Diseño de redes WAN y nuevas tecnologías

PID_00268541

Pere Barberán Agut

Tiempo mínimo de dedicación recomendado: 7 horas

Universitat Oberta de Catalunya

Pere Barberán

Ingeniero de Telecomunicaciones por la Universidad Politécnica de Cataluña. Profesor de la Escuela Universitaria Politécnica de Mataró donde forma parte del Área de Redes y Servicios. De 2005 a 2010 ha sido director del Departamento de Telecomunicaciones y Arquitectura de Computadores. Actualmente responsable del laboratorio de *networking* TCM NetLab en la Fundación Tecnocampus Mataró-Maresme.

La revisión de este recurso de aprendizaje UOC ha sido coordinada por el profesor: Ferran Adelantado Freixer (2019)

Segunda edición: septiembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

El *boom* de Internet ha provocado que el modelo de transporte de datos que utilizan las operadoras de telecomunicaciones en el núcleo de sus redes haya ido quedando obsoleto en el transcurso de estos últimos años. Eso ha llevado a trabajar en el desarrollo de nuevas tecnologías de red y protocolos de comunicación que hagan posible lindar con garantía de éxito el crecimiento de las necesidades de transporte de datos y los requisitos de los servicios previstos para el futuro.

Por otra parte, en el ámbito de la empresa estar conectado a Internet ha sido un imperativo, de manera que la sociedad actual está marcada por medidas asociadas a Internet y a su rápida evolución en el tiempo. Eso obliga a las organizaciones a desarrollarse y a reaccionar de manera rápida. Estos hechos provocan que el diseño de las redes, que habrían de hacerse de manera óptima, escalable, segura, disponible, etc., acaben realizándose con la falta de alguna de estas características básicas, o de todas. Esta ausencia acaba siendo un factor crítico dentro de la infraestructura.

Así, este módulo didáctico se puede dividir en dos partes bien diferenciadas. En la primera parte se ven los elementos básicos que tenemos que plantearnos cuando queremos realizar un buen diseño de red. El análisis de redes, la arquitectura y el diseño han sido tradicionalmente considerados un arte en el que se combinaban reglas particulares en la evaluación y la elección de las tecnologías de red. De este modo, el éxito o el fracaso de un diseño de red particular dependía básicamente de quien estaba realizando el trabajo. Hoy en día, en cambio, las redes forman parte del trabajo y por lo tanto se consideran elementos críticos. Eso hace que tanto la arquitectura como el diseño de red deban ser lógicos y reproducibles, y que se puedan defender. Esta parte por sí sola podría ser un libro entero, de manera que lo que se pretende es mostrar sólo los principios básicos en el diseño de redes.

En la segunda parte del módulo nos centramos en nuevas tecnologías. Empezamos con el protocolo IP y su evolución a IPv6. Más adelante, se intentan ver las diferentes tendencias actuales en redes metropolitanas y redes de área extendida. En el primer caso se explica cómo Ethernet va más allá actualmente de la red local. En el caso de las redes de área extendida se explican, por un lado, los usos que se le suele dar a la tecnología MPLS y, por otro lado, una nueva tendencia cada vez más importante, como es el Software-Defined WAN (SD-WAN).

Objetivos

Los materiales didácticos de este módulo os debe permitir que alcancéis los siguientes objetivos:

1. Entender que un buen diseño de red es básico para tener éxito en la implementación que se desarrolle.

2. Conocer los principios básicos que hay que seguir cuando se realiza un diseño de red.

3. Conocer los elemenos básicos para realizar una buena planificación IP, la cual debe permitir un correcto diseño lógico de la red.

4. Comprender la evolución de los requisitos actuales para las nuevas redes metropolitanas.

5. Estudiar las diferentes tecnologías actuales en entornos metropolitanos y justificar la evolución hacia las redes metropolitanas Ethernet.

6. Conocer el funcionamiento básico del protocolo IPv6 y, en especial, su direccionamiento.

7. Conocer la evolución más importante de la tecnología MPLS para dar calidad y servicio.

8. Comprender el nuevo enfoque basado en menos hardware para implementar las redes WAN mediante SD-WAN.

1. Diseño de redes

1.1. Introducción al diseño de redes WAN

Red de área extendida, en inglés *wide area network* (WAN).

Antes de empezar quizás haya que dejar claro que no hay una única posibilidad desde la idea inicial hasta la implementación real en el diseño de redes de área extendida (WAN).

Lo que pide el cliente al final es una red WAN lo más rápida posible sin perder de vista las restricciones, es decir, que trate los datos de forma fiable, segura y a un coste razonable.

Para conseguir estos principios básicos, pero a la vez lógicos, podemos empezar haciéndonos una serie de preguntas:

- ¿Es una instalación nueva o estamos sustituyendo una infraestructura existente?
- Si ya existe, ¿qué problemas le gustaría corregir al usuario?
- ¿Cuáles son los requisitos?
- ¿Cuál es la tasa de transferencia?
- ¿La red ha de ir a alta velocidad en las dos direcciones?

Estas preguntas iniciales pueden determinar los requisitos iniciales de rendimiento y fiabilidad. A partir de aquí podemos hacer otras preguntas, como:

- ¿Qué niveles de seguridad necesitamos?
- ¿Es necesario diseñar políticas de seguridad y cortafuegos si se quiere que los encaminadores den salida a Internet?
- ¿Qué áreas se podrían comprometer?
- ¿Es el alto rendimiento prioritario para todas las localizaciones?
- ¿Hay áreas no tan prioritarias?
- ¿Se enviarán sólo datos o se quiere una solución que integre voz y datos?
- ¿Se quiere que la solución de voz sea VoIP?
- ¿Se buscan estrategias de redundancia?
- ¿Qué coste representa para la empresa la caída de las conexiones?

VoIP son las siglas de voz sobre tecnología IP.

Podríamos continuar haciendo preguntas afinando cada vez más los requisitos iniciales. Lo que está claro es que no hay un camino único en el diseño de una red.

Importancia de la redundancia

La redundancia es un aspecto muy importante si queremos que el sistema no deje de funcionar nunca, aunque en muchas ocasiones acaba siendo uno de los últimos factores que se considera, ya que siempre se intenta reducir costes. Es necesario tener muy presente el efecto que puede suponer la caída total o parcial de la red por lo que respecta a la productividad de los usuarios.

> Robert Cahn escribe: "No se puede diseñar una red a ningún nivel sin algoritmos". Pero también añade: "Los problemas de diseño son demasiado complicados para darles solución de forma exacta".

1.1.1. Conceptos sobre redes WAN

En el sentido más genérico, una red WAN (*wide area network*) es una red dispersa geográficamente. En nuestro caso definiremos la red WAN como una red

creada para conectar dos o más redes de área local (LAN). Así, una red WAN puede conectar redes LAN ubicadas en la misma ciudad o que estén en cualquier punto del mundo.

1.1.2. Diferencias entre redes LAN y WAN

Normalmente la WAN se diferencia de la LAN en aspectos como coste, rendimiento y expansión:

- **Precio.** Las WAN tienen un coste recurrente. En la LAN, una vez instalada, el usuario tiene en propiedad tanto el cableado como los conmutadores. En la WAN se paga a la operadora por el alquiler de las líneas y de unos servicios.

- **Rendimiento**. Entre las redes LAN y WAN hay diferencias sustanciales en el ámbito físico, de distancias y de conexiones. La LAN, actualmente, se basa en Ethernet. En la WAN hay varias posibilidades a nivel 2. Así, tenemos aspectos como las latencias, los paquetes *broadcast* u otros que de entrada se ven afectados por las distancias.

- **Expansión**. En las redes WAN lo que estamos conectando son dos puntos a grandes distancias, los cuales, en función de la expansión que puedan tener, nos condicionarán el tipo de red.

1.1.3. Similitudes entre redes LAN y WAN

Podemos encontrar ciertas similitudes cuando hablamos de localización de los recursos. Hace falta tener claros y analizar los flujos de tráfico de las comunicaciones. Mirando la infraestructura de red del cliente tenemos que poder ver cómo son ciertos aspectos:

- Protocolos de red y arquitectura de interconexión.

- Funcionamiento de los servicios de web y correo.

- Los requisitos de seguridad.

- Distribución de la topología de la WAN. Qué localizaciones se quieren interconectar.

- El coste y rendimiento que ofrecen los diferentes proveedores de servicio y la logística y planificación para su desarrollo.

Evidentemente, para hacer la planificación no hay que olvidar los cambios que se pueden producir en el futuro.

1.2. Diseño de redes

Un buen diseño de red es la base a la hora de hacer una buena implementación de la red. La mayoría de redes se pueden agrupar en dos categorías: aquellas que se han ido formando en función de las necesidades del momento y las que realmente han sido pensadas a partir de un buen diseño. Este segundo grupo se caracteriza por su previsibilidad y consistencia en relación con los siguientes aspectos:

- **Rendimiento**. Son redes con un rendimiento adecuado en relación con los parámetros de rendimiento establecidos.
- **Disponibilidad**. Habría que intentar que la caída de líneas o dispositivos de red no afectaran a las sesiones cliente-servidor. Un parámetro muy importante es el tiempo de convergencia.

Tiempo de convergencia

El tiempo de convergencia es el intervalo de tiempo desde una caída de la red hasta su recuperación.

- **Escalabilidad**. Una red escalable es aquella que soporta de forma adecuada el crecimiento sin necesidad de ser rediseñada de nuevo. Así, la estructura de la topología de red y la tecnología usadas no han de ser rediseñadas para acomodarse al crecimiento.
- **Coste de funcionamiento**. La red no sólo debe reunir ciertas especificaciones técnicas, sino que debe ser rentable económicamente en su diseño e implementación. Por lo tanto, es importante prever que sea una red consistente en cuanto a costes de funcionamiento.

1.3. Objetivos en el diseño de redes

Es muy importante aclarar los objetivos desde el principio dentro del proceso de diseño de redes, ya que los parámetros usados en el diseño servirán para evaluarlo. Hay que tener unos parámetros de rendimiento definidos y unos niveles asociados. Quien marca estos niveles son las propias aplicaciones y, en consecuencia, hay que tener claras las aplicaciones tanto cuantitativa como cualitativamente. Estos parámetros principales son el ancho de banda, la pérdida de paquetes, el retardo y la variación del retardo. 

Otro nivel que hay que indicar en el diseño de la red es la disponibilidad o tiempo de caída. Es el tiempo que se permite que la red esté caída, en este caso se encuentra directamente relacionado con el tipo de funcionamiento, negocio, etc. de la empresa.

Un parámetro que hay que tener en cuenta, y que en muchas ocasiones se olvida, es la estimación de crecimiento potencial de la red. Hace falta tener clara la evolución de la empresa para saber su crecimiento en número de usuarios, nuevas sedes, etc. y poder prever el tráfico de las aplicaciones.

En último caso, el planteamiento debe ser realista con las posibilidades de la propia empresa.

Los objetivos del diseño de redes son muy lógicos, pero normalmente lo que es más lógico es lo que no se hace.

1.4. Tareas en el proceso de diseño

A continuación se enumeran unas cuantas tareas que se pueden considerar básicas en el proceso de diseño de la red:

- Determinar los parámetros de rendimiento que mejor especifican cada uno de los objetivos de diseño.
- Identificar las restricciones en el diseño.
- Con las restricciones en la mano, marcar los niveles de rendimiento más relevantes de la red.
- Empezar siempre por un diseño de alto nivel. No hay que perderse inicialmente en los detalles.
- Comparar este diseño inicial con las restricciones y realimentar el proceso de diseño.
- Ahora ya estamos en disposición de diseñar un plan específico.
- Es importante que todos los aspectos importantes de la solución técnica sean probados previamente en el laboratorio. Eso ayudará a refinar la solución.
- El diseño se ha completado cuando se ha acabado de refinar completamente.

1.5. Principios en el diseño de red

A continuación resumimos los principios clave que han de seguirse para tener éxito en el diseño de red:

- Las aplicaciones marcan los requisitos en el diseño. No se puede hacer un buen diseño de red si no se entienden las características de las aplicaciones.
- Hay que probar los diseños en el laboratorio. Están muy bien las herramientas de simulación, pero la mejor manera de comprobar un diseño de red es probándolo en el laboratorio. Aquí podremos resolver detalles técnicos específicos.
- No se ha de plantear el diseño de una red como imagen de la estructura corporativa.

- Hay que procurar ser independiente del vendedor. Intentar no optar por soluciones propietarias.

Independencia del vendedor

La independencia del vendedor es un principio muy interesante, pero en muchas ocasiones poco realista. Una vez ligado a un fabricante es complicado cambiar, ya que el valor añadido que dan sus equipos suelen ser soluciones propietarias.

- Es necesario intentar hacer el diseño lo más sencillo posible. Complicar la solución en muchas ocasiones sólo incrementa el coste y complica la administración posterior.

- No hay que partir de modelos predefinidos.

- El diseño debe ser lo bastante robusto para que los cambios que puedan darse no obligen a modificarlo todo. A la vez, debe ser bastante flexible para permitir cambios en la estructura.

- Un aspecto básico para un buen diseño es que es necesario que sea predictible, consistente en rendimiento, fiable y escalable.

2. Diseño IP

Como la mayoría de diseños de red actuales están montados sobre IP, comentaremos los elementos principales que hay que tener en cuenta para un diseño IP. No se pretende dar una explicación detallada de estos elementos, sino sólo explicar la importancia de cada uno de ellos cuando se quiere realizar un buen diseño lógico.

El plan de direccionamiento IP es básico para tener éxito a la hora de hacer el diseño de red. A continuación veremos de forma muy breve los elementos que hay que tener claros a la hora de formular un plan de direccionamiento IP escalable que pueda soportar la red, su crecimiento y los elemento clave.

2.1. Planificación de direcciones IP

Direcciones públicas y privadas

El espacio de direcciones IP está dividido en direcciones públicas y privadas. Las direcciones privadas están reservadas y sólo se pueden utilizar dentro de la red interna de la empresa, pero no en Internet. Así, estas direcciones tienen que ser mapeadas por direcciones públicas cuando se quiere salir a Internet.

El RFC 1918 (*address allocation for private Internet*) define los siguientes rangos de direcciones privadas:

10.0.0.0 - 10.255.255.255.
172.16.0.0 - 172.31.255.255.
192.168.0.0 - 192.168.255.255.

Criterios de selección entre direcciones privadas y públicas

El número de direcciones IP públicas es pequeño, de manera que los proveedores asignan pocas IP a sus clientes. En la mayoría de casos es insuficiente para hacer el menaje de todas las direcciones de la red.

La solución es trabajar con IP privadas y trasladarlas a IP públicas cuando sea necesario. En el diseño de la red hay que tener en cuenta las siguientes consideraciones principales:

- quién y cuántos dispositivos tienen que salir al exterior;

- qué servicios requieren, es decir, si están limitados los servicios o no (los dispositivos internos no tienen que ser visibles desde el exterior);

- qué dispositivos (servicios, normalmente) tienen que ser visibles desde el exterior (en estos casos la IP no puede variar).

Interconexión de direcciones privadas y públicas: el servicio de NAT

Como hemos explicado, una empresa puede tener direcciones privadas y públicas. Un router o cortafuegos actuará de interfaz entre la red privada y la pública.

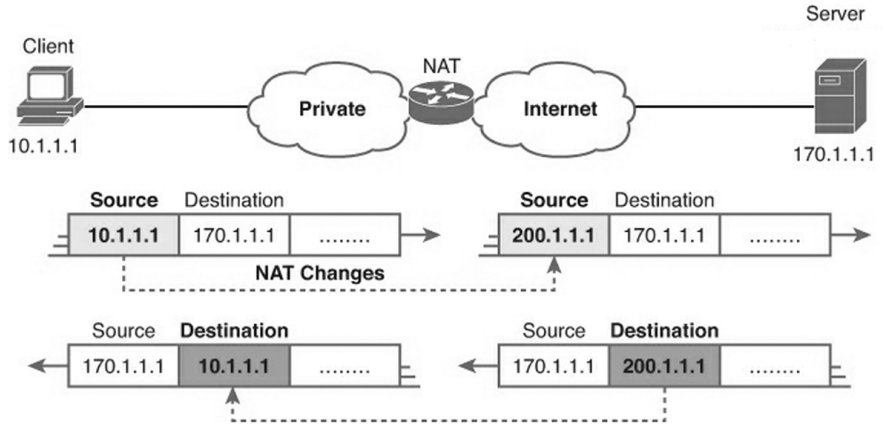
El mecanismo para trasladar las direcciones privadas a públicas puede ser a través de NAT o PAT.

NAT es la sigla de *network address translation.*
PAT es la sigla de *port address translation.*

Network Address Translation (NAT), junto a Classless Interdomain Routing (CIDR), es un protocolo diseñado para el ahorro y la optimización en la asignación de direcciones IP. Inicialmente, NAT estaba pensado para reducir el agotamiento del espacio de direcciones IP disponibles, y permitía que múltiples direcciones IP privadas pudieran ser representadas por un grupo mucho más pequeño de direcciones públicas. Así, sin soluciones como NAT, el espacio de direcciones se habría agotado por completo a mediados de la década de 1990 e internet no habría podido continuar creciendo.

El servicio NAT, definido en el RFC 3022, permite que un equipo que no tiene una dirección IP válida registrada se pueda comunicar por medio de internet. Básicamente, NAT mapea un grupo de direcciones en otro grupo de direcciones de manera transparente para el usuario. De este modo, permite que redes IP privadas con direcciones IP no registradas se puedan conectar a internet. NAT trabaja en los enrutadores y convierte o traduce las direcciones privadas que hay en la red interna privada en direcciones públicas, antes de que los paquetes salgan hacia la red exterior.

Figura 1. Mapeo de direcciones IP de la red privada en internet



Si nos fijamos en la figura anterior, podemos ver cómo el enrutador efectúa NAT cambiando la dirección IP origen del paquete (10.1.1.1) y transformándola en otra dirección, en este caso 200.1.1.1, cuando este deja la red privada de la organización. Del mismo modo, el enrutador vuelve a efectuar NAT y cambia la dirección destino del paquete (200.1.1.1) cuando este vuelve del servidor hacia la red privada (10.1.1.1).

Pero NAT no solo es beneficioso por este motivo. Otras ventajas que ofrece NAT pueden ser las siguientes:

- Ahorro de direcciones IP: permite disminuir el número de direcciones IP necesarias.
- Flexibilidad: posibilidad de cambiar de proveedor de internet sin tener que cambiar las direcciones de toda nuestra red.
- Permite solucionar problemas de solapamiento de direcciones.
- Evita que los *hosts* de la red externa vean las direcciones internas. No obstante, NAT no es un método para tener seguridad en la red privada.

Hay que tener presente, sin embargo, que la implementación de NAT en nuestra red también puede suponer ciertos problemas. Algunos de ellos pueden ser:

- Aumento de la latencia.
- Dificultades de monitorización.
- Pérdida de funcionalidades. Quizá alguna aplicación no funciona con el NAT activado.

Terminología basada en función de la localización del dispositivo

Cuando se realiza NAT, se usa la notación siguiente en función de dónde se encuentre el paquete y cuál sea su origen y destino:

- **Dirección local interna:** la dirección IP asignada a un *host* de la red interna, de manera estática o por medio de una asignación dinámica DHCP.
- **Dirección global interna:** la dirección IP de la red externa, normalmente proporcionada por el proveedor de internet, que puede representar una o más direcciones IP locales, en función del tipo de NAT que realicemos. Lo trataremos en el apartado siguiente.
- **Dirección local externa:** la dirección IP de un *host* externo tal como aparece en la red interna. No es necesario que sea la dirección legítima.
- **Dirección global externa:** la dirección asignada a un *host* en la red externa por el propietario del *host*.

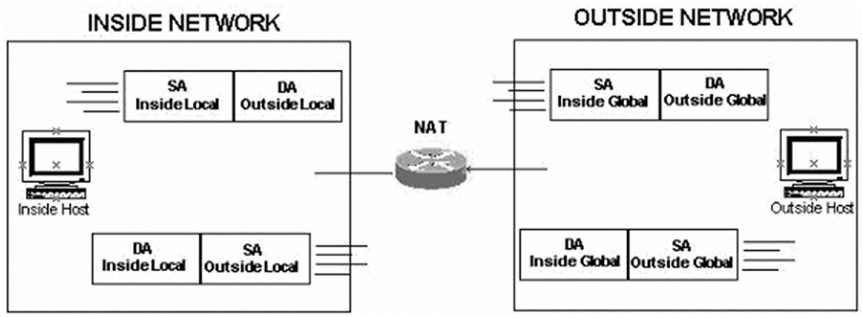
Hay que tener presente que los términos *interna* y *externa* son definiciones de NAT. Las interfaces de un enrutador NAT se definen como internas y externas con los comandos de configuración NAT del dispositivo. Así, las redes con las

cuales se conectan estas interfaces se pueden definir como redes internas o como redes externas:

Dirección local: una dirección local es cualquier direccionamiento que aparezca en la parte interna de la red.

Dirección global: una dirección global es cualquier direccionamiento que aparezca en la parte exterior de la red.

Figura 2. Ejemplo de notación. SA (*Source Address*) es la dirección origen y DA (*Destination Address*) es la dirección destino



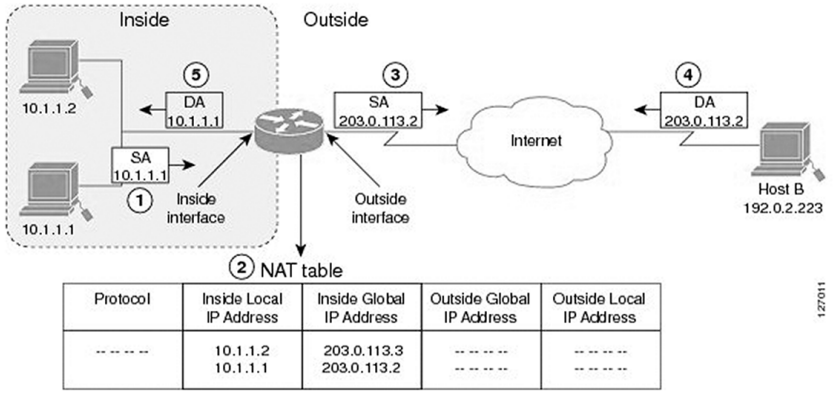
Los paquetes originados en la parte interna de la red tienen una dirección local interna como dirección origen, y una dirección local externa como dirección destino del paquete, mientras este paquete no salga de la parte interna de la red. Una vez que este paquete ha sido conmutado hacia el exterior, la dirección origen se conoce como dirección global interna y el destino del paquete se conoce como dirección global externa.

De manera inversa, cuando un paquete es originado en la parte exterior de la red, su dirección origen se conoce como dirección global externa, mientras está en la red externa. El destino del paquete se conoce como dirección global interna. Para el mismo paquete, una vez conmutado en la red interna, la dirección origen se denomina dirección local externa y la dirección destino del paquete se conoce como dirección local interna.

Hay tres posibilidades a la hora de hacer el NAT. A continuación mostraremos los diferentes tipos básicos de NAT que hay:

1) NAT estático. Como indica el nombre, el NAT estático hace un mapeo estático de cada dirección IP privada con una dirección IP pública, de manera que cada vez que una dirección IP concreta de la red privada salga hacia internet tendrá asignada la misma dirección IP pública.

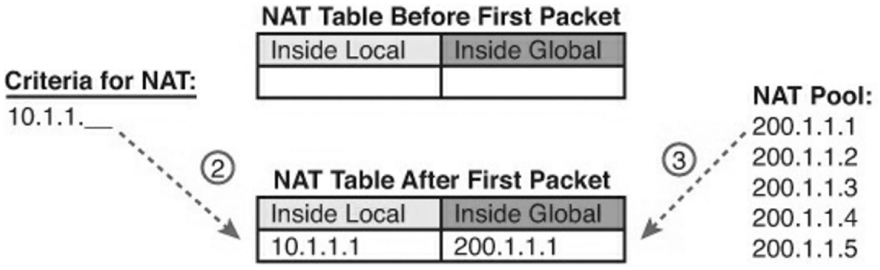
Figura 3. Ejemplo de funcionamiento de NAT estático



En el ejemplo de la figura la empresa tiene asignadas las IP públicas del rango 203.0.113.0/24. El usuario de la red interna 10.1.1.1/24 quiere abrir una conexión con el *host* B, que se encuentra en el exterior. Cuando el enrutador recibe el primer paquete de 10.1.1.1, este examina su tabla de traducción de direcciones (NAT). Dado que se trabaja con NAT estático, el enrutador cambia la dirección IP local interna 10.1.1.1 por la dirección global 203.0.113.2 y conmuta el paquete. El *host* B recibe el paquete y responde al *host* 10.1.1.1 mediante la dirección destino global interna (DA) 203.0.113.2. Cuando el enrutador recibe el paquete de respuesta con la dirección global interna, hace una búsqueda en la tabla NAT. Entonces, traslada la dirección a la dirección local interna y reenvía el paquete al *host* 10.1.1.1.

2) NAT dinámico. El NAT dinámico es similar al NAT estático, pero con alguna diferencia. En el caso estático hay un mapeo previo uno a uno entre las direcciones privadas (direcciones locales internas) y las direcciones públicas (direcciones globales internas). En el caso del NAT dinámico esto no es previo y se hace dinámicamente. Se define un grupo de direcciones IP privadas que pueden salir y un grupo de direcciones públicas que hay que asignar. La asignación se hace en el momento que llega un paquete de la red interna al enrutador y este quiere salir hacia internet.

Figura 4. NAT dinámico



En la figura se ve que el equipo con dirección IP: 10.1.1.1 envía el primer paquete en dirección a internet. En este caso se le asigna dinámicamente la dirección pública 200.1.1.1. Esta entrada dinámica en la tabla se mantendrá mientras haya tráfico de este usuario hacia el exterior.

En este tipo de configuración podemos tener más direcciones internas que direcciones públicas. En el supuesto de que el enrutador haya asignado todas las direcciones públicas y le llegue un paquete de un nuevo usuario interno que quiere salir a internet, el enrutador descartará el paquete. Si queremos evitar este problema con NAT dinámico, la única solución es que el número de direcciones públicas sea tan grande como el grupo de direcciones privadas que puedan salir.

3) Port Address Translation (PAT)

Hay fabricantes que denominan la traducción de direcciones por puerto (PAT) *overloading*.

Port Address Translation soluciona el problema que se ha visto en el caso de NAT estático o dinámico, en el que se requieren tantas direcciones públicas como privadas. PAT soporta que haya muchos clientes privados que salen a internet a través de pocas o incluso una sola dirección IP pública.

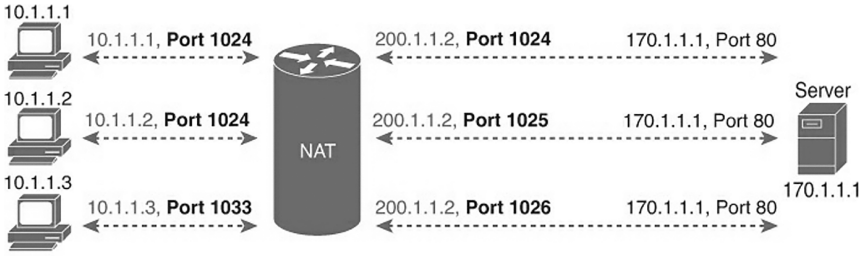
Para entender PAT, hay que recordar antes el concepto de conexión TCP entre dos dispositivos.

