Capa de Red – Resumen

PDU ⇨ Paquetes/Datagramas

Internet es un grupo de redes interconectadas, es una red de redes. La capa de red se encuentra presente en todos los protocolos de Internet.

La capa de red proporciona los servicios de enrutamiento y reenvío de paquetes (PDU) entre distintos hosts. El dispositivo principal de esta capa es el router. Es End-to-End (Extremo-a-extremo) y el ruteo se produce hop-by-hop (salto-a-salto) en donde cada nodo debe implementar IP.

IPv4 no es compatible con IPv6.

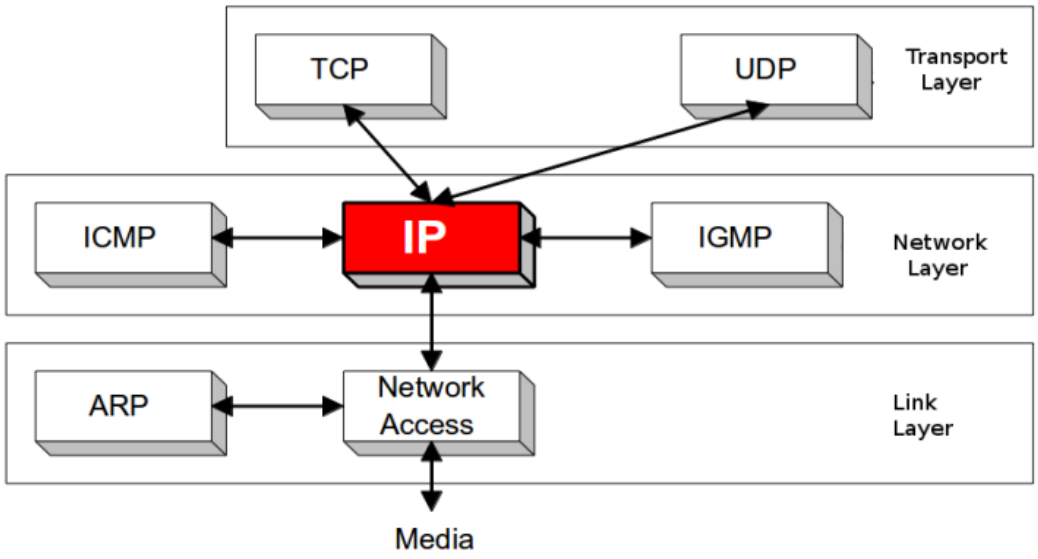
IPv4

Protocolo de Red no orientado a conexión y protocolo de mejor esfuerzo: best-effort, no confiable

Se lo considera un protocolo de mejor esfuerzo ya que se trata de un protocolo poco confiable, esto quiero decir que hace todo lo posible para entregar los datos, pero no garantiza que todos los paquetes llegarán al destino, ni de que lo harán en el orden correcto

La funcionalidad de este protocolo es la de:

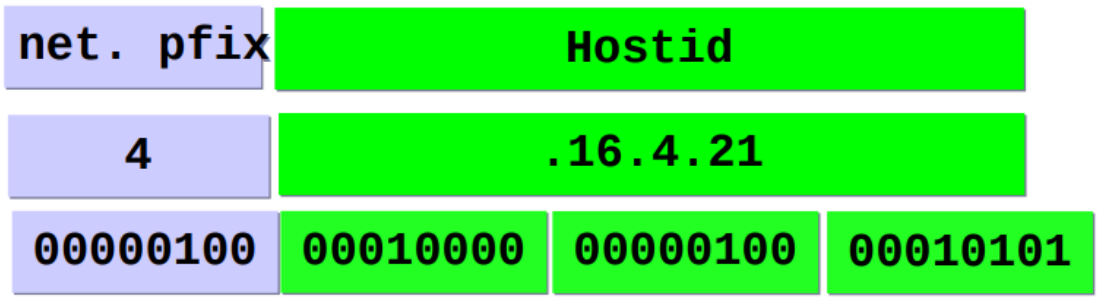
- Direccionamiento.
- Ruteo/Forwarding/Switching L3.
- Mux/Demux de protocolos superiores.
- Accesorias (Solucionar deficiencias del protocolo)
    - Fragmentación.
    - Otras: como evitar loops (TTL), detección de errores



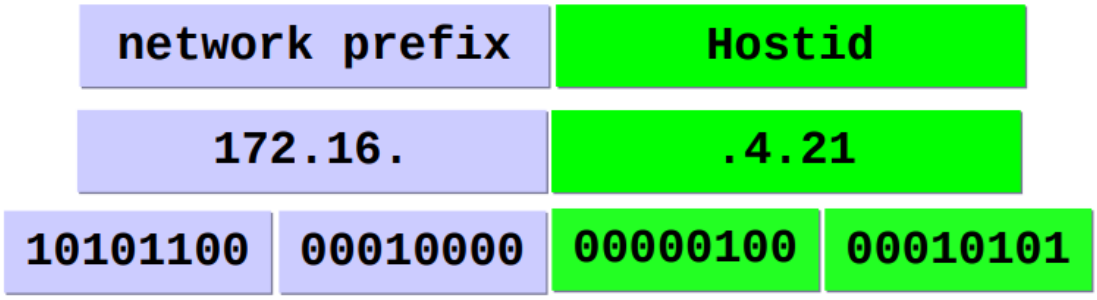
- Es el núcleo de la Internet.
- Requiere protocolos “Helpers”.

Dirección IP

- Identifica unívocamente un punto de acceso (interfaz) a la red.
    - Identifica red y luego host dentro de ella. Las redes se conectan a través de routers.
- Un router o un host multi-homed tienen varias IPs. Cada interfaz un valor único.
- Tienen un significado global en la Internet o privado (local).
    - Los globales son asignados por autoridad central (IANA).
- Números de 32 bits expresados en notación decimal delimitada por puntos byte a byte.
- 2^32 (4G de direcciones)
- Para facilidad de los usuarios, mapping con nombres de domino (DNS - Domain Name Server).
- Son necesarias para rutear la información por la Internet.
- Son direcciones lógicas.
- Dos partes
    - Red (Net).
    - Anfitrión (Host).



        - Hasta 1981, solo había pocas redes con muchos hosts disponibles. Sin clases. Redes 8 bits. Luego se definen las clases
- Hay clases para diferentes tipos de redes:
    - Clases A, pocas redes grandes.
    - Clases B, más redes medianas.
    - Clases C, muchas redes chicas.

