Networking
For everyone

MPLS Traffic Engineering

Возможности MPLS TE

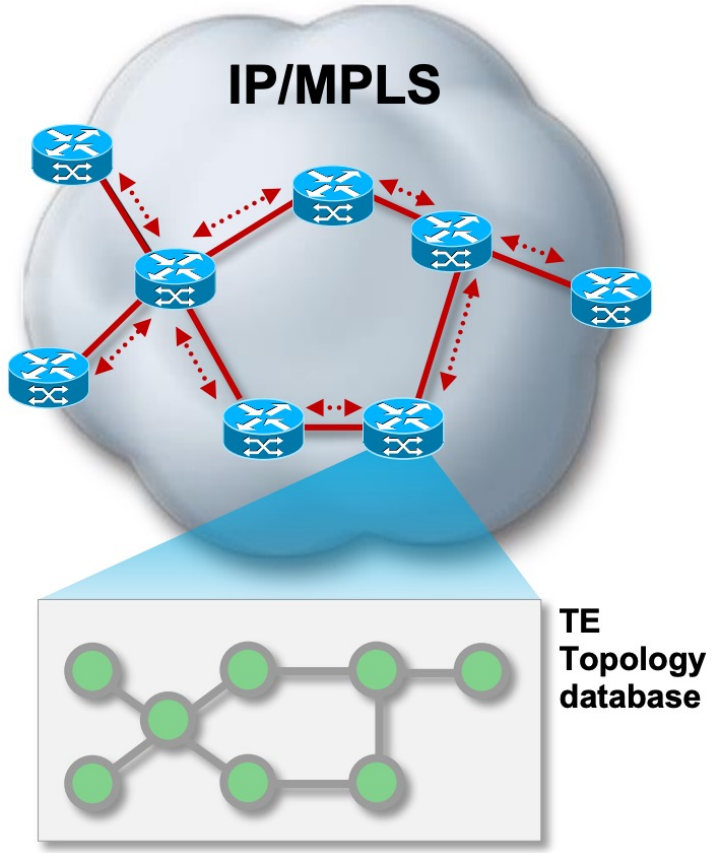
- Предоставляет Explicit Routing
- Поддерживает constraint-based routing
- Поддерживает admission control
- Предоставляет функции защиты установленных путей
- Использует RSVP TE для построения LSP

Принципы работы

- Распространение информации о состоянии каналов
  - OSPF TE, IS-IS TE
- Подсчёт пути (Constraint SPF, CSPF)
- Установление пути (RSVP TE)
- Передача данных в туннель
  - Auto-route
  - Static route
  - Policy based routing
  - Forwarding adjacency

Распространение информации о линках

- Дополнительные характеристики
  - Адрес интерфейса
  - Адрес соседа
  - Bandwidth
  - Maximum reservable bandwidth
  - TE метрика
  - Административная группа

