

# PROTOCOLLO ARP



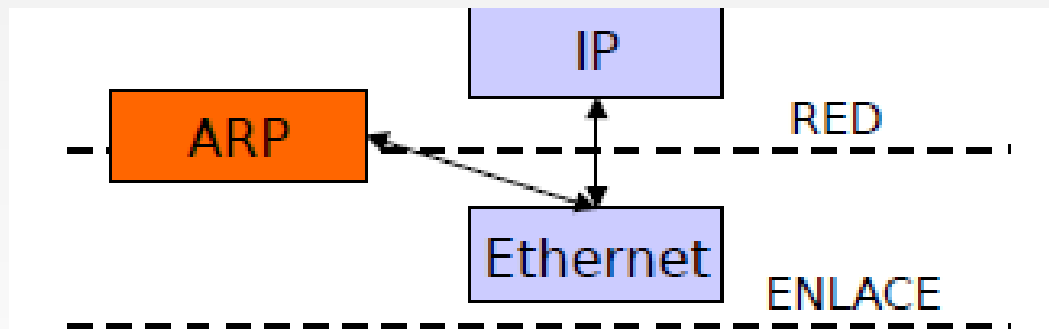
**ARP Spoofing**

# PROTOCOLO ARP

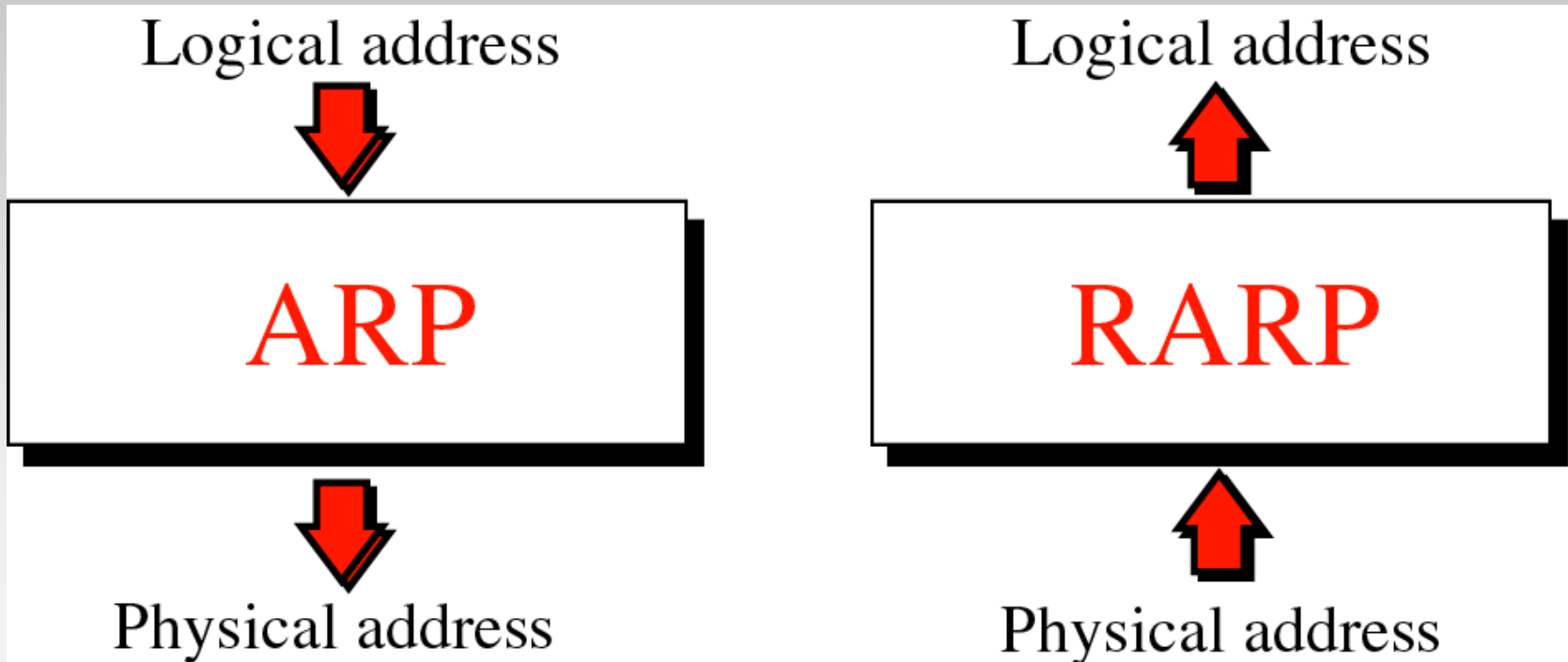
Protocolo responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast (MAC = xx xx xx xx xx)) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga.

# INTRODUCCION

- ARP (y RARP) proporcionan la correspondencia entre direcciones IP y direcciones hardware (nivel de enlace):
  - ARP: Address Resolution Protocol (RFC 826)
  - RARP: Reverse Address Resolution Protocol (RFC 903)
- ARP proporciona correspondencia dinámica.
  - Obtiene la dirección Ethernet asociada a una dirección IP.
- RARP permite obtener una dirección IP asociada a una dirección Ethernet, utilizando un servidor RARP (sustituido por DHCP).



# ARP ---- RARP



# Caché ARP

las parejas de direcciones (dirección IP, dirección MAC) se guardan en memoria por un cierto tiempo.

Existe un tiempo de validez de las entradas en esta tabla.

Transcurrido ese tiempo de validez la entrada se borra del caché y la consulta a la red, por difusión, debe repetirse.

Las entradas en la tabla se actualizan en dos instancias: cuando se recibe una difusión o cuando se recibe una pregunta por la dirección IP propia:

- Existen dos formas de almacenamiento en la cache:
  - Estático
  - Dinámico
- Puede ser vulnerable a un ataque de falsificación de paquetes ARP: ARP Spoofing.

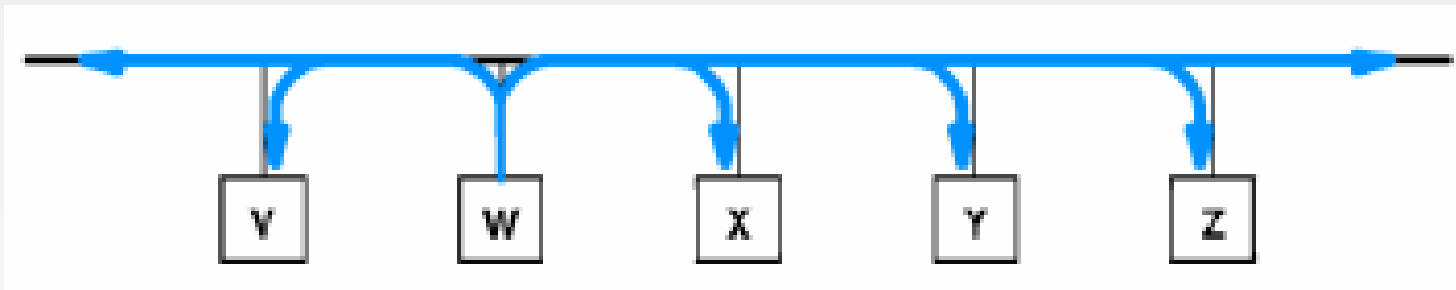
```
C:\Users\jaider>arp -a
```

Interfaz: 192.168.1.106	---	0xb		
Dirección de Internet		Dirección física		Tipo
192.168.1.1	00-1e-e5-3c-98-9e		dinámico	
192.168.1.255	ff-ff-ff-ff-ff-ff		estático	
224.0.0.2	01-00-5e-00-00-02		estático	
224.0.0.22	01-00-5e-00-00-16		estático	
224.0.0.251	01-00-5e-00-00-fb		estático	
224.0.0.252	01-00-5e-00-00-fc		estático	
239.255.255.250	01-00-5e-7f-ff-fa		estático	
239.255.255.253	01-00-5e-7f-ff-fd		estático	
255.255.255.255	ff-ff-ff-ff-ff-ff		estático	

# Gratuitous ARP – RFC 3927

Las solicitudes ARP gratuitas son empleadas por dispositivos para “**anunciar**” su dirección IP a los demás dispositivos. Los demás dispositivos de red utilizan las solicitudes ARP gratuitas para actualizar su caché ARP.

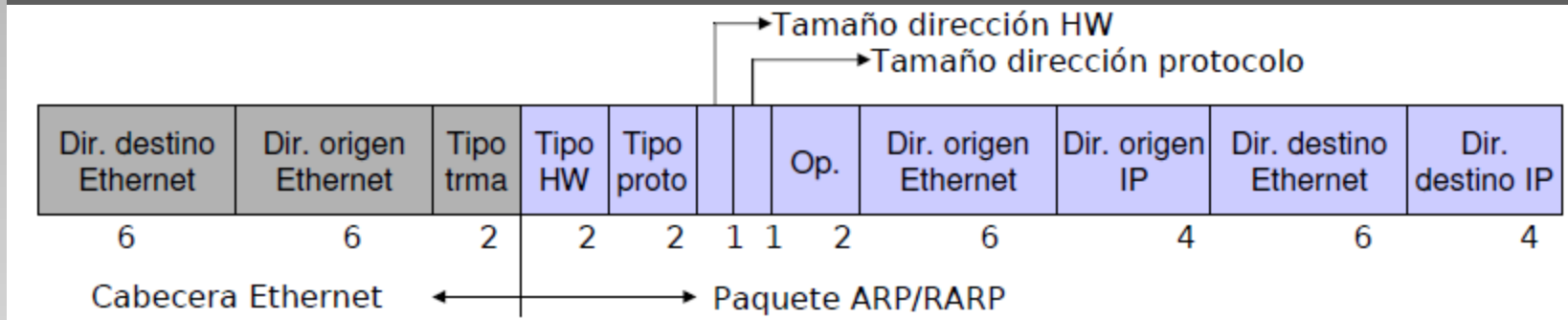
Se colocan en tramas broadcast al igual que las solicitudes ARP.



