

Voici le résultat d'une analyse de quelques secondes de mon réseau wifi domestique :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2603:1063:2000:1::2...	2a01:e0a:b94:e5a0:8...	TCP	74 443 → 49713 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
2	0.888102	192.168.0.38	192.168.0.22	TCP	164 49750 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=509 Len=0	
3	0.890248	192.168.0.22	192.168.0.38	TCP	54 8009 → 49750 [ACK] Seq=1 Ack=111 Win=245 Len=0	
4	0.894778	192.168.0.22	192.168.0.38	TCP	164 8009 → 49750 [PSH, ACK] Seq=1 Ack=111 Win=245 Len=0	
5	0.950225	192.168.0.38	192.168.0.22	TCP	54 49750 → 8009 [ACK] Seq=111 Ack=111 Win=509 Len=0	
6	3.439642	fe80::224:d4ff:fea9...	2a01:e0a:b94:e5a0:8...	ICMPv6	86 Neighbor Solicitation for 2a01:e0a:b94:e5a0:8125	
7	3.439774	2a01:e0a:b94:e5a0:8...	fe80::224:d4ff:fea9...	ICMPv6	86 Neighbor Advertisement 2a01:e0a:b94:e5a0:8125:41	
8	5.902514	192.168.0.38	20.231.121.79	TCP	66 49836 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460	
9	5.902954	192.168.0.38	192.168.0.22	TCP	164 49750 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=509	
10	5.905859	192.168.0.22	192.168.0.38	TCP	164 8009 → 49750 [PSH, ACK] Seq=111 Ack=221 Win=245	
11	5.949343	192.168.0.38	192.168.0.22	TCP	54 49750 → 8009 [ACK] Seq=221 Ack=221 Win=508 Len=0	

On constate qu'il y a 2 trames ICMP qui sont présentes.

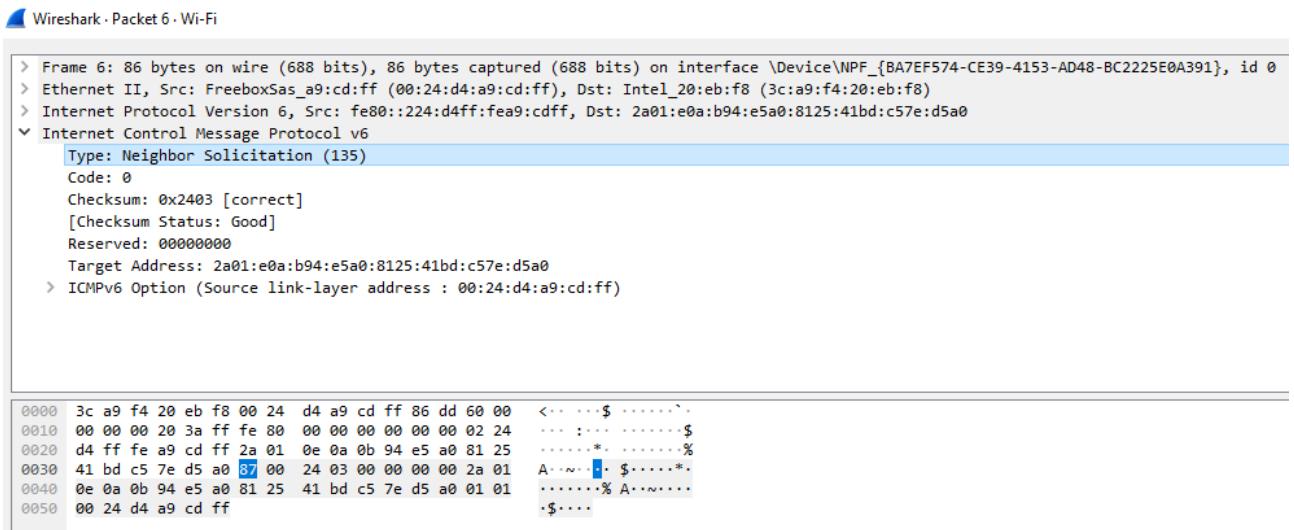
Leur nom et le fait qu'elles se suivent dans le temps laissent penser que la seconde répond à la 1ère.

