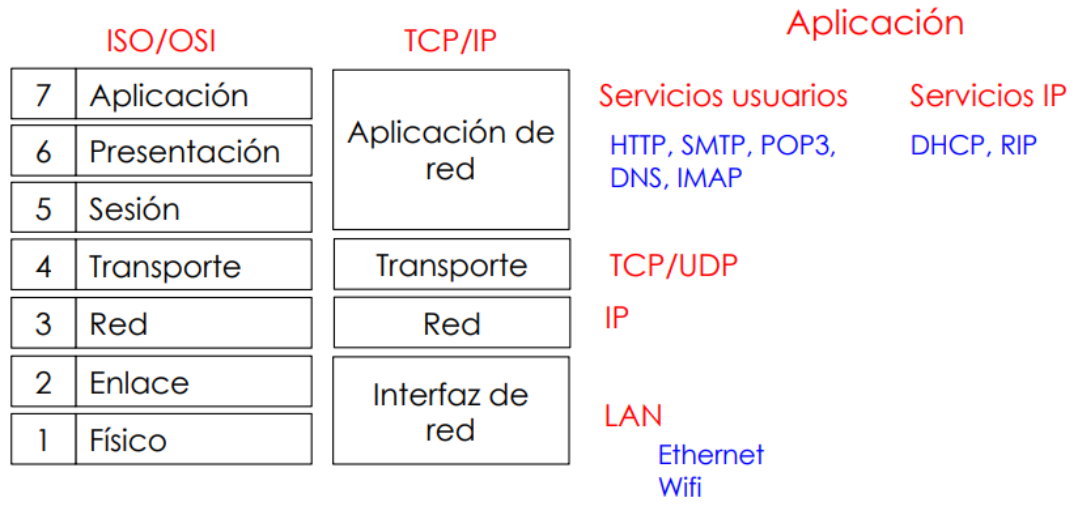
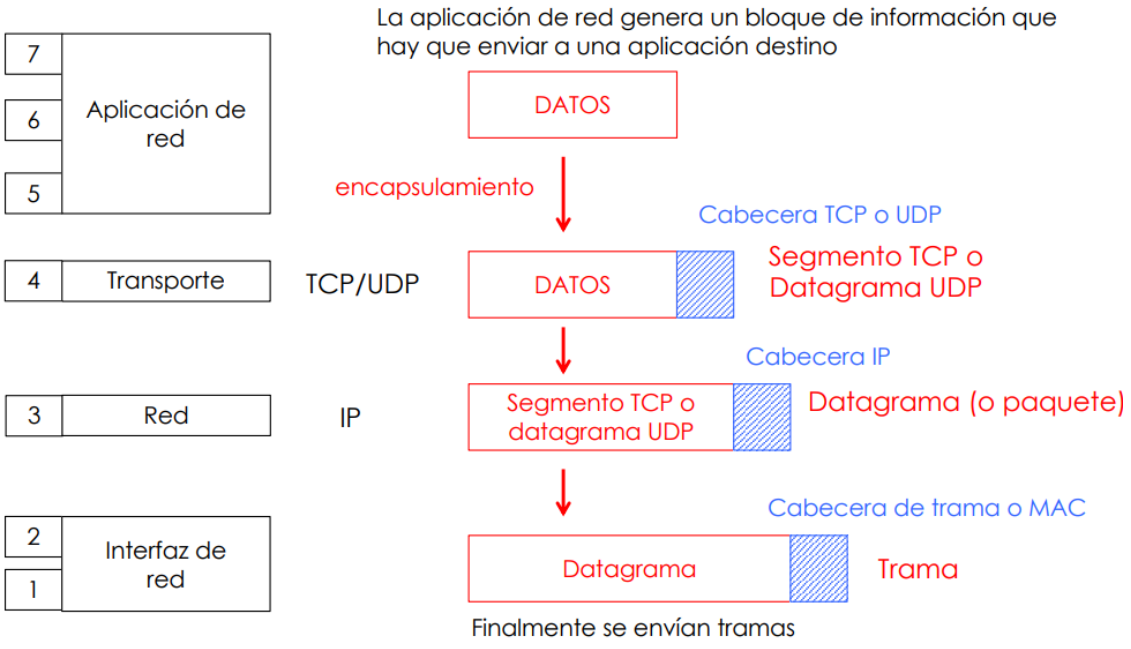
TEMA 1 INTRODUCCIÓN

ISO/OSI vs TCP/IP



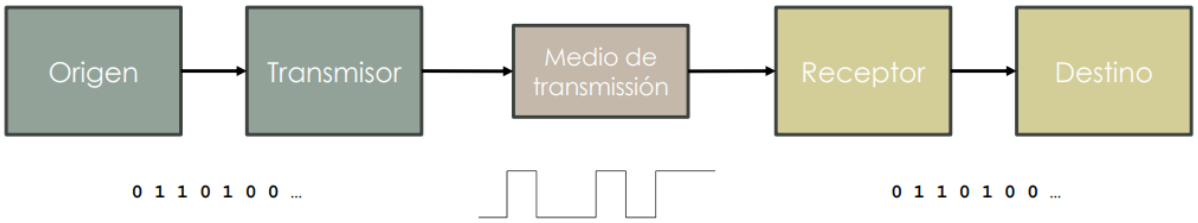


PC host ---> nivel 7
Router - - > nivel 3 (4 si se usa PAT o BGP)
Switch - - -> nivel 2
Hub - - - - -> nivel 1

Modelos de transmisión

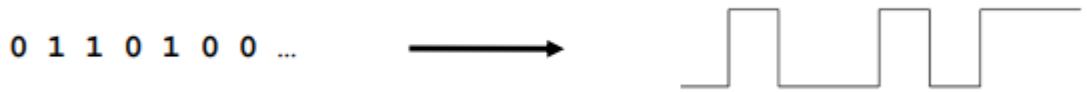
-> Simple

• Secuencia de bits del origen al transmisor.
• Señal electromagnética que se transmite por un medio de transmisión cableado o inalámbrico.
• Secuencia de bits del receptor al destino.



-> Codificación

Transformar una secuencia de bits en una señal electromagnética.



-> Multiplexación

Un medio de transmisión para más de una única transmisión.

- Time Division Multiplexing (**TDM**)
  Multiplexación por división de tiempo usada en Ethernet, WiFi, etc para evitar colisiones entre tramas.

- Frequency Division Multiplexing (**FDM**)
  Multiplexación por división de frecuencia. Dos señales se pueden transmitir al mismo tiempo si ocupan frecuencias diferentes.

  Modulación:
  Mover la señal a una frecuencia concreta para permitir FDM.

Transmisión de paquetes

-> Conmutación de circuitos

• Todos los paquetes circulan por un camino reservado entre origen y destino.
• Hay que establecer la conexión y reservar recursos (y luego liberar).
• Ventajas
    • Mismo camino para todos los paquetes -> llegan en orden, todo chill.

• Desventajas
    • Se necesita tiempo para establecer la conexión, si no se transmite, se están perdiendo recursos.

-> Conmutación de paquetes (como IP o red óptica opaca)

• No hay conexión establecida, se conoce el origen y el destino.
• Cada paquete se transmite independientemente.
• Los nodos deciden por dónde reenviar los paquetes según la tabla de forwarding.
• Ventajas
    • No se reservan recursos, más eficiente todo.

• Desventajas
    • Se pierde tiempo ya que se ha de almacenar cada paquete en los nodos y tomar una decisión. Encima, estos paquetes tienen + info para que estos sepan qué hacer cuando lleguen.
    • Los paquetes pueden llegar fuera de orden.

-> Conmutación de circuitos virtuales

• Cualquier origen puede usar una conexión para transmitir a un destino.

TEMA 2 Seguridad en las redes

Capa de aplicación -> cifrado, autenticación, integridad
Capa de transporte -> TLS
Capa de red -> Firewalls
Capa de enlace -> seguridad específica de la tecnología de nivel 2

Firewalls

• Un dispositivo o conjunto de dispositivos que está configurado para permitir o denegar transmisiones de red en función de un conjunto de reglas y otros criterios.
• ¿Qué puede hacer?
    • Más seguridad, acceso controlado.
    • Puede monitorear el tráfico entrante/saliente.
    • Puede limitar la exposición a una red insegura

• ¿Qué NO puede hacer?
    • Lo que pase dentro de la misma red segura, tráfico que no atraviesa
    • Errores/malas configuraciones de los servicios autorizados
    • Si la política de seguridad no es denegada por defecto, no puede proteger la red contra nuevos ataques

-> Tipos

Firewall a nivel de paquetes
Compara cada paquete con un conjunto de criterios establecidos (@IP, puertos, etc); si no cumple, es rechazado.
• Ventajas
    • Un solo dispositivo puede filtrar el tráfico de toda la red
    • Extremadamente rápido y eficiente en el escaneo del tráfico
    • Económico y uso muy limitado de recursos
    • Las reglas intuitivas y fáciles de configurar

• Desventajas
    • No controla el contenido de los paquetes
    • Puede ser inviable configurar reglas complejas
    • Un atacante podría descubrir las reglas de filtrado y hacerse pasar por un usuario legítimo

Firewall a nivel de circuito

• Se implementa en la capa de sesión del modelo OSI
• Inspecciona si el host remoto se considera confiable
• El Gateway no permite conexiones de un extremo a otro, en cambio configura dos conexiones
• Una vez establecidas las dos conexiones, el Gateway transmite paquetes de una conexión a otra sin examinarlos
• Ventajas
    • Sólo procesa las transacciones solicitadas
    • Fácil de configurar y administrar
    • Bajo costo

• Desventajas
    • No controla el contenido de los paquetes
    • No hay conexión extremo-a-extremo segura