Host W: “Soy 1.2.3.4 y mi MAC es 12:34:56:78:9A:BC”

**Soy Pedro Navajas**

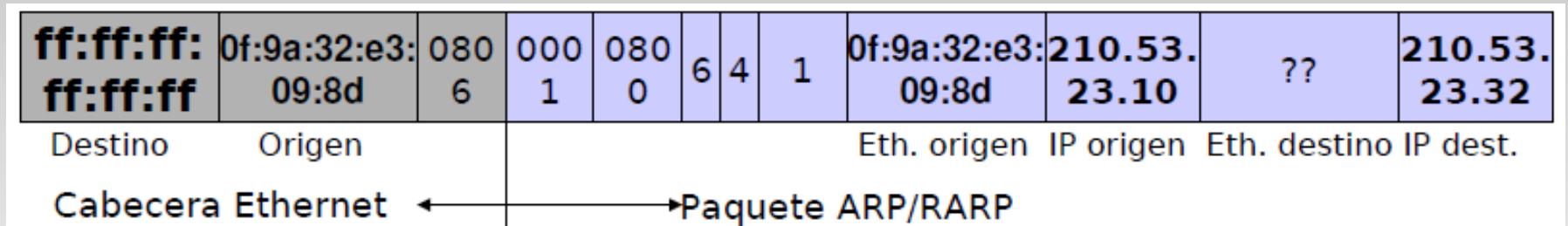
# FORMATO DE LA TRAMA ARP



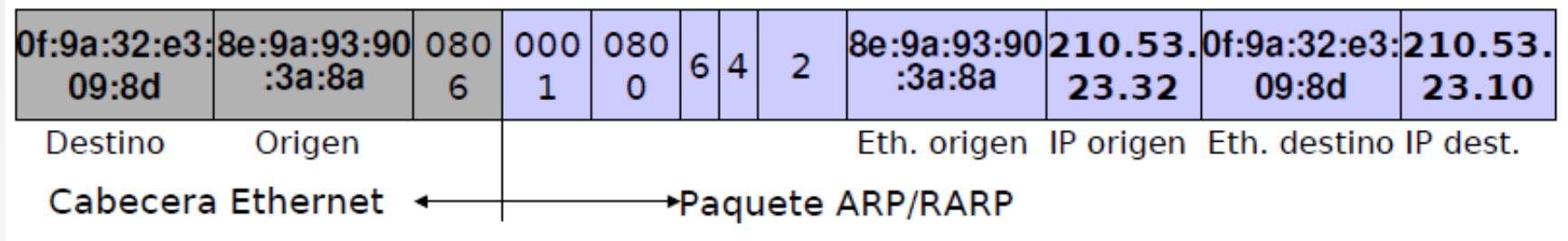
- Formato del paquete ARP y RARP para Ethernet:
- Tipo trama: ARP (0x0806) y RARP (0x8035)
- Tipo de HW: Ethernet (0x0001)
- Tipo de protocolo: IP (0x0800)
- Tamaño de direcciones: Ethernet (6 bytes), IP (4 bytes)
- Op.: Especifica el tipo de operación a realizar
  - ARP request (1) / ARP reply (2)
  - RARP request (3) / RARP reply (4)
- Direcciones Ethernet e IP de origen y destino.
  - La dirección Ethernet de origen está duplicada en el frame Ethernet, porque ya aparece en la cabecera Ethernet.
  - La dirección Ethernet de destino también se duplicará en las respuestas (en las peticiones se usa la dirección de broadcast).

