

MPLS Traffic Engineering

PacNOG20 July 3, 2017. Suva, Fiji.

Jessica Wei

Presenter

Jessica Wei

Training Officer, APNIC

After graduating from China's Huazhong University of Science and Technology in 2007 with a degree in electronic engineering, Bei (whose nickname is Jessica) joined Huawei as a network training officer.

Over the next six years, she provided Huawei technical training on LAN/WAN systems, broadband access, IP core and IP mobile backhaul networks as well as working on technical training course design and the development of IP training materials. At the Huawei training center in China she provided technical training to engineers and administrators from more than 15 nations including Viet Nam, Papua New Guinea, Thailand, Pakistan and Bangladesh. She has also travelled to Bangladesh, Venezuela, Colombia, Egypt, Malaysia, Australia, Thailand, Indonesia and Singapore to provide training.



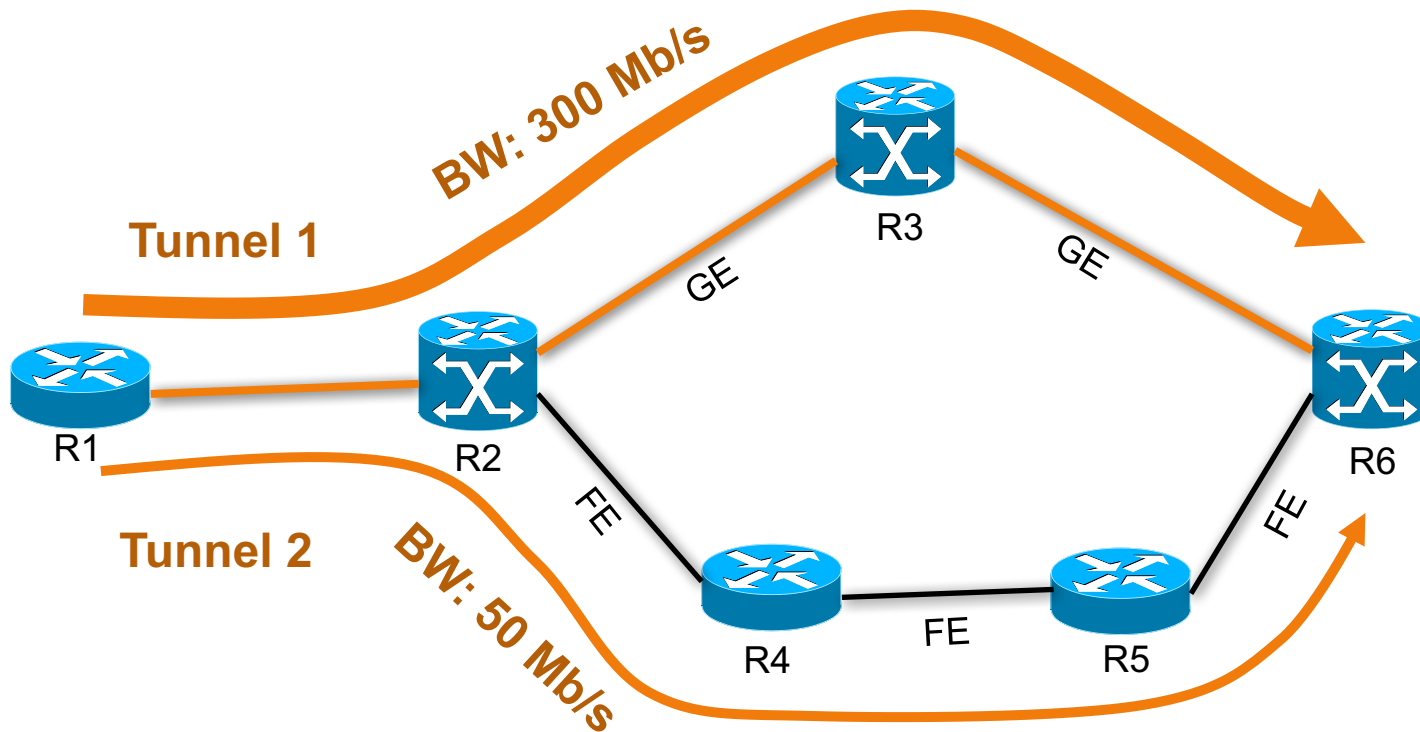
Contact:

Email: jwei@apnic.net

Why MPLS Traffic Engineering?

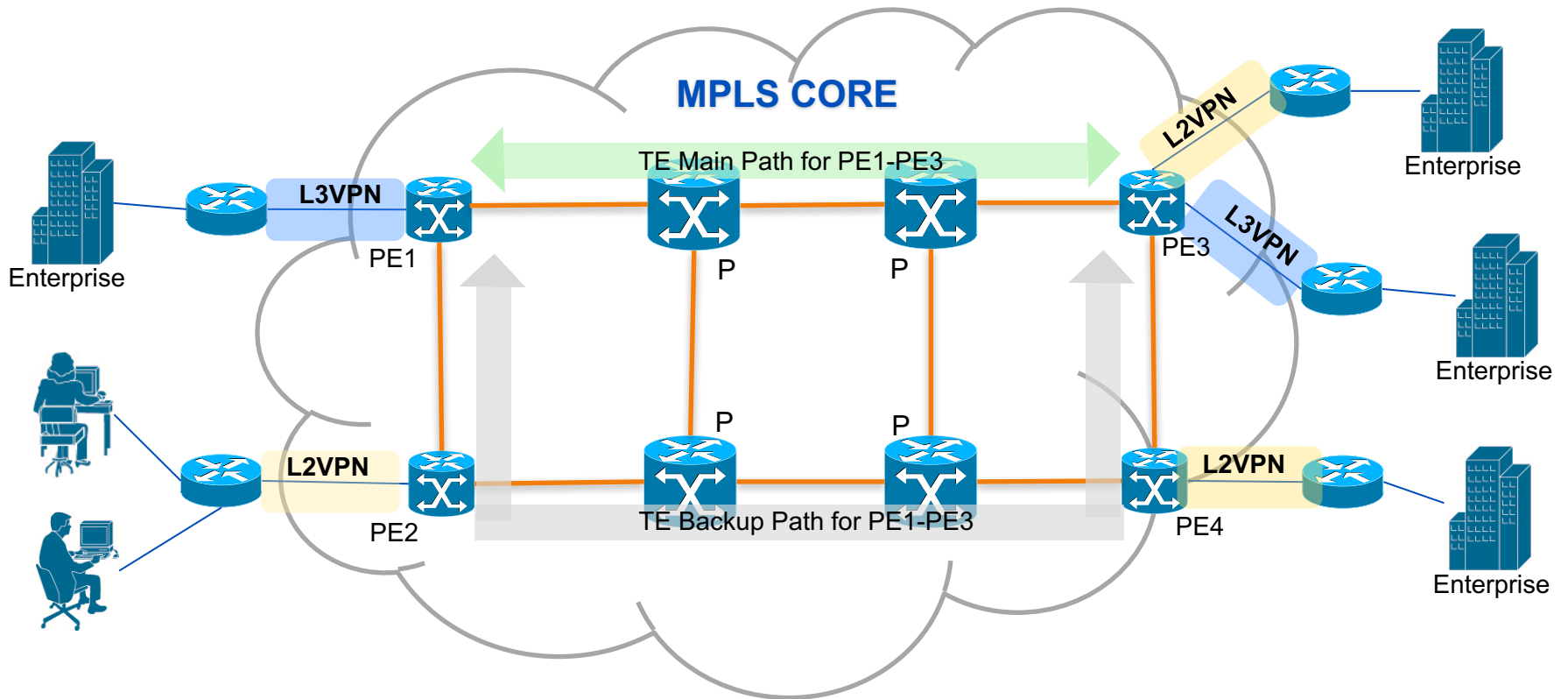
- Handling unexpected congestion
- Better utilization of available bandwidth
- Route around failed links/nodes
- Capacity planning

Optimal Traffic Engineering

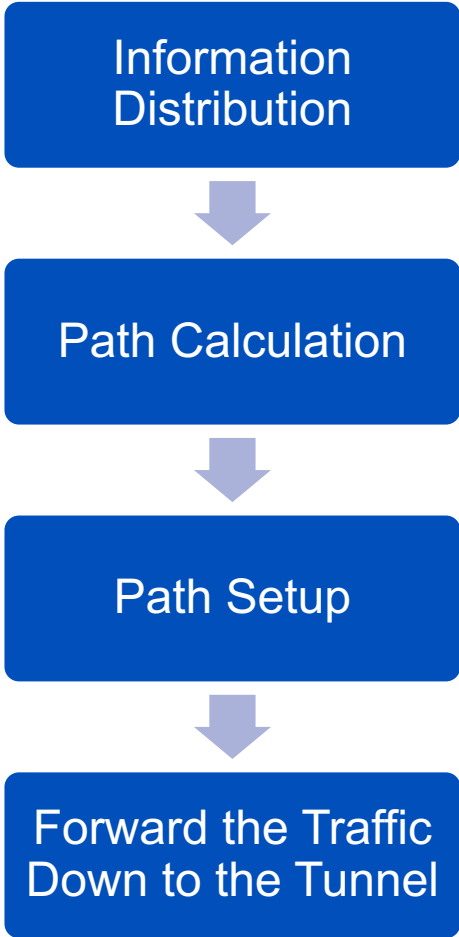


IP TE	MPLS TE
Shortest path	Determines the path at the source based on additional parameters (available resources and constraints, etc.)
Equal cost load balancing	Load sharing across unequal paths can be achieved.