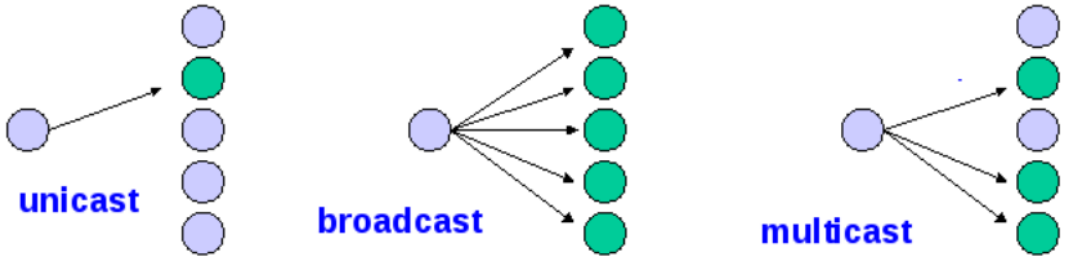


- Se agregan subredes y se requiere una máscara

Clase	Primer octeto	Rango	Objetivo	Cant. redes	Cant. hosts
A	0xxxxxxx	0.0.0.0 127.255.255.255	Organizaciones con grandes cantidades de hosts	2^7	$2^{24} - 2$
B	10xxxxxx	128.0.0.0 191.255.255.255	Organizaciones de tamaño mediano y grande	2^{14}	$2^{16} - 2$
C	110xxxxx	192.0.0.0 223.255.255.255	Pequeñas redes	2^{21}	$2^8 - 2$
D	1110xxxx	224.0.0.0 239.255.255.255	Direcciones de multicast	-	-
E	1111xxxx	240.0.0.0 255.255.255.255	Direcciones reservadas (para investigación y otros fines)	-	-

Tipos de Direcciones IP

- Unicast: destino a un host/interfaz en particular, son las más comunes. e.g: 172.16.4.21
- 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.



Direcciones especiales

- Loopback: unicast, red clase A. 127.0.0.1
  - La más utilizada: 127.0.0.1, localhost.
  - Va hasta 127.255.255.255
- Dirección de red: la primera (zero).
  - 172.16.0.0, 192.168.1.0.
- Dirección de broadcast:
- Directed Broadcast: la última (ones).
  - 172.16.255.255, 192.168.1.255.
  - Limited Broadcast: (all ones).
    - 255.255.255.255.

- “Este host”, cuando aún no tiene asignada una dirección:
    - 0.0.0.0 (Utilizada en BOOTP/DHCP)
- *También deberían estar las multicast i guess porque están reservadas para eso y la clase E.*

Direcciones privadas

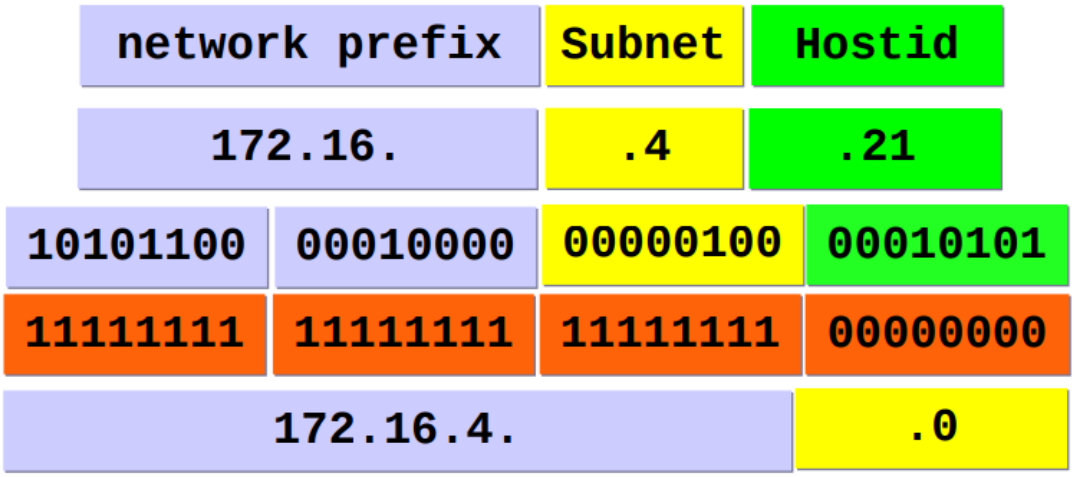
- No tienen significado global no son únicas.
- Se utilizan en redes locales.
- Para conectar a Internet requieren un proceso de transformación: NAT.
- No deberían pasar a la Internet. Filtradas por routers de borde.
    - 10.0.0.0 – 10.255.255.255, 1 Clase A.
    - 172.16.0.0 – 172.31.255.255, 16 Clases B.
    - 192.168.0.0 – 192.168.255.255, 256 Clases C.

Direccionamiento fijo

- Es por clase, uso los hosts que tengo según la clase.
- Provoca un uso ineficiente en el espacio de direcciones.
- Muchos equipos, produce escasez de direcciones (junto con un desperdicio)
- Crecimiento acelerado de la Internet, evidencia la falta de escalabilidad del esquema. Crecimiento de tablas de ruteo en el núcleo de la red.
- Codificar la red en la dirección IP implica que si un host cambia de red, cambiará su dirección (IP Mobility). Problema atacado en IPv4, mejor resuelto en IPv6.
- Soluciones IPv4: subnetting, CIDR, NAT, DHCP.

Subnetting

- Se toma una parte del hostid.
- Se utiliza para generar redes dentro de la red.
- Se agrega una “máscara” de bits.
- Para saber la subred se aplica un “AND” lógico.
- Permite que haya subgrupos en las redes, se utiliza para generar redes dentro de la red. Para ello toma una parte del hostid.
- La división en subredes plantea que si una red de clase desperdicia muchas direcciones IP entonces la misma sea dividida en N subredes más pequeñas que aprovechen mejor el espacio de direccionamiento
- Las máscaras se utilizan para saber en una dirección IP qué bits son de red y qué bits son de host.



- Agregar un nivel más en la estructura:
  - Red, Subred, Host.
  - Esto sirve para por ejemplo usar un bloque clase B como 256 clases C
- Las máscaras se escriben en notación decimal o hex.
- También pueden escribirse como longitud de prefijo: /24.
- Las máscaras defaults:
  - Clase A: 255.0.0.0.
  - Clase B: 255.255.0.0.
  - Clase C: 255.255.255.0.
- Cálculo de cantidad de subredes y hosts
  - Un cálculo muy común al realizar subnetting es el de computar la cantidad de hosts y de subredes que pueden obtenerse cuando se divide en subredes. Las cuentas son realmente simples y se basan en las siguientes fórmulas:
  - Cantidad de subredes utilizando bs bits para subred
    - 2^{bs}
  - Cantidad de hosts utilizando bh bits para hosts
    - $2^{bh} - 2$
    - El motivo por el cual se restan los dos bits en la última fórmula es porque la primer y última IP de una subred no pueden utilizarse, debido a que la primera dirección es la dirección de subred y la última la de broadcast.

Valen los mismos conceptos para redes completas.

