

## MPLS-TE

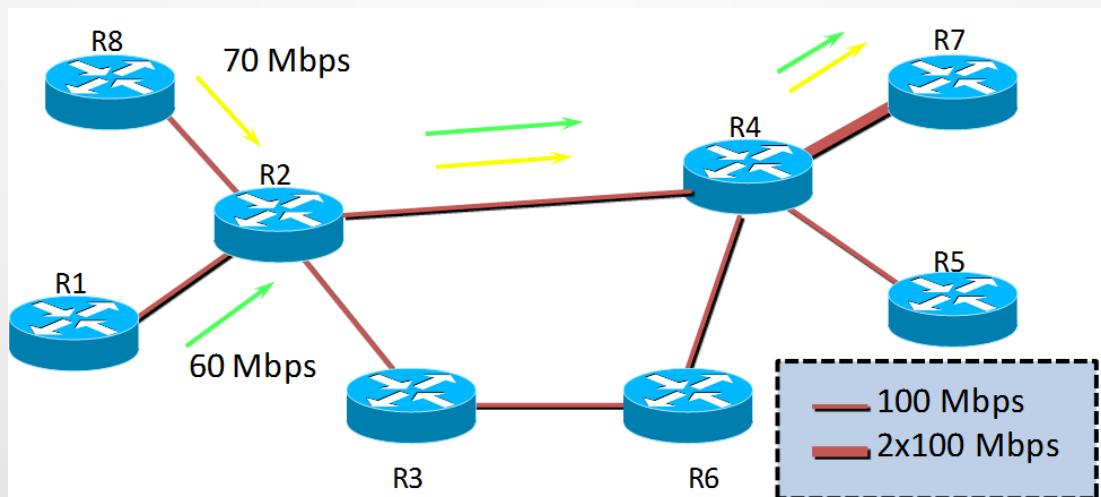
*Multi  
Protocol  
Label  
Switching  
Traffic Engineering*

# ¿Qué es Ingeniería de Tráfico en Redes?

- Es el proceso de mapear la demanda de tráfico sobre la topología de la red.
- Es la habilidad de controlar el flujo de tráfico en la red.
- Como controlar los flujos de datos en una red para cumplir con los requerimientos de los mismos y optimizar la utilización de los recursos de la red.
- Ingeniería de Tráfico (Traffic Engineering – TE) es un concepto general, no es dependiente de MPLS
- Existen propuestas básicas para redes TCP/IP
- Antecedente redes ATM (en desuso)

# Motivación - ¿Porqué necesito TE?

- En IPv4 el encaminamiento de paquetes se realiza por IP destino.
- En MPLS, el encaminamiento de tramas MPLS se realiza basado en la etiqueta negociada por LDP. A su vez está sigue el camino habitual de ruteo IPv4.



# Ingeniería de tráfico implica:

- Mover el tráfico del camino establecido por el IGP a un camino menos congestionado.
- Utilizar el exceso de ancho de banda sobre los enlaces sub-utilizados. Maximizar la utilización de los enlaces y nodos de la red.
- Aumentar la confiabilidad del servicio. Dividir el tráfico entre diversos enlaces minimiza el impacto de una falla simple. Asegurar capacidad necesaria para re-encaminar el tráfico en caso de fallas puntuales.
- Alcanzar requerimientos impuestos por el tráfico

# Ingeniería de Tráfico

- Objetivos:
  - Orientados al tráfico:  
Minimizar pérdidas de paquetes, minimizar retardos, maximizar flujo, minimizar la congestión
  - Orientados a los recursos:  
Principalmente Ancho de banda
  - Minimizar la intervención manual

# Conceptos genéricos de Ingeniería de Tráfico

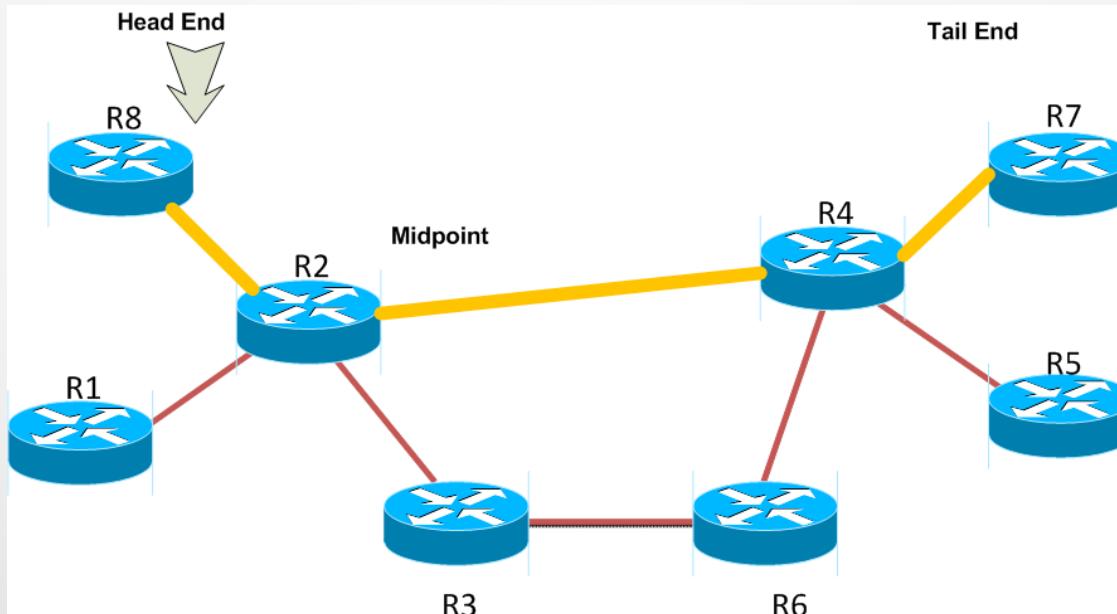
- Calculo de caminos (mapeo eficiente a recursos):
  - Offline vs Online
  - Centralizado vs Descentralizado
- Conocimiento de la topología de red y estado de la misma (IGP-TE)
- Mecanismo de señalizar el camino dentro de la topología.
- Capacidad de definir “necesidades” del tráfico, luego dada la topología y su estado, calcular el mejor camino con estas “restricciones”.
- Definir prioridad y capacidad “expulsar” tráfico menos prioritario.
- Utilizar mecanismos clásicos de QoS: contratos de tráfico, marcación, colas, schedulers, etc.

# MPLS – TE (conceptos)

- Introduce la capacidad de definir el camino de forma explícita
- Provee mecanismos para protección de camino.
- Utiliza un IGP con extensiones de TE para intercambiar información de atributos de links.
- Permite elegir el camino basado en restricciones.
- Utiliza un protocolo para señalizar (establecer) el camino: RSVP-TE o LDP-CR.
- Realiza control de admisión.

