# Capa de red

La capa de red tiene como objetivo, controlar el flujo de paquetes y ocuparse del direccionamiento entre redes. Los protocolos que más se usan en esta capa son el IP (*Internet Protocol*) y ICMP (*Internet Control Messege Protocol*).

## Protocolo IPv4

Es la cuarta versión del protocolo IP, y la primera en ser implementada a gran escala. Usa direcciones de 32 bits, es decir que hay 2^32 direcciones disponibles.
Los objetivos del protocolo IP son:

- Realizar la función de ruteo.
- Generar datagramas, los cuales son la unidad básica para la transferencia de datos a través de Internet.
- Incluir un conjunto de reglas para la entrega de paquetes no confiable.

## Cabecera IPv4

<table>
<tr><td>Versión</td><td>Longitud de cabecera</td><td>Tipo de servicio</td><td colspan="2">Longitud Total</td></tr>
<tr><td colspan="3">Identificador</td><td>Flag</td><td>Posición de Fragmento</td></tr>
<tr><td colspan="2">Tiempo de vida</td><td>Protocolo</td><td colspan="2">Checksum</td></tr>
<tr><td colspan="5">Dirección IP de Origen</td></tr>
<tr><td colspan="5">Dirección IP de destino</td></tr>
<tr><td colspan="4">Opciones</td><td>Relleno</td></tr>
</table>

- Versión (4 bits): Es el siguiente grupo de bits 0100 que representan el 4.
- Longitud de cabecera (4 bits): tendrá un tamaño entre 20 y 60 Bytes dependiendo de las opciones.
- Tipo de servicio (8 bits): Indica una serie de parámetros sobre la calidad de servicio deseada durante el tránsito por una red. Algunas redes ofrecen prioridades de servicios, considerando determinado tipo de paquetes "más importantes" que otros.
- Longitud Total (16bits): mide la cabecera + el campo de datos.
- Identificador(16bits): Se utilizará, en caso de que el datagrama deba ser fragmentado, para poder distinguir los fragmentos de un datagrama de los de otro.
- Flag (3 bits):utilizado sólo para especificar valores relativos a la fragmentación de paquetes.
- Posición de Fragmento (13 bits) :En paquetes fragmentados indica la posición que ocupa el paquete actual dentro del datagrama original.
- Tiempo de vida (8 bits):Indica el máximo número de enrutadores que un paquete puede atravesar. Cada vez que algún nodo procesa este paquete disminuye su valor en 1 como mínimo, una unidad. Cuando llegue a ser 0, el paquete será descartado.
- Protocolo (8 bits): Indica el protocolo de las capas superiores al que debe entregarse el paquete.

- Checksum (16 bits): Se recalcula cada vez que algún nodo cambia alguno de sus campos. Sirve para el control de errores.
- Dirección IP de origen (32 bits)
- Dirección IP de destino (32 bits)
- Opciones (variable): Aunque no es obligatoria la utilización de este campo, cualquier nodo debe ser capaz de interpretarlo. Puede contener un número indeterminado de opciones.
- Relleno (variable): Utilizado para asegurar que el tamaño, en bits, de la cabecera es un múltiplo de 32. El valor usado es el 0.

## Direcciones IP

| Clase | Formato | Rango | IP privadas | Máscara |
|---|---|---|---|---|
| A | r.h.h.h | 0.0.0.0 – 127.0.0.0 | 10.0.0.0 – 10.255.255.255 | 255.0.0.0/8 |
| B | r.r.h.h | 128.0.0.0 – 191.255.0.0 | 172.16.0.0 – 172.31.255.255 | 255.255.0.0/16 |
| C | r.r.r.h | 192.0.0.0 – 223.255.255.0 | 192.168.0.0 – 196.168.255.255 | 255.255.255.0/24 |
| D | - | 224.0.0.0 - 239.255.255.255 | - | - |
| E | - | 240.0.0.0 – 255.255.255.255 | - | - |

También hay algunas direcciones IP especiales como:

127.0.0.1 (127 y nada o 1) → Loopback (mi propio host)
0.0.0.10 (Todos 0 y host) → Anfitrión de esta red
192.3.0.0 (red y todos 0) → Identifica la red
192.3.255.255 (red y host todos en 1) → Difusión a esta red

## Ruteo de datagramas

Con ruteo nos referimos al proceso de selección de un camino para el envío de paquetes. El ruter es el dispositivo que realiza esta selección. Existen dos formas:

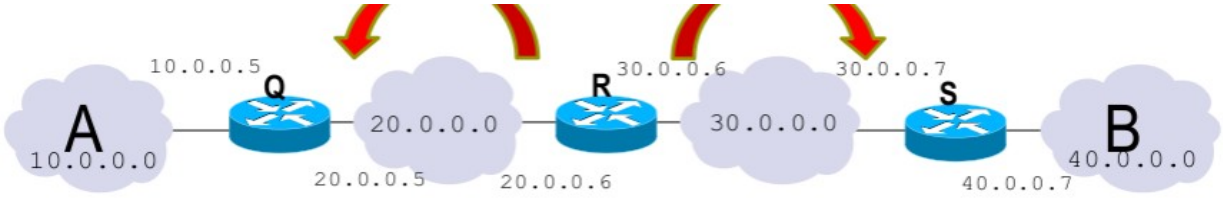
### Entrega directa

Transmisión del datagrama desde una máquina a través de una sola red física. Esto no involucra ruteadores, el transmisor encapsula el datagrama dentro de una trama física, transforma la dirección IP de destino en una dirección física de hardware y envía la trama resultante a ese destino.
Para saber si el destino esta conectado a la misma red que el transmisor, éste extrae la parte de red de su dirección IP y la compara esa misma porción de la IP la del destino, si son iguales quiere decir que están en la misma red.

### Entrega indirecta

El transmisor debe identificar un ruteador para enviar el datagrama. Éste debe encaminar el datagrama hacia la red de destino. El transmisor encapsula el

datagrama y lo envía hacia el ruteador más cercano, este lo recibe, lo extrae y el software IP elige el próximo ruteador a lo largo del camino hacia el destino.
¿Cómo elige el ruteador a donde enviar cada datagrama?
Esto se hace mediante tablas de ruteo IP. Estas se encuentran en cada host y ruteador, contienen información de todos los posibles destinos y cómo alcanzarlos.
Para mantener reducidas las tablas de ruteo, ocultar información y tomar decisiones de ruteo eficientes, el software de ruteo IP sólo puede guardar información sobre las direcciones de las redes de destino, no sobre las direcciones de anfitriones individuales.
Otra técnica para lograr esto es la de rutas asignadas por omision. Consiste en asignar un ruteador por omision con el objetivo de que si el software de ruteo IP no encuentra una ruta en la tabla, envían el datagrama a este ruter asignado.




R

| Para alcanzar los host de la Red (netid,0) | Entrega directa o siguiente salto |
|---|---|
| 20.0.0.0 | Directa |
| 30.0.0.0 | Directa |
| 10.0.0.0 | 20.0.0.5 |
| 40.0.0.0 | 30.0.0.7 |

Ruteo con direcciones IP

El ruteo IP no altera la trama (salvo por el TTL y Checksum). Cuando el IP ejecuta el algoritmo de ruteo y se elige una nueva dirección IP, que se conoce como dirección de salto siguiente. Esta dirección no se almacena en la trama sino que el IP pasa esta dirección y el datagrama al software de interfaz de red. Este transforma la dirección de salto siguiente en una dirección física, crea una trama usando esta dirección y el datagrama y envía este combo.

ARP (*Address Resolution Protocol*).