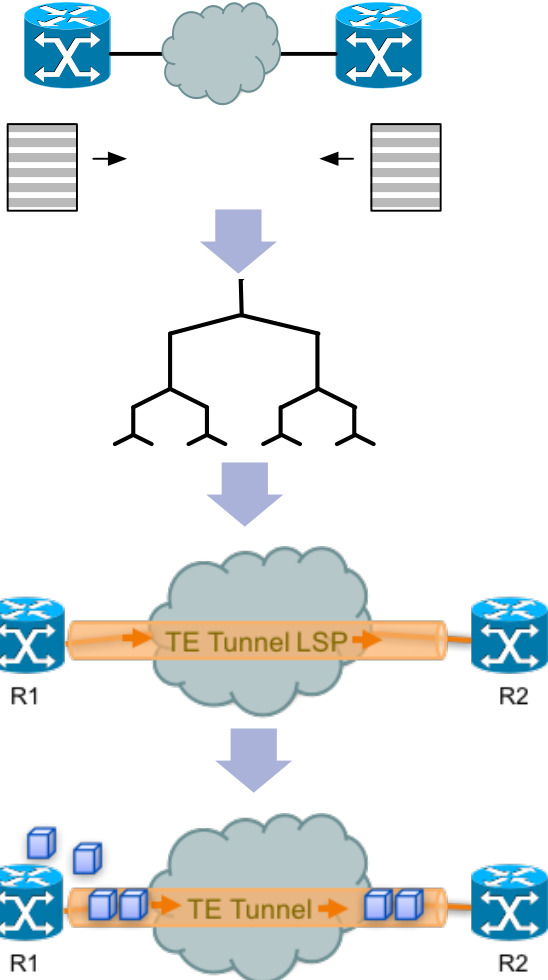
MPLS Application Scenario



How MPLS TE Works



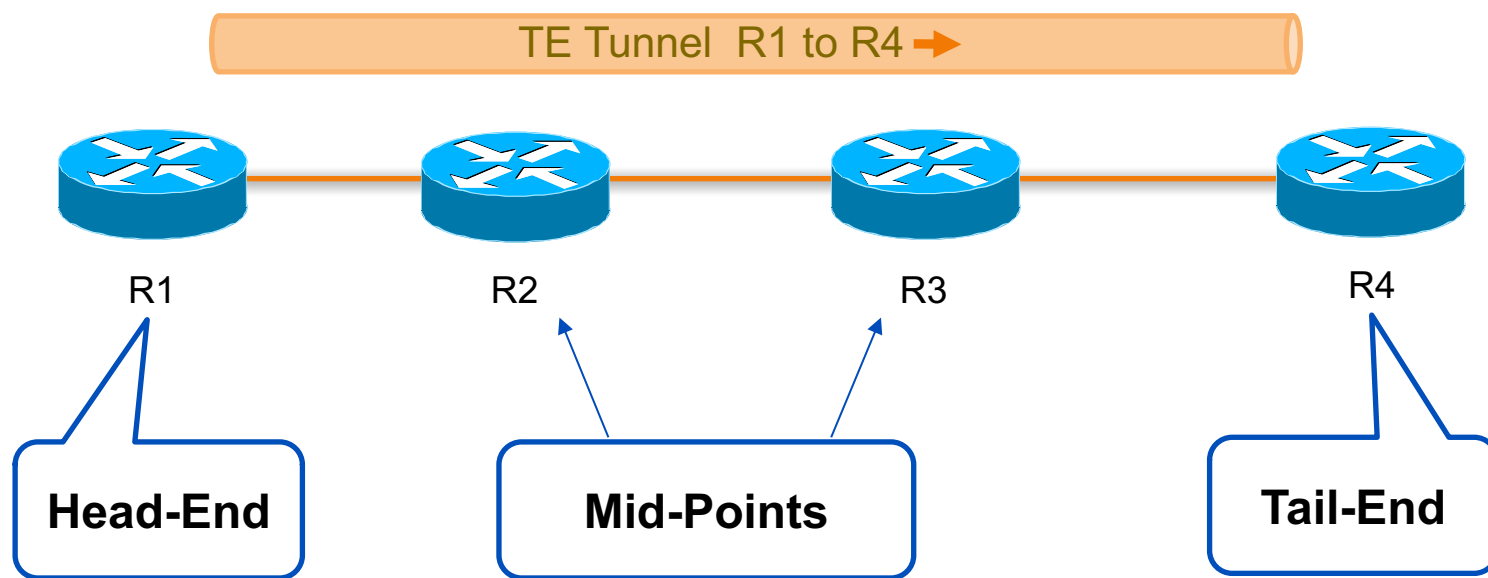
- What is the information?
- Dynamically
- Manually
- RSVP-TE
- (CR-LDP)
- Autoroute
- Static
- Policy



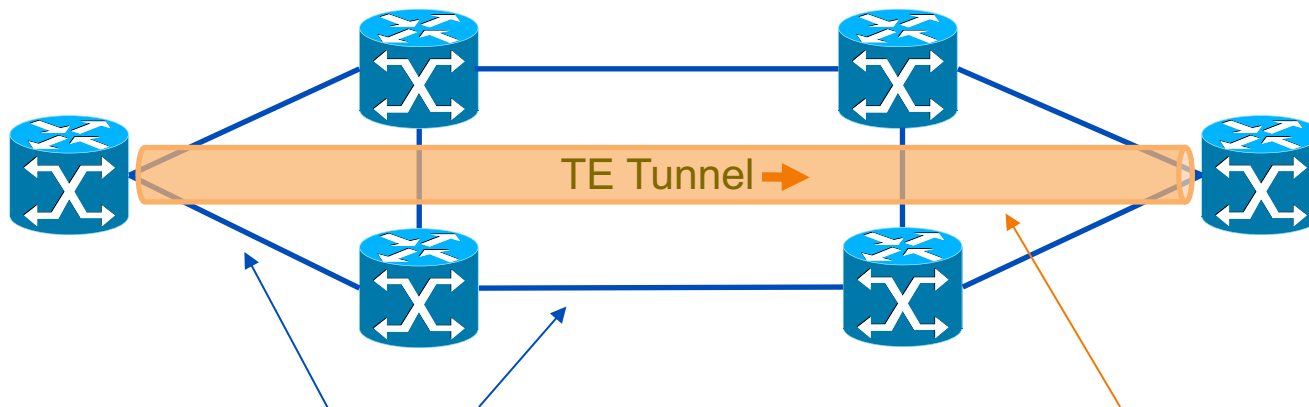
Terminology—Head, Tail, LSP

Upstream

Downstream



Attributes



Link Attributes

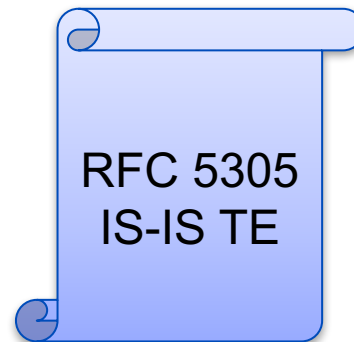
- Available Bandwidth
- Attribute flags (Link Affinity)
- Administrative weight (TE-specific link metric)

Tunnel Attributes

- Tunnel Required Bandwidth
- Tunnel Affinity & Mask
- Priority

Link-State Protocol Extensions/ IGP Flooding

- TE finds paths other than shortest-cost. To do this, TE must have more info than just per-link cost
- OSPF and IS-IS have been extended to carry additional information
 - Physical bandwidth
 - RSVP configured bandwidth
 - RSVP available bandwidth
 - Link TE metric
 - Link affinity