# MPLS – TE Tunnels

- Tuneles de Ingeniería de tráfico.
- Tuneles unidireccionales.
- Upstream (dirección hacia el head end)
- Downstream (dirección hacia el tail end)



# Link Information Distribution

- Link:
  - Bandwidth disponible para reservas.
  - Atribute-flag
  - Weight
- Tunnel:
  - Bandwidth
  - Priority and holding priority: de 0 (high) a 7 (low)
  - Affinity and Affinity Mask (atribute-flag)

# Link Information Distribution

- Para el control de admisión de un nuevo túnel se utiliza la prioridad (durante la señalización).
- El ancho de banda es utilizable por todas las prioridades.
- Durante la admisión un túnel con priority mayor obtiene los recursos frente a uno de priority menor.
- Una vez establecido el túnel, un túnel nuevo con priority Y puede hacer preempt a uno ya establecido con holding priority X, si  $Y < X$ .
- El túnel expulsado puede volver a establecerse por otro camino, siempre y cuando haya recursos suficientes.
- Affinity y Mask Affinity, hacen que solo se utilicen los links “afines” en la topología. (AFFINITY&&MASK==ATTRIBUTE&&MASK)

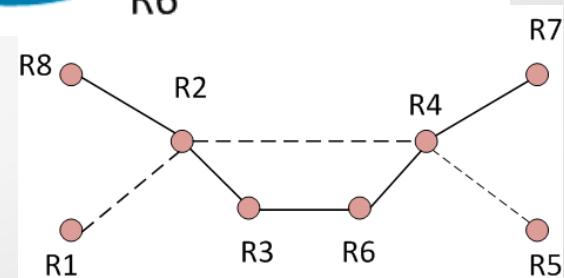
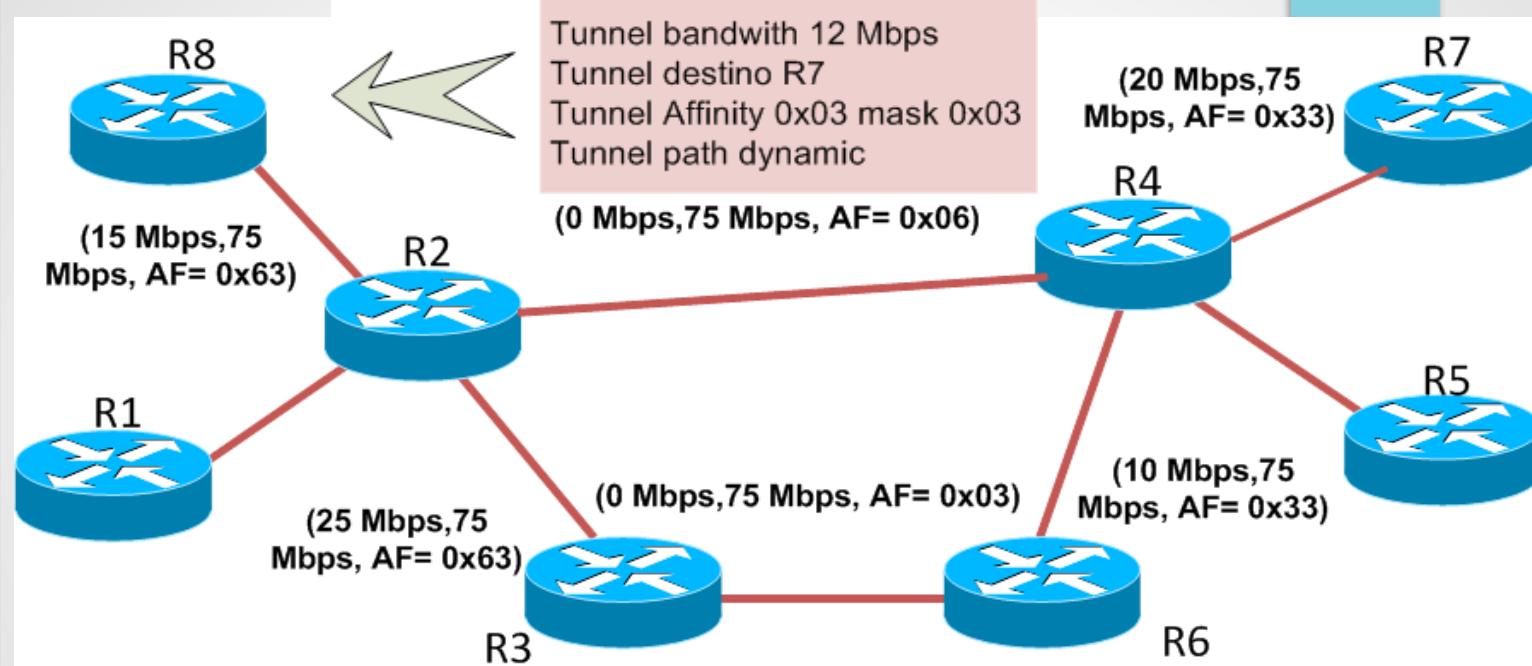
# Extensiones IGP para IGP-TE

- Intercambio de Información:
  - Información del Link
  - Traffic Engineering Metric (Weight).
  - Maximum Link Bandwidth
  - Maximum Reservable Bandwidth
  - Unreserved Bandwidth (per priority level)
  - Attribute Flags
- En OSPF como LSA opaco type 10, formato TLV.

# IGP selección de camino

- El nodo Head end “generalmente” es el responsable por el calculo de camino (veremos otras alternativas)
- Constrained Short Path First (CSPF), solo contempla los links que cumplen las restricciones
  - 1) Topología
  - 2) Eliminar los links que no cumplen las restricciones.
  - 3) Mecanismo de desempate cuando hay mas de un candidato final
- Los nodos son capaces de realizar Constrain Base Routing (CBR), seleccionar un camino con restricciones (utilizando CSPF).
- CSPF busca un camino, no necesariamente el óptimo..
- Una vez encontrado el camino, este se señaliza por RSVP-TE o CR-LDP.
- Hay pocas implementaciones de CR-LDP, CISCO y Juniper solo implementaron RSVP-TE

# Cálculo de Caminos



# RSVP-TE

- RFC 3209
- Extensiones a RSVP definido en RFC 2205 y RFC 2210
- Se agregarán varios Objetos:
  - LABEL\_REQUEST (utilizado en PATH)
  - RSVP\_LABEL (RESV)
  - EXPLICIT\_ROUTE (PATH)
  - RECORD\_ROUTE (PATH/RESV)
  - SESSION\_ATTRIBUTE (PATH)
  - HELLO (una “especie” de keepalive RSVP)
- Recordar RSVP es soft-state

