Capa de red
Función

Enviar paquetes de un host a otro host. Esto involucra de funciones importantes funciones:

Reenvío

- Cuando llega un paquete por un enlace de un router, este debe salir por el enlace apropiado (puede que no salga o hasta salga duplicado por multiples enlaces).
- Plano de datos.
- Se implementa en hardware.

Enrutamiento

- Determina la ruta que deben seguir los paquetes, a nivel del router donde están. (Algoritmos de enrutamiento).
- Plano de control.
- Se implementa en software.

Protocolos IP actuales

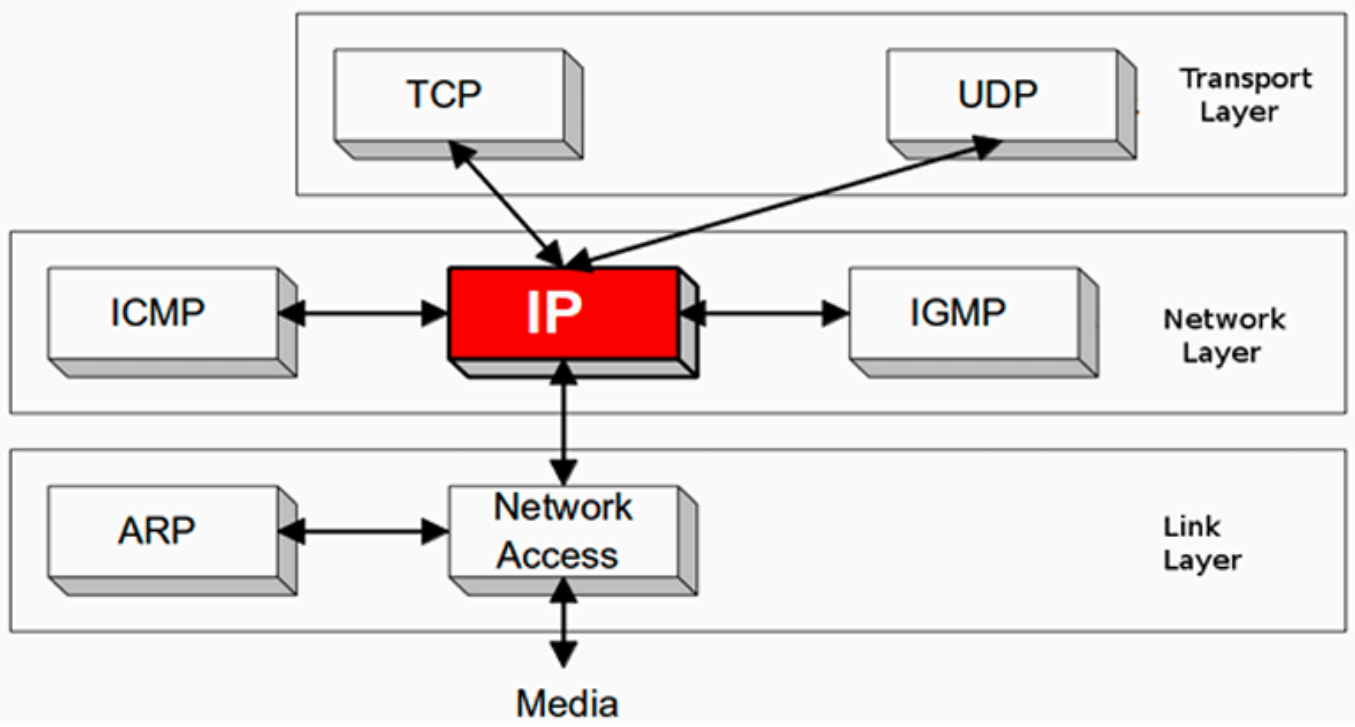
Son incompatibles entre si.

- IPv6, IPv4.

IPv4

- Sin conexión.
- Best effort.
- No confiable.
- Funcionalidades:
  - Direccionamiento.
  - Ruteo/forwarding/switching L3.
  - Mux/demux de protocolos superiores.
  - Accesorias:

    - Fragmentación.
    - Evitar loops TTL, detección de errores.
- Requiere de *ICMP* y *IGMP* como protocolos helpers.