Voici la 1ère plus détaillée :

Wireshark · Packet 6 · Wi-Fi	
> Frame 6: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{BA7EF574-CE39-4153-AD48-BC2225E0A391}, id 0	
> Ethernet II, Src: FreeboxSas_a9:cd:ff (00:24:d4:a9:cd:ff), Dst: Intel_20:eb:f8 (3c:a9:f4:20:eb:f8)	
> Internet Protocol Version 6, Src: fe80::224:d4ff:fea9:cdf, Dst: 2a01:e0a:b94:e5a0:8125:41bd:c57e:d5a0	
Internet Control Message Protocol v6	
Type: Neighbor Solicitation (135)	
Code: 0	
Checksum: 0x2403 [correct]	
[Checksum Status: Good]	
Reserved: 00000000	
Target Address: 2a01:e0a:b94:e5a0:8125:41bd:c57e:d5a0	
ICMPv6 Option (Source link-layer address : 00:24:d4:a9:cd:ff)	
0000	3c a9 f4 20 eb f8 00 24 d4 a9 cd ff 86 dd 60 00 <...-\$...`.
0010	00 00 00 20 3a ff fe 80 00 00 00 00 00 02 24 ...:.....\$
0020	d4 ff fe a9 cd ff 2a 01 0e 0a 0b 94 e5 a0 81 25 .....*....%
0030	41 bd c5 7e d5 a0 87 00 24 03 00 00 00 00 2a 01 A~~...\$.~*.
0040	0e 0a 0b 94 e5 a0 81 25 41 bd c5 7e d5 a0 01 01 .....%A..n+..
0050	00 24 d4 a9 cd ff \$....

On constate qu'il occupe 32 octets (32 couples de 2 chiffres hexadécimaux).

La même trame où j'ai surligné le type (Neighbor Sollicitation (135)), et l'endroit dans le paquet d'octets où ce type apparaît :