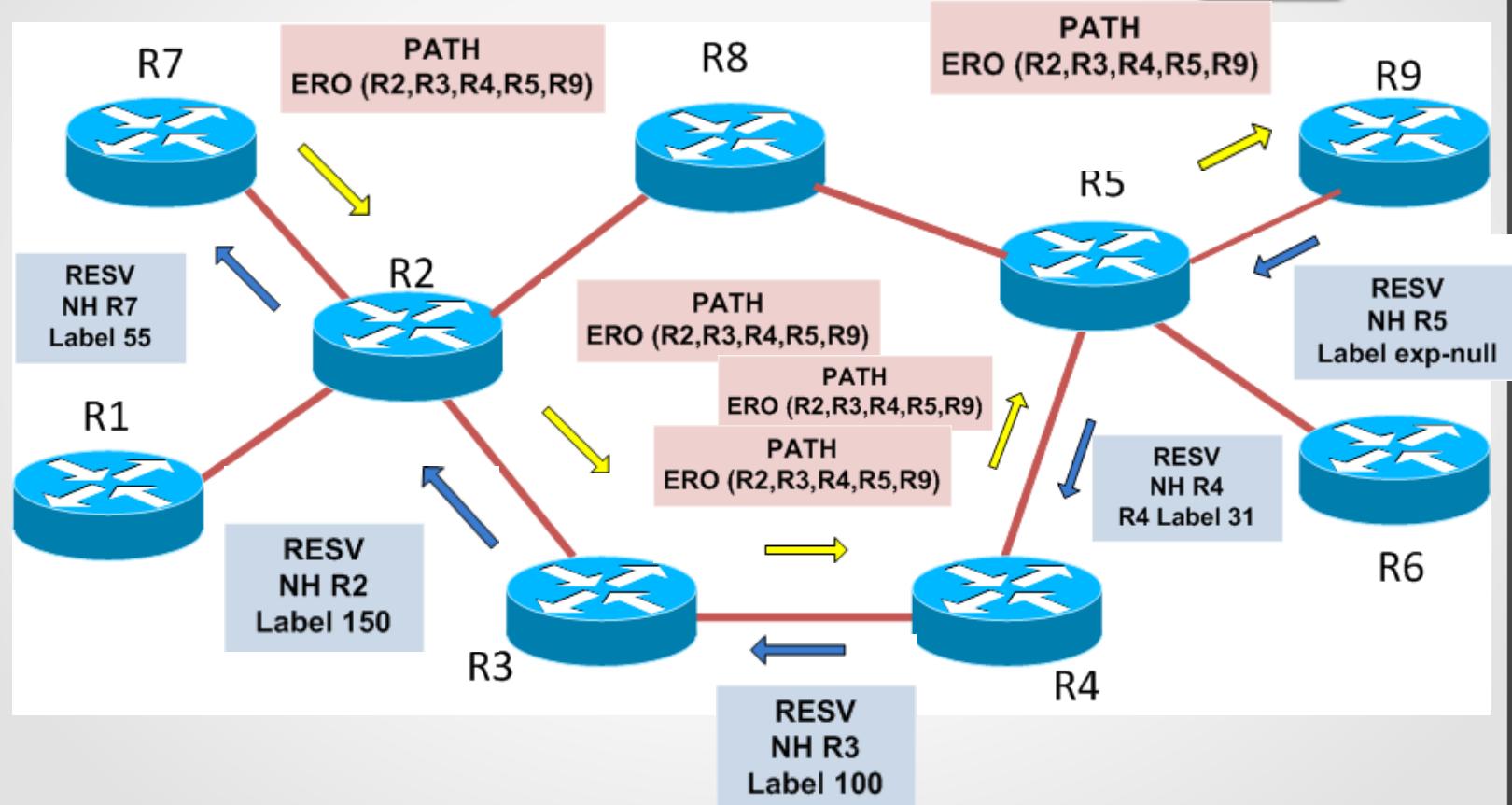
# RSVP-TE

- EXPLICIT\_ROUTE Object (ERO), lista de objetos:
  - Dirección IP
  - lose bit (lose/strict)
- RECORD\_ROUTE:
  - Type: IPv4 o Label
  - Flag:
    - (IPv4) Local protection aviable o Local protection using
    - (Label) Global Space

# RSVP-TE

- SESION\_ATTRIBUTE:
  - Setup-priority
  - Holding-priority
  - Flags:
    - Label Recording
    - Protection Desired.
    - Shared Explicit (SE)
- FLOWSPEC: la solicitud de reserva de ancho de banda utiliza el objeto “original” de RSVP

# RSVP-TE



# RSVP-TE

- Re-optimización vs Fallas
- Re-optimización periódica (CISCO default 60 min)
- Re-optimización Manual
- Bloqueo de Optimización (no realizar optimizaciones)
- Re-optimización invocada por eventos (establecimiento de un link)
- Un túnel puede tener varios explicit route con diferentes prioridades.
- Auto-bandwidth (max,min,timer) y load-share entre túneles a un mismo destino.
- Make-before-break: cambio de parámetros del túnel sin pérdida de datos.
- Shared-explicit-reservation: “compartir” temporalmente el ancho de banda entre el túnel actual y el nuevo camino.

# RSVP-TE Interarea

- El CSPF queda circunscripto a un área. ¿Qué pasa cuando tengo varias áreas?
- Inter-area Tunnels
  - Originalmente no era posible utilizar re-optimización por confusión entre soft-state y re-optimización, flag “path re-evaluation request” dentro de SESSION\_ATTRIBUTE
  - No se puede utilizar Afinidad (topología del área)
  - No se puede utilizar explicit route dynamic (topología del área)
- Loose hop: el hop debe formar parte del camino, pero no en un orden.
- Strict hop: debe estar directamente conectado
- Idea: Utilizar loose hop con los ABR. Los saltos intermedios los resuelve el CSPF de cada área.

# RSVP-TE Interarea

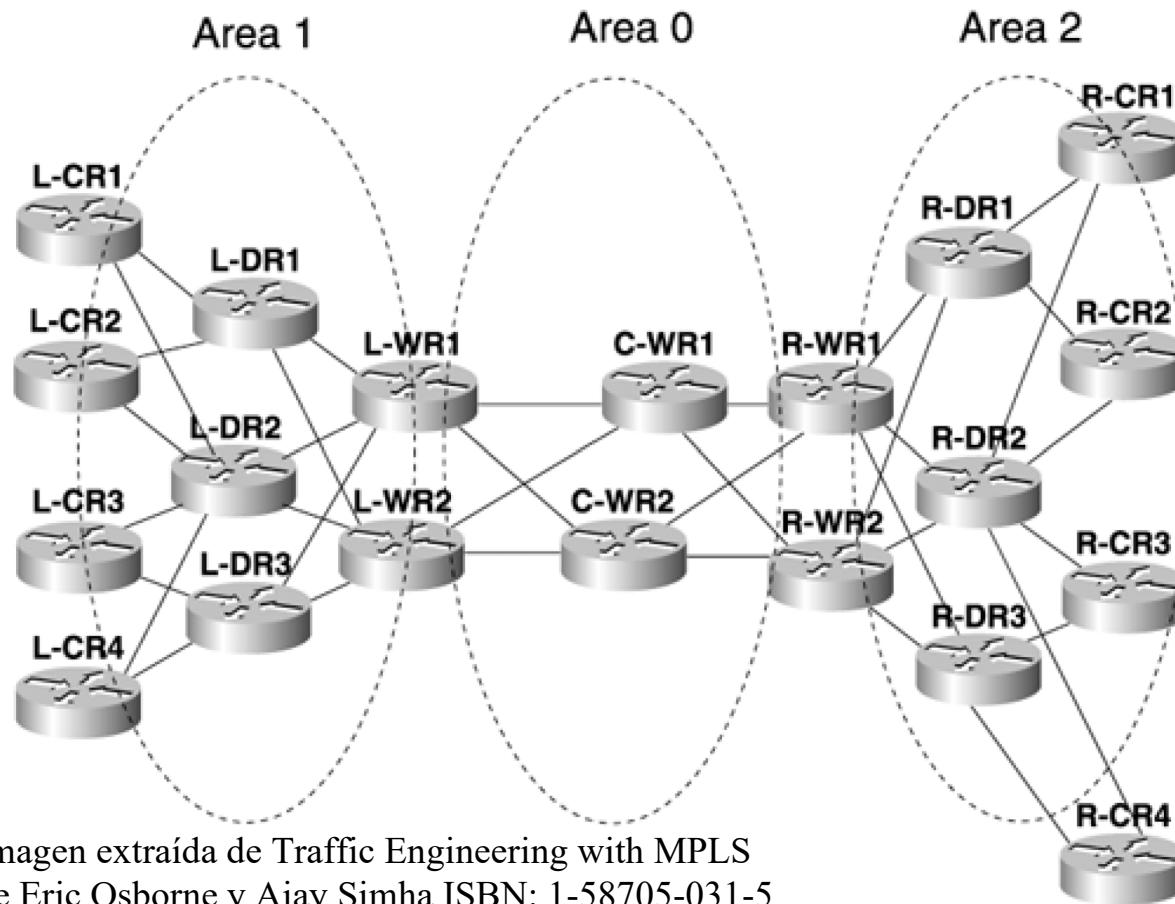


Imagen extraída de Traffic Engineering with MPLS  
de Eric Osborne y Ajay Simha ISBN: 1-58705-031-5

