Capa de red: Plano de Datos

Esta capa puede descomponerse en dos partes que interaccionan mutuamente: el plano de datos y el plano de control

La **capa de red** transporta paquetes desde un host emisor a un host receptor.

La **funcion principal** del **plano de datos** de cada router consiste en **reenviar** los datagramas desde sus enlaces de entreada a sus enlaces de salida.

La **funcion principal** del **plano de control** consiste en **coordinar** estas acciones de reenvío locales de cada router individual, de modo que los datagramas terminan transfiriéndose de extremo a extremo, a lo largo de series de routers comprendidos entre los hosts de origen y de destino.

Funciones de la capa de red

Reenvio:

- Cuando un paquete llega al enlace de entrada de un router, este tiene que pasar el paquete al enlace de salida apropiado.
- Implementado por el plano de datos
- Hace referencia a la accion local que realiza un router al tranferir un paquete desde una interfaz de un enlace de entrada a una interfaz de un enlace de salida.
- Escalas de tiempo muy cortas

Enrutamiento:

- determina la ruta o camino que deben seguir los paquetes a medida que fluyen de un emisor a un receptor.
- Son determinados por un algortimo de enrutamiento
- Hace referencia al proceso que realiza la red para determinar las rutas extremo a extremo que los paquetes siguen desde el origen al destino.
- Escalas de tiempo mucho más largas
- Implementación en software

Tabla de reenvío:
Un router reenvia un paquete examinando el valor de uno o mas campos de la cabecera del paquete entrante y utilizando despues esos valores de la cabecera para realizar una indexacion dentro de la tabla de reenvio, el valor almacenado en la tabla correspondinte indica la interfaz del enlace de salida del router a la que hay que reenviar el paquete.

Plano de control:

El algortimo de enrutamiento determina el contenido de las tablas de reenvío de los routers.

Hay dos enfoques:

- Tradicional:
    - Cada router contiene funciones tanto de reenvío como de enrutamiento.
    - La funcion encargada del algortimo de enrutamiento en un router se comunica con la funcion correspondiente en otros routers para calcular los valores con lo que rellenar su tabla de reenvío.
    - Intercambian mensajes por medio de un protocolo de enrutamiento

- SDN:
    - Hay un controlador remoto separado físicamente de los routers
    - Este controlador calcular y distribuye las tablas de reenvío que hay que usar en cada router.
    - El controlador puede ser gestionado por el ISP o por algun otro provedor
    - El dispositivo de enrutamiento solo se encarga del reenvio y el Controlador remoto calcula y distribuye las tablas de reenvio
    - reenvio -> Hardware. Enrutamiento -> software

La capa de red de internet propociona un unico servicio: **best effort service**, es decir, hace lo mejor que puede para entregar los paquetes pero no garantiza la entrga de ellos, ni sobre el retardo ni si están corrompidos.

Posibles servicios que podria proporcionar la capa de red
- Entrega garantizada
- Entrega garantizada con retardo limitado
- Entrega de los paquetes en orden
- Ancho de banda mínimo garantizado
- Seguridad

Interior de un router

Los routers son dispositivos de conmutación de paquetes de almacenamiento y reenvío que reenvían los paquetes utilizando direcciones de la capa de red

4 componentes de un router:

- Puertos de entrada:
    - lleva a cabo una **funcion de busqueda** en el puerto de entrada
    - enviar el paquete a través del entramado de conmutación al puerto de salida especificado (“acción”)

- Entramado de conmutacion
    - conecta los puertos de entrada del router a sus puertos de salida

- Puerto de salida
    - Almacena los paquetes recibidos desde el entramado de conmutacion y los transmite al enlace de salida.

- Procesador de enrutamiento
    - Lleva a cabo las funciones del plano de control
    - En los routers tradiciones, ejecuta los protocolos de enrutamiento, mantiene las tablas de enrutamiento y la info asociada al estado de los enlaces y calcula la tabla de reenvio del router
    - En los routers SDN se encarga de comunicarse con el controlador remoto para recibir entradas de la tabla de reenvio calculadas por el controlador remoto e instalar dichas entradas en los puertos de entrada del router.