Firewall a nivel de aplicación (Proxy firewall)

• Funciona en la capa de aplicación del modelo OSI
• Su función es bloquear o reenviar paquetes en función de la información de las capas de aplicación
• Ventajas
    • Examina todas las comunicaciones entre hosts externas e internos, verificando TODO (contenido tmb si)
    • Proporciona anonimato

• Desventajas
    • Puede ser muy costoso económicamente, compleja configuración
    • Puede no funcionar para todas las posibles aplicaciones
    • Las prestaciones se ven muy afectadas

Firewall con inspección de estados

• Examina cada paquete y registra los datos relevantes
• Inspecciona el tráfico de paquetes y compara el tráfico futuro con ese registro para validarlo.
• Esto ofrece más seguridad que el filtrado de paquetes o circuitos
• Ventajas
    • Supervisa toda la sesión para conocer el estado de la conexión
    • Efectivos contra ataques de tipo DDoS

• Desventajas
    • Consume muchos recursos, más caro que otras opciones de firewall
    • Interfiere con la velocidad de las comunicaciones
    • No suele proporcionar autenticación para validar que los hosts orígenes no sean falsificadas

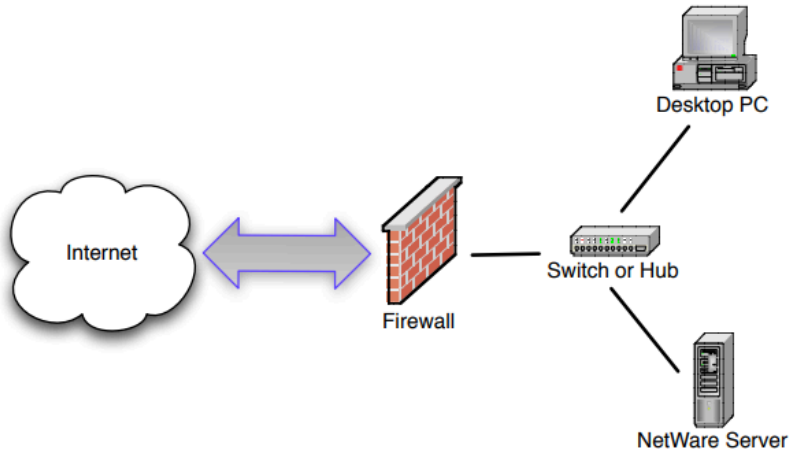
Firewall de próxima generación

• Filtrado de paquetes
• Inspección de estado + Inspección profunda de paquetes (DPI)
• Y otros sistemas de seguridad de red (IDS e.g), filtrado de malware y antivirus
• Ventajas
    • Hace un seguimiento del tráfico desde la capa de enlace hasta la aplicación.
    • Se puede actualizar automáticamente para proporcionar el contexto actual

• Desventajas
    • Proceso complejo al tener que integrarlo con más sistemas de seguridad
    • Más costoso que otros tipos de firewalls

-> Arquitecturas

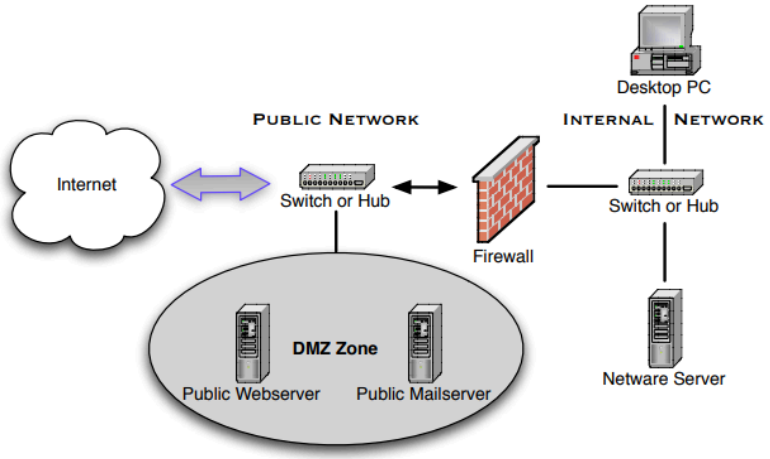
Dual - homed



• Ventajas
    • Muy fácil de configurar
    • Toda la red interna está protegida
    • Es suficiente un único firewall con solo 2 interfaces
    • La red interna puede usar direccionamiento privado

• Desventajas
    • No hay DMZ / O bien no se usan servidores públicos
    • O bien estos se ponen en la red interna con reglas específicas en el firewall. Esto puede ser crítico ya que son accesibles desde la red externa y los atacantes pueden saltar de un servidor comprometido a cualquier equipo interno sin control

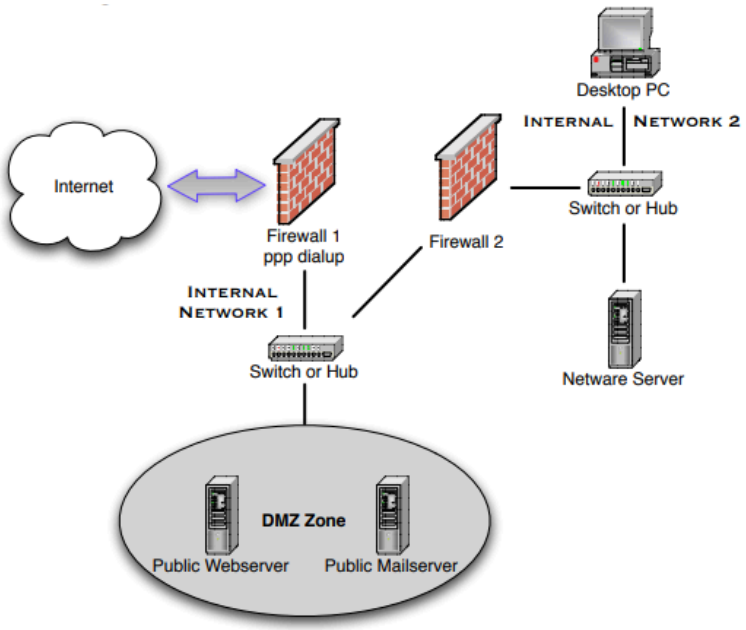
Two - Legged network with a full exposed DMZ



• Ventajas
  • Sigue siendo fácil de configurar
  • Toda la red interna está protegida
  • Es suficiente un único firewall con solo 2 interfaces
  • La red interna puede usar direccionamiento privado

• Desventajas
  • La zona DMZ está completamente expuesta
  • Esto puede ser crítico ya que son accesibles desde la red externa y los atacantes pueden saltar de un servidor comprometido a cualquier equipo interno sin control

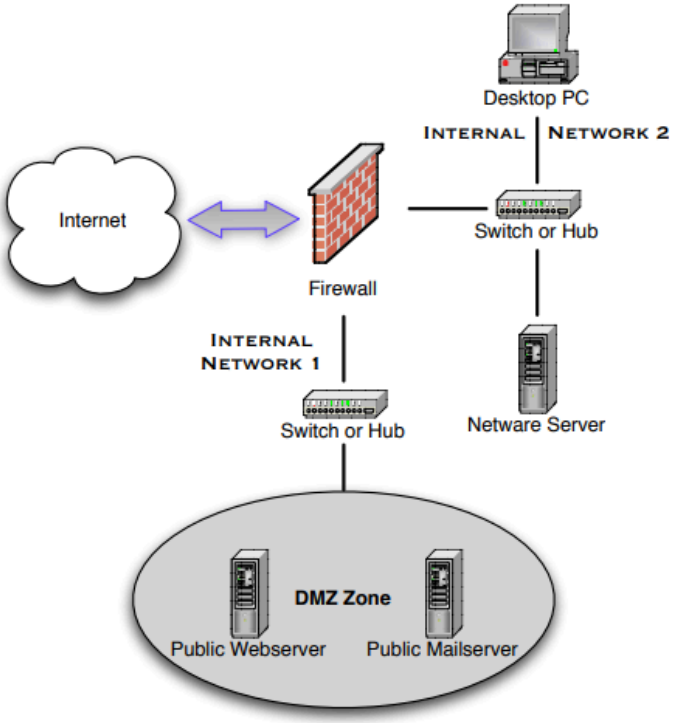
Restricted DMZ via Dialup Firewall



• Ventajas
  • Relativamente fácil de configurar
  • La red interna + DMZ está protegida, pueden usar direccionamiento privado

• Desventajas
    • Se necesitan 2 Firewalls
    • Se necesita mantener la configuración de los 2 Firewalls coherente

Three - legged firewall



• Ventajas
    • Se necesita un único Firewall
    • La red interna + DMZ está protegida, pueden usar direccionamiento privado

• Desventajas
    • Se necesita un Firewalls con 3 interfaces (coste)
    • Más complejo de configurar (más reglas)