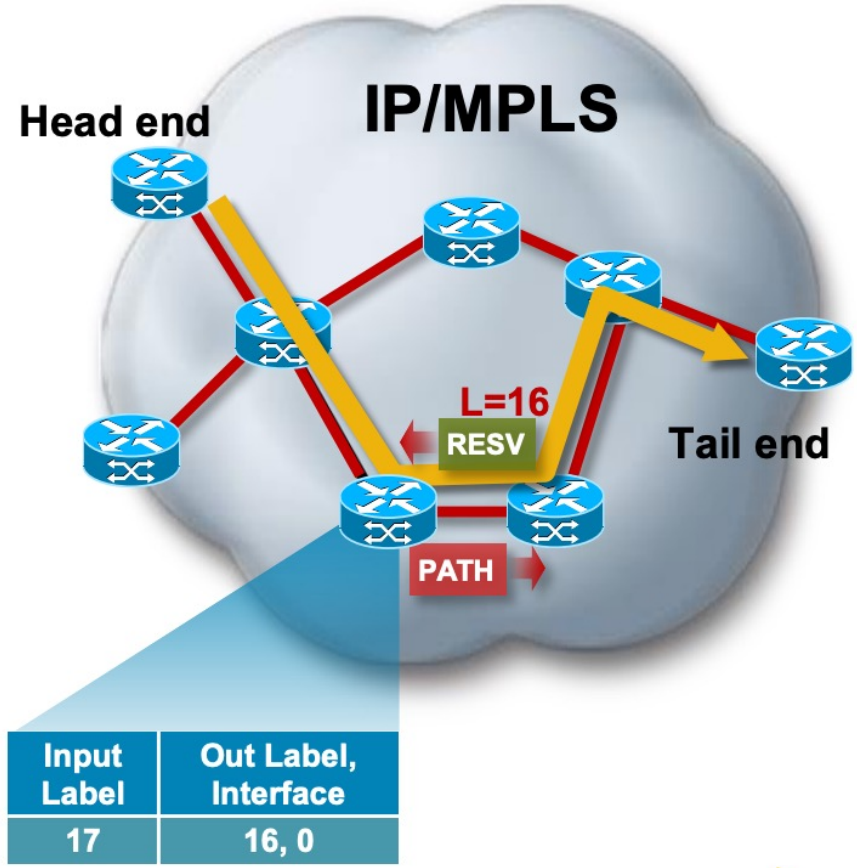


Подсчёт пути (Constraint SPF, CSPF)

- TE устройства поддерживают constraint-based routing
- За подсчёт пути ответственен Tunnel head end
- Constraints и топология подаются на вход алгоритму SPF
- SPF игнорирует интерфейсы, не подходящие под условия
  - Напр. не учитывать низкоскоростные интерфейсы
- Сигнализация туннеля – после того, как найден подходящий путь

Установление пути (RSVP TE)

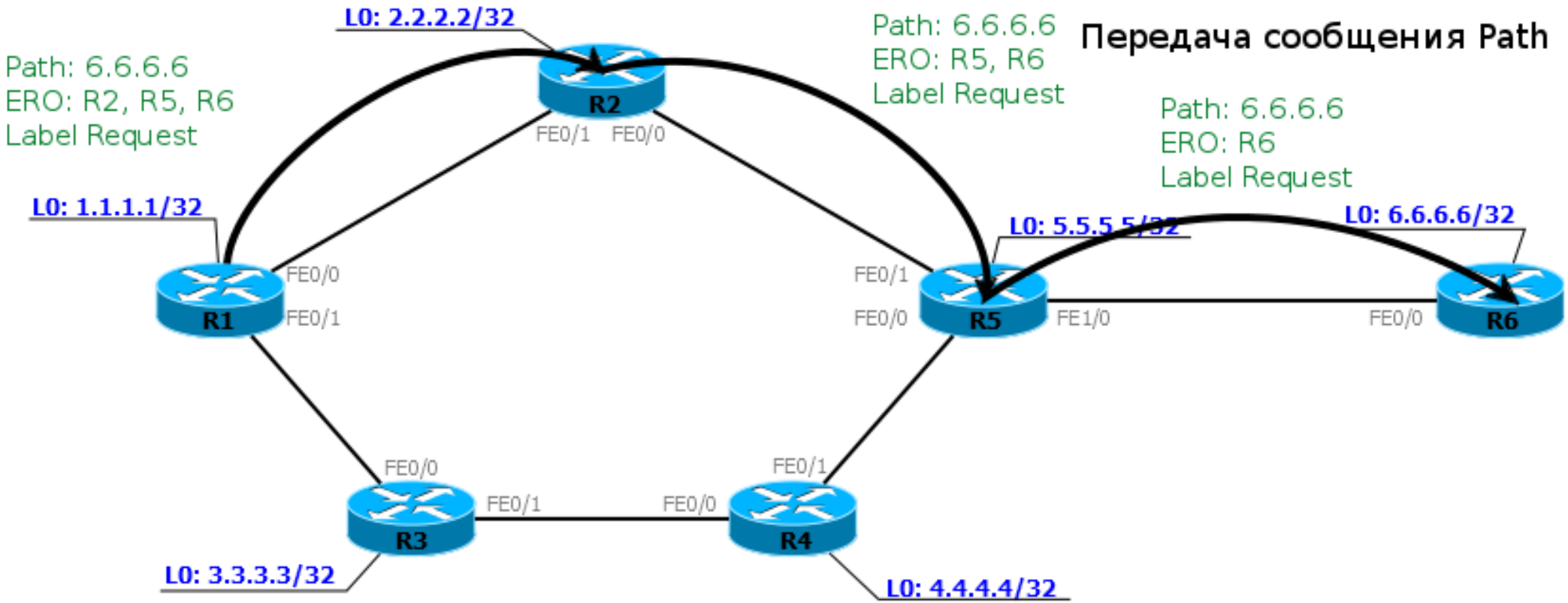
- Установление туннеля происходит посредством RSVP
- Типы RSVP сообщений
  - **PATH**
  - **RESERVATION**
  - **ERROR**
  - **TEAR**
- Дополнительные RSVP объекты
  - LABEL_REQUEST (PATH)
  - LABEL (RESV)
  - EXPLICIT_ROUTE (PATH)
  - RECORD_ROUTE (PATH/RESV)
  - SESSION_ATTRIBUTE (PATH)



