ARP y NDP

Address Resolution Protocol

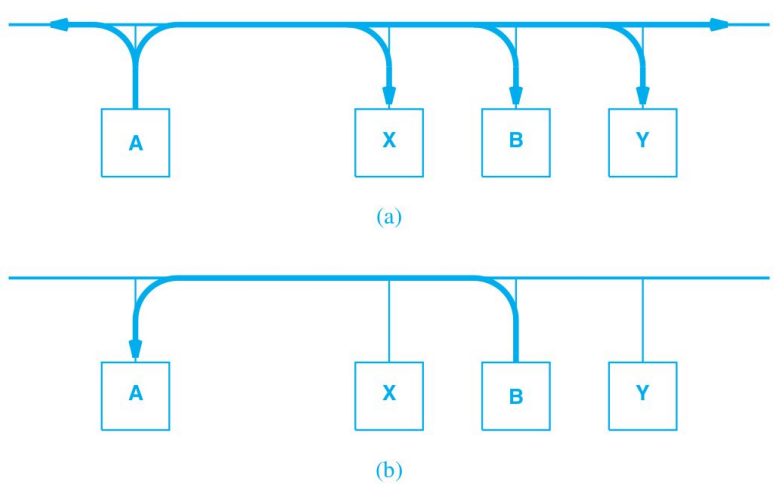
Address Resolution Protocol (ARP) para redes

Familia	Familia de protocolos de Internet
Función	Resolución de la dirección MAC de una dirección IP dada
Ubicación en la pila de protocolos	
Enlace	**ARP**
	IP, MAC
Estándares	
	RFC 826

[editar datos en Wikidata]

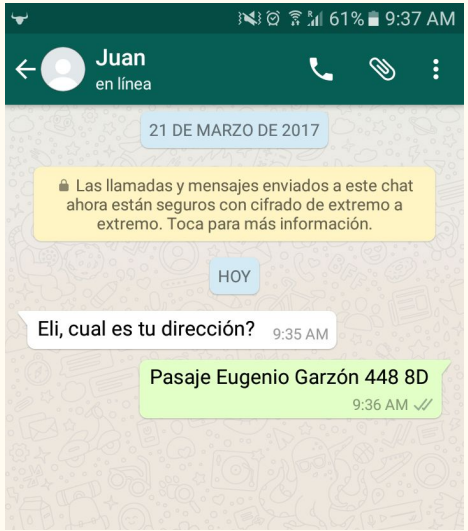
En red de computadoras, el protocolo de resolución de direcciones (ARP, del inglés Address Resolution Protocol) es un protocolo de comunicaciones de la capa de enlace, responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

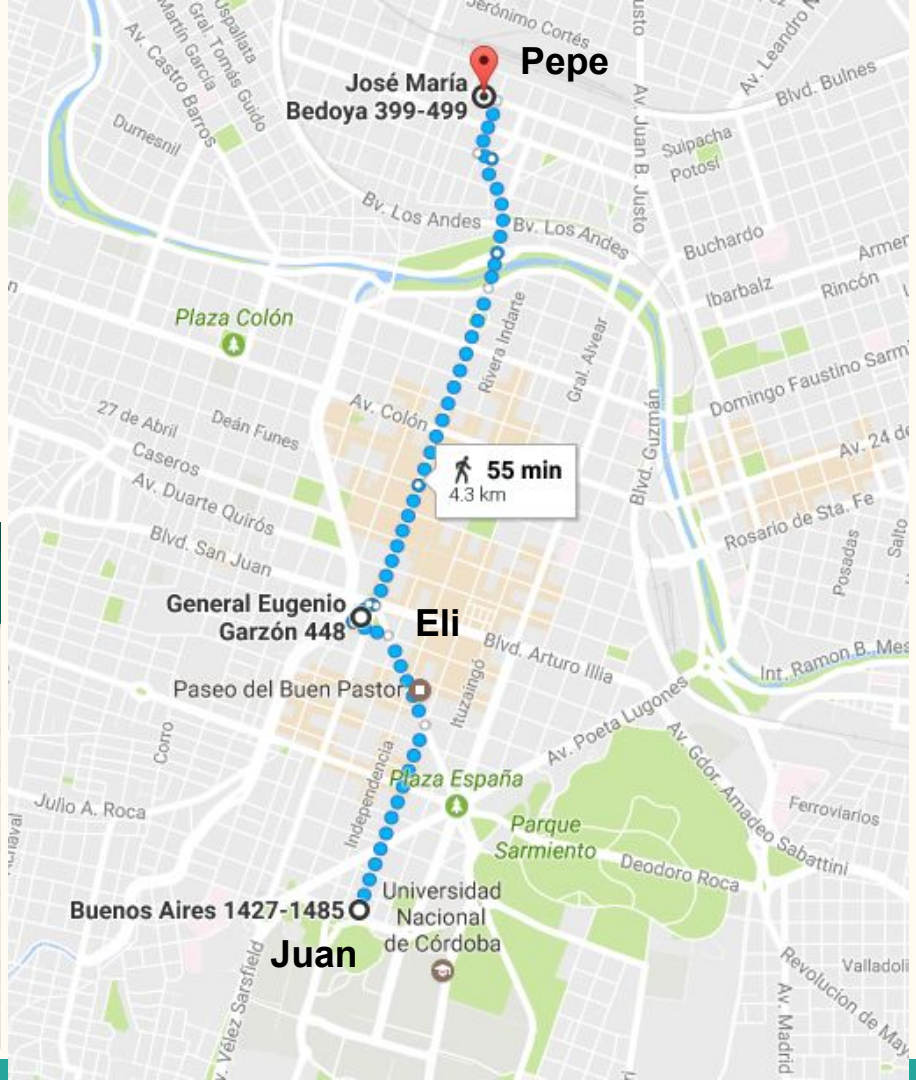
¿Por qué no alcanza con la IP?