TAMBIÉN SE PUEDEN COMBINAR, E.G 2 Y 4

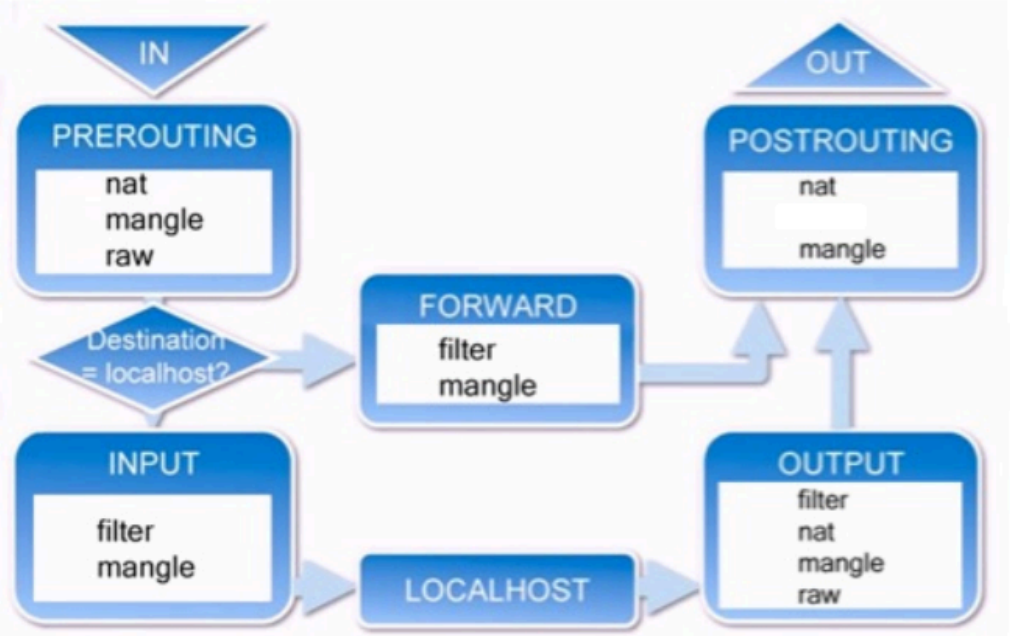
Hay otras soluciones como:
• **Dispositivos hardware ->** Dispositivos físicos que se instalan en las infraestructura de la organización
• **Host-based firewall ->** Firewall software que se instalan directamente en los hosts que se quieren proteger
• **Cloud-based firewall ->** Servicios en la nube
    • Costes reducidos
    • Se pueden combinar fácilmente con otros servicios de seguridad
    • Fácilmente actualizable a nuevas tecnologías
    • Fácilmente adaptables a nuevas amenazas

Reglas de filtrado -> iptables -> Firewall con inspección de estados

• Un conjunto de reglas secuenciales para denegar/permitir cierto tráfico de red según algunos criterios.

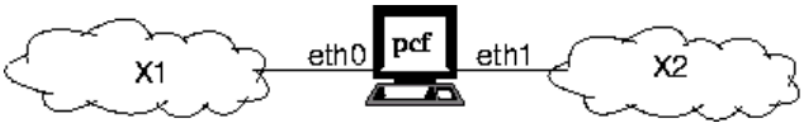
• Las reglas se agrupan en cadenas (chains)

• Las cadenas se agrupan en tablas (tables)



Básicamente, FILTER -> input, **forward**, output

NAT -> **prerouting**, output, **postrouting**

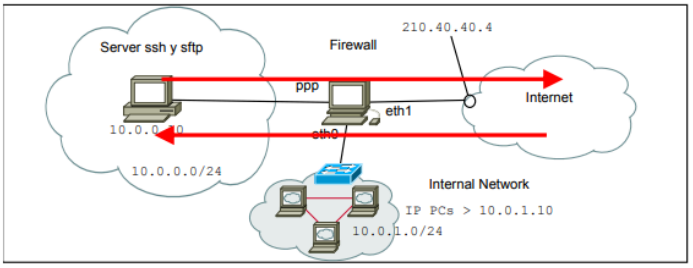


- Se quiere que los hosts de la red X1 puedan empezar una comunicación con los hosts de la red X2 (y estos puedan contestar) pero no viceversa

iptables –t filter –A FORWARD –i eth0 –o eth1 –j ACCEPT

iptables –t filter –A FORWARD –i eth1 –o eth0 –m conntrack –cstate ESTABLISHED –j ACCEPT

iptables –P FORWARD DROP

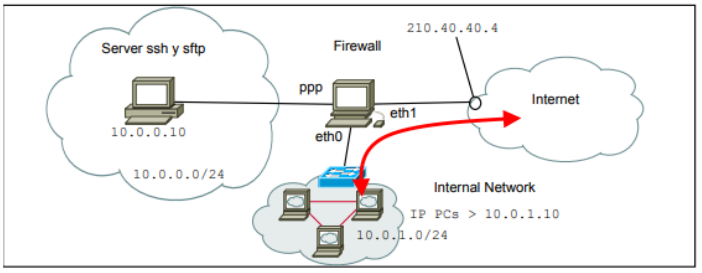


- Configurar el servicio NAT en el firewall para que la @IP del servidor 10.0.0.10 se vea en Internet como 210.40.40.4

iptables –t nat –A POSTROUTING –s 10.0.0.10 –o eth1 –j SNAT --to-source 210.40.40.4

iptables –t nat –A PREROUTING –d 210.40.40.4 –i eth1 –j DNAT --to-destination 10.0.0.10

NAT -> ip a internet -> hacer nat justo antes de transmitir -> POSTROUTING
internet a ip -> hacer nat lo antes posible -> PREROUTING



- Configurar el firewall para que los hosts de la red 10.0.1.0/24 tenga acceso al servicio HTTP de Internet y que este pueda solo contestar
- NAT dinámico: suponemos se reserva el rango 210.40.40.10-210.40.40.40

iptables –t nat –A POSTROUTING –i eth0 –o eth1 –s 10.0.1.0 0.0.0.255 –j SNAT
--to-source 210.40.40.10-210.40.40.40

- En este caso, no hace falta poner la vuelta ya que iptables mantiene estados e Internet ya solo podrá contestar (no puede empezar una comunicación)

Internet Protocol Security (IPsec)

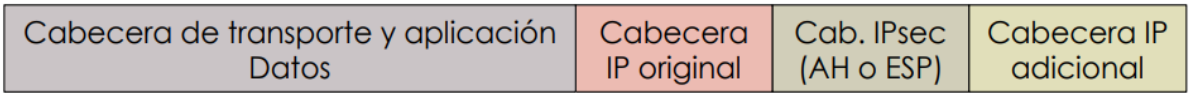
• Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre IP autenticando y/o cifrando cada paquete en la capa de red. Su uso más común es el servicio **VPN**. Puede proporcionar las siguientes protecciones:

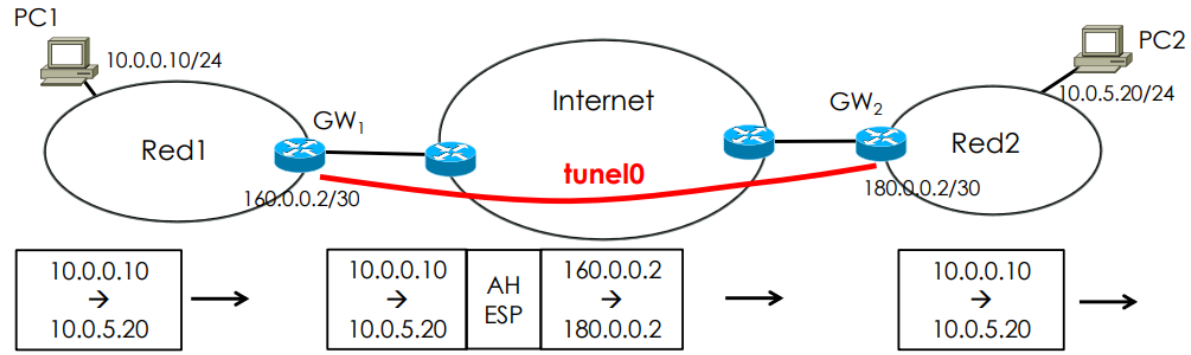
• Confidencialidad: el datagrama no puede ser leído por alguien no autorizado
• Integridad: puede saber si un paquete ha sido modificado durante la transmisión
• Autentificación: identificación de manera que los paquetes se están enviando entre los extremos correctos
• Protección de acceso: los extremos pueden filtrar para asegurar que solo los usuarios autorizados IPsec pueden acceder a recursos particulares de la red
• Protección de análisis de tráfico: una persona que monitoriza el tráfico no puede saber qué partes se están comunicando, con qué frecuencia se producen las comunicaciones o cuántos datos se intercambian

Modos de funcionamiento

Tunnel mode

• Se añaden la cabecera IP adicional + IPSEC
• Suele ser usada para GW-GW





Transport mode

• Se añaden la cabecera IP adicional solamente
• Suele ser usada para Host-Host
• Si los hosts usan IP privadas, los routers NAT traducen las IPs a públicas

Protocolos principales

Security Association (SA)

Se crea una asociación de seguridad habiendo establecido unos parámetros (AH/ESP? tunnel/transport?) de seguridad compartidos entre los dos extremos. Una vez establecido, se asocia a esta conexión un identificador Security Parameter Index (SPI). Existen varios protocolos que gestionan esto: Internet Key Exchange (IKE) y Kerberized Internet Negotiation of Keys (KINK)

Authentication Header (AH)

• Proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados sobre **todo el paquete**. Opcionalmente, también protección de acceso.
• Hay campos dinámicos en la cabecera IP -> la integridad se verifica excluyendo estos campos para no dar falsos positivos.
• Si se usa NAT -> NAT transversal.

Encapsulating Security Payload (ESP)

• Puede proporcionar autenticidad, cifrado e integridad.
• La cabecera del paquete IP no está protegida -> no hay problemas como AH. Se cifran **solamente** los datos y la cabecera IP original.