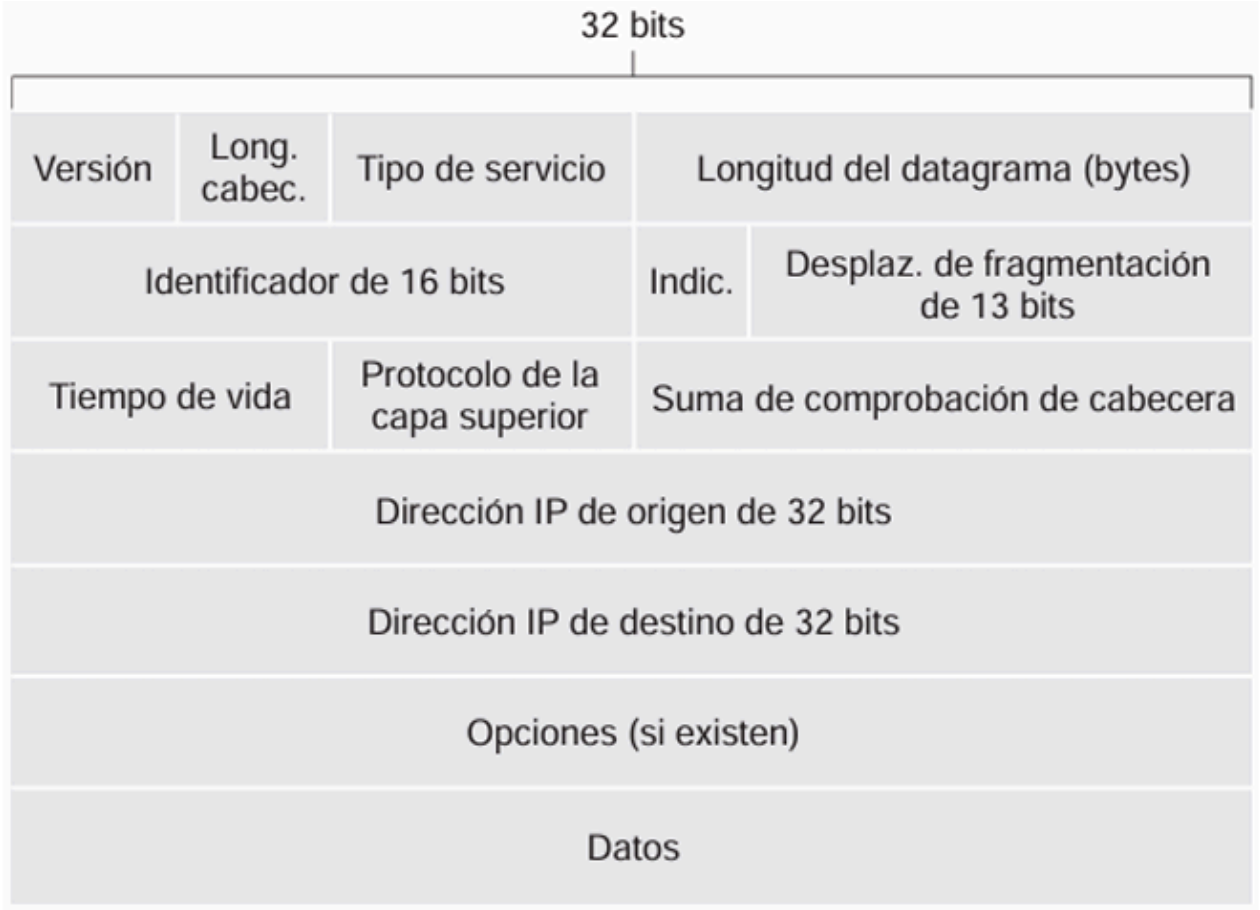


Esquema de IP en TCP/IP

Datagrama

- Numero de version, 4 bits.
- Longitud de cabecera, bits (la cabecera es 20bytes pero extensible)
- Tipo de servicio.
- Longitud de datagrama, 16 bits. Tamaño máximo de los datos es 65.535bytes, pero no suelen ser mas de 1.500bytes.
- Fragmentación:
    - Desplazamiento de fragmentación, por ejemplo al tener 72 acá sabemos que en el datagrama anterior viajaron 72 * 8 bytes
    - DF bit (que no se fragmente)
    - MF bit (hay mas fragmentos)
- TTL: Timecodes vida, se decrementa cada vez que un router procesa el datagrama y si llega a 0 lo elimina.
- Protocolo: Para indicar el protocol0 de transporte cuando llega a la terminal SI es TCP (Código 6) o UDP (Código 17). Sino por ejemplo ICMP seria 1, y IGMP 2.
- Checksum de cabecera.

- Direcciones IP de origen y destino.
- Opciones.
- Datos.



Direccionamiento IP

- Dispositivos se identifican por IP (su punto de acceso).
- Routers poseen varias IPs porque tienen varios enlaces.
- Pueden ser privadas o publicas, las privadas las asigna la IANA.

Direcciones IP

- Números de 32 bits en ipv4, usando notación dot decimal.
- 2^32 direcciones, organizadas de forma jerárquicas.
- Mapeadas en el DNS.
- Son lógicas.
- Tienen 2 partes:
  - Red, determinado por su mascara
  - Host, la parte que no cubre su mascara

Tipos

- Unicast: Destino a un host/interfaz en particular, son las más comunes.
- Broadcast: Destino a todos los hosts en una red.
- Multicast: Destinada a un grupo de hosts en una red o varias redes. Clase D.
- Anycast: Destinada al primero que resuelva. IPv4 no hay casos especiales.
- Asignables:
  Privadas: 10.x.x.x, 172.16.x.x - 172.31.x.x, 192.168.x.x
  Públicas: Cualquier IP fuera de los rangos privados y especiales.
- No asignables:
  Multicast: 224.x.x.x - 239.x.x.x
  Loopback: 127.x.x.x

Clases

- Clase A: Rango de 0.0.0.0 a 127.255.255.255 (con red privada 10.0.0.0/8).
- Clase B: Rango de 128.0.0.0 a 191.255.255.255 (con red privada 172.16.0.0/12).
- Clase C: Rango de 192.0.0.0 a 223.255.255.255 (con red privada 192.168.0.0/16).