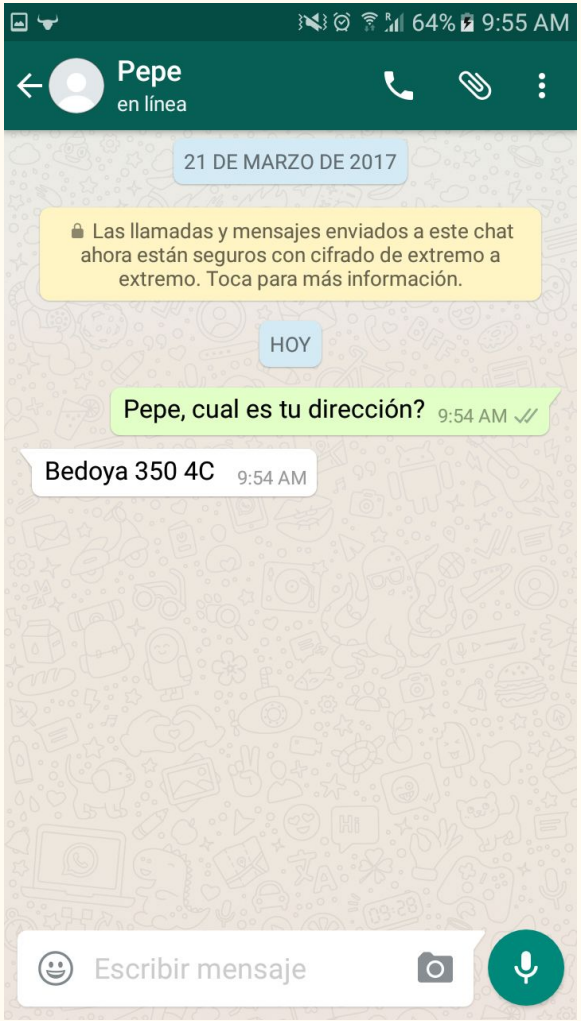


una analogía:

- Juan, Eli y Pepe están estudiando para el coloquio de Redes.
- Juan necesita darle un apunte a Pepe.
- Decide entregarselo a través de Eli.
- Nadie sabe la dirección del otro.







- Eli averigua la dirección de Pepe y le entrega el apunte de Juan.
- ¿Juan sabe la dirección de Pepe? ¿Pepe sabe la dirección de Juan?