Ejemplo para 172.16.4.21:

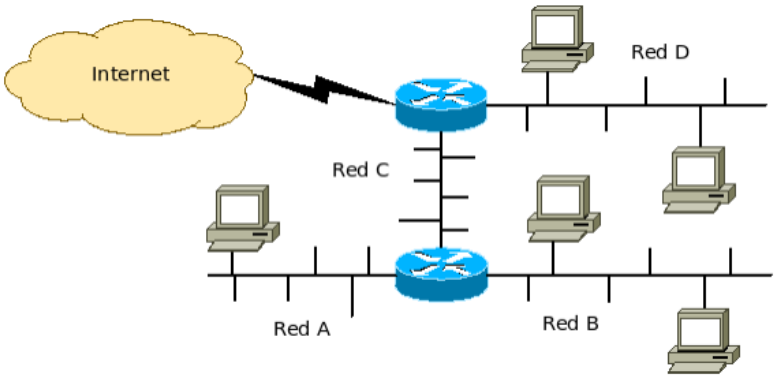
- Dirección de broadcast: 172.16.4.255.
- Dirección de red: 172.16.4.0.
- Redes y hosts: (2^n), (2^(32-(m+n))).
- Ejemplo Clase B con /24: n=8, m=16.
  - Cantidad de hosts: (2^8).
  - Cantidad de hosts útiles: (2^8)-2.
  - Cantidad de subredes: (2^8).
  - Cantidad de subredes útiles: (2^8)-2.
  - Las 2 que se restan a las subredes se pueden utilizar: dando: 2^8 redes útiles.

Subnetting fijo y Subnetting variable

En el subnetting fijo se tiene una misma marcara para todas las subredes de la red, sigue habiendo un desperdicio (aunque no tanto como el que se tenía antes).

Si cada red menos de 254 hosts, por ejemplo 25 c/red. Se pueden utilizar 1 clase C dividida en 4:

Red A: 193.168.4.0 255.255.255.192 o /26
Red B: 193.168.4.64 “
Red C: 193.168.4.128 “
Red D: 193.168.4.192 “



Ejemplo Subnetting Fijo

4 Redes físicas, pueden direccionarse con una red I

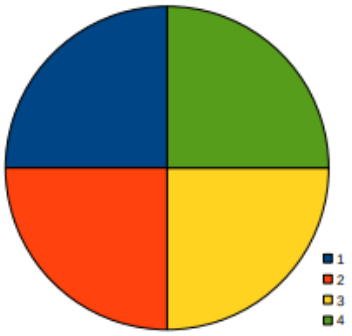
- 4 redes requieren 2 bits 2^2 = 4.
- Si fuesen 6, se requieren 2^3 = 8 ~ 6. Siempre potencias de 2.

193.168.4.			0	
193.168.4.			--	------
1100001	10101000	0000100	--	------
11111111	11111111	11111111	11000000	
193.168.4.			00	
			01	

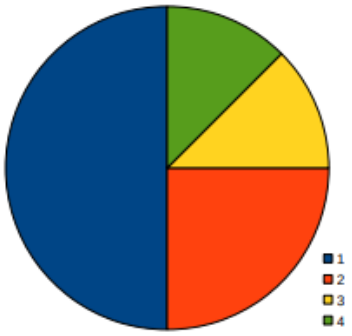
El subnetting variable (VLSM) permite que la longitud de la máscara no tenga la necesidad de ser igual para todas. Se amolda mejor a las necesidades de hosts de cada subred evitando que haya un desperdicio de direcciones y por lo tanto, evitando el agotamiento de esta.

VLSM Subnetting

- Subredes iguales: /26
  255.255.255.192
  255.255.255.192
  255.255.255.192
  255.255.255.192



- VLSM: /25, /26, /27, /27:
  255.255.255.128
  255.255.255.192
  255.255.255.224
  255.255.255.224



Mecanismo de subnetting variable

1. Subnetear para la red con mayor cantidad de hosts.

2. De las subredes obtenidas, asignar todas las que se puedan con el menor desperdicio posible.
3. Si quedan segmentos de red sin una subred asignada volver al paso 1.

CIDR

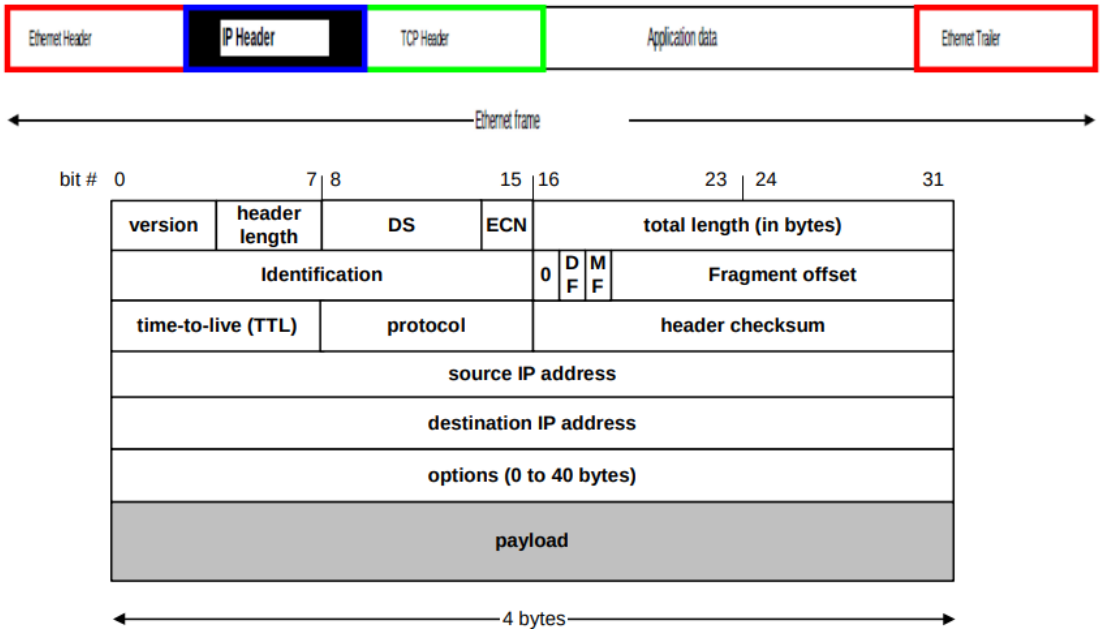
CIDR (Classless Inter Domain Routing) es una estrategia para frenar algunos problemas que se habían comenzado a manifestar con el crecimiento de Internet. Los mismos son:

- Agotamiento del espacio de direcciones de clase B.
- Crecimiento de las tablas de enrutamiento más allá de la capacidad del software y hardware disponibles.
- Eventual agotamiento de las direcciones IP en general.

CIDR consiste básicamente en permitir máscaras de subred de longitud variable (VLSM) para optimizar la asignación de direcciones IP y utilizar resumen de rutas para disminuir el tamaño de las tablas de enrutamiento.