# ARP: Ejemplo

## ○ ARP Request (PC1 → broadcast)

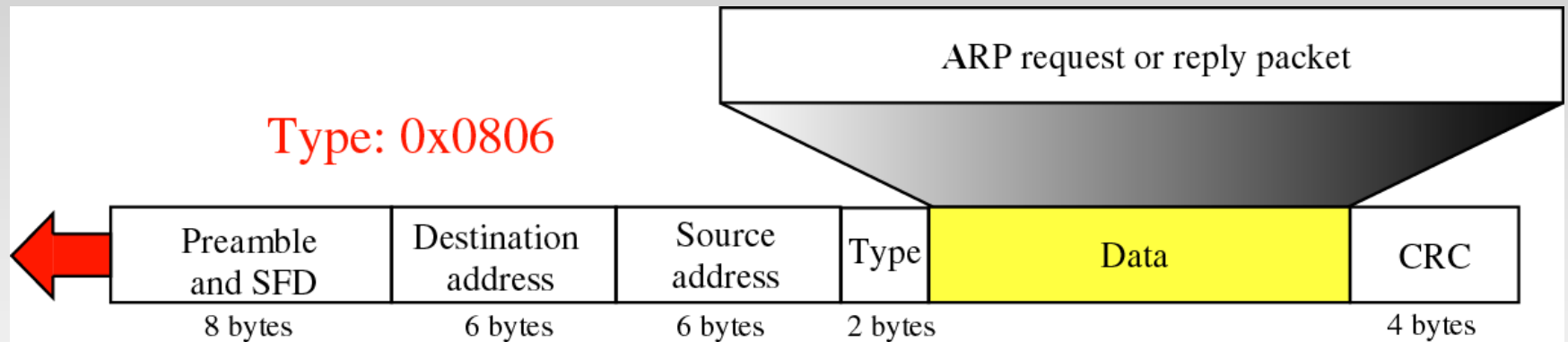


## ○ ARP Reply (PC2 → PC1)

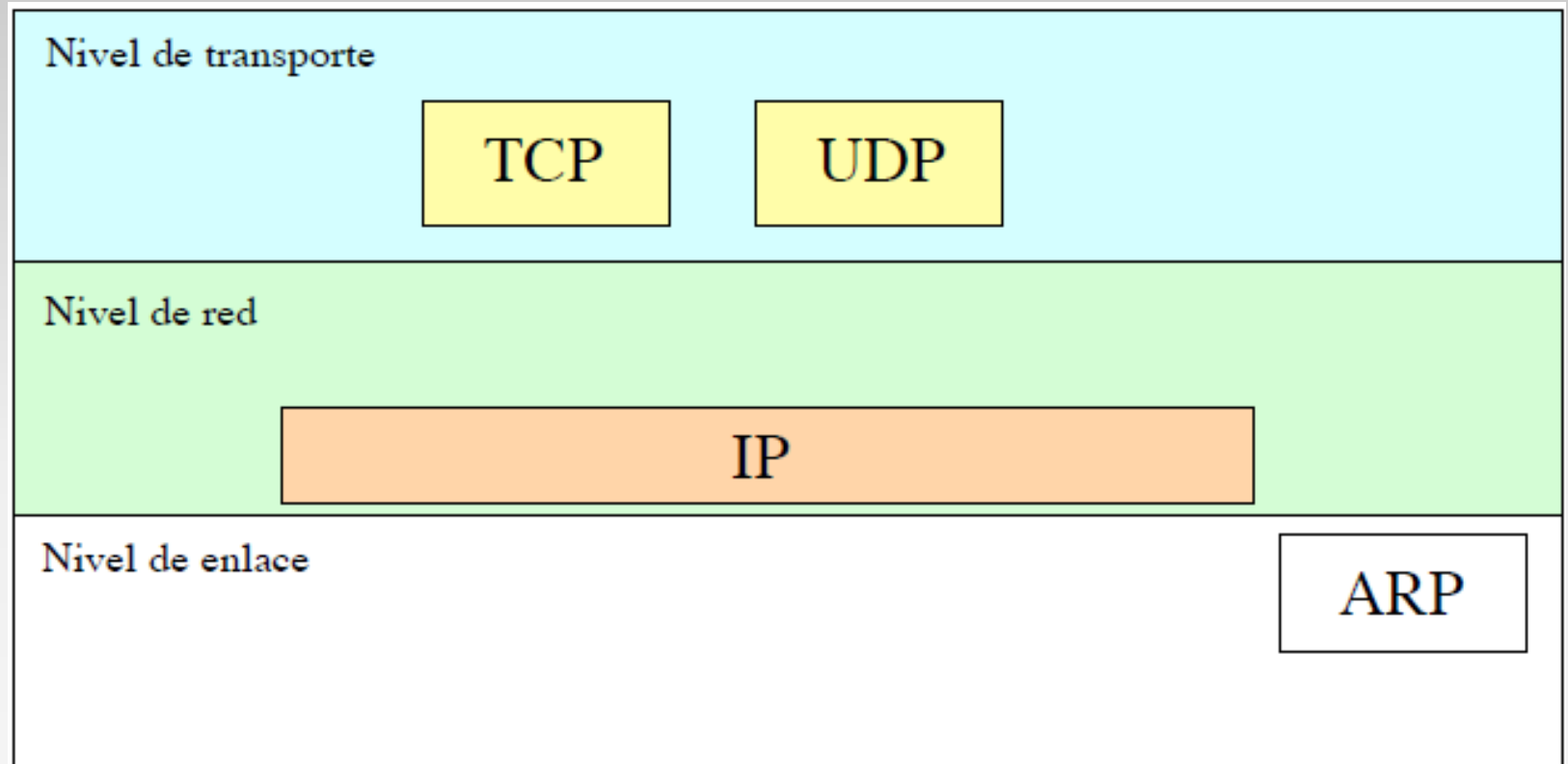




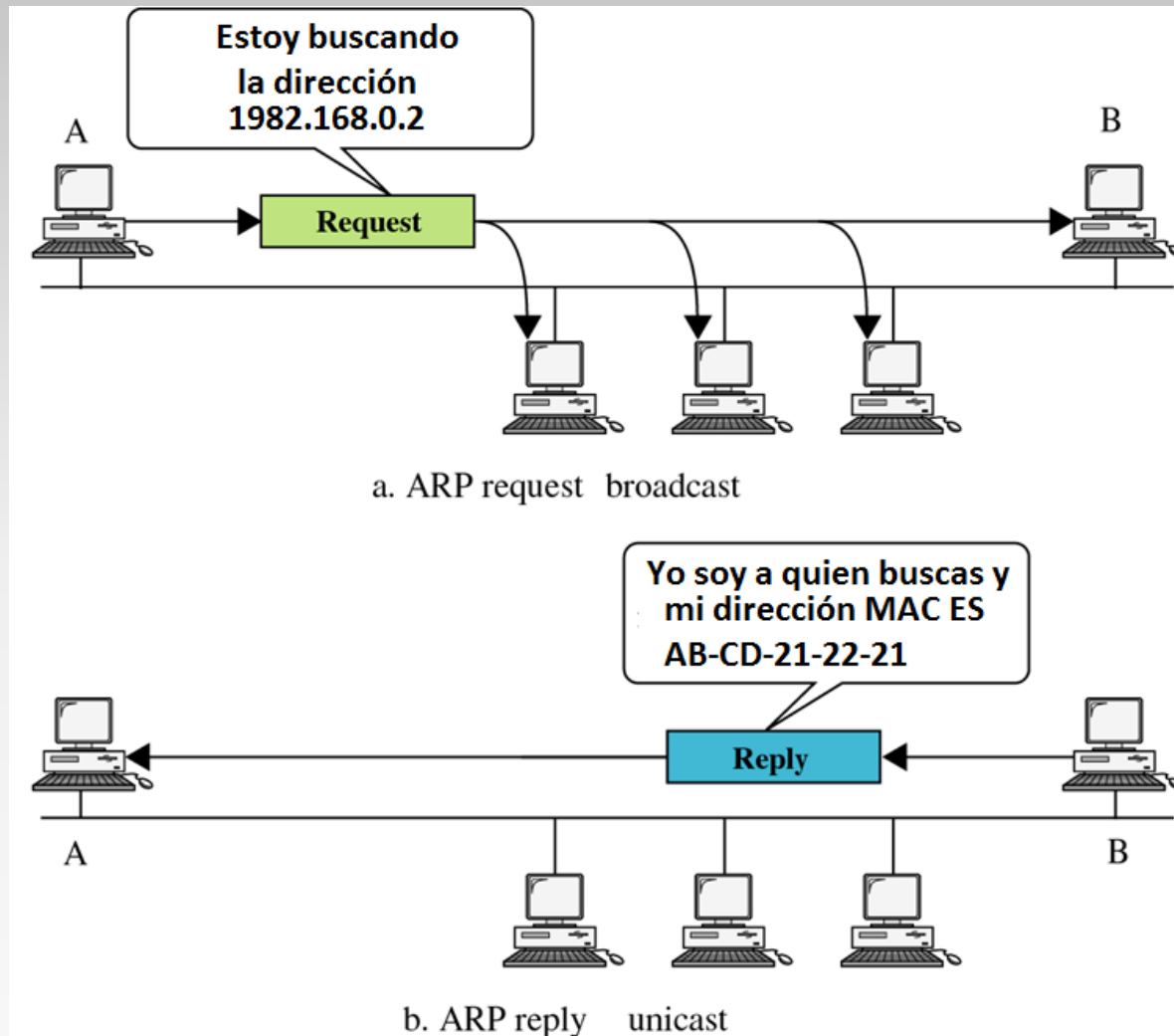
# Encapsulamiento de ARP



# ARP en la pila TCP/IP



# BUSQUEDA ARP



# Funcionamiento del ARP

**1. Obtener la dirección IP del destino.**

**2. Crear un mensaje ARP de pedido (*request*)**

Insertar la dirección física del emisor (*sender*).

Insertar la dirección IP del emisor.

Insertar la dirección IP del destino.

La dirección física del destino se llena con 0.

**3.El mensaje se pasa a la capa link donde es encapsulado en un frame.**

- Dirección fuente: dirección física del emisor.
- Dirección destino: dirección broadcast.

# Funcionamiento del ARP

**4. Cada host o router en la red recibe el frame.**

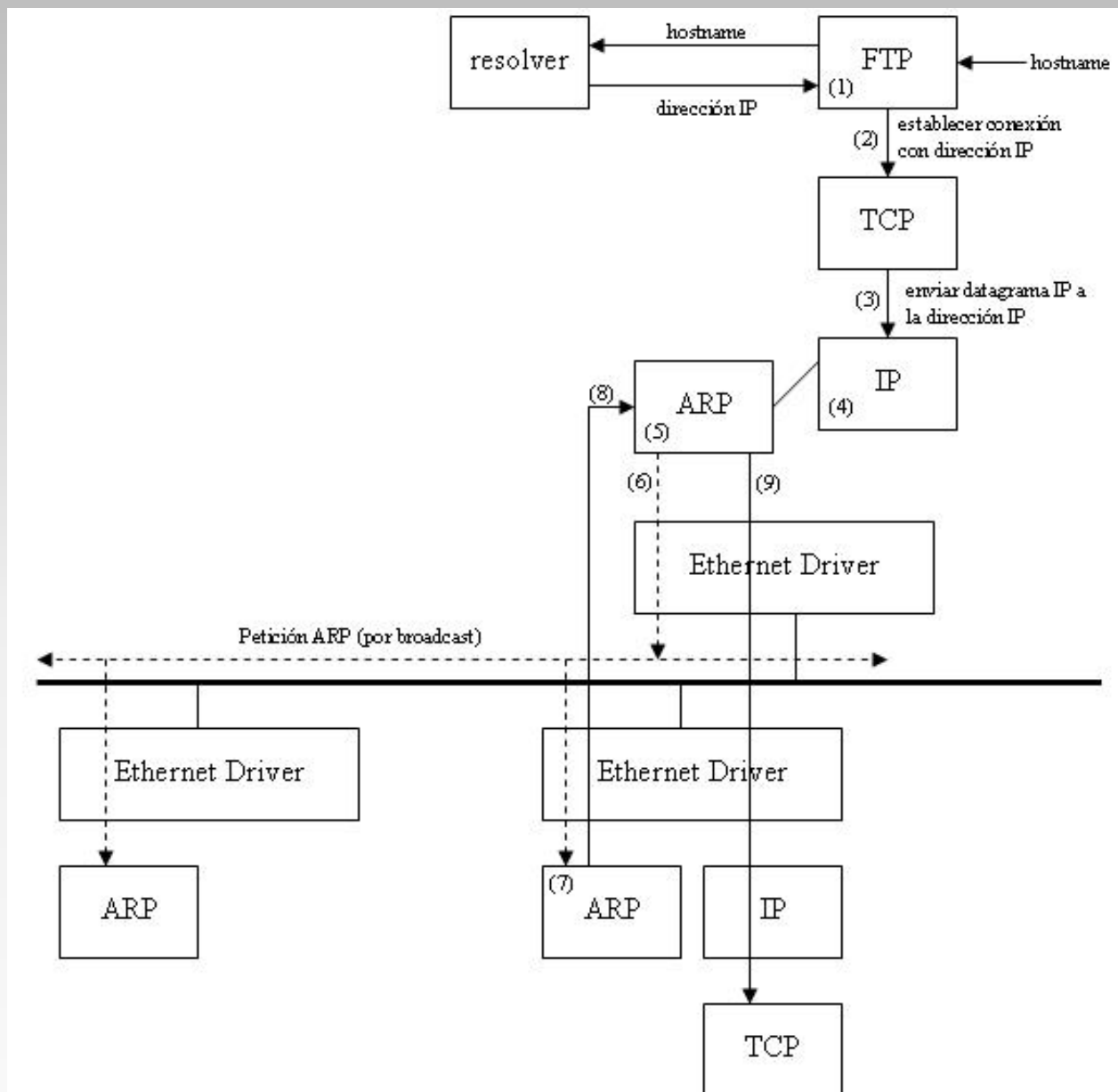
- Todos los equipos lo pasan al ARP.
- Todas las máquinas, excepto la destino, descartan el paquete.

**5. La máquina destino responde con un mensaje ARP que contiene su dirección física.**

- Mensaje unicast.

**6. El emisor recibe el mensaje de respuesta y obtiene la dirección física de la máquina destino.**

# ARP EN UN PROCESO FTP



# Puntos de taque a la caché ARP

**El protocolo ARP es *stateless***, por lo tanto la mayoría de los sistemas operativos actualizarán su cache si reciben una respuesta (*reply*), sin importar si enviaron o no un pedido (*request*).

**Ausencia absoluta de autenticación** en el protocolo. Un computador modificará su comportamiento acorde con las tramas ARP recibidas, sin poder determinar de ningún modo la autenticidad de las mismas.

# Puntos de ataque a la caché ARP

- **Cachés sujetas a alteraciones externas.** Es posible modificar los contenidos de una caché ARP tan sólo con construir y enviar una consulta o respuesta adecuada.



# Envenenamiento ARP

Este tipo de vulnerabilidad consiste en el **envenenamiento de las tablas ARP** de los host implicados.