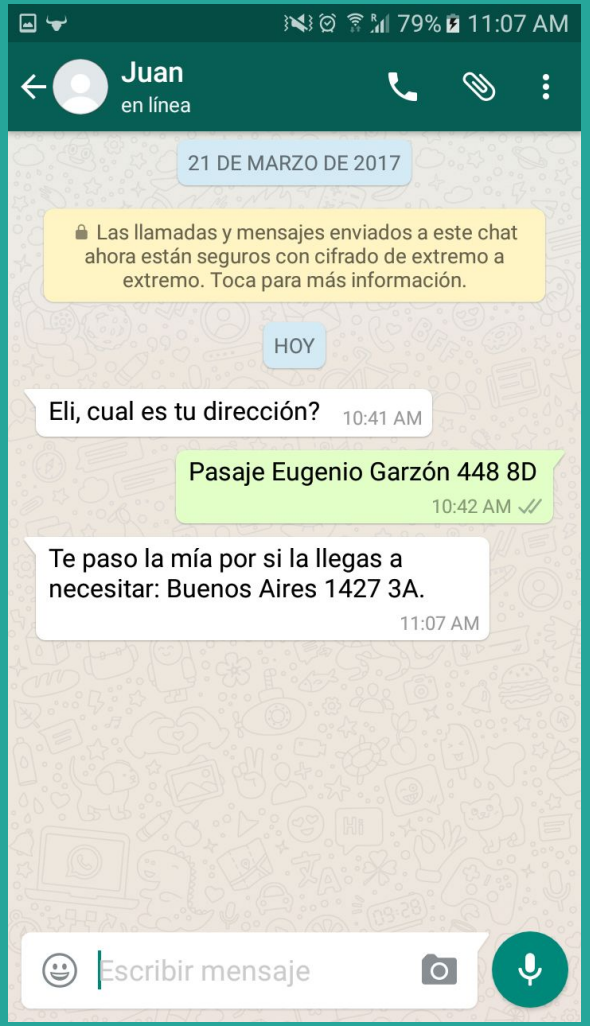
- ¿Es suficiente saber el nombre de la persona para entregar el apunte?

Persona	conoce dirección de:
Juan	Eli
Eli	Pepe
Pepe	-

Conclusión: Solamente cuando una persona necesita tener un trato directo con la otra persona, averigua su dirección. Si no, no le interesa.

Los integrantes de las redes saben que la comunicación es bidireccional - cuando surge la pregunta, ambos comparten su dirección.

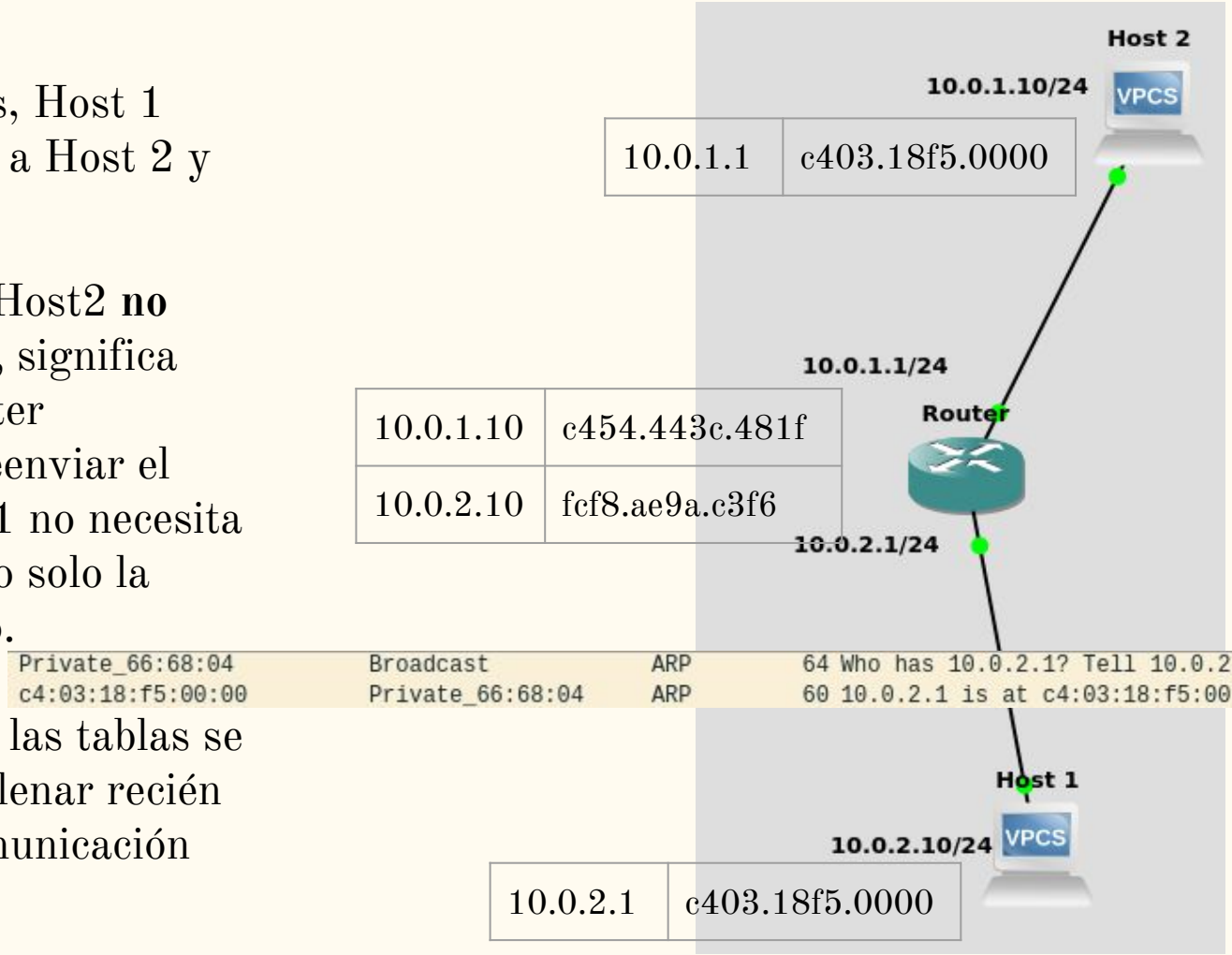
Persona	conoce dirección de:
Juan	Eli
Eli	Pepe, Juan
Pepe	Eli