Las direcciones IP se asignan independientemente de la dirección física (MAC) de hardware de una máquina. Para enviar un paquete de red de redes a través de una red física desde una máquina hacia otra, el software debe transformar la dirección IP en una dirección física de hardware y utilizar esta para transmitir la trama.
Si la dirección física es más pequeña que la IP, se establece una transformación directa.
Sino, la transformación se hace de manera dinámica mediante el protocolo ARP. Cuando A se quiere comunicar con B, A transmite por difusión una solicitud ARP que contiene la dirección IP de B. Luego todas las máquinas reciben este

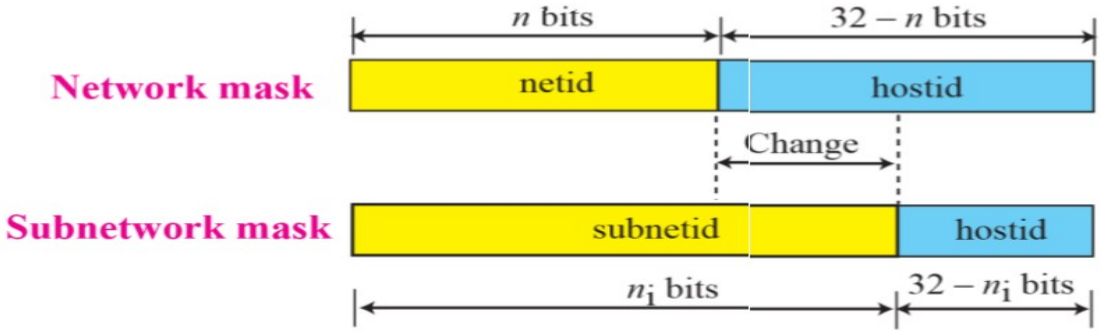
menaje pero solo B responderá a A con su dirección de hardware.
Para lograr que ARP sea eficiente, cada máquina guarda en su memoria temporal las últimas asignaciones de dirección IP a dirección física, entonces con esto se ahorra mandar muchos mensajes de difusión.

## ICMP (Internet Control Message Protocol)

Los diseñadores agregaron a los protocolos TCP/IP un mecanismo de mensajes especial, para permitir que los ruteadores en una red de redes reporten errores o proporcionen información sobre situaciones inesperadas. El protocolo de mensajes de control de internet, permite que los ruteadores o anfitriones, envíen mensajes de error o de control hacia otros ruteadores o anfitriones.
Los mensajes ICMP, viajan a través de la red de redes en la porción de datos de los datagramas IP. Al llegar al destino son recibidos por el software IP de la maquina.
Cuando un datagrama causa un error, el ICMP solo podrá reportar la condición del error a la fuente original del datagrama. Pero será ella quien deberá reaccionar al error y buscarle una solución.
Esto es porque los datagramas sólo contienen campos que especifican la fuente y el destino, no lleva un registro completo de su viaje a través de los ruteadores.

## Extensión de direcciones: Subredes

Como solución paliativa al problema del crecimiento y la necesidad de más direcciones IPv4, se empezaron a crear las subredes.
Esto consiste en "robar" algunos bits de la parte de host de una red para crear una subred.




Subredes clase B:

| $2^N-2$ | Redes | Mascara Binario | Máscara Decimal |
|---|---|---|---|
| $2^2-2$ | 2 | 11111111 . 11111111 . 11000000 . 00000000 | 255 . 255 . 192 . 0 |
| $2^3-2$ | 6 | 11111111 . 11111111 . 11100000 . 00000000 | 255 . 255 . 224 . 0 |
| $2^4-2$ | 14 | 11111111 . 11111111 . 11110000 . 00000000 | 255 . 255 . 240 . 0 |
| $2^5-2$ | 30 | 11111111 . 11111111 . 11111000 . 00000000 | 255 . 255 . 248 . 0 |
| $2^6-2$ | 62 | 11111111 . 11111111 . 11111100 . 00000000 | 255 . 255 . 252 . 0 |
| $2^7-2$ | 126 | 11111111 . 11111111 . 11111110 . 00000000 | 255 . 255 . 254 . 0 |
| $2^8-2$ | 254 | 11111111 . 11111111 . 11111111 . 00000000 | 255 . 255 . 255 . 0 |
| $2^9-2$ | 510 | 11111111 . 11111111 . 11111111 . 10000000 | 255 . 255 . 255 . 128 |
| $2^{10}-2$ | 1022 | 11111111 . 11111111 . 11111111 . 11000000 | 255 . 255 . 255 . 192 |

# Protocolo IPv6

## Origen y objetivos de diseño

En 1990 comienza el estudio del agotamiento de direcciones IPv4 de las que sólo había 2^32.
Como soluciones paliativas:

- Usaban IP temporarias asignadas en forma dinámica (DHCP).
- Se conectaba toda una red de computadoras usando una sola dirección IP (NAT+RFC 1918).