Установление пути

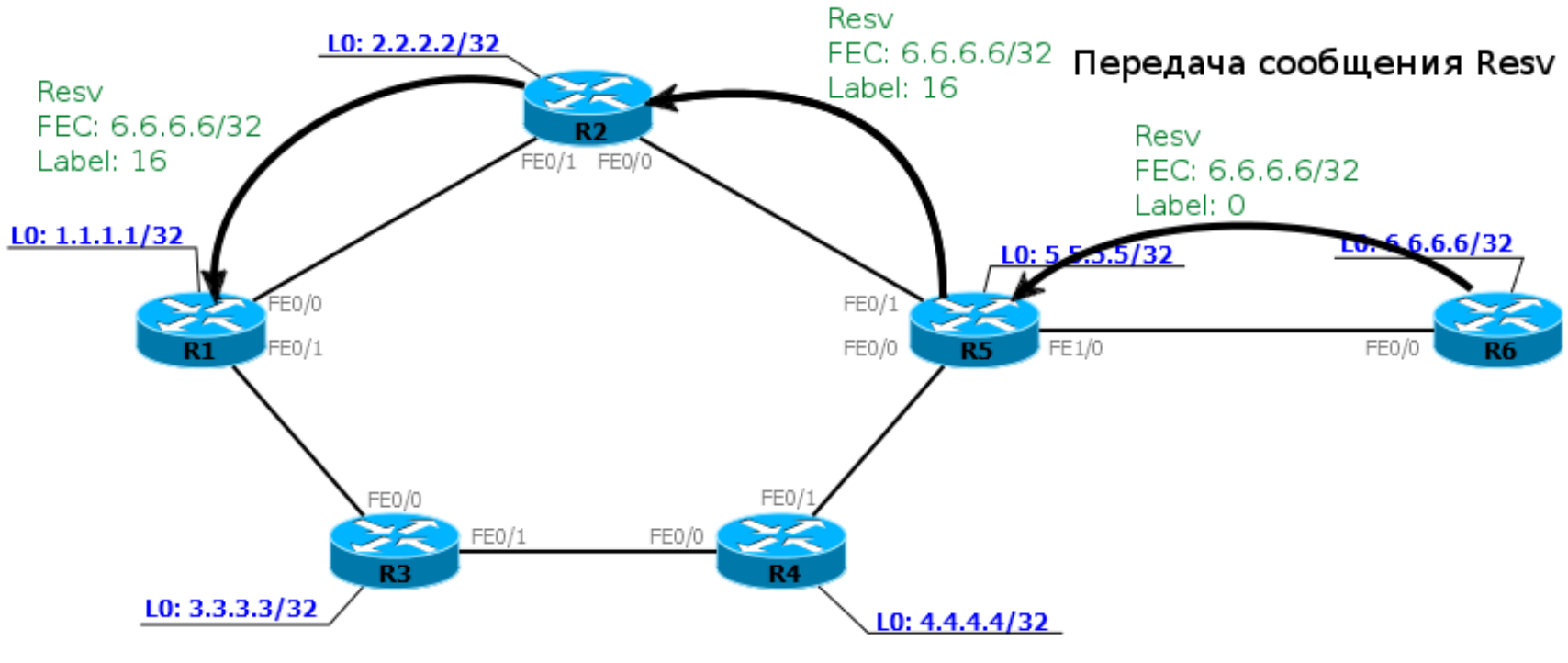
- PATH передаётся по пути, установленному на Ingress PE
- Путь = список узлов от источника до получателя
- **Explicit Route Object** (ERO)— специальный объект сообщения RSVP Path. Он содержит список узлов, через которые надо пройти этому сообщению.
- RSVP PATH передаётся согласно ERO
- Сосед при получении RSVP PATH проверяет наличие требуемых ресурсов и, если они есть, выделяет метку MPLS для FEC