Procesamiento en el puerto de entrada y reenvio basado en el destino

El router utiliza la tabla de reenvio para determinar el puerto de salida (a partir de la busqueda del puerto de entrada) al que sera reenviado un paquete entrante a traves del entramado de conmutacion.

La tabla de reenvio es calculada y actualizada por el procesador de enrutamiento o se recibe desde un controlador SDN remoto.
La tabla de reenvío es copiada en las tarjetas de línea desde el procesador de enrutamiento a traves de un bus independiente.

Con la tabla de reenvío (prefijo e interfaz) el router busca la coincidencia de un **prefijo** de la direccion de destino del paquete con las entradas de la tabla.
Si existe una coincidencia, el router reenvia el paquete a un enlace asociado a esa coincidencia.

Prefijo	Interfaz de enlace
11001000 00010111 00010	0
11001000 00010111 00011000	1
11001000 00010111 00011	2
En otro caso	3

ej:
llega el paquete 11001000 00010111 00010110 10100001 y si prefijo de 21 bits coincide con la primer entrada de la tabla. Entonces reenvia el paquete a la interfaz de enlace 0.
Si la direccion de destino puede corresponderse con más de una entrada se aplica **la regla de coincidencia con el prefijo más largo**, es decir, busca la entrada más larga de la tabla con la que exista una coincidencia.

Cuando no se encuentra un match en la forwarding table, el router reenvía el paquete por lo que se conoce como **default gateway.**

Una vez determinado el puerto de salida de un paquete, este puede ser enviado al entramado de conmutacion. En algunos diseños se puede bloquear termporalmente la entrada del paquete si es que hay paquetes procedentes de otros puertos de entrada que está usando actualmente el entramado.
Los paquetes bloqueados seran puestos en cola en el puerto de entrada, planificandose su paso por el entramado para algun instante de tiempo posterior.

Conmutacion

Se encuentra en el corazón de todo router, ya que es a traves de este entramado donde los paquetes son realmente conmutados(enviados) desde un puerto de entrada a un pouerto de salida.

Esta puede ser:
- via memoria
- via bus
- via una red de interconexion

Procesamiento en el puerto de salida

Toma los paquetes que hayan sido almacenados en la memoria del puerto de salida y los transmite a traves del enlace de salida.

¿Dónde se crean las colas?

- Pueden formarse colas de paquetes en los puertos de entrada y en los puertos de salida.
- Podrian esperar en las entradas y en las salidas de la interseccion de tráfico
- La longitud y ubicacion de las colas dependerá de la carga de tráfico, de la velocidad relativa del entramado de conmutacion y de velocidad de la línea.
- a medida que las colas crecen, la memoria del router podria terminar agotandose generando así perdida de paquetes. ACÁ ES DONDE REALMENTE SE DESCARTAN Y SE PIERDEN LOS PAQUETES
- Rline = velocidad de transmision
- Rswitch = la velocidad a la que el entramado puede mover los paquetes desde los puertos de entrada hasta los puertos de salida.
- si R_{switch} es N veces mayor que R_{line} entonces las colasque se produzcan en los puertos de entrada seran despreciables.

Colas de entrada

¿Qué pasa si el entramado de comuntacion no es lo suficientemente rapido como para transferir todos los paquetes que llegan sin producir retardos?

Solucion: Pueden crearse colas de paquetes en los puertos de entrada ya que los paquetes se iran añadiendo a las colas de los puertos de entrada con el fin de **esperar su turno** para ser transferidos hacia el puerto de salida a traves de entramado de conmutacion.

Colas de salida

Puesto que el puerto de salida solo puede transmitir un unico paquete en cada unidad de tiempo, todos los paquetes que llegan mientras se está mandando uno son colados en la cola de espera para poder ser transmitidos a traves del enlace saliente.

Cuando no hay suficiente memoria, hay que tomar la decicion de eliminar el paquete entrante o eliminar uno o más paquetes que ya se encuentran en la cola para dejar lugar al paquete que recien llega.