NAT

Ventajas:

- Reduce la necesidad de direcciones públicas.
- Facilita la numeración interna de las redes.
- Oculta la topología de la red.
- Sólo permite la entrada de paquetes generados en respuesta a un pedido de la red.

Desventajas:

- Rompe con el modelo end-to-end de Internet.
- Dificulta el funcionamiento de una serie de aplicaciones.
- No es escalable.
- Aumento del procesamiento de el dispositivo traductor.
- Imposibilidad de rastrear el camino del paquete.
- Imposibilita el uso de seguridad como IPSec.

Los objetivos al diseñar IPv6 fueron:

- Datagrama eficiente: Base + Extensión.
- Mayor número de direcciones: ahora habrá disponibles 2^128 direcciones IPv6
- Fragmentación en origen/destino.
- Compatibilidad con IPv4.
- Seguridad incorporada.

## Datagrama y Cabeceras

### Cabeceras Base

Comparación de cabeceras base:

| IPv4 (20 bytes + opcional) | IPv6 (40 bytes) |
|---|---|
| Versión | Igual |
| Internet Header Length | Removido, pues la longitud es fija de 40 bytes. |
| Type of service | Reemplazado por Traffic class. |
| Total length | Reemplazado, por Payload length. |
| Identification Fragmentation Flags/Fragment Offset | Removido, pues la x de fragmentación esta en la cabecera de Fragmentación. |

| | |
|---|---|
| Time to live | Reemplazado por Hop Limit |
| Protocol | Reemplazado por Next Header |
| Header Checksum | Removido, puesto que la detección bit-level error es realizada en el paquete completo por la capa de enlace. |
| Source Address 32 bits | Incrementado en 128 bits = 16 byes |
| Destination Address 32 bits | Incrementado en 128 bits = 16 byes |
| Options | Reemplazado por cabeceras de extensión. |

- Versión (4 bits) - Identifica la versión del protocolo IP utilizado.
- Clase de Tráfico (8 bits) - Identifica y diferencia los paquetes por clases de servicios o prioridad. Este continúa ofreciendo las mismas funcionalidades y definiciones del campo Tipo de Servicio de IPv4.
- Identificador de Flujo (20 bits) - Identifica y diferencia paquetes del mismo flujo en la capa de red. Este campo permite que el router identifique el tipo de flujo de cada paquete, sin necesidad de verificar su aplicación.
- Tamaño de los Datos (16 bits) - Indica el tamaño, en bytes, solamente de los datos enviados junto con el encabezado de IPv6. Reemplaza al campo "Tamaño Total" usado en IPv4, que indica el tamaño del encabezado más el tamaño de los datos transmitidos. En el cálculo del tamaño también se incluyen los encabezados de extensión.
- Siguiente Encabezado (8 bits) - Identifica el encabezado que sigue al encabezado de IPv6. El nombre de este campo fue modificado (en IPv4 se llamaba Protocolo) para reflejar la nueva organización de los paquetes IPv6, ya que ahora este campo no solo contiene valores referentes a otros protocolos sino que también indica los valores de los encabezados de extensión. Por ejemplo, el valor 58 indica que el paquete es un paquete ICMPv6.
- Límite de Encaminamiento (8 bits) - Indica el número máximo de routers que el paquete IPv6 puede pasar antes de ser descartado; se decrementa en cada salto. Estandarizó el modo en que se utilizaba el campo Tiempo de Vida (TTL) de IPv4, a pesar de la definición original del campo TTL, diciendo que éste debe indicar, en segundos, el tiempo que el paquete demorará en ser descartado en caso de no llegar a su destino.
- Dirección de Origen (128 bits) - Indica la dirección de origen del paquete.
- Dirección de Destino (128 bits) - Indica la dirección de destino del paquete.

