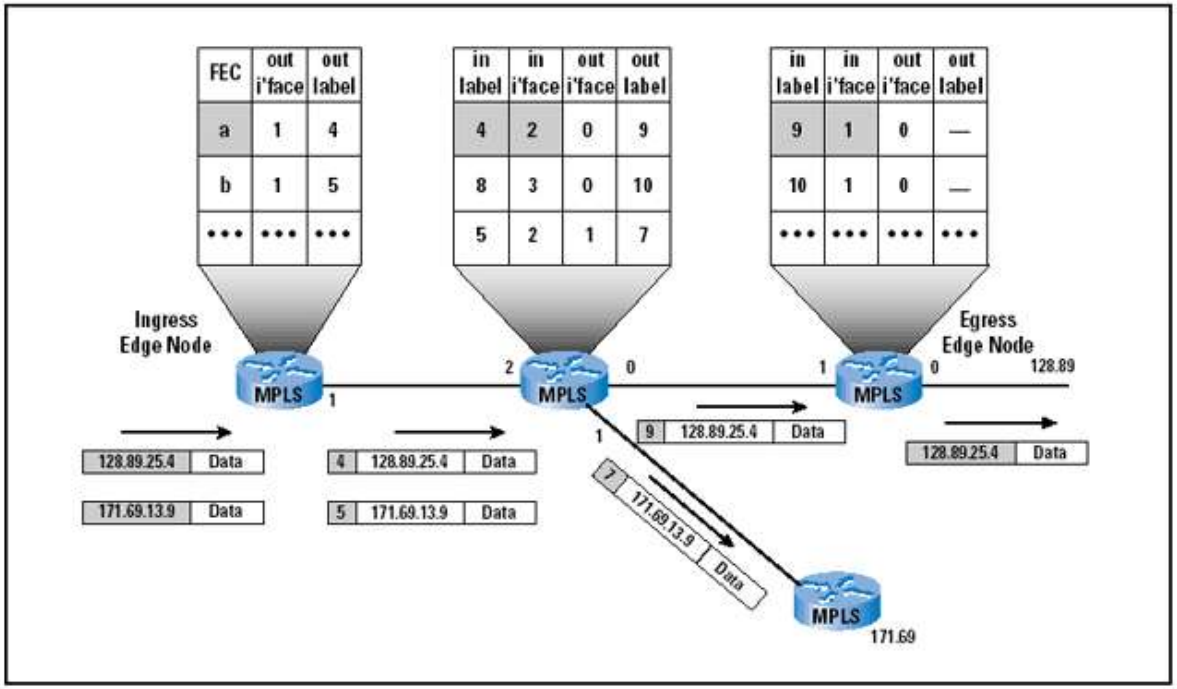
- **LDP (Label Distribution Protocol):** protocol for label distribution
  - A bi-directional communication is established between two LSR routers to exchange labeling information
  - Labels:
    - **Label-Value:** 20-bit to number labels
    - **Exp:** 3-bit to define QoS
    - **S:** 1-bit de flag (bottom of stack) → yes or no
    - **TTL:** 8-bit
  - The label has local meaning, it is to say, a router that receives a packet labeled, checks it, assigns a new one and switches to the output interface



Topic 5: Corporate Networks: Switching Blocks.

- Routers route using LSP (Label Switched Path), a pre-established path (e.g., using some IGP routing such as OSPF)
- Packets with different label (belong to a different FEC) will receive a different treatment in the routers (e.g. priorities, schedulers, …)