# RSVP-TE Inter-area

```
ip explicit-path name to-R-CR4.1  
next-address loose L-WR1  
next-address loose R-WR1  
next-address loose R-CR4
```

```
ip explicit-path name to-R-CR4.2  
next-address loose L-WR1  
next-address loose R-WR2  
next-address loose R-CR4
```

```
ip explicit-path name to-R-CR4.3  
next-address loose L-WR2  
next-address loose R-WR1  
next-address loose R-CR4
```

```
ip explicit-path name to-R-CR4.4  
next-address loose L-WR2  
next-address loose R-WR2  
next-address loose R-CR4
```

```
tunnel mpls traffic-eng path-option 10 explicit name to-R-CR4.1  
tunnel mpls traffic-eng path-option 20 explicit name to-R-CR4.2  
tunnel mpls traffic-eng path-option 30 explicit name to-R-CR4.3  
tunnel mpls traffic-eng path-option 40 explicit name to-R-CR4.4
```

Ejemplo: Traffic Engineering with MPLS de Eric Osborne y Ajay Simha

# RSVP- TE Interarea

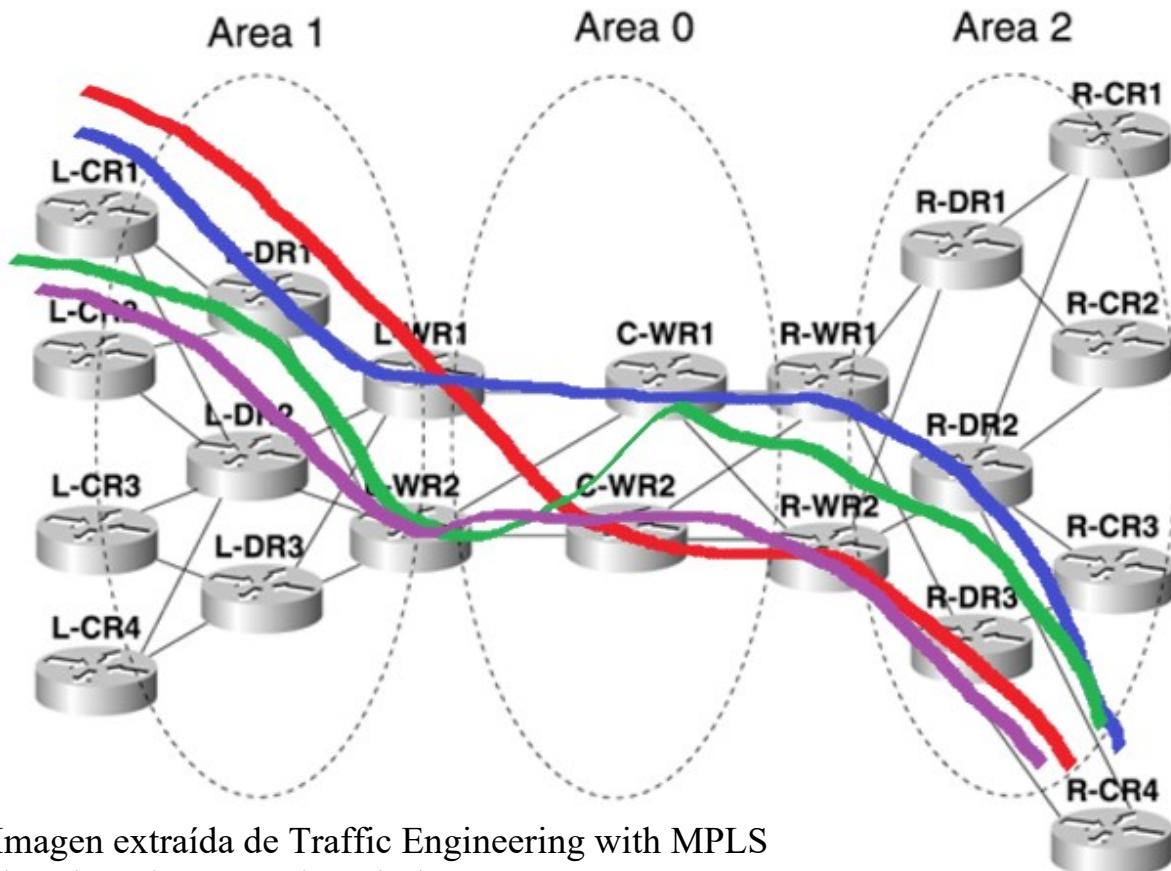


Imagen extraída de Traffic Engineering with MPLS  
de Eric Osborne y Ajay Simha ISBN: 1-58705-031-5