El datagrama en IPv6, es mas simple (pues tiene una longitud fija de 40 bytes), mas flexible (pues se le pueden agregar opcionalmente cabeceras), y mas eficiente (ya que minimiza al overhead).

| | | |
|---|---|---|
| IPv6 Headder | Extension Headers | Upper layer Protocol Data Unit |

---

Payload

Paquete IPv6

# Cabeceras de Extensión

Las cabeceras de extensión son identificadas por el next header, cada tipo puede aparecer solo una vez en el paquete, el orden es importante ya que le facilita el procesamiento a los router intermedios.

- Encabezado de Opciones Salto-por-Salto – Hop by hop (protocolo 0): Este campo es leído y procesado por cada nodo a lo largo de la trayectoria de envío, el tamaño del encabezado es de 1 byte. Contiene una o más opciones. Los primeros dos bits, codifican que hacer en caso de que el nodo no reconozca la opción:
  - 00: ignorar y continuar el procesamiento.
  - 01: descartar el paquete.
  - 10: descartar el paquete y enviar un mensaje ICMP Parameter Problem a la dirección de origen del paquete.
  - 11: descartar el paquete y enviar un mensaje ICMP Parameter Problem a la dirección origen del paquete, solamente si el destino no es una direcciona multicast.
- Encabezado de Opciones de Destino - Destination (protocolo 60): Lleva información opcional que está específicamente dirigida a la dirección de destino del paquete.
- Encabezado de Enrutamiento - Routing (protocolo 43): Puede ser usado por un nodo fuente IPv6 para forzar a un paquete para que atraviese ruteadores específicos en su trayectoria al destino. Se puede especificar una lista de ruteadores intermediarios dentro del encabezado cuando se pone en 0 el campo de Tipo de Enrutamiento. El primer salto es la dirección del header base, cuando llega a esa dirección, el router cambia la dirección destino del header base con la próxima dirección.
- Encabezado de Fragmentación (protocolo 44): En IPv6 se recomienda que el mecanismo PMTUD esté en todos los nodos. Si un nodo no soporta PMTUD y debe enviar un paquete más grande que el MTU se utiliza el Encabezado de Fragmentación. Cuando esa situación ocurre el nodo fragmenta el paquete y envía cada parte utilizando Encabezados de Fragmentación, los cuales son acumulados en el extremo receptor donde el nodo destino los reensambla para formar el paquete original.
- Encabezado de Autenticación (protocolo 51). Este se utiliza en IPSec para proveer autenticación, integridad de datos y protección ante una repetición, e incluye también protección a algunos campos del encabezado básico de IPv6. Este encabezado es conocido como AH.
- Encabezado de Carga de Seguridad Encapsulada (protocolo 50): Es usado en IPSec para proveer autenticación, integridad de datos, protección ante repetición y confidencialidad del paquete IPv6. Es conocido como ESP.

## Direccionamiento

Componentes:

- Nodo: nombre genérico que se le asigna a hosts y ruters.
- Encaminador o ruter IPv6 : Nodo que envía paquete IPv6.
- Host IPv6: nodo con al menos una dirección IPv6. Al igual que en IPv4 los hosts IPv6 no reenvían paquetes.
- Vinculo, link o enlace: Uno solo soporte contiguo de red conectado por un encaminador en cualquiera de sus extremos.
- Vecino: Nodo IPv6 que se encuentra en el mismo vinculo que el nodo local.

Las direcciones IPv6 se dividen en 8 campos de 16 bits cada uno, ejemplo:
2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1

| Dec | Hexa | Bin | Dec | Hexa | Bin |
|---|---|---|---|---|---|
| 0 | 0 | 0 0 0 0 | 8 | 8 | 1 0 0 0 |
| 1 | 1 | 0 0 0 1 | 9 | 9 | 1 0 0 1 |
| 2 | 2 | 0 0 1 0 | 10 | A | 1 0 1 0 |
| 3 | 3 | 0 0 1 1 | 11 | B | 1 0 1 1 |
| 4 | 4 | 0 1 0 0 | 12 | C | 1 1 0 0 |
| 5 | 5 | 0 1 0 1 | 13 | D | 1 1 0 1 |
| 6 | 6 | 0 1 1 0 | 14 | E | 1 1 1 0 |
| 7 | 7 | 0 1 1 1 | 15 | F | 1 1 1 1 |

## Tipos de direcciones IPv6

Una dirección IPv6 puede ser clasificada en alguno de los tres tipos creados:

Unicast: Se utilizan únicamente para identificar una interfase de un nodo IPv6. "De uno a otro".