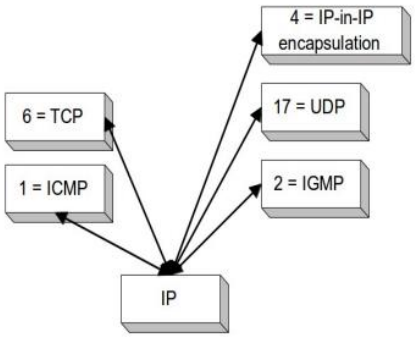
- Hasta 1993, se asumía, de acuerdo a la clase de la Dir. IP la máscara default.
- Los bits de la red definida por la clase eran fijos.
- El direccionamiento era Classful.
- Con CIDR, se sacan las clases: Classless y siempre debe haber una máscara o long. de Pref.
- Básicamente permite agrupar para reducir la longitud de las tablas de ruteo

Datagrama IPv4



- Version (4 bits): versión actual 4, la nueva 6
- Header length (4 bits): longitud en múltiplos de 4B.
- DS/ECN field (1 byte)

    - TOS (Type of Service), DSCP DiffService Codepoint.
    - Differentiated Service (DS) (6 bits): Usado para marcar QoS
    - Explicit Congestion Notification (ECN) (2 bits): Usado en control de congestión con TCP.
- Identification (16 bits): identificador único. Utilizado para la fragmentación.
- Flags (3 bits)
    - Primero es 0.
    - DF bit (Do not fragment) y MF bit (More fragments)
        - Utilizados para la fragmentación.
- Time To Live (TTL) (1 byte)
    - Cuantos saltos puede dar el datagrama.
    - Evita loops.
    - Emisor lo pone a un valor, e.g. 128 o 64.
    - Cada router por el que pasa lo decrementa en 1.
    - Si esta más de un segundo también.
    - Si llega a un router que no está en la red destino y TTL=0, se descarta.
- Protocol (1 byte): Para mux/demux.



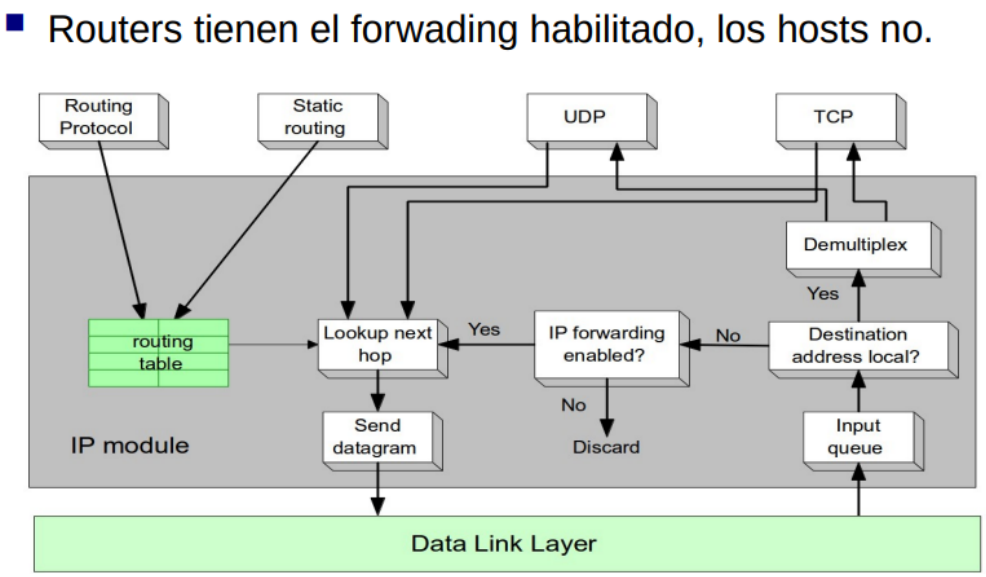
- Header checksum (2 bytes): 16 bit checksum del header solamente.
- Options
    - Security restrictions.
    - Record Route
    - Timestamp.
    - (loose) Source Routing
    - (strict) Source Routing.
- Padding: agregado para ser múltiplo de 4B.

Ruteo

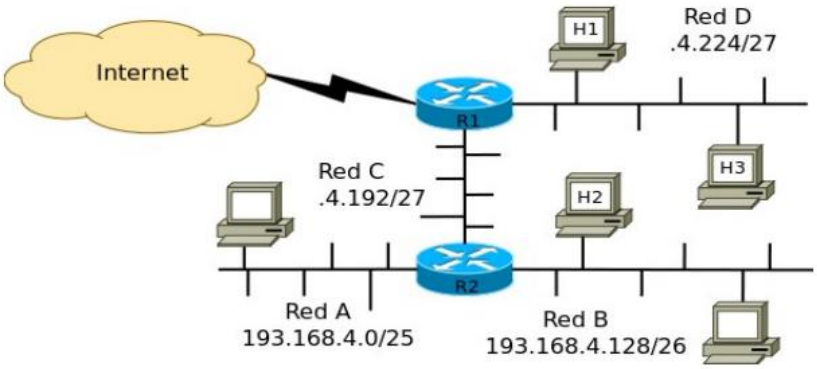
- Tabla de ruteo: estructura en hosts y routers (gateways) que indica como despachar un mensaje. Perspectiva del vecino, siguiente salto.
- Host: no despacha mensajes que recibe que no son para él. Despacha solo sus mensajes mirando su tabla de ruteo.
- Router: Nodos intermedios, más de una interfaz, despacha mensajes mirando tabla de ruteo, desde cualquier interfaz.
- Host multihome: tiene varias interfaces, no rutea.
- Ruteo: seleccionar la interfaz de salida y el próximo salto. Routers y Hosts.
- Forwarding/Despacho: pasar el paquete desde una interfaz de entrada hacia una de salida. Solo routers.

- El ruteo es de control, alimentado por protocolos de enrutamiento (routing).
- El forwarding es de datos, envía protocolos enrutados (routed).
    - Decisiones de “forwarding” en IP se llevan a cabo localmente
    - Deriva en conectividad entre los diferentes puntos de la red
    - Se requieren recolectar y procesar un estado global
    - Se mantiene un estado global localmente en cada router
    - Los estados locales deben ser consistentes, si son inconsistentes la red no habrá convergido a un estado estable, se generan loops
    - Se requiere:
        - Consistencia
        - Completitud
        - Escalabilidad
    - Se desea:
        - Camino óptimo
        - Balanceo
        - Adaptabilidad
- El protocolo ENRUTADO (Routed) IP, requiere los servicios del protocolo de ENRUTAMIENTO/RUTEO (Routing) para construir las tablas de ruteo en cada router (gateway)
- Ruteo: proceso mediante el cual se construye la tabla de ruteo o RIB (Routing Information Base) Protocolo de ENRUTAMIENTO. Plano de Control. Algunos routers lo hacen
- FIB: Forwarding Information Base / Forwarding Table, el proceso de forwarding que se hacer a partir de la RIB se optimiza generando una tabla más eficiente, FIB.
- Todos los equipos en la red corren el protocolo ENRUTADO (IP)
- Los hosts no requieren correr protocolos de ENRUTAMIENTO/RUTEO
- Los router requieren hacer el ENRUTAMIENTO podrían trabajar de dos formas/ tipos de Routing:
    - Ruteo Estático
        - Las rutas son establecidas por el administrador manualmente
        - Propenso a errores
        - Si se cambia la topología requiere cambios manuales en los routers
        - Sirve cuando se tiene una red sencilla
        - No tiene problemas de seguridad ni de incompatibilidad
        - No implica costo de procesamiento extra
        - Mayor control
        - Esquema NO escalable y NO tolerante a fallos
    - Ruteo Dinámico
        - Requiere una configuración inicial por el administrador
        - Si se cambia la topología se adapta de forma automática
        - Facilita mantenimiento cuando se tiene una red compleja
        - Implica costo de procesamiento extra
        - Esquema escalable y tolerante a fallos
        - Resolución de Problemas/Debugging, más complejo