Figura 5. Ejemplo de conexión TCP/IP

Si nos fijamos en la figura anterior, cada conexión es fijada por una IP origen, un puerto origen, una IP destino y un puerto destino. Si estas conexiones están iniciadas desde un mismo origen y van hacia un mismo destino, la asignación de diferente puerto origen consigue que no haya dos conexiones iguales.

PAT aprovecha este hecho en el enrutador, en el cual no solo se hace un mapeo de la dirección, sino también del puerto. De este modo se consigue que, aunque el mapeo entre direcciones privadas se realice siempre con la misma IP pública, el enrutador pueda diferenciar cada uno de los mapeos realizados mediante el puerto.

Figura 6. PAT entre direcciones 10.1.1.0/24 con dirección pública 200.1.1.2



Inside Local	Inside Global
10.1.1.1: **1024**	200.1.1.2: **1024**
10.1.1.2: **1024**	200.1.1.2: **1025**
10.1.1.3: **1033**	200.1.1.2: **1026**

En la figura se muestra un ejemplo de cómo quedaría la tabla PAT del enrutador. Si nos fijamos en los equipos 10.1.1.1 y 10.1.1.2, inicialmente los dos tienen el mismo puerto origen. Al hacer NAT, los dos tienen la misma IP global interna. Para diferenciarlos, el enrutador cambia el puerto origen de la segunda conexión. El usuario 10.1.1.1:1024 pasa a tener la dirección global interna 200.1.1.2:1024, mientras que el usuario 10.1.1.2:1024 pasa a tener la dirección global interna 200.1.1.2:1025.

Asignación de direcciones IP en los dispositivos. Direcciones estáticas y dinámicas

Cuando se quiere hacer un plan de menaje IP, hay que saber el tamaño de la red para poder establecer el número de subredes y el número de IP por subred. Por lo tanto, hay que tener claro las localizaciones, número de dispositivos por localización y requerimientos de menaje para las localizaciones específicas.

Vamos a ver el efecto en el ámbito administrativo del mecanismo de asignación de direcciones IP a los dispositivos finales.

La asignación de direcciones incluye dar IP, una puerta de enlace, servidores de DNS, etc. Por lo tanto, hay que tener clara la respuesta a una serie de preguntas como son:

- ¿Cuántos dispositivos necesitan IP?
- ¿Qué dispositivos requieren de una IP estática?
- ¿Puede haber cambios de menaje en el futuro?
- ¿El administrador necesita hacer un seguimiento de los dispositivos y de su dirección de IP?
- ¿Hay requerimientos de disponibilidad?
- ¿Hay requerimientos de seguridad?

Hay dos estrategias básicas para asignar direcciones:

a) Estática. Se asigna tanto la IP como los posibles parámetros asociados de forma manual. Implica una sobrecarga para el administrador, sobre todo para redes grandes.

b) Dinámica. Se asignan las IP de forma automática. Libera de esta tarea al administrador. Éste configura un servidor que se encarga de estas tareas. El protocolo más común es DHCP.

¿Cuándo usaremos una estrategia o la otra? Para usar un tipo o el otro o los dos, hay que tener presente las siguientes consideraciones:

- **Tipo de nodo**. En general dispositivos como un router, *switch* o servidores tienen IP estáticas. Los dispositivos finales (PC) tienen IP dinámicas.
- **Número de dispositivos**. Es preferible IP dinámicas cuando el número de dispositivos es elevado.
- **Seguimiento de direcciones**. Si se quiere poder hacer un control (seguimiento) de las direcciones para políticas de red, es mejor emplear direcciones dinámicas. Se puede hacer con DHCP configurando adecuadamente el servidor.
- **Parámetros adicionales**. Si hace hay que configurar parámetros adicionales, es más sencillo hacerlo con DHCP.
- **Alta disponibilidad**: La IP dinámica depende de un servidor. Si queremos que esté siempre disponible, serán necesarios mecanismos de redundancia.

2.2. Subredes con máscara de longitud variable (VLSM)

Una subred permite crear redes más pequeñas a partir de la asignación inicial por clases. Si hacemos eso debemos definir un nuevo parámetro, que denominamos máscara. La máscara nos permite saber en esta nueva asignación cuántos bits representan la red creada y cuántos el *host* concreto dentro de la misma.

IP con clase. Las direcciones IP se pueden clasificar en clase A, B y C.
Clase A: 8 bits parte de red, 24 bits parte de *host*. Bit de más peso = 0
Clase B: 16 bits parte de red, 16 bits parte de *host*. Bits de más peso = 10
Clase C: 24 bits parte de red, 8 bits parte de *host*. Bits de más peso = 110

División en clases del espacio de direcciones IP

El espacio de direcciones IP está dividido inicialmente en clases. Clase A, B y C principalmente. En función de la clase podemos saber qué parte de la dirección representa en la red y cuál en el equipo concreto de la misma red.

Subred con máscara de longitud variable significa la implementación de subredes con máscaras diferentes provenientes de la misma dirección de red basada en clase.

Esta posibilidad permite un uso más eficiente del espacio de direcciones IP, tanto en términos de subredes posibles como de dispositivos por subred. Se basa en redes donde se dispone de rangos pequeños de direcciones IP. Ligado en VLSM es necesario que haya un protocolo de encaminamiento que soporte VLSM. Estos protocolos de encaminamiento se llaman protocolos de encaminamiento sin clase y lo que hacen es que cuando se genera información de las nuevas rutas (redes) se incorpora la máscara asociada a cada una de estas redes.

Algunos ejemplos de protocolos sin clase son RIPv2, OSPF, IS-IS y BGP.

Ejemplo de *subnetting*

Subnetting

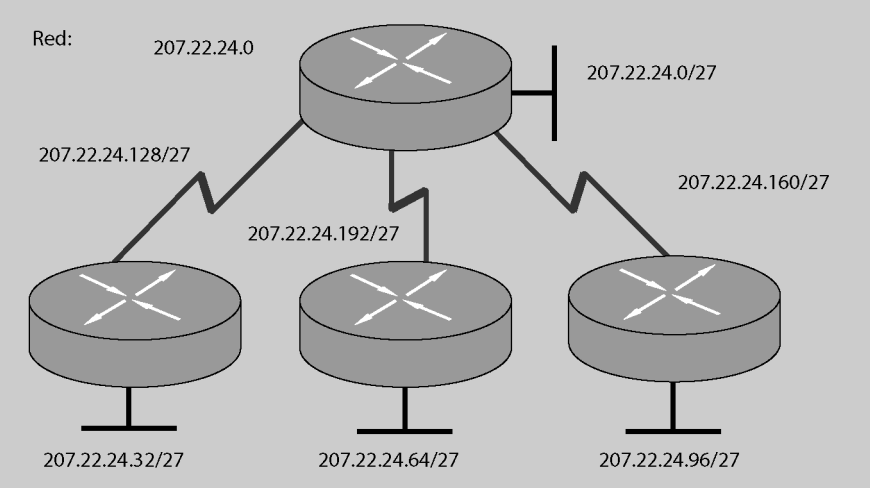
A partir de una dirección con clase, el *subnetting* nos permite hacer redes más pequeñas, todas con la misma máscara (máscara de longitud fija).

A continuación, se muestra un ejemplo de ***subnetting*** donde, dada la dirección de red de clase C, 207.22.24.0, aplicamos una máscara de 27 bits y queda así:

Subred 0	207.22.24.0/27
Subred 1	207.22.24.32/27
Subred 2	207.22.24.64/27
Subred 3	207.22.24.96/27
Subred 4	207.22.24.128/27
Subred 5	207.22.24.160/27
Subred 6	207.22.24.192/27
Subred 7	207.22.24.224/27

Este ejemplo podría ser aplicado directamente a la red de la figura 7, donde tenemos siete redes diferentes. Puede imaginarse que es una empresa con una sede central y tres subsedes conectadas ente ellas mediante líneas WAN punto por punto (tres en total). Cada sede a su vez dispone de su red Ethernet. Si nos fijamos, esta empresa está formada por un total de siete subredes. Aprovechando el *subnetting* del ejemplo anterior, quedaría como se muestra en la figura 3.

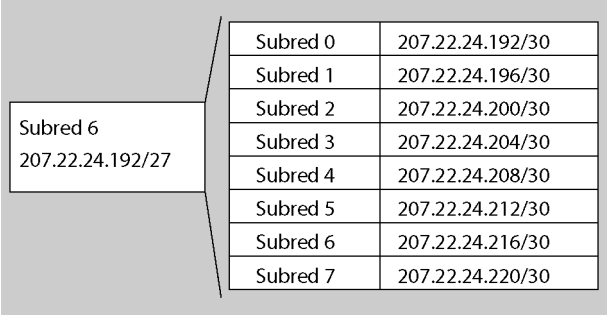
Figura 7. Topología con *subnetting*



Si nos fijamos en la solución adoptada, veremos que hemos asignado un rango de 30 direcciones para cada subred. Este rango puede ser correcto para las redes Ethernet, pero es totalmente ineficiente para las líneas WAN, que sólo necesitan dos direcciones (una para cada extremo de la conexión).

Una solución mucho más adecuada para esta empresa sería emplear VLMS. Aplicando VLSM podemos hacer una subred de una de las subredes anteriores, como muestra la figura 8.

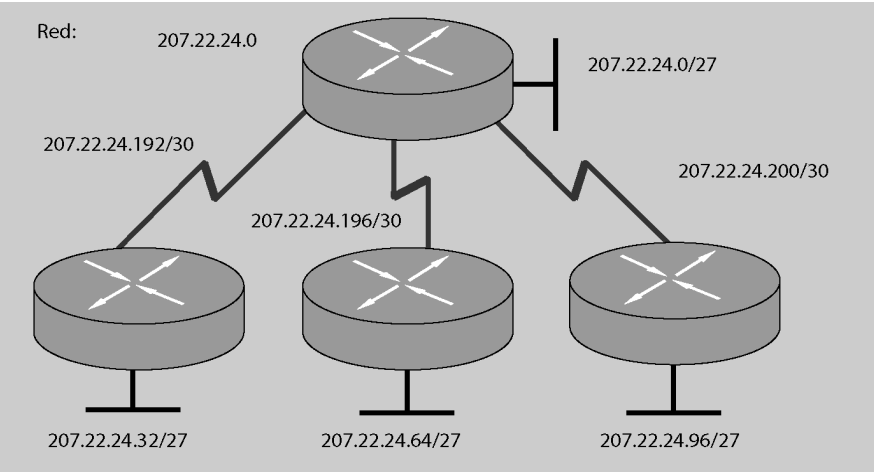
Figura 8. Ejemplo de VLSM



Estas subredes se podrían usar para hacer el direccionamiento en una red WAN de los diferentes enlaces punto a punto que pueda tener; sólo necesitan dos direcciones IP, una para cada punto del enlace.

En nuestro caso concreto el *subnetting* final quedaría como se muestra en la figura 9.

Figura 9. Topología aplicando VLSM



Hemos conseguido liberar unos rangos de direcciones que nos pueden ser útiles en el caso de que la empresa crezca.

2.3. Sumarización de rutas

La sumarización de rutas es la posibilidad de agrupar una serie de rutas para que se puedan anunciar como una sola. El resultado de esta sumarización es la reducción del tamaño de las tablas de encaminamiento a los nodos de la red.

Usos de la sumarización de rutas

La sumarización es muy interesante para redes muy grandes. En Internet la sumarización ha permitido que los encaminadores troncales sigan funcionando, ya que se han reducido las tablas de encaminamiento.

Conseguimos entre otros efectos reducir el tiempo de latencia asociado en la busca en las tablas de encaminamiento cada vez que llega un paquete IP.

Otro aspecto conseguido con la sumarización es la mejora de la estabilidad de la red, ya que la caída puntual de algún enlace no se propaga por toda la red haciendo recalcular las tablas de todos los encaminadores, es decir, que evitamos actualizaciones de encaminamiento innecesarias y hacemos que la convergencia sea más rápida.

Para poder realizar la sumarización de rutas es vital que el esquema de direccionamiento IP se elabore de manera que permita esta sumarización y, por lo tanto, es un elemento estratégico en el diseño de la red WAN. Los rangos de direcciones han de estar formados por bloques contiguos.

Veamos un par de ejemplos de sumarización. En el primero explicaremos la mecánica del mismo. En el segundo caso veremos cómo se aplica en una topología de red cumplida.

Ejemplo de sumarización

Supongamos que tenemos las direcciones consecutivas que se ven en la tabla siguiente. Sin sumarización, el encaminador ha de mantener entradas individuales para cada red de la tabla.

Direcciones clase B consecutivas				
Dirección	**Primer octeto**	**Segundo octeto**	**Tercer octeto**	**Cuarto octeto**
172.24.0.0/16	**10101100**	**00011000**	00000000	00000000
172.25.0.0/16	**10101100**	**00011001**	00000000	00000000
172.26.0.0/16	**10101100**	**00011010**	00000000	00000000
172.27.0.0/16	**10101100**	**00011011**	00000000	00000000
172.28.0.0/16	**10101100**	**00011100**	00000000	00000000
172.29.0.0/16	**10101100**	**00011101**	00000000	00000000
172.30.0.0/16	**10101100**	**00011110**	00000000	00000000
172.31.0.0/16	**10101100**	**00011111**	00000000	00000000

En la tabla anterior, en negrita, tenemos la parte correspondiente a red para cada dirección. Si aplicamos sumarización miramos dentro de la parte de red qué bits son comunes a todas ellas. Así, en la siguiente tabla se ve en negrita la parte de red común.

Direcciones clase B consecutivas. 13 bits comunes				
Dirección	**Primer octeto**	**Segundo octeto**	**Tercer octeto**	**Cuarto octeto**
172.24.0.0/16	**10101100**	**0001**1000	00000000	00000000
172.25.0.0/16	**10101100**	**0001**1001	00000000	00000000
172.26.0.0/16	**10101100**	**0001**1010	00000000	00000000
172.27.0.0/16	**10101100**	**0001**1011	00000000	00000000
172.28.0.0/16	**10101100**	**0001**1100	00000000	00000000
172.29.0.0/16	**10101100**	**0001**1101	00000000	00000000
172.30.0.0/16	**10101100**	**0001**1110	00000000	00000000
172.31.0.0/16	**10101100**	**0001**1111	00000000	00000000

De este modo, el encaminador puede sumarizar estas ocho direcciones con una dirección única con un prefijo de 13 bits: 1010110000011

Obtenemos la dirección sumarizada: 172.24.0.0/13

Ejemplo de sumarización aplicada a topología de red completa

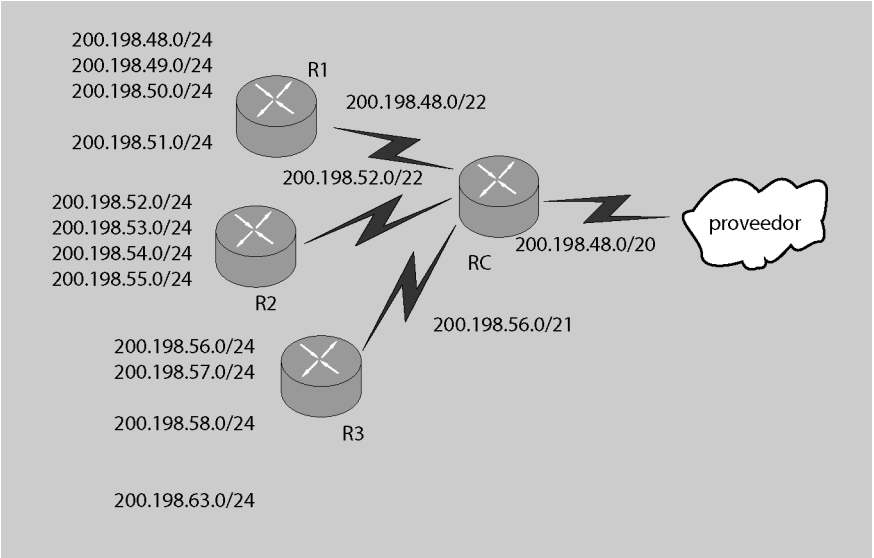
En la figura 10 se muestra una topología concreta donde un proveedor de red tiene un encaminador (RC) al cual están conectados varios encaminadores de acceso (pueden ser, por ejemplo, clientes). Este es un ejemplo en el que es interesante hacer sumarización.

En la figura 6 la ruta sumarizada que llega al proveedor contiene un prefijo de 20 bits común a todas las redes que llegan a RC: 200.199.48.0 /20 o 11001000 11000111 0001.

En este caso, las tablas de RC se simplifican por el hecho de llegar sumarizadas por los encaminadores de acceso, y, a la vez, RC, cuando envía las actualizaciones al proveedor (a los encaminadores que están en el núcleo de su red) le envía una única ruta. La sumarización de rutas, por lo tanto, reduce el tamaño de las tablas de encaminamiento mediante la suma de rutas de múltiples redes en una única super-red.

Por otra parte, para que la sumarización funcione correctamente hay que tener cuidado en el momento de asignar de forma jerárquica, para poder realizar después la agregación.

Figura 10. Sumarización de rutas



Planificación de un menaje IP jerárquico

Una buena planificación IP hará que tengamos una mejor o peor solución de encaminamiento. Como sabéis, las direcciones IP tienen un esquema de menaje jerárquico donde las direcciones están divididas en: parte de red (prefijo) y parte de *host*. Los routers toman las decisiones en función del prefijo y del siguiente salto que se haya de realizar, es decir, del siguiente nodo al que pasar el datagrama sin necesidad de conocer los detalles para llegar al destino.

Beneficios de un menaje jerárquico

Como se ha explicado, el menaje IP se realiza en función del tamaño, la localización geográfica y la topología de la red. En redes grandes, un menaje jerárquico es básico, incluso para que las tablas de encaminamiento de los routers sean estables.

Así, una buena planificación afectará a:

- **Encaminamiento**. Una buena planificación IP puede mejorar la estabilidad de encaminamiento, disponibilidad del servicio, escalabilidad y modularidad de la red.

- **Diseño modular y escalable**. Permite la agregación de encaminamiento sin afectar al diseño existente.

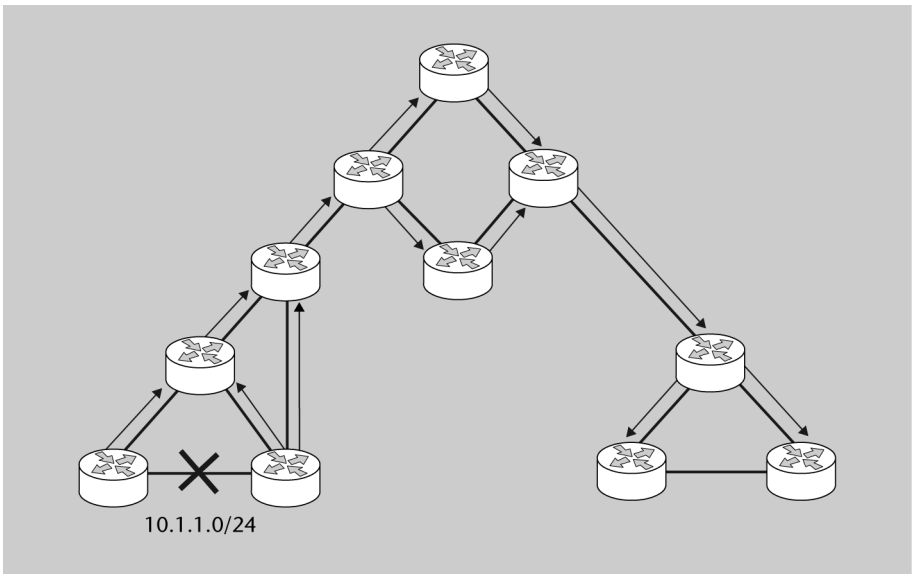
- **Agregación de rutas**. Reduce las tablas de encaminamiento y mejora la estabilidad y la escalabilidad. Para hacerlo, hay que dividir la red en grupos IP que estén contiguos.

Impacto de un mal diseño IP

En el caso de que la asignación de direcciones IP se haya hecho en función del crecimiento de la red, el reparto de los IP es aleatorio y, por lo tanto, sin crear grupos o sumarización. Esto provoca que no se pueda dividir la red en grupos de direcciones contiguos y no podamos implementar sumarización de rutas.

Un ejemplo típico del impacto de un mal diseño se da cuando tenemos una red con encaminamiento dinámico y uno de los enlaces va cambiando de estado periódicamente (figura 11). Como usamos un encaminamiento dinámico, cada vez que haya un cambio de estado al enlace, éste se propagará por toda la red, a la vez que hará actualizar las tablas de encaminamiento de todos los routers.

Figura 11. Un mal menaje puede provocar un exceso de tráfico de encaminamiento



Algunos de los efectos que provoca un mal diseño son:

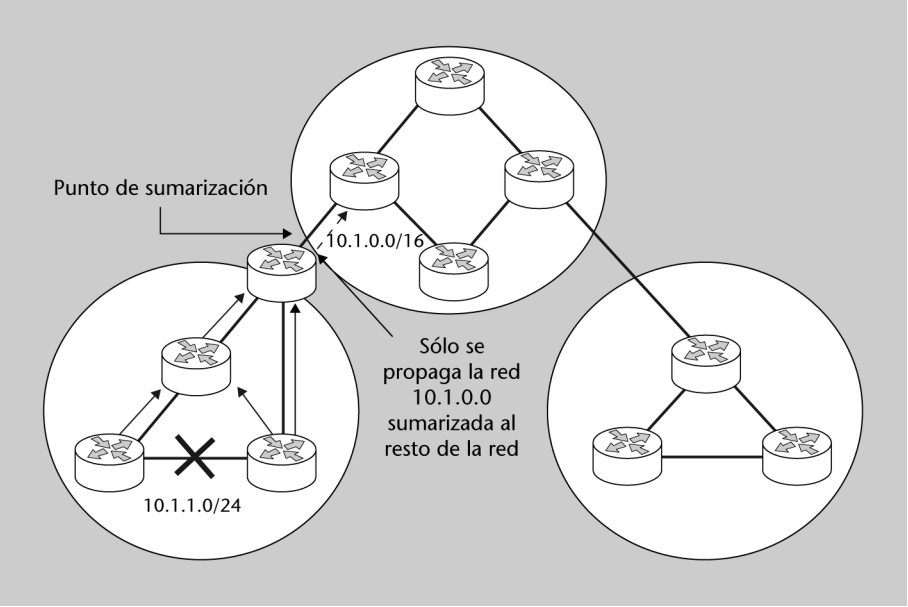
- El exceso de tráfico de encaminamiento consume ancho de banda. Cuando hay un cambio en una ruta, los routers se envían actualizaciones. Sin sumarización, hay más actualizaciones y un ayor consumo de ancho de banda.

- Un aumento del número de actualizaciones en los routers. Afectará al rendimiento de los mismos.

Beneficios de la agregación de rutas

La implementación de agregación de rutas en los nodos que actúan de frontera entre áreas de direcciones contiguas controla el tamaño de las tablas de encaminamiento. En la figura se muestra un ejemplo de lo que acabamos de explicar.

Figura 12. Un menaje jerárquico permite distribuir sólo las rutas sumarizadas



En este caso, si un enlace dentro de un área cae, éste no se propaga en el resto de la red, ya que sólo se envía una ruta sumarizada; por lo tanto, no se ve reflejado el cambio. La información de la ruta que ha fallado se propaga sólo dentro del área. Conseguimos, por lo tanto, reducir el consumo de ancho de banda asociado a la actualización de *routers* entre vecinos, y además disminuye el número de cálculos que tiene que hacer el *router* cada vez que recibe una nueva actualización.

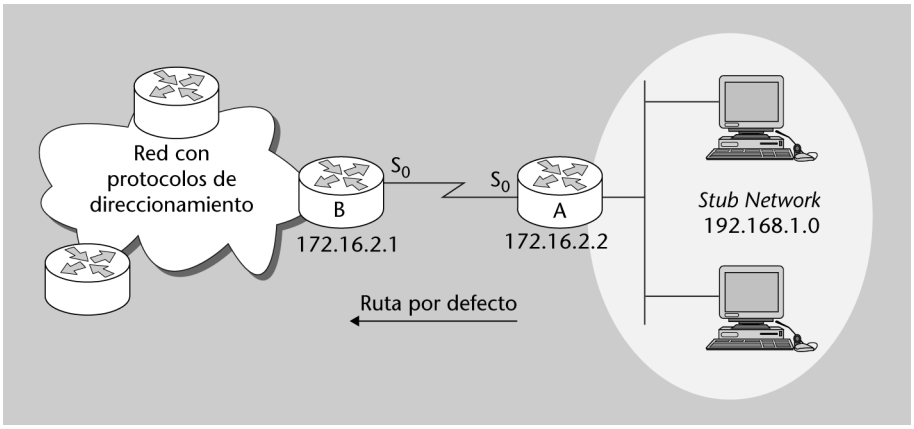
2.4. Conceptos sobre el encaminamiento IP

Existen dos formas de configurar el encaminamiento, cada una de ellas con sus ventajas o inconvenientes:

1) **Encaminamiento estático**. Apropiado en las siguientes circunstancias:

- enlaces con muy baja velocidad, donde no sea deseable enviar actualizaciones de encaminamiento;
- casos en los que el administrador necesite control absoluto sobre las rutas;
- cuando sólo hay una ruta de acceso al resto de la red (*stub network*). En la figura siguiente se muestra esta situación.

Figura 13. *Stub network*



Hay que tener presente que configurar y mantener rutas estáticas implica tiempo y, además, requiere un conocimiento completo de toda la red.

2) Encaminamiento dinámico. Permite a la red ajustar los cambios de la topología a los cambios de la red de forma automática. Una ruta estática no puede responder de forma dinámica a los cambios de la red. Esto es evidente si tenemos caídas de las líneas o añadimos líneas nuevas, y puede llevar a que el administrador tenga que dedicar mucho tiempo y esfuerzo en estos cambios.

¿Qué pedimos que cumplan los protocolos de encaminamiento?

- encontrar fuentes que les proporcionen información de encaminamiento (normalmente, los *routers* vecinos);
- seleccionar el mejor camino en función de la información recibida;
- mantener la información de encaminamiento;
- tener mecanismos que permitan verificar y actualizar esta información.

Los principales protocolos de encaminamiento actuales se muestran en la tabla siguiente:

Protocolos de encaminamiento IP	
Categoría	**Protocolo de encaminamiento**
Vector-distancia	RIPv1, RIPv2
Estado-enlace	OSPF, IS-IS
Híbrido	EIGRP

Características del protocolo de encaminamiento

A continuación comentaremos las diversas características que evalúan los diferentes protocolos. Estas características nos han de permitir hacer la mejor elección del protocolo en función de nuestra topología y nuestras necesidades concretas:

- **Estabilidad**. El protocolo de encaminamiento debe ser estable contra bucles de encaminamiento, que pueden perjudicar la red en el caso de que se generen actualizaciones cada vez que haya fluctuaciones en algún enlace.