Direccionamiento fijo

- IP asignada permanentemente, no puede cambiar como si una dinámica asignada por un server DHCP.
- Uso los host que mi clase me da, usa ineficiente de hosts.
- Poco escalable.
- Al cambiar de red un dispositivo cambia de su IP. (Mejor resuelto en IPv6)
- Se soluciona con subnetting, CIDR, NAT y DHCP, Y EN IPv6 se va el problema.

Subnetting

- Dividir un grupo de red en subgrupos, tomando una parte de lo que seria para hosts para apuntar a la subred. Se agrega una mascara de bits.
- Para saber dirección hacemos un AND entre la dirección IP y la mascara.

- La estructura pasa a ser:
  - Red
  - Subred
  - Host
- Si un red de clase desperdicia muchas direcciones IP entonces que sean divididas en N subredes mas pequeñas.
- Mascara se escriben con la notación de las IP o hexadecimal. 32 bits.
- Para calcular la cantidad de subredes, hosts, etc es 2^n donde n es la cantidad e bits asignados. Tener en cuenta que la cantidad de hosts es -2 (dirección de red y broadcast).

Fijo

- Las subredes tienen la misma mascara, y por tanto mismo numero de hosts, se desperdician hosts.

Variable (VLSM:Variable-Length Subnet Masking)

- Mascaras de longitud variable
- Pasos:
  1. Asignamos la mascara para la subred con mayor cantidad de hosts
  2. Asignamos su bloque de red.
  3. Los bloques libres entre la mascara del bloque usado y la mascara asignada a la subred lo usamos para repetir el paso 1.

CIDR: (Supernetting)

- Metodología para agrupar direcciones IP, la idea de superar el sistema de clases tradicional donde las clases A y B son el 50% de las las asignadas y solo el 2% las C.
- No usa clases.
- Reduce el tamaño de las tablas de enrutamiento.

Ruteo

Tabla de ruteo:

- Estructura hosts y routers que indica como despachar un mensaje (siguiente salto para llegar a una dirección y su interfaz).

Dispositivos

- Host
  - No despacha mensajes que recibe que no son para él. Despacha solo sus mensajes mirando su tabla de ruteo.
  - Participa de forma pasiva.
- Router
  - Son los intermedios, con varias interfaces.
  - Participan de forma activa de routing: Reciben generan y propagan.
- Host multihome:
  - Tiene varias interfaces, no rutea

Ruteo

- Proceso de terminar el camino a seguir.
- Selecciona la interfaz y el proximo salto. Implementado por routers y hosts.
- Toma decisiones de control en cuanto a como enrutar, no sobre los datos.
- Utiliza RIB (Routing information base) para almacenar los resultados del ruteo.

Tipos de ruteo

- Estático:
  - Configurado MANUALMENTE.
  - Fácil de implementar.
  - Menor consumo de recursos.
  - Ofrece mayor control y seguridad
  - No se adapta a los cambios de la red automáticamente
  - No escalable ni tolerante a fallos
- Dinámico:
  - Usa protocolos de enrutamiento para aprender y actualizar las rutas automáticamente. (En un inicio debe ser configurado por el admin)
  - Es automático, escalable y tolerante a fallos, bueno para redes complejas.
  - Requiere mas recursos y una configuración mas compleja.

Protocolos de enrutamiento

Según ámbito de operación

- IGP (interior gateway protocols), dentro un sistema autónomo, OSPF, EIGRP, RIP.
- EGP (Exterior), BGP.

Según método de operación

- Vector de distancia (DV): Calcula la ruta basada en al distancia hacia el destino (RIP).
- Estado de enlace (Link state): Cada router tiene una vista completa de la topología de red, (OSPF).
- Vector de camino (PV) similar a DV pero incluye información del camino, BGP.
- Hibrido: Combinan DV y Link state, EGIRP.

Conceptos randoms

Routing Domain:

- Conjunto de routers que comparten el mismo protocolo de ruteo. Un AS puede contener uno o más Routing Domains.