Las tablas están vacías, Host 1 quiere mandar un ping a Host 2 y recibir el eco:

El hecho que Host1 y Host2 **no están en la misma red,** significa que se requiere un router (intermediario) para reenviar el ping, por lo cual Host 1 no necesita la MAC del Host 2 sino solo la MAC del intermediario.

Después de un tiempo, las tablas se vacían y se vuelven a llenar recién cuando se requiere comunicación entre los dispositivos.



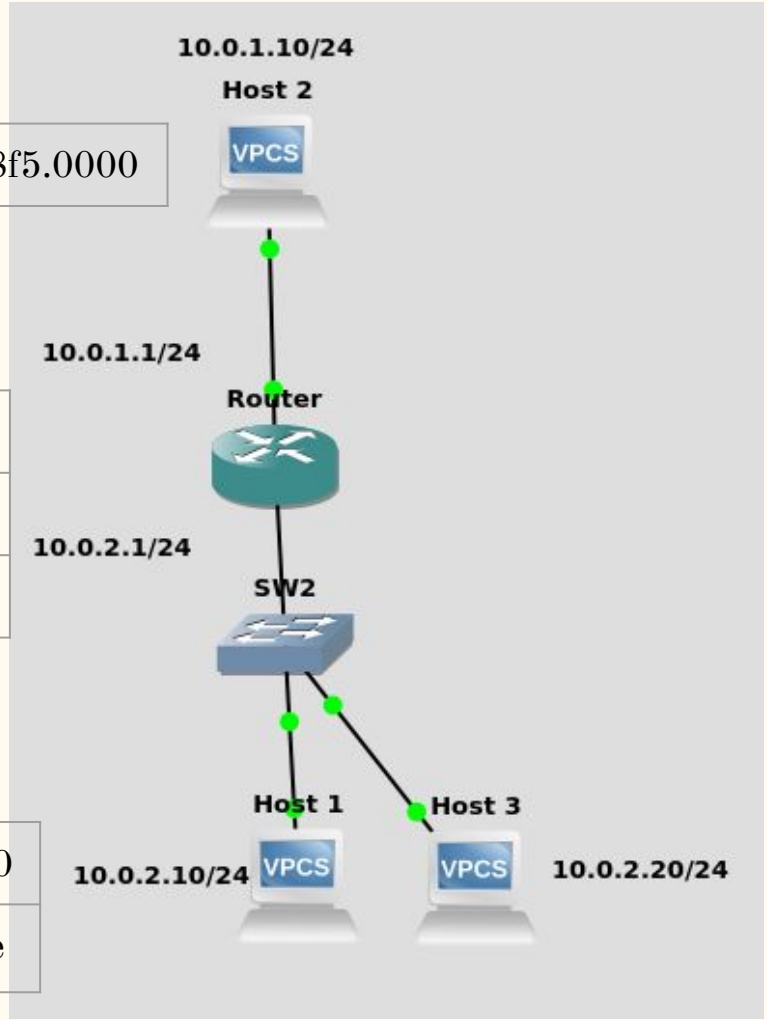
Dependiendo de marca y modelo del router, cada interfaz puede tener su propia MAC, ó la MAC puede ser única por equipo.