Planificacion de paquetes

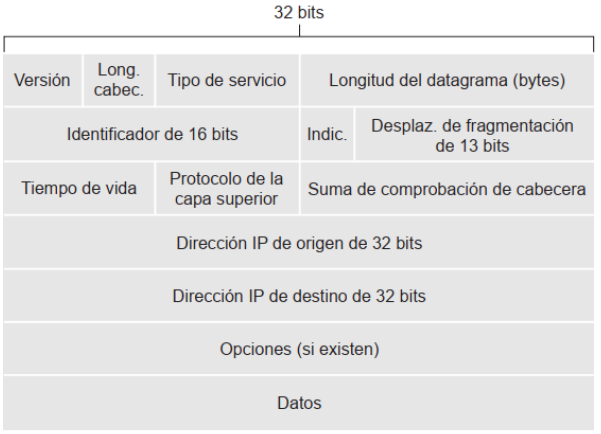
Se debe determinar el orden en el que se transmiten a traves de un enlace saliente los paquetes existente en la cola.

Existintes distintas politicas:

- **FIFO**: selecciona los paquetes para su transmision a traves del enlace en el mismo orden en el que llegaron a la cola de salida del enlace.
- **Colas con Prioridad**: los paquetes que llegan al enlace de salida se clasifican en clases de prioridad al llegar a la cola. Cada clase de prioridad suele tener su propía cola. Para elegir un paquete a transmitir, se transmiten primero los paquetes de la cola con mayor prioridad que tenga paquetes.

- **Round Robin**: los paquetes se distribuyen en clases. Hay un planificador round robin que va alternando el servicio entre las distintas clases. Se transmite un paquete de clase 1, luego uno de clase 2, luego vuelve a transmitir de clase 1, luego de clase 2 y así sucesivamente
- **WFQ**(cola equitativa ponderada): llegan los paquetes y los coloca en su cola a partir de su clase. Luego el planificador WFQ presta un servicio a las clases de forma circular: primero transmite clase 1, luego a la clase 2 y por último a la clase 3 y va repitiendo la secuencia.
  A diferencia de round robin, a cada clase se le asigna un peso wi y a la clase i se le garantiza que recibira una fraccion de tiempo igual a wi /Σ(wj).

Protocolo de internet IP



Formato de datagramas IPv4:

Los campos del datagrama son:

- **Numero de version**: especifican la version del protocolo IP del datagrama
- **Longitud de la cabecera**: es util ya que IPv4 permite tener un campo de opciones. El datagrama IP tipico tiene una cabecera de 20 bytes
- **Tipo de servicio**
- **Longitud del datagrama**: es la longitud total del datagrama IP(la cabecera mas los datos)
- **Identificador, indicadores (Flags), offset**: relacionados con la fragmentacion IP (SOLO EN IPV4, ipv6 no permite la fragmentacion)
- **Tiempo de vida, TTL**: se incluye con el fin de garantizar que los datagramas no esten eternamente en circulacion a traves de la red.
- **Protocolo**: indica el protocolo específico de la capa de transporte(ej: TCP, UDP)
- **Checksum**: ayuda a los routers a detectar errores de bit en un datagrama IP recibido
- **Direcciones IP origen y destino.**
- **Opciones**
- **Dato**: contiene el segmento de la capa de transporte TCP o UDP que va a entregarse al destino.

Fragmentacion IPv4

No todos los protocolos de la capa de enlace pueden transportar paquetes de la capa de red del mismo tamaño. Algunos pueden transportar datagramas más grandes y otros más pequeños.

MTU = cantidad máxima de datos que un tramo de la capa de enlace puede transportar
Como al transportar un datagrama este puede pasar por distintos enlaces cuyos protocolos de la capa de enlace pueden ser distintos y por lo tanto tener una MTU diferente, se debe tener en cuenta tranportar ese datagrama por todos los enlaces.

Solucion: Fragmentar los datos del datagrama IP en dos o más datagramas IP más pequeños(**fragmentos**), y enviarlos a traves del enlace de salida.