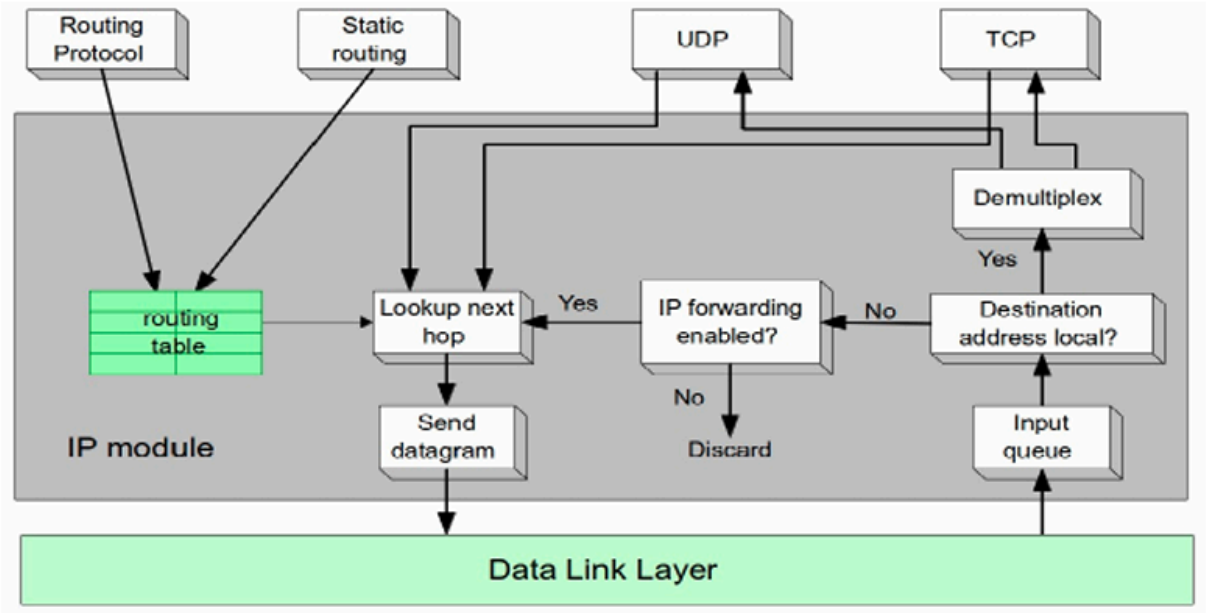
Sistema autonomo:

- Conjunto de redes bajo una misma administración y política de ruteo.
- Cada AS tiene un número único llamado ASN (Autonomous System Number).

Forwarding

- Mover un paquete de datos desde la interfaz de entrada hasta la de salida usando al info de la tabla de ruteo.
- Solo en routers.
- Intensivos.
- Plano de datos, envía protocolos enrutados.

- Utiliza la información de la RIB para hacer una version optimizada FIB.