        - Caminos “óptimos” de acuerdo a la información manejada por el protocolo (métrica, costo)
        - Clasificación protocolos:
            - IGP (Interior Gateway Protocols), trabajan en el mismo AS (definición de AS más abajo)
            - EGP (Exterior Gateway Protocols), trabajan entre diferentes AS
        - Otra clasificación:
            - Protocolos de DV (Vector de Distancia)
            - Protocolos de PV (Vector de Camino)
            - Link State (Estado de Enlace)
            - Vector de Distancia Avanzado (Advanced VD) (considerado Híbrido)
- Routers pueden participar de forma activa en el routing: reciben, generan y propagan información, los hosts lo hacen de forma pasiva
- Routing Domain: seleccionamos el/los protocolo/s de Ruteo en un Routing Domain, conjunto de routers con Routing Protocols comunes. Uno o más de estos incluidos en un AS.
- Sistema Autónomo (Autonomous System, AS): conjunto de redes bajo la misma administración (podría ser gestionada por más de un operador de red), y utilizando un protocolo de ruteo o combinaciones para rutear internamente, independientemente de la red de su proveedor. Hay una clara y única política de ruteo. Cada AS en Internet debe tener un número identificador: ASN (AS Number).

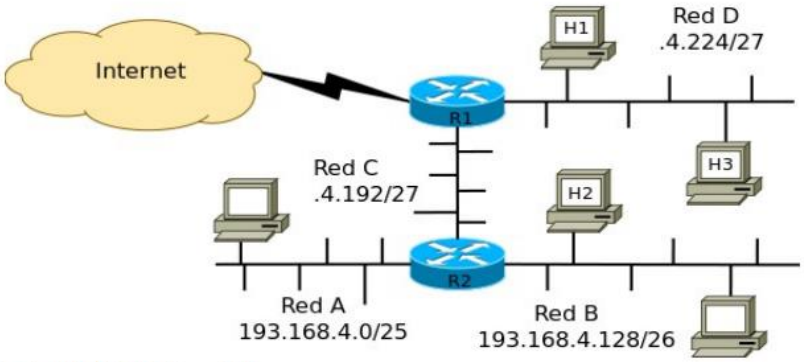


Ejemplo
H1



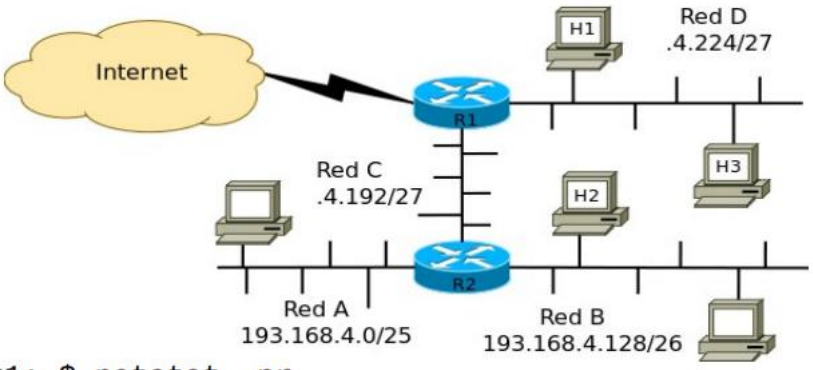

```
root@h1:~# ifconfig e0 193.168.4.226 netmask 255.255.255.224

root@h1:~# route add default gw 193.168.4.225

root@h1:~# netstat -nr
Destination     Gateway         Genmask         Metric Iface
193.168.4.224   0.0.0.0         255.255.255.224 0       e0
0.0.0.0         193.168.4.225   0.0.0.0         -       e0
```


R2




```
root@r2:~# netstat -nr
Destination     Gateway         Genmask         Metric Iface
193.168.4.0     0.0.0.0         255.255.255.128   0       e0
193.168.4.128   0.0.0.0         255.255.255.192   0       e1
193.168.4.192   0.0.0.0         255.255.255.224   0       e2
0.0.0.0         193.168.4.193   0.0.0.0           -       e2
```

R1



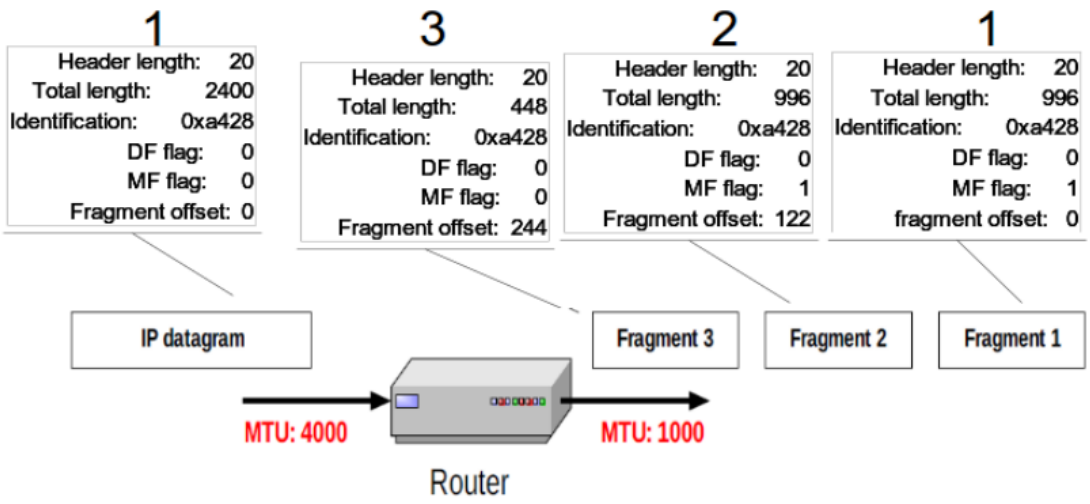

```
andres@r1:~$ netstat -nr
Destination     Gateway         Genmask         Metric Iface
193.168.4.224   0.0.0.0         255.255.255.224   0       e1
193.168.4.192   0.0.0.0         255.255.255.224   0       e0
200.3.4.0       0.0.0.0         255.255.255.252   0     ppp0
193.168.4.0     193.168.4.194   255.255.255.128   0       e0
193.168.4.128   193.168.4.194   255.255.255.192   0       e0
0.0.0.0         200.3.4.1       0.0.0.0           -     ppp0
```