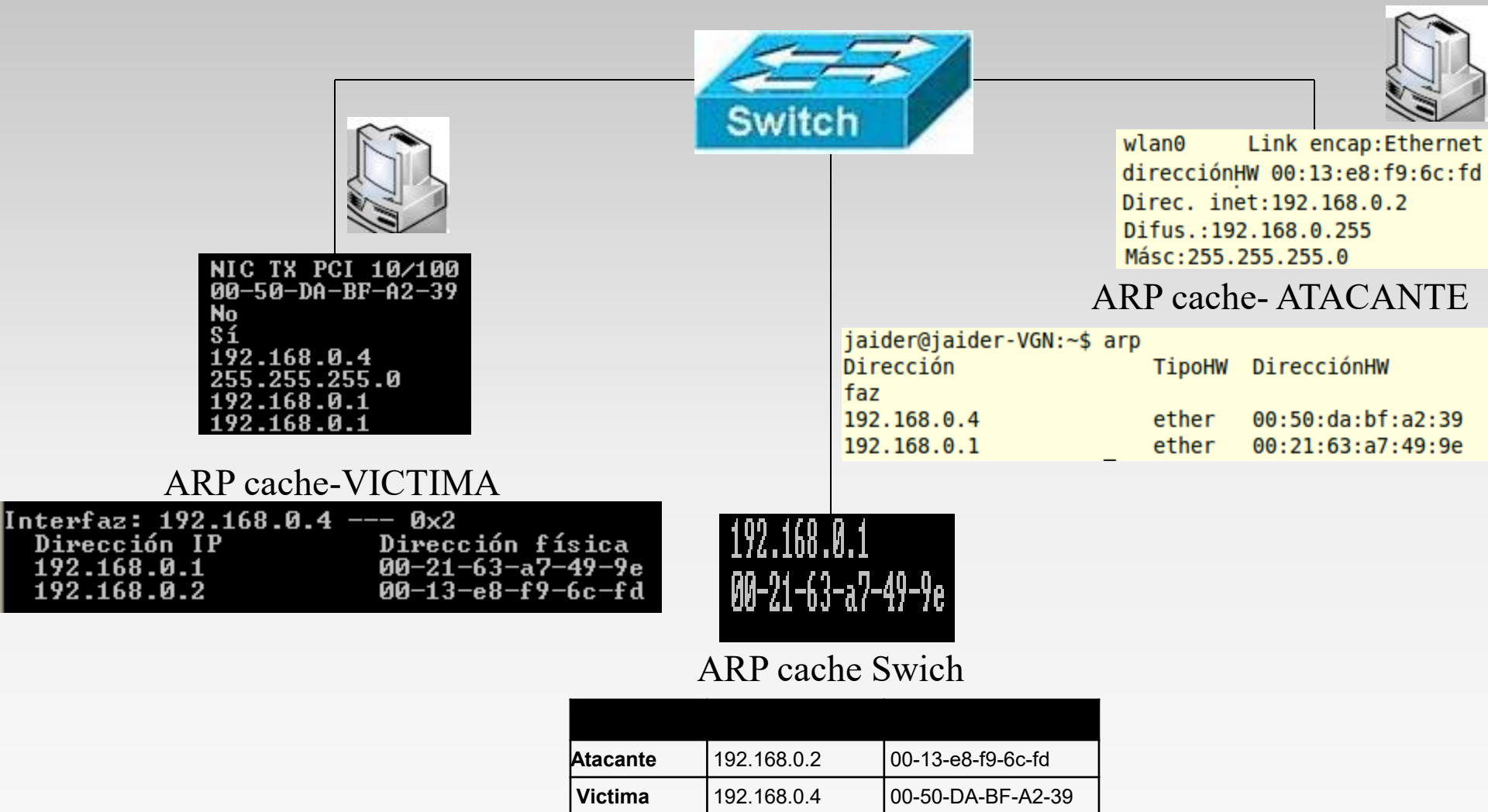
También conocido como ARP Spoofing, y falsificación ARP...

Se aprovecha de que **las tablas son dinámicas** y cambian conforme le llegan respuestas ARP, aunque no hayan pedido petición ninguna.

# Envenenamiento ARP-- ESCENARIO

- Se tiene un switch y dos host una la víctima y otra el atacante.
- El objetivo es envenenar la tabla ARP para poder llegar a situarse en medio de la comunicación entre el switch y el host víctima.
- Este método se conoce como **MITM (Man in the Middle)**.

# ESCENANARIO INICIAL



```
jaider@jaider-VGN:~$ arp -a
? (192.168.0.4) en 00:50:da:bf:a2:39 [ether] en wlan0
? (192.168.0.1) en 00:21:63:a7:49:9e [ether] en wlan0
jaider@jaider-VGN:~$ ifconfig /all
/all: error al obtener información sobre la interfaz: Dispositivo no encontrado
jaider@jaider-VGN:~$ ifconfig
lo        Link encap:Bucle local
          Direc. inet:127.0.0.1  Másc:255.0.0.0
          Dirección inet6: ::1/128 Alcance:Anfitrión
          ACTIVO BUCLE FUNCIONANDO MTU:16436 Métrica:1
          Paquetes RX:28 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:28 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:0
          Bytes RX:2048 (2.0 KB) TX bytes:2048 (2.0 KB)

wlan0     Link encap:Ethernet direcciónHW 00:13:e8:f9:6c:fd
          Direc. inet:192.168.0.2 Difus.:192.168.0.255 Másc:255.255.255.0
          Dirección inet6: fe80::213:e8ff:fef9:6cfd/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:210982 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:198594 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:223261830 (223.2 MB) TX bytes:133161167 (133.1 MB)

jaider@jaider-VGN:~$
```

## Datos de atacante Antes de ataque

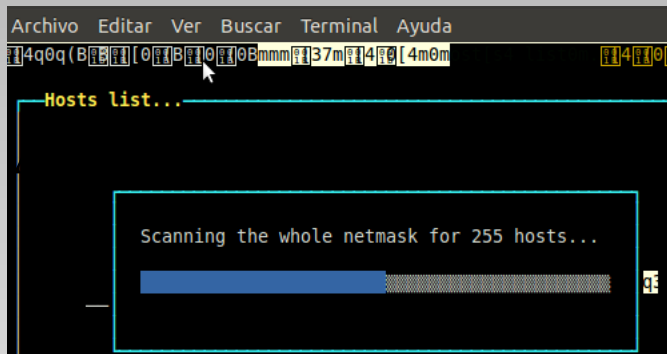
```
Adaptador Ethernet Conexión de área local 3 :
Sufijo de conexión específica DNS :
Descripción. . . . . : NIC TX PCI 10/100 de 3Com EtherLink XL (3C905B-TX) #4
Dirección física. . . . . : 00-50-DA-BF-A2-39
DHCP habilitado. . . . . : No
Autoconfiguración habilitada. . . : Sí
Dirección IP. . . . . : 192.168.0.4
Máscara de subred. . . . . : 255.255.255.0
Puerta de enlace predeterminada : 192.168.0.1
Servidor DHCP. . . . . : 192.168.0.1
Servidores DNS. . . . . : 200.75.51.132
                          200.75.51.133
Concesión obtenida. . . . . : sábado, 16 de diciembre de 2000 14:52:59
Concesión expira. . . . . : domingo, 17 de diciembre de 2000 14:52:59

C:\Documents and Settings\HILANDER>arp -a

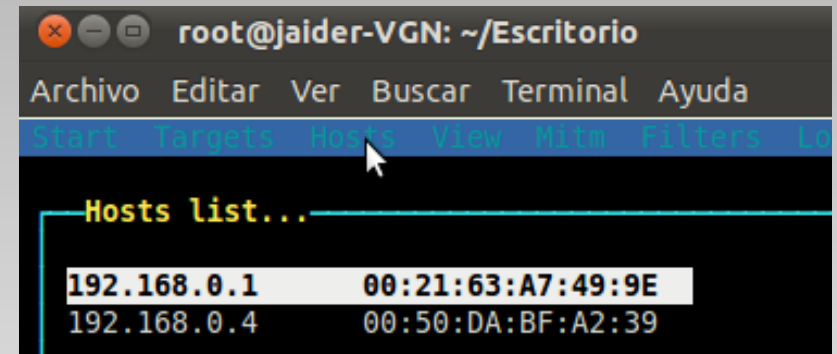
Interfaz: 192.168.0.4 --- 0x2
Dirección IP      Dirección física      Tipo
192.168.0.1      00-21-63-a7-49-9e    dinámico
192.168.0.2      00-13-e8-f9-6c-fd    dinámico
```

## Datos de victima Antes de ataque

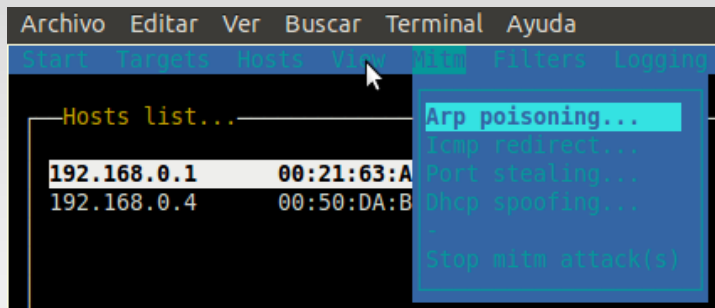
# Preparación de ettercap



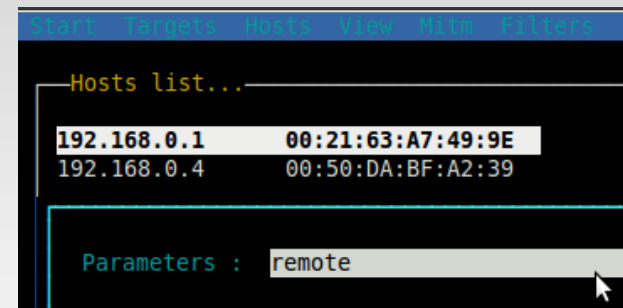
**A. Escaneo del segmento**



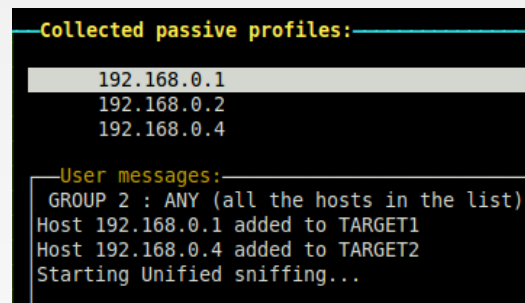
**B. Listado de host detectados.**



**C. Selección del ataque.**



**D. Selección parámetros.**



**D. Escenario ataque**

# ARP-GRATUITOUS EN EL ATAQUE

Con el objeto de corroborar la generación de paquetes ARP-Gratuitous, se encendió el pc victima, tras preparar wireshark sobre el pc atacante, . Con el siguiente obteniendo el siguiente reporte.