- **Velocidad de convergencia**. Cuando hay un cambio en la topología, como puede ser supresión o inclusión de una subred, transcurre un período antes de que todos los encaminadores adquieran conocimiento de este cambio. Durante este intervalo de tiempo, denominado tiempo de convergencia, algunos encaminadores operan con información inconsistente.

- **Métrica**. El encaminador elige la métrica como mecanismo para determinar el mejor camino para llegar a un destino determinado. Cada protocolo usa una métrica diferente, es decir, cada protocolo usa un mecanismo distinto para determinar cuál es el mejor camino.

- **VLSM**. Ya hemos hablado en el apartado anterior de VLSM. Los protocolos de encaminamiento sin clase soportan VLSM, ya que incorporan la máscara de las redes en sus actualizaciones.

- **Sumarización de rutas**. Igual que en el caso anterior, la sumarización de rutas ya ha sido explicada, y, como se ha visto, es imprescindible para redes con crecimiento que el protocolo soporte la posibilidad de configurar sumarización de rutas.

- **Protocolos con clase o sin clase**. La diferencia entre un protocolo de encaminamiento con clase y otro sin clase es sencilla. Los protocolos sin clase incorporan la máscara en sus actualizaciones, mientras que los otros no lo hacen. Esta diferencia es básica porque implica que los protocolos con clase no soportan VLSM, redes discontinuas o la posibilidad de configurar sumarización de rutas. Se puede decir que estos protocolos no son adecuados para las redes modernas.

Protocolo RIP

Un protocolo de encaminamiento muy conocido y ampliamente utilizado es el protocolo RIP. Este protocolo es un protocolo con clase y, por lo tanto, es un protocolo que no escala de manera adecuada.

- **Escalabilidad**. La escalabilidad está relacionada con la posibilidad de crecimiento de la red IP. Así, la escalabilidad tiene asociados aspectos comentados, como la posibilidad de sumarización o velocidad de convergencia. También son importantes los mecanismos utilizados para informar de las actualizaciones.

Dirección recomendada

Podéis encontrar una descripción del protocolo RIP en http://es.wikipedia.org/wiki/RIP_%28protocolo%29

Una vez vistas las características principales observemos un par de protocolos que son actualmente básicos para las redes modernas: el *open shortest path first* y el *border gateway protocol*.

Open shortest path first

Open shortest path first (OSPF) es un protocolo de estado enlace, es decir, que lo que envía son las actualizaciones del estado de los enlaces. Es un protocolo estandarizado por Internet Enginneering Task Force y está pensado para redes escalables. Está descrito en varios RFC, y el más reciente es RFC 2328. El primer objetivo del protocolo es reducir la frecuencia de actualización del tráfico. Un segundo objetivo es la rápida convergencia. El inconveniente de estos dos objetivos es el mayor consumo de recursos de memoria y CPU en comparación con los encaminadores que trabajan con protocolos de vector-distancia.

Los protocolos de encaminamiento

Los protocolos de encaminamiento se pueden clasificar de dos formas: según la clase (con clase o sin clase) y según si son protocolos que trabajan con vector a distancia o con estado enlace.

Protocolos de encaminamiento con vector distancia o con estado enlace

Hay que recordar que los protocolos de encaminamiento se pueden clasificar con vector distancia o estado enlace. Esta clasificación describe el algoritmo que usan los encaminadores para calcular el intercambio de información de encaminamiento. Los encaminadores que trabajan con vector distancia normalmente envían sus tablas de encaminamiento completas a los encaminadores vecinos a intervalos regulares de tiempo.

La capacidad de escalabilidad de OSPF se consigue mediante un diseño jerárquico. Podemos dividir la red OSPF en múltiples áreas, lo que permite un mayor control de las actualizaciones de encaminamiento. Hacer un buen diseño de la red en áreas permite al administrador reducir la sobrecarga de paquetes de encaminamiento y mejorar el rendimiento de los encaminadores.

Por lo tanto, las características más importantes del protocolo son las siguientes:

- Velocidad de convergencia. En redes grandes RIP puede tardar unos minutos al converger, ya que toda la tabla de encaminamiento de cada uno de los encaminadores se copia y comparte con los encaminadores vecinos directamente conectados. Con OSPF la convergencia es más rápida, ya que sólo se envían entre encaminadores OSPF los cambios de encaminamiento.

- Soporta VLSM. RIPv1 es un protocolo con clase y no soporta VLSM. OSPF como protocolo sin clase soporta VLSM.

- Tamaño de la red. En entornos RIP, si una red está a más de 15 saltos se considera que no es accesible. Esta restricción limita el uso de RIP a topologías pequeñas. OSPF no tiene esta limitación y por lo tanto está pensado para redes medias y grandes.

- Uso del ancho de banda. RIP envía actualizaciones a sus vecinos de todas sus tablas en forma de *broadcast* cada 30 segundos. Es especialmente problemático en enlaces WAN de baja velocidad, ya que las actualizaciones consumen ancho de banda. OSPF sólo envía actualizaciones cuando se producen cambios.

- Selección del camino. RIP selecciona la mejor ruta en función del número de saltos sin tener en cuenta otros factores, como el retardo de la línea, el ancho de banda, etc. OSPF busca la mejor ruta en función de un parámetro denominado coste que calcula a partir del ancho de banda de la línea.

- Agrupación de miembros. RIP usa una topología plana, de manera que todos los encaminadores forman parte de la misma red. Así, los cambios deben viajar por toda la red. OSPF utiliza un concepto denominado área y crea grupos de encaminadores. Eso provoca que la comunicación de los cambios se realice dentro del área sin que afecte al resto de áreas. Con eso conseguimos que el rendimiento de un área no afecte al resto de áreas.

Border gateway protocol

Cuando miramos Internet desde la perspectiva del usuario aparece como una colección de recursos a los cuales puedes acceder mediante el ISP. La estructura de la topología de Internet, los procesos que permiten la comunicación entre las diferentes entidades de todo el mundo, son irrelevantes desde el punto de vista del usuario. En cambio, si lo que queremos es entender el funcionamiento del protocolo BGP es útil tener unas nociones sobre la topología Internet y la comunicación entre diferentes empresas.

Una *Internetwork* es un grupo de redes más pequeñas que son independientes. Cada una de estas pequeñas redes puede ser propiedad y operar para diferentes organizaciones, como universidades, empresas u otros grupos. Por lo tanto, no sorprende que quien opera con estas redes desee autonomía, administración propia con sus propios sistemas. En muchas ocasiones, el encaminamiento y las políticas de seguridad de una organización pueden entrar en conflicto con las políticas de otros. Así, Internet está dividida en dominios o sistemas autónomos. Cada sistema autónomo representa una organización independiente donde aplica su política de encaminamiento y seguridad.

Los protocolos denominados EGP facilitan el intercambio de información de encaminamiento entre sistemas autónomos.

Se puede decir que un sistema autónomo está formado por un grupo de encaminadores que comparten políticas de encaminamiento similares y operan dentro de un mismo dominio administrativo. Un sistema autónomo puede ser un grupo de encaminadores que siguen todos un mismo protocolo IGP o puede ser una colección de encaminadores que siguen diferentes protocolos pero que pertenecen a una misma organización. En cualquiera de los dos casos, desde el mundo exterior el sistema autónomo se ve como una única entidad.

Los sistemas autónomos quedan identificados por un número asignado por un registro de Internet o por un operador de servicios entre los valores 1 y 65535. Actualmente, el protocolo BGP4 es el protocolo estándar en el mundo de Internet de encaminamiento entre sistemas autónomos.

En general, Internet es una colección arbitraria de sistemas autónomos. Los protocolos EGP se usan para comunicar sistemas autónomos, mientras que dentro de los sistemas autónomos su uso es irrelevante.

Una empresa que quiera usar BGP para intercambiar información de encaminamiento con el ISP debe tener su número de AS. La conexión entre un encaminador de un sistema autónomo y otro encaminador de otro sistema autónomo se llama conexión BGP externa (*external BGP*).

Los encaminadores que hablan BGP entre ellos se comunican sobre una sesión entre iguales (*peer*). Los encaminadores que forman la pareja se llaman vecinos (*neighbors*).

Una vez se establece la comunicación entre encaminadores con una sesión BGP se envían actualizaciones que incluyen rangos de direcciones sumarizadas y el número de AS correspondiente. Los mensajes BGP se envían en una conexión TCP mediante el puerto 179.

A diferencia de los protocolos que trabajan con métricas en BGP, una ruta no es una red o una subred, sino que es una información que tiene el par destino y atributos de camino.

Métricas

Las métricas son los valores que utilizan los protocolos de encaminamiento para decidir el mejor camino hasta un destino.

Los protocolos de encaminamiento basan sus métricas en medidas diferentes, como son el número de saltos, velocidad del enlace, retardo u otras métricas más complejas. La mayoría de protocolos de encaminamiento incorporan bases de datos que contienen todas las redes que el protocolo de encaminamiento reconoce y todos los caminos para cada red. Si el protocolo reconoce más de un camino para llegar a la red de destino, compara la métrica de cada camino y coge el de menor métrica.

Así, tenemos protocolos con métricas muy sencillas, como son RIPv1 y RIPv2 (con métrica número de saltos). Hay otras más complejas, como es el protocolo EIGRP.

Ejemplo. Cálculo de la métrica del protocolo EIGRP

El EIGRP calcula su métrica con los pesos según las diferentes características de la línea de origen hasta el destino. La expresión es la siguiente:

Métrica = (k1 x ancho_de_banda) + (k2 x ancho_de_banda) / (256 - carga) + (k3 x retardo)

Hay un parámetro k5 que, si es diferente a 0, entonces la expresión queda:

Métrica = métrica x k5 / (fiabilidad + k4)

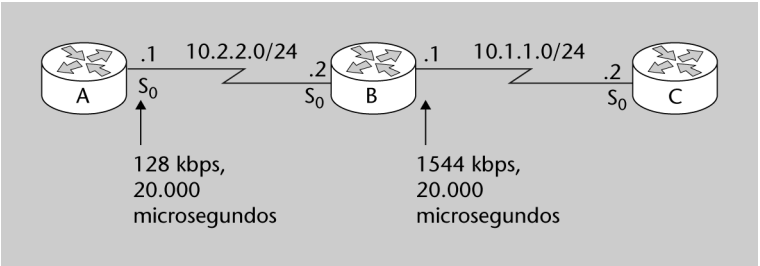
En general, k1 = k3 = 1 y k2 = k4 = k5 = 0.

En este caso, la expresión es:

Métrica = ancho_de_banda + retardo

El ancho de banda se calcula cogiendo el ancho de banda del peor enlace entre el origen y el destino en Kbps. Entonces se divide 10^7 por este valor y el resultado se multiplica por 256. El retardo es la suma de retardos en microsegundos multiplicado por 256.

Figura 14. Topología de ejemplo de cálculo de la métrica EIGRP



Vamos a calcular la métrica que obtendrá el *router* A de la red 10.1.1.0 en el ejemplo de la figura anterior:

a) El *router* B le enviará la actualización de la red 10.1.1.0 al *router* A con la siguiente métrica:

- Ancho_de_banda = (10000000/1544) × 256 = 1658031
- Retardo = (20000/10) × 256 = 512000
- Métrica = 2170031

b) El *router* A calcula su métrica de 10.1.1.0 y pone lo siguiente en su tabla de encaminamiento:

- Ancho_de_banda = (10000000/128) × 256 = 20000000 (considerando el menor ancho de banda de los dos enlaces)
- Retardo = ((20000 + 20000)/10) × 256 = 1024000
- Métrica = 21024000

Convergencia de los protocolos de encaminamiento

Siempre que se produce un cambio en la topología de la red, todos los *routers* de la misma tienen que aprender la nueva topología. Este proceso es a la vez colaborativo e independiente. Los *routers* tienen que compartir información entre ellos, pero deben calcular el impacto del cambio de topología de forma independiente.

Se considera que la red ha convergido cuando todas las tablas de encaminamiento están sincronizadas y cada una de ellas contiene una ruta correcta hacia todas las redes de destino.

Las propiedades de convergencia incluyen la velocidad de propagación de la información de encaminamiento y el cálculo del mejor camino. Cuanto más rápida es la convergencia, más óptimo es el protocolo de encaminamiento.

3. IPv6

3.1. Introducción

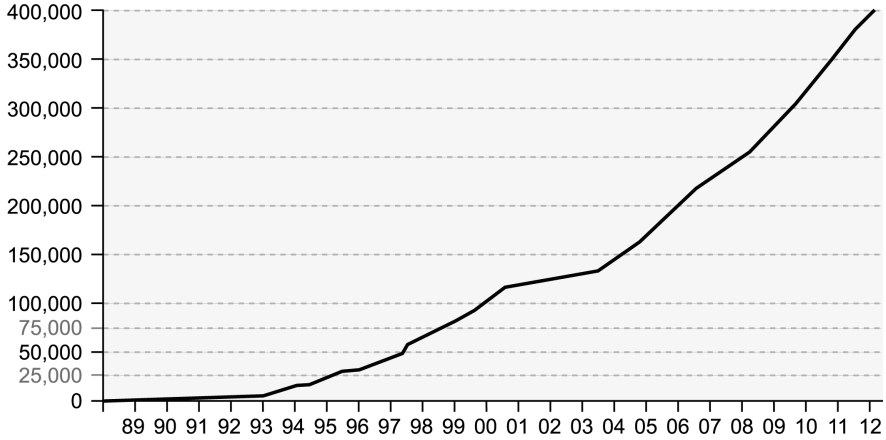
Internet Protocol versión 6 (IPv6) ha sido diseñado como sucesor del protocolo IPv4. No es necesario explicar el rápido crecimiento de internet durante los últimos años, que ha hecho que hoy en día internet sea mucho más que un conjunto de páginas web, servicios de correo electrónico o transferencia de ficheros. Se ha producido un crecimiento del número de dispositivos móviles, las conexiones *peer to peer*, juegos en red, etc., lo que hace que pasemos del internet de los ordenadores al internet de las cosas.

Este crecimiento no fue previsto en el diseño inicial y, por lo tanto, han surgido problemas a los que hay que hacer frente. Los principales problemas de IPv4 son los siguientes:

- El espacio de direcciones IPv4 es insuficiente para dirigir la cantidad de dispositivos conectados.

- Los enrutadores de la red troncal (*backbone network*) de internet mantienen un número excesivo de entradas en sus tablas de enrutamiento. Esto se debe a la mala planificación en las fases iniciales de IPv4, de modo que hay bloques de direcciones IP que están asignados de manera discontinua. Esto dificulta la convergencia de rutas.

Figura 15. Evolución del tamaño de las tablas BGP (1989-211)



En la figura anterior se muestra el crecimiento del número de redes en las tablas de enrutamiento a internet en el periodo entre 1989 y 2012. Si nos fijamos, el crecimiento es especialmente intenso a partir de 1990.

- IPv4 no ayuda a solucionar los problemas de seguridad, cada vez más importantes.

Se han desarrollado algunas soluciones que resuelven el problema de la falta de direcciones a corto plazo, tal como ya hemos visto anteriormente con CIDR y NAT, pero no representan una solución definitiva del problema.

3.1.1. Ventajas de IPv6

- Estructura de direcciones de 128 bits, que garantiza un espacio de direccionamiento suficiente en comparación con los 32 bits de las direcciones IPv4. La disponibilidad de un número casi ilimitado de direcciones IP es el beneficio más convincente para implementar las redes IPv6. Pasamos de tener $4{,}3 \times 10^9$ direcciones disponibles a tener $(4{,}3 \times 10^9)^4$.

- Cabecera simplificada. La simplificación de la cabecera mejora el rendimiento al mismo tiempo que hace más eficiente el enrutamiento; no utiliza suma de verificación (*checksum*); y la extensión de cabecera es más sencilla y eficiente.

- Eliminación de los *broadcast*. IPv6 no usa el *broadcast* de nivel 3. En su lugar, trabaja con direcciones *multicast*.

- Soporte para movilidad y seguridad.

- Varios mecanismos de transición de IPv4 a IPv6.

  Además, incorpora otras ventajas, como son:

  – permite agregar prefijos que son anunciados en las tablas de enrutamiento;
  – es más fácil de gestionar por el hecho de estar conectado a más de un proveedor de internet, y
  – consiente la autoconfiguración, que incluye las direcciones *link-layer* para disponer de la funcionalidad *plug and play* y la comunicación extremo a extremo sin necesitar NAT.

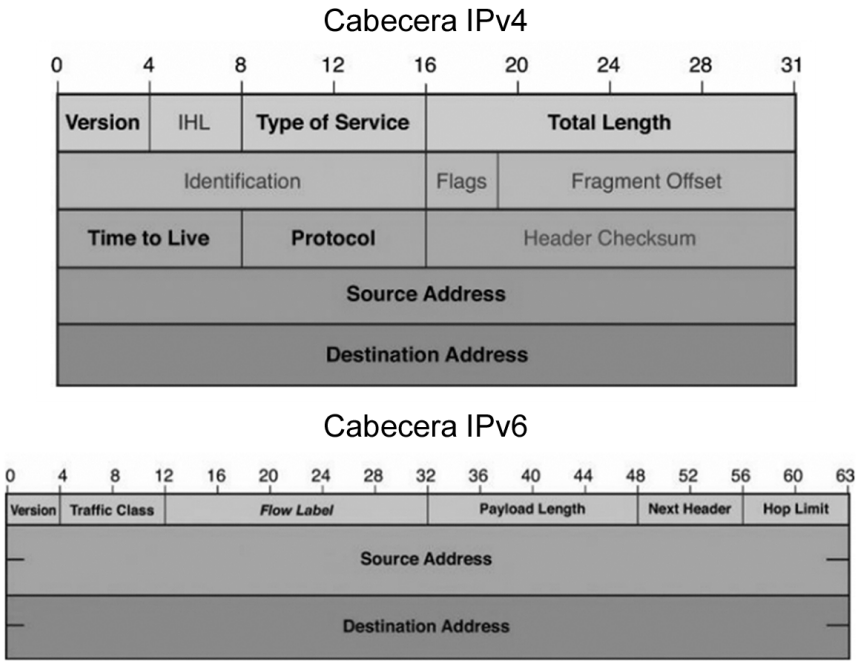
3.2. El protocolo IPv6

Ya se ha comentado que las direcciones de IPv6 son de 128 bits, lo que provoca que no tengamos ningún problema en cuanto al número de direcciones. A pesar de esto, hay que tener presente que este incremento en el número de bits aumenta el tamaño de la cabecera IPv6, dado que pasamos de 64 bits para el campo de direcciones (32 bits de la dirección origen y 32 bits de la dirección destino) a 256 bits en IPv6 (128 bits para cada dirección, la de origen y la de destino).

3.2.1. Cabecera IPv6

La cabecera IPv6 tiene 40 octetos, a diferencia de la cabecera de IPv4, que tiene 20 octetos, tal como se muestra en la figura siguiente:

Figura 16. Cabecera IPv4 respecto a IPv6



IPv6 tiene menos campos, y su tamaño es múltiplo de 64 bits para mejorar la eficiencia y la velocidad de procesamiento. Los campos de IPv6 se explican a continuación:

- **Versión (*Version*) (4 bits):** campo de cuatro bits similar al de la cabecera de IPv4. Este campo tiene un valor de 6 para indicar que se trata de la versión 6 del protocolo.

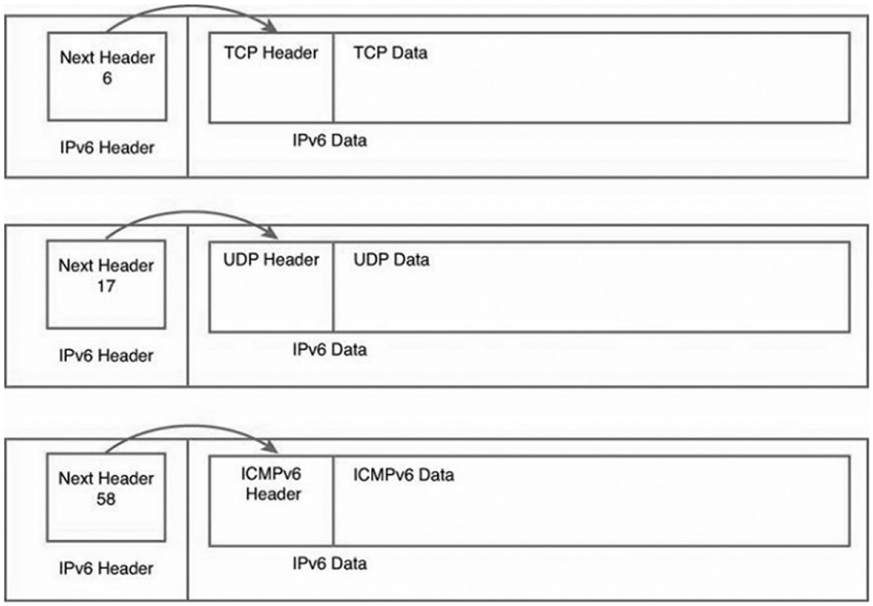
- **Clase de tráfico (*Traffic class*) (8 bits):** es similar al campo de IPv4 llamado tipo de servicio (ToS). Etiqueta los paquetes en servicios diferenciados de calidad de servicio. Al disponer de 6 bits para indicar el DSCP (*Differentiated Service Code Point*), permite una granularidad mucho mayor en el marcado respecto al existente en IPv4, que solo disponía de 3 bits. En la figura se muestra con detalle este campo, tanto para IPv4 como para IPv6.

- **Etiqueta de flujo (*Flow label*):** campo de 20 bits. Lo puede usar el origen del paquete para etiquetar el paquete como parte de un flujo específico, de modo que permite a los enrutadores y *switchs* de nivel 3 gestionar este tráfico como parte de un flujo, en vez de hacerlo paquete por paquete. Esto permite una conmutación más rápida.

- **Longitud de la carga (*Payload length*):** 16 bits similares a los de IPv4.

- **Siguiente cabecera (*Next header*):** campo de 8 bits que indica el tipo de información que viene a continuación de la cabecera. En la figura siguiente se muestran tres ejemplos de cómo funciona este campo. Si el valor de *next header* es igual a 6, se trata de TCP; si el valor es 17, se trata de UDP, y si el valor es 58, entonces se trata de ICMP.

Figura 17. Campo *next header*



- **Límite de saltos (*Hop limit*):** campo de 8 bits que indica el número máximo de saltos que un paquete puede pasar. Es similar al tiempo de vida (TTL) de IPv4 y cada enrutador hace decrecer el valor en unidades. Al no disponer de suma de verificación, no es necesario recalcular su valor.

- **Dirección origen:** campo de 128 bits que identifica el origen del paquete.

- **Dirección destino:** campo de 128 bits que identifica el destinatario del paquete.

Si comparamos las cabeceras de IPv4 y de IPv6, podemos concluir lo siguiente:

- Se mantiene el campo de Versión en ambos protocolos con el mismo número de bits.

- Pasamos de direcciones de 32 bits en IPv4 a direcciones de 128 bits en IPv6, tal como ya se ha indicado.

- El campo Tipo de servicio (*Type of service*) en IPv4 pasa a ser el campo Clase de servicio (*Traffic class*) en IPv6, con un mayor número de bits para diferenciar servicios.

- El campo Longitud total (*Total length*) definido en IPv4 incluye la longitud de los datos y de la cabecera, mientras que el campo Longitud de carga útil (*Payload length*) en IPv6 solo incluye la parte de datos.

- El Tiempo de vida (*Time to live*) en IPv4 pasa a ser Límite de saltos (*Hop limit*) en IPv6, a pesar de que mantiene la misma funcionalidad.

- El campo Protocolo (*Protocol*) de IPv4 pasa a ser el campo Cabecera siguiente (*Next header*), también con la misma funcionalidad.

- En IPv6 se han eliminado los campos siguientes: longitud de la cabecera (*Internet header length*), Identificador (*Identification*), Banderas (*Flags*), *Offset* del fragmento (*Fragment offset*), Suma de verificación, Opciones (*Options*) y Relleno (*Padding*).

- Se ha incluido el campo Etiqueta de flujo (*Flow label*).

Una última característica interesante que incorpora IPv6 respecto a IPv4 es lo que se denomina Descubrimiento del MTU. IPv4 debe tratar con la posibilidad de fragmentación de paquetes en el enrutamiento desde el origen hasta el destino. IPv6 ya no realiza fragmentación. Para conseguirlo, utiliza un proceso de descubrimiento que le permite determinar el MTU óptimo que hay que usar durante una sesión determinada. En este proceso de descubrimiento, el dispositivo origen intenta enviar un paquete (paquete de descubrimiento) con el tamaño especificado por su capa superior (capa de transporte). Si recibe un mensaje IMCP donde se le indica que el paquete es demasiado grande, vuelve a repetir el proceso, pero con un paquete de descubrimiento con MTU más pequeño. Este proceso lo repetirá hasta que el destinatario le envíe un paquete de respuesta de descubrimiento que indique que ha llegado correctamente.

3.2.2. Estructura de las direcciones IPv6

Como se ha dicho, la dirección IPv6 es un conjunto de 128 bits dividido en grupos de 16 bits expresado en hexadecimal. Los grupos de 16 bits están separados por dos puntos (:). Una dirección IPv6, por lo tanto, tiene la forma siguiente:

X : X : X : X : X : X : X : X

Donde cada X representa 4 números hexadecimales de forma que la X puede tomar valores que van de 0000 hasta FFFF. Los números hexadecimales pueden estar expresados en mayúscula y minúscula. Así, una dirección IPv6 puede ser, por ejemplo:

FDEC:BA58:5678:3210:FDEC:BC98:7654:3210

La dirección se puede simplificar si hay ceros consecutivos dentro de la dirección y se expresa como (::). Veamos algún ejemplo:

1080:0:0:0:8:800:200c:417a es equivalente a 1080::8:800:200c:417a

Otros ejemplos de simplificación o equivalencias:

Tabla 1.

Dirección	Dirección equivalente
FF01:0:0:0:0:0:0:101	FF01::101
0:0:0:0:0:0:0:1	::1
0:0:0:0:0:0:0:0	::

En cambio, si tenemos la dirección 2001:0:0:0012:0:0:1234:5456, entonces no se puede hacer 2001::0012::1234:5456. El motivo es que en este caso no podemos saber cuántos ceros han sido eliminados en cada uno de los dos conjuntos. Así, la expresión reducida debería ser, por ejemplo: 2001::0012:0:0:1234:5456.

Ejercicio

Expresad de manera comprimida las direcciones siguientes:

a) 2001:0db8:0000:0000:0000:0000:0000:0c50
b) 2001:0db8:0000:0000:b450:0000:0000:00b4

Solución:

a) En este caso podemos simplificar los ceros intermedios y quedará:

2001:db8::c50.

b) En este segundo caso no se puede hacer como en el apartado a), ya que, como se ha explicado, no sabríamos cuántos ceros hemos eliminado en cada conjunto. La solución entonces será: 2001:db8::b450:0000:0000:b4.