Установление пути (PATH)



Установление пути (RESV)

- Egress PE выделяет метку и вставляет её как объект **Label** в ответное сообщение RESV
- Сообщение RESV передаётся к Ingress PE, генерируя LSP
- RESV должно пройти через те же узлы, что Path, но в обратном порядке



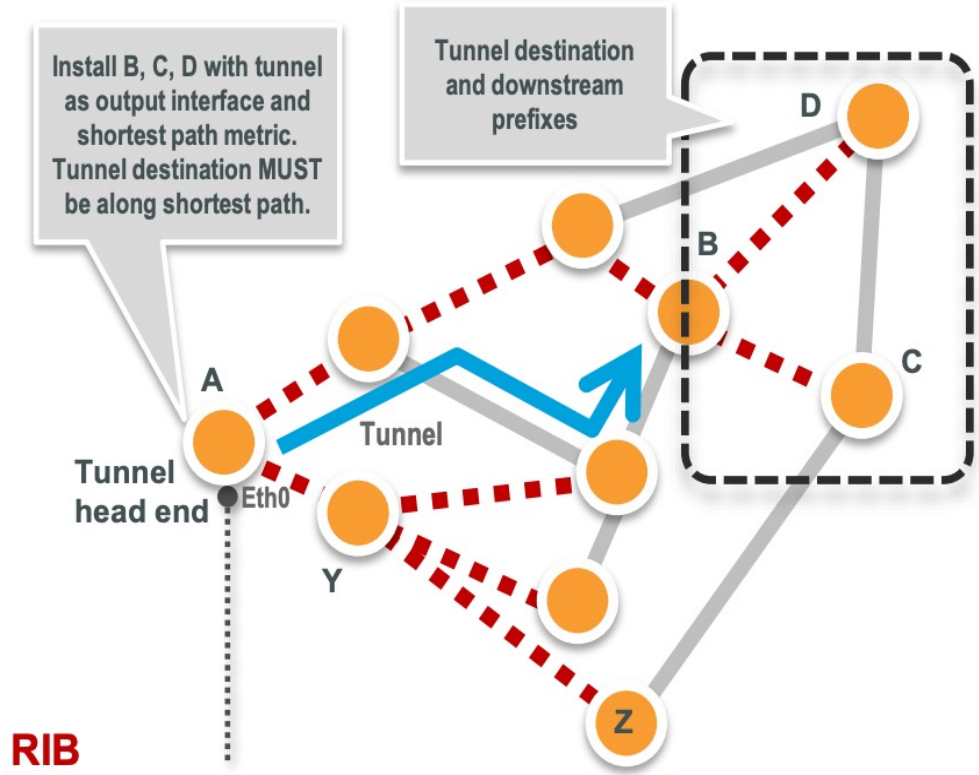
Помещение трафика в туннель

- Траффик попадает в туннель на Head End
- Много разных опций для проведения данной операции
  - PBR
  - Autoroute announce (IGP shortcut)
  - Tunnel-policy
  - автоматическое помещение
- Подсчёт пути никак не зависит от метода помещения трафика в туннель