1242	503.920724	3com_bf:a2:39	Broadcast	ARP	Gratuitous ARP for 192.168.0.4 (Request)
1243	504.922216	3com_bf:a2:39	Broadcast	ARP	Gratuitous ARP for 192.168.0.4 (Request)
1259	514.160835	3com_bf:a2:39	Broadcast	ARP	who has 192.168.0.1? Tell 192.168.0.4
1287	889.058317	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	who has 192.168.0.1? Tell 192.168.0.2
1288	889.059254	AskeyCom_a7:49:9e	IntelCor_f9:6c:fd	ARP	192.168.0.1 is at 00:21:63:a7:49:9e
1290	919.331206	IntelCor_f9:6c:fd	Broadcast	ARP	who has 192.168.0.4? Tell 192.168.0.2
1291	919.332972	3com_bf:a2:39	IntelCor_f9:6c:fd	ARP	192.168.0.4 is at 00:50:da:bf:a2:39
1291	919.332972	IntelCor_f9:6c:fd	3com_bf:a2:39	ARP	who has 192.168.0.4? Tell 192.168.0.2

+ Frame 1243 (60 bytes on wire, 60 bytes captured)

+ Ethernet II, Src: 3com\_bf:a2:39 (00:50:da:bf:a2:39), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Address Resolution Protocol (request/gratuitous ARP)

Hardware type: Ethernet (0x0001)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (0x0001)

[Is gratuitous: True]

Sender MAC address: 3com\_bf:a2:39 (00:50:da:bf:a2:39)

Sender IP address: 192.168.0.4 (192.168.0.4)

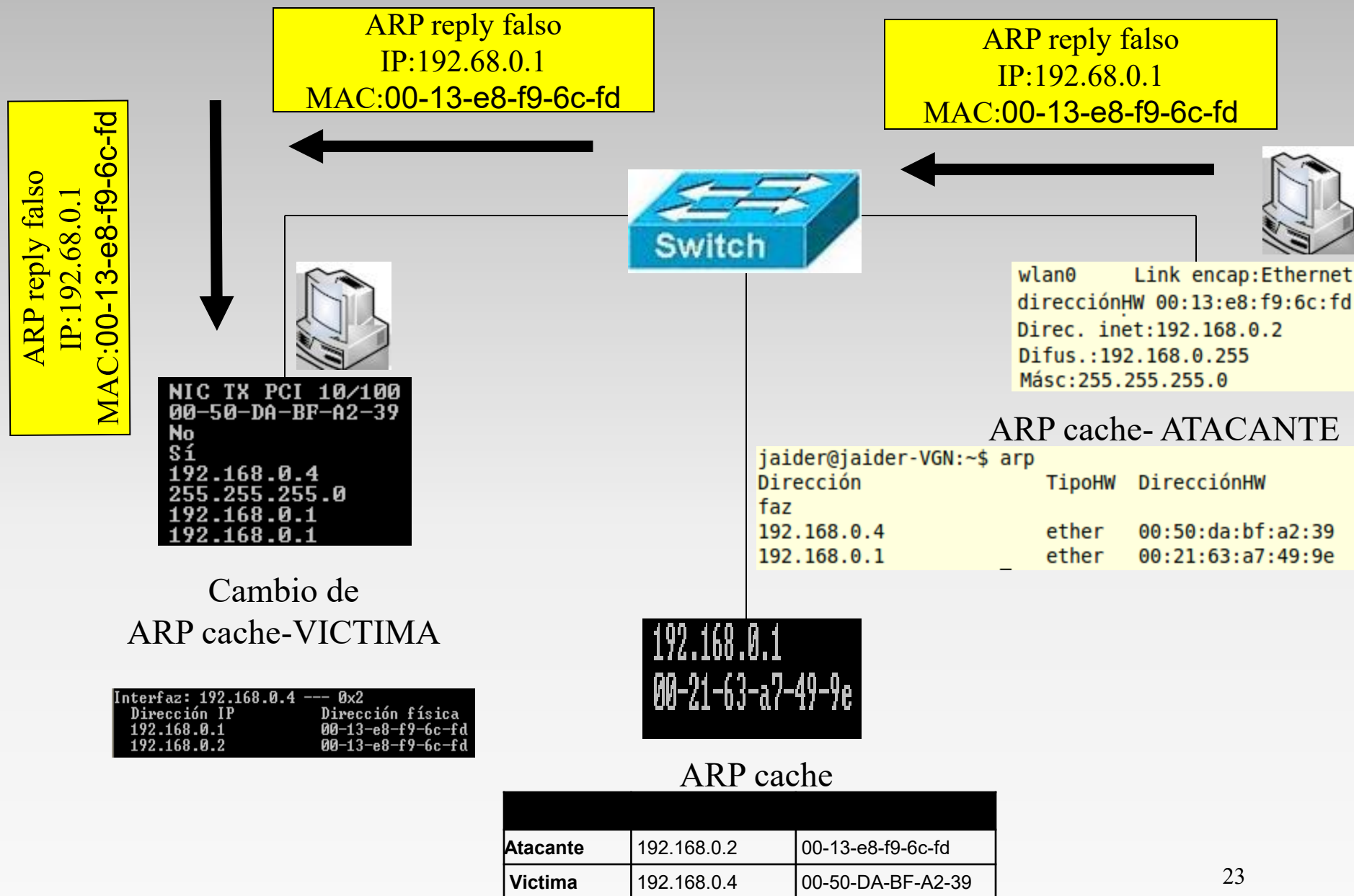
Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.0.4 (192.168.0.4)

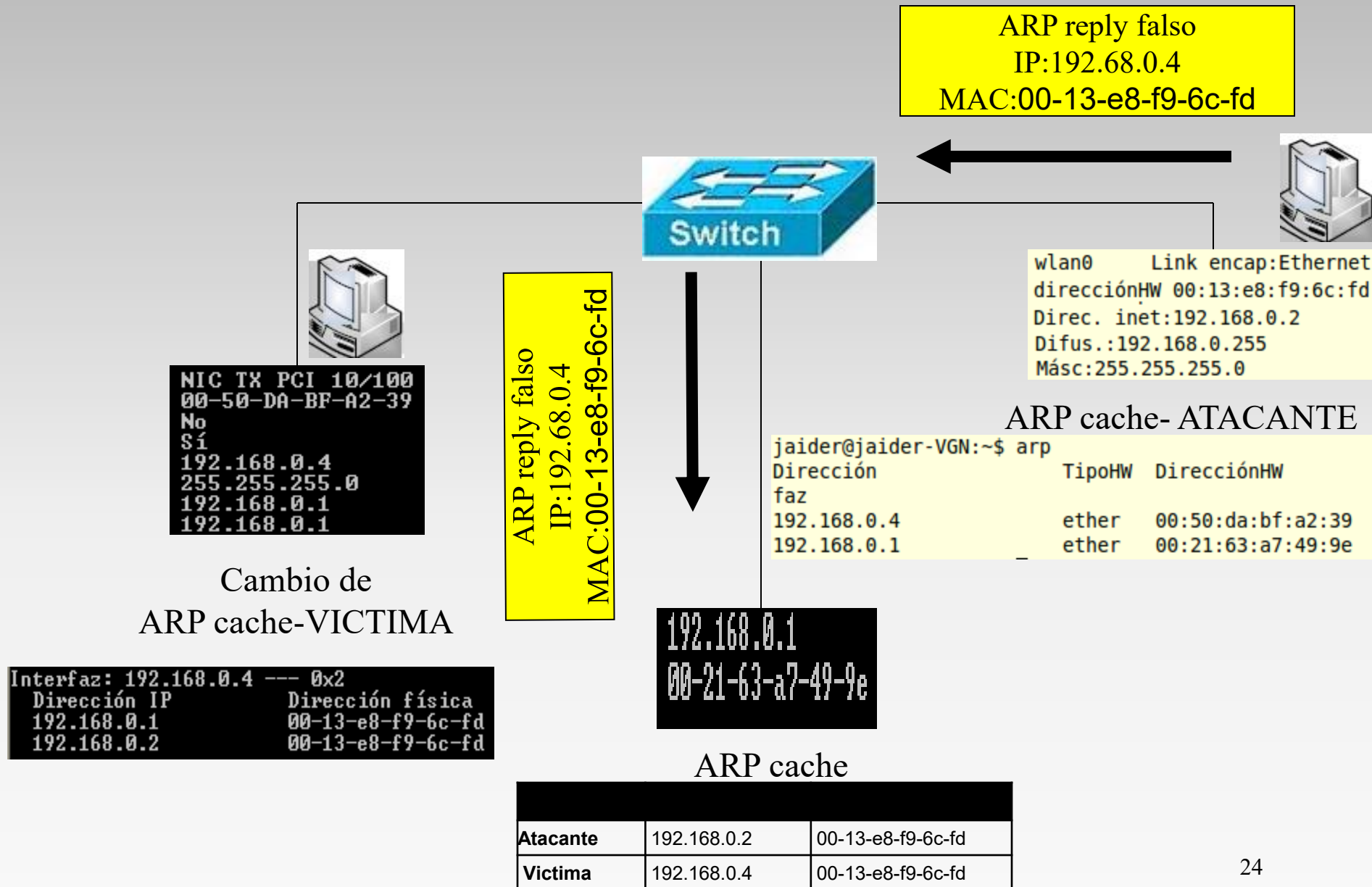
Direcciones IP destino y fuente son iguales  
Dirección MAC ES 00:00:00:00:00:00

El interés en detallar esta acción, radica en que es por medio de esta técnica que la máquina atacante consigue el envenamiento de la red!!!!!!!.