Prefijo

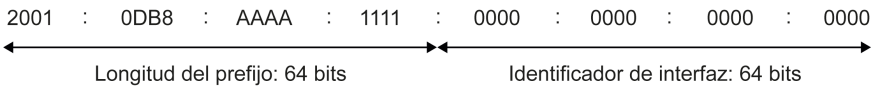
De manera similar a IPv4, los prefijos en IPv6 siguen el formato siguiente:

dirección IPv6 / longitud del prefijo.

La longitud del prefijo es un número decimal que indica la parte de red de la dirección.

Con esta notación tendremos, por ejemplo, para la dirección: 2001:0BD8:AAAA:1111:0000:0000:0000:0000 / 64

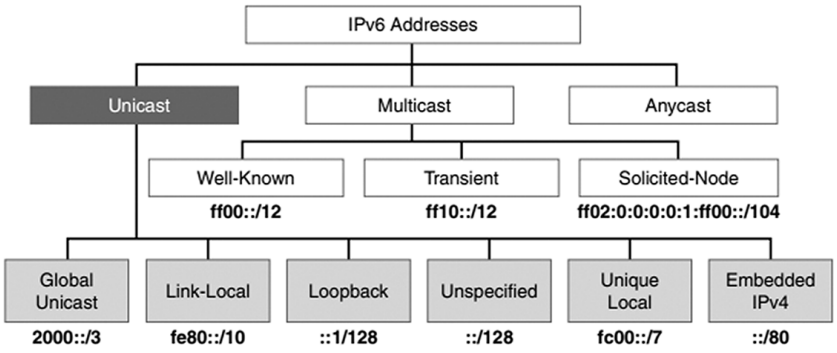
Figura 18.



3.3. Tipos de direcciones

Si recordamos, en IPv4 disponemos de direcciones *unicast*, *broadcast* y *multicast*. En el caso de IPv6 estas tres posibilidades se modifican y se introducen las direcciones *anycast*. Además, en IPv6 se han eliminado las direcciones *broadcast*. Observemos el funcionamiento de cada uno de los tipos de direcciones:

- ***Unicast*:** los paquetes enviados a una dirección *unicast* se transmiten a una única interfaz. Una interfaz puede tener varias direcciones IPv6, además de una dirección IPv4. En el gráfico siguiente se muestran los diferentes tipos de direcciones, destacando las diversas opciones para el caso de *unicast*. De estas posibilidades las dos más importantes son dirección *unicast* global (*global unicast address*) y dirección de enlace local (*link-local address*).



Diferentes tipos de direcciones en IPv6

- **Direcciones *multicast*:** como sabemos, el *multicast* permite que un usuario envíe un paquete a diferentes destinatarios simultáneamente. Una dirección *multicast* define un grupo de dispositivos conocido como grupo *multicast*. IPv6 usa el prefijo ff00::/8 para las direcciones *multicast* de manera equivalente a las direcciones 224.0.0.0/4 utilizadas en IPv4. Hay que recordar que una dirección origen nunca puede ser *multicast*. Además, tal como se ha dicho, IPv6 no dispone de direcciones *broadcast*.

- **Direcciones *anycast*:** una dirección *anycast* es una dirección que puede ser asignada a más de una interfaz (normalmente diferentes dispositivos). Es decir, múltiples dispositivos pueden tener la misma dirección *anycast*. Un paquete enviado a una dirección *anycast* se encamina a la interfaz más cercana que tenga esta dirección, según la tabla de enrutamiento del enrutador.

Las direcciones *anycast* utilizan el mismo rango de direcciones que las direcciones globales *unicast*. Cada dispositivo participante se configura con la misma dirección *anycast*. Así, por ejemplo, podemos tener tres servidores DHCPv6. Los tres tienen la misma dirección *anycast*. El enrutador más cercano al cliente reenviará la petición al servidor «más cercano» identificado en su tabla de enrutamiento. Las direcciones *anycast* no deben usarse como direcciones origen de los paquetes IPv6.

A continuación, explicaremos con más detalle cada una de ellas.

3.3.1. Las direcciones *unicast* globales

Las direcciones *unicast* globales (2000::/3) son las direcciones públicas y se pueden encaminar en internet. Son equivalentes a las direcciones públicas IPv4. Las direcciones globales empiezan en la dirección 2000::/3.

En la figura siguiente se ve cómo se estructuran las direcciones *unicast*. La dirección *unicast* global se puede dividir en tres partes:

- **Prefijo de enrutamiento global (*global routing prefix*):** es la parte de red de la dirección asignada por el proveedor. Este prefijo es equivalente a la parte de red de las direcciones IPv4 y es la parte que los enrutadores examinan para decidir por qué puerto de salida conmutan los paquetes que les llegan.

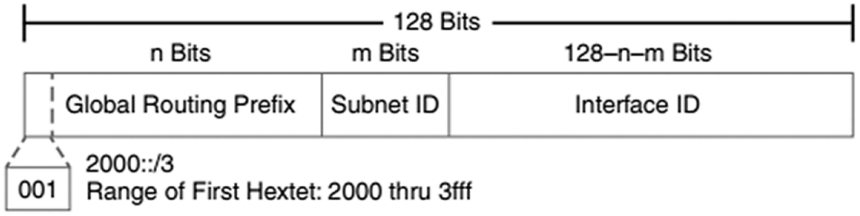
- **ID de subred (*subnet ID*):** a diferencia de IPv4, donde la parte de subred la obteníamos tomando unos bits de la parte de *host*, en IPv6 el identificador de subred es un campo separado y no se toma de la parte de *host*. Sirve como IPv4 para crear diferentes subredes dentro de una organización, sede, departamento, etc.

- **Identificador de interfaz (*interface ID*):** identifica la interfaz dentro de la subred.

En la figura siguiente se pueden ver las tres partes en las que se divide una dirección *unicast* global.

Una diferencia importante con IPv4 es que en IPv6 son legales las direcciones donde en la parte del *host* tiene todo ceros o todo unos.

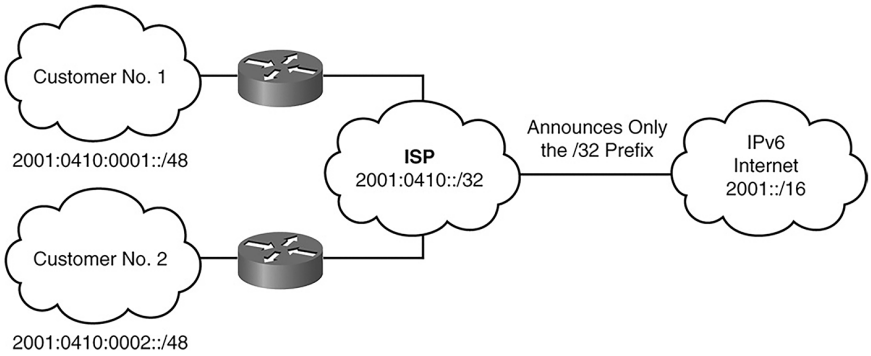
Figura 19. Dirección *unicast* global



La estructura de las direcciones *unicast* globales permite la agregación de prefijos de enrutamiento, de manera que el número de entradas en las tablas de enrutamiento global se puede reducir.

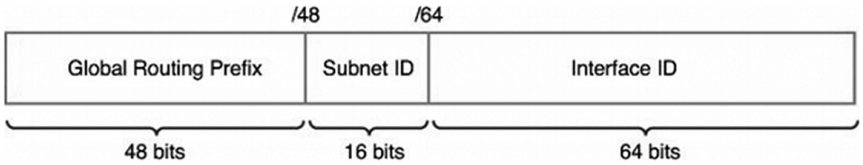
Las direcciones *unicast* globales que se usan en los enlaces se agregan hacia arriba a través de las organizaciones y, finalmente, a los proveedores (ISP).

Figura 20. Ejemplo de agregación de prefijos



La dirección *unicast* global está formada en general por un prefijo de enrutamiento global de 48 bits, 16 bits de identificador de subred y 64 bits de identificador de interfaz.

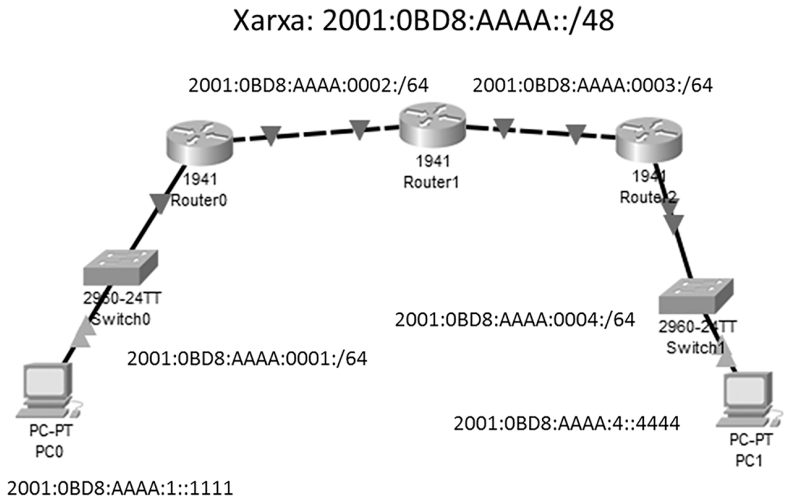
Figura 21. Estructura típica de una dirección global *unicast*



Una manera fácil de identificar cada una de las partes en caso de que sea una dirección típica es la regla 3-1-4, donde tenemos 3 grupos de 16 bits que identifican el prefijo de enrutamiento global, 1 grupo que identifica la subred y 4 grupos que identifican la interfaz.

En la topología siguiente se muestra un ejemplo de direccionamiento:

Figura 22. Topología IPv6



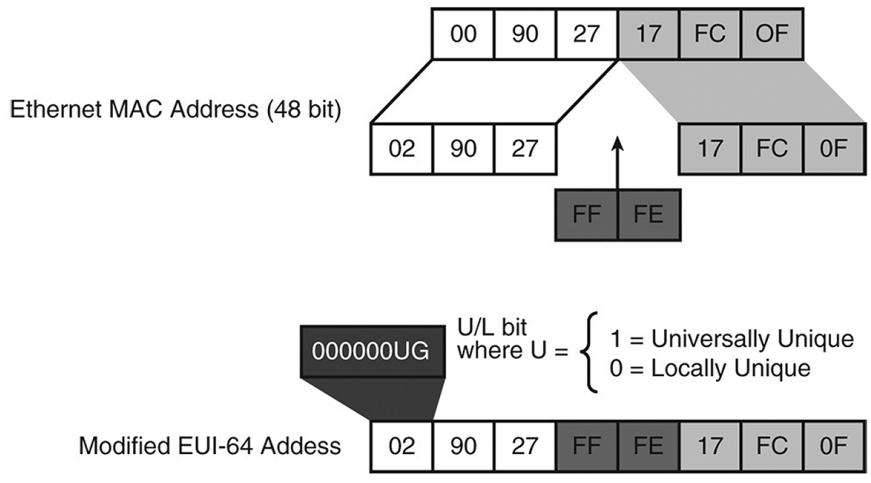
En la figura anterior tenemos inicialmente una dirección de red /48 que indica el prefijo de enrutamiento global. A partir de esta dirección se han creado cuatro subredes /64, las cuales mantienen el prefijo global 2001:0BD8:AAAA y se diferencian mediante los 16 bits de subred.

Un aspecto importante que hay que destacar es la parte de identificador de interfaz. El identificador de interfaz (ID) en IPv6 sirve para identificar una interfaz única en un enlace. Cuando el identificador de interfaz deriva directamente de la dirección del nivel de enlace de la interfaz, el alcance de este identificador se supone que es global.

Los identificadores de interfaces son siempre de 64 bits y se crean de manera dinámica de acuerdo con el nivel 2 del medio y el encapsulamiento.

En el caso, por ejemplo, de Ethernet, el ID se crea a partir de la dirección MAC de la interfaz. Lo que se hace es insertar el número hexadecimal FFFE entre los tres bytes de más peso de la dirección MAC y los tres de menos peso.

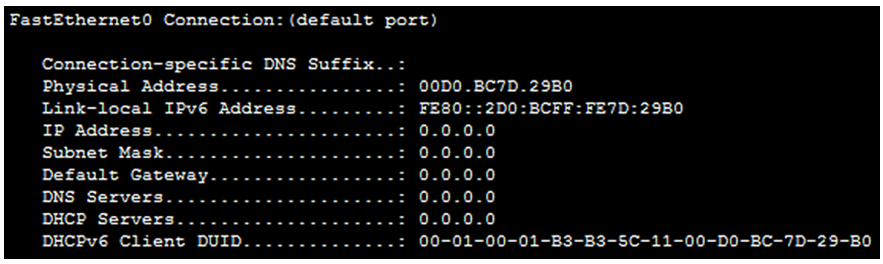
Figura 23. Identificador de interfaz en el caso Ethernet



Además, el segundo bit del byte de más peso de la dirección MAC se pone a 1 para indicar que la dirección es única. Como se ve en la figura, este bit se indica como *U*.

En la figura siguiente se muestra cómo queda el identificador de interfaz IPv6 en el caso concreto de una interfaz Fast Ethernet en un PC. Tal como se ha explicado, se genera a partir de la dirección MAC del dispositivo y con el prefijo FE80::

Figura 24. Identificador de interfaz IPv6 de un ordenador



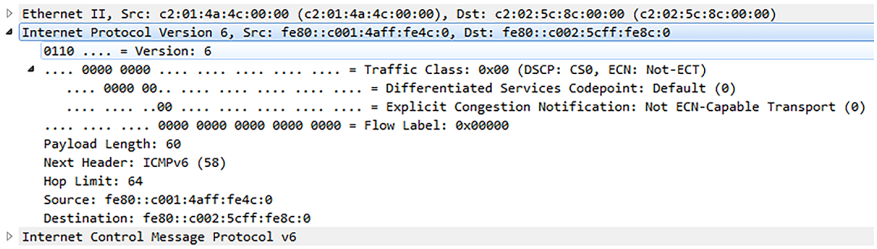
La MAC en esta captura es: 00d0.bc7D.29B0.

Para obtener la dirección IPv6 se divide la dirección MAC en dos partes separadas por FFFE. Las dos partes separadas por FFFE son 00D0BC y 7D29B0.

Finalmente, el segundo bit del byte de más peso se pone a 1, de forma que queda: 02D0BC, como muestra la figura.

Ejercicio

Mientras se manda un mensaje ICMP (*ping*) entre dos dispositivos se hace una captura del tráfico. A continuación, se muestra el detalle de uno de los paquetes enviados.



Se pide:

a) Indicad cuál es la dirección MAC origen y destino.
b) Indicad cuál es la dirección IPv6 origen y destino.
c) Explicad cómo se obtiene la dirección IPv6 sabiendo que el *ping* se ha hecho por medio del identificador de la interfaz IPv6.

Solución

a) Examinando la captura, en la cabecera Ethernet II podemos obtener la dirección MAC origen y destino:

Origen: c2:01:4a:4c:00:00

Destino: c2:02:5c:8c:00:00

b) Dirección IPv6 origen y destino

Origen: FE80::C001:4AFF:FE4C:0

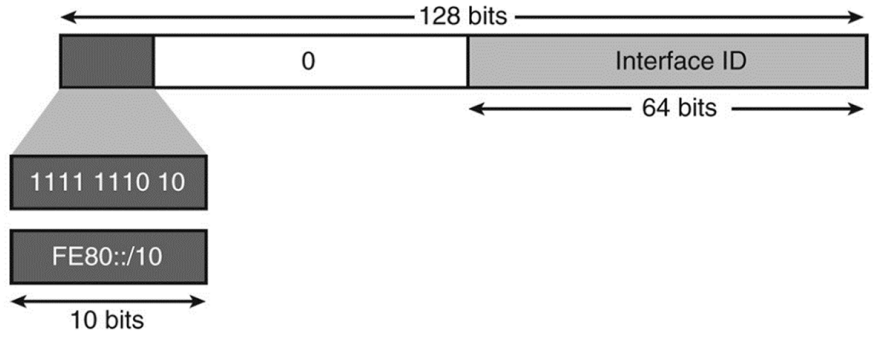
Destino: FE80::C002:5CFF:FE8C:0

c) La dirección IPv6, tal como se ha explicado, se obtendría a partir de la dirección MAC. En concreto, la dirección MAC se divide en dos partes separadas por FFFE.

3.3.2. Direcciones *unicast* de enlace local

Estas direcciones tienen, tal como ya se ha explicado, un alcance local y se crean dinámicamente en todas las interfaces IPv6 mediante un prefijo de enlace local, FE80::/10, y 64 bits del identificador de interfaz. Se usan para la configuración automática de direcciones, descubrimiento de vecinos, descubrimiento de enrutador y para varios protocolos de enrutamiento. En la figura siguiente se muestra la forma de una dirección de enlace local.

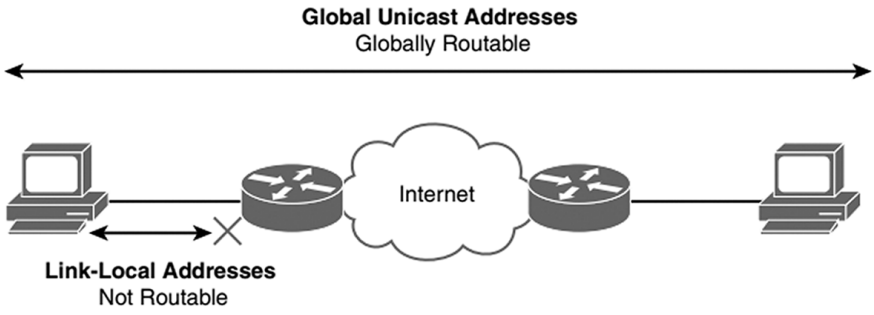
Figura 25. Dirección de enlace local



Un dispositivo IPv6 no ha de tener necesariamente una dirección *unicast* global, sino una dirección *unicast* de enlace local. Normalmente, las direcciones locales empiezan por fe80: y las suele crear automáticamente el sistema operativo del dispositivo.

En la figura siguiente se muestra la diferencia en ámbito de actuación entre dirección *unicast* global y local.

Figura 26. Comparación entre dirección global y local IPv6



3.3.3. Direcciones *anycast*

Como ya se ha avanzado anteriormente, las direcciones *anycast* son direcciones *unicast* globales que se asignan a más de una interfaz. A veces hay servicios en la red que se ofrecen por medio de más de un *host* o enrutador. De este modo se consigue:

- **Redundancia:** el servicio no depende de un único servidor, de modo que si un equipo falla, los otros asumen las tareas y el servicio continúa disponible.

- **Balanceo de carga:** los diferentes servidores se reparten el trabajo de forma que no haya un equipo sobrecargado y otros servidores inactivos.

Cuando un usuario, aplicación o *host* quiere acceder al servicio, no le importa cuál de los múltiples servidores que lo ofrece lo atiende.

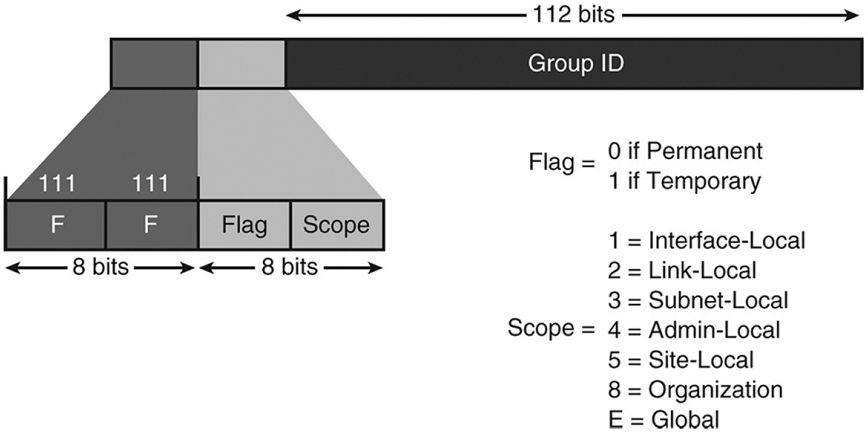
Las direcciones *anycast* permiten este modo de funcionamiento. Cuando un *host* envía un datagrama a una dirección *anycast*, la infraestructura de red buscará el camino más corto hasta uno de los equipos que aceptan datagramas dirigidos a la dirección *anycast* utilizada.

La ventaja más importante de *anycast* es que simplifica la búsqueda del servidor más apropiado, que suele ser el más próximo.

3.3.4. Direcciones *multicast*

El formato de las direcciones *multicast* se muestra en la figura siguiente. Las direcciones *multicast* tienen el prefijo FF00::/8. El segundo octeto define el tiempo de vida (*flag*) y el alcance de la dirección *multicast*, como se muestra en la figura.

Figura 27. Formato de dirección *multicast*



Así, una dirección que empiece por FF02::/16 es una dirección permanente *multicast* con un alcance local. El ID del grupo *multicast* lo forman los 112 bits de menos peso de la dirección *multicast*. El rango comprendido entre FF00:: y FF0F:: tiene el *flag* a 0 y está reservado.

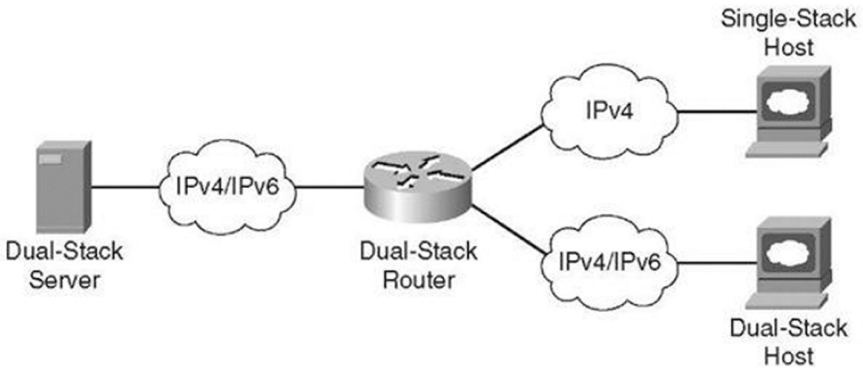
3.4. Tecnologías para hacer la transición de IPv4 a IPv6

Hay dos métodos básicos de compatibilidad entre IPv4 e IPv6: *dual-stack* y *tunneling*. A continuación se explican con algo más de detalle.

- ***Dual-stack*:** el dispositivo se configura para disponer de las dos pilas (*stacks*) IPv4 e IPv6. La configuración de *dual-stack* se puede implementar en una interfaz o en múltiples. En este caso el dispositivo decide cómo envía el tráfico en función de la dirección del otro dispositivo, de modo que elige qué pila utilizar en función de la dirección destino.

  En la figura se ve el ejemplo de un enrutador con *dual-stack*.

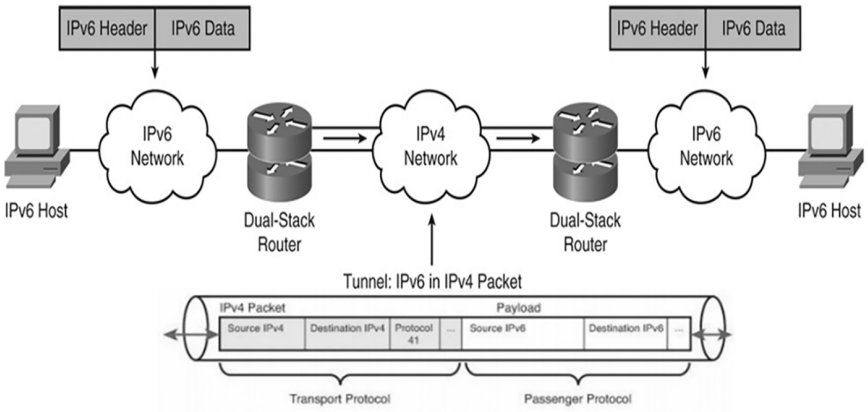
  Figura 28. Ejemplo de enrutador con *dual-stack*



- ***Tunneling*:** cuando se utiliza esta técnica, el enrutador transmite los datos IPv6 por medio de la red IPv4, colocando el paquete IPv6 en el campo de datos del paquete IPv4. Es decir, todo el paquete IPv6 (cabeceras incluidas) se transforma en el campo de datos (*payload*) de un paquete IPv4. El campo «protocolo» de la cabecera IPv4 indica que la parte de datos corresponde a la cabecera IPv6 encapsulada.

Los túneles involucran dos dispositivos, que son los puntos finales del túnel: punto de entrada del túnel (*tunnel entry point*) y punto de salida del túnel (*tunnel exit point*).

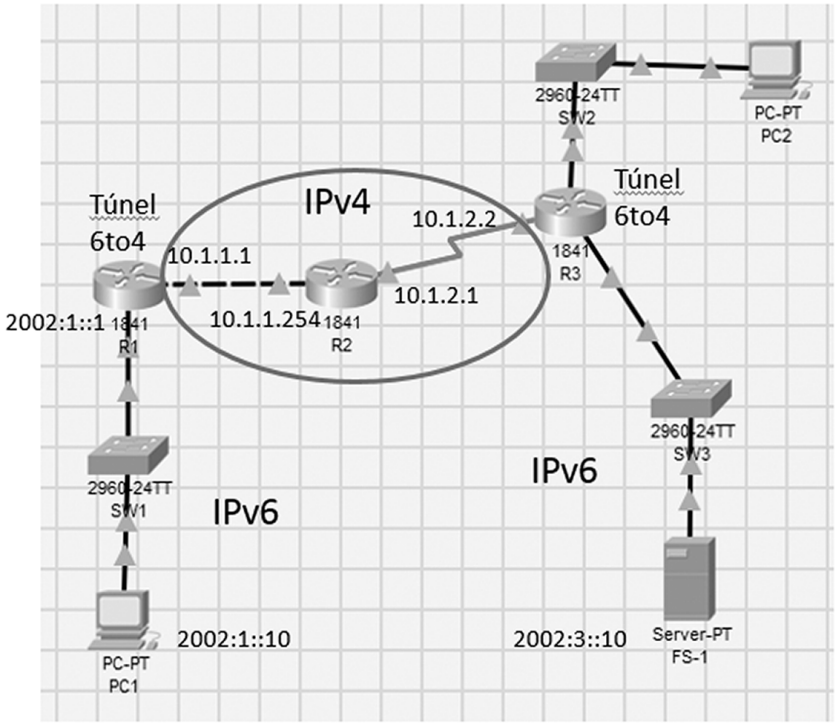
Figura 29. Ejemplo de *tunneling*: IPv6 por medio de una red IPv4



Ejemplo

A continuación, se ha configurado la topología que muestra la figura siguiente para ver el funcionamiento del *tunneling*. La topología está formada por dos redes IPv6, que son: 2002:1::/64 y 2002:3::/64. Estas dos redes están conectadas entre ellas mediante una red que funciona con IPv4. La configuración que se ha realizado es con *tunneling* y lo que se quiere mostrar es cómo este realiza el encapsulamiento y el desencapsulamiento de la cabecera IPv6. Para comprobar el funcionamiento correcto se hace un *ping* entre PC1 y FS-1 (ambos están configurados con IPv6). Tal como se ve en la figura, la transición de una red IPv6 a una red IPv4 se denomina 6to4, mientras que la transición de una red IPv4 a una red IPv6 se denomina 4to6.