Autoroute announce

- Префикс устанавливается в RIB, в качестве выходного интерфейса – tunnel
- Установка с кратчайшей IGP метрикой

  Egress LSR будто бы подключен непосредственно
- IGP Shortcut



RIB

Prefix	Next Hop	Metric	Out Interface
B	B	30	Tunnel
C	B	40	Tunnel
D	B	40	Tunnel
Z	Y	20	Ethernet0

Forwardind Adjacencies

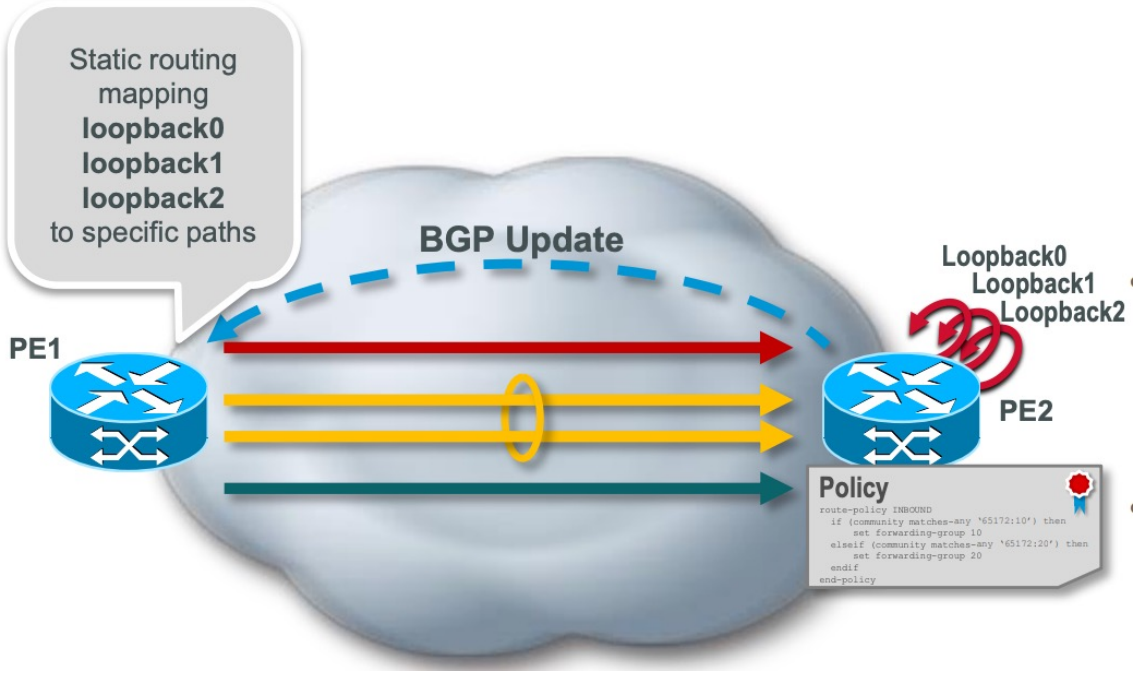
- Возможность объявления MPLS TE туннеля внутрь IGP как обычный интерфейс
- Все окружающие маршрутизаторы будут учитывать его в своих расчётах SPF

Выбор пути на основе policy

- Локальный механизм на Head End
- Политика PBR выставляет forwarding class для входящего трафика
- Трафик перенаправляется в туннель в соответствии с выставленным forwarding class
- Поддерживается 7 классов