# Envenenamiento de cache de la victima



# Envenenamiento de cache del switch





# Análisis desde el atacante

3380	2347.620006	IntelCor_f9:6c:fd	3com_bf:a2:39	ARP	192.168.0.1	is	at	00:13:e8:f9:6c:fd
3379	2347.619927	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4	is	at	00:13:e8:f9:6c:fd
3378	2347.609509	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4	is	at	00:13:e8:f9:6c:fd
3377	2347.609422	IntelCor_f9:6c:fd	3com_bf:a2:39	ARP	192.168.0.1	is	at	00:13:e8:f9:6c:fd
3376	2337.598977	IntelCor_f9:6c:fd	3com_bf:a2:39	ARP	192.168.0.1	is	at	00:13:e8:f9:6c:fd
3375	2337.598899	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4	is	at	00:13:e8:f9:6c:fd
3374	2337.588434	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4	is	at	00:13:e8:f9:6c:fd
3373	2337.588337	IntelCor_f9:6c:fd	3com_bf:a2:39	ARP	192.168.0.1	is	at	00:13:e8:f9:6c:fd
3372	2327.577781	IntelCor_f9:6c:fd	3com_bf:a2:39	ARP	192.168.0.1	is	at	00:13:e8:f9:6c:fd
3371	2327.577690	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4	is	at	00:13:e8:f9:6c:fd

Frame 3387 (42 bytes on wire, 42 bytes captured)

Ethernet II, Src: IntelCor\_f9:6c:fd (00:13:e8:f9:6c:fd), Dst: AskeyCom\_a7:49:9e (00:21:63:a7:49:9e)

Address Resolution Protocol (reply)

Hardware type: Ethernet (0x0001)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (0x0002)

[Is gratuitous: False]

Sender MAC address: IntelCor\_f9:6c:fd (00:13:e8:f9:6c:fd)

Sender IP address: 192.168.0.4 (192.168.0.4)

Target MAC address: AskeyCom\_a7:49:9e (00:21:63:a7:49:9e)

Target IP address: 192.168.0.1 (192.168.0.1)

Respuesta de la víctima al switch, donde informa que su dirección es 00-13-e8-f9-6c-fd (MAC DEL ATCANTE). En este momento ya se encuentra envenenada la víctima!!.

NIC TX PCI 10/100

00-50-DA-BF-A2-39

No

Si

192.168.0.4

255.255.255.0

192.168.0.1

192.168.0.1

Datos originales de la víctima  
(sin enveneno).

```
0000 00 13 e8 f9 6c fd 08 06 00 01  !c.I... ..l....
0001 08 00 06 04 00 02 00 13  e8 f9 6c fd c0 a8 00 04  !..... ..l....
0002 00 21 63 a7 49 9e c0 a8 00 01  !c.I... ..
```

# Análisis desde el atacante

⊕ Frame 3384 (42 bytes on wire, 42 bytes captured)  
⊕ Ethernet II, Src: IntelCor\_f9:6c:fd (00:13:e8:f9:6c:fd), Dst: 3com\_bf:a2:39 (00:50:da:bf:a2:39)  
⊖ Address Resolution Protocol (reply)  
    Hardware type: Ethernet (0x0001)  
    Protocol type: IP (0x0800)  
    Hardware size: 6  
    Protocol size: 4  
    Opcode: reply (0x0002)  
    [Is gratuitous: False]  
    Sender MAC address: IntelCor\_f9:6c:fd (00:13:e8:f9:6c:fd)  
    Sender IP address: 192.168.0.1 (192.168.0.1)  
    Target MAC address: 3com\_bf:a2:39 (00:50:da:bf:a2:39)  
    Target IP address: 192.168.0.4 (192.168.0.4)

switch "envenenado"

**MAC reportada**

00-13-e8-f9-6c-fd

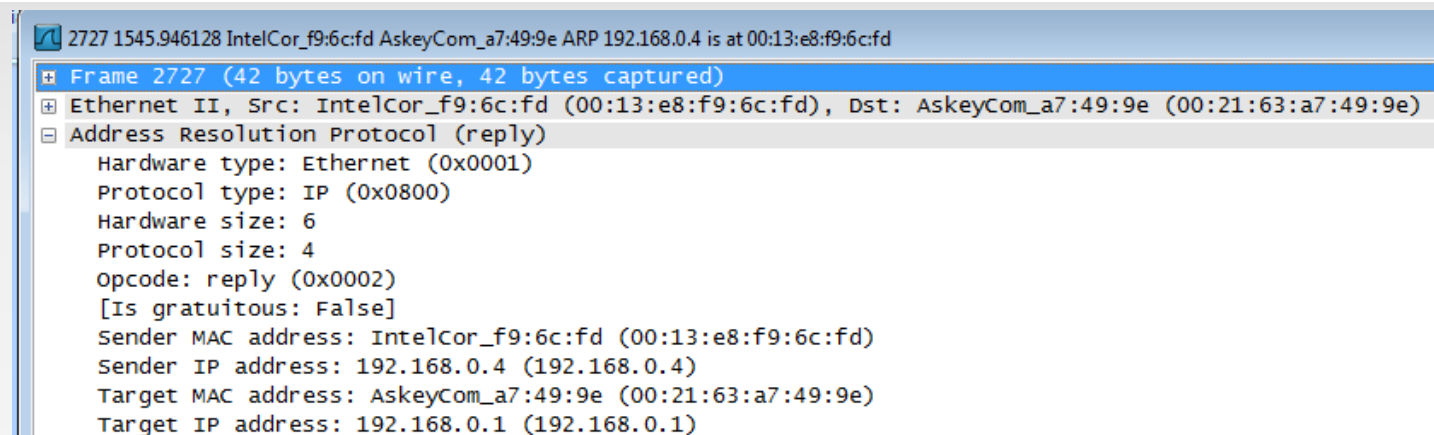
**MAC REAL**

**00-21-63-a7-49-9e**

# Análisis desde el atacante

2727	1545.946128	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4 is at 00:13:e8:f9:6c:fd
2728	1545.946230	IntelCor_f9:6c:fd	3com_bf:a2:39	ARP	192.168.0.1 is at 00:13:e8:f9:6c:fd
2729	1555.956658	IntelCor_f9:6c:fd	3com_bf:a2:39	ARP	192.168.0.1 is at 00:13:e8:f9:6c:fd
2730	1555.956749	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4 is at 00:13:e8:f9:6c:fd
2731	1555.966930	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4 is at 00:13:e8:f9:6c:fd
2732	1555.967000	IntelCor_f9:6c:fd	3com_bf:a2:39	ARP	192.168.0.1 is at 00:13:e8:f9:6c:fd
2766	1565.977444	IntelCor_f9:6c:fd	3com_bf:a2:39	ARP	192.168.0.1 is at 00:13:e8:f9:6c:fd
2767	1565.977500	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4 is at 00:13:e8:f9:6c:fd
2768	1565.987660	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4 is at 00:13:e8:f9:6c:fd
2769	1565.987690	IntelCor_f9:6c:fd	3com_bf:a2:39	ARP	192.168.0.1 is at 00:13:e8:f9:6c:fd

- ▶ Frame 2728 (42 bytes on wire, 42 bytes captured)
- ▶ Ethernet II, Src: IntelCor\_f9:6c:fd (00:13:e8:f9:6c:fd), Dst: 3com\_bf:a2:39 (00:50:da:bf:a2:39)
- ▶ [Duplicate IP address detected for 192.168.0.1 (00:13:e8:f9:6c:fd) - also in use by 00:21:63:a7:49:9e (frame 2727)]
- ▶ Address Resolution Protocol (reply)