Figura 30. Ejemplo de funcionamiento del *tunneling*



Para poder visualizar las diferentes cabeceras de los datagramas enviados en el *ping* se ha hecho una captura de los datagramas en los enrutadores R1 y R3, que son respectivamente los que hacen el encapsulamiento y el desencapsulamiento.

Así, en la figura 32 se muestran las cabeceras de uno de los datagramas enviados por PC1 cuando llega al enrutador R1. Posteriormente, en la figura 33 se muestra cómo el enrutador encapsula el datagrama IPv6 en IPv4. Comentamos con detalle los pasos realizados por el enrutador:

- Una vez que le llega el paquete a R1, examina su tabla de enrutamiento (figura 31) para saber por dónde ha de encaminar para llegar al destino. En la tabla del enrutador tenemos la entrada siguiente:

Figura 31. Tabla del *tunneling* en el enrutador R1

```
R    2002:3::/64 [120/3]
      via FE80::201:C7FF:FED9:CCA, Tunnel1
```

que nos dice que para llegar a la red destino hay que hacerlo vía FE80::201:C/FF:FED9:CCA.

- Decrece el TTL de la cabecera IPv6. En la figura 33, donde se muestra el paquete de entrada, lo indica con *Hop Limit = 128* y en la figura 35, donde se muestra el paquete de salida del enrutador, ha pasado a 127.

- El paquete debe salir por el túnel y, por lo tanto, se encapsula con la cabecera IPv4 (figuras 34 y 35), indicando en el campo protocolo de la cabecera IPv4 valor 41 (0x29), que señala que en el campo de datos se encuentra la cabecera IPv6. Si examinamos la cabecera IPv4 (figura 35), vemos que el destinatario del paquete IPv4 es el enrutador R3, dado que el túnel está hecho entre R1 y R3 (R2 solo funciona con IPv4).

Figura 32. Resumen de las cabeceras del datagrama a la llegada al enrutador R1

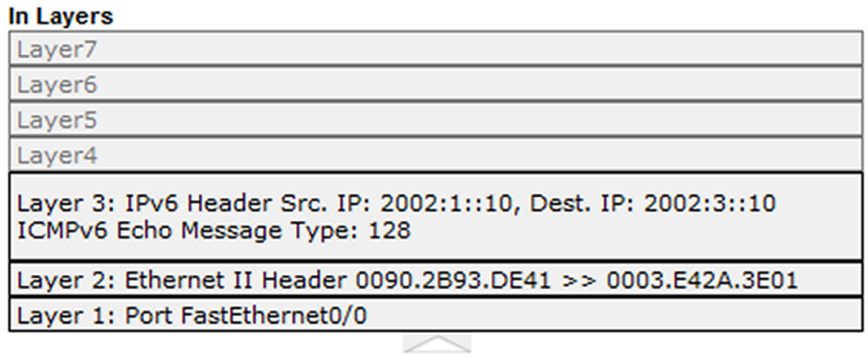


Figura 33. Detalles de los campos de las cabeceras del datagrama enviado por PC1 cuando llega al enrutador R1

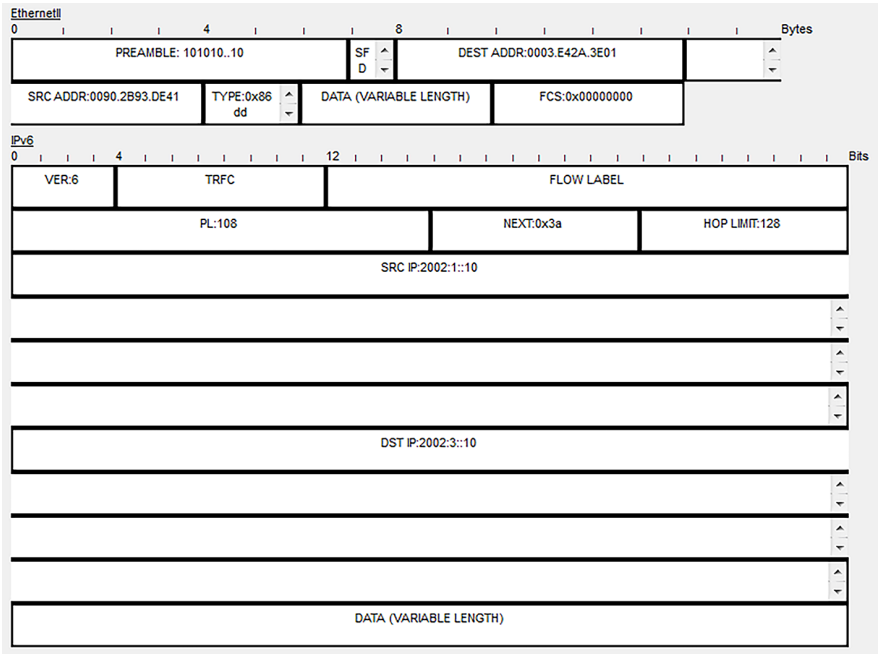


Figura 34. Resumen de las cabeceras del datagrama una vez hecho el *tunneling* en el enrutador R1

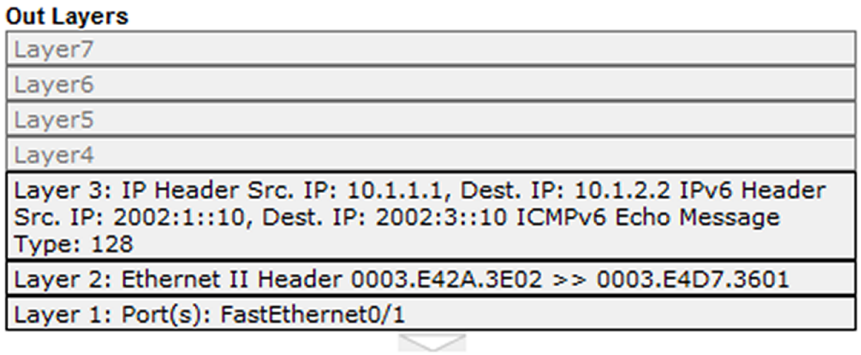
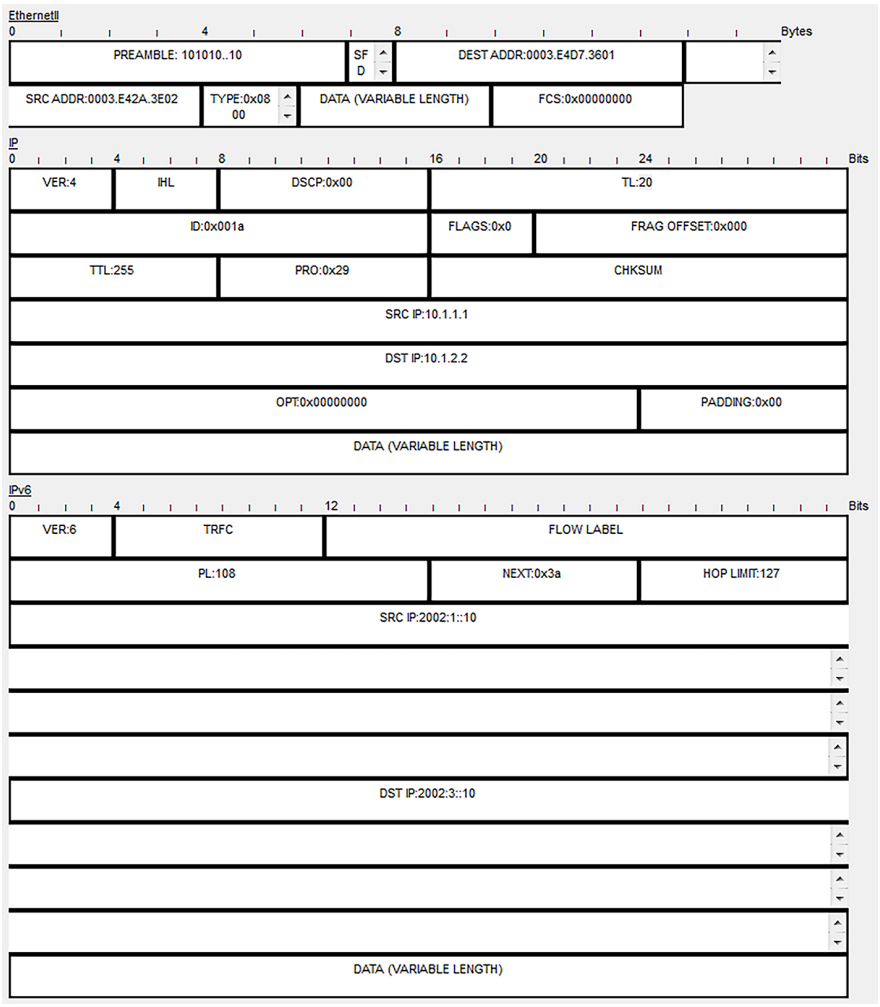


Figura 35. Detalles de las cabeceras del datagrama enviado por R1 una vez hecho el *tunneling*



En R3 se haría el proceso de desencapsulado. Es decir, se quitaría la cabecera IPv4 y el datagrama se continuaría enviando con IPv6.

4. Redes metropolitanas

En este apartado veremos las características principales de las redes metropolitanas, su evolución en los últimos años y las nuevas tecnologías que están emergiendo a causa de los nuevos servicios y necesidades de los clientes. Introduciremos Ethernet como una tecnología de conectividad dentro de la red metropolitana y describiremos las diferentes tecnologías que se pueden usar sobre la infraestructura Ethernet, a la vez que incluiremos la integración con las tecnologías ya existentes, como SDH/SONET o tecnologías emergentes como "el anillo de paquetes fiable" (RPR).

4.1. Las redes metropolitanas

La red metropolitana *metropolitan area network* (MAN) es un tipo de red que siempre se ha clasificado como una red que está entre LAN y WAN. Una red MAN por el hecho de tener órdenes de magnitud cubriría un área que puede ir de 5 a 50 km, aunque estos valores son siempre relativos.

LAN: *local area network*. WAN: *wide area network*.

La red metro es el primer tramo de la red que conecta usuarios finales y empresas a la red WAN. La parte de red metro que llega al usuario final se llama "la última milla", con el fin de indicar que es el último tramo de la red portadora.

El concepto MAN no es nuevo. Surge en torno a los años noventa. En aquella época los anillos TDM (*time division multiplexing*) formaban la red MAN con amplificadores ópticos para cumplir los objetivos de distancia. A mediados de los años noventa fue ATM la tecnología dominante en las redes MAN, por el hecho de que existía la promesa de que ATM sería la tecnología que permitiría la convergencia de datos, voz y vídeo. Además, ATM permitía usar ATM por encima del anillo SDH. El problema consistió en que mientras SDH fue incrementando su estructura, ATM no consiguió introducirse como la solución empleada por el usuario final.

Si miramos en perspectiva la red metro, se puede ver que está básicamente dividida en tres partes:

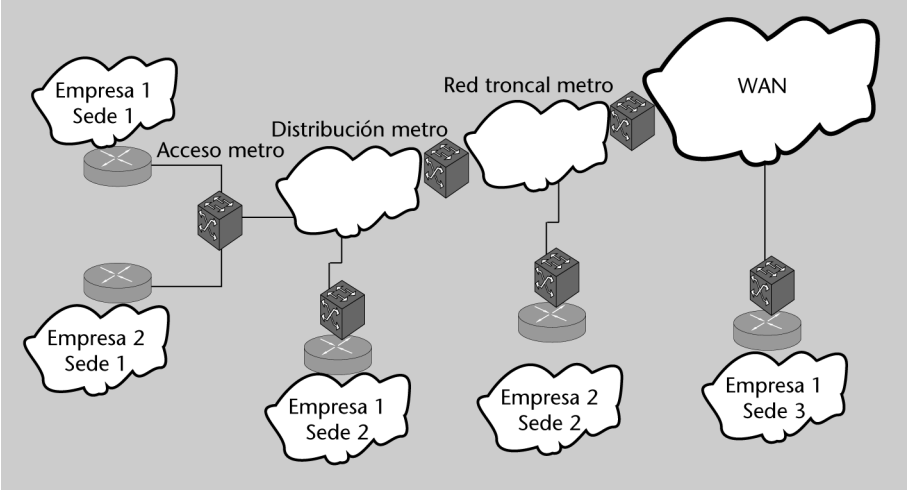
1) Acceso metro (*access metro*). Este segmento constituye la última milla, que es la parte que tocaría al usuario final.

2) Distribución metro (*metro edge*). Este segmento constituye el primer nivel de la agregación metro. Las conexiones que salen de los edificios son agregadas a la CO en conexiones más grandes que sucesivamente son transportadas mediante la red metro o la red WAN.

CO: oficina central.

3) Red troncal metro (*metro core*). Este segmento constituye el segundo nivel de agregación, donde las CO lindantes son agregadas a una CO central. A la vez, las CO centrales se conectan con otras, de modo que forman la red troncal metro desde donde el tráfico es enviado mediante la WAN.

Figura 36. Topología de la red metro



4.1.1. Nuevos requisitos de las redes metropolitanas

La evolución que han tenido las redes metropolitanas ha estado ligada a una serie de nuevos requisitos que se han pedido a la red:

- **Aumento del tráfico de datos y conectividad de banda ancha**. Quizás el reto dominante en entornos MAN es el incremento exponencial de tráfico enviado a la red, atendido mayoritariamente en la explosión en el uso de Internet en todos los entornos. Además del incremento en número de usuarios, la misma naturaleza de las aplicaciones Internet cada vez requieren más ancho de banda.

- **Convergencia y servicios heterogéneos**. Otro factor clave que ha marcado cuál debe ser la evolución de las redes MAN es la convergencia de servicios. Las infraestructuras tradicionales MAN fueron creadas y optimizadas para transportar tráfico de voz, sin prever la posibilidad de que surgieran nuevas necesidades relacionadas con los datos.

- **Expansión de la capacidad de la fibra**. Otro aspecto ha sido el incremento de la capacidad de la fibra. De la misma manera, cuando se hacen infraestructuras se suelen tirar más fibras de lo que se necesita y, por lo tanto, hay fibra infrautilizada.

WDM

WDM (*wavelength division multiplexing*) es una tecnología que permite multiplexar varias señales sobre una fibra óptica mediante portadoras ópticas de diferentes longitudes de onda usando luces procedentes de un láser o un LED.

Un aspecto relacionado con fibra, aunque no sea físicamente, es el incremento de capacidad que ofrece el multiplexado por longitud de onda (WDM). Actualmente WDM soporta hasta cuarenta canales en una fibra y tiene la capacidad de soportar hasta ochenta por fibra.

4.1.2. Retos y oportunidades para los proveedores de servicios

Este cambio en las redes MAN ofrece importantes oportunidades competitivas a los proveedores de servicios, ya que ya no están ligados a las antiguas infraestructuras. Hasta hace pocos años, los usuarios corporativos estaban en manos de los proveedores de servicios de telecomunicaciones tradicionales para mover datos mediante la red MAN, ya que debían alquilar circuitos mantenidos por los proveedores. Además del tiempo de aprovisionamiento o tasas que se debían pagar en función del tráfico solicitado hacía falta añadir la redundancia en cabeceras necesaria para pasar de Ethernet en la red LAN a los protocolos de red MAN.

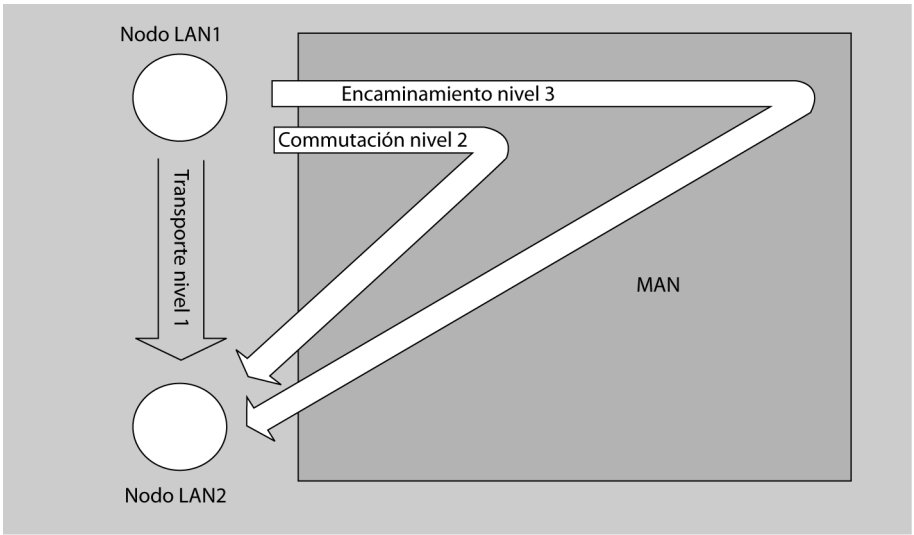
Para el cliente es más cómodo, evidentemente, poder estar conectado a la red MAN y usar protocolos que sean compatibles en las dos redes.

Por lo tanto, para los proveedores de servicios MAN surge una oportunidad si ofrecen nuevas redes con servicios convergentes basados en las capacidades que puede ofrecer Ethernet.

Desde el punto de vista del mercado hay que tener claro lo siguiente:

- Capa óptica de transporte: transporta siempre que puedas.
- Capa de conmutación Ethernet: conmuta cuando lo debas hacer.
- Capa de encaminamiento IP: encamina si no queda otra alternativa.

Figura 37. Entorno de aplicación de cada una de las capas



4.1.3. Restricciones de SDH/SONET

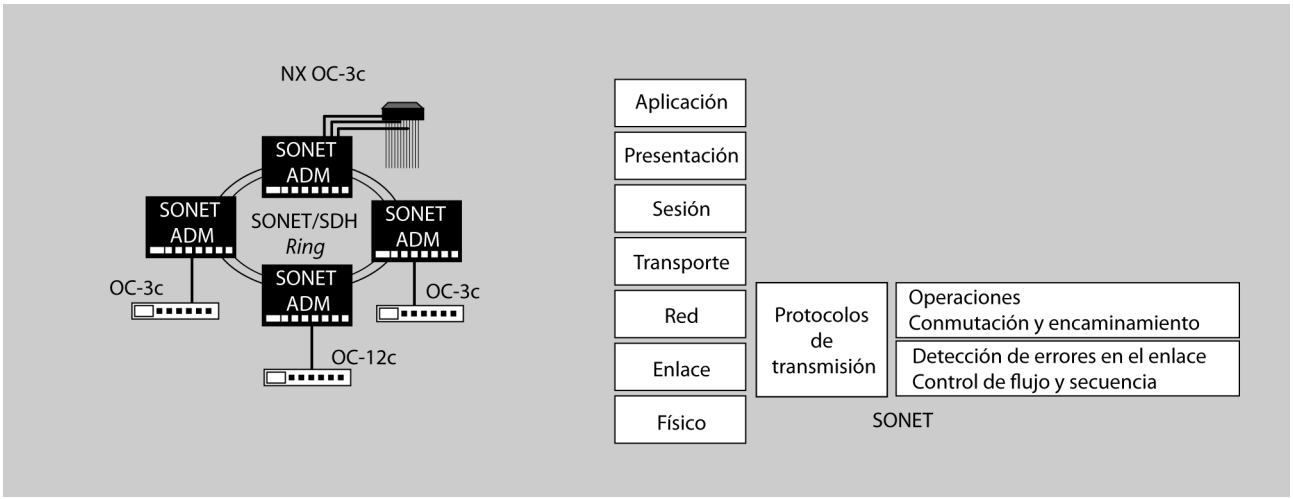
Aunque SDH/SONET está muy extendido por algunas de sus características, como la recuperación ante fallas, la interoperabilidad entre fabricantes, etc., tiene una serie de limitaciones ligadas a su propio origen:

- **Está pensada principalmente para voz**. SONET es una tecnología de multiplexado (conmutación de circuitos), lo cual quiere decir que implementa una arquitectura de telecomunicaciones muy rígida. Va muy bien para voz (ancho de banda y latencia constantes), pero no cumple bien las necesidades básicas de datos, como son la flexibilidad y la escalabilidad.

- **Tiene un coste de expansión muy elevado.** El alto coste de los equipos SONET dificulta a los proveedores de servicios encarar las necesidades de la MAN asociadas al espectacular aumento del tráfico de datos. Los conmutadores (*switchs*) de nueva generación ofrecen precios mucho más bajos.

- **Tiene redundancia de cabeceras**. SONET/SDH proporciona protección de los circuitos e integridad a costa de incorporar una nueva capa de enlace a la ya existente. En el caso de transporte IP lo que hace es que esta nueva cabecera consume capacidad del ancho de banda total (figura 38).

Figura 38. Redundancia de cabeceras en los anillos SONET/SDH



- **Sufre una dificultad de tarifación.** Otra limitación para los proveedores es la dificultad de tarifar adecuadamente estos nuevos servicios, ya que, como sabéis, no se comportan de manera uniforme como el tráfico de voz.

4.2. Las redes Ethernet metropolitanas

Lo primero que hay que hacer es intentar definir qué se entiende por red Ethernet Metropolitana (MEN). Se define como una red que conmuta o conecta empresas LAN geográficamente separadas, mientras que también conecta con las redes *backbone* o WAN de las operadoras. La red MEN proporciona ser-

MEN: ***metro ethernet network.***

Las redes MAN basadas en tecnología Ethernet se llaman MEN.

protocolo central y permitiendo aplicaciones *broadcast*.

Como se ha dicho, Ethernet es una tecnología sobradamente extendida a un precio adecuado y, a la vez, la mayoría de dispositivos de telecomunicaciones disponen de interfaz Ethernet. Las interfaces pueden ir a velocidades de 10/100/1.000 Mbps y desde el año 2002 está ratificado por el IEEE el estándar a 10 Gbps.

Dirección recomendada

Podéis encontrar información, varios documentos y presentaciones con información detallada de las redes Metro Ethernet en http://metroethernetforum.org/

En entornos metropolitanos Ethernet posee un gran potencial, teniendo en cuenta la capacidad que tiene de incrementar la red a un coste efectivo y el hecho de que ofrece la posibilidad de introducir nuevos servicios de manera escalable, sencilla y flexible. Algunos proveedores están extendiendo Ethernet a la red WAN.

Desde el punto de vista empresarial Ethernet tiene dos servicios de aplicación clave: por una parte, conectividad con la red Internet y, por otra, la conectividad entre sedes geográficamente separadas mediante extensiones LAN.

Los enlaces normalmente son punto a punto. Los nodos pueden ser o *switchs* o encaminadores, en función de su localización.

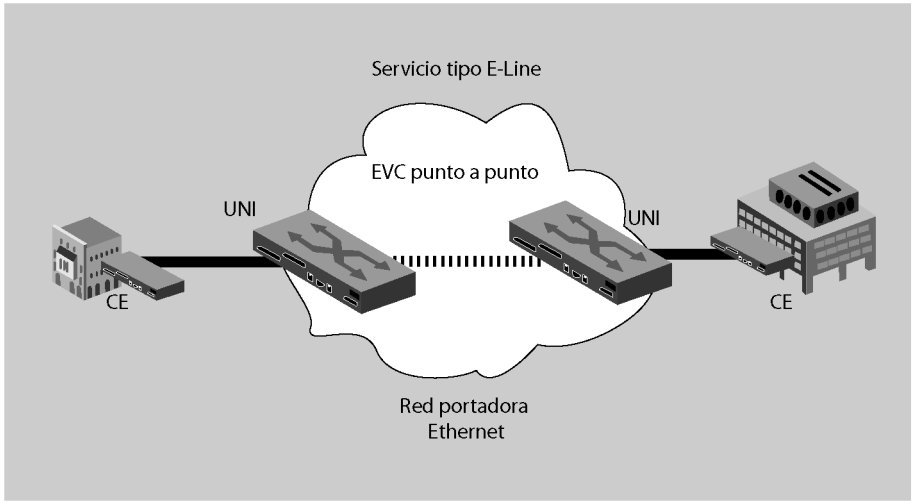
Otro aspecto importante dentro de los servicios Ethernet metropolitanos son las conexiones virtuales Ethernet (EVC). Estas EVC conectan dos o más sedes de usuario (UNI). Los servicios Ethernet, en función de la topología de EVC, se pueden clasificar en:

UNI

El UNI (*user network interface*) es la interfaz física o puerto que es la demarcación entre el usuario y el servicio del operador. El UNI es proporcionado por el operador del servicio.

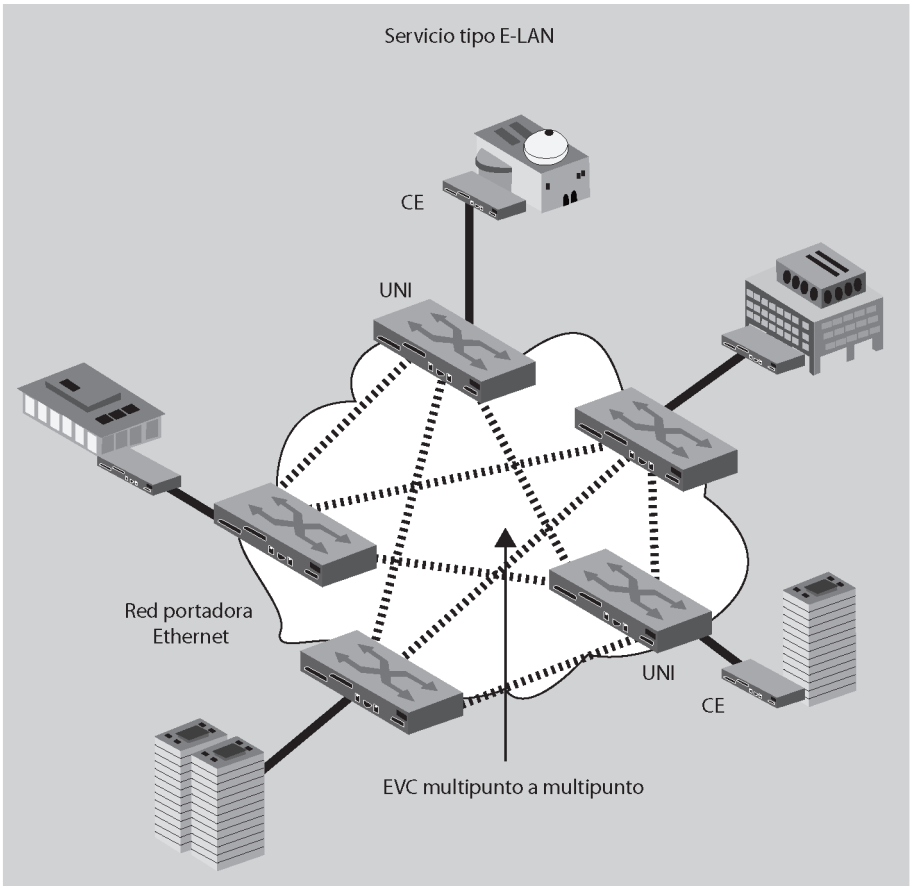
- E-Line: enlaces punto a punto (figura 39).
- E-LAN: enlaces multipunto a multipunto (figura 40).