Выбор туннеля на основе сервиса

- Сервисы (L2VPN / L3VPN) обычно получают путь динамически
  - Рекурсивный поиск BGP NH
- При использовании BGP можно использовать разные Loopback для разных сервисов
  - Разные BGP NH отправляются в разные туннели



Метрики

- Есть два типа метрик
  - IGP
  - TE
- По умолчанию, метрика TE = метрика IGP
- По умолчанию, используется TE
- При равенстве метрик маршрутизатор выберет именно туннель

Приоритеты туннелей

- Setup priority
- Hold priority
- Каждый приоритет может быть в диапазоне 0 … 7
  - меньше - лучше
- Обычно выбираются одинаковые для Setup и Hold
- Нельзя настроить Hold ниже, чем Setup

Перестроение туннелей

- Hard Preemption
  - LSP с более высоким приоритетом просто замещает LSP с низким
- Soft Preemption
  - Make-Before-Break
  - Маршрутизатор через RSVP-TE сообщает Ingress LSR низкоприоритетного LSP, что нужно искать новый путь
  - LSP с высоким приоритетом ожидает, пока трафик низкоприоритетного LSP переключится на новый LSP
  - если путь найти не удалось в течение некоторого времени, низкоприоритетный LSP всё равно ломается

Explicit Path

- CSPF вычисляет кратчайший путь с учётом ограничений
- Транзитные узлы можно явно указать в Explicit-Path, который станет одним из входных ограничений для CSPF
- Локальное ограничение

Attribute-Flag

- Каждый интерфейс окрашивается
- При настройке указываем, что этот туннель может идти по красным и фиолетовым линиям, но не может по зелёным
- Attribute Flag = 32 битное число, каждый бит означает какой-то параметр
- В Affinity мы указываем, что именно нам нужно

Networking
For everyone

Надёжность и сходимость

- Две опции для повышения стабильности и уменьшения времени прерывания сервисов
  - Path Protection
    - защита на уровне целого LSP
  - Local Protection
    - защита на уровне интерфейса/узла
      - FRR ☺

Path Protection

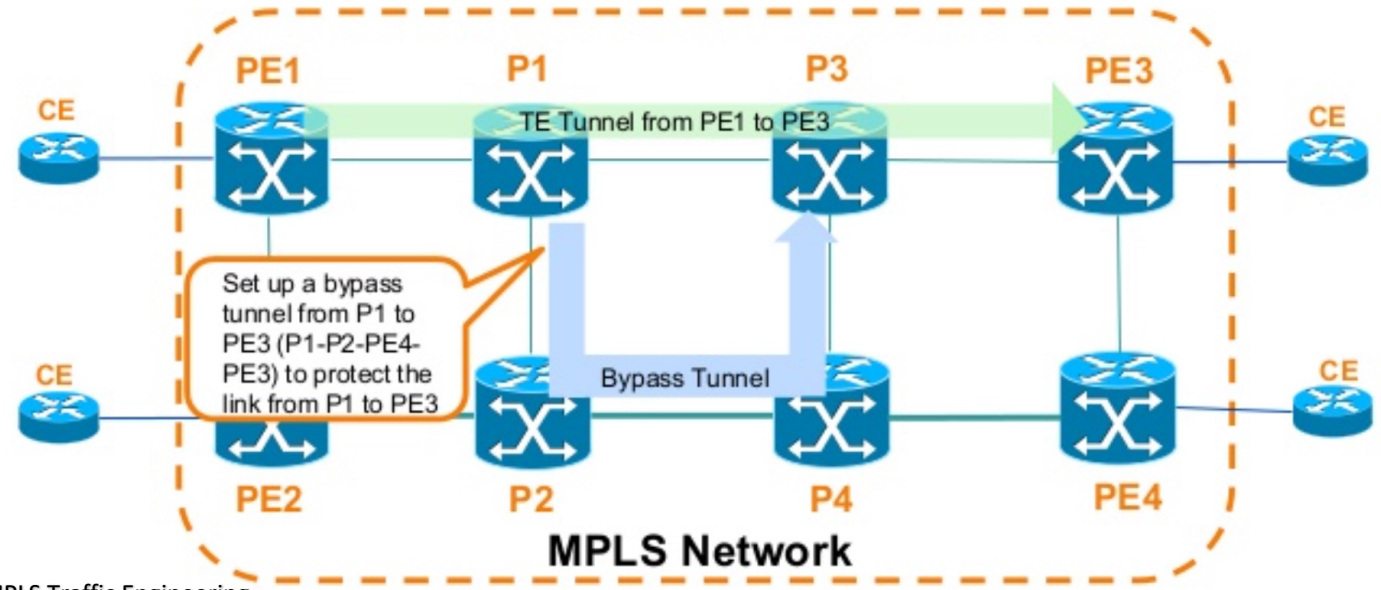
- При настройке указываем, сколько и каких LSP необходимо построить
- Primary – основной LSP
- Secondary – резервный LSP
  - Standby
    - путь заранее вычислен и LSP пре-сигнализиован
  - Non-standby
    - путь заранее вычислен, но LSP не сигнализирован
- Best Effort
  - как-нибудь без резервирования ресурсов

