Fonctionnement

Fonctionnement régulier

Le fonctionnement du protocole ARP est parmis les protocoles réseau les plus simples. Il suffit d'envoyer une requête à tous les appareils situé au sein du même domaine de diffusion (adresse MAC FF:FF:FF:FF:FF:FF) demandant quelle adresse MAC possède une adresse IP particulière. Si un appareil possède cette adresse IP, l'appareil répondra avec son adresse MAC pour savoir à quelle adresse MAC adresser une trame ethernet.

Exemple d'une requête ARP :

```
Frame 76: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0
Ethernet II, Src: 00:50:79:66:68:02, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 00:50:79:66:68:02
    Sender IP address: 192.168.255.3
    Target MAC address: ff:ff:ff:ff:ff:ff
    Target IP address: 192.168.255.6
```

Dans cette requête ARP, le demandeur doté de l'adresse MAC 00:50:79:66:68:02 configuré avec l'adresse IP 192.168.255.3 demande à l'ensemble de son domaine de diffusion qui est configuré avec l'adresse IPv4 192.168.255.6.

Exemple d'une réponse ARP :

```
Frame 77: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0
Ethernet II, Src: 00:50:79:66:68:05, Dst: 00:50:79:66:68:02
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
```

```
Sender MAC address: 00:50:79:66:68:05
Sender IP address: 192.168.255.6
Target MAC address: 00:50:79:66:68:02
Target IP address: 192.168.255.3
```

Puisque l'adresse MAC du demandeur est mentionné dans la requête, la réponse contenant l'adresse MAC de la destination sera acheminée seulement au demandeur et contiendra l'adresse IP ainsi que l'adresse MAC de la destination concernée par la demande.

Empoisonnement ARP

Le protocole ARP étant aussi simple, même si un appareil n'émet par de demande, il est possible d'informer un appareil ou même un réseau complet de notre adresse MAC et notre adresse IP. Ceci peut être utilisé pour permettre l'établissement plus rapide de connexion entre plusieurs appareils. En contrepartie, ceci est généralement utiliser pour empoisonner la table ARP de victimes pour effectuer une attaque de type man-in-the-middle. Ce type d'attaque consiste à constamment s'annoncer comme possédant l'adresse IP du routeur dans un domaine de diffusion pour recevoir l'ensemble des communications des appareils de ce réseau étant destinées au réseau étendu. Ceci peut être utilisé pour intercepter ou capturer le trafic des appareils d'un réseau, que ce soit pour modifier les réponses transmises aux émetteurs ou espionner les appareils d'un réseau. Il est aussi possible d'utiliser cette méthode pour effectuer une attaque de déni de service pour empêcher un appareil d'accéder à un autre appareil ou accéder au réseau étendu.

Malgré que 192.168.122.229 n'ait effectué aucune requête ARP, 192.168.122.1 s'annonce comme étant 8.8.8.8 avec l'adresse MAC 52:54:00:e6:6e:44.

```
52:54:00:e6:6e:44    ff:ff:ff:ff:ff:ff    ARP     Who has 192.168.122.229? Tell 192.168.122.1
52:54:00:e6:6e:44    00:00:00:00:00:00    ARP     8.8.8.8 is at 52:54:00:e6:6e:44
52:54:00:e6:6e:44    00:00:00:00:00:00    ARP     8.8.8.8 is at 52:54:00:e6:6e:44
52:54:00:e6:6e:44    00:00:00:00:00:00    ARP     8.8.8.8 is at 52:54:00:e6:6e:44
52:54:00:e6:6e:44    00:00:00:00:00:00    ARP     8.8.8.8 is at 52:54:00:e6:6e:44
52:54:00:e6:6e:44    00:00:00:00:00:00    ARP     8.8.8.8 is at 52:54:00:e6:6e:44
```

Revision #3
Created 2025-02-05 01:33:42 UTC by Alexandre Arsenault-Jetté
Updated 2025-02-05 04:15:12 UTC by Alexandre Arsenault-Jetté