Función de Ruteo

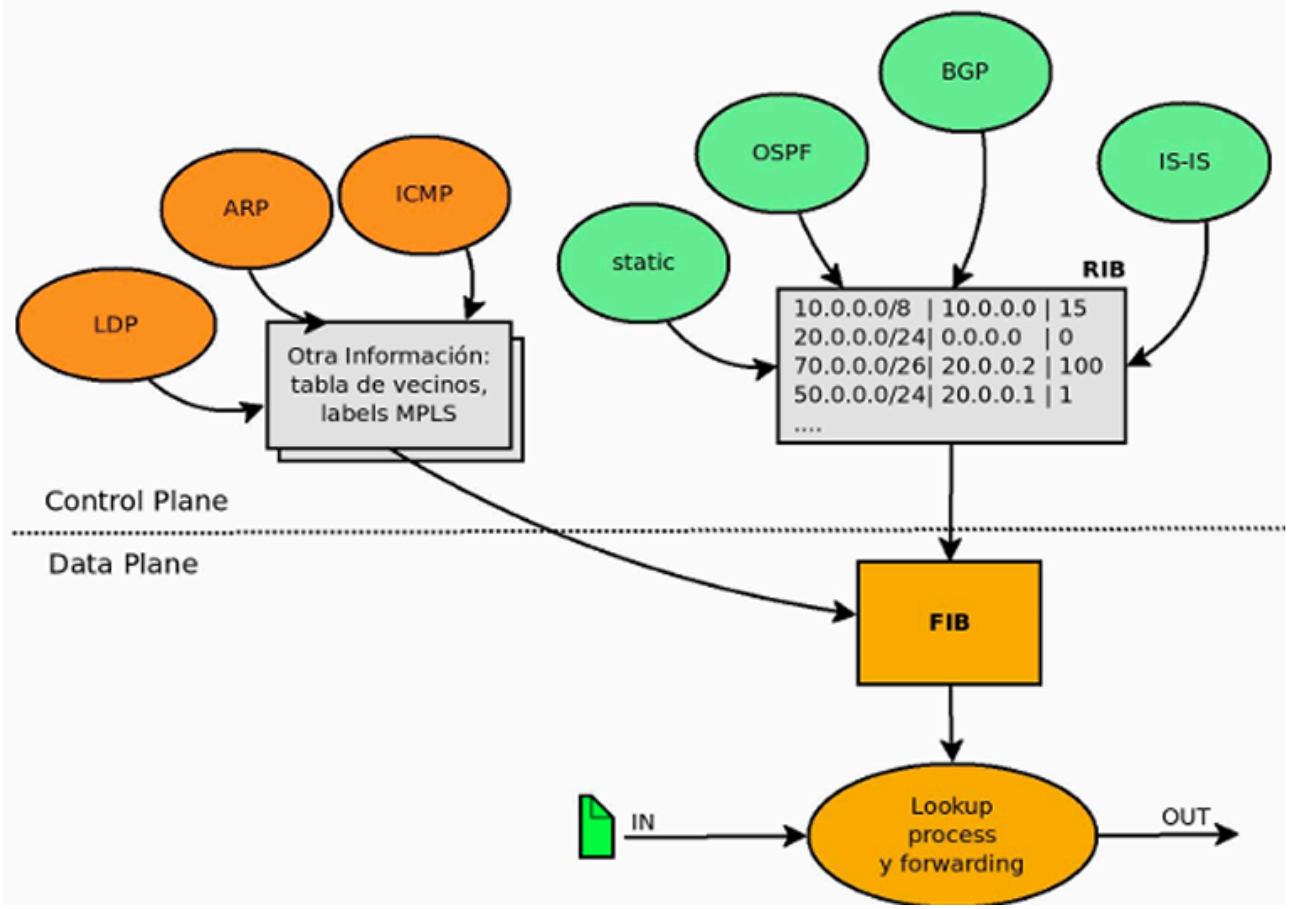


Tabla de Ruteo

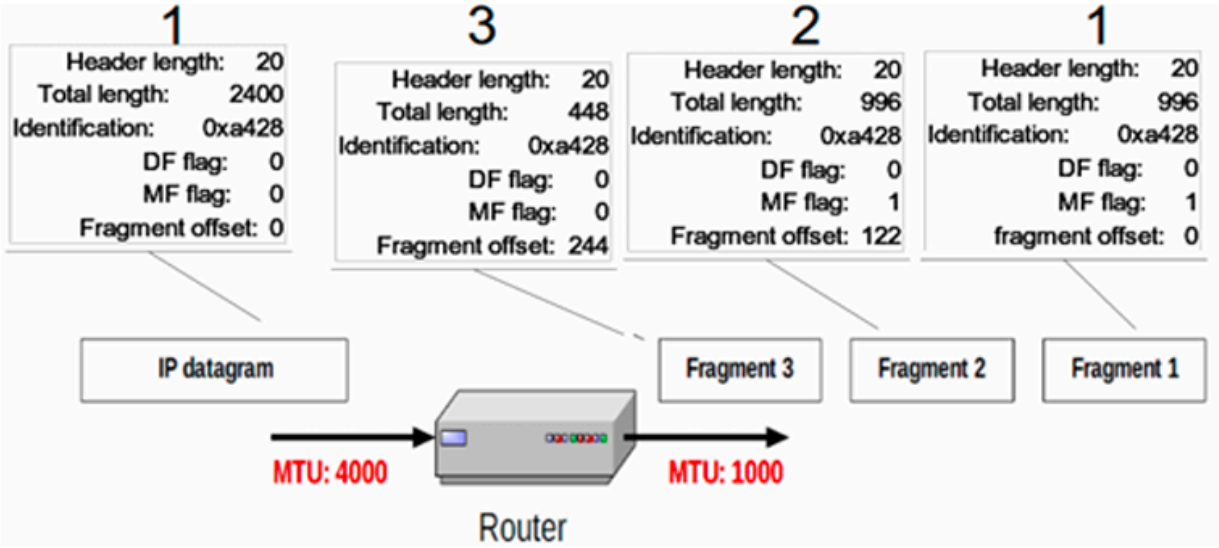
Estructura:

- Red Destino(Net/Mask) .

- Next Hop(Próximo salto) (Gateway).
- Interfaz de salida.
- Mascara.
  En un Host está estructura es más simple.

Tareas de ruteo

- Cuando llega un paquete a un router:
  - Validamos el datagrama
  - Calculamos el checksum
  - Leemos le destino
  - Buscamos el best match de la tabla de ruteo
  - Decrementar TTL
  - Fragmentarlo (si es que llega pasar).



Ejemplo de Fragmentación

- Trasmitimos o descartamos.
- Generamos ICMP.

ICMP (Internet Control Message Protocol)

- Protocolo auxiliar de IP para control de errores en IP.
- Protocolo de la capa de red.
- Proporciona una forma de que los hosts y routers intercambien información vital sobre la red, errores y diagnósticos.

Mensajes ICMP

- Tipo: Identifica el mensaje ICMP
- Código: Proporciona info sobre el tipo del mensaje.
- Cabecera y primeros 8 bytes del datagrama IP, permite al host origen identificar el datagrama.

Tipo ICMP	Código	Descripción
0	0	respuesta de eco (para ping)
3	0	red de destino inalcanzable
3	1	host de destino inalcanzable
3	2	protocolo de destino inalcanzable
3	3	puerto de destino inalcanzable
3	6	red de destino desconocida
3	7	host de destino desconocido
4	0	regulación del origen (control de congestión)
8	0	solicitud de eco
9	0	anuncio de router
10	0	descubrimiento de router
11	0	TTL caducado
12	0	Cabecera IP errónea

Echo Request/Echo Reply (PING)

- Para probar si dos host entran conectados, mide el RTT min/avg/max/dev y loss para diagnosticar.
- El envió es une echo request con tipo 8 al destino con código 0.
- La respuesta e sun echo reply con código.
- Si un nodo recibe un ICMP echo request debe responder copiando el contenido con un echo reply (PONG)

ICMP Destino inalcanzable

- Tipo 3.
- Código 0: No se puede alcanzar la red.
- Código 1: Host no alcanzable.

- Código 2: Protocolo no compatible:
- Código 3: Puerto inalcanzable.
- Código 13: Trafico bloqueado por firewall o ACL.