Estos fragmentos tienen que ser reensamblados antes de llegar a la capa de transporte del destino. Este trabajo se hace en los sistemas terminales ya que realizarlo en los routers añadiria una complejidad significativa al protocolo y por lo tanto reduciria el rendimiento de los routers.

Cuando a un host destino le llega una serie de datagramas procedentes del mismo origen, tiene que determinar si alguno de estos **datagramas son fragmentados**, también tiene que determinar cual es el **último fragmento** y como debe **unirlos**. Es por ello que se utilizan los campos:

- **identificacion**: indica el número de indentificacion del datagrama original, es utilizado por el host destino para poder ver si los datagramas que llegaron son fragmentos de un mismo datagrama mas grande
- **indicadores**: se pone 0 si se trata del último fragmento o 1 en caso de que le sigan otros fragmentos.
- **offset**: indica la posicion dentro del datagrama IP original en donde encaja el fragmento

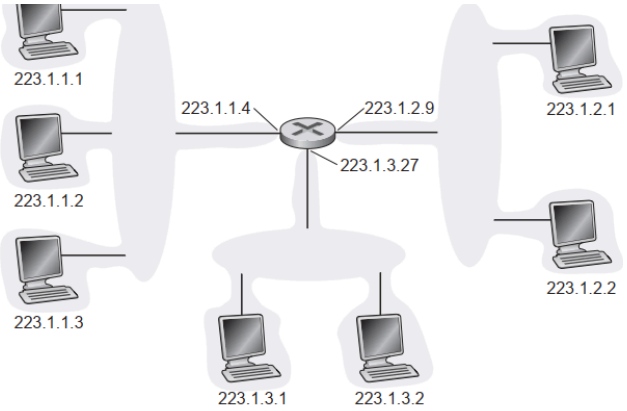
Direccionamiento IPv4

Conexion entre hosts y routers:

- un host dispone de un unico enlace hacia la red
- El límite entre el host y el enlace fisico se denomina **interfaz**.
- Puesto que la tarea de un router consiste en recibir un datagrama por enlace y reenviarlo a algun otro enlace, necesariamente el router está conectado a dos o más enlaces.
- El límite entre el router y cualquiera de sus enlaces tambien se conoce como **interfaz**.
- El protocolo IP requiere que cada interfaz de host y de router tenga su propia direccion IP globalmente unica(excepto en las interfaces utilizadas para NAT)
- Una parte de la direccion IP de una interfaz estara determinada por la subred a la que la interfaz este conectada

Cómo funciona:

Se tiene un router con 3 interfaces para interconectar 7 host. Los 3 host de la izquierda están conectados a una interfaz del router. Todos tienen una direccion IP con el formato 223.1.1.xxx. (los 24 bits más de la izquierda son iguales)



Esta red que interconecta tres interfaces de host y una interfaz de router forma una **subred.**

Para determinar las subredes, desconecte cada interfaz de su host o router, creando islas de redes aisladas, en las que las interfaces actúan como puntos terminales de las redes aisladas. Cada una de estas redes aisladas se dice que es una subred.

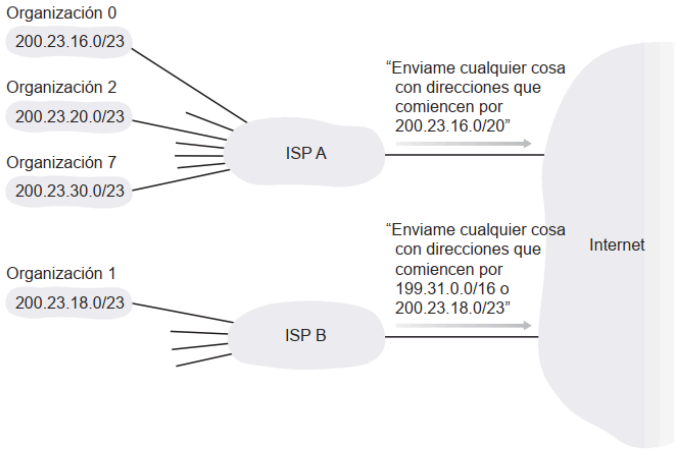
El direccionamiento IP asigna una direccion a esta subred: 223.1.1.0 / 24 donde /24 es una **máscara de la subred**.
Una **máscara** nos define qué bits nos interesan de un espacio de direcciones. Es una secuencia de bits de izquierda a derecha que contienen un 1.
Se utiliza en subnetting por ejemplo para indicar las distintas subredes. Se utiliza aplicándola sobre una dirección ip con la operación AND para obtener la dirección de red.