Mientras la MAC sea única en el dominio de broadcast, eso no tiene mucha importancia.

10.0.1.1	c403.18f5.0000

10.0.1.10	c454.443c.481f
10.0.2.10	fcf8.ae9a.c3f6
10.0.2.20	14da.e9c7.4a6e

10.0.2.1	c403.18f5.0000
10.0.2.20	14da.e9c7.4a6e



NDP

Neighbor discovery protocol

Funcionalidades

- Autoconfiguración de Nodos
- Descubrimiento de enrutadores y otros hosts en la red
- Detección de direcciones duplicadas
- Encontrar servidores DNS
- Controlar la alcanzabilidad de los hosts y routers de la red
- Mapear direcciones IP con direcciones MAC (equivalente de ARP)

Mensajes empleados por NDP

1. Neighbor Solicitation: Se envía cuando se inicia la interfaz de red para poder obtener información sobre vecinos.
2. Neighbor Advertisement: Se envía como respuesta a la solicitud de vecinos.
3. Router Solicitation: Se envía cuando se inicia la interfaz de red para poder obtener información sobre vecinos.
4. Router Advertisement: Se envía como respuesta a la solicitud de vecinos y periódicamente para asegurar que el router está alcanzable.
5. Redirect: Se envía a un host para informar un next-hop más eficiente.

Link local address (dirección de enlace local)

- tiene el formato FE80::/64 y los últimos bits se completan con la MAC del equipo.
- Cada interfaz tiene su dirección de enlace local automáticamente.
- NO es ruteable, solamente es alcanzable en la red local.
- Importante para máquinas virtuales ya que no tienen MAC.

Es una segunda dirección IP para cada interfaz, puede tener la MAC incluida.

- Grupo multidifusión a todos los nodos: FF02::1
- Grupo multidifusión a todos los routers: FF02::2

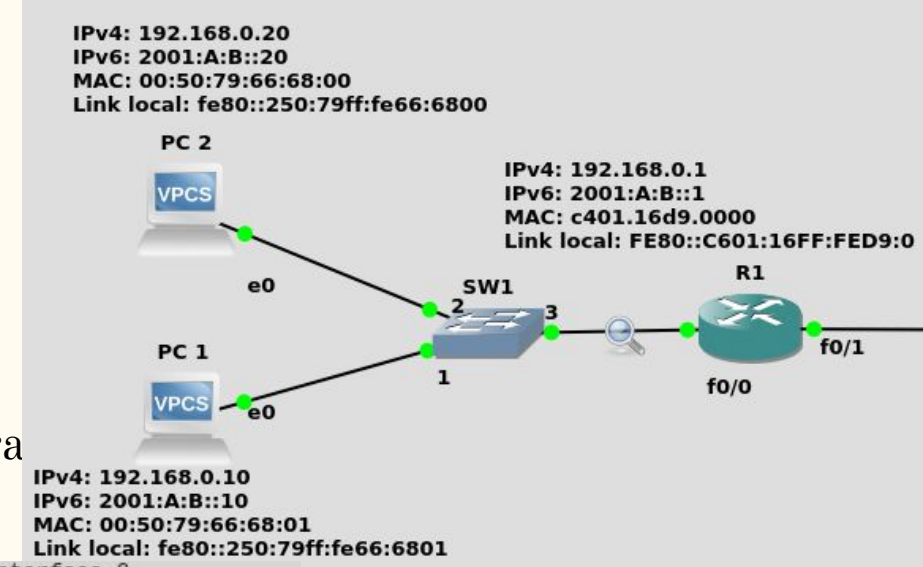
Router solicitation

Se envía para descubrir routers en la red local. (Equivalente a router discovery en ICMPv4)

<u>Capa 2:</u>

Orígen: MAC del host de origen.