CON CIDR

```
andres@r1:~$ netstat -nr
Destination     Gateway         Genmask         Metric Iface
193.168.4.224   0.0.0.0         255.255.255.224   0       e1
193.168.4.192   0.0.0.0         255.255.255.224   0       e0
200.3.4.0       0.0.0.0         255.255.255.252   0     ppp0
193.168.4.0     193.168.4.194   255.255.255.0     0       e0
0.0.0.0         200.3.4.1       0.0.0.0           -     ppp0
```

Tareas de ruteo

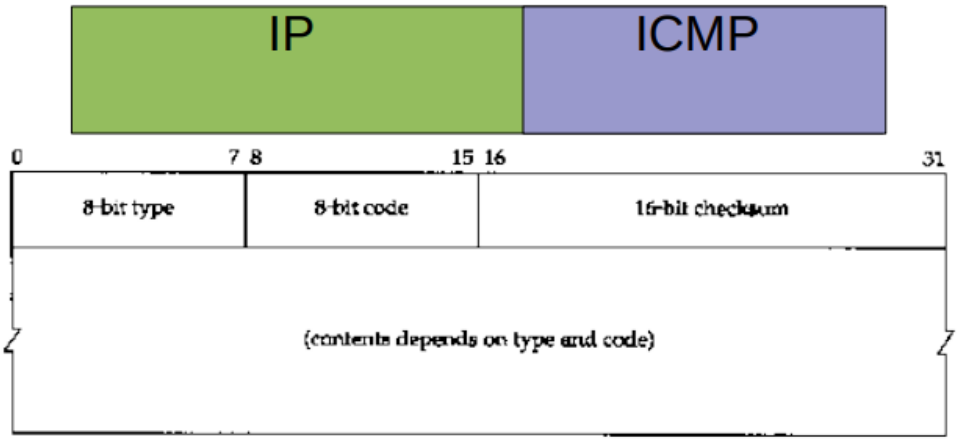
- Validación de datagrama: IP header.
- Calcula checksum (solo header).
- Leer IP destino.
- Buscar en tabla de ruteo, seleccionar prefijo más largo (“best match”).
- Decrementar TTL.
- Fragmentar (alternativo).
    - Debido a que hay diferentes capas de enlaces con diferentes MTUs.
    - Fragmentos múltiplos de 8 bytes.
        - Offset en unidades de 8 bytes.
    - Se deben agregar los headers.



- Transmitir o Descartar.
- Generar ICMP (alternativo).

ICMP

- Protocolo de la capa 3.
- Helper de IP
- IP carece de control, el mismo es dado por un protocolo auxiliar.
- Brinda feedback
- ICMP podría ser prescindible de en IPv4,
- se encapsula en IP
- no es un protocolo de transporte
- Formato de mensaje



- Tipos de Mensajes ICMP:
  - Echo Request/Echo Reply (PING).
    - Se utiliza para probar la conectividad entre dos hosts en una red IP.
    - Permite medir el tiempo que tarda en viajar la solicitud y regresar la respuesta. Esto se conoce como el RTT (Round-Trip Time), y el "ping" muestras estadísticas como el RTT mínimo, promedio, máximo y desviación estándar, junto con la pérdida de

paquetes lo que puede ayudar a diagnosticar problemas de conectividad.
        - Básicamente, envía un mensaje de solicitud (Echo Request) a un host y espera una respuesta (Echo Reply).
        - Cuando un nodo recibe una solicitud "Echo Request", debe responder copiando el contenido del mensaje con un "Echo Reply" (pong).
            - Ping envía un paquete ICMP tipo 8 (Echo Request) con código 0. Este paquete contiene un mensaje de solicitud de eco. El código 0 especifica que es una solicitud estándar sin código específico.
            - Cuando el destino recibe una solicitud de eco (paquete ICMP tipo 8), responde con un paquete ICMP tipo 0 (Echo Reply) con código 0. l código 0 especifica que es una respuesta estándar sin código específico.
    - Destino Inalcanzable.
        - Para indicar que una red, un host, un puerto es inalcanzable, diferentes causas.
            - Host Inalcanzable (Host Unreachable): no esta el host en la red.
            - Red Inalcanzable (Network Unreachable): router no esta en tabla de ruteo.
            - Puerto Inalcanzable (Port Unreachable): no hay un proceso UDP en el puerto
            - Los mensajes requieren fragmentación.
            - El mensaje fue filtrado
            - Etc.
    - TTL expirado.
        - El tiempo de vida ha expirado. En realidad es el hop count con el cual salió el mensaje ha expirado.
            - Excedido en viaje o en re-ensamblado.
            - Valor máximo de TTL=255.
            - Puede salir con otro valor.
            - Si TTL == 0, pero ya llegó a la red destino debería enviarse.
    - Source Quench (Control de Congestión).
    - Redirección de Ruta.
    - Address Mask y Timestamp.

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

DHCP

- Un host para conectarse a una red IP requiere 3 parámetros + 1.
- Red local:
    - Dirección IP
    - Máscara de red
- Otras redes:
    - Router por default (Default Gateway).
- Usar servicios:
    - Servidor(es) de DNS
- Estos parámetros los puede obtener de forma:
    - Estática:
        - Configuración manual
        - Difícil de mantener
        - No escalable
        - No sirve para movilidad
    - Dinámica
        - RARP
        - ICMP
        - BOOTP
        - DHCP
- DHCP es un protocolo de capa 3 helper de IP, como esta montado en UDP se lo suele considerar un protocolo de capa de aplicación. Se utiliza tanto para IPv4 como para IPv6.
    - Permite la configuración dinámica de los parámetros de red de los hosts.
    - Cuando los hosts arrancan solo tienen acceso a su red local de forma broadcast.
    - En la red local existe un o más servidor de autoconfiguración:
        - DHCP servers.
    - Los hosts sin parámetros de red envían requerimiento.
    - Los servidores los atienden asignando los valores que brindan conectividad.