Unicast-Global (2000::/3)

Son globalmente ruteables (equivale en IPv4 a IP publicas), su rango va desde 2000 a 3FFF.

| 001 | Global routing prefix | Subnet ID | IID |
|---|---|---|---|
| 3 | 45 | 16 | 64 |

(Bits)

Si me dan una dirección por ejemplo 2001:0DB8:0015:0000:0000:1A2F:1A2B / 48, tendré 64 – 48 = 16 → $2^{16}$ subredes.

Link-Local (FE80::/10)

Jamas se rutean, su uso esta limitado a tareas administrativas por ejemplo el

descubrimiento de vecinos. No tienen subneteo. Es generada automáticamente. Son válidas en el enlace local donde la interfaz esta conectada.

| FE80 | 0 | ID |
|---|---|---|
| 10 | 54 | 64 |

(Bits)

Unique-Local (FC00::/7): se usa para ruteos internos dentro de conjuntos de enlaces. No son ruteables en internet global.

| Pref. | L | ID Global | Subnet ID | IID |
|---|---|---|---|---|
| 7 | 1 | 40 | 16 | 64 |

(Bits)

Si L = 1 (11111101,FD00) prefijo asignado localmente.

Si L = 0 (FC00) prefijo asignado por IANA.

Direcciones de una interfaz: loopback, link-local, unique-local, autoconfigurada IPv4 compatible, multicast, global.

IID (Identificador de interfaz)

Estos deben ser únicos dentro del mismo prefijo de subred. El mismo IID puede usarse en múltiples interfaces de un mismo nodo si están en subredes distintas. Normalmente el IID se genera manualmente, o basado en la MAC (EUI-64).

- Si la MAC es de 64 bits (EUI-64):

- Si la MAC es de 48 bits (IEEE 802)
  - Agregar FF-FE en el medio (3er o 4to byte)
  - Cambiar el IID: bit U/L

Anycast: Se asigna a múltiples interfases (usualmente en múltiples nodos). " De uno a alguno". Son asignadas a partir de direcciones unicast (igual sintaxis).

Se utilizan para descubrir servicios de la red, balanceo de carga, localizar routers que proveen acceso a una determinada subred.

Un paquete enviado a esta dirección es entregado al router más próximo al origen dentro de la misma subred.

Todos los routers deben aceptar la dirección *Anycast Subnet-Router* formada por:

Prefijo de la subred + IID=0 Ej: 2001:DB8:CAFE:DAD0::/64

Multicast (FF00::/8) : Se utiliza para identificar a un grupo de interfases IPv6. "De uno a todos los del grupo".

Identifica un grupo de interfaces. El soporte *multicast* es obligatorio en todos los nodos de IPv6. La dirección *multicast* deriva del bloque FE00::/8.

Prefijo FF + 4 bits de flags + 4 bits que definen el alcance de la dirección *multicast* + 112 bits para identificar el grupo *multicast*:

| 11111111 | Flgs | Scop | Group ID |
|---|---|---|---|
| 8 | 4 | 4 | 112 |

(bits)

Multicast Solicited Node: todos los nodos deben formar parte de este grupo. La dirección se forma agregando el prefijo FF02::1:FF00:0000/104 a los 24 bits mas a la derecha de IID. Ejemplo: 2037::1:800:20**0E:8C6C** -----> FF02::1::FF0E:8C6C

## ICMPv6

Internet Control Message Protocol, sus funciones son (mismas que en IPv4 pero no compatibles): informar características de la red,realizar diagnósticos, informar errores en el procesamiento de paquetes.

Se debe implementar en todos los nodos. Se encuentra luego del encabezado base y extensión (si los hay). Es identificado por *next header* = 58.