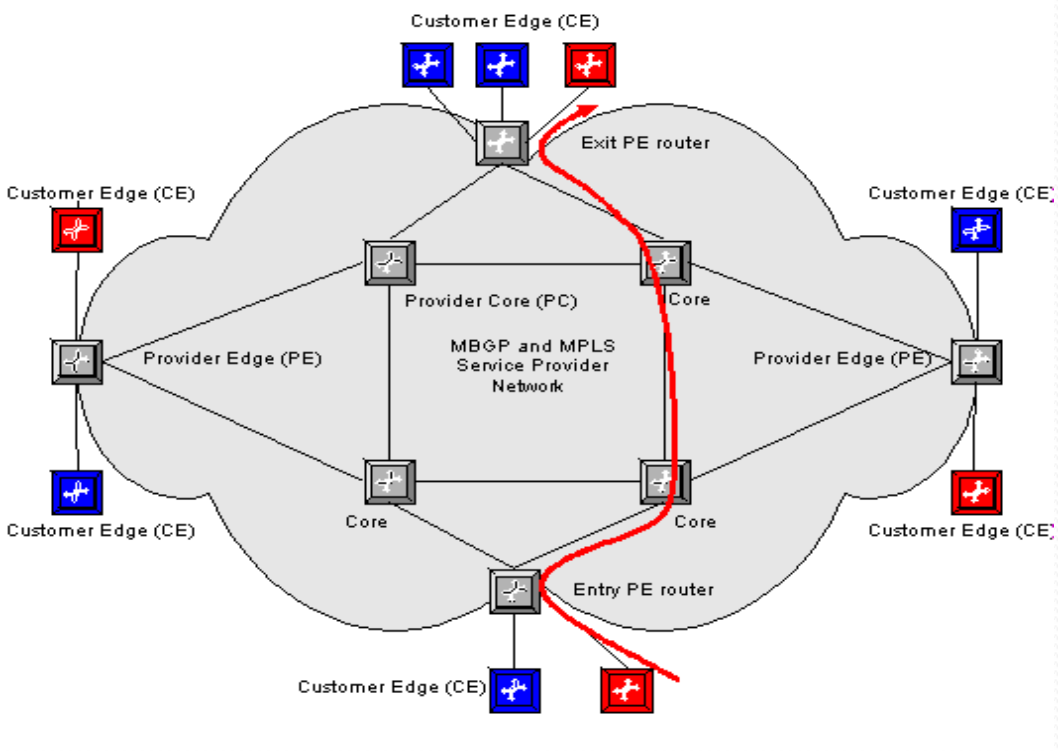
Figure 2: MPLS Packet Forwarding



• **Label stacks:** it is allowed to stack labels forming a sequence, so traffic with a same behavior is aggregated (FEC)

Topic 5: Corporate Networks: Switching Blocks.

- **MPLS-VPN:**
  - Combines MPLS and BGP to create an IP (L3) VPN (Virtual Private Network)



- **CE:** Customer Edge equipment
- **PE:** Provider Edge equipment
- **P/PC:** Provider (Core) router

- **MPLS-VPN:**
  - **VPN-IPv4 addresses (12B):** address that identifies the VPN and is composed by a **"Route Distinguisher - RD"** (8 bytes) and an IP@ network → 8B of RD + 4B of @IP = 12B of identifier (e.g. **VPN 146:10.1.1.0** is different of **VPN 37:10.1.1.0**)
  - **VPN-IPv4@ should be globally unique** → RD should be globally unique.

RD= 2B (Type Field) + 2B (Admin Field) + 4B (Assigned # Field)

- **Type 0:** The administrator field must contain an AS number (using private AS numbers is discouraged). The assigned field given by the ISP.

RD= 2B (Type Field) + 4B (Admin Field) + 2B (Assigned # Field)

- **Type 1:** The administrator field must contain an IP address (using private IP address space is discouraged). The assigned field given by the ISP.
- **Type 2:** The administrator field must contain a 4-octet AS number (using private AS numbers is discouraged). The assigned field given by the ISP