Figura 39. Ejemplo de E-Line



Los servicios también se pueden clasificar en función del ancho de banda abastecido, de manera que pueden ser exclusivos o compartidos entre varios usuarios.

Figura 40. Ejemplo de E-LAN



4.2.1. Justificación de Metro Ethernet

Las antiguas redes metro (como se ha dicho en apartados anteriores) se basaban en la tecnología TDM (*time division multiplexing*), la cual está optimizada para transportar servicios de voz. Una red metro clásica consiste en un equipo TDM instalado en la planta baja del edificio del cliente y en la central de la operadora. Los equipos TDM son básicamente multiplexores digitales.

La instalación de una red TDM es cara de desarrollar, ya que TDM es una tecnología rígida y no tiene la flexibilidad de escalabilidad económica que necesita el usuario. Para la operadora, una vez hecha la instalación, cuanto menos haya que modificar los espacios habilitados para el usuario y la central local para incrementar los servicios al usuario, mayor será el retorno de la inversión inicial hecha. Así, uno de los problemas de la tecnología TDM es que el ancho de banda de las interfaces TDM no crece de manera lineal a la demanda de los usuarios, sino de manera escalonada.

La tecnología Ethernet está extensamente aceptada en la mayoría de empresas y hay millones de puertos Ethernet instalados. La sencillez de esta tecnología permite escalar las interfaces Ethernet y aumentar el ancho de banda a un precio controlado.

Tanto los precios como el rendimiento y la simplicidad de uso están haciendo que las operadoras de red se planteen Ethernet como una tecnología de acceso.

En este nuevo modelo el usuario tiene una interfaz Ethernet en vez de una interfaz TDM.

Los aspectos siguientes son los que dan valor añadido en Ethernet con respecto a las líneas privadas TDM:

- **Efectivo en costes**. El coste de infraestructura en Ethernet es menor que el de otras soluciones, como son ATM o *frame relay*. Esto se debe a dos motivos:

– La relativa simplicidad técnica de Ethernet.
– La economía de escala, es decir, una base instalada de Ethernet asegura una mejora en los precios. A la vez, los costes de aprovisionamiento son menores comparados con otras soluciones.

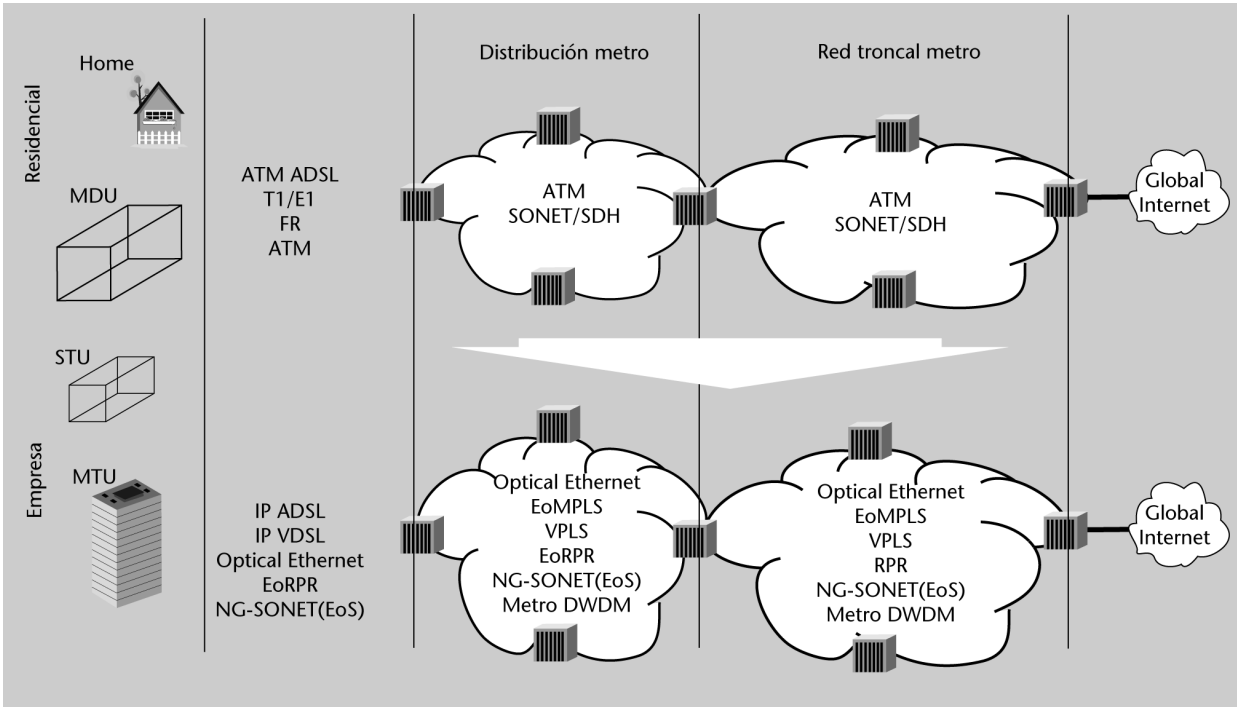
- **Escalabilidad en el ancho de banda**. Desde el punto de vista del operador la velocidad de servicio es una de las claves que lo distingue con respecto a los competidores. Los sistemas ligados a TDM o ATM tienen poca flexibilidad y a la vez no permiten mucho juego a la hora de asignar el ancho de banda que requieren en cada momento los clientes.

- **Basado en paquetes**. Otra ventaja con respecto a otras tecnologías es que Ethernet es una tecnología de tramas asíncrona, lo cual da más flexibilidad que las que son síncronas o basadas en celdas.

- **Fácil de interconecta**r. Este aspecto está asociado al anterior, ya que la simplicidad de interconexión simplifica el aprovisionamiento y permite migraciones a más alta velocidad y con un coste muy menor.

En la figura 41 se muestra la evolución de las redes metropolitanas hacia una red Metro Ethernet.

Figura 41. Evolución de las redes metropolitanas



Aunque, como vemos, las redes Ethernet metropolitanas (MEN) tienen una serie de ventajas si las comparamos con otras redes actuales, como ATM o *frame relay*, podemos encontrar algunas limitaciones, aunque tienen solución:

- **Calidad de servicio garantizada extremo a extremo**. Así, Ethernet necesita incorporar mecanismos para llevar a cabo lo siguiente:

  – Control de admisión por demanda de nuevos servicios. La incorporación de un nuevo servicio no puede comprometer, en ningún caso, el rendimiento de los servicios existentes.
  – Políticas para tener un acceso justo. Mencanismos para asegurar que en momentos de congestión se podrá disponer del ancho de banda en igualdad de condiciones.
  – Establecimiento de un camino óptimo en la red. El algoritmo de STP no busca el camino óptimo.
  – Marcado de los paquetes. Poder marcar los paquetes para dar prioridades, políticas de acceso, etc.

- **Mecanismos de protección**. Al estar pensado inicialmente para entornos LAN no dispone de buenos mecanismos de protección contra interrupciones en la red. Asimismo, tiene una lenta recuperación contra fallos. Ethernet usa el algoritmo de árbol extendido (*spanning tree*) para solucionar problemas en los enlaces, que tarda órdenes de magnitud de segundos para recuperar la red. Por contra, en entornos SONET la recuperación se hace en aproximadamente 50 ms, que son órdenes de magnitud pensadas para aplicaciones críticas, voz y vídeo.

El algoritmo de árbol extendido (*spanning tree*) gestiona los bucles en una red conmutada.

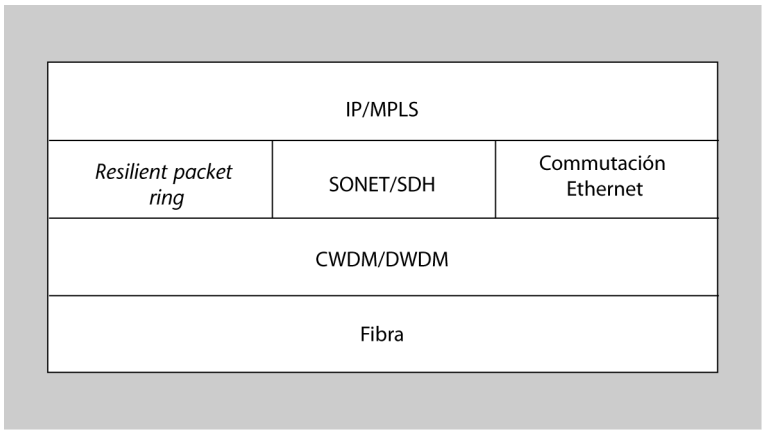
- **Operación, administración y mantenimiento (OAM)**. Ethernet no dispone de las características específicas de SDH para la gestión y mantenimiento de la red.

OAM: *operation, administration and maintenance.*

- **Escalabilidad y utilización de los recursos de la red**. Una de las ventajas de Ethernet es la posibilidad de hacer particiones lógicas sobre la misma red mediante LAN virtuales (VLAN). Si este concepto, usado sobradamente en entorno empresarial, lo extendemos al ámbito de red metropolitana, incorpora nuevos retos que conseguir. El problema que tenemos es que el espacio de etiquetas de VLAN es limitado. El estándar 801.Q define un espacio de direcciones de 4.096 etiquetas disponibles. Este valor es insuficiente para un proveedor de servicios.

Actualmente, hay varias soluciones que conjugan lo mejor de las diferentes tecnologías que existen. Por una parte, hay que aprovechar la infraestructura montada, pero, por otra, hay que aprovechar las ventajas que proporcionan las nuevas tecnologías. En la figura 42 se muestran las distintas posibilidades existentes.

Figura 42. Ethernet en relación con otras tecnologías de los proveedores



4.3. Ethernet sobre SDH (EOS)

EOS: ***Ethernet over SONET/SDH.***

Muchos de los grandes operadores de red han gastado mucho dinero en su infraestructura de SDH en la red metropolitana. A estos operadores les gustaría poder usar esta infraestructura como base para transmitir la nueva generación de servicios Ethernet. El reto principal que tienen es la mejora en la optimización del uso del ancho de banda y el comportamiento del tráfico del servicio de datos.

EOS permite introducir los servicios Ethernet preservando los atributos que proporciona la infraestructura SDH: rápida recuperación, monitorización de la calidad de la línea y la gestión OAM&P.

Con respecto al funcionamiento, EOS encapsula toda la trama Ethernet en la entrada de la red SDH y la desencapsula en la salida.

En la figura 43 se muestra el encapsulado que realiza.

Figura 43. Encapsulado Ethernet en SDH

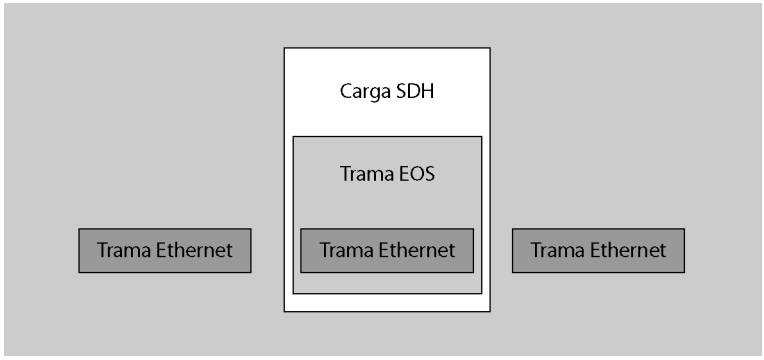
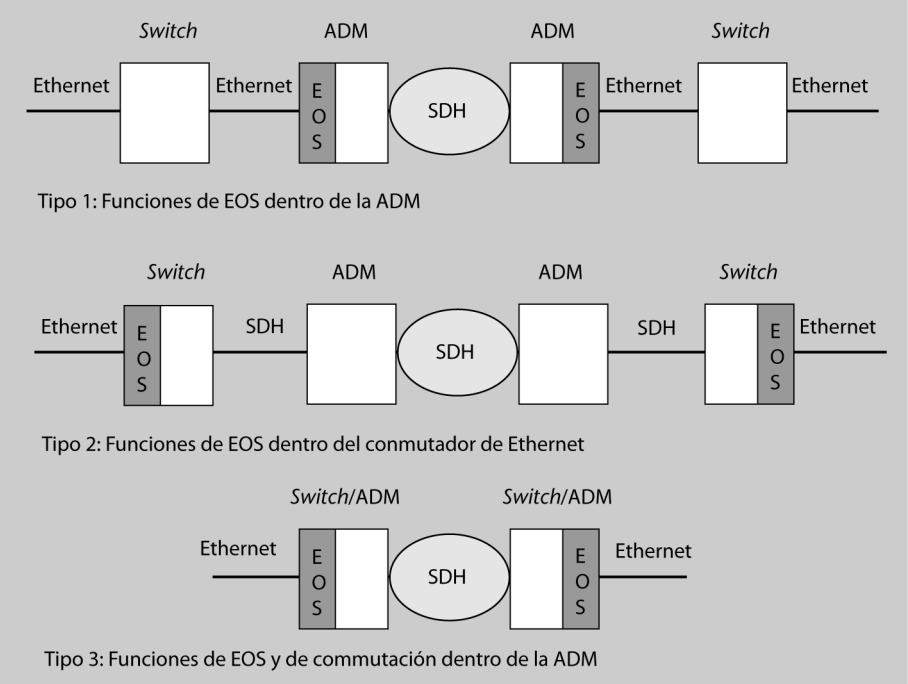


Figura 44. Diferentes escenarios de conexión EOS



Podemos encontrar dos estándares para transportar Ethernet sobre la red SDH:

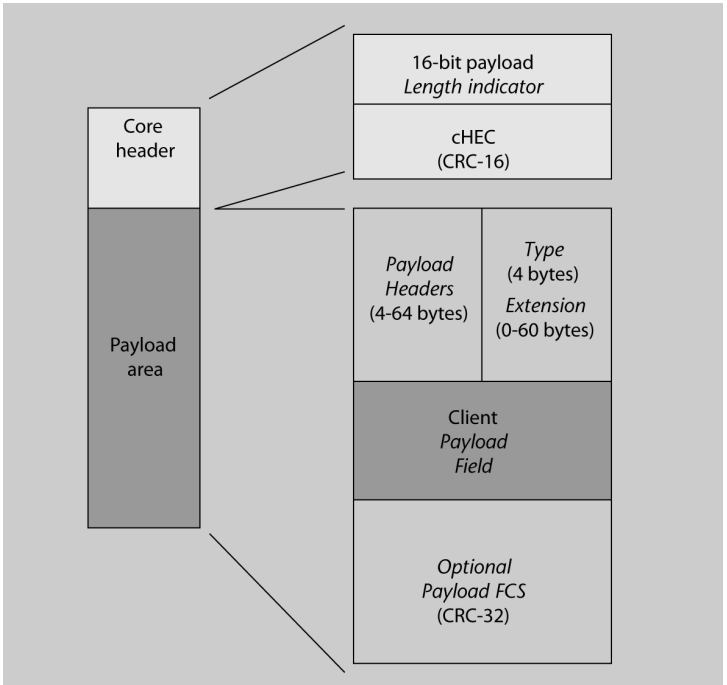
- **LAPS**. Está definido por la ITU-T, que publicó el estándar X.86 en febrero del 2001. LAPS es un protocolo no orientado a conexión similar al protocolo HDLC.

LAPS: *link access procedure SDH.*
HDLC: *high level data link control.*

- **GFP**. También es un estándar de la ITU que usa el protocolo SDL como punto de inicio. Una de las diferencias entre LAPS y GFP es que este último puede acomodar tramas que no sean Ethernet, como son PPP, canales de fibra (*fiber channel*), etc. (figura 45).

Para ampliar la información sobre las tecnologías de acceso, podéis ver el módulo "WAN".

Figura 45. Formato de trama GFP



Las funciones EOS pueden residir dentro de los equipos SONET/SDH o dentro de los equipos de conmutación de paquetes. Eso es bueno porque genera varios escenarios de competencia entre vendedores de equipos de conmutación y vendedores de equipos de transporte para ofrecer conexiones Ethernet.

Uno de los aspectos que hay que solucionar es el ineficiente uso del ancho de banda de los circuitos SDH al transmitir Ethernet. Estas ineficiencias están ligadas a la poca granularidad de los circuitos SDH/SONET y el difícil vínculo con los requisitos de ancho de banda de Ethernet. Para mejorarlo, se incorpora el mecanismo de concatenación virtual (VCAT).

VCAT: ***virtual concatenation.***

4.3.1. Concatenación virtual

La concatenación virtual, como ya habéis visto cuando hemos hablado de SDH, es un mecanismo para reducir el ineficiente ancho de banda de TDM en los anillos SDH/SONET. Por lo tanto, SDH dentro de su estándar incorpora la concatenación, que intenta ajustar el ancho de banda de los circuitos TDM en los anillos SDH a los requisitos de ancho de banda que necesitan en cada momento.

VCAT permite hacer mejor este ajuste del ancho de banda. Así, la concatenación virtual permite agrupar n * VT, lo que posibilita, al mismo tiempo, la creación de conexiones que se pueden ajustar al ancho de banda que se necesita.

4.3.2. Ajustar la capacidad de la conexión (LCAS)

Un segundo aspecto que hay que solucionar en el transporte Ethernet o datos en general es el hecho de que el ancho de banda que necesita el usuario va cambiando en el tiempo y es necesario que las conexiones se vuelvan a redimensionar.

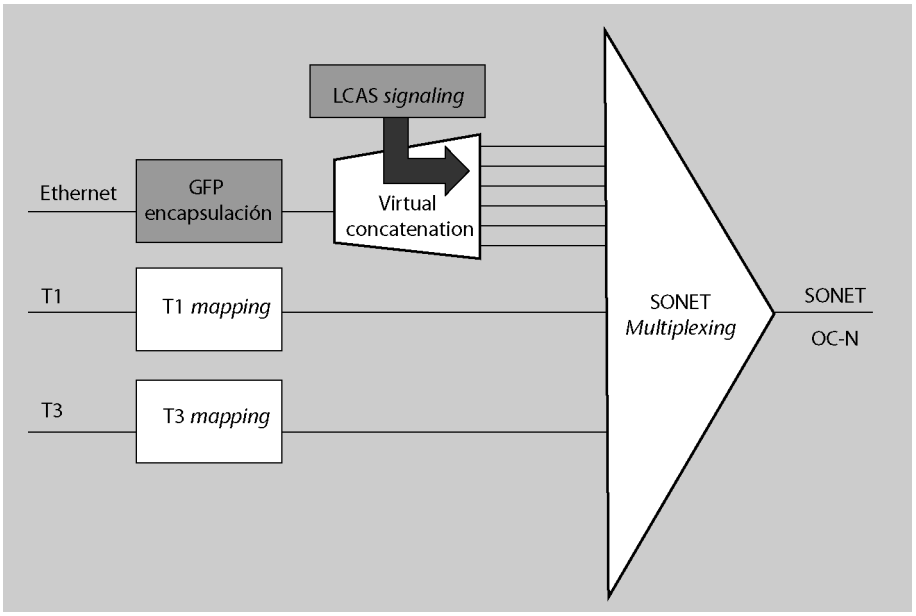
LCAS: ***link capacity adjustment scheme.***

LCAS es un protocolo que permite redimensionar los canales sin necesidad de interrumpir el tráfico de la línea. LCAS también hace un seguimiento de los fallos de la línea, de manera que pueden ser eliminados y se pueden añadir nuevas líneas de manera dinámica sin interrupciones de la línea.

Como conclusión, podemos decir que para transmitir servicios Ethernet sobre SDH lo que proporciona una mejor eficiencia es la combinación de EOS, VCAT y LCAS.

En cuanto a servicio, OES ofrece uno comparable a los de conmutación de paquetes en líneas dedicadas punto a punto.

Figura 46. Señalización LCAS que permite cambiar el ancho de banda bajo demanda



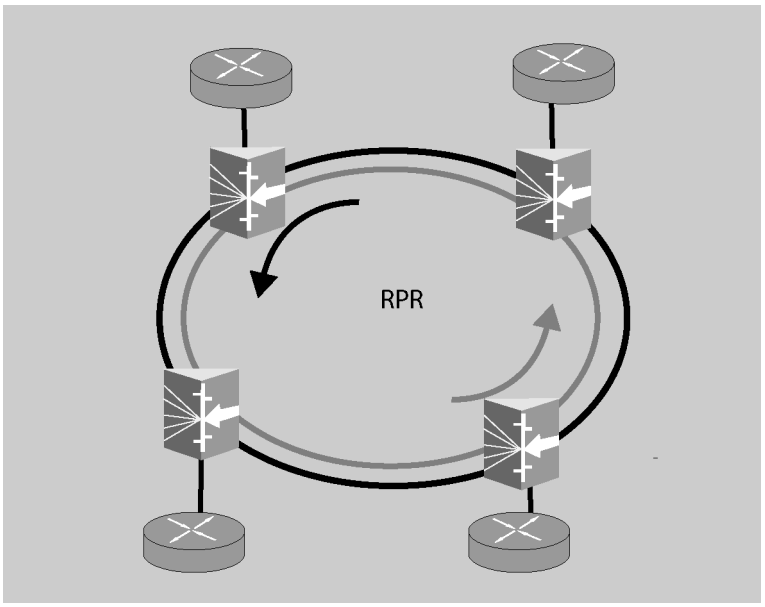
4.4. *Resilient packet ring* (RPR) IEEE 802.17

RPR es un nuevo protocolo de control de acceso al medio diseñado para optimizar la gestión de ancho de banda y facilitar el desarrollo de servicios de datos sobre una red en anillo. El origen es una tecnología propietaria de Cisco, *data packet transport* (DPT).

Para los operadores con infraestructura SDH no resulta una tecnología atractiva, ya que es complicado aplicar RPR sobre SDH.

RPR sirve para conmutación de paquetes en redes en anillo desarrollada sobre fibra oscura o WDM (figura 47).

Figura 47. Topología en anillo en RPR



Se puede decir que RPR y EOS compiten entre sí en el entorno de redes metropolitanas.

La principal ventaja del estándar RPR 802.17 es que los nodos conmutan el paquete sin almacenarlo, si el tráfico no pertenece a este nodo. Esto reduce el trabajo del mismo nodo.

La ventaja con respecto a SDH es que debido a que RPR es conmutación de paquetes se comparte el ancho de banda del anillo. La tarea de RPR consiste en gestionar este ancho de banda.

Recordar que SDH es conmutación de circuitos y lo que asigna son unidades de tiempo (*time slots*) a cada circuito.

El otro punto fuerte de RPR es que el tiempo de recuperación del anillo es de 50 ms, comparable a SDH.

5. Ingeniería de tráfico y VPN en MPLS

En un módulo anterior hemos estudiado MPLS, pero este protocolo ha evolucionado sustancialmente desde los inicios de su desarrollo. Los motivos de uso de MPLS en las redes también han cambiado, ya que actualmente no se utiliza para proporcionar un atajo para el enrutamiento IP. Los dos cambios más significativos de la tecnología MPLS son los siguientes:

- El protocolo RSVP se extiende para dar soporte a la distribución de etiquetas MPLS, que en este caso es conocido como RSVP-TE. Las letras TE se refieren a *traffic engineering* y aportan una serie de características importantes a la ingeniería del tráfico y la tecnología del túnel MPLS.

- MPLS VPN: esta característica permite a la operadora que utiliza la tecnología MPLS crear canales virtuales dentro de la red y usarlos para transmitir de manera privada el tráfico de usuario entre múltiples localizaciones.

5.1. Ingeniería de tráfico MPLS

MPLS: *Traffic Engineering* (MPLS TE)

Como hemos visto en el apartado 2.4, los protocolos de enrutamiento intentan determinar, mediante el uso de las métricas, el mejor camino para encaminar los paquetes. De hecho, el paradigma de conmutación en IP se basa en el enrutamiento de los paquetes por medio del camino de menor coste. Más allá de esto, debemos tener presente que en el enrutamiento de paquetes IP se dan las características siguientes:

- Los paquetes IP se conmutan en cada nodo en función solo de la dirección IP destino, independientemente del camino que han tomado el resto de los paquetes.

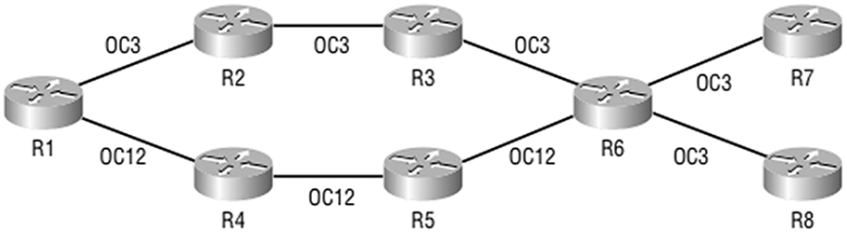
- No se tiene en cuenta la disponibilidad de ancho de banda de la línea en función del tráfico, lo que es diferente al coste que tiene asignado esta línea.

- El conmutador puede continuar conmutando paquetes por una línea a pesar de que esta descarte paquetes por falta de ancho de banda. Esto sucede porque el enrutamiento se realiza en función de la tabla de conmutación y no del volumen de tráfico.

En consecuencia, el paradigma de enrutamiento IP puede provocar situaciones en las que algunos enlaces pueden estar sobreutilizados y, a la vez, otros enlaces pueden estar infrautilizados.

Habitualmente se utiliza una red con forma de pez como ejemplo ilustrativo que permite explicar y justificar el uso de la ingeniería de tráfico. En la figura se ve una red con varios conmutadores con conexiones a diferentes velocidades indicadas por OC3 y OC12.

Figura 48. Red sencilla para justificar la ingeniería de tráfico



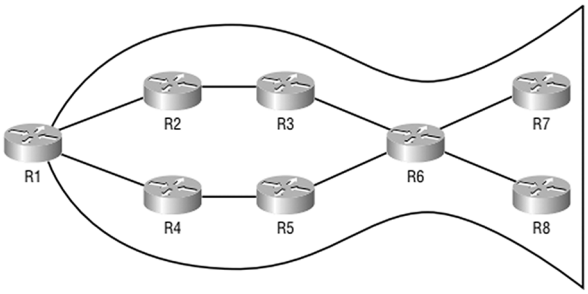
En primer lugar, el objetivo es encontrar cuál es el mejor camino para un flujo de tráfico desde el enrutador R1 hasta R7. Si el protocolo de enrutamiento utiliza el ancho de banda como métrica, entonces el tráfico seguirá el camino R1-R4-R5-R6 y R7.

Imaginemos que ahora tenemos un segundo flujo de tráfico que sale de R8 y llega a R1. Entonces, y del mismo modo que pasaba en el caso anterior, el tráfico seguirá la misma ruta, pero en sentido contrario: R8-R6-R5-R4-R1. Si miráramos el tráfico que va desde R7 hasta R1, el tráfico seguiría el mismo camino. Por lo tanto, si nos fijamos, siempre se usa la misma ruta para encaminar el tráfico mientras los enrutadores R2 y R3 no se utilizan.