Destino: MAC 33:33:00:00:00:2 multicast para routers




```
▸ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
▾ Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: IPv6mcast_02 (33:33:00:00:00:02)
  ▸ Destination: IPv6mcast_02 (33:33:00:00:00:02)
  ▸ Source: Private_66:68:01 (00:50:79:66:68:01)
    Type: IPv6 (0x86dd)
▾ Internet Protocol Version 6, Src: ::, Dst: ff02::2
    0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 8
    Next header: ICMPv6 (58)
    Hop limit: 255
    Source: ::
    Destination: ff02::2
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▸ Internet Control Message Protocol v6
```

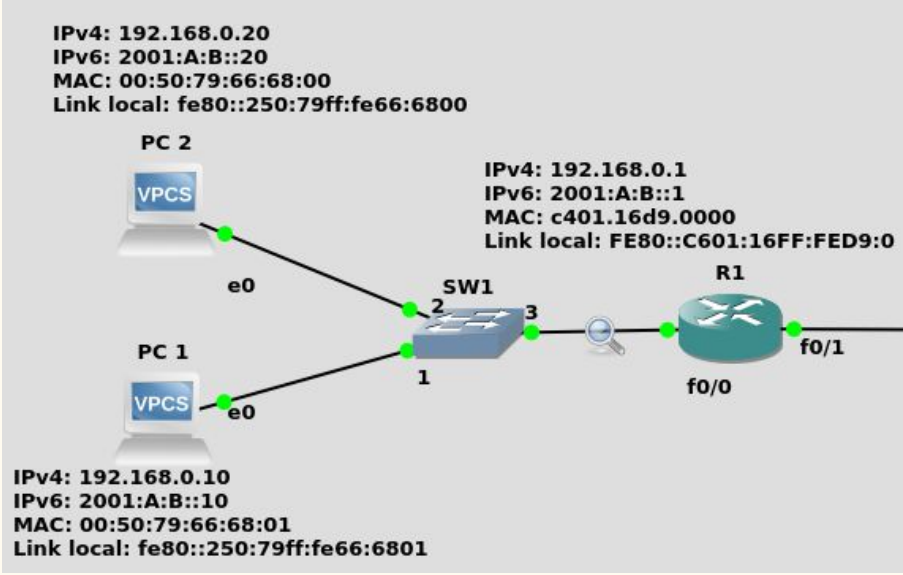
Capa 3:
orígen: IPv6, LL, ó ::
destino: ff02::2
(dirección de multidifusión para routers)

Router Advertisement

se envía pseudo-periódicamente ó como respuesta a una solicitud.

<u>capa 2</u>
Origen: MAC del router.

Destino: MAC del solicitante ó MAC multicast para todos los nodos - 33:33:00:00:00:01




```
▸ Frame 56: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
▾ Ethernet II, Src: c4:01:16:d9:00:00 (c4:01:16:d9:00:00), Dst: IPv6mcast_01 (33:33:00:00:00:01)
    ▸ Destination: IPv6mcast_01 (33:33:00:00:00:01)
    ▸ Source: c4:01:16:d9:00:00 (c4:01:16:d9:00:00)
      Type: IPv6 (0x86dd)
▸ Internet Protocol Version 6, Src: fe80::c601:16ff:fed9:0, Dst: ff02::1
▸ Internet Control Message Protocol v6
```

capa 3
origen: IPv6/LL del router

destino: IPv6/LL del solicitante ó IP multidifusión a todos los nodos.

Solicited node multicast address
(dirección multicast del nodo solicitado)

Mensajes broadcast en ARP ocupan tiempo de procesamiento a todos los hosts.

cada interfaz de red se subscribe a su propio grupo multicast. La dirección de dicho grupo se compone por ff02::1:ff00:0/104 + los últimos 24 bits de la dirección

```
fe80::2aa:ff:fe28:9c5a                      Target address (compressed notation)
fe80:0000:0000:0000:02aa:00ff:fe28:9c5a     Target address (uncompressed notation)
                                 -- ----    the last 24-bits
ff02::1:ff00:0/104                          Solicited-node Multicast Address prefix
ff02:0000:0000:0000:0000:0001:ff00:0000/104 (uncompressed)
---- ---- ---- ---- ---- ---- --           The first 104 bits
ff02:0000:0000:0000:0000:0001:ff28:9c5a     Result
ff02::1:ff28:9c5a                           Result (compressed notation)
```

es altamente probable que dicho grupo tenga un solo integrante.

```
IPv6 is enabled, link-local address is FE80::C601:16FF:FED9:0
Global unicast address(es):
  2001:A:B::1, subnet is 2001:A:B::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
  FF02::1:FFD9:0
MTU is 1500 bytes
```