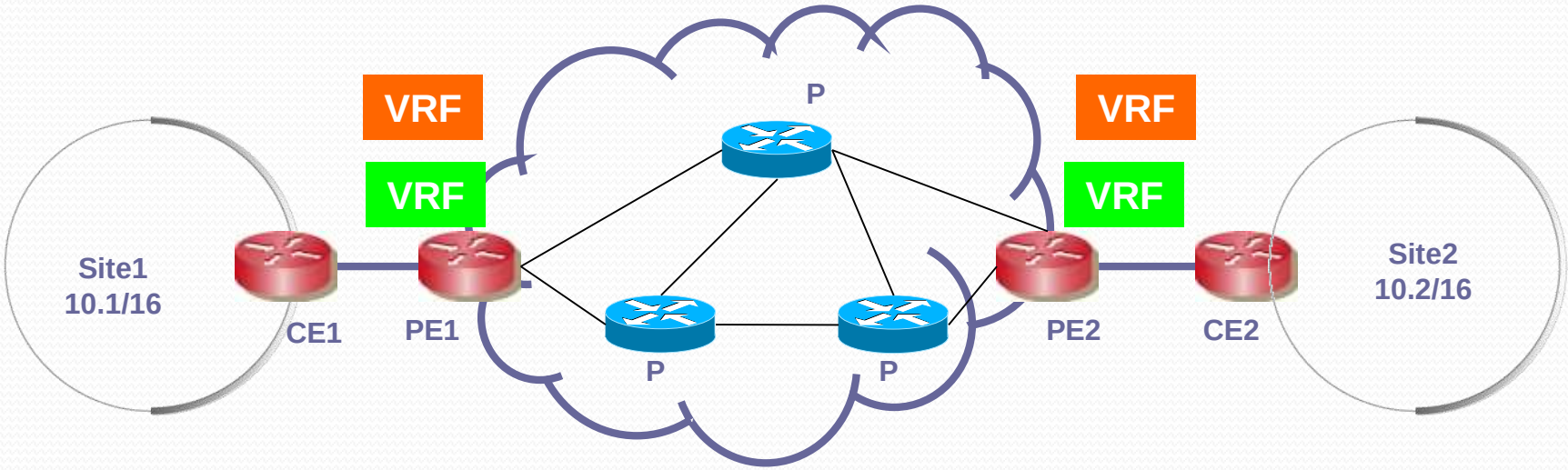
- **CE:** Customer Edge equipment
  - Router that give access to the provider
  - Uses E-BGP to announce/learn routes
- **PE:** Provider Edge equipment
  - Exchange routes via BGP with CE
  - Maintains a Virtual Routing and Forwarding (**VRF**) table for each of the connected sites
    - **VRF** defines the VPN membership of a customer site attached to a PE router
  - Exchange VRF information with other PE using **MBGP**
    - **MBGP (Multi-protocol BGP):** BGP version that carries VPN-IPv4 addresses traversing an ISP and that allows to a PE router learn routes from other PE router
  - Acts as ingress and egress point for the Label Switched Paths (LSP): inserts and removes MPLS labels

- **P/PC:** Provider (Core) router
  - Any router that is not attached to a CE
  - Forward traffic between PE routers acting as Label-Switched Routers (LSRs)
  - Only need to know routing information to reach PE routers
  - Required to support LDP at a minimum

- **How to exchange packets between two CE ?**
  - Use BGP to export routes
  - Use **Extended Communities** (8-byte) to filter and associate BGP traffic to a VRF (Virtual Router and Forwarding)
  - VRF are tables associated to PE routers
  - Use MPLS to switch traffic in the Internet core

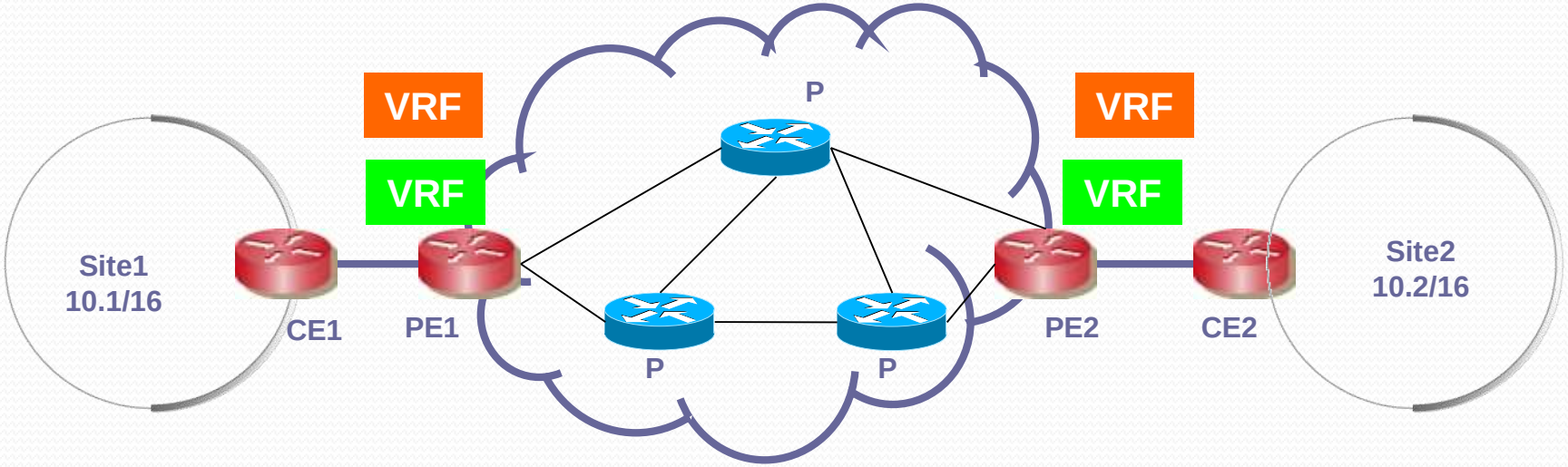
MPLS-VPN:

- Site 1 and Site 2 share the green VRF
- CE1 announces network 10.1/16 via E-BGP to PE1
- PE1 adds 10.1/16 to the green VRF using the RD identifier (Router Distinguished). PE1 determines that 10.1/16 has to be attached to the green VRF using the physical receiving port
- PE1 exports via I-BGP (using MBPG) the route defined by the VPN-IPv4@:
  - **Associates the route to the green VRF adding an extended communities** (8B=RD)
  - **Selects a MPLS label as "site-id" and adds it to the route** (e.g., label 353)
  - **Selects its loopback IP address as next-hop**



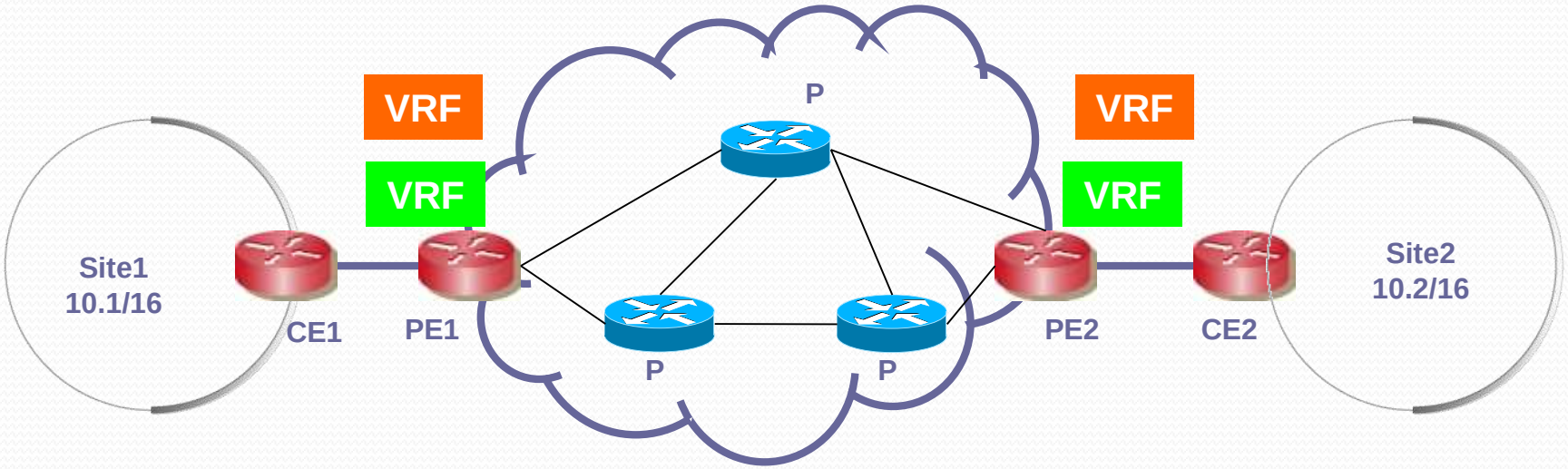
MPLS-VPN:

- **PE2 receives the VPN-IPv4@ route for 10.1/16 from PE1 and performs route-map filtering**
  - Extended BGP communities are inspected to determine if the route pertains to a known VRF
- PE2 accepts the route because it pertains to Green VRF
  - VRF determined based on extended community
  - PE2 records label 353 to use for forwarding customer packets to site 1
- PE2 also announces local Green VRF routing information to PE1