La estrategia de asignación de direcciones en Internet se conoce como **enrutamiento entre dominios sin clase**.
Los x bits más significativos de una direccion en el formato a.b.c.d/x constituyen la parte de red de la direccion IP y se denomina **prefijo** de la direccion.

Los 32-x bits restantes de una direccion pueden emplearse para diferenciar los dispositivos dentro de una organizacion (todos los cuales tienen el mismo prefijo de red). Estos 32-x identifican a los **host** especificos de la organizacion.

Antes de que se utilizara el enrutamiento CIDR se utilizaba el direccionamiento con claves donde las subredes con direcciones de 8, 16 y 24 se conocian como redes de clase A, B y C.
Esto tenía un problema porque por ejemplo si eras de clase C (/24) solo se podian acomodar acomodar hasta 2^8 - 2 =254 host(lo que puede ser muy poco) mientras que si eras de clase B(/16) podias acomodar 65634 host lo cual era muy grande.

Ejemplo ISP



Se conectan 8 organizaciones a internet.
La ISP A anuncia al mundo que se le debe enviar cualquier datagrama a la direccion 200.23.16.0/20, el resto del mundo no debe porque saber que dentro del bloque de direccion 200.23.16.0/20 hay 8 organizaciones.
Esto de poder emplear un mismo prefijo para anunciar multiples redes se lo conoce como **agregacion de direcciones.**

También existe la direccion IP de **difusion 255.255.255.255** en la cual cuando un host envía un datagrama cuya direccion de destino es 255.255.255.255, el mensaje es entragado a todos los host existentes en una misma subred.

Cómo obtener un bloque de direcciones:

Para obtener un bloque de direcciones IP que pueda ser utilizado dentro de la subred de una organizacion, el administrador de red tiene que contactar a su ISP, que le proporciona direcciones extraídas de un bloque de direcciones mayor.

DHCP (Dynamic Host Configuration Protocol)

DHCP permite a un host obtener (permite que se le asigne) automáticamente una dirección IP. Un administrador de red puede configurar DHCP de modo que un host dado reciba la misma dirección IP cada vez que se conecte a la red, o bien a un host puede asignársele una dirección IP temporal que será diferente cada vez que el host se conecte a la red.
DHCP también permite que un host obtenga información adicional, como por ejemplo su máscara de subred, la dirección de su router del primer salto (gateway) y la dirección de su servidor DNS local

Traduccion de direcciones de red (NAT)

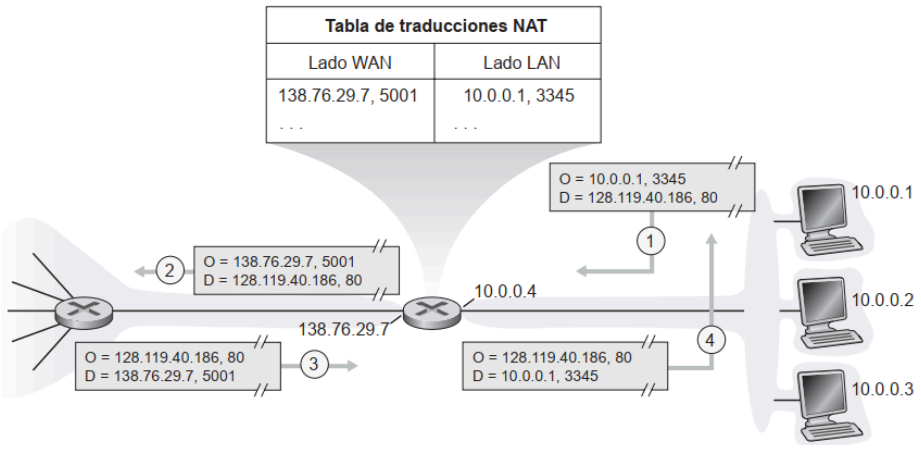
Busca resolver es otorgar más ips de las que ofrecia ipv4