# RSVP-TE InterAS

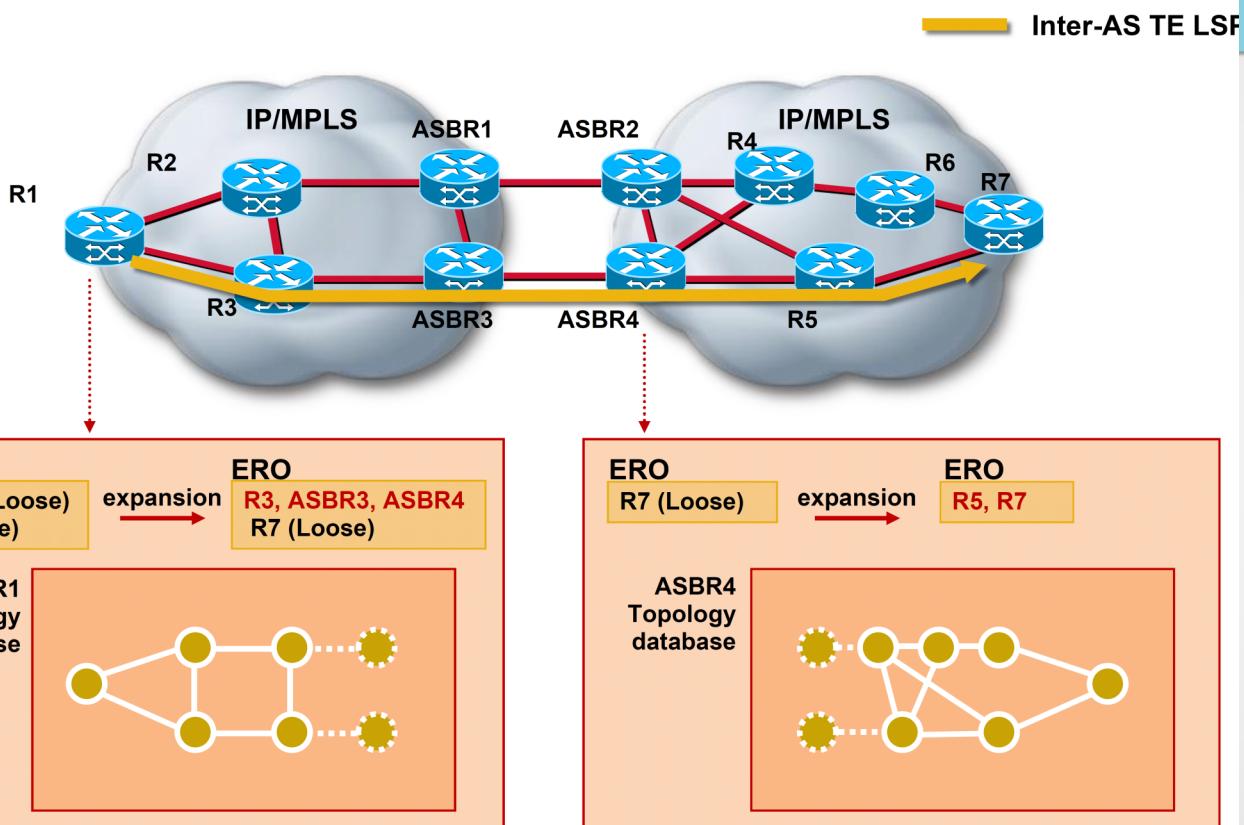


Imagen extraída de la presentación “Deploying MPLS Traffic Engineering (BRKMPL-2104)”  
CISCO Live febrero 3 del 2012, UK

# RSVP – TE Path Computation Element

- Existe un nodo externo al cual le puedo solicitar el calculo de camino.
- Requiere conocer la topología física y la utilización (los LSP ya establecidos)
- Alternativas para conocer la topología: IGP, BGP-LS, SNMP, etc.
- Cliente en los routers (Path Computation Client)
- RFC 4655

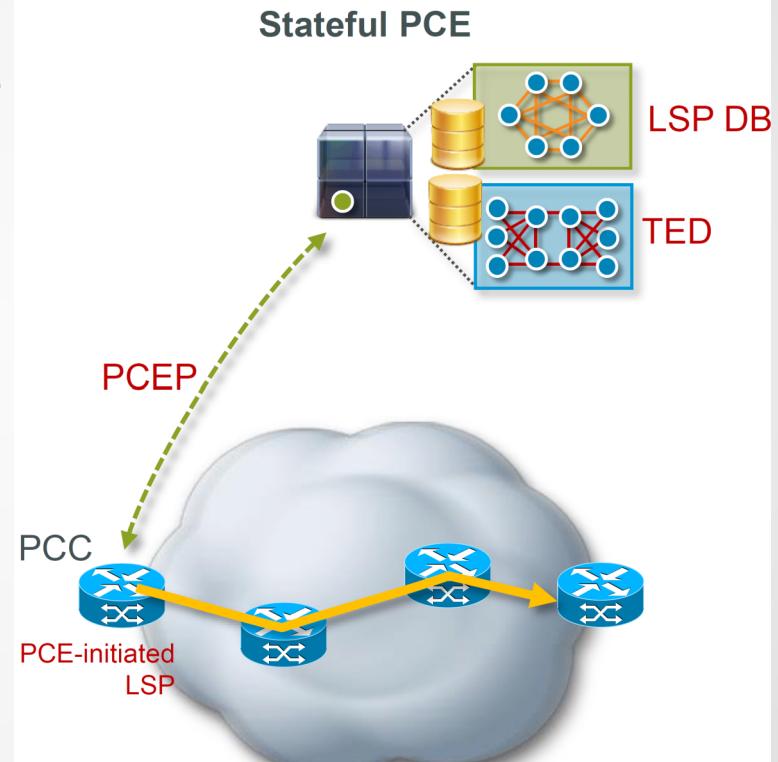


Imagen extraída de la presentación Deploying MPLS Traffic Engineering (BRKMPL-2100)"  
Gregory Johnson, CISCO Live julio 10 al 14 del 2016, Las Vegas

# MPLS – TE ¿Cómo selecciono el Tunnel?

- **¿Cómo uso el túnel?**
- Servicio VPLS, tengo dos etiquetas, una asociada a la VPN, la etiqueta externa asociada al LSR que hostea el destino del paquete transportado .
- **Misma idea:** por MBGP intercambio la etiqueta del servicio, pero en vez de utilizar la etiqueta externa para alcanzar la loopback del LSR destino (aprendida por LDP), utilizo la etiqueta asociada al túnel.
- El control de admisión debo realizarlo al ingreso, el ancho de banda reservado del túnel es para todos los EXP bits.
- **Ruta estática**, next-hop interfaz del túnel.
- **Rutas automáticas** (autoroute), los destinos “detrás” del Tail End, se incorporan automáticamente en la FIB.
- **Policy Base Route**, implica reglas donde defino el next-hop (no solo por IP de destino)

# MPLS -TE Clase Base Tunnel Selection

- Selección de túnel basada en EXP bits, varios túneles hacia el mismo destino.
- Decisión en el Headend
- El Tunnel master bundles lista a los tunnel members
- La selección del túnel se realiza hacia el tunnel master
- A los diferentes túneles miembros se les configura que valores EXP lleva

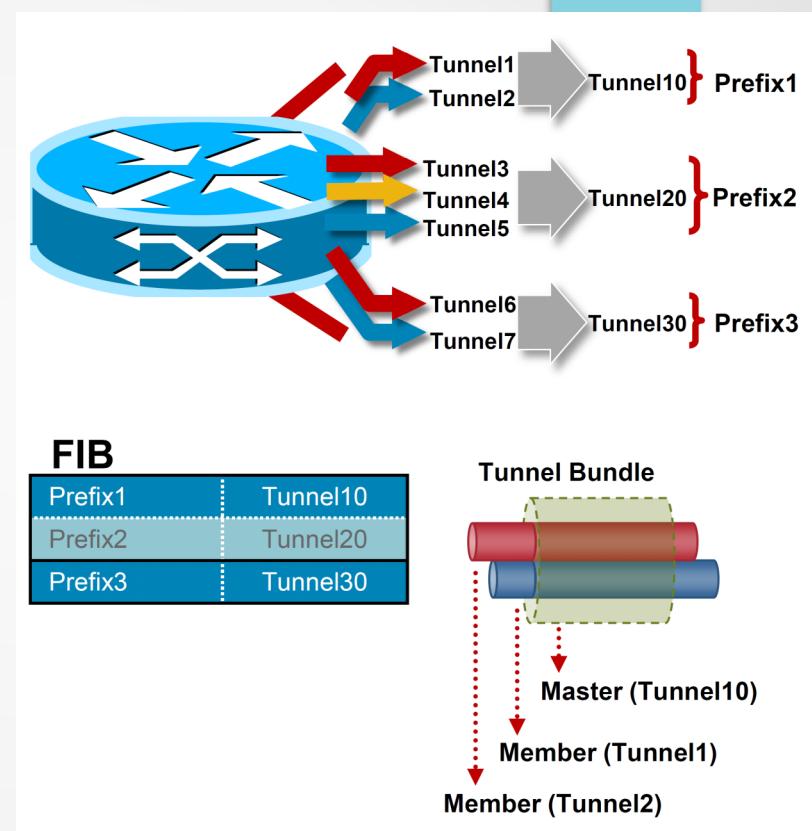


Imagen extraída de la presentación Deploying MPLS Traffic Engineering (BRKMPL-2100)"  
Gregory Johnson, CISCO Live, julio 10 al 14 del 2016, Las Vegas

# MPLS – TE Tunnel per Service

- Los servicios (L2VPN / L3VPN) definen el camino utilizando:
  - Por MBGP el/los next-hops
  - Los next-hop por lo aprendido de los LDP peers
- Cuando utilizamos BGP (L2VPN, L3VPN, IP) es posible utilizar una loopback diferente por servicio.
- En el Tail end una política que defina el next hop diferente por servicio.
- En el Head end una ruta estática a la loopback de cada tipo de servicio por el respectivo túnel.