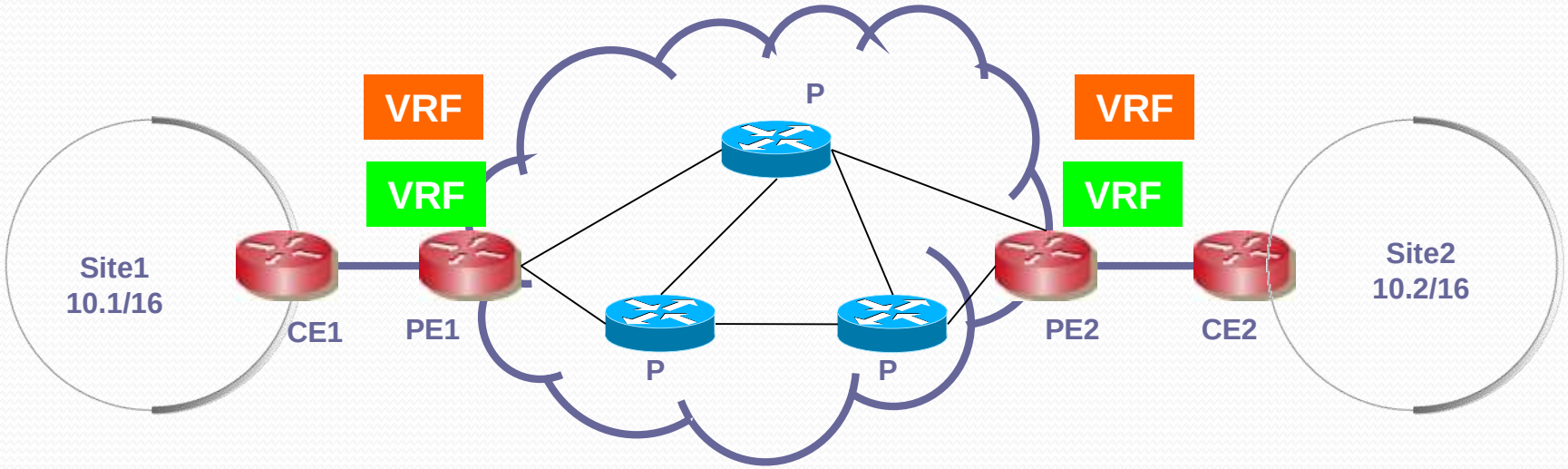
MPLS-VPN:

- Use MPLS to forward traffic. For that a MPLS route between PE1 and PE2 must be established
  - Created by PE2 when it learns the route announced by PE1 (and viceversa)
- E.g., label 979 propagated to all Ps in the path between PE1 and PE2
  - Different than "site label“ 353
- There are two MPLS lablels
  - **LSP tag:** Label 979 is used to forward packets in the MPLS network from PE1 to PE2
  - **Site-tag:** Label 353 is used to identify who is the Remote site (i.e., site 1)



MPLS-VPN:

- Host 10.2.1.1 in site2 communicates with host 10.1.1.1 in site1
- PE2 determines VRF based on receiving port, and looks up 10.1.1.1, obtaining:
  - MPLS Tag associated to remote site: 353
  - Next-hop of 10.1/16 route: PE1's loopback
  - MPLS Tag associated to reach PE1: 979
- "LSP tag" used to forward packets over the appropriate LSP
- "Site tag" used by remote PE to forward packets to the appropriate port



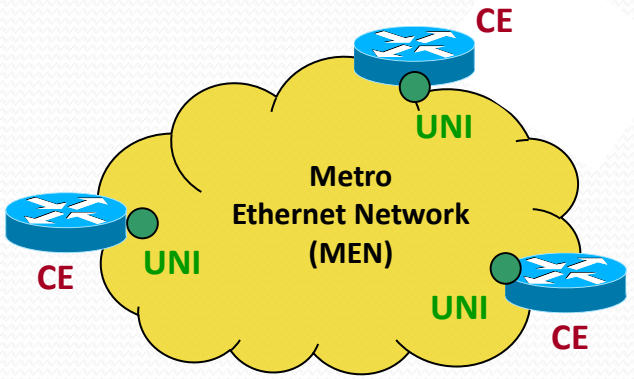
Metro Ethernet:

- **Goal**: Ethernet in the MAN (Metropolitan Area Network)

- **Interconnect Ethernet switches and routers with the operator or ISP to transport any service using broadband VPN** (10/100/1000/10000 Mb/s)
  - In the last years L2 VPN were over FR or ATM
  - Metro Ethernet may switch based in VLAN traffic (same way that FR does with the DLCI or ATM with the VC/VP)
- Solutions
  - Optical Ethernet or Native Ethernet
  - EFM Ethernet over the First Mile or IEEE802.3ah
  - Ethernet over MPLS (ISPs)
  - EoS: Ethernet over SDH
  - EoW: Ethernet over WDM (Wavelength Division Multiplexing)

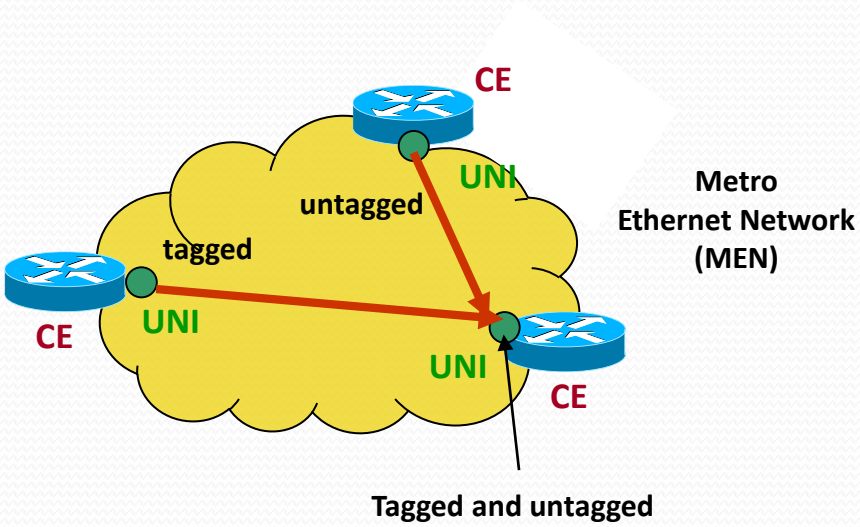
Topic 5: Corporate Networks: Switching Blocks.

- When an ISP offers a Metro Ethernet service, **two logical entities called UNI sited in the CE transports frames through a logical channel called EVC,**
  - **CE (Customer Equipment):** switch (with IEEE 802.1Q – VLAN support) or router
  - **UNI (User Network Interface):** IEEE 802.3 PHY/MAC with 10/100/1000/10000 Mb/s and QoS support
  - **MEN (Metro Ethernet Network):** the operator can use any kind of L2 technology o L3 (FR, ATM, SONET/SDH, WDM, MPLS, etc)
  - **EVC (Ethernet Virtual Connection):** logical association between one or more UNI that transports frames from the origin UNI towards one (point-to-point) or more (point-to-multipoint) destination UNIs (allowing then the creation of a L2 VPN) → equivalent to a VLAN,
- Multiplexing services: a UNI associated to more than one EVC
- In Metro Ethernet there is **three types of services**:
  - **Ethernet Line** (point-to-point)
  - **Ethernet LAN** (multipoint-to-multipoint)
  - **Ethernet Tree** (point-to-multipoint)