Protocolos ampliamente utilizados, como por ejemplo el OSPF, no soportan balanceo de carga por costes no iguales (por ejemplo, velocidades diferentes). Esto provoca que, a pesar de que hay dos caminos posibles entre el origen y el destino, solo se utilizará uno de los caminos en función de la métrica, incluso si esta ruta se satura y llega a perder paquetes.

Nos encontramos, en conclusión, con que la mitad de los enlaces que se han desplegado no se usan. Este problema se denomina «el pez» (*the fish*) por la forma de la red.

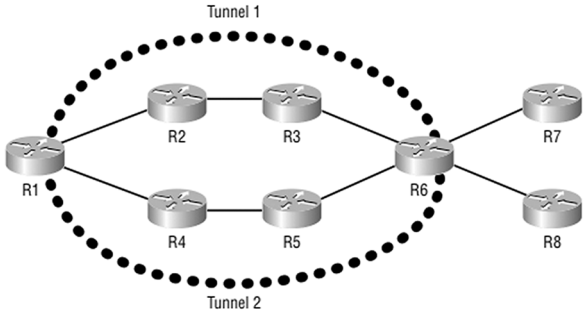
Figura 49. El problema del pez



MPLS soluciona el problema gracias a la ingeniería de tráfico MPLS. MPLS permite crear túneles mediante una pila de etiquetas. En la figura se ve cómo se

pueden crear dos túneles, uno para cada una de las dos rutas. Dado que MPLS soporta túneles con balanceo de carga de diferente coste, el tráfico será balanceado por medio de estos dos túneles.

Figura 50. Ingeniería de tráfico con túneles



MPLS TE es la solución al problema anterior, ya que:

- Proporciona una distribución eficiente del tráfico por medio de la red, evitando que haya enlaces sobreutilizados y otros infrautilizados.

- Tiene en cuenta el ancho de banda configurado de los enlaces. Por ejemplo, en caso de que haya dos enlaces, no distribuye el tráfico de igual manera, sino que tiene en cuenta el ancho de banda de cada enlace.

- Tiene en cuenta métricas del enlace, como por ejemplo el retardo o las diferencias de retardo.

- Se aplica enrutamiento basado en la carga del origen y no solo la dirección destino.

Para conseguirlo, MPLS TE usa las funcionalidades/mecanismos siguientes para un funcionamiento correcto:

- Tener en cuenta las restricciones de los enlaces. Es decir, cuánto tráfico puede soportar cada enlace.

- Emplear un algoritmo que calcula el mejor camino desde el origen LSR hasta el destino LSR.

Recordad que LSR (*label swith router*) es un enrutador/*switch* que es capaz de conmutar paquetes basado en etiquetas.

Utilizar un protocolo de señalización que crea el túnel por medio de la red. Este protocolo es una ampliación de RSVP.

Emplear un mecanismo para conmutar el tráfico por medio del túnel.

5.2. MPLS VPN

Una red VPN es una red que emula una red privada, pero sobre una infraestructura común. La VPN puede proporcionar comunicación en los niveles 2 y 3 de OSI.

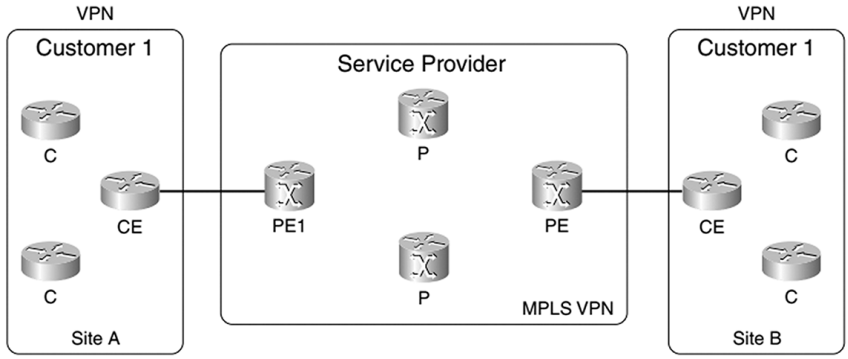
Así, una red privada virtual es una manera fácil de crear una red segura sobre una red compartida para permitir conectar diferentes sedes o el acceso remoto de usuarios a sedes. En lugar de disponer de conexiones dedicadas entre redes, la VPN encamina sus conexiones mediante túneles por medio de las redes públicas, que son lo que ofrecen normalmente los operadores.

VPN (*virtual private network*): red privada virtual.

En el RFC 4364 se define la red VPN sobre MPLS, donde se usa la red compartida MPLS para montar una VPN y poder tener los clientes separados a pesar de que compartan los elementos comunes de la red MPLS. El protocolo de intercambio de etiquetas usado en esta red es MP-BGP (Multiprotocolo-BGP).

En el dibujo se muestran los elementos de red que forman el modelo MPLS VPN.

Figura 51. Esquema de MPLS VPN



Si recordáis, el PE (*provider edge*) es el enrutador que tiene conexión directa con el enrutador CE (*customer edge*) en nivel 3. Un enrutador P (*provider*) es un enrutador sin conexión directa a los enrutadores de los usuarios. En la implementación MPLS VPN, tanto los enrutadores P como los PE trabajan con MPLS. Esto significa que tienen que poder distribuir etiquetas entre ellos y conmutar los paquetes en función de la etiqueta.

El enrutador C (*customer*) es un enrutador sin conexión directa con el enrutador PE. El enrutador CE no necesita trabajar con MPLS.

Para conseguir un funcionamiento correcto MPLS VPN, se requiere el uso de un protocolo de enrutamiento, que en este caso sería el Multiprotocolo BGP, que explicaremos a continuación.

5.2.1. Multiprotocolo BGP

BGP: *Border Gateway Protocol.*

BGP es el protocolo de enrutamiento a la red troncal de internet. Es el protocolo de comunicación mediante el cual se intercambia información de enrutamiento entre sistemas autónomos. Los proveedores (ISP) registrados en internet suelen estar formados por varios sistemas autónomos, y en este caso el protocolo de comunicación entre ellos es BGP. Dentro de los sistemas autónomos es donde se aplicarían los protocolos de enrutamiento, como por ejemplo RIP u OSPF. BGP, a diferencia de estos otros protocolos, no trabaja con mecanismos de vector distancia o estado enlace. En cambio, realiza un intercambio de prefijos o vectores de rutas entre los diferentes sistemas autónomos. Estos vectores de rutas tienen una serie de atributos que pueden influir en el enrutamiento del tráfico. La ventaja de este protocolo es la personalización. Así, cuando se combinan los atributos BGP con políticas de enrutamiento, la personalización del tráfico es muy alta.

Dado que BGP no es capaz de transmitir la información MPLS, ha habido que crear una extensión del protocolo que soporte la creación de MPLS VPN. Este protocolo es el llamado Multiprotocolo BGP (MP-BGP). En concreto, se ha extendido alguno de los atributos para que proporcionen las herramientas necesarias para desarrollar la solución VPN.

5.2.2. VPN de nivel 2 y nivel 3

La tecnología MPLS soporta dos tipos de servicios VPN: VPN de nivel 2 y VPN de nivel 3.

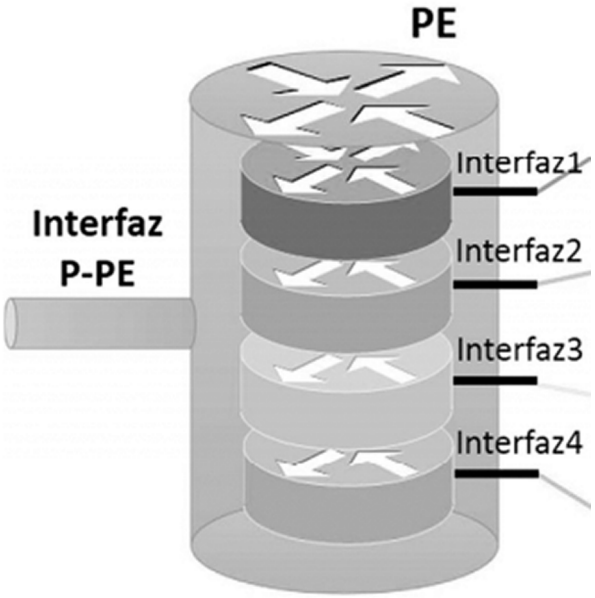
La VPN de nivel 2 también es conocida como Servicio Virtual Privado LAN (VPLS: *Virtual Private LAN Service*). Este servicio crea un canal virtual entre las sedes de usuario que se mantiene totalmente privado para el resto del tráfico de la red de la operadora. Cabe destacar que, con VPN de nivel 2, el enrutamiento se hace en la sede del cliente. Es decir, en el dispositivo CE. Se puede considerar que la operadora es ciega aceptando el tráfico de nivel 2 y transportándolo por medio de interfaces de nivel 2 dentro de la red MPLS.

Con VPN de nivel 3, es la operadora la que se encarga de todo el enrutamiento entre las diferentes sedes del cliente. La VPN de nivel 3 usa las tablas VRP (tabla de enrutamiento VPN).

Para mantener la red de los clientes aislada y que su tráfico no se mezcle en cada PE, se crea un PE virtual dentro de este PE que tiene su propia tabla de enrutamiento VPN (VRF). Este enrutador virtual PE tiene los recursos necesarios para operar como si fuera un enrutador independiente; de este modo se pueden compartir los PE y no hay que montar PE para cada cliente, lo que generaría un aumento de coste en material y mantenimiento. En la figura se mu-

estra este concepto. Se ve un PE que contiene cuatro PE virtuales, lo que permite aislar el tráfico de cada uno de los clientes.

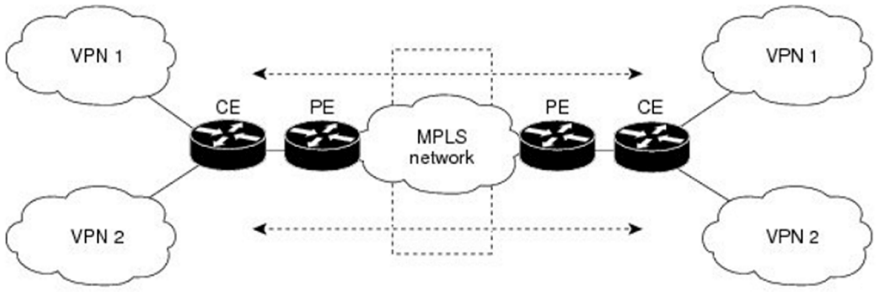
Figura 52. VRF en los PE para dar acceso a diferentes VPN



Con esta tecnología VRF se puede reutilizar el direccionamiento privado, dado que tanto el tráfico como las rutas están separadas en los PE. Cuando a un PE le llega un paquete IP de un CE por una interfaz, sabe a qué VRF pertenece y busca la dirección IP destino en su tabla de enrutamiento para determinar el destino y saber la etiqueta que debe insertar para conmutarlo en el P siguiente y por qué interfaz.

Este modelo es muy escalable porque si introducimos otra sede solo hay que configurar uno o dos PE para que reciba las rutas que el CE anuncia en el PE.

Figura 53. Multi-VRF



5.2.3. Ventajas de las redes MPLS VPN

Estas redes poseen varias ventajas. Las más importantes son las siguientes:

- **Flexibilidad de la tecnología de acceso:** la red MPLS permite usar cualquier tecnología de acceso para conectar la sede del cliente.

- **Flexibilidad de direccionamiento:** con VPN-MPLS los clientes pueden continuar usando el direccionamiento que tengan, dado que se permite el solapamiento de redes entre clientes.
- **Escalabilidad:** cuando incorporamos una nueva sede en la red solo hay que instalar un nuevo CE y darle acceso al PE. En el resto de la red del cliente no hay que hacer ninguna modificación adicional.
- **Calidad de servicio:** se pueden configurar diferentes clases de servicio para priorizar ciertos tipos de flujo.
- **Disponibilidad:** esta red permite varios niveles de redundancia, lo que minimiza los problemas de conectividad y mejora la disponibilidad global de la red.

6. SD-WAN

Software-defined networking (SDN) es un concepto que surgió alrededor de 1990 y cuyo objetivo principal era aportar programabilidad al sector de las redes (*networking*) con el fin de proporcionar más innovación en este campo. Lo que impulsa la necesidad de SDN es la evolución de las tecnologías en la nube (*cloud*) y su virtualización.

6.1. Introducción

En las redes tradicionales, la mayoría de las funcionalidades de red se implementan directamente en los dispositivos, como por ejemplo los enrutadores o *switchs*. Además, dentro de estos dispositivos dedicados la mayoría de las funcionalidades se implementan en hardware dedicado. Este modo de funcionamiento tiene una serie de características:

- La evolución del hardware está bajo el control del fabricante del dispositivo.
- Los dispositivos son propietarios.
- Cada dispositivo está configurado de manera individual.
- Tareas como el aprovisionamiento o la gestión del cambio requieren mucho tiempo y son susceptibles de errores.

Por otro lado, es evidente que el mundo digital se traslada íntegramente hacia la nube. Aplicaciones en la nube, máquinas virtuales que se mueven (migran) dinámicamente entre servidores de manera muy rápida, etc. En cambio, en el modelo tradicional, se puede tardar bastante tiempo en configurar los equipos de red, si se quiere dar servicio en una nueva ubicación.

Utilizando los principios de la red definida por software (*software-defined network*, SDN), SD-WAN permite a las empresas encaminar y priorizar la conectividad de red en las diferentes sedes por medio de la nube, a la vez que simplifica y agiliza el despliegue y reduce el coste de los gastos de hardware asociados, normalmente, a las soluciones WAN tradicionales. SD-WAN está diseñado para permitir a las empresas no solo conectar sedes remotas, como puede hacer MPLS, sino también una rápida conectividad a todas las aplicaciones de la nube que lo necesiten.

SD-WAN utiliza software y tecnologías basadas en la nube para simplificar la entrega de servicios WAN en las diferentes sedes de la empresa. La virtualización basada en software permite la abstracción de la red y, en consecuencia, la simplificación de sus operaciones. SD-WAN permite a los administradores de

tecnologías de la información y de negocio desarrollar conectividad basada en internet de manera fácil, rápida y con calidad, fiabilidad y seguridad.

Las redes definidas por software son un nuevo enfoque de red que permite que la red sea controlada de manera central e inteligente mediante aplicaciones software. El objetivo es que los operadores gestionen la red de manera integral, independientemente de la tecnología de red subyacente. La aplicación de las redes definidas por software al sector WAN se hace por medio de lo que hemos denominado SD-WAN.

6.2. SDN (*software-defined network*)

Tal como se ha explicado, la red definida por software (SDN) es un concepto que emerge alrededor de 1990 y cuyo objetivo es llevar la programabilidad al sector de las redes.

SDN permite la programación del comportamiento de la red de una manera centralizada mediante aplicaciones de software que utilizan API abiertas. Con la apertura de las plataformas de red (normalmente cerradas) y la implementación de una capa de control SDN común, los operadores pueden gestionar toda la red y sus dispositivos de manera consistente y, como se ha dicho, de manera independiente de la complejidad de la tecnología subyacente.

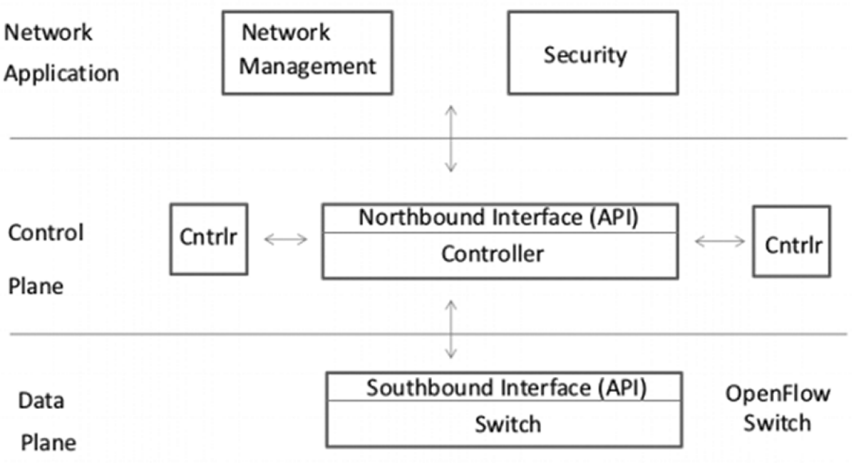
6.2.1. Fundamentos SDN

Las áreas en las que la tecnología SDN puede marcar la diferencia según la Open Networking Foundation (ONF) son las siguientes:

- **Programabilidad o automatización y virtualización de la red:** SDN permite que el comportamiento de la red se controle mediante software, que no está ligado a los dispositivos que proporcionan la conectividad física. Así, se desacopla el hardware del software, de manera que los operadores pueden introducir nuevos servicios diferenciados de manera rápida.

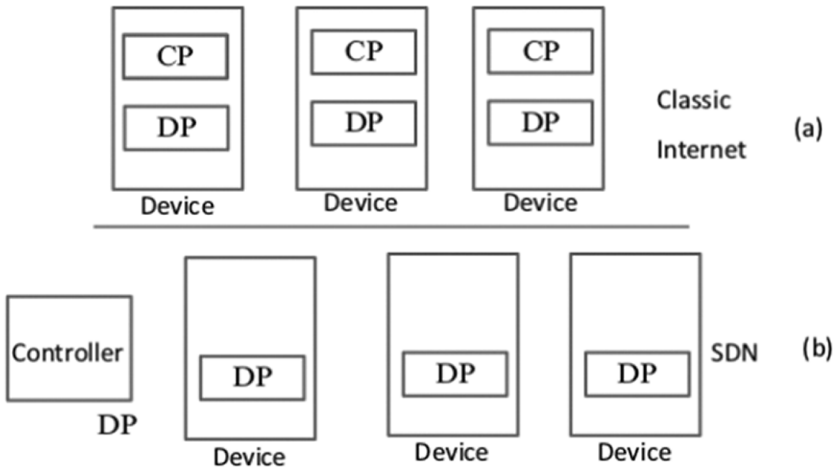
  Esta abstracción permite la virtualización de las funciones de red y una mayor productividad. Esta virtualización es la que permite que SDN no sea específica del vendedor. En la figura se ve una arquitectura SDN con sus dos tipos de enlaces (API), denominados interfaces *northbound* y *southbound*. La API *northbound* se usa para conectar el controlador al plano de gestión donde residen todas las aplicaciones. Este tipo de interfaz puede servir como pasarela hacia la automatización de los niveles altos de la red. La API *southbound* permite al controlador configurar de manera dinámica la conmutación de los dispositivos de red. La API más importante actualmente es OpenFlow.

Figura 54. Arquitectura SDN según la Open Networking Foundation



- **Inteligencia centralizada y control lógico:** SDN permite tener una visión integral de la red, de forma que la administración, restauración, seguridad y políticas de ancho de banda pueden ser óptimas. En la figura siguiente se muestra una comparación entre el internet clásico y los modelos en planos SDN. La arquitectura de internet clásico hace posible los planos de datos y control en cada dispositivo. Esto lleva a una aproximación centrada en el hardware y hace que sea necesario configurar cada dispositivo de manera individual con los comandos específicos de cada fabricante. Como consecuencia, la implementación en entornos de redes grandes significa un trabajo costoso en tiempo y recursos económicos. Por el contrario, tal como se muestra en el apartado b) de la figura, la arquitectura SDN proporciona un modelo centralizado por medio del cual un elemento llamado controlador distribuye las configuraciones necesarias en los otros dispositivos.

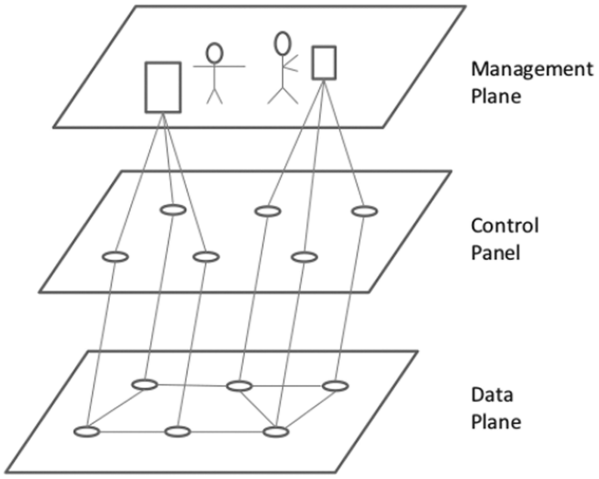
Figura 55. Internet clásico y arquitectura SDN



- **Abstracción de la red:** los servicios y aplicaciones que se ejecutan en la tecnología SDN se abstraen de las tecnologías subyacentes y del hardware que proporciona la conectividad física de control de red. Las aplicaciones interactúan con la red por medio de API, en vez de hacerlo con interfaces de administración estrechamente ligadas al hardware.

La abstracción de la red se concreta en la separación en tres planos. El plano de datos o conmutación, que es responsable de la transmisión de los paquetes basada en las tablas de conmutación. El plano de control, donde tenemos los protocolos que se usan para manipular los mecanismos de conmutación de los datos. Y el plano de gestión, que se apoya en herramientas de software que se usan para interactuar con los protocolos en el plano de control.

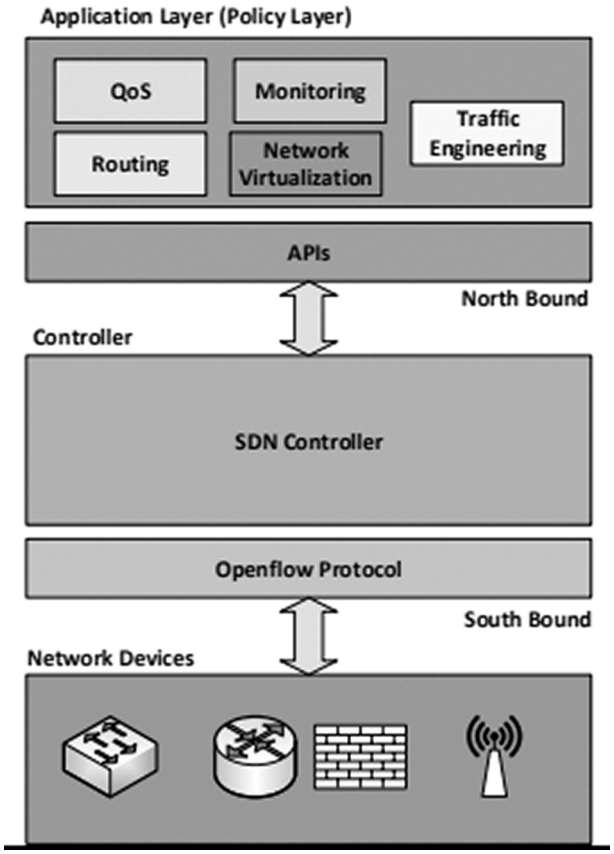
Figura 56. Red a tres niveles



- **Apertura:** la arquitectura SDN permite la interoperabilidad de diferentes proveedores y la posibilidad de no estar vinculado. El software inteligente puede controlar el hardware de múltiples proveedores con interfaces de programación abiertas, como por ejemplo OpenFlow. Desde SDN los servicios de red y las aplicaciones inteligentes pueden ejecutarse dentro de un entorno en software común.

En la figura siguiente se muestra un ejemplo de arquitectura SDN en el que se puede ver que está dividido en tres capas. En la capa inferior tenemos los servidores, cortafuegos, equipos de red, etc., que corresponderían al plano de datos de la arquitectura SDN. Los controladores (*controllers*), que estarían en la capa de control, toman decisiones sobre el destino del tráfico y se comunican con los equipos mediante una interfaz estándar, como puede ser OpenFlow. En redes grandes estos controladores están gestionados por lo que se denomina orquestador (*orchestrator*), por medio de interfaces estándares como Open Stack. Finalmente, en el nivel superior se halla el nivel de aplicación.

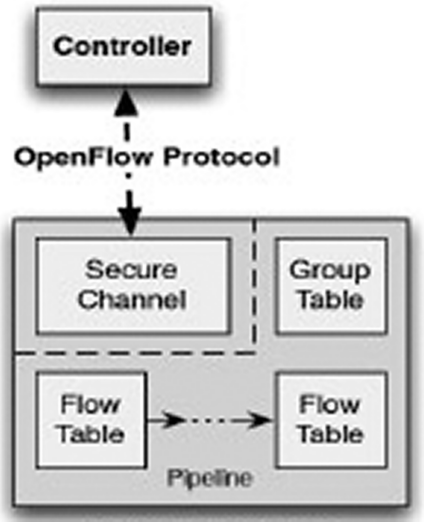
Figura 57. Ejemplo de red aplicando la arquitectura SDN



6.3. OpenFlow

Originalmente, OpenFlow fue creado en la Universidad de Stanford con propósitos experimentales, pero luego fue estandarizado por el ONF. OpenFlow es un protocolo abierto de comunicaciones que permite a un servidor de software determinar el camino de conmutación de paquetes en una red de *switchs*. En una red convencional, cada conmutador tiene software propietario que determina qué acciones (es decir, qué enrutamiento) debe hacer. Gracias al uso de OpenFlow, una parte del enrutamiento reside en el mismo *switch*, pero es el controlador el que realiza las decisiones de enrutamiento de alto nivel. La comunicación entre los dos se hace mediante el protocolo OpenFlow. Utilizando este protocolo, el controlador indica al conmutador cómo debe tratar los paquetes que le llegan.

Figura 58. Conmutador OpenFlow



Fuente: ONF OpenFlow 1.3.0 Switch Specification

El conmutador OpenFlow puede ser programado para realizar las funciones siguientes:

- Identificar y categorizar paquetes de un puerto de entrada basado en varios campos de la cabecera del paquete.
- Procesar los paquetes de varias maneras, incluida la modificación de la cabecera.
- Eliminar o conmutar los paquetes por un puerto de salida o al controlador OpenFlow.

Las instrucciones transmitidas desde el controlador OpenFlow al conmutador OpenFlow se estructuran como flujos. Cada flujo individual contiene unos campos de concordancia de paquete, prioridad del flujo, instrucciones de procesamiento, *timeout* del flujo, etc. Los flujos se organizan en tablas. Un paquete de entrada puede ser procesado por varias tablas de flujos antes de ser conmutado por el puerto de salida.

6.4. SD-WAN

Hay tres grandes factores que conducen a la evolución de las WAN:

- La nube transforma la red.
- Las comunicaciones unificadas se convierten en una parte crítica de la empresa. La computación tradicional toma una aproximación centrada en la red.

SD-WAN es una tecnología que tiene el potencial de revolucionar el sector de las redes WAN. Facilita un nuevo concepto para el sector de las redes que debe permitir que estas se adapten a las necesidades de las aplicaciones (red centrada en las aplicaciones). Este concepto permite a las SD-WAN convertirse en un

sustituto de los servicios de optimización de redes WAN, reducir los costes de gestión, etc.

6.4.1. Arquitectura SD-WAN

Como se muestra en la figura siguiente, SD-WAN tiene una arquitectura basada en tres niveles:

- **Red en la nube (*cloud network*).** Facilita la capacidad de establecer conexiones por medio tanto de infraestructura privada como de infraestructura pública. Está diseñada para facilitar la comunicación entre localizaciones separadas geográficamente, y también con aplicaciones en la nube y servicios. Una parte muy importante de sus funcionalidades se centra en la seguridad, dado que SD-WAN usa la infraestructura de internet como red de transporte.