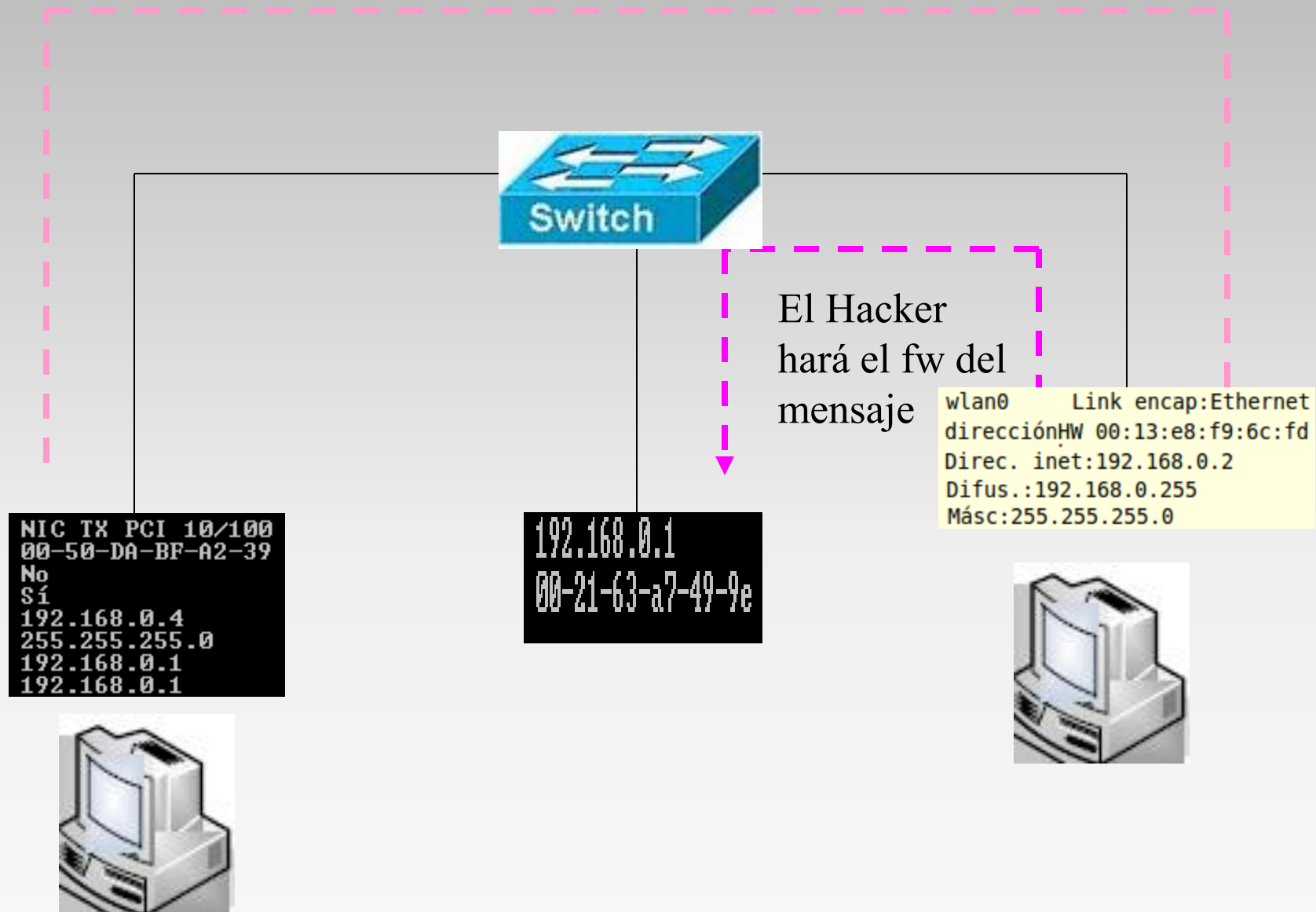


2727 1545.946128 IntelCor\_f9:6c:fd AskeyCom\_a7:49:9e ARP 192.168.0.4 is at 00:13:e8:f9:6c:fd

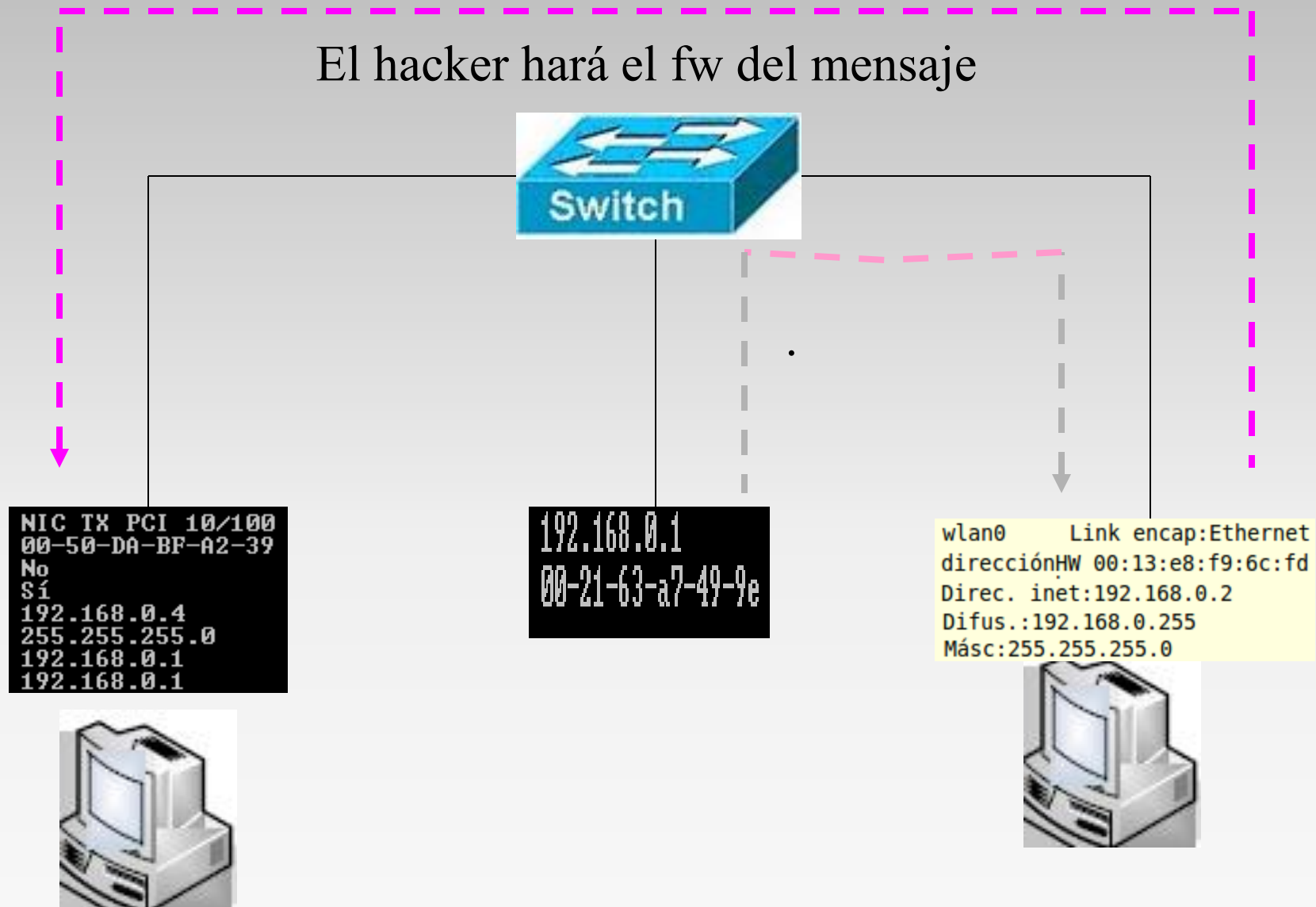
- Frame 2727 (42 bytes on wire, 42 bytes captured)
- Ethernet II, Src: IntelCor\_f9:6c:fd (00:13:e8:f9:6c:fd), Dst: AskeyCom\_a7:49:9e (00:21:63:a7:49:9e)
- Address Resolution Protocol (reply)
  - Hardware type: Ethernet (0x0001)
  - Protocol type: IP (0x0800)
  - Hardware size: 6
  - Protocol size: 4
  - Opcode: reply (0x0002)
  - [Is gratuitous: False]
  - Sender MAC address: IntelCor\_f9:6c:fd (00:13:e8:f9:6c:fd)
  - Sender IP address: 192.168.0.4 (192.168.0.4)
  - Target MAC address: AskeyCom\_a7:49:9e (00:21:63:a7:49:9e)
  - Target IP address: 192.168.0.1 (192.168.0.1)

Duplicación de direcciones detectada por wireshark

# Mensaje que debería haber ido al Switch



# Mensaje que debería ir a la víctima



# RESULTADOS DEL ATAQUE

Captura del tráfico generado  
por y para la víctima!!

## Collected passive profiles:

65.54.186.107	login.live.com
65.54.254.139	nexus.passport.com
65.55.7.11	workspace.office.live.com
69.63.190.10	www.facebook.com
69.192.147.235	armmf.adobe.com
72.14.204.17	mail.google.com
72.14.204.18	mail.google.com
161.69.12.13	updatekeepalive.mcafee.com
161.69.13.21	liteapps.mcafee.com
192.168.0.1	
192.168.0.2	
192.168.0.4	
200.69.125.73	www.download.windowsupdate.com
200.69.125.89	www.download.windowsupdate.com
200.75.51.132	
200.75.51.133	
* 201.245.193.147	www.google.com
201.245.193.154	
201.245.193.155	safebrowsing.clients.google.com
201.245.193.210	safebrowsing-cache.google.com
201.245.193.215	safebrowsing-cache.google.com

## Connection data

192.168.0.4:1117

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; es-ES; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3.  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8.  
Accept-Language: es-es,es;q=0.8,en-us;q=0.5,en;q=0.3.  
Accept-Encoding: gzip,deflate.  
Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7.  
Keep-Alive: 115.  
Connection: keep-alive.  
Cookie: utmb=173272373; GoogleAccountsLocale\_session=es; utma=173272373.38038692.1239200153.1239200153.1239200153.1; utmb=173272373; utmz=173272373.1239200153.1.1.utmccn=(organic)|utmcsr=google|utmctr=gmail|utmcmd=organic; GALX=n0ew8p3mqTw; LSID=cl|s.CO:DQAAAJkAAABSwqDzV0sV0SmlynuE9Z2by2LP0iPiyyll1wh-Jk0UdF1PDzNeRtb7b2682bVeoyiyVHCbXhQA41Uf0jrzB0vt7Fz507EBs91z3GK9jh55ScoDo\_J2svuPQbgKCBcEfHm3RYPTFLPFvVf8PTDG57a7RbSo3EtU7EK61CNityPscjpbIpF3btUhiSNkSNHGGPKK2z4ZFDTLMULE6VVRM; GAUSR=s.CO:jaiderr.ospina@gmail.com; P REF=ID=1777b0509f4bb596:U=824b067f3bcf0744:FF=0:TM=1239199780:LM=1289474758:GM=1:S=8ZSFmSp0xXtLRHwC; rememberme=false; NID=40=nVll8PCksbA\_PGHemthNJHUB3130mESMouhH2eSwcmtpqCUHdgDrayf0Tb2RcSz897H3FLmG6nm1aJHAH-fceeKt7Wla4hdf-00sajYpPs qL2DYaxDayskAMkoDIWg; TZ=300; GMAIL\_LOGIN=T976831041635/976831041635/976831106332; SID=DQAAAJYAAAAmivI5a7idBQ9r9eU9gWu0y\_53PF5TLPD4MqLVfxLE10tcbhm9Z3Ztjx qKL0GIrWknL9tWTWUFGHfANy50ZbAHTC rJI18a0Wwv8ZUY6KgC wkWcjI56nkrU35pG\_3eV68e0EH0pwXiQ81D0EeBxKzWEEER4pnCsSYSZQccuOXFRBssSsLmaBGVQAsi-iHrwwhQPUfZyJEbsGzmNqEe; HSID=A7X31FJP7wewnIb2b; SSID=AKDDxC5PAW1HQIhsU.