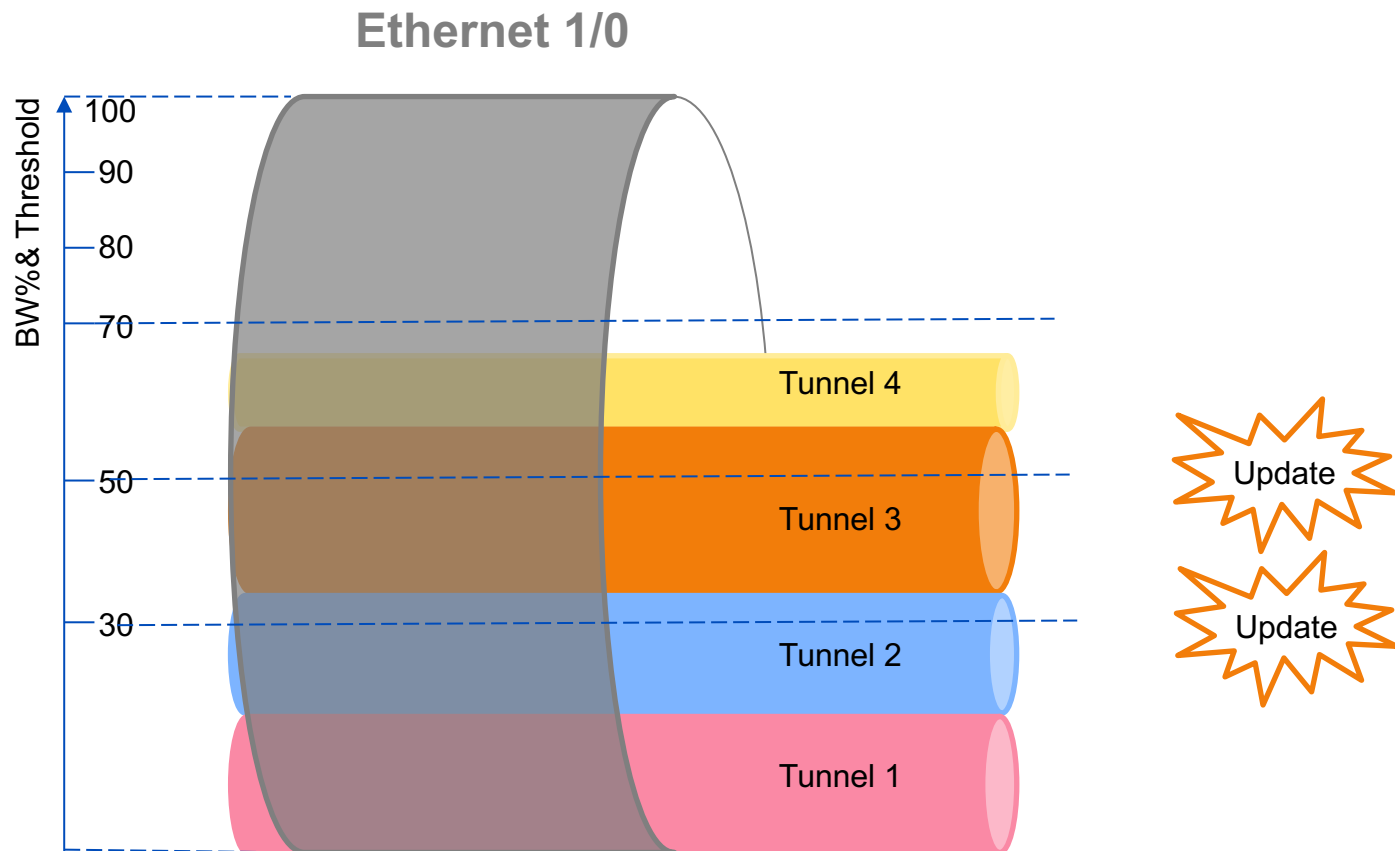


When to Flood the Information

- When a link goes up or down
- When a link's configuration is changed
- Periodically reflood the router's IGP information
- When link bandwidth changes **significantly**

Bandwidth Significant Change

- Each time a threshold is crossed, an update message is sent.



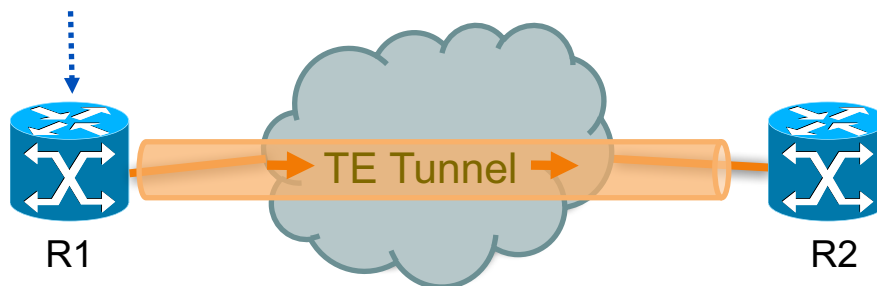
Tunnel Path Selection

- Tunnel has two path options
 1. Dynamic
 2. Explicit
- Path is a set of next-hop addresses (physical or loopbacks) to destination
- This set of next-hops is called Explicit Route Object (ERO)

Dynamic Path Option

- Dynamic = router calculates path using TE topology database
- Router will take best IGP path that meets BW requirements, also called CSPF algorithm.

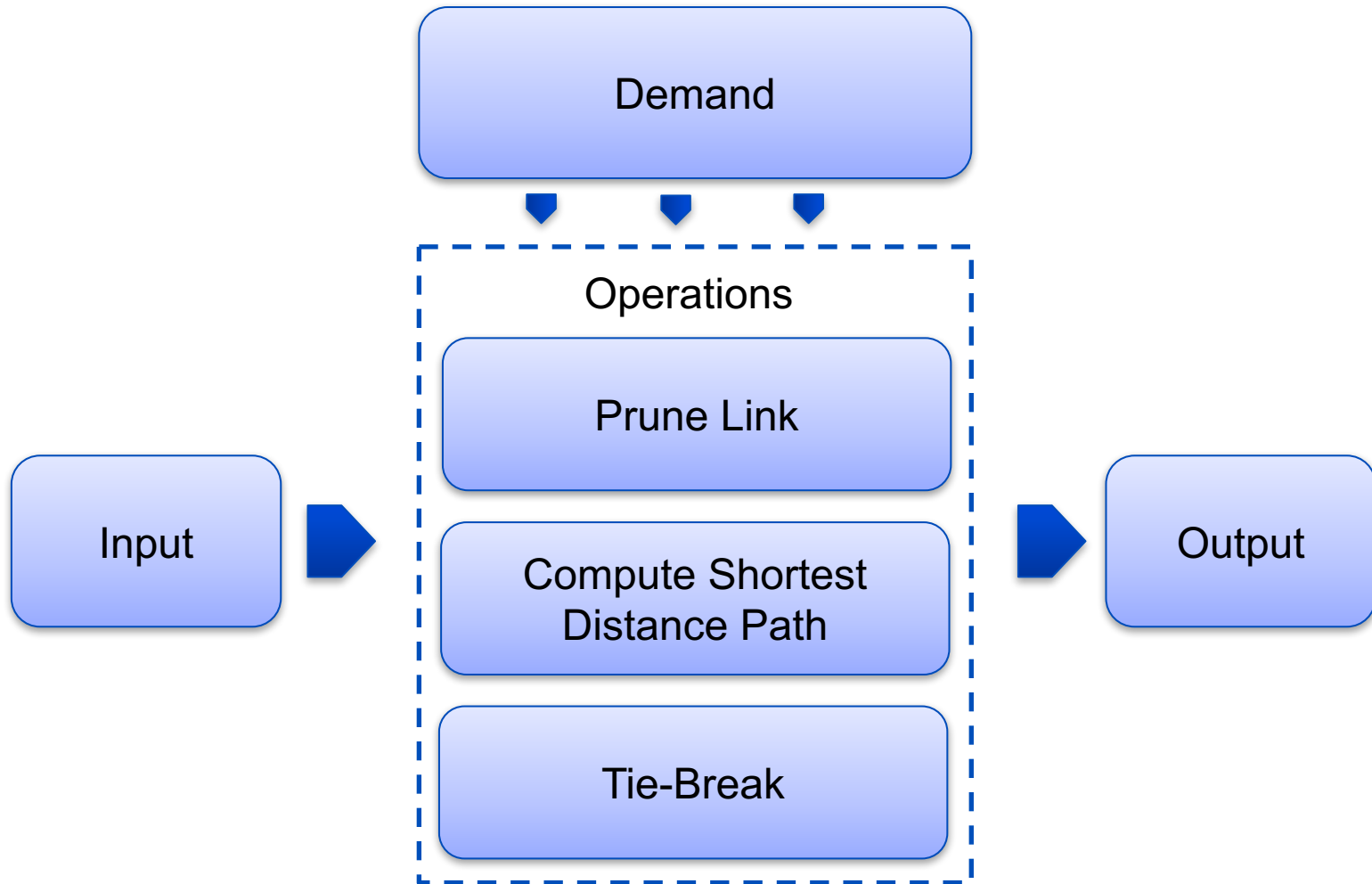
```
R1(config)# interface tunnel 1  
R1(config-if)# tunnel mpls traffic-eng path-option 10 dynamic
```



C-SPF

- Shortest-cost path is found that meets administrative constraints
- These constraints can be
 - bandwidth
 - link attribute (aka color, resource group)
 - priority
- The addition of constraints is what allows MPLS-TE to use paths other than *just* the shortest one

Path Computation

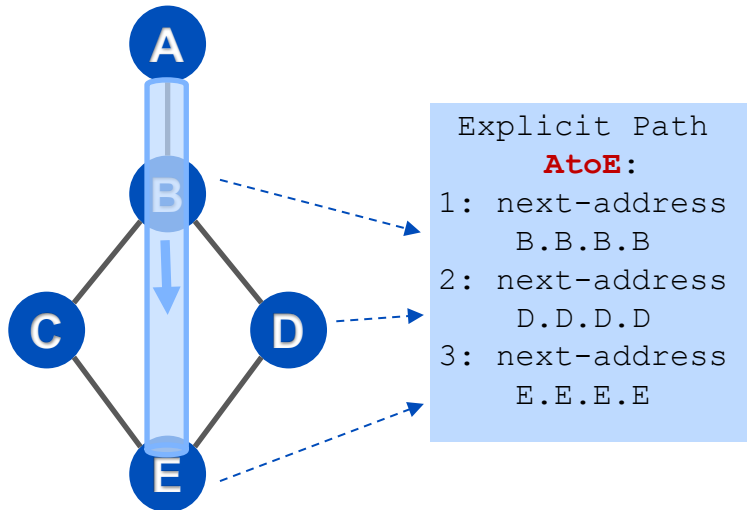


Explicit - Strict and Loose Path

- Paths are configured manually. Each hop is a physical interface or loopback.