- **Servicios virtuales (*virtual services*).** Combina tres tipos de servicios: servicios en sedes, servicios en los centros de datos (*data centers*) y servicios en la nube. Es responsable de la optimización de la comunicación de los flujos para cada uno de los diferentes tipos de servicios.

- **Orquestación y análisis (*orchestration and analytics*).** Como se ha explicado cuando hablábamos de los principios de funcionamiento de SDN, SDN se basa en la separación entre planos de control y de datos. Los principios de operación en SD-WAN facilitan el mismo mecanismo, aislando el plano de control en lo que se denomina nivel de orquestación.

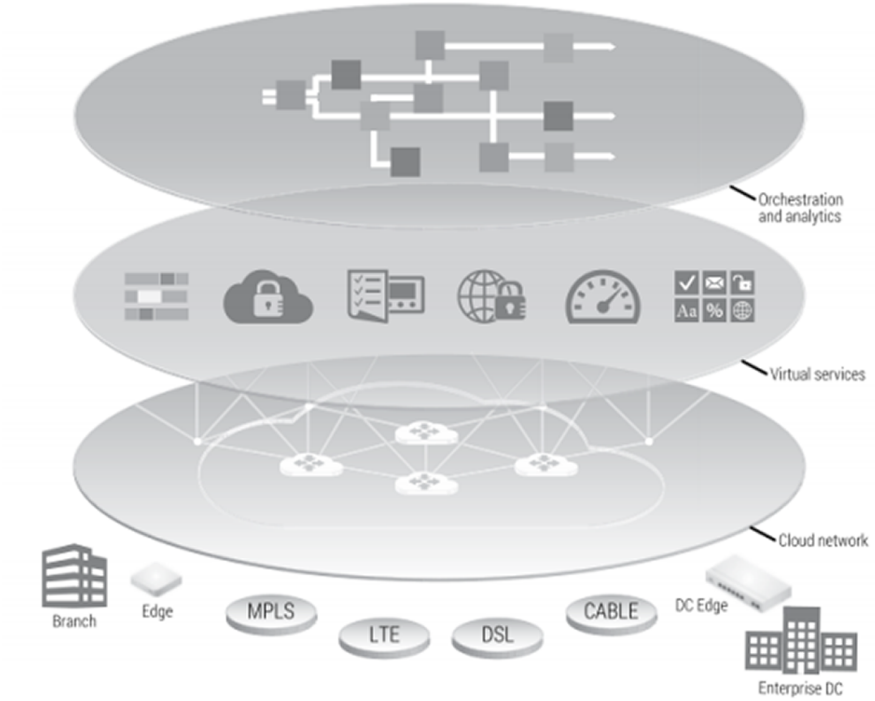
Este nivel tiene tres funciones principales:

1) Plano de gestión: representa un nivel alto de abstracción para el desarrollo de políticas, gestión de la configuración, gestión de errores, monitorización y presentación de informes. La consolidación de estas características crea una interfaz superior de gestión donde no hay que configurar individualmente cada equipo local de cliente (CPE), sino que la configuración se descarga desde el plano de control centralizado una vez que ha sido autenticado. Esta automatización elimina la necesidad de personal cualificado en cada una de las sedes.

2) Plano de control con alta disponibilidad y flexibilidad: permite una transición sin problemas de las tecnologías WAN tradicionales a SD-WAN. Las funciones de gestión del plano de control son accesibles por medio de servicios web o API.

3) Marco de política empresarial: se ocupa de las políticas de garantía de servicio y las estrategias de gobernanza empresarial.

Figura 59. Arquitectura SD-WAN



Resumen

En este módulo didáctico se ha intentado cubrir dos grandes objetivos. Por una parte, ver los elementos básicos en el diseño de redes. En ningún momento se ha pretendido realizar un recetario de lo que ha de ser el diseño, sino hacer una pequeña introducción al tema. La información de lo que se quiere y hacia dónde se quiere ir son dos de los elementos clave en el diseño.

Una vez explicado el diseño de red, se ha explicado la evolución del protocolo IPv4 a IPv6. Se han explicado sus mejoras y sus características más importantes, y nos hemos centrado en dos aspectos fundamentales: el cambio en el direccionamiento en IPv6 y la transición de IPv4 a IPv6.

En cuanto a la red metropolitana se ha explicado el entorno de actuación, soluciones actuales con sus limitaciones para cubrir las nuevas necesidades existentes. A partir de estas limitaciones se han querido introducir las nuevas propuestas actuales, como Metro Ethernet, y las diferentes soluciones para hacer convivir las tecnologías ya implantadas (SDH) con Metro Ethernet.

En el ámbito de red troncal de las operadoras e internet se han explicado las dos tendencias más importantes del mercado. Por un lado, el uso de MPLS con la ingeniería de red y las redes privadas virtuales y, por otro, la posibilidad de trabajar con redes definidas por software (SD-WAN). Tal como se ha explicado, son un nuevo enfoque de red que permite que la red sea controlada de manera central e inteligente mediante aplicaciones de software.

En todo momento debe quedar claro que estas nuevas tecnologías no son únicas y que no siempre son la mejor solución para todos los casos. Los requisitos nos han de marcar cuál debe ser la solución, y no ha de ser la solución la que nos marque los requisitos.

Actividades

1. Buscad en Wikipedia información sobre el protocolo de encaminamiento RIPv1. Determinad las características principales y los inconvenientes.

2. Justificad por qué motivo una red conmutada con conmutadores (*switchs*) no puede tener bucles.

3. Buscad información sobre el estándar 802.1p.

4. Determinad las características según el mercado del sistema ideal en redes metropolitanas.

Dirección recomendada

Podéis consultar Wikipedia en la dirección http://www.wikipedia.org

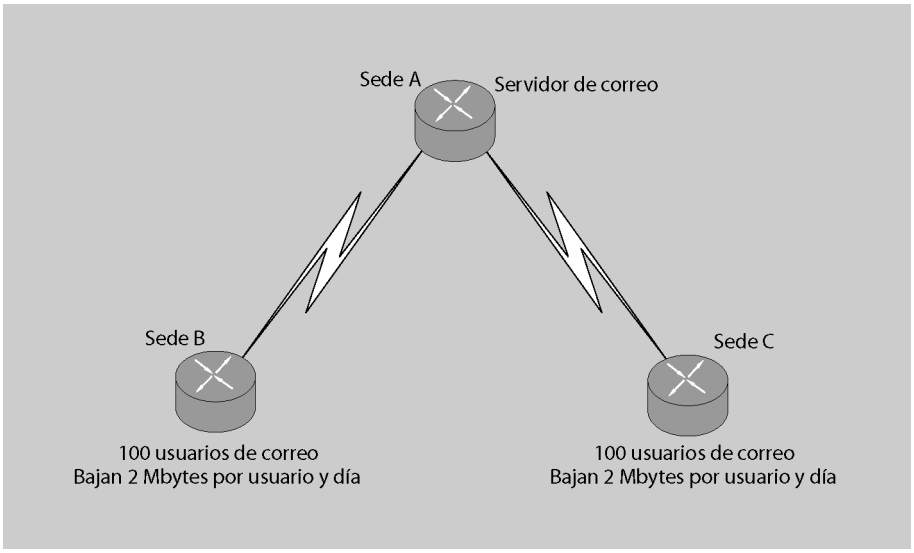
Ejercicios de autoevaluación

1. En la figura 60 se muestra el esquema de la topología de una empresa donde se presentan unos requisitos mínimos. Determinad el ancho de banda requerido para cada una de las sedes en los siguientes casos:

a) El correo se descarga durante todo el día.

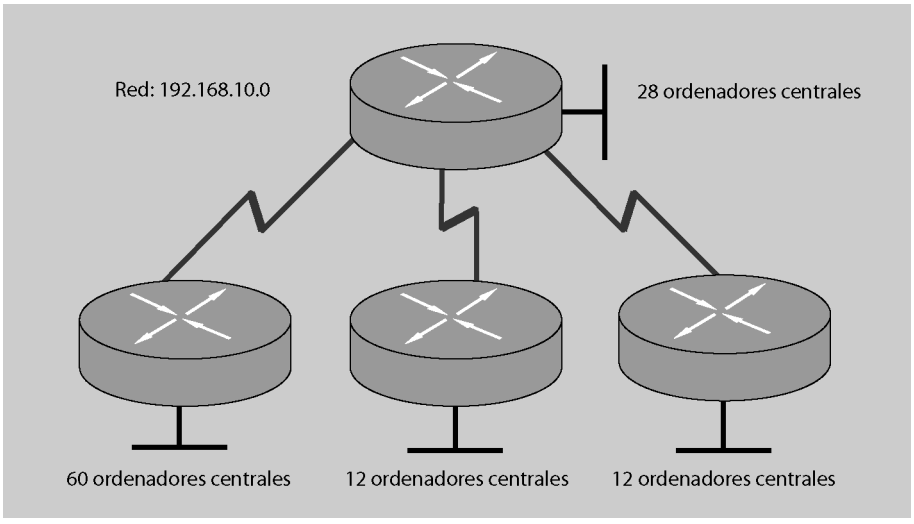
b) Hay un pico de tráfico cuando arrancamos el Outlook por la mañana, entre las 8 y las 8.15 horas.

Figura 60.



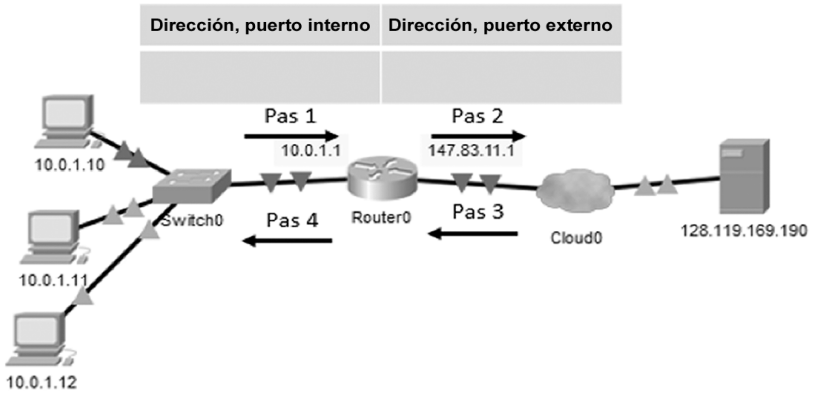
2. Realizad el direccionamiento IP de longitud variable (VLSM) adecuado para la topología de red de la figura 61.

Figura 61.



3. Suponed el escenario de una figura en la que hay tres *hosts* con direcciones IP 10.0.1.10, 10.0.1.11 y 10.0.1.12 en una red local Ethernet detrás del enrutador que realiza NAT para salir a internet. El enrutador tiene en la interfaz Ethernet la IP 10.0.1.1, mientras que por su lado internet tiene la IP 147.83.11.1. Suponed que el *host* con IP 10.0.1.12 envía un datagrama con destino 128.119.174.185. El puerto origen es el 3344 y el destino el 80.

Sabiendo que se realiza NAT *overloading* con la IP externa del enrutador, indicad para cada uno de los casos que se muestran en la figura (paso 1, paso 2, paso 3 y paso 4) cuáles son las direcciones IP origen y destino del datagrama y cuáles son los números del puerto origen y destino de los segmentos TCP dentro del datagrama.



4. A continuación, se muestran las tablas NAT de dos enrutadores. Se pide que justifiquéis el tipo de NAT que realizan en cada uno de los dos casos:

```
Router#show ip nat trans
Pro   Inside global   Inside local   Outside local   Outside global
---   192.2.2.1       10.1.1.1       ---             ---
---   192.2.2.2       10.1.1.2       ---             ---
```

```
Router#sh ip nat trans
Pro Inside global      Inside local       Outside local      Outside global
tcp 170.168.2.1:11003  10.1.1.1:11003     172.40.2.2:23      172.40.2.2:23
tcp 170.168.2.1:1067   10.1.1.1:1067      172.40.2.3:23      172.40.2.3:23
```

5. Expresad de forma comprimida las direcciones siguientes:

a) 2000:0000:0000:0000:0000:ABCD:0000:0025

b) 3FFF:FF00:0000:0000:ACAD:0025:0000:0127

c) FF00:ACAD:0000:0000:1234:0000:0000:0001

6. A partir de las direcciones simplificadas siguientes, obtened la dirección sin simplificar:

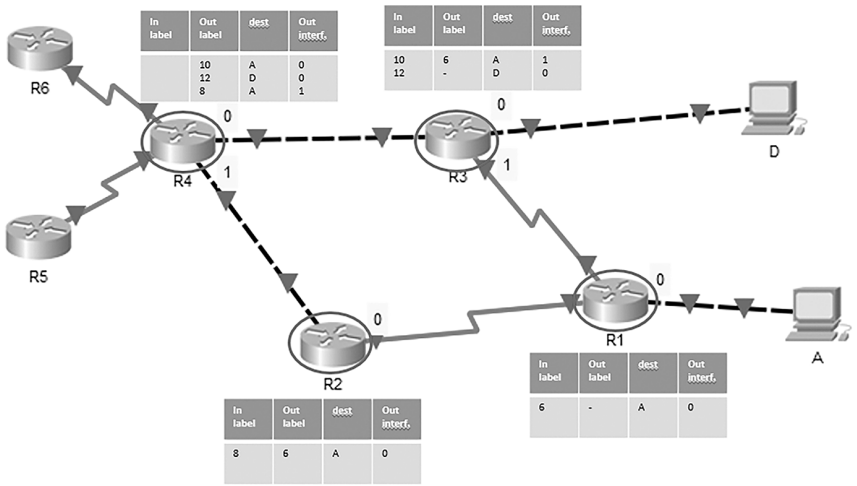
a) ::1

b) 3E80:0070::0098:0000:0001

c) FFFF::4E00:1235:0:34

7. Considerad la red siguiente con los enrutadores R1 a R4 con MPLS. Supongamos que los enrutadores R5 y R6 pasan a formar parte de la red MPLS. Se quiere realizar ingeniería de tráfico de manera que los paquetes desde R6 con destino A sean encaminados por R6-R4-R3-R1 y los paquetes desde R5 destinados a A sean encaminados por R5-R4-R2-R1. Obtened las tablas MPLS en R5 y R6 y las modificaciones necesarias en la tabla R4 para un funcionamiento correcto.

Nota: etiquetad R6 con destino A: 7, etiquetad R5 con destino A: 5.



Solucionario

1. En la figura 60 observamos lo siguiente: las sedes A y B requieren 2 Mbytes de datos en una dirección por usuario y día.

a) Si el correo se va descargando en período laboral (8 horas) vemos que:

(2.000.000 bytes × 8 bits/byte) / 8 horas × 3.600 segundos/hora = 556 bps

Si como se ha indicado tenemos 100 usuarios, el resultado será 55,6 kbps.

b) Si lo que tenemos es un pico de tráfico concentrado en 15 minutos, en tal caso los requisitos de ancho de banda serán:

(2.000.000 bytes × 8 bits/byte)/15 minutos × 60 segundos/minuto = 88,9 kbps

Si tenemos 100 usuarios, necesitamos un ancho de banda de 889 kbps. En este caso deberíamos contratar una línea que nos diera un mínimo de 1 Mbps.

2. Si nos fijamos en la topología de la figura 55 vemos que nos dan una dirección IP de clase C. A partir de esta dirección hay que hacer VLSM para cuatro redes con 28, 60, 12 y 12 *hosts*, respectivamente. En este caso, crearemos cuatro subredes con 62 direcciones cada una. La primera la asignaremos a la red que necesita 60 IP. Quedan ahora tres subredes. Tomamos la primera y volvemos a repetir el proceso creando dos subredes más.

192.168.10.0 /24	192.168.10.0 255.255.255.192	Direccionamiento para la red con 60 *hosts*
	192.168.10.64 255.255.255.192	
	192.168.10.128 255.255.255.192	
	192.168.10.192 255.255.255.192	

192.168.10.64 255.255.255.192	192.168.10.64 255.255.255.224
	192.168.10.96 255.255.255.224

Hemos creado dos redes de 30 IP cada una. El primer rango nos sirve para la red que necesita 28 IP.

Ahora repetiremos el mismo proceso para cubrir las necesidades de las redes de 12 IP. Con el rango 192.168.10.96 255.255.255.224 hacemos *subnetting*:

192.168.10.96 255.255.255.224	192.168.10.96 255.255.255.240
	192.168.10.112 255.255.255.240

Con esta solución tenemos todavía dos rangos de direcciones para futuras ampliaciones:

192.168.10.128 255.255.255.192
192.168.10.192 255.255.255.192

3.

Paso 1:

Dirección origen del datagrama: 10.0.1.12

Dirección destino del datagrama: 128.119.174.185

Puerto origen: 3344

Puerto destino: 80

Paso 2:

Dirección origen del datagrama: 147.83.11.1

Dirección destino del datagrama: 128.119.174.185

Puerto origen: 5066

Puerto destino: 80

Una vez que recibe el datagrama, el enrutador genera un nuevo número de puerto que no esté ya utilizado en la tabla NAT. Se ha elegido el 5066. Además, en este caso, como se ha indicado, se emplea NAT *overloading* con la misma IP externa del enrutador.

Dirección, puerto interno	Dirección, puerto externo
10.0.1.12 - 3344	147.83.11.1 - 5066

Paso 3:

Dirección origen del datagrama: 128.119.174.185

Dirección destino del datagrama: 147.83.11.1

Puerto origen: 80

Puerto destino: 5066

Paso 4:

Dirección origen del datagrama: 128.119.174.185

Dirección destino del datagrama: 10.0.1.12

Puerto origen: 80

Puerto destino: 3044

En el paso 4 el enrutador recibe el datagrama y examina su tabla NAT para obtener la IP y el puerto correspondientes en la red interna.

4. En el primer caso se puede tratar tanto de NAT estático como dinámico, ya que hay una traslación uno a uno de la dirección local interna a la dirección global externa. En consecuencia, solo mirando la tabla no podemos saber con cuál de los dos tipos de NAT se trabaja. Lo que se puede garantizar es que no se trabaja con PAT.

En el segundo caso, en cambio, se utiliza NAT *overload*. El protocolo de salida es TCP, y la dirección global interna es la misma para las dos entradas de la tabla.

5.

a) Se eliminan los ceros consecutivos del primer conjunto de la dirección.

2000::ABCD:0:25

b) Se eliminan los ceros consecutivos del primer conjunto de la dirección.

3FFF:FF00::ACAD:25:0:127

c) En este caso, dado que los ceros consecutivos en los dos conjuntos pueden permitir expresar la dirección comprimida de dos formas posibles, mostraremos las dos posibilidades. Recordad que :: para representar conjuntos de ceros consecutivos solo se puede utilizar una única vez en una dirección IPv6.

FF00:ACAD::1234:0:0:1 o también FF00:ACAD:0:0:1234::1

6. Recordad que la dirección IPv6 es un conjunto de 128 bits dividido en grupos de 16 bits expresado en hexadecimal. Esto implica que una dirección IPv6 tenga siempre 8 grupos. Por

lo tanto, siempre que haya :: habrá que añadir tantos grupos de ceros como haga falta para llegar a 8 grupos.

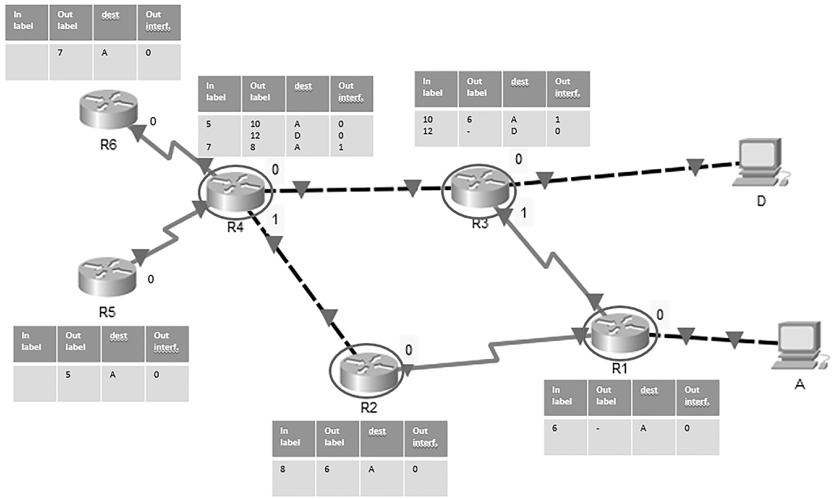
a) 0000:0000:0000:0000:0000:0000:0000:0001

b) 3EF8:0070:0000:0000:0000:0098:0000:0001

c) FFFF: 0000: 0000: 0000:4E00:1235:0000:0034

7. Como se ha indicado, hay que crear las tablas MPLS de R5 y R6, en que solo tenemos la etiqueta de salida, destino e interfaz de salida.

Además, hay que modificar la tabla MPLS de R4. En la figura inicial, si examinamos las tablas MPLS, se muestra que el tráfico con destino A va por dos rutas: por R4-R3-R1 y por R4-R2-R1. Sabiendo esto, la única modificación que hay que hacer en la tabla MPLS de R4 es incluir qué etiqueta de entrada se quiere que vaya por una interfaz de salida u otra. En la nueva tabla de R4 se muestra que el tráfico con etiqueta 5 se enviará por la interfaz 0, mientras que el tráfico de la etiqueta 7 se enviará por la interfaz 1.



Glosario

border gateway protocol *m* Protocolo para el intercambio de información de encaminamiento entre encaminadores normalmente entre sistemas autónomos.
sigla **BGP**

BGP *m* Véase ***border gateway protocol***.

contenedor virtual *m* Señal SDH que transporta una carga más pequeña que una carga STM-0.
sigla **VC**

E-LAN *m* Véase ***Ethernet LAN service***.

EOS *m* Véase **Ethernet sobre SONET/SDH**.

Ethernet LAN service *m* Servicio Ethernet multipunto a multipunto.
sigla **E-LAN**

Ethernet sobre SONET/SDH *m* Tecnología que permite en los paquetes Ethernet ser transportados por medio de una red SONET/SDH.
sigla **EOS**

Ethernet virtual connection *m* Servicio Ethernet punto a punto.
sigla **EVC**

EVC *m* Véase ***Ethernet virtual connection***.

FEC *m* Véase ***forwarding equivalence class***.

forwarding equivalence class *m* Conjunto de paquetes de nivel tres que son conmutados de la misma manera por el mismo camino, con el mismo tratamiento de conmutación.
sigla **FEC**

GE *m* Véase ***gigabit Ethernet***.

gigabit Ethernet *m* Estándar de Ethernet de alta velocidad, aprobado por el IEEE 802.3z en 1996.
sigla **GE**

ingeniería de tráfico *f* Técnica y métodos usados que hacen que el tráfico encaminado mediante una ruta o camino determinado no siga los estándares de los protocolos de encaminamiento.
en *traffic engineering*

label distribution protocol *m* Protocolo estándar que permite en los encaminadores MPLS negociar etiquetas (direcciones) que se usan para reenviar los paquetes.
sigla **LDP**

label edge router *m* Encaminador que hace la imposición de las etiquetas.
sigla **LER**

label forwarding information base *m* Estructura usada en la conmutación de etiquetas para mantener información de las etiquetas de entrada y salida, interfaces y FEC asociado.
sigla **LFIB**

label switch path *m* Camino que los paquetes MPLS atraviesan entre dos LSR frontera.
sigla **LSP**

LAN *f* Véase **red de área local**.

LDP *m* Véase ***label distribution protocol***.

LER *m* Véase ***label edge router***.

LFIB *m* Véase ***label forwarding information base***.

LSP *m* Véase ***label switch path***.

MAN *f* Véase **red de área metropolitana**.

multiprotocol label switching *m* Método de conmutación que permite reenviar paquetes IP usando etiquetas.
sigla **MPLS**

OAM and P *f* Operación, administración, mantenimiento y aprovisionamiento. Proporciona las facilidades y el personal requerido para gestionar la red.

open shortest path first *m* Protocolo de encaminamiento entre encaminadores dentro de los sistemas autónomos; mejora el antiguo protocolo de encaminamiento RIP.
sigla **OSPF**

OSPF *m* Véase ***open shortest path first***.

red de área local *f* Grupo de computadores y dispositivos asociados que comparten líneas de comunicación y recursos dentro de un área geográfica pequeña.
sigla **LAN**

red de área metropolitana *f* Red que conecta usuarios en un área superior a la LAN pero inferior a lo que cubriría una red de área extendida.
sigla **MAN**

SDH *m* Véase ***synchronous digital hierarchy***.

SONET *m* Véase ***synchronous optical network***.

synchronous digital hierarchy *m* Estándar para la transmisión de datos por medio de la fibra óptica. SDH se usa en Europa.
sigla **SDH**

synchronous optical network *m* Estándar para la transmisión de datos mediante la fibra óptica. SONET se usa en Norteamérica y partes de Asia.
sigla **SONET**

TDM *m* Véase ***time division multiplexing***.

time division multiplexing *m* Técnica en la cual la información de varios canales en un único cable se puede asignar a un ancho de banda basado en espacios de tiempo previamente asignados. Se asigna el ancho de banda de cada canal sin mirar si la estación está transmitiendo.
sigla **TDM**

UNI *m* Véase ***user to network interface***.

user to network interface *m* Especificación de la interfaz entre un sistema final y el sistema *backbone*.
sigla **UNI**

VC *m* Véase **contenedor virtual**.

Bibliografía

Alwayn, V. (2001). *Advanced MPLS Design and Implementation.* Indianápolis: Cisco Press.

Citrix. «SDN 101: Introducción a Software Defined Networking». https://www.citrix.com/content/dam/citrix/en_us/documents/oth/sdn-101-an-introduction-to-software-defined-networking-es.pdf

Ghein, L. de (2007). *MPLS Fundamentals*. Indianápolis: Cisco Press.

Göransson, P.; Black, C. (2014). *Software Defined Network. A comprehensive approach*. Elsevier.

Graziani, R.(2017). *IPv6 Fundamentals* (2.ª ed.). Cisco Press.

Hagen, S. (2014, 3.ª ed.) *IPv6 Essentials*. O'Reilly.

Halabi, S. (2003). *Metro Ethernet*. Indianápolis: Cisco Press.

McCabe, J. (2003). *Network Analysis, Architecture and Design*. San Francisco: Elsevier Science.

Metro Ethernet Forum
http://www.metroethernetforum.org

Metzler, J. (2015). *Guide to WAN Architecture & Design*. Webtorials.

Nadeau, T. D.; Gray, K. (2013). *SDN. Software Defined Network*. O'Reilly.

Open Networking Foundation Website. https://www.opennetworking.org/software-defined-standards/overview/

Rubio, J. H. *¿Qué es SDN?* https://www.ciena.com.mx/insights/what-is/What-is-SDN_es_LA.html

Uppal, S. (2015). *Software Defined WAN for Dummies*. John Wiley & Sons, Ltd.