Funcionamiento de un router con funcionalidad NAT:

Diferentes hosts pueden compartir la misma IP privada ya que sus routers están configurados para usar NAT. Estos routers tienen lo que se conoce como la tabla de traducciones NAT cuyas entradas incluyen numeros de puerto junto con las direcciones ip.
El procedimiento es el siguiente:

Cuando un host quiere comunicarse con alguien que está fuera de la red privada, crea el datagrama con la direccion destino y puerto destino a la LAN. Dicho datagrama es recibido por el router NAT, y este genera un nuevo puerto origen para el datagrama y sustituye la direccion origen por su propia direccion origen (la del router NAT). El nuevo puerto origen que selecciona el NAT es un número que aún no está en la tabla. El router NAT finalmente agrega una entrada en su tabla con este puerto origen nuevo y la direccion del host que envio el datagrama. Cuando el host que está fuera de la red envía su respuesta, el puerto al que se dirige el datagrama es el que creo el router NAT. Así, finalmente para que el host de la red privada reciba el datagrama de respuesta, el router NAT indexa su tabla con el puerto de origen que creó.

El router NAT se comporta de cara al exterior como un unico dispositivo con una direccion IP unica. Todo paquete que netra tiene una direccion IP de destino igual y todo paquete que sale tiene una misma direccion IP de origen.
NAT oculta los detalles de la red doméstica al mundo exterior.



IPv6

La principal motivación de esta iniciativa fue que se dieron cuenta de que el espacio de direcciones IP de 32 bits estaba comenzando a agotarse, a causa de la velocidad pasmosa con que estaban conectándose a Internet nuevas subredes y nodos IP

Formato de datagrama IPv6

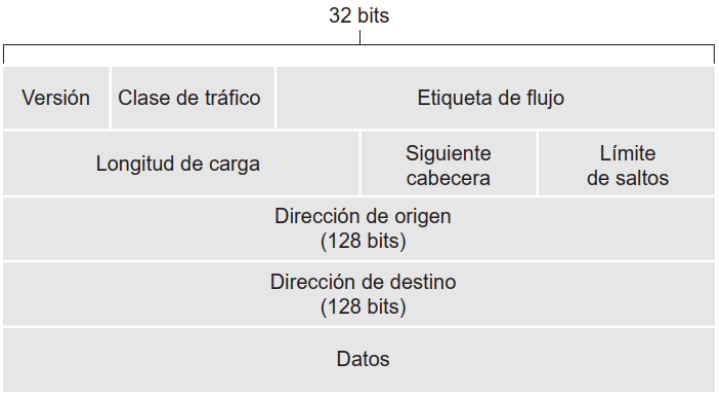
Los cambios más importantes introducidos en IPv6 son:

- Capacidades ampliadas de direccionamiento: aumenta el tamañno de direcciones IP de 32 a 128 bits.
  IPv6 ha introducido un nuevo tipo de dirección, dirección **anycast**, que permite entregar un datagrama a uno cualquiera de un grupo de hosts.
- Una cabecera de 40 bytes simplificada. long fija
- Etiquetado de flujo

CAMPOS DEL DATAGRAMA:

- Version: 4 bits identifica el numero de version IP

- Clase de tráfico: puede darse prioridad a ciertos datagramas dentro de un flujo
- Etiqueta de flujo: se utiliza para identificar un flujo de datagramas
- Longitud de datos
- Siguiente cabecera: identifica el protocolo(TCP, UDP)
- Límite de saltos: cada router que reenvia un datagrama decrementa el contenido de este campo en una unidad
- Direccion de origen y destino
- Datos