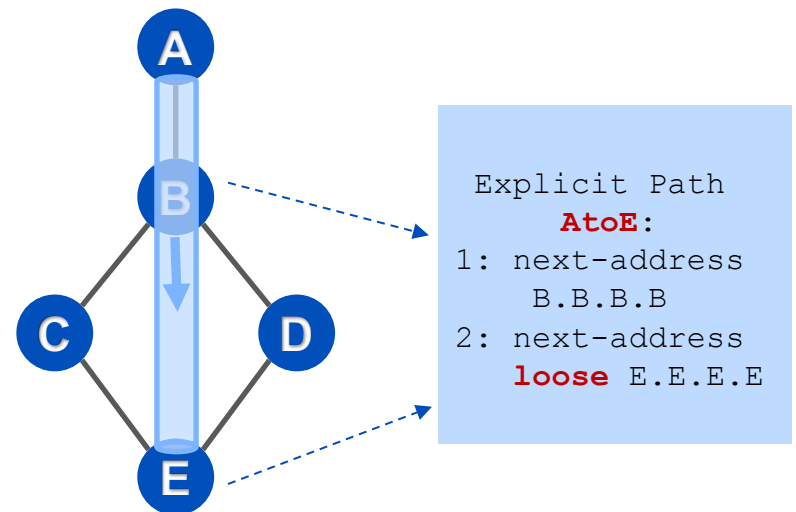
Strict Path

A network node and its preceding node in the path must be adjacent and directly connected.



Loose Path

A network node must be in the path but is not required to be directly connected to its preceding node.

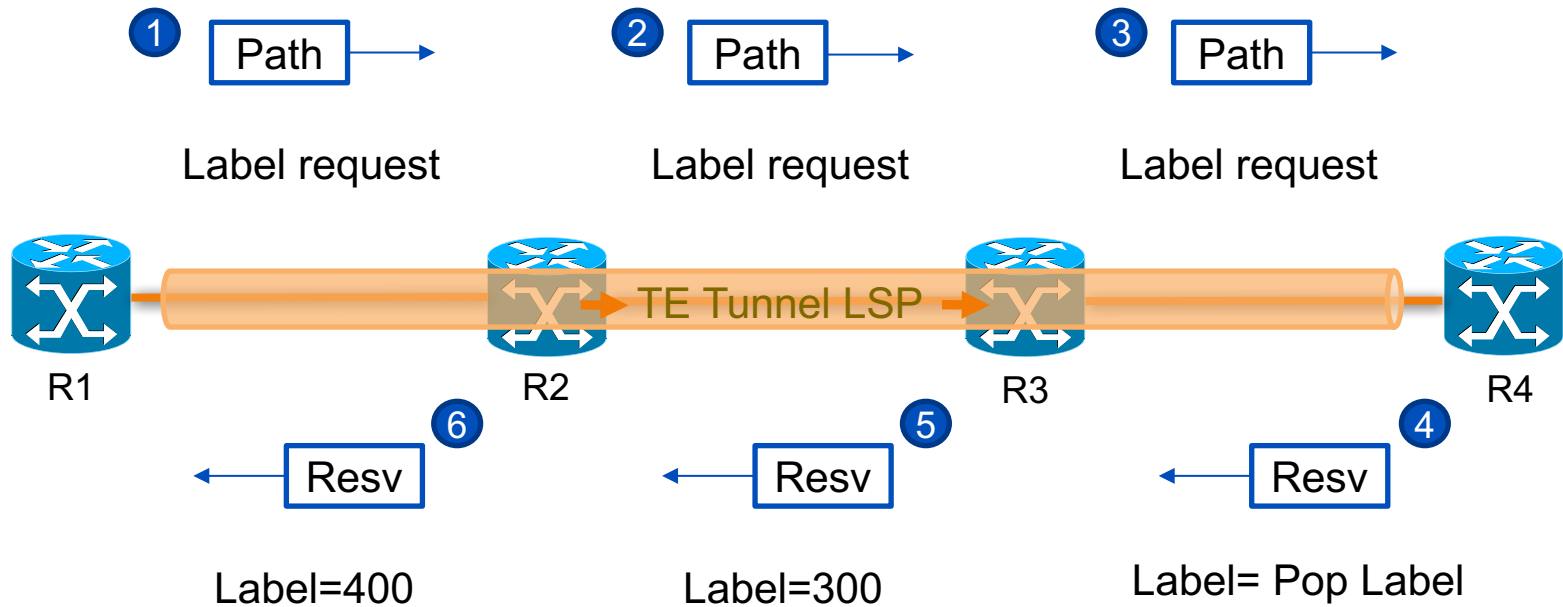


RSVP-TE

- After calculating the path, tunnel will be set up by using RSVP-TE.
- RSVP has three basic functions:
 - Path setup and maintenance
 - Path teardown
 - Error signalling

Setup of TE LSP

- In following topo, R1 will set up a TE tunnel from R1 to R4:



Routing Traffic Down a Tunnel

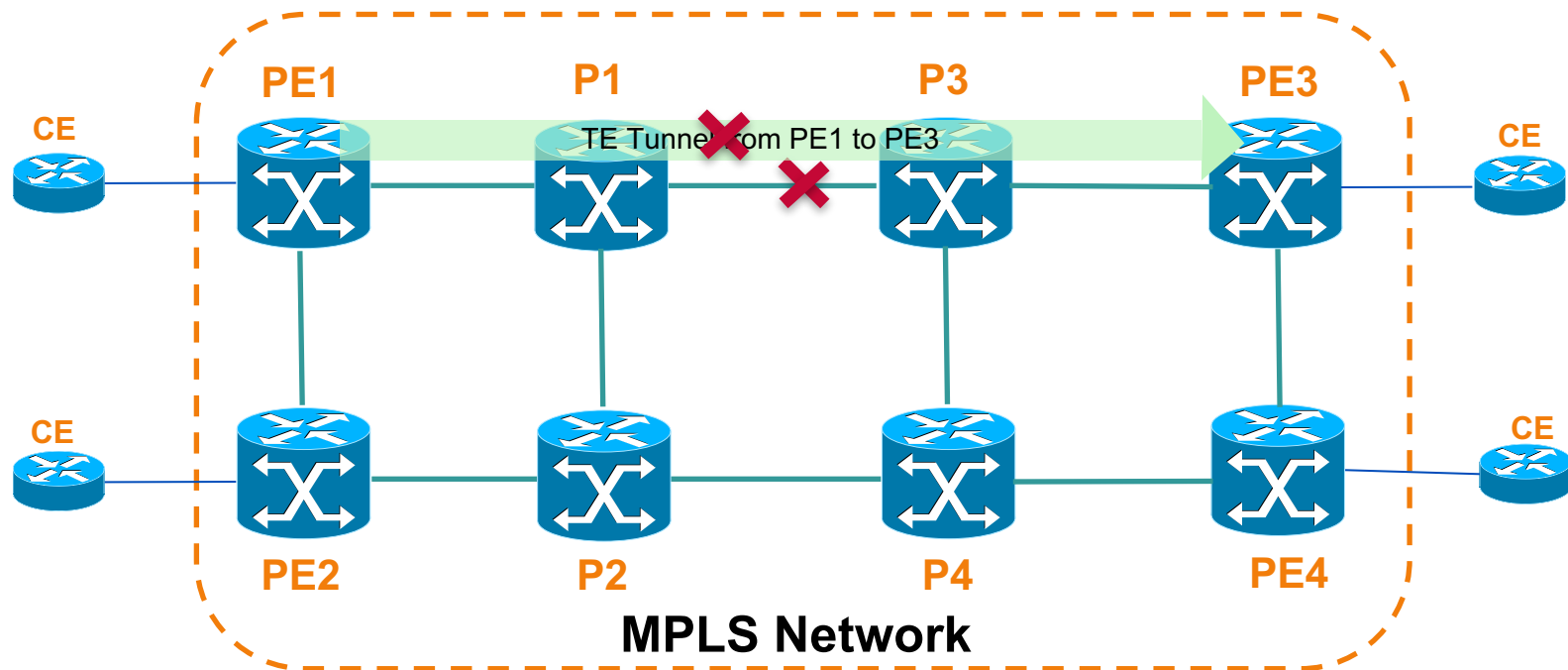
- Once the tunnel is established and operational, it's ready to forward data traffic.
- However, no traffic will enter the tunnel unless the IP routing tables and FIB tables are modified.
- How to get traffic down the tunnel?
 1. Static route
 2. Auto route
 3. Policy routing

MPLS TE Fast Re-Route

- Traffic engineering fast reroute (TE FRR) provides protection for MPLS TE tunnels.
- If a link or a node fails, FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or node, minimizing traffic loss.
 1. Link Protection
 2. Node Protection