Funciones en IPv6: gestión de grupos *multicast*, descubrimiento de vecinos, descubrimiento de la Path MTU.

Variedades en tipos de mensajes ICMPv6:

| | | |
|---|---|---|
| 1 | Destination Unreachable | Fallas en la entrega del paquete o problemas en la comunicación |
| 2 | Packet too big | El tamaño del paquete es mayor a la MTU de un enlace |
| 128 | Echo Request | Utilizados por el comando ping |
| 129 | Echo Reply | Utilizados por el comando ping |
| 133 | Router Solicitation | Utilizados por el protocolo de descubrimiento de vecinos |
| 134 | Router Advertisement | Utilizados por el protocolo de descubrimiento de vecinos |
| 135 | Neighbor Solicitation | Utilizados por el protocolo de descubrimiento de vecinos |
| 136 | Neighbor Advertisement | Utilizados por el protocolo de descubrimiento de vecinos |

## Descubrimiento de vecinos

Está basado en mensajes ICMPv6. Provee en IPv6 lo que ARP y DHCP proveen en IPv4.

Se utiliza principalmete para:

- A - Determinar la MAC de los nodos de la red
- B - Encontrar ruters vecinos.
- C - Autoconfiguracion de direcciones.

A)

1. El Host 1 envía un NS: Quien tiene la dirección IPv6 2001:db8::1?

2. El Host 2 responde con una NA: Yo teng o la dirección 2001:db8::1, y la MAC address correspondiente es 06:09:12:cf:db:55.

3. El Host 1 "cachea" la informacíón recibida y ahora podra enviar paquetes al host 2

B) Los nodos IPv6 hacen esto para encontrar routers que estan en su mismo enlace. Los nodos envian mensajes RS cuando se conectan a la red, o los routers periodicamente mandan RA. Ambos se mandan con una direccion multicast a todos los nodos de la red.

C) Es el mecanismo seguido por un host para autoconfigurar interfaces IPv6. A grandes rasgos, funciona así:

1. Se genera una direccion link-local.
2. Esta direccion pasa a formar parte de los grupos multicast-all-nodes y all nodes.
3. Se verifica que esta sea unica.
4. Si la direccion esta OK, el host envia un mensaje de RS al grupo multicast-all-routers.
5. Todos los routers del enlace responden con un RA, informando prefijos, MTU, etc...

## Path MTU Discovery (PMTUD)

Busca garantizar mandar el paquete con el mayor tamaño posible. Todos los nodos IPv6 deben soportar PMTUD. La fragmentación de paquetes en caso de IPv6 se produce en el origen. En IPv4 se producía en los ruters.

Discovery process: Manda un mensaje al destino con tu MTU, si recibo un mensaje de error entonces mandame cual es tu MTU. Y así hasta que me quede el camino libre para mandar el paquete.

## Calidad de servicio

Aquí dos campos son importantes: Traffic class y Flow Label.

Hay tres modelos de calidad de servicio:

- Best Effort: Todos los paquetes son tratados igual y no provee calidad de tráfico.
- Integrates services (IntServ): El usuario solicita de antemano los recursos que necesita; cada router del trayecto ha de tomar nota y efectuar la reserva solicitada. Este metodo es complejo y hace reserva en cada router por cada flujo. Además tampoco es escalable.
- Differentiated Services (DiffServ): El usuario marca los paquetes con una determinada etiqueta que marca la prioridad y el trato que deben recibir por parte de los routers; estos no son conscientes de los flujos activos.

## Coexistencia y transición

Transición de IPv4 a IPv6

- IP capa dual: los ruters y los host soporta IPv4 e IPv6.
- Túneles de IPv6 sobre IPv4: los paquetes IPv6 se encapsulan con encabezados IPv4.

Estas técnicas de transición se dividen en 3 categorías:

- Doble pila: provee soporte a ambos protocolos en el mismo dispositivo.
- Tunelización: permite el trafico de paquetes IPv6 sobre la estructura de la red IPv4.
- Traducción: Permite la comunicación entre nodos que sólo soportan IPv6 y nodos que sólo soportan IPv4.