Local Protection (Fast reroute, FRR)

- При Path Protection, в случае аварии, страдают пакеты, которые уже находятся в туннеле
- FRR же позволяет защитить либо узел, либо интерфейс
  - node protection
  - link protection
- Не следит за всем LSP

Link Protection

- Защита интерфейса
- Когда PLR замечает, что транзитный интерфейс LSP упал, он мгновенно перенаправляет трафик
- Ingress PE об этом ничего не знает
- Чтобы так быстро перенаправить пакеты, Bypass LSP должен быть построен заранее



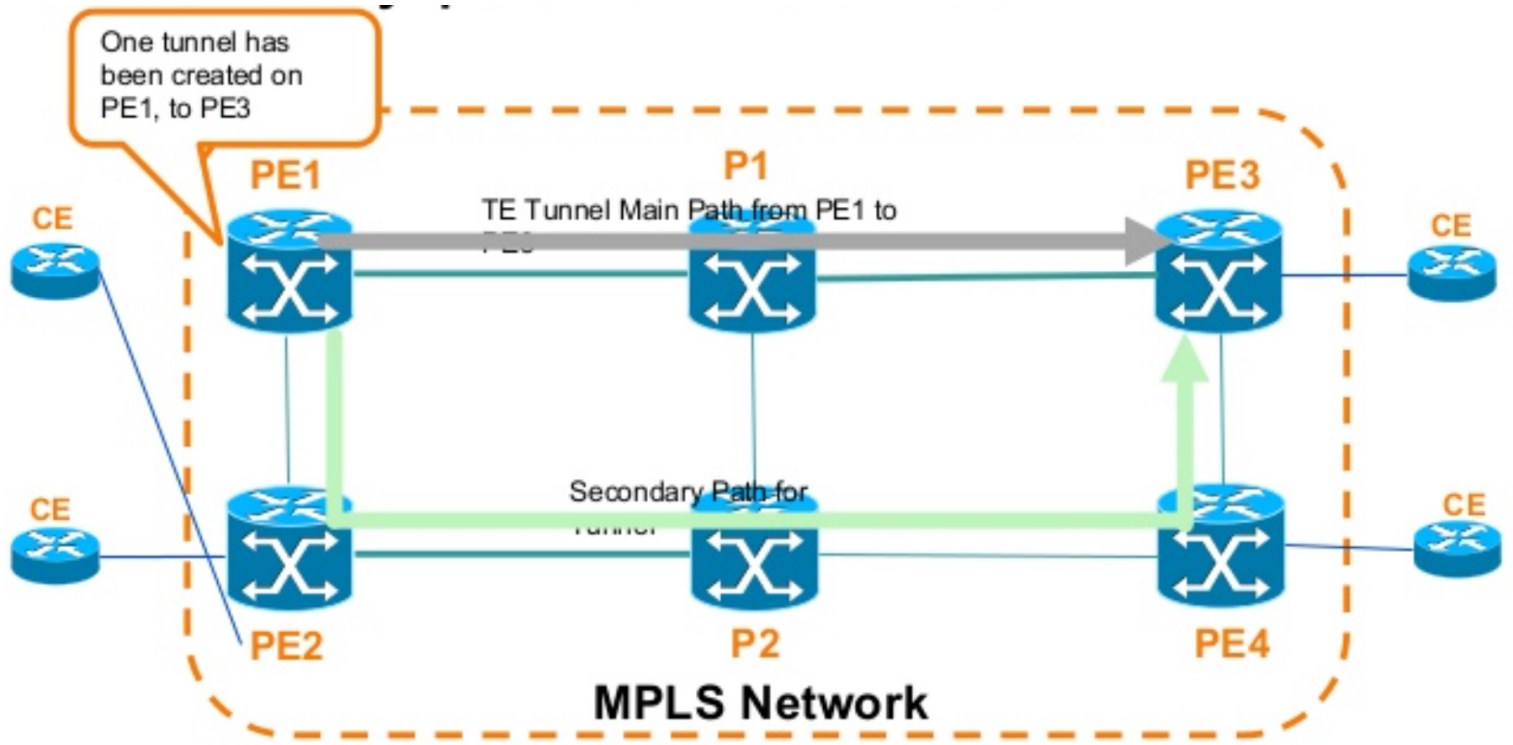
Link Protection

- Каждый узел по пути Primary LSP ищет, как обойти падение следующего линка
- Запускается полный механизм построения LSP
  - CSPF до MP (NHOP для случая падения линка и NNHOP для случая падения узла)
  - RSVP PATH по рассчитанному пути
  - RSVP RESV, если резервирование удалось
- Туннели могут строиться автоматически или ручками ☺

- Когда пакет приходит на PLR во время аварии, тот сначала делает обычный SWAP внешней метки
- он знает, что надо передать его в FRR туннель — добавляет ещё одну метку
- Далее пакет коммутируется по Bypass LSP по стандартным правилам
  - меняется внешняя (FRR) метка, а две внутренние остаются неизменными.

Node Protection