- Se establece una conexión IPsec permanente entre el gateway G_A y el G_B con ESP en modo Tunnel
  - G_A inicia una negociación con G_B para definir los parámetros de seguridad (entre otros, autenticación, integridad del payload y cifrado) y crear la SA con identificador SPI_{AB}
  - G_A usa los parámetros configurados en la SA para negociar la conexión IPsec. En este caso se usa ESP en tunnel mode

- Un usuario H_A del sistema A quiere enviar datos al usuario H_B del sistema B
  - H_A envía datagramas IP al H_B
  - La red del sistema A se ocupa de re-enviar los datagrama hacia G_A
  - G_A recibe los datagramas de H_A y ve que el destino está en el sistema B
  - G_A cifra los datagramas según los parámetros indicados en la SPI_{AB}
  - G_A añade una nueva cabecera IP (@IP origen G_A e @IP destino G_B) a todos los datagramas
  - G_A envía los datagramas por Internet con destino G_B

- G_B recibe el paquete y usa el SPI_{AB} de la cabecera ESP para reconocer la conexión segura
- G_B quita la cabecera IP adicional, comprueba la integridad del paquete y descifra el paquete original
- G_B envía el paquete a H_B

VPN

• Es un mecanismo para crear una conexión segura entre un dispositivo y una red, o entre dos redes, utilizando un medio de comunicación inseguro como es Internet
• Ventajas
    • Seguridad
    • Costes reducidos
    • Mayor flexibilidad para los trabajadores remotos

-> Tipos

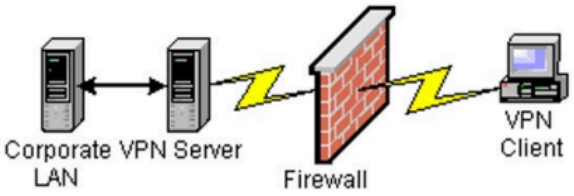
Gateway-to-Gateway (site-to-site)
• Comunicaciones de red seguras entre dos sistemas mediante el establecimiento de una conexión VPN entre los dos routers (gateways) de acceso de cada sistema.
• Se encamina a través de IPsec.
• Suele ser una conexión permanente

Host-to-Gateway (remote access)
• Acceso remoto seguro desde una red externa a los servicios internos de un sistema/empresa
• La conexión VPN la establece el usuario cuando la necesita
• Típicamente el gateway necesita una autenticación del usuario
• Es un modelo más complejo de gestionar y el gateway puede que necesite mantener un número elevado de conexiones VPN

Host-to-host
• La conexión la establece uno de los dos hosts.
• Este modelo es el único que proporciona seguridad extremo a extremo: los paquetes se quedan cifrado durante todo el recorrido
• Esto puede ser un problema, ya que los firewalls, IDS y otros dispositivos no pueden inspeccionar los paquetes, lo que puede provocar algo de inseguridad en la red interna

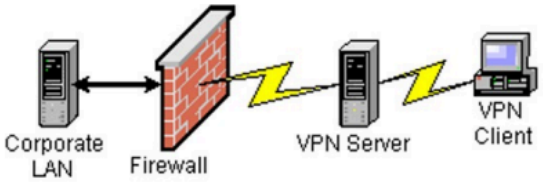
Firewall + VPN

-> VPN Gateway detrás del Firewall



- Ventajas
  - El VPN Gateway está protegido por el Firewall
  - La configuración es como un servidor más en la DMZ/red interna
- Desventajas
  - El Firewall no puede controlar el contenido de los paquetes
  - El Firewall necesita reglas de filtrado para dejar pasar el trafico VPN

-> VPN Gateway antes del Firewall



- Ventajas
  - El Firewall puede controlar que recursos internos son accesibles para clientes autenticados por el VPN Gateway
  - Si un atacante compromete el VPN Gateway, el Firewall puede aún actuar para bloquear este atacante
- Desventajas
  - El trafico entre el VPN Gateway y el Firewall no está cifrado

-> VPN Gateway y Firewall en un mismo dispositivo

- Ventajas
  - El Firewall puede controlar que recursos internos son accesibles para clientes autenticados por el VPN Gateway
  - Todo el trafico va cifrado
- Desventajas
  - Un único dispositivo para dos cosas
  - Único punto de defensa

Sistema de detección de intrusos (IDS)

• Hace una inspección profunda del contenido del tráfico de la red (también de paquetes (DPI)) para buscar, desviar y/o contrarrestar posibles ataques, incumplimiento de protocolo, etc.
• Un IDS activa alarmas o toma varios tipos de acciones automáticas.

- **Signature-based IDS**
  • Compara los patrones de actividad o tráfico que ven en los logs que están monitoreando contra esta base de datos. Si una regla coincide, se activa una alerta.
  • Problema: nuevos ataques no se pueden reconocer ya que no hay entradas en la base de datos.

- **Anomaly -based IDS**
  • Cuando se detecta una desviación del modelo, se envía una alerta.

+ **Network IDS (NIDS)**
  • Monitorea y analiza la actividad de la red en uno o más segmentos de la red.
    + En línea: el tráfico monitoreado debe pasar por sensor
    + Pasivo: monitorea una copia del tráfico de red real

  • Los NIDS pueden recopilar información sobre hosts y actividad de red para identificar usuarios, SO, aplicaciones o características de red.

  SNORT
  -> Signature-based.
  -> Aplicación de packet sniffer

Se quiere que salte una alarma cuando alguien intenta acceder a la web http://www.store-txc.com en la red 10.0.1.0/24

```
log TCP any any -> 10.0.1.10 80 (msg: "Acceso web"; contenido: "www.store-txt.com")
```

Se quiere bloquear un posible ataque del botnet Zeus a la red interna que tiene una firma conocida "5a 4f 4f 4d 00 00".

```
block TCP any any -> 10.0.0.0/24 any (msg: "Botnet Zeus"; contenido: "5a 4f 4f 4d 00 00")
```

+ **Host IDS (HIDS)**
  • Monitorea las características de un solo host y los eventos que ocurren en este host y busca alguna actividad sospechosa.
    + Honeypot: Simula una vulnerabilidad de un host o red. El atacante ataca este señuelo pensando haber encontrado un hueco para acceder a un sistema.

+ **Distributed IDS (DIDS)**
  Un gestor recibe toda la información de los sensores HIDS y NIDS, este la analiza y decide en tiempo real.

TEMA 3 Redes troncales

Multiprotocol Label Switching (MPLS)

• Para agilizar y acelerar el proceso de consulta y toma de decisión de tablas de forwarding en los routers con la ayuda de etiquetas. Nivel 2,5, funciona por defecto con PHP.
• También proporciona ahora
    • Servicio VPN
    • Servicio de agregación de rutas
    • Mecanismos de búsqueda rápida de caminos alternativos en caso de fallo
    • Ingeniería de Tráfico (TE)

Tabla de routing -> muchas entradas

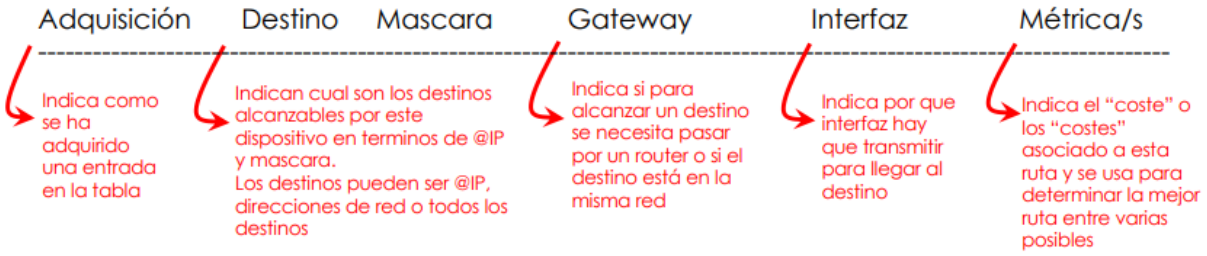
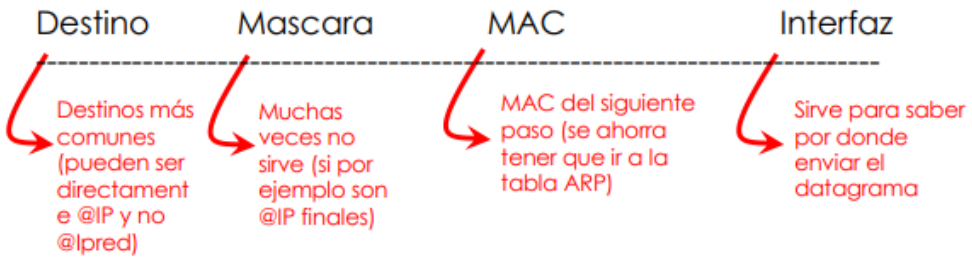
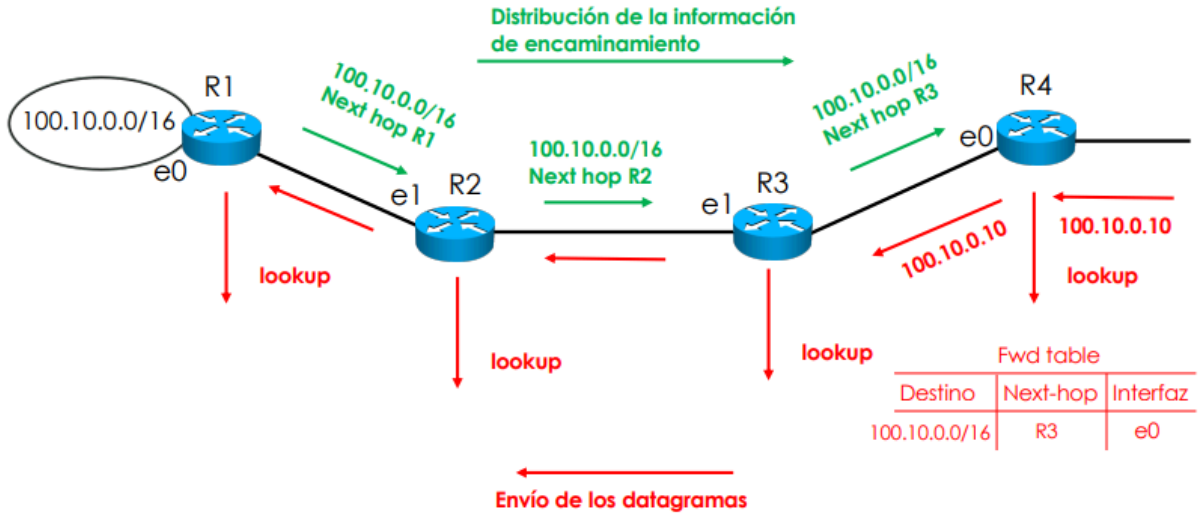
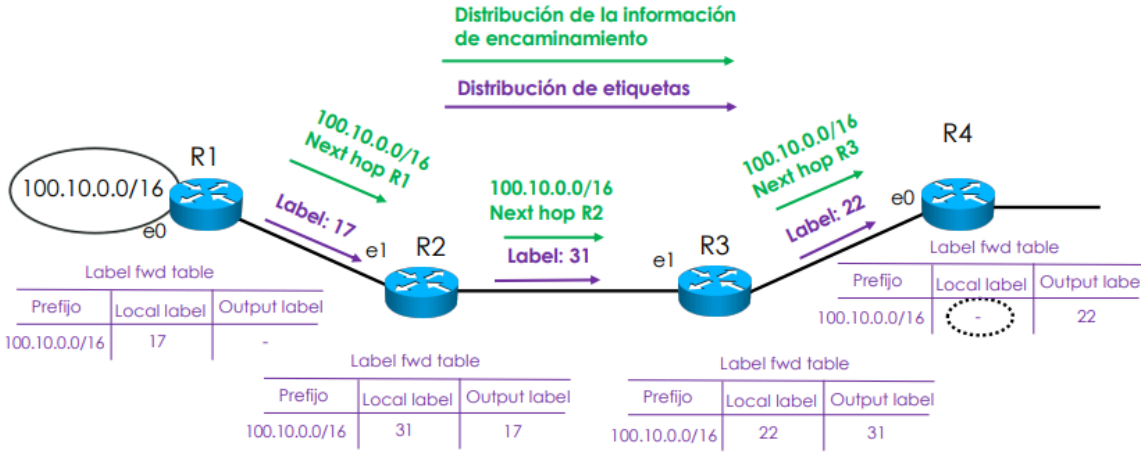