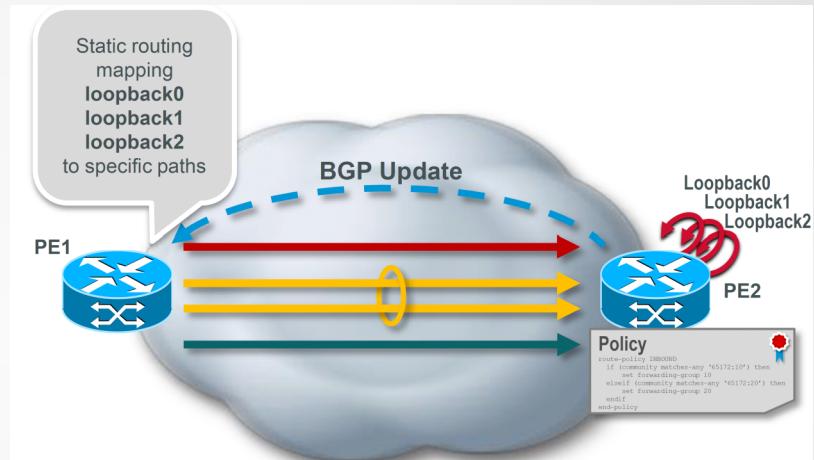


Imagen extraída de la presentación Deploying MPLS Traffic Engineering (BRKMPL-2100)” Gregory Johnson, CISCO Live, julio 10 al 14 del 2016, Las Vegas

# MPLS – TE y Diffserv

- Con un túnel, todos los EXP bit utilizan el BW reservado, pero no puedo garantizar.
- En Class base Selection, puedo reservar BW por EXP bit, pero no se comparte entre ellos, consume del mismo total.
- DiffServ-Aware TE:
- Permite TE por clase, requiere cambios en el IGP-TE y en RSVP (reportar BW por clase y reservar por clase).
- Los diferentes nodos gestionan el BW de un link utilizando un modelo de restricciones.
  - Maximum Allocation Model (MAM)
  - Russian Doll Model (RDM)
- Cada clase potencialmente puede utilizar caminos diferentes.
- Las implementaciones actuales solo soportan dos clases.

# MPLS – TE MAM vs RDM

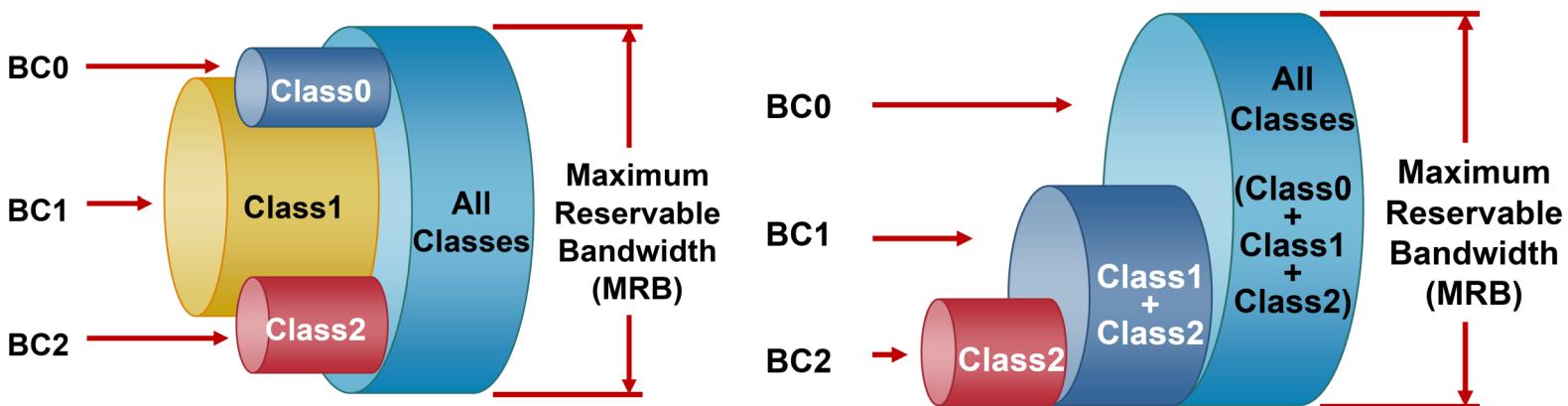


Imagen extraída de Deploying MPLS Traffic Engineering (BRKMPL-2104)  
CISCO Live febrero 3 del 2012, UK

- BW aplica a una clase
- La suma de BWs puede exceder el MRB
- No requiere preemption para garantizar BW por clase.
- BW aplica a una o mas clases
- BC0 es igual al MBR
- Requiere preemption para garantizar BW por clase

# MPLS – TE Protecciones

- Path Protection.
- Local Protection:
  - Link Protection
  - Node Protection
- La protección de camino implica tener un segundo LSP en paralelo para utilizar en caso de falla. Puede ser costoso en recursos sub-utilizados.
- Problema de escala, solo protejo un LSP.
- Local Protection es basado en Fast Re-route (FRR) extensions to RSVP-TE para tunneles MPLS-TE.