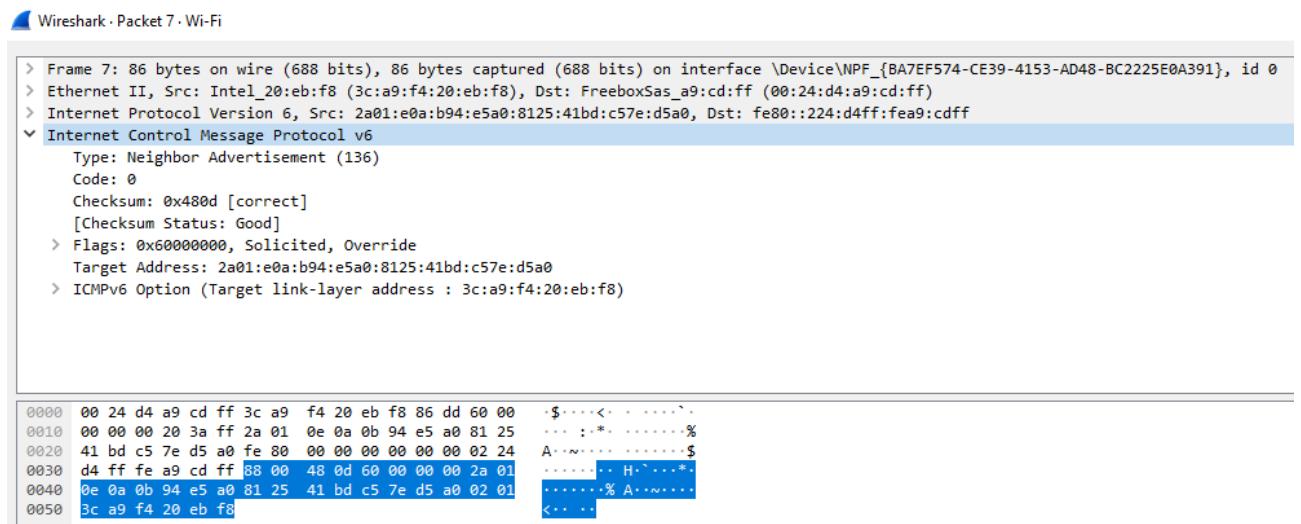


```
> Frame 6: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{BA7EF574-CE39-4153-AD48-BC2225E0A391}, id 0
> Ethernet II, Src: FreeboxSas_a9:cd:ff (00:24:d4:a9:cd:ff), Dst: Intel_20:eb:f8 (3c:a9:f4:20:eb:f8)
> Internet Protocol Version 6, Src: fe80::224:d4ff:fea9:cdff, Dst: 2a01:e0a:b94:e5a0:8125:41bd:c57e:d5a0
< Internet Control Message Protocol v6
    Type: Neighbor Sollicitation (135)
        Code: 0
        Checksum: 0x2403 [correct]
        [Checksum Status: Good]
        Reserved: 00000000
        Target Address: 2a01:e0a:b94:e5a0:8125:41bd:c57e:d5a0
    > ICMPv6 Option (Source link-layer address : 00:24:d4:a9:cd:ff)

0000  3c a9 f4 20 eb f8 00 24  d4 a9 cd ff 86 dd 60 00  <...-$....`.
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 02 24  ...:.....$.
0020  d4 ff fe a9 cd ff 2a 01  0e 0a 0b 94 e5 a0 81 25  ....,*....%.
0030  41 bd c5 7e d5 a0 87 00  24 03 00 00 00 00 2a 01  A~~~. $....*.
0040  0e 0a 0b 94 e5 a0 81 25  41 bd c5 7e d5 a0 01 01  .....% A~~~...
0050  00 24 d4 a9 cd ff                               .$....
```

On voit que le type "Neighbor Sollicitation" possède le code "d'erreur" 135 et qu'il est bien en hexadécimal dans la trame, sous la forme du 87 (qui est égal à 135 en décimal) surligné en bleu.

Voici la seconde trame en détails :



```
> Frame 7: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{BA7EF574-CE39-4153-AD48-BC2225E0A391}, id 0
> Ethernet II, Src: Intel_20:eb:f8 (3c:a9:f4:20:eb:f8), Dst: FreeboxSas_a9:cd:ff (00:24:d4:a9:cd:ff)
> Internet Protocol Version 6, Src: 2a01:e0a:b94:e5a0:8125:41bd:c57e:d5a0, Dst: fe80::224:d4ff:fea9:cdff
< Internet Control Message Protocol v6
    Type: Neighbor Advertissement (136)
        Code: 0
        Checksum: 0x480d [correct]
        [Checksum Status: Good]
        Flags: 0x60000000, Solicited, Override
        Target Address: 2a01:e0a:b94:e5a0:8125:41bd:c57e:d5a0
    > ICMPv6 Option (Target link-layer address : 3c:a9:f4:20:eb:f8)

0000  00 24 d4 a9 cd ff 3c a9  f4 20 eb f8 86 dd 60 00  .$...<...`...
0010  00 00 00 20 3a ff 2a 01  0e 0a 0b 94 e5 a0 81 25  ...:.*....%.
0020  41 bd c5 7e d5 a0 fe 80  00 00 00 00 00 00 02 24  A~~~.....$.
0030  d4 ff fe a9 cd ff 88 00  48 0d 60 00 00 00 2a 01  .....H~....*.
0040  0e 0a 0b 94 e5 a0 81 25  41 bd c5 7e d5 a0 02 01  .....% A~~~...
0050  3c a9 f4 20 eb f8                               <....
```

Et maintenant les mêmes champs d'information surlignés que dans la 1ère trame :