201.245.193.147:443

Content-Type: text/html; charset=UTF-8.  
P3P: CP="This is not a P3P policy! See http://www.google.com/support/accounts/bin/answer.py?hl=en&answer=151657 for more info.".  
Location: https://mail.google.com/mail/?hl=es&tab=wm&pli=1&auth=DQAAAL8AAADYaxIauv3oS\_xIApufPCJkyY3PoyDyngWjJIxwQkSydn9\_iLEuPwtXLTurKwdTCe0dHsiCb9QN3G5PXTHPd\_tVtFC\_-seGtpcV6Rz2lygAP8mPhdJJUzTi-v89\_hCxeiwzG7a7LYCR04ne0Z38mLRagglX6cUAYaeL22DEGKFI-USiiP2LjvXRJOPeGyGrR0rCt7TJRWieReShGi\_-QJz-TX4MAUp251ldZMHC0EPEXTLR0lvfy4VSDVmbsv0&gausr=jaiderr.ospina%40gmail.com.  
Content-Encoding: gzip.  
Date: Mon, 22 Nov 2010 10:56:13 GMT.  
Expires: Mon, 22 Nov 2010 10:56:13 GMT.  
Cache-Control: private, max-age=0.  
X-Content-Type-Options: nosniff.  
X-XSS-Protection: 1; mode=block.  
Content-Length: 445.  
Server: GSE.  
.....mR.r@.....S3;..D..S@...b....J...  
4(~).....}.:s.l..dS.ZW..A}....p..E^..&.,].....lk'.Pmh.  
.c...l.C.(.....m.(\".d..p.=N...+...+. 'AH1Mfa... ]....?Q....N....  
k..EB.q...E.....y....q.L...[...~ST..=M.....8.....]...6...>.z....Q).\...D....  
.....xp<d....l.....!p.....e.....1.3xR]q...u20.....{..A...  
\$M7^V..~G..#...v.v.q  
.R.U6C.f...%....pk....n....4x.....A.N..vz....5b/J...TbL.R.....9..^..NY~

Detalles de sección

# RESULTADOS DEL ATAQUE

## EXTRACCIÓN DE CONTRASEÑAS Supuestamente seguras!!

```
Live connections:
192.168.0.4:1091 - 74.117.174.60:1863 T opening TX: 0
192.168.0.4:1092 - 74.117.174.60:1863 T opening TX: 0
192.168.0.4:1093 - 74.117.174.60:1863 T opening TX: 0
192.168.0.4:1066 - 200.75.51.132:53 U idle TX: 1488
192.168.0.4:1094 - 201.245.193.144:80 T closed TX: 3904
192.168.0.4:1095 - 201.245.193.144:80 T killed TX: 1298
192.168.0.4:1096 - 201.245.193.147:80 T closed TX: 34096
192.168.0.4:1065 - 200.75.51.132:53 U idle TX: 902
192.168.0.4:1041 - 200.75.51.132:53 U idle TX: 748
192.168.0.4:1097 - 74.117.174.60:1863 T opening TX: 0
192.168.0.4:1098 - 74.117.174.60:1863 T opening TX: 0
192.168.0.4:1099 - 72.14.204.17:80 T closed TX: 1846
M 192.168.0.4:1100 - 201.245.193.147:443 T opening TX: 0
192.168.0.4:1101 - 74.117.174.60:1863 T opening TX: 0
M 192.168.0.4:1102 - 201.245.193.147:443 T opening TX: 0
M 192.168.0.4:1103 - 201.245.193.147:443 T opening TX: 0
M 192.168.0.4:1104 - 201.245.193.147:443 T killed TX: 13901
192.168.0.4:1105 - 74.117.174.60:1863 T opening TX: 0
M 192.168.0.4:1106 - 201.245.193.153:443 T opening TX: 0
M 192.168.0.4:1107 - 201.245.193.147:443 T killed TX: 900
M 192.168.0.4:1108 - 201.245.193.147:443 T killed TX: 2935
M 192.168.0.4:1109 - 72.14.204.17:443 T opening TX: 0
M 192.168.0.4:1110 - 72.14.204.17:443 T opening TX: 0
192.168.0.4:1111 - 74.117.174.60:1863 T opening TX: 0
M 192.168.0.4:1112 - 72.14.204.17:443 T opening TX: 0

User messages:
Starting Unified sniffing...

Unified sniffing already started...
HTTP : 201.245.193.147:443 -> USER: jaider.ospina PASS: n+...j*0014 INFO: https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http://mail.google.com/mail/?hl=es&tab=wm&ui=html&zy=l&bsv=1
```

YA LA  
CAMBIAMOS!!!!  
POR SI ACAS....



# Ataques que usan ARP Spoofing

## ○ **Switch Port Stealing (Sniffing):**

Utilizando ARP Spoofing el atacante consigue que todas las tramas dirigidas hacia otro puerto del switch lleguen al puerto del atacante para luego re-enviarlos hacia su destinatario y de esta manera poder ver el tráfico que viaja desde el remitente hacia el destinatario (Una especie de sniffing half-duplex).

## ○ **Man in the Middle (Sniffing):**

Utilizando ARP Spoofing el atacante logra que todas las tramas que intercambian las víctimas pasen primero por su equipo (Inclusive en ambientes switcheados).



# Ataques que usan ARP Spoofing

## ○ **Secuestro (Hijacking):**

El atacante puede lograr redirigir el flujo de tramas entre dos dispositivos hacia su equipo. Así puede lograr colocarse en cualquiera de los dos extremos de la comunicación (previa deshabilitación del correspondiente dispositivo) y secuestrar la sesión.

## ○ **Denial of service (DoS):**

El atacante provoca que un equipo crítico de la red tenga una dirección MAC inexistente. Con esto se logra que las tramas dirigidas a la IP de este dispositivo se pierdan.

# Port Security (Ejemplo)

- Conjunto de medidas de seguridad a nivel de
- puertos disponibles en la mayoría de los switchs
- de gama media y alta.
- • La funciones provistas dependen de la marca, el modelo y la versión de firmware del switch en cuestión.
- • Permite entre otras cosas:
  - – Restringir el acceso a los puertos según la MAC.
  - – Restringir el numero de MACs por puerto.
  - – Reaccionar de diferentes maneras a violaciones de las restricciones anteriores.
  - – Establecer la duración de las asociaciones MAC-Puerto.

# Port Security (Ejemplo)

- Configuración del puerto 15 del para que no acepte más de dos direcciones MAC. MAC-Puerto.

No se puede activar port security en puertos dynamic access o trunk.

- Port Security está desactivado por default.
- Por default port security sólo almacena una sola MAC por puerto.

```
Switch> enable
Switch# configure terminal
Switch(config)# interface FastEthernet 0/15
(Dentro del modo configuración de interface del puerto a configurar)
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
```

# Port Security (Ejemplo)

- Agregación de una lista estática de direcciones MAC:
- Con la primera se agregan las MACs que van aprendiendo a la lista de MACs seguras.
- Con la segunda que agregue la MAC 00:0a:5e:5a:18:1b a la lista de MACs seguras.

(Dentro del modo configuración de interface del puerto a configurar)

```
Switch(config-if)# switchport port-security mac-address sticky
```

```
Switch(config-if)# switchport port-security mac-address mac-address 000a.5e5a.181b
```

# Protocolo NDP en IPV6

El protocolo NDP (Neighbor Discovery Protocol) usado en IPv6 y el protocolo ARP usado en IPv4 cumplen con la misma finalidad. La diferencia está en los términos que se emplean para referirse a las diferentes acciones que se llevan a cabo.

Aquí en lugar de hablar de una consulta ARP (ARP request) tenemos una solicitud de vecino (Neighbor Solicitation), y en vez de hablar de una respuesta ARP (ARP reply) tenemos lo que se conoce como anuncio de vecino (Neighbor Advertisement) que aunque suenen a cosas diferentes en realidad el comportamiento que tienen es casi el mismo. Es decir, el primero es usado para llegar a conocer alguna dirección de hardware como fue descrito en la sección anterior de las consultas ARP y el segundo es usado para responder a una solicitud de manera similar como también ya fue explicado. Otra diferencia, es el nombre que recibe la caché ARP de los nodos; la cual en NDP se la conoce como caché de vecinos (Neighbor Cache).

Dadas las similitudes de ambos protocolos, en el caso de NDP se presentan problemas similares a los que actualmente presenta el protocolo ARP. Por esta razón, ya se ha planteado una alternativa segura denominada S NDP (Secure Neighbor Discovery Protocol), la cual es una extensión al protocolo NDP que usa criptografía para asegurar las comunicaciones.

Gracias...

Ahh, y sabemos lo que hicieron el  
verano pasado!!.



Preguntas???

# Bibliografía y direcciones de interés

- ◉ [http://book.chinaunix.net/special/ebook/oreilly/Understanding\\_Linux\\_Network\\_Internals/0596002556/understandlni-CHP-28-SECT-3.html](http://book.chinaunix.net/special/ebook/oreilly/Understanding_Linux_Network_Internals/0596002556/understandlni-CHP-28-SECT-3.html)
- ◉ <http://www.ks.uni-freiburg.de/download/inetworkSS05/practical/arp/arp-spoofing.pdf>
- ◉ [http://wiki.wireshark.org/Gratuitous\\_ARP](http://wiki.wireshark.org/Gratuitous_ARP)
- ◉ [http://ariadna.ii.uam.es/wiki/wii\\_rc2/doku.php?id=arp](http://ariadna.ii.uam.es/wiki/wii_rc2/doku.php?id=arp)
- ◉ [http://en.wikipedia.org/wiki/Secure\\_Neighbor\\_Discovery](http://en.wikipedia.org/wiki/Secure_Neighbor_Discovery)