- El parámetro se reserva por un tiempo.
- Algunos Mensajes DHCP:
  - Discover.
  - Offer.
  - Request.
  - ACK.
  - Release.
  - NAK.
- Montado sobre UDP:
  - Bootpc (client) 68
  - Bootps (server) 67
- DHCP Mensajes Broadcast
  - Broadcast
    - Discover.
    - Request.
  - Unicast/Broadcast
    - Offer
      - En general se envía unicast, pero debido a que pueden existir equipos que no procesan mensajes unicast antes de tener configurada la dirección IP completa, se podrían enviar en forma broadcast.
- Relay: Los routers pueden funcionar como agentes DHCP Relay y enviar los mensajes de DHCP broadcast de forma unicast a helper (DHCP server). *(EH?)*

NAT (Network Address Translation)

- Traslación de direcciones de un espacio privado (no “enrutable” en Internet) a un espacio público.
  - La traslación solo se realiza a la salida y se deben mantener tablas

NAT básico

- One-to-one
- Se mapea una dirección IPv4 privada a una dirección IPv4 pública. Permite acceso en ambas direcciones.
- Estático: requiere tantas direcciones públicas como privadas.
- Dinámico: no necesita tantas públicas como privadas pero sí se requiere un timer por cada entrada. Limita acceso simultaneo de acuerdo al pool pub.

NAPT (Network Address Port Translation)

- PAT (Port Address Translation): “one-to-many”.
- No es implementable cuando se tiene un pool chico de direcciones o no se posee direcciones publicas asignadas.
- Se trabaja con campos de la capa de transporte o del payload.
- Utilizan los puertos (u otros valores como ICMP Identifier para el mapeo).

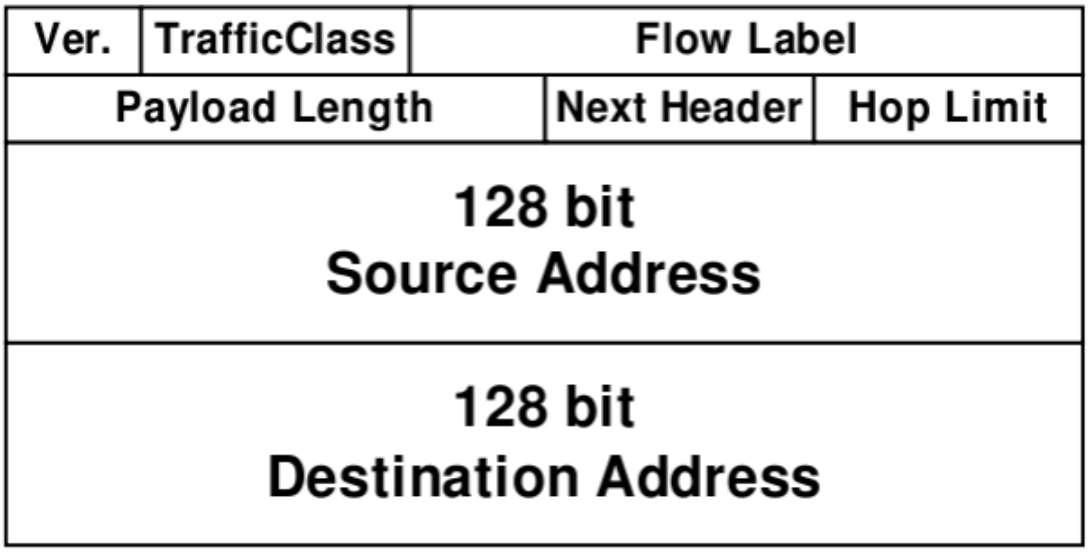
    - Están en las tablas de traslaciones.
    - Se intenta conservar el de origen pero si está ocupado se reemplaza
    - Básicamente si hay otro que genera mismo puerto y destino y no hay mas direcciones, se cambia el puerto origen (por uno que no está ocupado)
- Se pueden usar timers y sesiones de protocolo.
- Dinámico sobre pool: utiliza un pool y hace PAT sobre este (habitual en nuestras casas)
- Dinámico sobre dirección overload/masquerade: utiliza la dirección IP externa y haciendo overloading/masquerading sobre esta.

Port Forwarding

- Overloading/Masq no permiten acceso desde “afuera” hacia “adentro”.
- Solo se permite entrar tráfico de conexiones generadas internamente.
- Permite poder tener servicios en una red privada accesibles desde “afuera”.
- No se requiere NAT estático, se implementa con NAPT y mapeo reverso estático de puertos.
- Se configura a mano.

IPv6

- Mayor espacio de direcciones - 128 bits:
- Formato de cabecera simplificado.
- Menor overhead de procesamiento.
- Ordenar las tablas de enrutamiento
- Conectar todo, usar autoconfiguración de direcciones
- Arquitectura de red jerárquica para un ruteo eficiente.
- Seguridad a nivel IP (IPSec obligatorio).
- Jumbogramas, size(datagrama) > 64KB.
- Movilidad y más direcciones de multicast.
- No puedo desactivar ICMP
- Datagramas de 40 bytes
- Simplifica cabecera
    - No hay fragmentación
    - No hay checksum
    - Tamaño fijo de header
    - Hay identificador de flujo (Flow Label): Si hay mensajes que son de una misma conexión debo meterme a transporte, Flow Label se usaba para eso pero no se termino usando.
    - Se renombran los campos: Traffic Class (TOS, permite tratar paquetes de forma diferenciada), Hop Limit (TTL), Next Header (Protocol)
    - Cabeceras de extensión
        - Permite la extensibilidad del protocolo.
        - Se encuentran a continuación del header.
        - En general, son procesadas por los extremos.



Funcionalidad

- Direccionamiento
- Ruteo/Forwarding
- Mux/Demux de protocolos superiores.
- Otras: como evitar loops.
- Nuevas:
    - Descubrimiento de Vecinos (NDP):
        - ND propiamente
        - Router discovery y autoconfiguración
    - Manejo de Grupos de Multicast.

Dirección IP

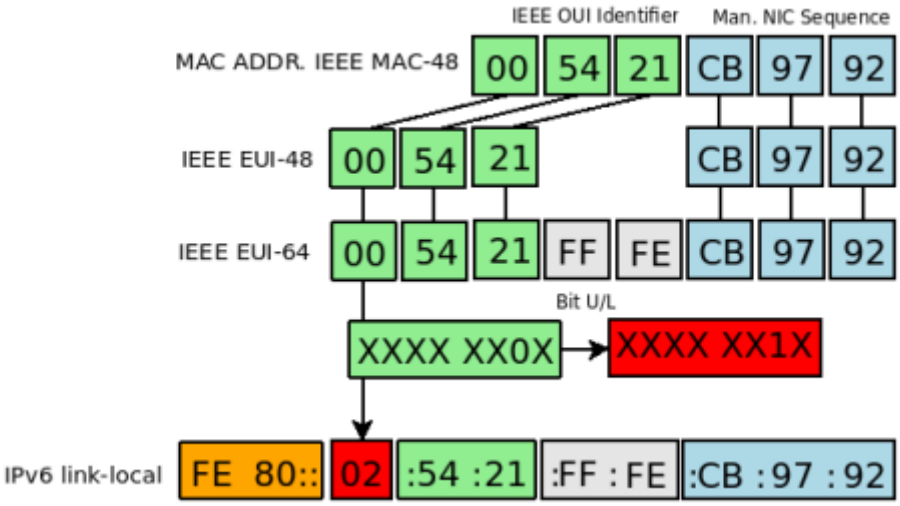
- Son de 128 bits
- Se anotan en hexadecimal en grupos de 16 bits, separadas por ":".
- Los ceros al inicio de cada grupo se pueden obviar.
- Ceros contiguos se puede eliminar con "::". Sólo se puede utilizar una vez
- Se utilizan "[","]"para indicar port en URL: http://[2001:db8:1011:1:0:0:0:1]:8080
- No se usa máscara, solo prefix length.