Tabla de forwarding -> otros campos useless si queremos algo más rápido





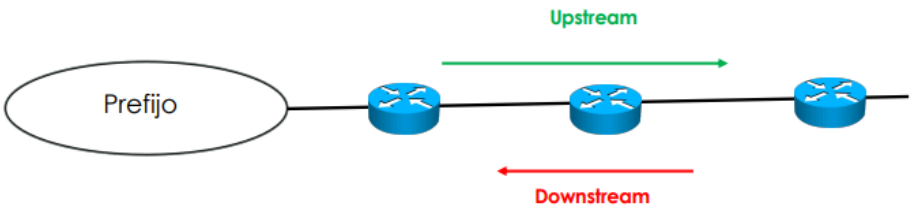
• Las etiquetas tienen un significado local para cada pareja de routers MPLS
• Un router MPLS consulta una tabla de etiqueta para reenviar los paquetes MPLS
• Solo los routers de frontera de esta zona MPLS necesitan hacer un IP route lookup
• A través de estas etiquetas, se construyen caminos MPLS llamados Label Switched Path (LSP)

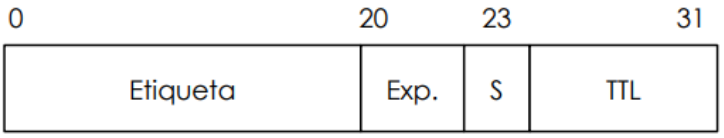


- En este caso, R4 es el último router donde se usa MPLS
- No hay etiqueta local

- Control Plane
  - Proporciona la funcionalidad de identificar los prefijos alcanzables y como
  - Protocolo de encaminamiento como OSPF o RIP
  - Protocolo de distribución de etiquetas como LDP o RSVP
- Data Plane
  - Proporciona la funcionalidad de reenviar datagramas (forwarding)
- Label Switch Router (LSR)
  - Un router MPLS que trata datagramas MPLS, sabe hacer label pop, push y swap
- Edge LSR (E-LSR) o Label Edge Router (LER)
  - Un LSR en la frontera de una infraestructura MPLS
  - Un ingress E-LSR hace label push
  - Un egress E-LSR hace label pop
- Label Switched Path
  - Un camino MPLS entre un ingress E-LSR y un egress E-LSR

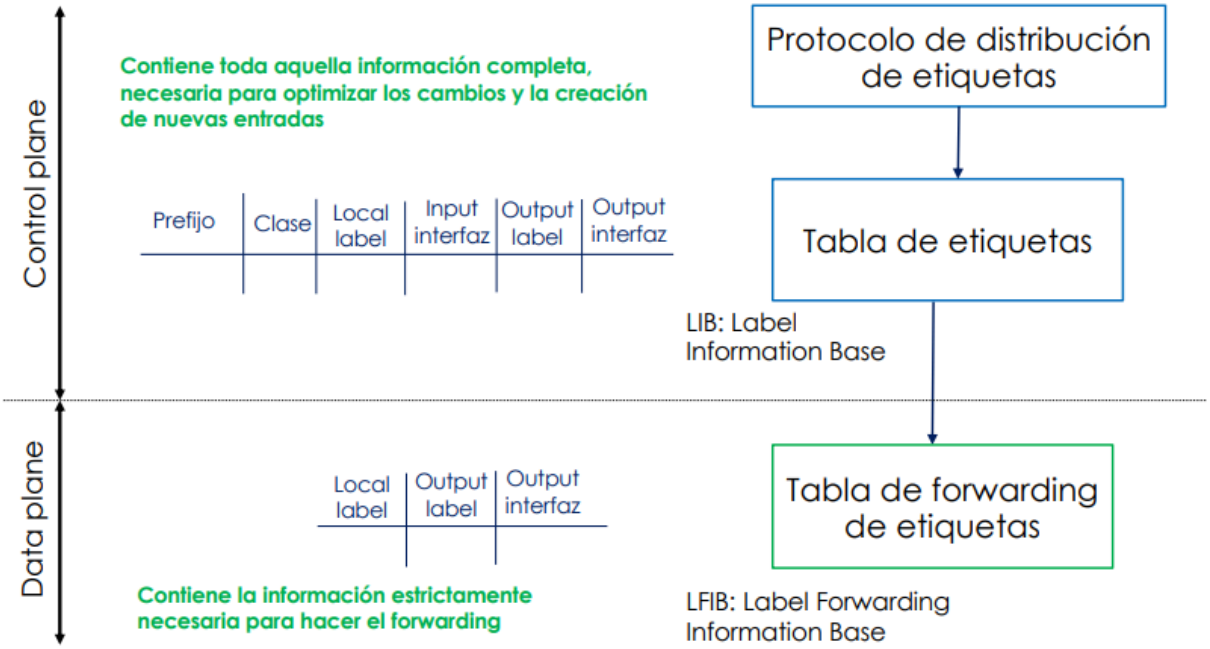
- Upstream
  - Sentido por donde va la información de encaminamiento y de distribución de etiquetas a partir de un prefijo
- Downstream
  - Sentido por donde circulan los datagramas de datos hacia un prefijo

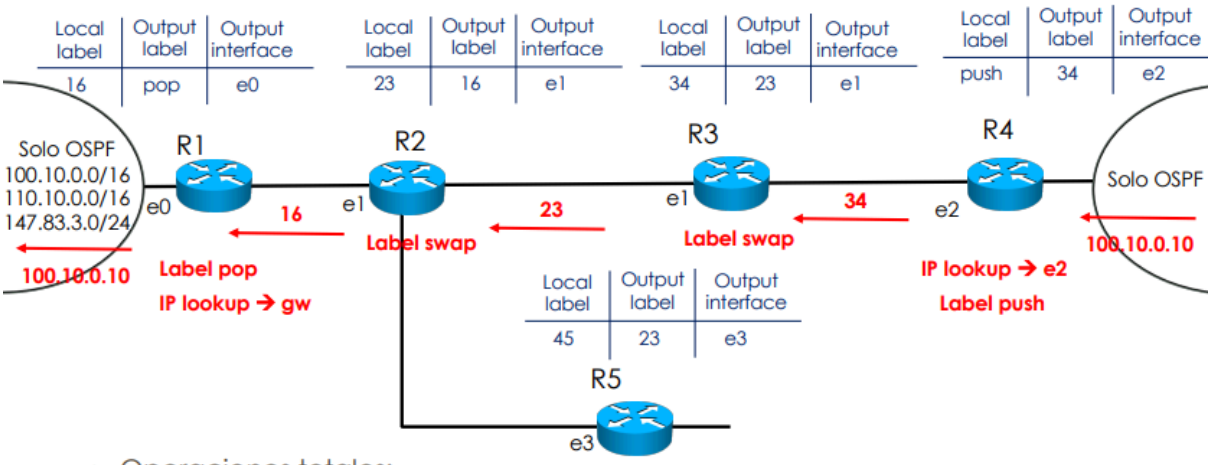




- Etiquetas (20 bits)
  - Los valores de 0 a 15 están reservados para funciones particulares
- Exp. (3 bits)
  - Campo experimental usado con la idea de definir prioridades diferentes
  - No se suele usar
- S (1 bit)
  - Se usa para poder encapsular cabeceras MPLS dentro de otro MPLS
  - Función que se llama label stack
  - Cuando el valor es 0, quiere decir que hay otra etiqueta interna
  - Cuando es 1, es la última cabecera