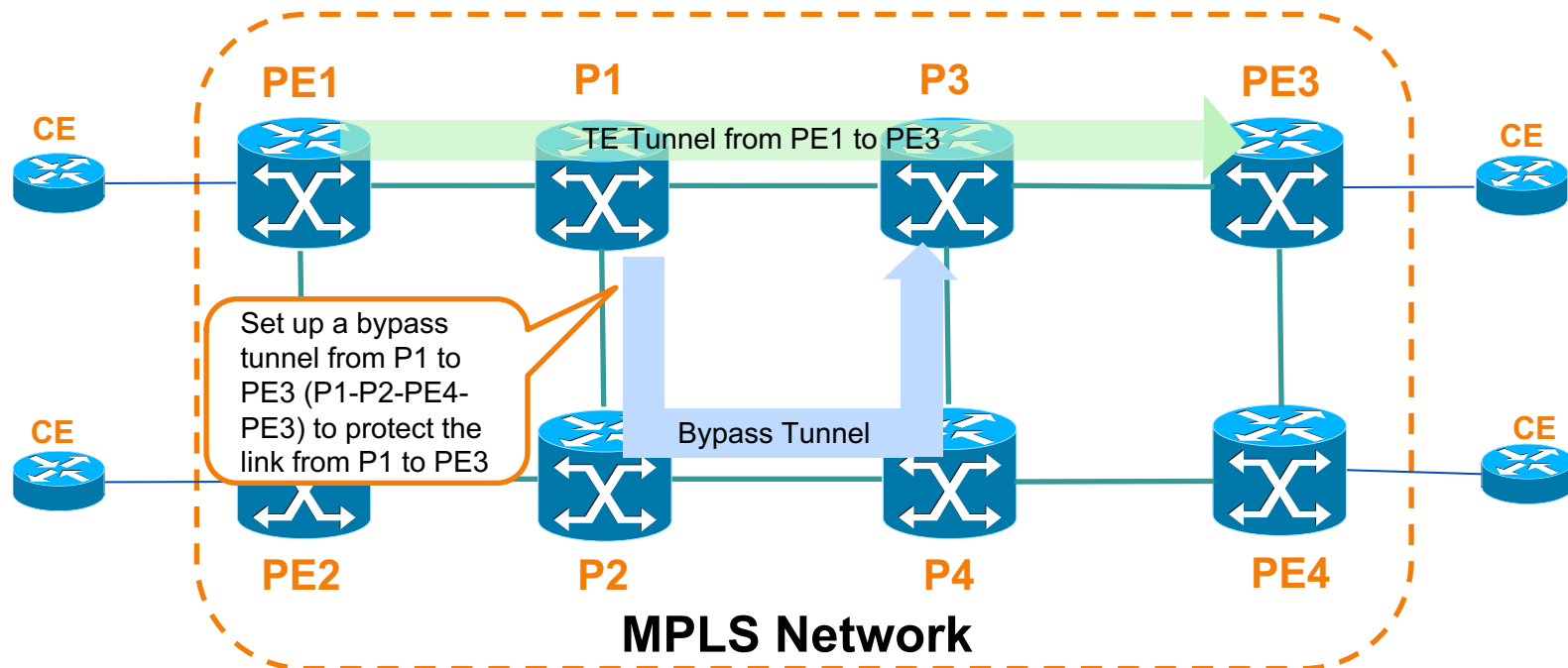
Link Failure

- If the link between P1 to P3 is down, the TE tunnel LSP will be torn down and take time to recompute a new path if autoroute.



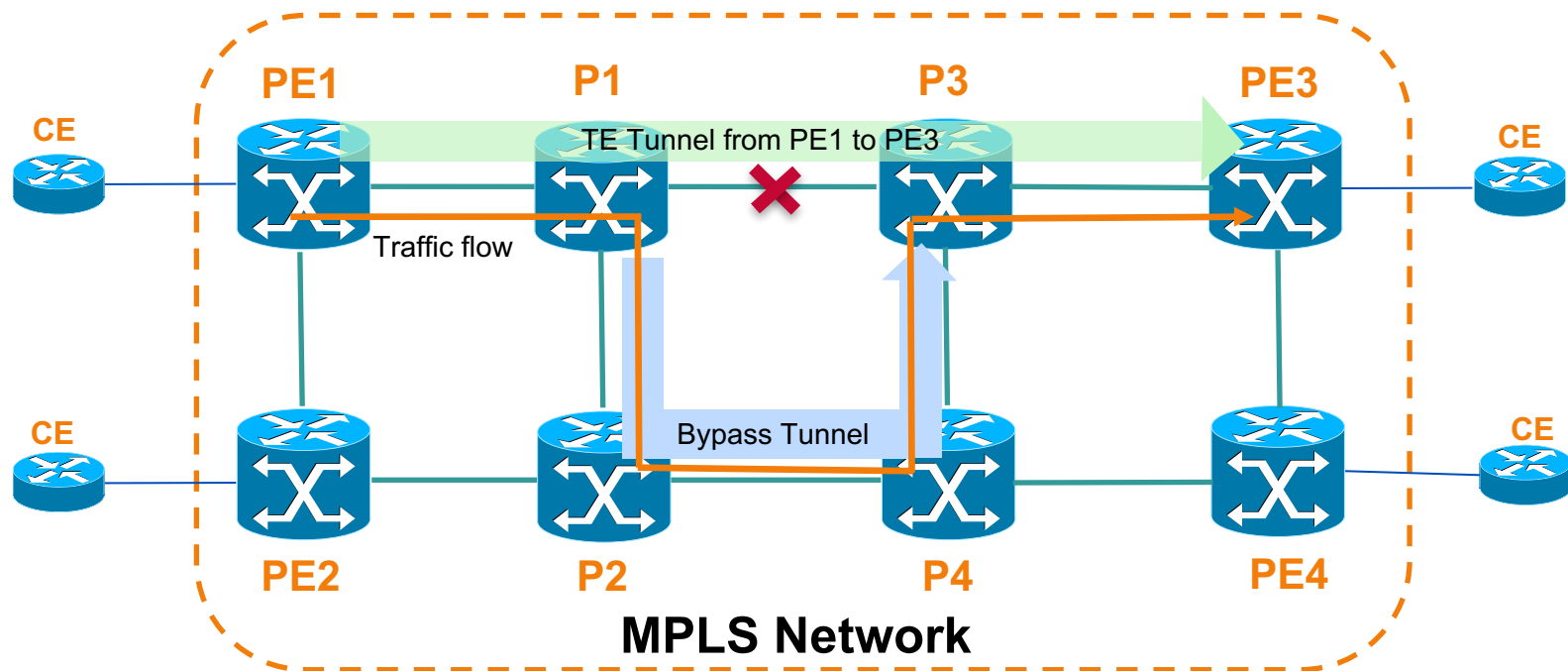
Fast Re-Route ---- Link Protection

- In link protection, the bypass tunnel has been set up to bypass only a single link of the LSP's path.



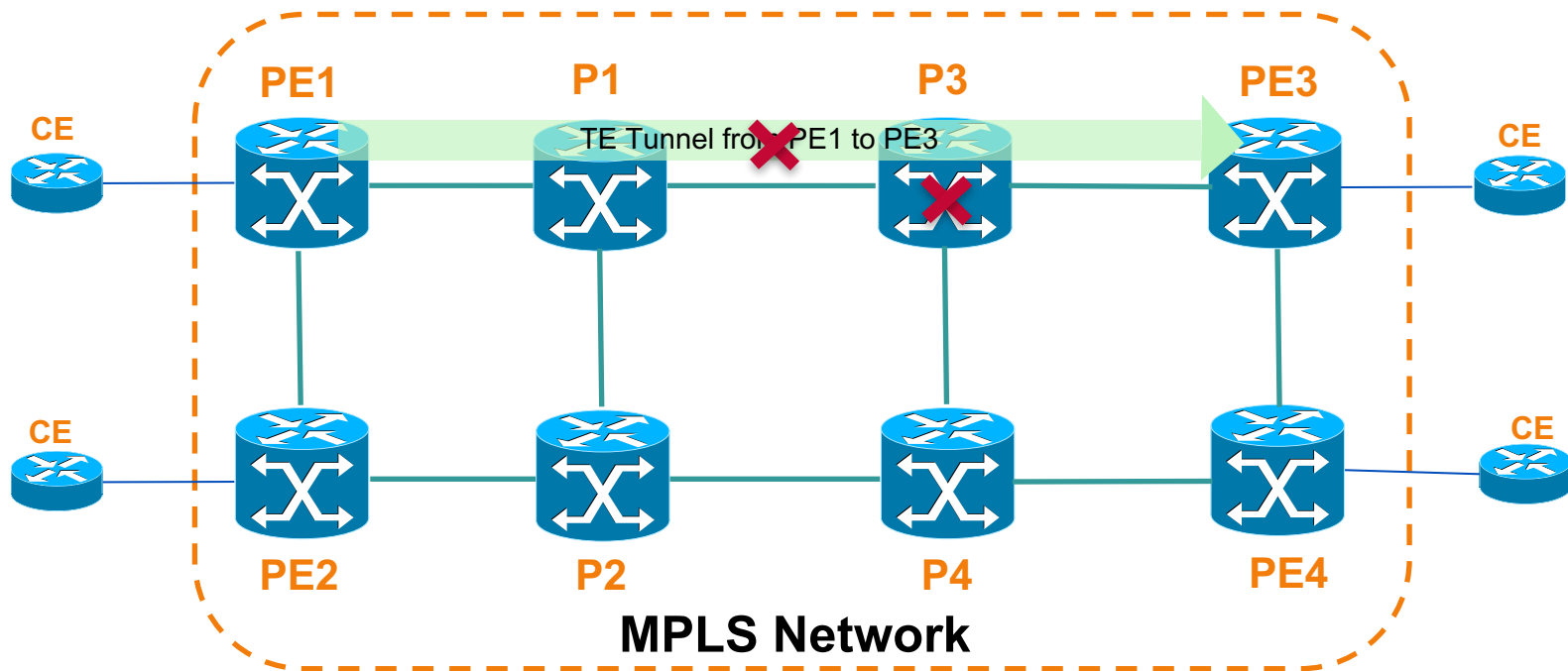
Fast Re-Route ---- Link Protection

- The bypass tunnel protects LSP if the protected link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link).