# MPLS-TE Path Protection

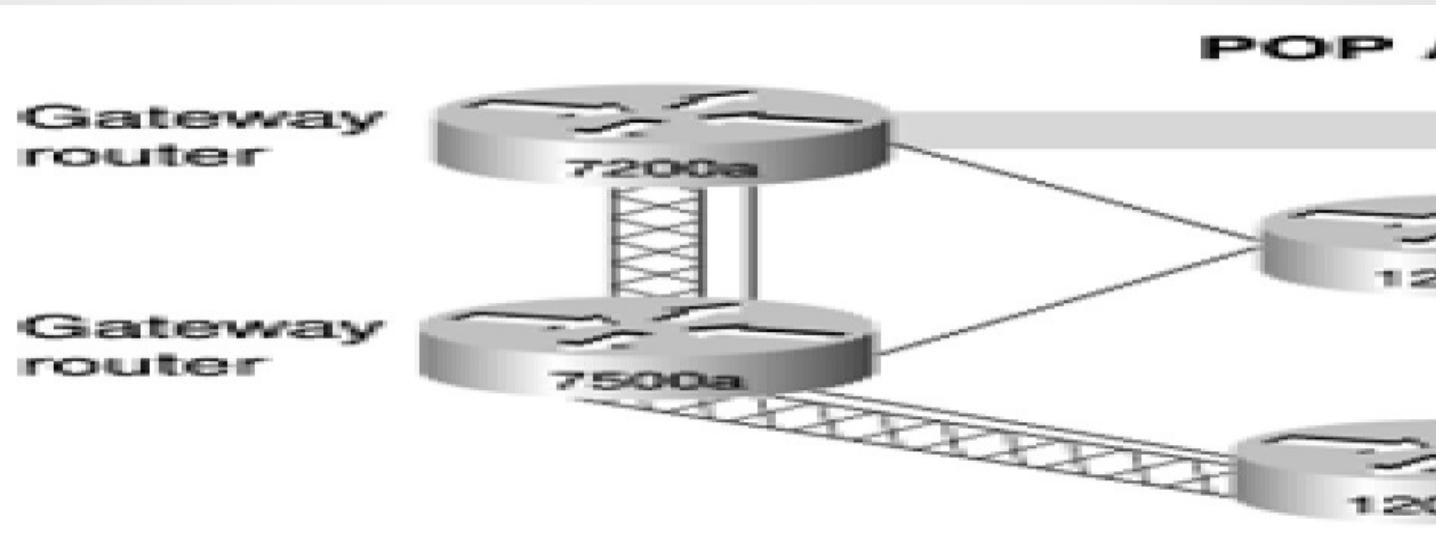
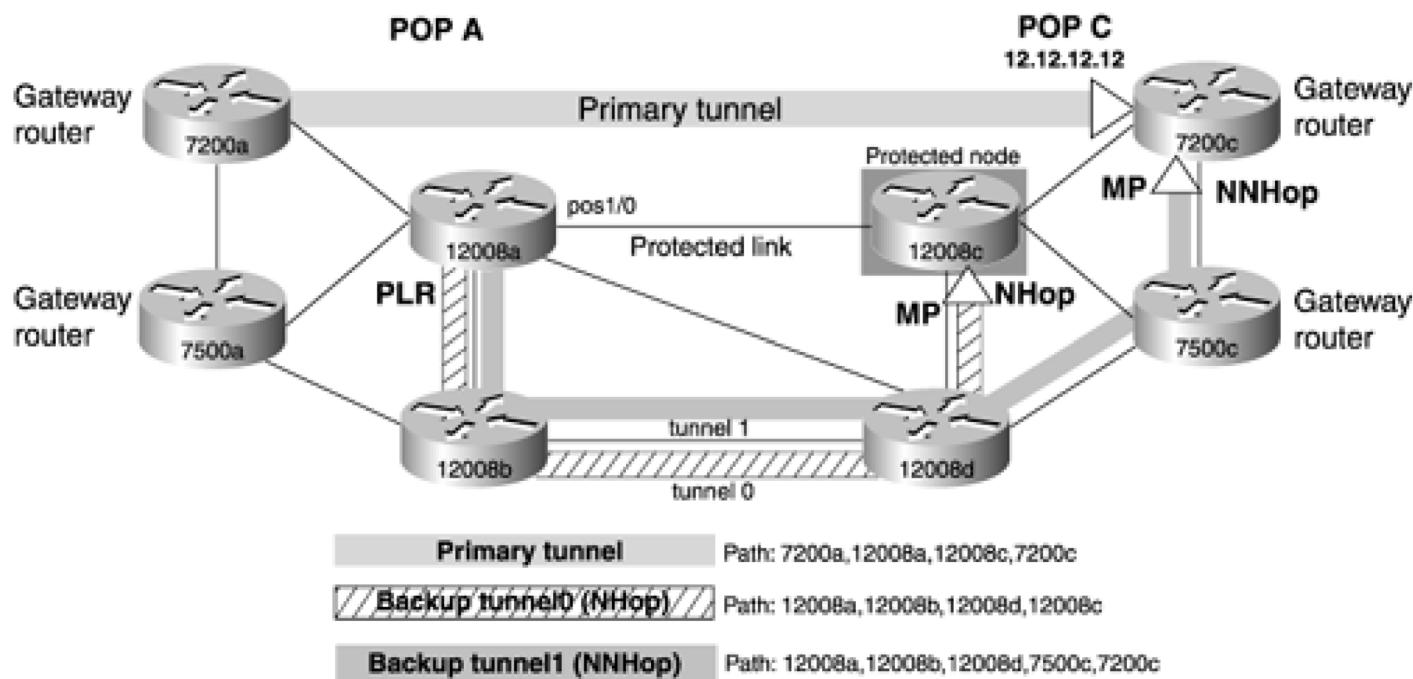


Imagen extraída de Traffic Engineering with MPLS  
de Eric Osborne y Ajay Simha ISBN: 1-58705-031-5

# MPLS – TE Protección Local de Link



- Point of Local Repair (PLR)
- MP (Merge Point)

Imagen extraída de Traffic Engineering with MPLS  
de Eric Osborne y Ajay Simha ISBN: 1-58705-031-5

# MPLS – TE FRR Link

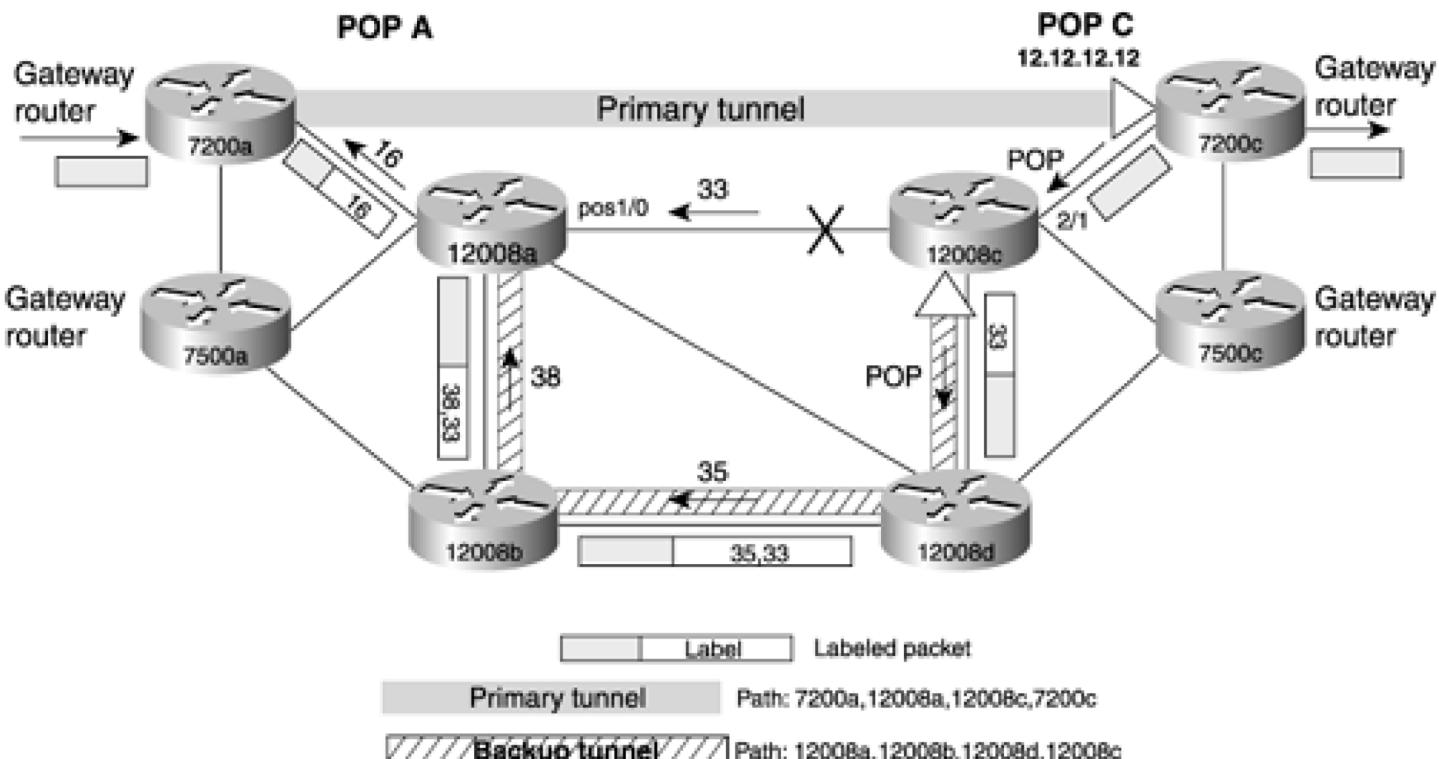


Imagen extraída de Traffic Engineering with MPLS  
de Eric Osborne y Ajay Simha ISBN: 1-58705-031-5