- TTL (8 bits)
  - Tiempo de vida del datagrama MPLS
  - Funciona igual que en IP
  - Sirve para que un datagrama perdido no se quede en la red eternamente
  - El origen pone un valor; cada router reduce el valor de 1; si el valor llega a 0, el datagrama se tira





- Operaciones totales:
  - 2 IP lookup
  - 1 label pop
  - 1 label push
  - 2 label swap

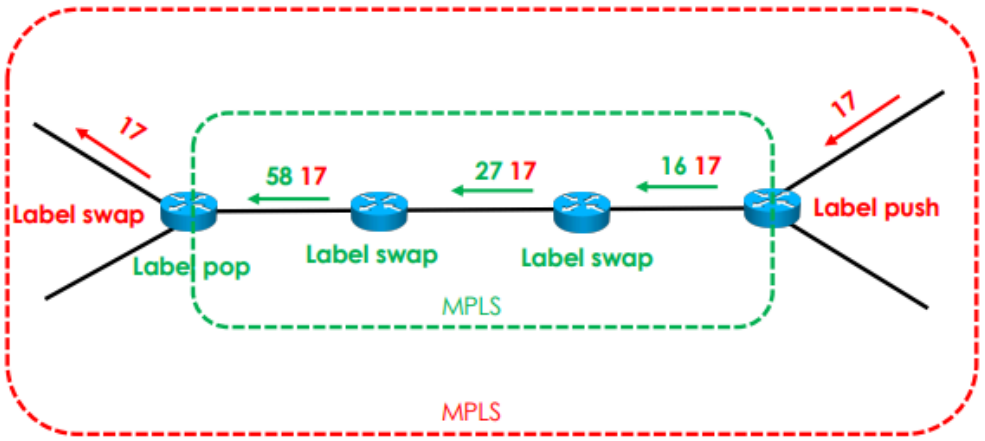
Mejora: Penultimate Hop Popping (PHP) -> poner pop en R2 para que cuando llegue a R1 haga pop directamente y se ahorre un label swap.

Servicio VPN

• Se puede añadir un servicio de autenticación antes de establecer un LSP
• Los paquetes encapsulados con MPLS se pueden cifrar, los routers intermedios necesitan tomar decisiones solo sobre las etiquetas
• Se puede añadir integridad de los paquetes encapsulados con MPLS

Label stack

Una zona MPLS puede encapsular otra zona MPLS. Agregación de caminos LSP.



Local label	Output label
58	pop
→ 17	23
18	47

Local label	Output label
27	58

Local label	Output label
16	27

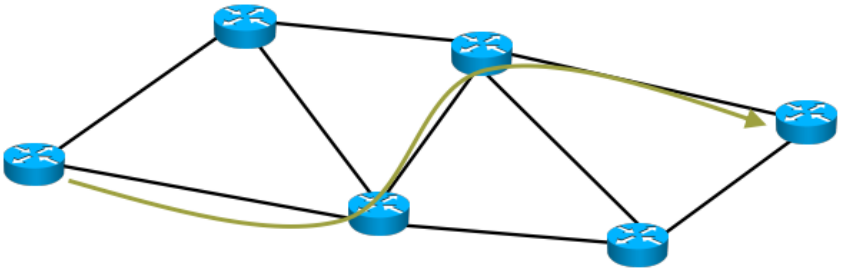
Local label	Output label
17	push
18	push
push	16

Recuperación de fallos

En redes IP hay que recalcular los caminos y las entradas y puede ser muy lento este método de tipo reactivo. En cambio en redes MPLS, usando un método de tipo proactivo es más rápida la convergencia ya que se calculan caminos alternativos desde el principio que se activan solo cuando se detecta un fallo.

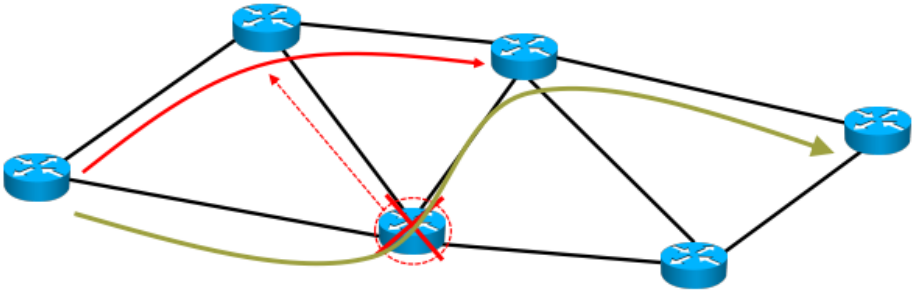
-> Protección del enlace

Cada enlace se protege con un LSP de backup.



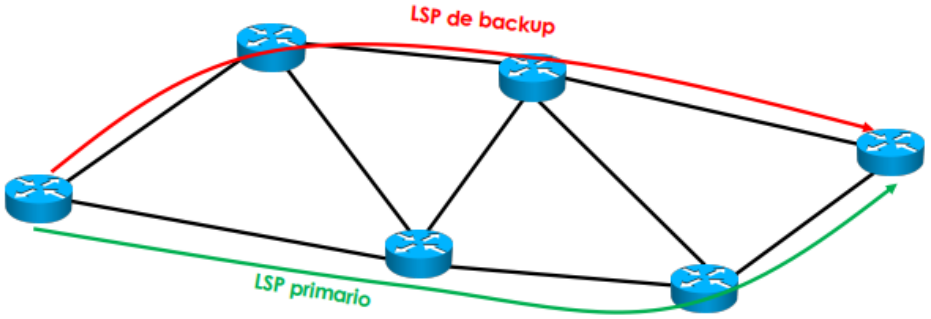
-> Protección del nodo

Cada nodo (router) se protege con un LSP de backups



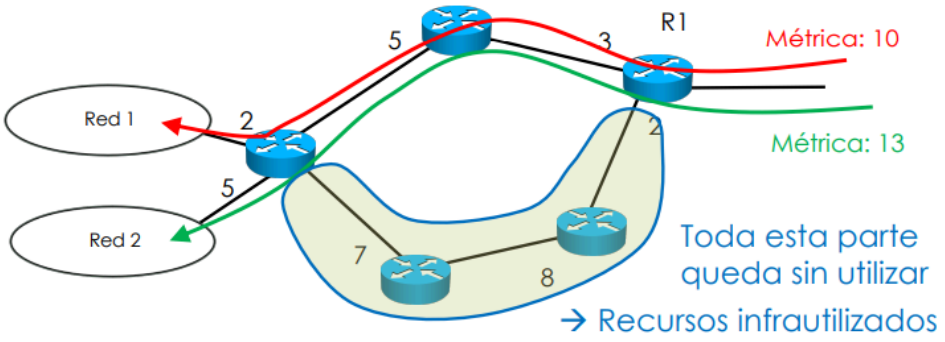
-> Protección del LSP

A la hora de establecer un LSP (llamado primario), se crea otro de backup que no debe compartir ningún enlace o nodo con el primario (excepto origen y destino)

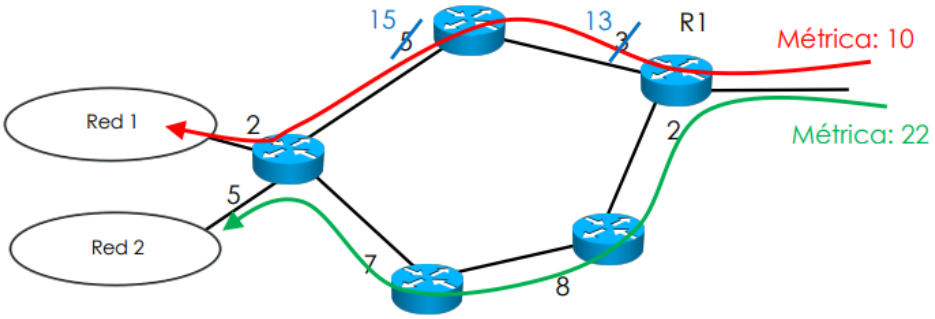


Traffic Engineering

Si nunca se usan son recursos infrautilizados -> métricas dinámicas.



Ahora al establecer tráfico de R1 a la red 1, cambian las métricas:



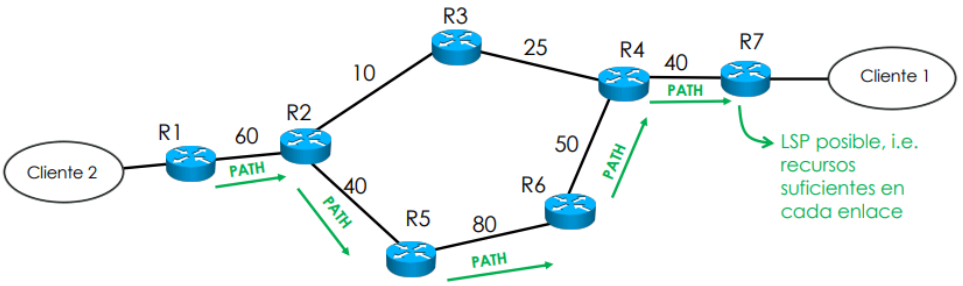
Para que esto funcione:

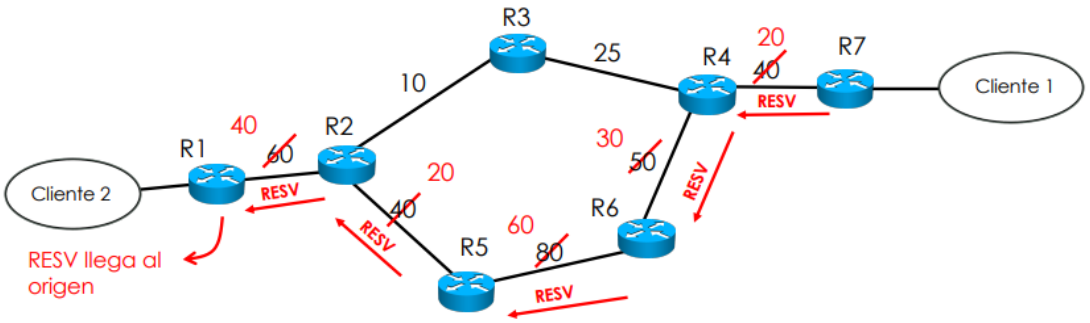
- Protocolo de encaminamiento dinámico que permita el envío de cambios de métrica.
- MPLS
- Constraint-Based Routing (**CBR**)

CBR

- Un cliente pide sus requisitos para su LSP(s).
- Se usa un algoritmo CBR para determinar los caminos óptimos.
- Está basado en restricciones. Dados los requisitos busca el mejor camino que proporciona, como mínimo, estos requisitos.