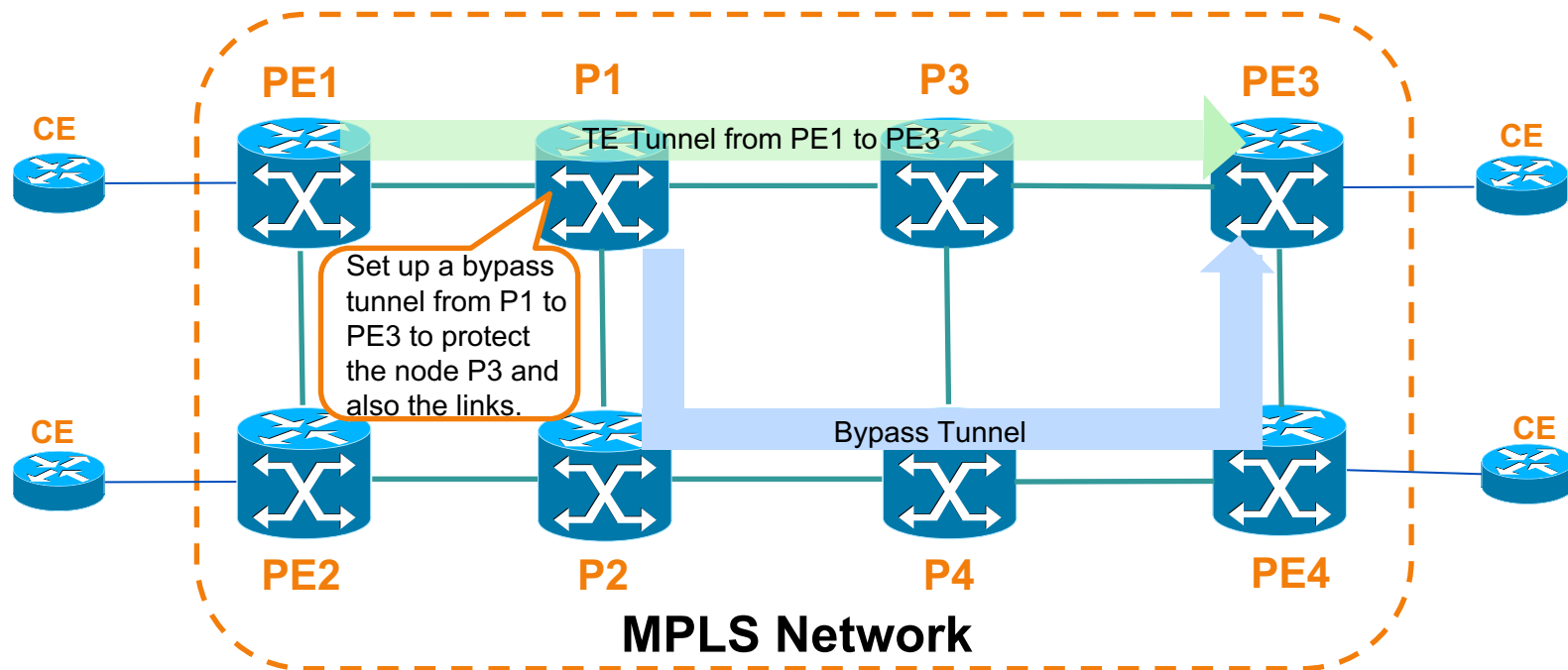
Node Failure

- If one node on the LSP fails, TE tunnel also will be torn down.



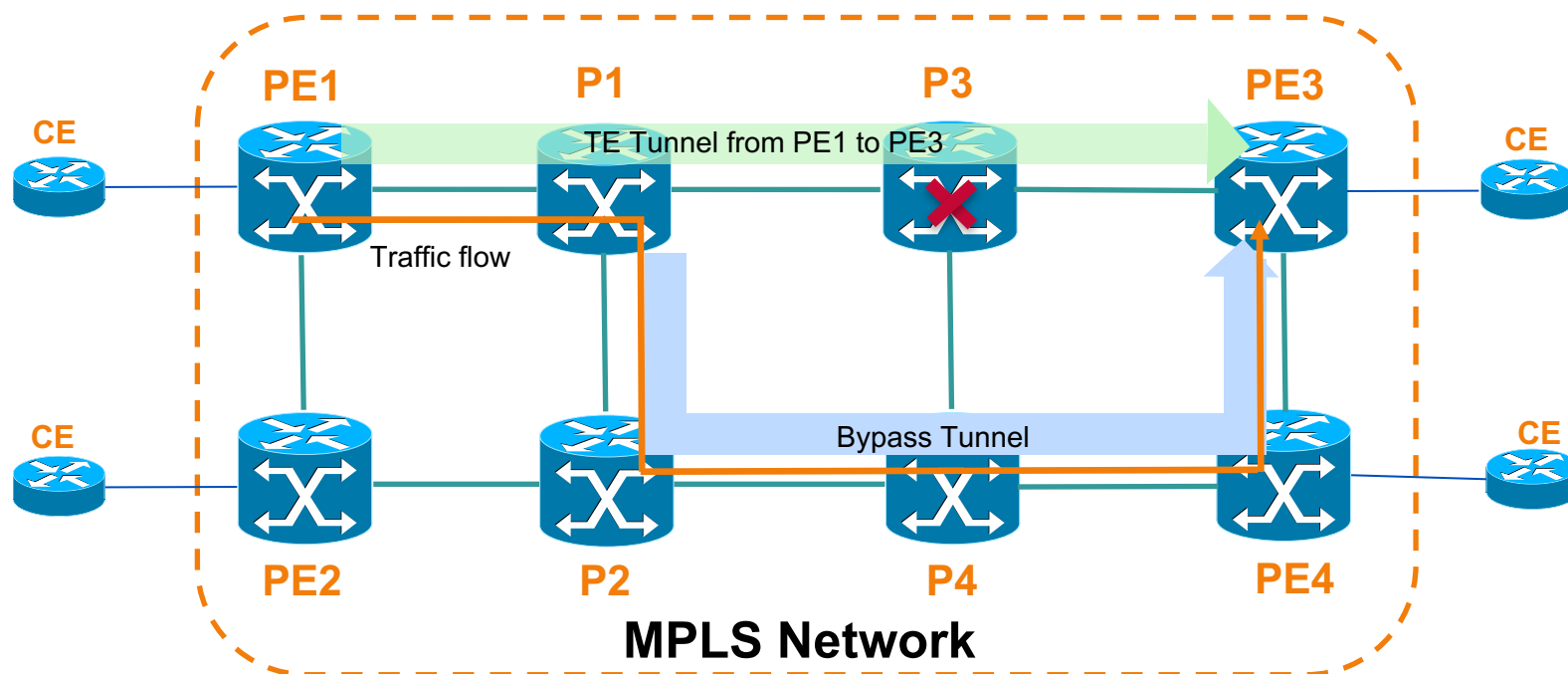
Fast Re-Route ---- Node Protection

- Node protection is similar to link protection in most ways, the backup tunnel is set up to bypass the protected node.

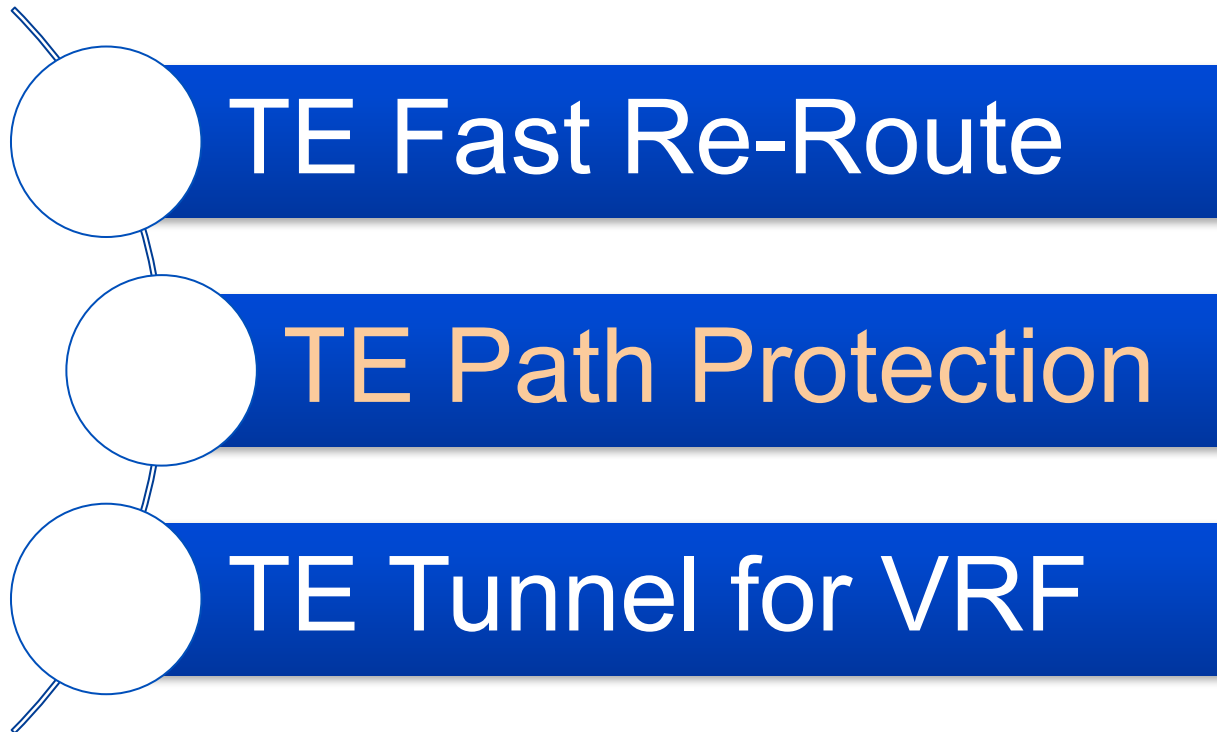


Fast Re-Route ---- Node Protection

- The backup tunnel can reroute the traffic to bypass the failure node.
- Backup tunnels also provide protection from link failures, because they bypass the failed link and the node.