ICMP TTL expirado

- Tipo 11: Se descarta el paquete y se envía este código.
- Usado por Traceroute

ICMP route redirect

- Tipo 5
- EL host debe ir por otra ruta para llegar a donde quiere ir.

ICMP source quench

- Tipo 4
- Control de congestion, obsoleto.

ICMP address mask

- Tipo 17 (request) y tipo 18 (reply).
- Solicita la mascara de subred de una red local.

ICMP Timestamp

- Tipo 13 y 14 (request y reply).
- Para sincronizar la hora entre dispositivos.

DHCP(Dynamic Host Configuration Protocol)

- Protocolo de nivel de aplicación (montado sobre UDP)
- Sirve para que los dispositivos de red obtengan la información de configuración para comunicarse en la red.
- Para IPv4 o IPv6.
- Para conectarse a un red requiere:
  - Dirección IP, mascara de red. (Solo local)

- Default gateway (dirección del router que el host usa para enviar trafico redes externas) (entre redes)
- Para usar servicios (DNS).
- DHCP automatiza esto con servidores locales en la red, los hosts sin parámetros le piden requerimientos, el server responde y guarda el parámetro un tiempo.

DHCP Mensajes

- Discover.
- Offer.
- Request.
- ACK.
- Release.
- NAK.
  De broadcast:
- Discover.
- Request.
  Unicast:
- Offer.

NAT (Network Address Translation)

- Es un mecanismo que permite que múltiples dispositivos dentro de una red privada puedan acceder a una red pública (como Internet) utilizando una sola dirección IP pública.
- Usa tablas de traducción.
- Proceso sobre redes stubs (de salida).

NAT Básico.

- One-to-one
- Mapea un IPv4 privada a una publica.
- Acceso en ambas direcciones.

Modo estático:

- Mapea una dirección privada a una dirección pública de manera fija.

Modo dinámico:

- No requiere tantas direcciones publicas como privadas pero si un timer por cada uno. Limitado el acceso simultaneo.

NAPT(Network Address Port Translation)

- NAPT utiliza **campos de la capa de transporte o del payload**, como los **puertos de los protocolos u otros valores como el ICMP Identifier**, para realizar el mapeo de direcciones.
- **Uno a muchos**.
- La tabla de traducciones de NAPT almacena información sobre el **protocolo, los puertos de origen y destino**, y utiliza **temporizadores y sesiones de protocolo** para administrar las conexiones.
- NAPT **intenta conservar el puerto de origen** del dispositivo privado. Sin embargo, si el puerto ya está en uso, se reemplaza por otro disponible. En esencia, NAPT extiende la funcionalidad de NAT al **multiplexar múltiples conexiones de una red privada a través de una única dirección IP pública**, utilizando la información de puerto para distinguir las diferentes conexiones.

Port Forwarding

- Se implementa con NAPT, se configura a mano, permite tener servicios en una red privada accesibles desde "afuera".