Tipos de Direcciones IP

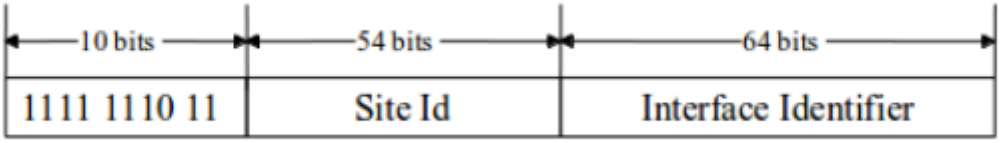
- Unicast.
    - Alcance
        - Locales (Link-local)
        - De sitio site-local (desaconsejadas), unique-local.
        - Compatibilidad ipv4-compat (desaconsejadas), ipv4-mapped.
        - Globales
- Anycast (tomadas del rango Unicast).
- Multicast (no hay direcciones broadcast): FF00::/8.

Direcciones IPv6 unicast

- Link-local.
  - Alcance: solo red directamente conectada
  - Prefijo Asignado: FE80::/10.
  - Prefijo Utilizado: FE80::/64 (len. en LAN /64)
  - IID se usan direcciones del hardware
    - De forma manual.
    - Se generan con el prefijo link-local y realiza DAD (Duplicate Address Detection)

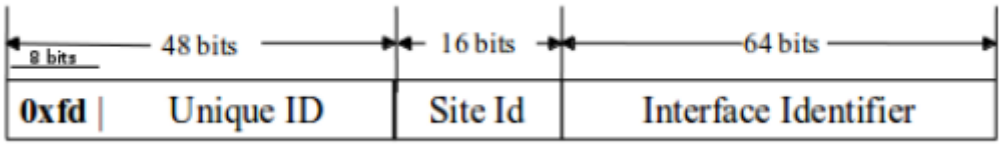


- Site-local.
  - Prefijo: FEC0::/10
  - Alcance: sitio u organización. Similar a las redes privadas de IPv4.
  - Dificultad de establecer los límites.

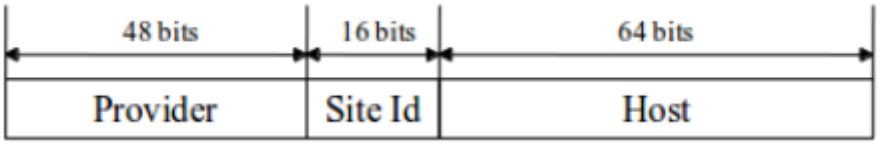


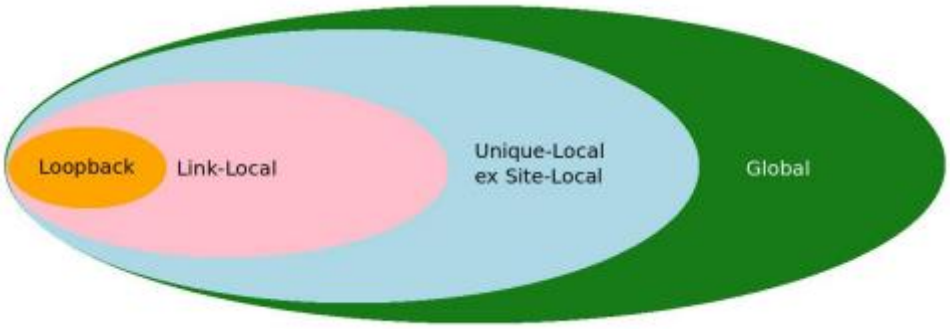
- Unique-Local.
  - Prefijo: FC00::/7, dividido en FC00::/8 y FD00::/8.
  - Prefijo Utilizado: FD00::/8, [xxxxxxxL] L bit = 1 (def. local).
  - Alcance: sitio u organización.

- Reemplazan las direcciones de Site Local. Unique ID generado de forma pseudoaleatoria



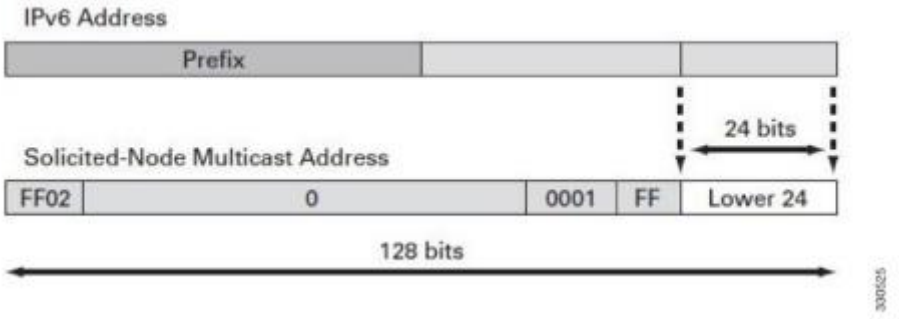
- IPv4-Compatible.
  - Usadas para la transición.
  - Asigna a un IPv4 global única una IPv6.
- IPv4-Mapped.
- Global
  - Prefijo: cedidos por un provider
  - Alcance: Internet. Similar a las direcciones públicas de IPv4.
  - La parte del host la genero como quiero pero debe ser única.
  - Siempre siempre se deja 64 para el host. El proveedor puede usar menos de 48 bits lo que significa que me queda más para subredes





Direcciones IPv6 Multicast

- Prefijo: FF00::/8
- Flags: permanente, temporaria. Otros reservados.
- Alcance: 1: nodo local, 2: link local, 5: site local, 8: org. local,
- E: global.
- GID: grupo de multicast.



- Solicited Node Multicast Address (SD)
  - Usada para ND (Neighbor Discovery) en lugar de flooding en la LAN.
  - Generada a partir de unicast/anycast.
  - Por cada unicast/anycast debe hacer join de la multicast.

Direcciones especiales

- Any (sin especificar):
  - ::0/0
- Loopback/Localhost:
  - ::1/128
- Documentación:
  - 2001:db8::/32
- 6Bone:
  - 3FFE::/16, devueltas al IANA en 2006.

Ruteo

Hay tabla

- RIB (Tabla de Ruteo)

```
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
...
```

- Ruteo Estático.
- RIP-ng.
- OSPFv3.
- IS-IS.
- MP-BGP.
- ...