The Wireshark interface shows a captured packet labeled "Frame 7". The packet details are as follows:

- Frame 7: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF\_{BA7EF574-CE39-4153-AD48-BC2225E0A391}, id 0
- Ethernet II, Src: Intel\_20:eb:f8 (3c:a9:f4:20:eb:f8), Dst: FreeboxSas\_a9:cd:ff (00:24:d4:a9:cd:ff)
- Internet Protocol Version 6, Src: 2a01:e0a:b94:e5a0:8125:41bd:c57e:d5a0, Dst: fe80::224:d4ff:fea9:cdf
- Internet Control Message Protocol v6
  - Type: Neighbor Advertisement (136)
  - Code: 0
  - Checksum: 0x480d [correct]  
[Checksum Status: Good]
  - Flags: 0x60000000, Solicited, Override
  - Target Address: 2a01:e0a:b94:e5a0:8125:41bd:c57e:d5a0
  - ICMPv6 Option (Target link-layer address : 3c:a9:f4:20:eb:f8)

The hex dump of the packet shows the following bytes:

Hex	Dec	ASCII
0000	00 24 d4 a9 cd ff 3c a9 f4 20 eb f8 86 dd 60 00	\$ . . . < . . . . .
0010	00 00 00 20 3a ff 2a 01 0e 0a 0b 94 e5 a0 81 25	... ; * . . . . %
0020	41 bd c5 7e d5 a0 fe 80 00 00 00 00 00 02 24	A . . . . . . . . \$
0030	d4 ff fe a9 cd ff 88 00 48 0d 60 00 00 00 2a 01	. . . . . H . . . *
0040	0e 0a 0b 94 e5 a0 81 25 41 bd c5 7e d5 a0 02 01	....% A . . . .
0050	3c a9 f4 20 eb f8	< . . . .

On voit que le type "Neighbor Advertisement" possède le code "d'erreur" 136 et qu'il est bien en hexadécimal dans la trame, sous la forme du 88 (qui est égal à 136 en décimal) surligné en bleu.

Apparemment, en IPv6, il n'y a plus de protocole ARP, donc c'est le protocole ICMP qui assure sa fonction de découverte et de conservation des adresses MAC des autres machines du réseau. Il tient un "Neighbor Cache" qui est une "table des voisins" avec lesquels la machine a communiqué récemment.

## Neighbor Solicitation Messages in IPv6 (NS)

The Neighbor Solicitation message (NS) is ICMPv6 Type 135.

It is used to find the Link Layer address, so the Layer 2 or MAC address of another host to establish ethernet communication. A Neighbor Solicitation (NS) is **sent to the solicited-node multicast address of the neighbor** (like ARP in IPv4).

also, a NS is sent to unicast address of neighbor, to find out if it is still alive and reachable

## Neighbor Advertisement Messages in IPv6 (NA)

The Neighbor Advertisement message (NA) is ICMPv6 Type 136.

This message is used to reply to **Neighbor Solicitation (NS) message**

# How IPv6 Neighbor Processing works

You have learned before, that in IPv6 there is no ARP anymore. Instead there is ICMPv6 and the Solicited-Node Multicast address, but how does that all fit together? Let's find the answers in the following chapters.

## The IPv6 Neighbor Cache keeps Track of all Neighbors

The neighbor cache is a table on a device (host or router) which lists all **neighbors** that have been communicated with recently.

The neighbor cache contains the MAC address of the corresponding IPv6 address and a flag, if it is a router or a host

The neighbor cache also lists **reachability information** (similar to the ARP cache of IPv4), so if a device is not seen for some time, it is aged out and ultimately dropped from the neighbor cache table.

## The IPv6 Destination Cache keeps Track of all Destinations

The destination cache lists all **targets** that have been communicated with recently.

The destination cache contains the MAC address of the local neighbor or the MAC address of the next hop, in case the IPv6 target is remote and not accessible locally on a connected link.