## MPLS – TE FRR falla de Link

- Se señaliza por RSVP al momento de crear el tunnel.
- Se asume que el respaldo es temporal, mientras corre el algoritmo de selección de un nuevo camino para el túnel. Por lo que no se reserva BW.
- El LSP secundario está pre-señalizado antes de la falla, el destino es el NHOP del camino primario.
- Detección de fallas RSVP Hellos (por defecto 100 ms)
- Puedo tener túneles protegidos y no protegidos por un mismo link.
- Los túneles no protegidos, los detecta la pérdida de soft-state (PathErr) e intentan encontrar un nuevo camino.
- Los túneles protegidos, igual se notifica con PathErr al Head-end para buscar un nuevo camino.

# MPLS – TE FRR falla de Nodo

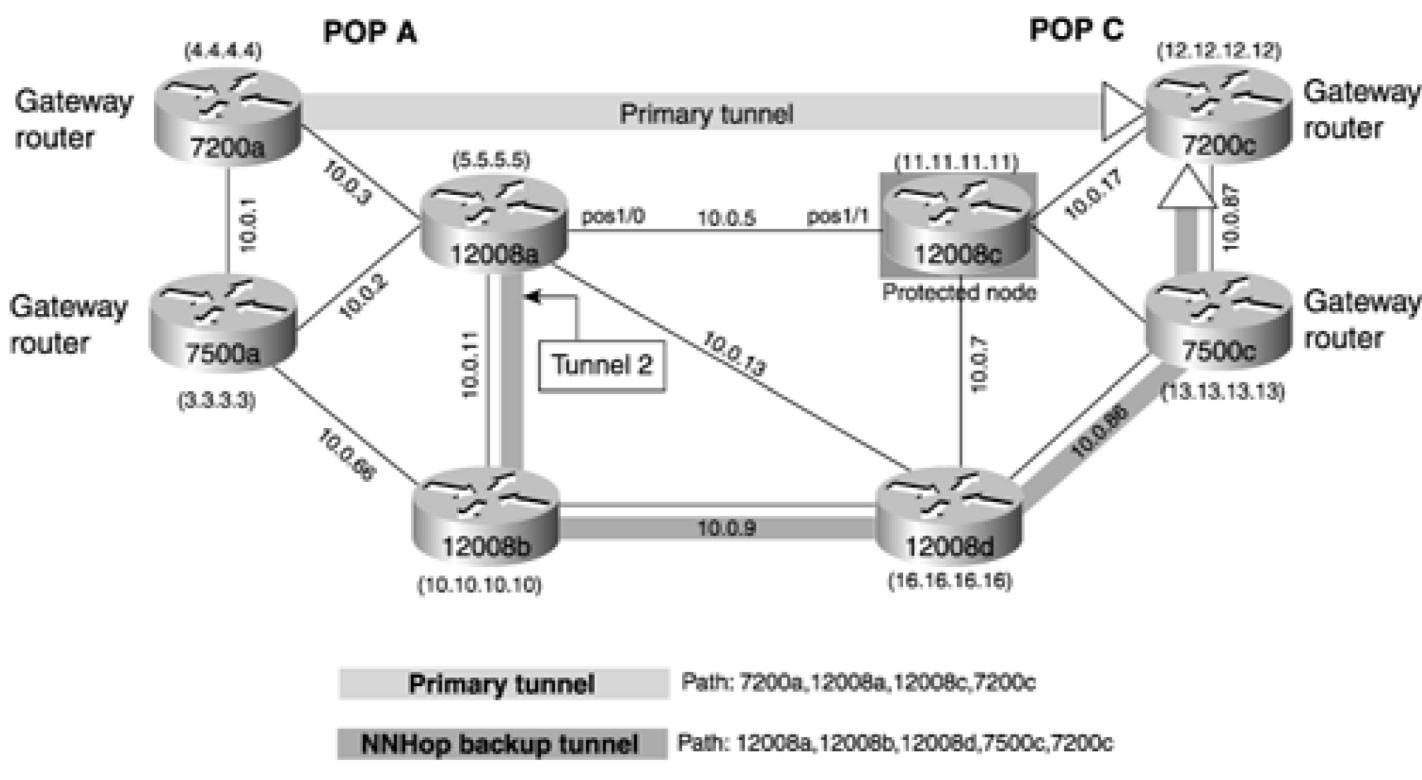


Imagen extraída de Traffic Engineering with MPLS  
de Eric Osborne y Ajay Simha ISBN: 1-58705-031-5

## MPLS – TE FRR falla de Nodo

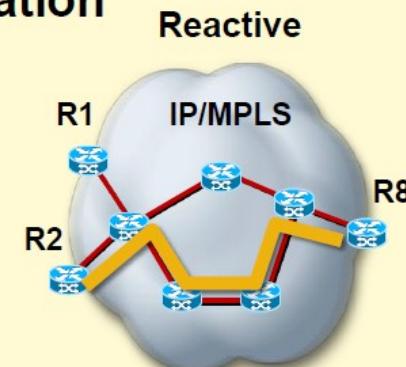
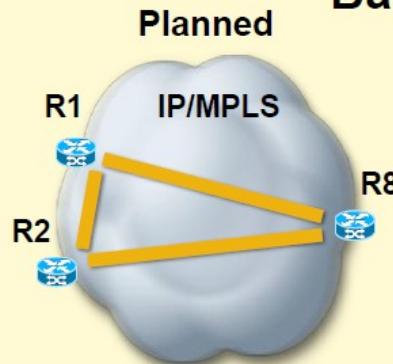
- El túnel debe estar pre-señalizado antes de la falla.
- La protección del túnel termina en en Next Next-hop, requiere habilitarlo al inicio junto con la creación del túnel primario (ROUTE\_RECORD).

# MPLS - TE Consideraciones Finales

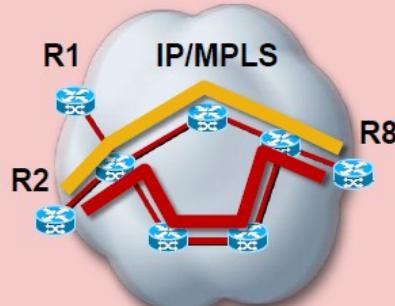
- La complejidad escala con la cantidad de nodos en la red:
  - Hay mas nodos
  - Mas diversidad de caminos
  - De acuerdo a la estrategia de DiffServ TE utilizada.
  - Tengo muchos servicios
- Lo recomendable es disponer de un sistema de gestión centralizado. Evitar errores.
- En una red chica, que varíe poco se podría hacer la concesión de no utilizarlo.

# MPLS-TE Utilización

## Bandwidth Optimization



## Point-to-Point SLA



## Protection