Hay campos del datagrama IPv4 que **ya no aparecen** en IPv6

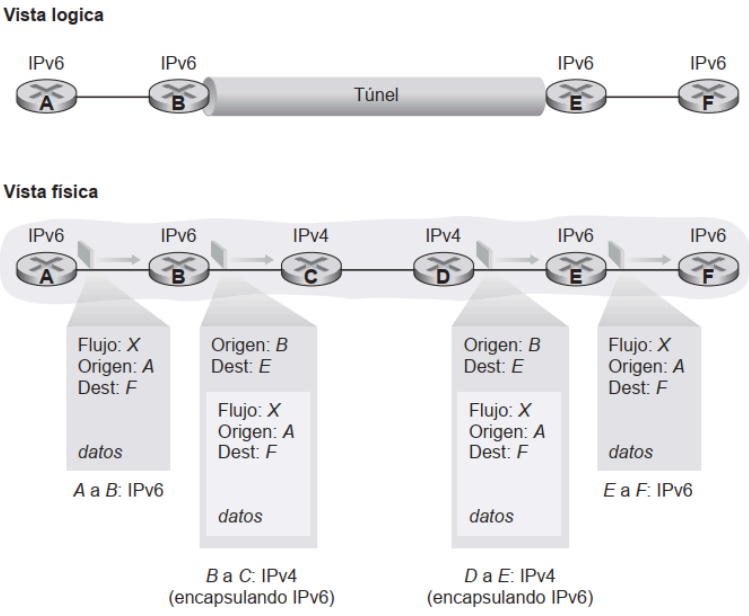
- La **fragmentacion**: ya no se permite la fragmentacion en routers intermedios, esto es porque consume mucho tiempo. Si llega un datagrama muy grande el router lo descarta y envía de vuelta al emisor un mensaje de error ICMP “Paquete demasiado grande”. Delega la ffrag los sistemas terminales y asi se acelera considerablemente el reenvío IP dentro de la red.

- **Checksum**: lleva mucho tiempo ya que esta se recalcula en cada router. Puesto que los protocolos de la capa de transporte y de la capa de enlace de datos utilizan checksum, esta funcionalidad es redundante

- **Opciones**: no se eliminaron las opciones sino que se sacó el campo. Esto es para tener una cabecera IP de 40 bytes fija.

Transicion de IPv4 a IPv6

La solucion más ampliamente adoptada en la práctica para transicionar de IPv4 a IPv6 es la de **tunelizacion**.



Idea: supongamos que tenemos dos nodos IPv6 que desean comunicarse utilizando datagramas IPv6 pero están conectados entre sí a traves de routers IPv4. El conjunto de routers intermedios se denomina tunel.
Por medio de tunelizacion, **el nodo IPv6 del lado emisor del tunel toma el datagrama IPv6 completo y lo incluye como carga util en un datagrama IPv4.** Este es pasado por todos los routers intermedios como un datagrama IPv4.
El nodo del lado receptor recibe el datagrma IPv4, determina que el datagrama contiene en su carga util un datagrama IPv6, extrae el datagrama IPv6, y lo enruta exactamente igual a si hubiera recibido el datagrama IPv6 desde un vecino IPv6 directamente conectado.

Openflow

Cada entrada de la tabla de reenvío correspondencia-acción, que se conoce con el nombre de tabla de flujo en OpenFlow, incluye:

- Un conjunto de valores de campos de cabecera: con los que se buscará una correspondencia en el paquete entrante. La búsqueda de correspondencias basada en hardware puede llevarse a cabo con la máxima velocidad usando memorias TCAM, Un paquete que no se corresponda con ninguna entrada de la tabla de flujo puede ser eliminado o enviado al controlador remoto para un procesamiento adicional.

- Un conjunto de contadores: que se actualizan a medida que se encuentran correspondencias de paquetes con entradas de la tabla de flujo

- Un conjunto de acciones: que hay que tomar cuando un paquete se corresponde con una entrada de la tabla de flujo. Estas acciones podrían consistir en reenviar el paquete a un puerto de salida determinado, eliminar el paquete, hacer copias del paquete y enviarlas a múltiples puertos de salida y/o reescribir ciertos campos seleccionados de la cabecera.