  PATH para ver si hay suficiente recurso y se reserva en caso de que sí.
  Si no hay -> PATH_error. Luego se puede volver a intentar con menos recurso u otro camino.





RESV -> hace efectiva las reservas, define las etiquetas locales y las entradas en las tablas MPLS. Se ha creado entonces el LSP, y se anuncian los cambios.

Redes ópticas

• El núcleo (core) es donde pasa la señal óptica
• El cladding mantiene la señal óptica en el núcleo
• El revestimiento externo (coating) sirve para proteger la fibra

- Fibra óptica
  - Baja atenuación (un amplificador cada 60/100 km)
  - Ancho de banda muy grande (> 1 Pbit/s)
  - Coste bajo
  - Resistencia a las interferencias
  - Mejor durabilidad
- Cable de cobre
  - Alta atenuación (un amplificador cada pocos km)
  - Ancho de banda limitado (10 Gbit/s)
  - Coste del cobre muy elevado
  - Subjeto a interferencias electromagnéticas
  - Baja durabilidad

• Va de acuerdo a la longitud de onda (nm) de la transmisión. Hay bandas diferentes. Se usó primero la O, actualmente se usan las bandas C y S, y la idea es usarlas todas.
• Estas bandas tienen mucha capacidad -> se dividen en “canales” de 50 GHz, que cada canal se pueda usar para cada transmisión. Se parece a FDM.
Así que básicamente la fibra óptica es la multiplexación por división de longitud de ondas (**WDM**) y cada canal puede ir a 2,5, 10, 40, 100, 400 Gbit/s.
• Hay unos 80-160 longitudes de onda/canales por fibra.
• La señal transmitida es óptica, no existen aún routers y switches ópticos -> cómo se encamina la información? **Redes opacas & redes transparentes.**

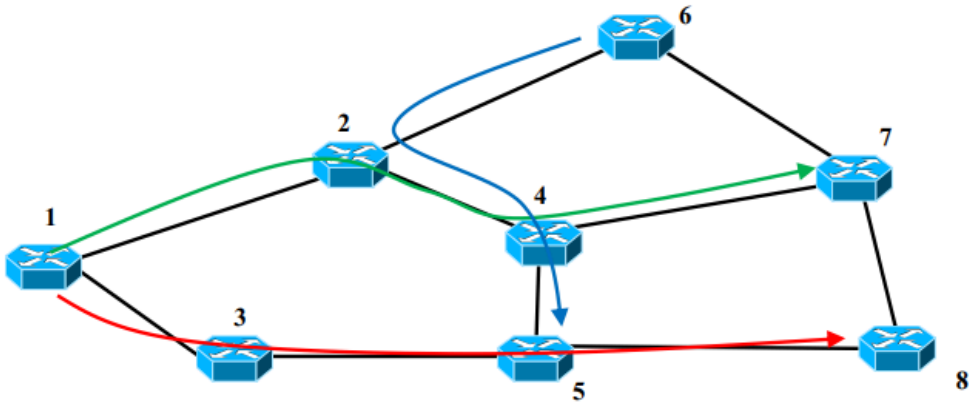
Redes opacas

• La capacidad óptica solo se usa para transmitir:
• Cada router/switch (nodo)
    • **Traduce** la señal en eléctrica
    • Almacena el paquete en memorias eléctricas
    • Procesa el paquete para tomar una decisión
    • Mueve el paquete a la interfaz de salida
    • Convierte el paquete en una señal óptica
    • Transmite la señal óptica al siguiente nodo
• Inconvenientes
    • Muchas conversiones, muy lento, muy ineficiente.

Redes transparentes

• Mantener la señal en óptico desde el nodo origen hasta el nodo destino
• Cada router/switch (nodo)
    • Debe decidir qué hacer con una señal sin pararla ni procesarla ni transformarla.
    • **Decidir qué hacer según la longitud de onda de la señal**
    • Los nodos usan una matriz de conmutación programable desde la unidad de control. Permite conectar una interfaz de entrada a una de salida según la longitud de onda de la señal, aunque hay que configurarla antes que llegue la transmisión
    • No es una operación rápida (ms/s) pero sí rápida respecto a la velocidad a la cual llegan los paquetes (en ns)
    • Se crean de esta forma caminos totalmente ópticos llamados **lightpaths.**

- Router 4
    - Si llega una señal con una longitud de onda verde, este ya debe estar configurado previamente para reenviar automáticamente toda la señal hacia el router 7
    - Si llega una señal con una longitud de onda azul, esta señal debe ir hacia el router 5

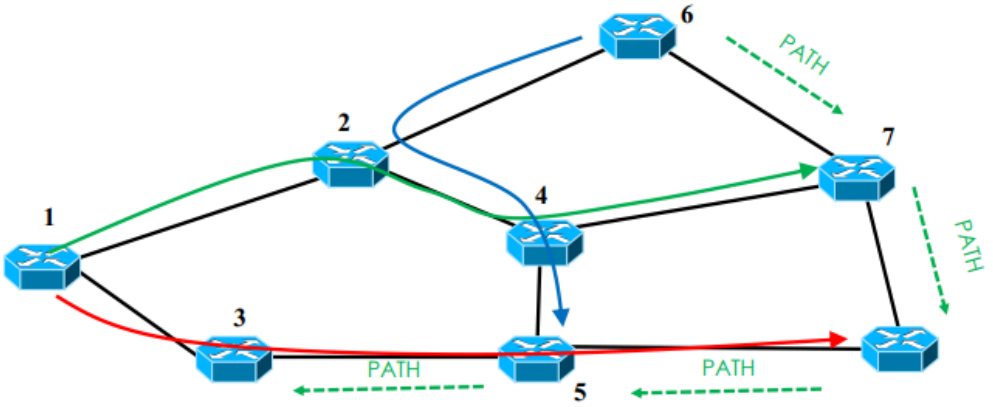


• Una transmisión desde un origen hasta el destino debe mantener la misma longitud de onda durante todo el camino
• No puede haber dos transmisiones diferentes en el mismo enlace con la misma longitud de onda (dos tramos verdes en un mismo tramo e.g).
• Los nodos usan los algoritmos Routing and Wavelength Assignment (**RWA**)
    • Routing porque se necesita encontrar un camino disponible entre origen y destino
    • Wavelength porque hay que encontrar una longitud de onda disponible enteramente entre origen y destino

Generalised Multiprotocol Label Switching (GMPLS) -> conm. circuitos

• Sirve para crear y gestionar los lightpaths en redes ópticas.
• Usa un protocolo de encaminamiento que mantiene la información actualizada en cada router sobre las longitudes de onda disponibles en cada enlace
• Usa una familia de algoritmos RWA que funciona basados en restricciones
• Usa el intercambio de etiquetas para crear y verificar los caminos ópticos

- El router 6 quiere establecer un lightpath hacía el router 3
- El router 6 consulta su base de datos y ejecuta el RWA
- RWA le dice que el mejor camino es 6-7-8-5-3 usando el verde
- El router 6 lanza el intercambio de labels para crear el lightpath



PATH es para revisar que sí se puede, después RESV la reserva definitiva y la creación de labels.

PCE

• RWA es un problema NP-completo así que se creó Path Computation Element (PCE), eliminando el cómputo de RWA de los nodos y asignando esta tarea a un elemento externo dedicado exclusivamente en calcular el RWA.
• PCE está conectado con todos los nodos y conoce el estado del sistema.
• Si algún router necesita algún camino, le pregunta cuál es el mejor lightpath. Este ejecuta el RWA y se lo dice.
• Luego se sigue haciendo PATH y RESV.

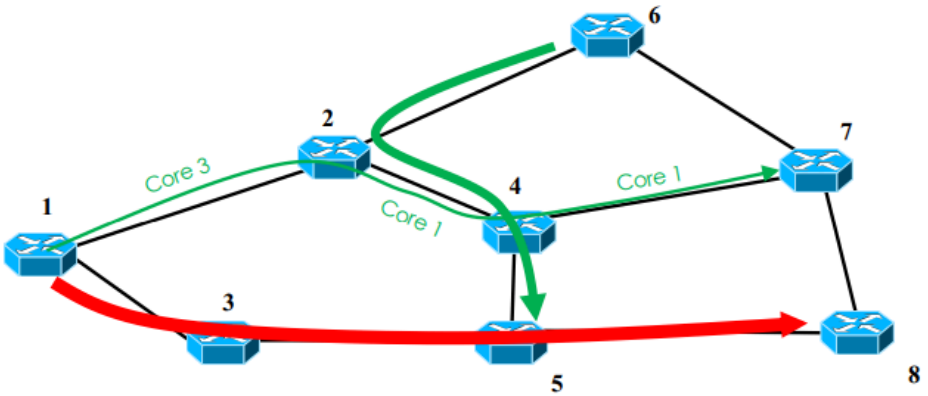
Redes transparentes flexibles

• Cuanto más rápido se quiere ir, más ancho de banda ocupan las señales.
• El espacio de los canales se hace flexible y se adapta a la señal transmitida
• Se usan algoritmos llamados Routing and Spectrum Assignment (**RSA**)
    • Routing porque se necesita encontrar un camino disponible entre origen y destino
    • Spectrum porque ahora hay que encontrar una espacio de espectro de banda disponible enteramente entre origen y destino
    • También es NP-Completo -> PCE.