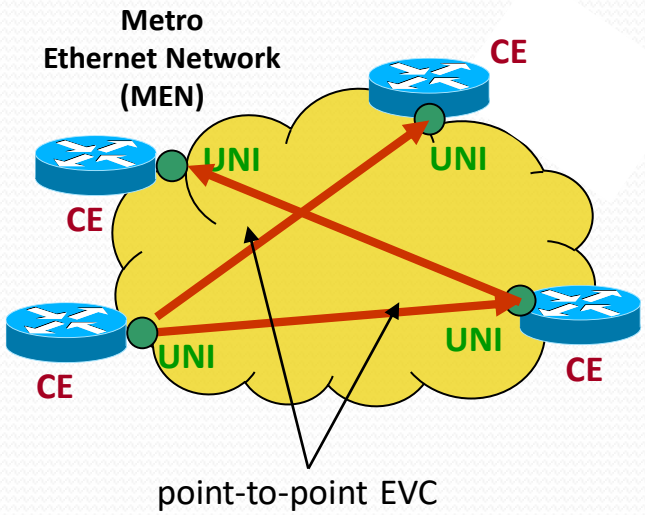


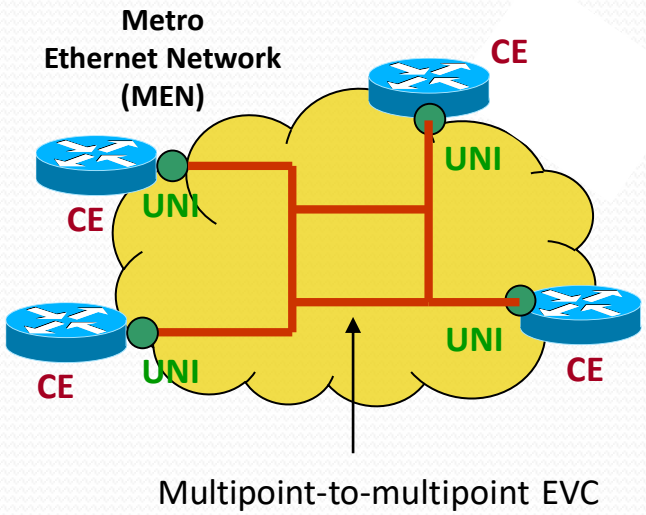
VLAN-tag support:

- The services can support only 802.1Q tagged frames, only not tagged frames or both of them
- The user may mark frames with a label and the provider may add a new one to tag the traffic of other users
  - CE-VLAN ID is the tagging performed by the user at the CE. This tagging is different to the provider's tagging



- **Metro Ethernet services:**
  - **Point-to-point services (E-Line):**
  - **Multipoint-to-multipoint services (E-LAN):**





The **services** have attributes that represent them:

- **UNI attributes**: Tx media, data rate, VLAN support, multiplexing, …
- **EVC attributes**: traffic parameters (CIR, PIR, EIR, CBS), QoS parameters (delay, jitter, losses), Service Class parameters (VLAN-ID), unicast delivery, multicast delivery, etc

- **Ether-Line (E-Line) service**
  - Can operate with both dedicated/switched bandwidth and is a **point-to-point architecture,**
  - **EPL (Ethernet Private Line)**
    - Is a point-to-point EVC where the user defines CIR, CBS, EIR, EBS, …
    - Can be seen as pure point-to-point where the EPL supports a **unique** EVC between two UNI's
    - Since there is only one EVC, the user doesn't see the "VLAN tag"
  - **EVPL (Ethernet Virtual Private Line)**
    - Allows service multiplexing, thus, the point-to-point supports several EVC between two UNI's
    - Exists a CIR and EIR and a metric for SLA´s support
    - Very similar to Frame Relay or ATM (where VC are multiplexed)
    - Since there are several EVC, the user has to tag packets with a "VLAN tag" per EVC

- **Ether-LAN (E-LAN) service**
  - Can operate with both dedicated/switched bandwidth in a **multipoint-to-multipoint architecture**,
  - **EPLan** (Ethernet Private LAN)
    - Multipoint-to-multipoint connectivity between two or more UNI´s
    - Each UNI is only attached to one EVC (if the user wants other EVC he has to activate other UNI)
    - Since there is only one EVC, the user will not see the “VLAN tag”
  - **EVPLan** (Ethernet Virtual Private LAN)
    - Same as VPLS (Virtual Private Lan Service), TLS (Transparent Lan Service) or VPSN (Virtual Private Switched Network)
    - Multipoint-to-multipoint connectivity between two or more UNI´s, with multiple EVC’s support, the user has to tag packets with a “VLAN tag” per EVC

- # Ether-Tree (E-Tree) service
  - **Point-to-multipoint connectivity** with dedicated bandwidth and tree topology
  - It is not a any-to-any communication since there is a root UNI