MPLS TE Services

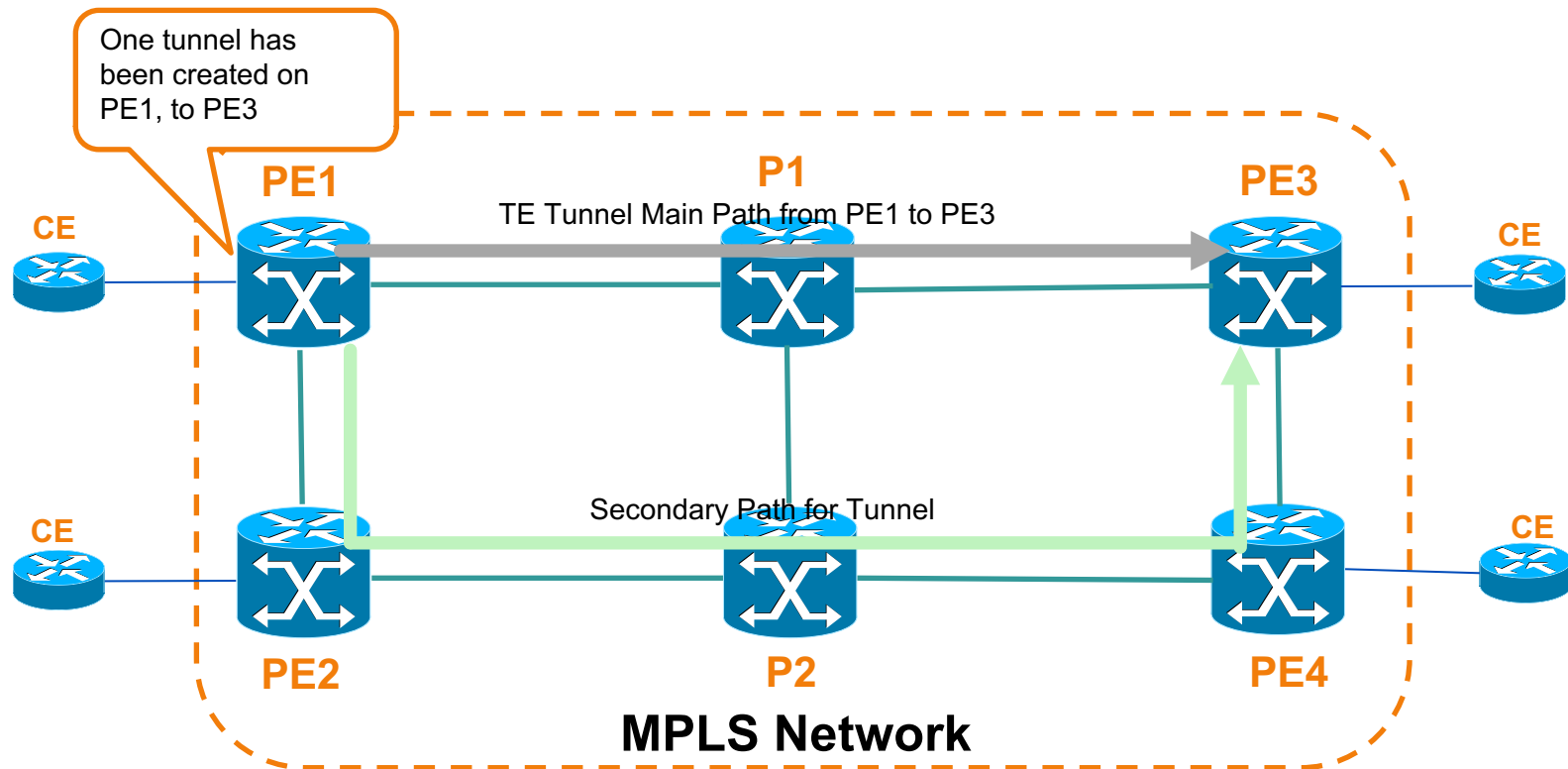


MPLS TE Path Protection

- **Path protection** provides an **end-to-end** failure recovery mechanism for MPLS TE tunnels.
- If the ingress node detects a failure of the primary LSP, it switches traffic to a backup LSP. After the primary LSP recovers, traffic switches back to the primary LSP.
- Path protection reduces the time required to recalculate a route in case of a failure within the MPLS tunnel.

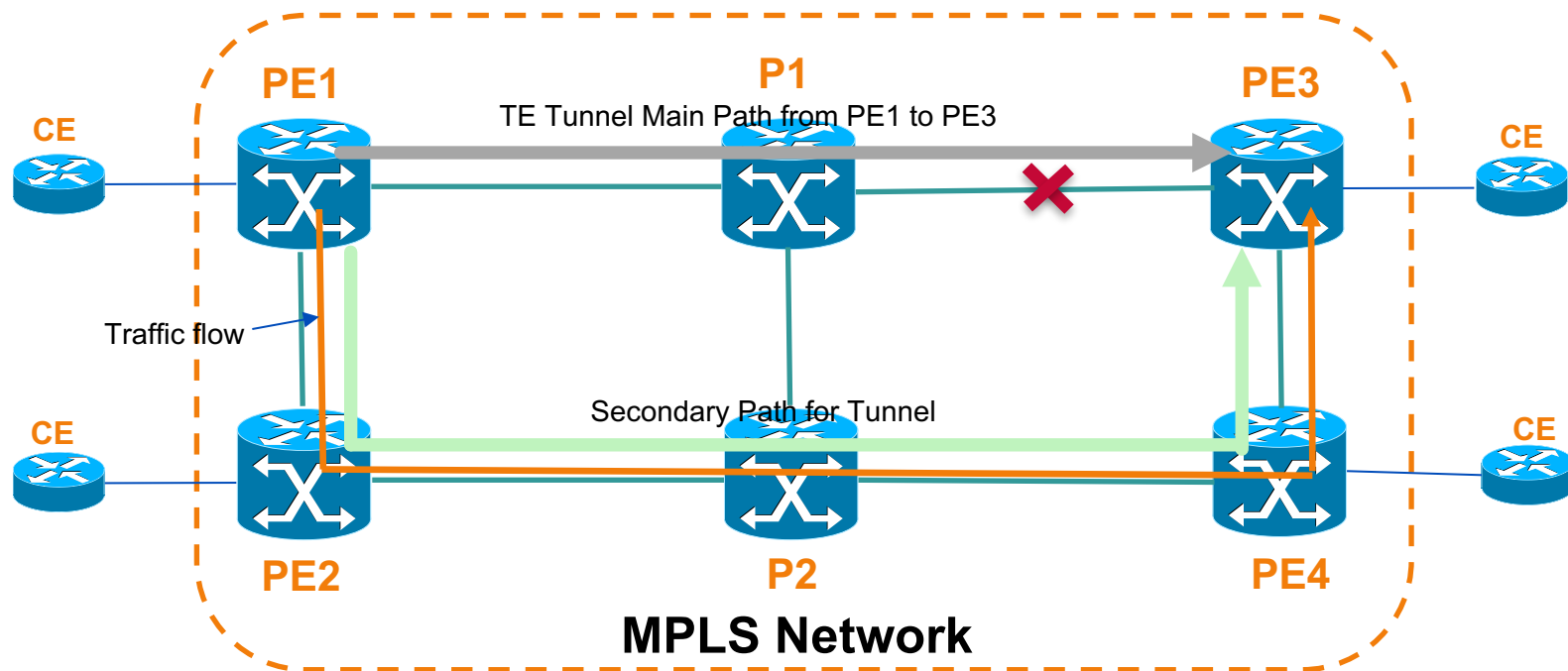
TE Path Protection Example

- Under on tunnel, both main path and secondary path are created.



TE Path Protection Example

- When main path is not available, secondary path will be active. Traffic will go via secondary path.