Neighbor Solicitation

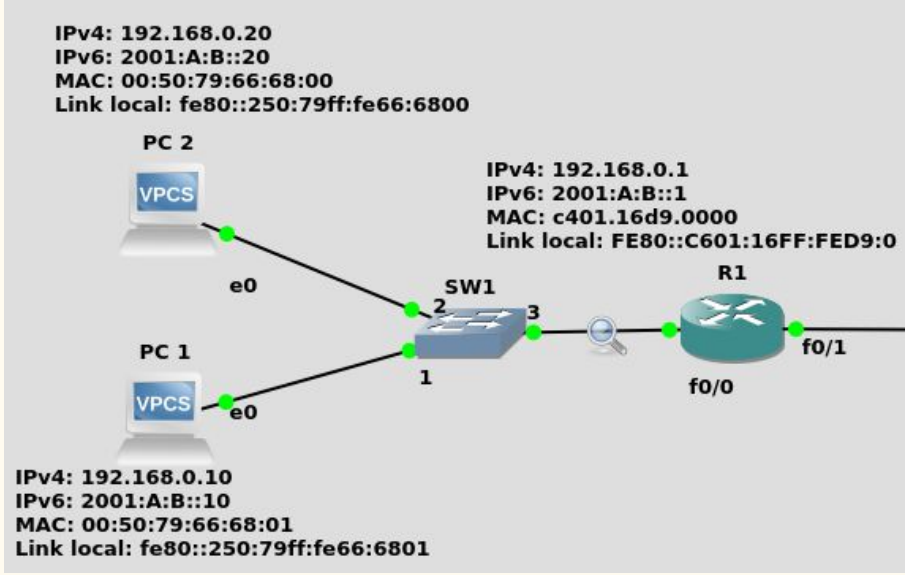
se envía para obtener una dirección MAC de un vecino ó para confirmar que éste sigue alcanzable.

<u>capa 2</u>

origen: MAC del solicitante

destino: MAC de destino en el caso de una confirmación de alcanzabilidad ó MAC multicast con *solicited node multicast address*.

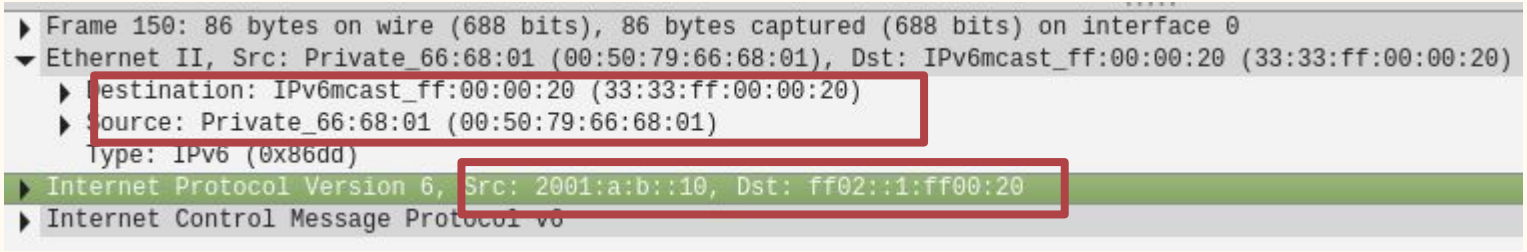
33:33:FF:xx:xx:xx (Los últimos 24 bits de la IP)



<u>capa 3</u>

origen: IPv6, LL ó :: del solicitante.

destino: IP de destino para confirmación ó s*olicited node multicast address* del destino.