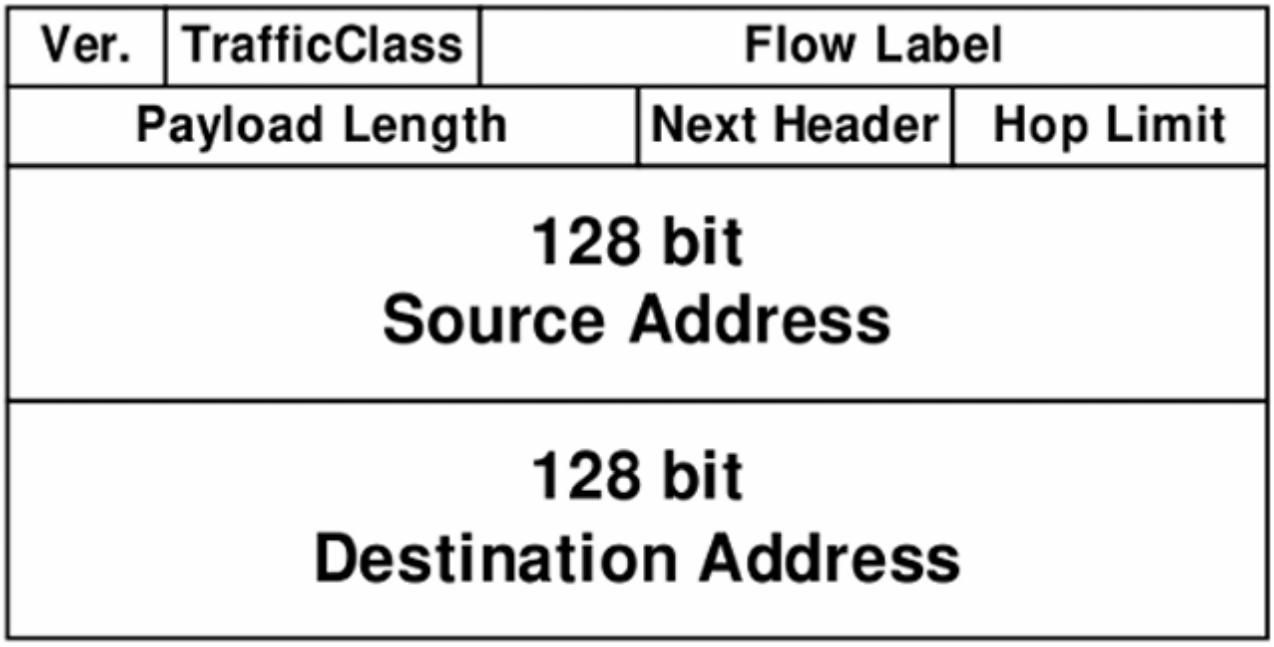
IPv6

- **Espacio de Direcciones**: 128 bits para una mayor cantidad de direcciones.
- **Menor Overhead de Procesamiento**: Procesamiento más eficiente.
- **Tablas de Enrutamiento**: Ordenación de las tablas de enrutamiento.
- **Autoconfiguración de Direcciones**: Conectar todo usando autoconfiguración sin ayuda (Ni DHCP).
- **Arquitectura de Red Jerárquica**: Ruteo más eficiente.
- **Seguridad a Nivel IP**: IPSec obligatorio para mayor seguridad.
- **Jumbogramas**: Soporte para datagramas de más de 64KB.

- **Movilidad y Multicast**: Mejor soporte para movilidad y direcciones de multicast.
- **ICMP**: ICMP no se puede desactivar.
- **Tamaño de Cabecera**: Datagramas con cabecera de 40 bytes.

Simplificación de la Cabecera

- **Fragmentación**: Eliminada, se realiza solo de extremo a extremo.
- **Checksum de Cabecera**: Eliminado.
- **Tamaño Fijo de la Cabecera**: No hay más opciones variables.
- **Flow Label**: Identificador de flujo de 20 bits (aunque no se usa ampliamente).
- **Renombrado de Campos**:
  - **Traffic Class**: Para tratamiento diferenciado de paquetes (antes TOS).
  - **Hop Limit**: Anteriormente TTL.
  - **Next Header**: Anteriormente Protocol.
- **Cabeceras de Extensión**:
  - Permiten la extensibilidad del protocolo.
  - Se encuentran después de la cabecera principal.
  - Generalmente procesadas por los extremos.



Funcionalidades de IPv6

- **Direccionamiento**: Asignación y gestión de direcciones IP.
- **Ruteo/Forwarding**: Enrutamiento y reenvío de paquetes de datos.
- **Generalidades de IPv6**: Características generales y mejoras sobre IPv4.

- **Mux/Demux de Protocolos Superiores**: Multiplexación y demultiplexación de protocolos de nivel superior.
- **Otras**: Prevención de bucles de enrutamiento.
- **Descubrimiento de Vecinos (NDP)**:
  - **ND propiamente**: Protocolos de descubrimiento de vecinos.
  - **Router Discovery y Autoconfiguración**: Detección de routers y configuración automática de direcciones.
- **Manejo de Grupos de Multicast**: Administración de grupos de multicast para la transmisión eficiente de datos.

Direcciones IPv6

- Se anotan en hexadecimal, cada 16 se separan con `:`, ceros contiguos se pueden eliminar con `::` pero solo una vez.
- Se usa `"[" "]"` para indicar puerto en la URL.
- Sin mascara, solo usa prefix length.

Tipos de direcciones:

- **Unicast:** Estas direcciones se utilizan para identificar una única interfaz de red. Se clasifican según su alcance:
  - **Locales (Link-local):**
    - **Alcance:** Limitadas a la red directamente conectada.
    - **Prefijo:** FE80::/10.
    - **Prefijo utilizado:** FE80::/64 (la longitud del prefijo en una LAN suele ser /64).
    - **IID (Identificador de Interfaz):** Se utilizan direcciones derivadas del hardware o generadas manualmente.
    - Las direcciones link-local se generan combinando el prefijo link-local con un IID único.
    - Se utiliza DAD (Detección de Direcciones Duplicadas) para garantizar la unicidad de la dirección.
  - **De sitio site-local (desaconsejadas):**
    - **Prefijo:** FEC0::/10.
    - **Alcance:** Limitadas a un sitio u organización (similar a las redes privadas en IPv4).
    - **Desaconsejadas:** Debido a la dificultad para definir los límites del sitio.
  - **De Sitio Únicas:**

        - **Prefijo:** FC00::/7, dividido en FC00::/8 y FD00::/8.
        - **Prefijo utilizado:** FD00::/8, [xxxxxxxL] donde el bit L = 1 indica una dirección local.
        - **Alcance:** Limitadas a un sitio u organización.
        - **Reemplazan las direcciones site-local.**
        - Se genera un ID único de forma pseudoaleatoria.
    - **Compatibilidad ipv4-compat (desaconsejadas):**
        - **Uso:** Transición de IPv4 a IPv6.
        - **Mapeo:** Asignan una dirección IPv6 a una dirección IPv4 global única.
        - **Tipos:** IPv4-mapped IPv6.
    - **Globales:**
        - **Prefijo:** Asignado por un proveedor de servicios de Internet (ISP).
        - **Alcance:** Internet (similar a las direcciones públicas en IPv4).
        - **Parte del host:** Se puede generar de cualquier forma, pero debe ser única.
        - **Longitud del prefijo del host:** Siempre se reservan 64 bits para la parte del host.
        - **Subredes:** El ISP puede usar menos de 48 bits para el prefijo de red, lo que deja más espacio para la creación de subredes dentro de la organización.
- **Multicast:** Estas direcciones se utilizan para enviar un paquete a un grupo de interfaces.
    - **Prefijo:** FF00::/8.
    - **Flags:** Indican si la dirección es permanente o temporal, entre otros.
    - **Alcance:**
        - 1: Nodo local.
        - 2: Link local.
        - 5: Site local.
        - 8: Organización local.
        - E: Global.
    - **GID (Identificador de Grupo):** Identifica el grupo multicast específico.
    - **Solicited Node Multicast Address (SD):**
        - **Uso:** Neighbor Discovery (ND), en lugar de inundar la red local con paquetes.
        - **Generación:** Se deriva de la dirección unicast o anycast.