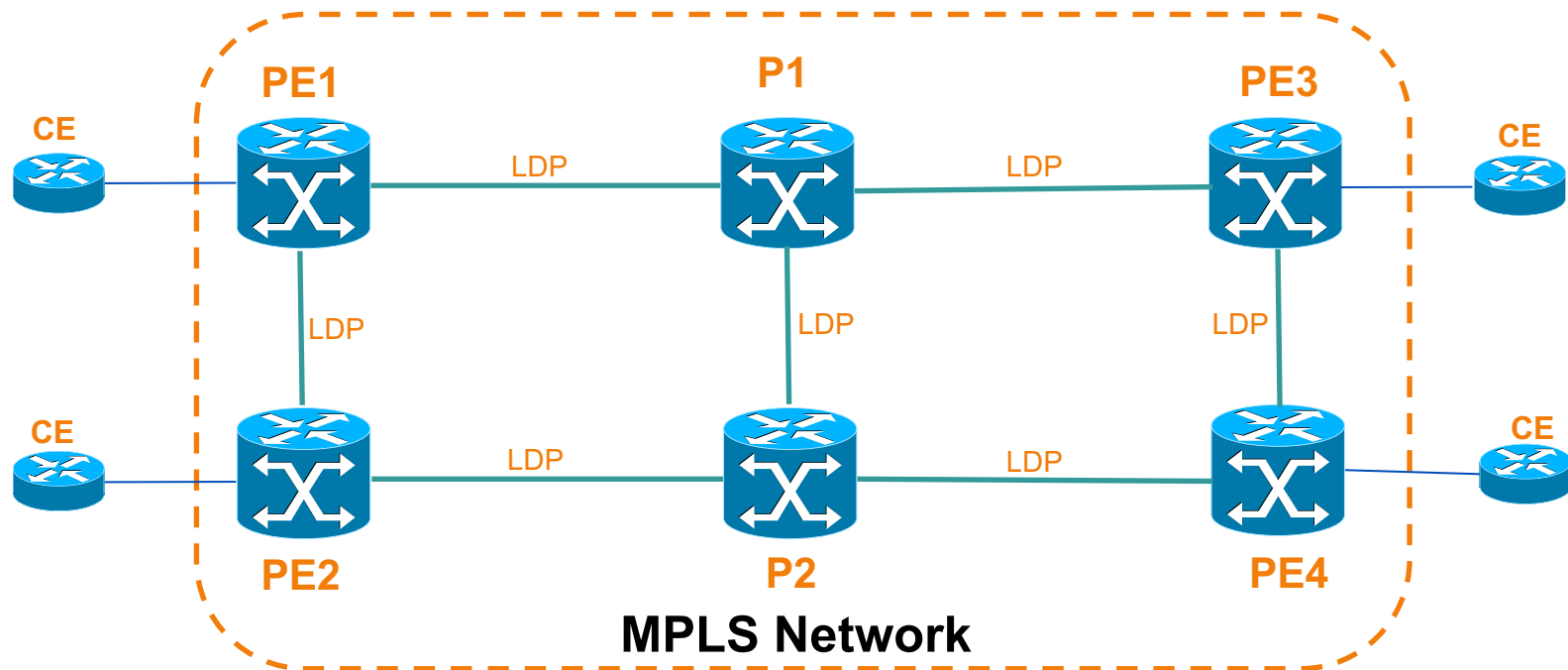


MPLS TE Services



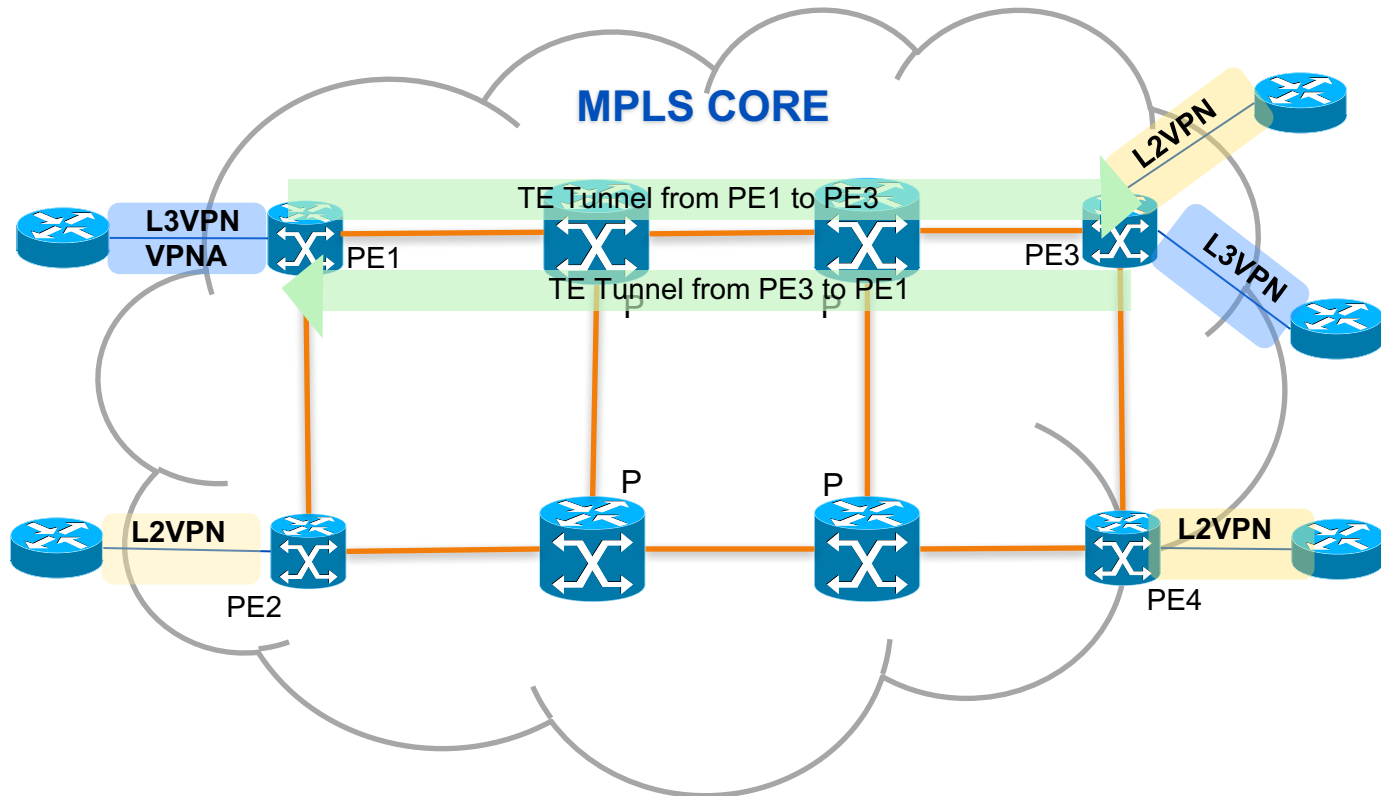
LDP for VPN Tunnel LSP

- In many ISPs, LDP LSP is the tunnel LSP for MPLS L3VPN service. LDP labels are the outer label for traffic forwarding.



TE Tunnel for VPN Tunnel LSP

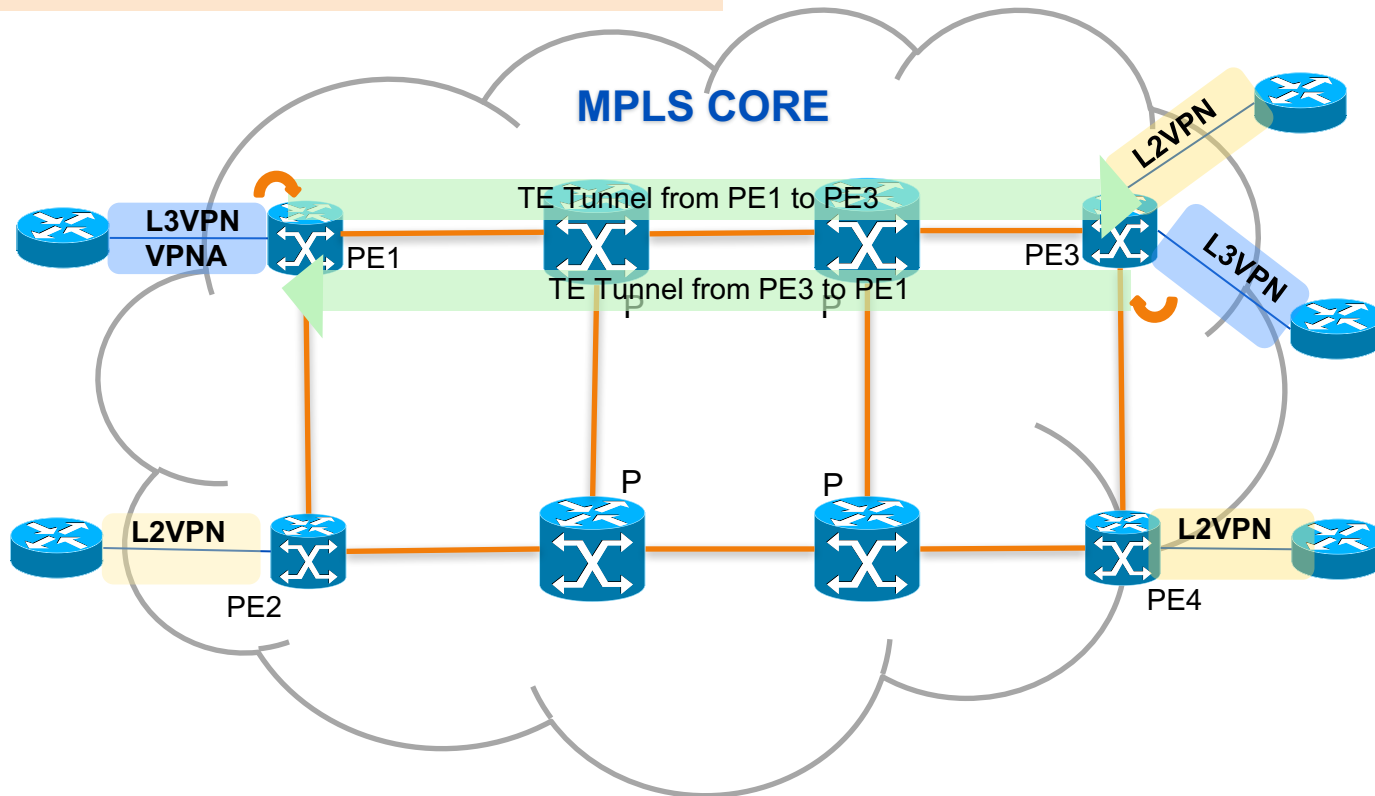
- MPLS TE tunnels also can be used for VPN tunnel LSP.
 1. Set up TE tunnels between PEs



TE Tunnel for VPN Tunnel LSP

- MPLS TE tunnels also can be used for VPN tunnel LSP.

- Set up TE tunnels between PEs
- Guide the VPN traffic into the TE tunnel



Thank You!