Fibras multi - core

• Hay múltiples núcleos pero un solo cladding en cada fibra
• Cada núcleo es “independiente” de los otros y se puede usar para transmitir como si fuera una fibra separada
• ¿Qué núcleo usar? Routing, Spectrum and Core Assignment (**RSCA**)
    • Routing porque se necesita encontrar un camino disponible entre origen y destino
    • Spectrum porque hay que encontrar una espacio de espectro de banda disponible enteramente entre origen y destino
    • Core porque ahora hay que encontrar cual de los núcleos de la fibra usar. En este caso pero, el core seleccionado puede modificarse al pasar por un nodo
    • También es NP-Completo -> PCE.

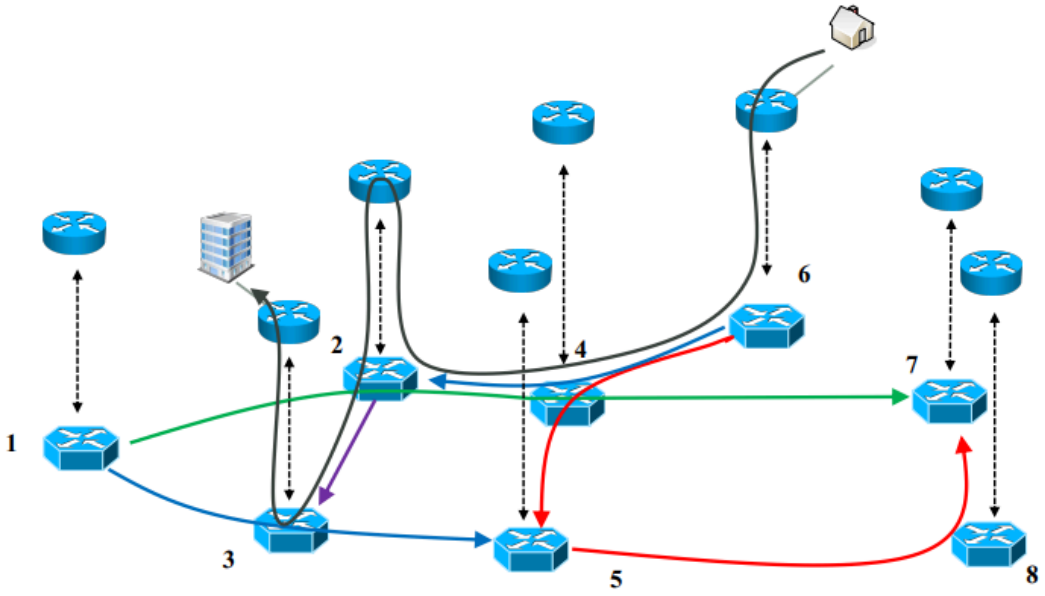
- En cada enlace, se puede usar el mismo canal usando núcleos diferentes
- Además un nodo puede conmutar de un núcleo a otro para un mismo lightpath



Redes multi - capas

• Ahora la parte óptica crea caminos de determinadas velocidades entre un nodo origen y un nodo destino. Estos caminos son lentos de establecer.
• Todo eso implica que esta parte óptica sirve para crear grandes autopistas para transmitir grandes cantidades de información durante mucho tiempo
• Encima de estas autopistas (lightpaths) se crean las entradas

- La red **óptica** transparente se ve simplemente como una red de conexiones a alta velocidad entre determinados nodos
- Todos estos nodos son completamente ópticos
+ La red superior es la red de agregación que junta los flujos
+ Estos nodos suelen ser opto-eléctricos



Plan de control/gestión

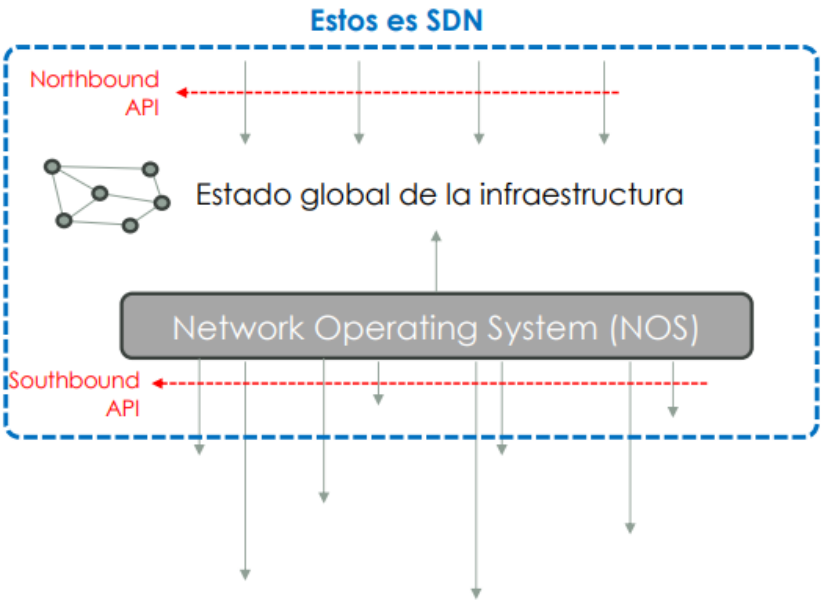
• **Plan de control**
    • Generalmente un sistema semiautomático
    • **Se ocupa de hablar con los equipos de red**
    • Configura los equipos según las conexiones necesarias
    • Involucra: protocolos de encaminamiento, cálculo de la ruta, protocolo de intercambio de etiquetas, protocolos de descubrimiento de fallos
• **Plan de gestión**
    • Generalmente un sistema manual
    • Se ocupa de comprobar el **correcto funcionamiento** de la infraestructura según las expectativas de los **clientes**
    • Implementa funciones de telemetría (prestaciones), seguridad, contabilidad, mantenimiento, etc.

1) Un cliente pide un servicio al plan de gestión
2) El plan de gestión acepta el cliente
3) El plan de gestión encarga el plan de control de actuar
4) El plan de control determina como proporcionar el servicio hablando con los equipos de red
5) El plan de control proporcionar el servicio y se lo dice al plan de gestión
6) El plan de gestión informa el cliente
7) El plan de gestión mantiene el servicio y verifica las prestaciones

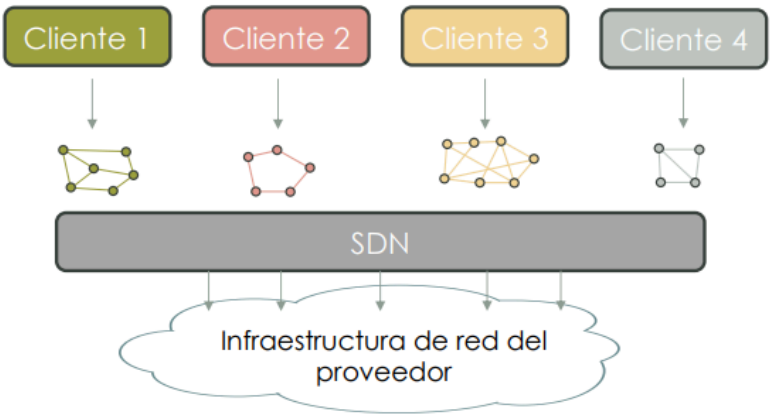
Plan de control redes multi-capa

- El plan de control incluye para una red multi-capa:
  - Plan de control de la parte IP/MPLS
  - Plan de control de la parte óptica (GMPLS)
- Los dos necesitan
  - Protocolo de encaminamiento dinámico
    - intercambio de información sobre el estado de la red en tiempo real
  - Calculo de la mejor ruta CBR
    - Puede estar en el PCE (enfoque centralizado) o ejecutarse en cada nodo (enfoque distribuido)
  - Protocolo de intercambio de etiquetas y creación de la ruta
  - Protocolo de recuperación en caso de fallo de la ruta

• La interoperabilidad entre fabricantes diferentes, aunque las tecnologías y los protocolos sean estándares, se convierte en una tarea inviable
• El resultado es que cada proveedor de red solía comprar equipos de un único fabricante. Solución? Software Defined Network (**SDN**)
  • Usar una interfaz abierta (**API**) común para la configuración de los equipos
  • Añadir una capa de abstracción y un control centralizado
  • Hacer la red programable según determinadas aplicaciones de red



- Permite la virtualización de la infraestructura del proveedor
- Clientes ven "su parte" de la infraestructura, aislada de los demás clientes
- Esta operación se llama Network Slicing



• Permite la interoperabilidad entre infraestructuras diferentes a través de un orquestador

Software Defined Network (SDN) - Desventajas

- Seguridad
  - Se añade una capa adicional subjeta a ataques
  - Muy critica ya que controlan toda la infraestructura
- Coste
  - El personal necesita ser formado
  - Hay que cambiar los equipos de red para que permitan esta Southbound API
- Prestaciones
  - Un control centralizado puede tener problemas de escalabilidad
- Tiempo
  - Se necesita desarrollar y desplegar SDN en todo el sistema