    - **Funcionamiento:** Cada interfaz con una dirección unicast o anycast debe unirse al grupo multicast correspondiente.
- **Anycast:** Estas direcciones se utilizan para enviar un paquete a la interfaz más cercana dentro de un grupo de interfaces que comparten la misma dirección anycast.
    - IPv6 no tiene casos especiales para direcciones anycast.
- **Especiales**:
    - Any `::0/0`
    - Loopback (local host) `::1/128`
    - Documentación `2001:db8::/32`
    - 6bone `3FFE::/16` devueltas al IAN en 2005

Ruteo

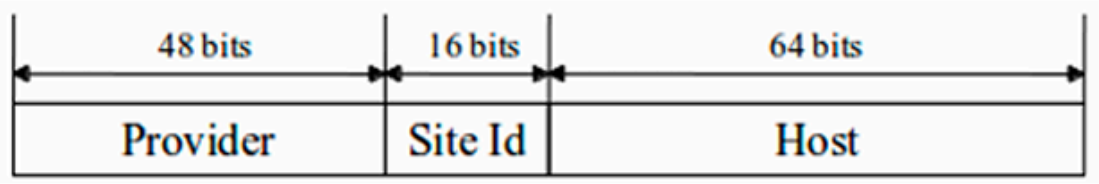
Se hace uso del RIB

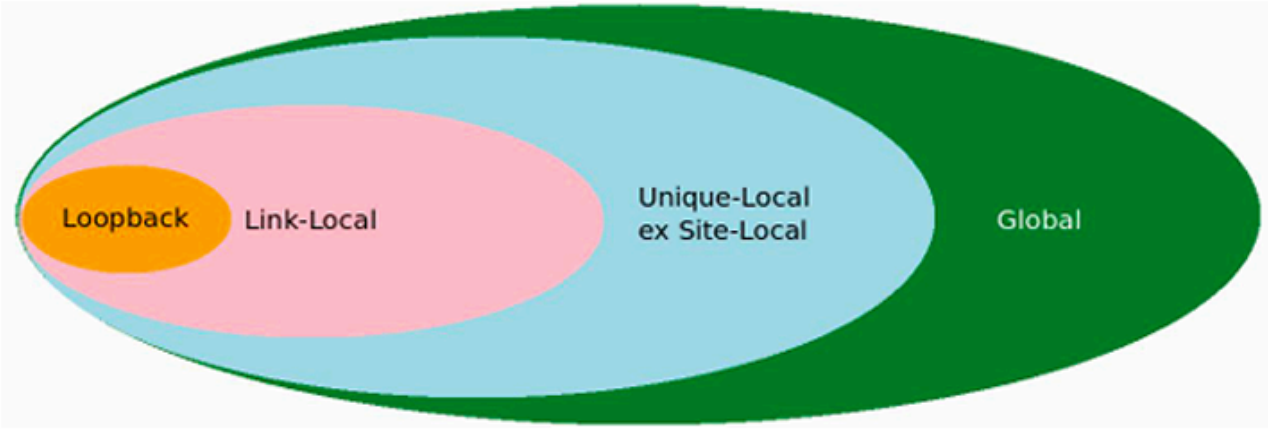
```
root@n7:/# ip -6 route show
2001:db8:1234:3::/64            dev eth0  proto kernel  metric 256
fe80::/64                       dev eth0  proto kernel  metric 256
default via 2001:db8:1234:3::1  dev eth0  metric 1024
default via fe80::200:ff:feaa:5 dev eth0  proto kernel ... expires 24sec
...

root@n7:/# netstat -nr -A inet6
Kernel IPv6 routing table
Destination           Next Hop            Flag   Met Ref   Use If
2001:db8:1234:3::/64  ::                  U      256 0     1   eth0
fe80::/64             ::                  U      256 0     0   eth0
::/0                  2001:db8:1234:3::1  UG    1024 0     0   eth0
::/0                  fe80::200:ff:feaa:5 UGDAe 1024 0     0   eth0
::1/128               ::                  Un       0 1     1   lo
...
```

- RuteoEstático.
- RIP-ng.
- OSPFv3.
- IS-IS.

- MP-BGP


48 bits
16 bits
64 bits
Provider
Site Id
Host


Loopback
Link-Local
Unique-Local
ex Site-Local
Global