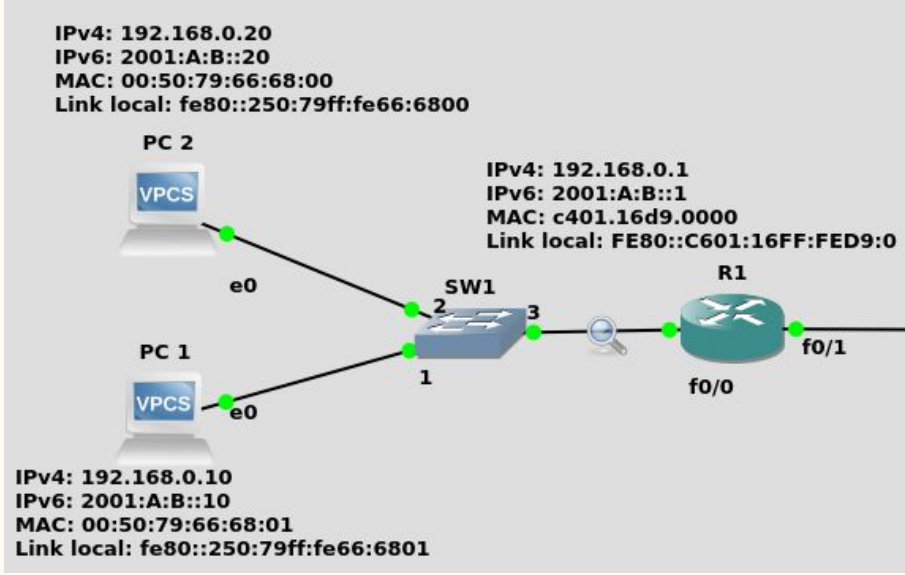


Neighbor advertisement

se envía como respuesta a la solicitud de vecinos, para informar sobre cambios de la dirección MAC ó para informar sobre cambios de estado del vecino.

<u>Capa 2</u>
origen: MAC de origen

destino: MAC del solicitante, si no fue solicitado, MAC multicast para todos los nodos.
33:33:00:00:00:01



<u>Capa 3</u>
origen: IP, LL de origen
destino: IPv6, LL del solicitante ó FF02::1

```
▸ Frame 142: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
▾ Ethernet II, Src: c4:01:16:d9:00:00 (c4:01:16:d9:00:00), Dst: IPv6mcast_01 (33:33:00:00:00:01)
    ▸ Destination: IPv6mcast_01 (33:33:00:00:00:01)
    ▸ Source: c4:01:16:d9:00:00 (c4:01:16:d9:00:00)
      Type: IPv6 (0x86dd)
▸ Internet Protocol Version 6, Src: fe80::c601:16ff:fed9:0, Dst: ff02::1
▸ Internet Control Message Protocol v6
```

???

Redirect

Se envía a un host de orígen para informarlo sobre un first hop mejor para un destino determinado.

Este tipo de mensaje se envía solamente de los routers a direcciones unicast.

ND Message	ND Options That Might Be Included
Router Solicitation	Source Link-Layer Address option: Used to inform the router of the link-layer address of the host for the unicast Router Advertisement response.
Router Advertisement	Source Link-Layer Address option: Used to inform the receiving host(s) of the link-layer address of the router.
	Prefix Information option(s): Used to inform the receiving host(s) of on-link prefixes and whether to autoconfigure stateless addresses.
	MTU option: Used to inform the receiving host(s) of the IPv6 MTU of the link.
	Advertisement Interval option: Used to inform the receiving host how often the router (the home agent) is sending unsolicited multicast router advertisements.
	Home Agent Information option: Used to advertise the home agent's preference and lifetime.
	Route Information option(s): Used to inform the receiving host(s) of specific routes to add to a local routing table.
Neighbor Solicitation	Source Link-Layer Address option: Used to inform the receiving node of the link-layer address of the sender.
Neighbor Advertisement	Target Link-Layer Address option: Used to inform the receiving node(s) of the link-layer address corresponding to the Target Address field.
Redirect	Redirected Header option: Used to include all or a portion of the packet that was redirected.
	Target Link-Layer Address option: Used to inform the receiving node(s) of the link-layer address corresponding to the Target Address field.

Bibliografia

- https://en.wikipedia.org/wiki/Address_Resolution_Protocol
- https://www.google.com.ar/maps?source=tldso
-
- https://es.wikipedia.org/wiki/Neighbor_Discovery
- https://en.wikipedia.org/wiki/Neighbor_Discovery_Protocol
- https://en.wikipedia.org/wiki/Solicited-node_multicast_address
- https://www.slideshare.net/Heba_a/i-pv6-part2nd
- http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-15-2mt-book/ip6-neighb-disc.html
- https://tools.ietf.org/html/rfc4861#section-7.2
- https://www.ietf.org/proceedings/65/slides/16ng-3/sld5.htm
- “Understanding IPv6”, third edition by Joseph Davies (http://www.advancedtechnologysupportinc.com/website/labfiles/network/understanding_ipv6_3rd_edition.pdf)