- Абсолютно то же самое, что и Link Protection за исключением транспортной метки — PLR должен знать какую метку ждёт NNHOP
- Туннель строится не до следующего узла, а через один — NNHOP



Разновидности FRR

- many to one
  - много LSP могут использовать один Backup LSP
  - предпочтителен в большинстве ситуаций
- one to one
  - для каждого LSP строится свой собственный LSP
  - насколько мне известно, Cisco не поддерживает данный режим

Порядок настройки

Порядок настройки

- Включить TE для IGP
- Включить RSVP на всех интерфейсах
- Настроить туннельный интерфейс типа TE
- Настроить FRR / резервные туннели

Включение TE для IGP

```
R1(config)#router isis
R1(config-router)# metric-style wide
R1(config-router)# mpls traffic-eng router-id Loopback0
R1(config-router)# mpls traffic-eng level-1
```

Включение RSVP

```
R1(config)#interface gi1.15
R1(config-if)#mpls traffic-eng tunnels
R1(config-if)#ip rsvp bandwidth 5000
```

Настройка туннельного интерфейса

```
R1(config)#interface Tunnel4
R1(config-if)#description To R4
R1(config-if)#ip unnumbered Loopback0
R1(config-if)#tunnel mode mpls traffic-eng
R1(config-if)#tunnel destination 4.4.4.4
R1(config-if)#tunnel mpls traffic-eng bandwidth 8000
R1(config-if)#tunnel mpls traffic-eng path-option 1 dynamic
```

Networking For everyone