Les adresses MAC, le IP et le spoofing

Par Patrick Sentinel – 29a.ca

Les adresses MAC, le IP, et spoofing : comment ça fonctionne (et pourquoi ça peut poser problème 😳)

Dans le vaste monde des réseaux informatiques, deux types d'adresses jouent un rôle clé : les **adresses IP** et les **adresses MAC**. Ces deux identifiants permettent aux appareils de communiquer entre eux, mais ils peuvent aussi être manipulés par des techniques comme le **MAC *spoofing***. Vous êtes prêt à comprendre tout ça sans finir avec un mal de tête ? C'est parti !

L'adresse IP : l'identité numérique sur Internet

L'**adresse IP (*Internet Protocol*)** est un identifiant **unique** attribué à chaque appareil connecté à un réseau. Imaginez-la comme une adresse postale qui permet d'envoyer et de recevoir des informations sur Internet.

Deux types d'adresses IP :

IPv4 (exemple : 192.168.1.1) : Le format classique, limité à environ 4,3 milliards d'adresses (et oui, on commence à en manquer depuis un certain temps). Vous vous souvenez de l'article sur les bits ? Alors ce type d'adresse tient sur 32 bits 😊.

IPv6 (exemple : 2001:0db8:85a3::8a2e:0370:7334) : La version moderne, avec un espace d'adressage quasi infini (celle-ci tient sur 128 bits).

Comment fonctionne une adresse IP ?

Grossièrement, lorsqu'un appareil veut envoyer des données sur Internet :

1. Il envoie la demande à un **routeur**, qui attribue une adresse IP publique;
2. Cette adresse IP permet aux serveurs distants de savoir où envoyer les réponses;
3. Une fois la connexion établie, la communication se fait entre adresses IP, un peu comme l'envoi de lettres entre deux adresses postales.

Mais attention : l'adresse IP seule ne suffit pas pour qu'un réseau fonctionne. Il lui faut un allié puissant : l'**adresse MAC**.

L'adresse MAC : l'empreinte unique d'un appareil

L'**adresse MAC (*Media Access Control*)** est un identifiant unique attribué à chaque carte réseau (Wi-Fi, Ethernet, etc.). Contrairement à une adresse IP, qui peut changer en fonction du réseau (parfois statique, parfois dynamique), l'adresse MAC est censée être permanente.

À quoi ça ressemble ? Une adresse MAC est un ensemble de **12 caractères hexadécimaux**, souvent séparés par des deux-points ou des tirets :

- Exemple : 00:1A:2B:3C:4D:5E

Comment fonctionne une adresse MAC ? En gros, lorsqu'un appareil se connecte à un réseau local (Wi-Fi ou filaire) :

- Le routeur ou le switch utilise l'adresse MAC pour identifier l'appareil;
- Une table appelée ARP (*Address Resolution Protocol*) associe les adresses MAC aux adresses IP sur le réseau local.
- Grâce à cette association, les appareils d'un même réseau peuvent communiquer entre eux avant d'envoyer les données sur Internet.

On pourrait dire que si l'adresse IP est l'adresse postale, l'adresse MAC est le numéro unique de votre boîte aux lettres. Ça va jusque là ? Pas trop sorcier hein ?

Le spoofing d'adresse MAC : quand les règles sont détournées 😳 hoooo…Scary!

Le **MAC spoofing** consiste à **modifier l'adresse MAC d'un appareil pour se faire passer pour un autre**. Pourquoi ? Les raisons varient, allant du simple contournement de restrictions réseau… à des activités bien moins éthiques. Pourquoi quelqu'un ferait-il du spoofing MAC ?

Contourner des restrictions réseau

Certains réseaux Wi-Fi restreignent l'accès à certaines adresses MAC autorisées. En changeant son adresse MAC, un appareil non autorisé peut se faire passer pour un appareil légitime.

Renforcer l'anonymat

Certaines entreprises ou gouvernements suivent les adresses MAC pour tracer les utilisateurs. En modifiant cette adresse, il devient plus difficile d'être suivi.

Éviter le filtrage MAC

Certains pare-feux ou systèmes de contrôle parental bloquent l'accès à Internet pour certains appareils via leur adresse MAC. Le spoofing permet de contourner ces restrictions! Hey oui, surprise!

Attaques malveillantes

Un attaquant pourrait usurper l'adresse MAC d'un autre appareil sur le réseau pour intercepter des données (attaque **Man-in-the-Middle**), perturber le réseau ou accéder à des ressources protégées. Ce n'est pas garantie que ça fonctionne car ça dépend de la configuration du routeur et autres éléments. Et, conservez en tête qu'en sécurité informatique il n'y a JAMAIS rien de garantie!

Comment fonctionne le spoofing MAC ?

Le processus est simple et peut être fait avec des commandes basiques sur un ordinateur :

Sous Windows

- Ouvrir le Gestionnaire de périphériques.
- Trouver la carte réseau.
- Aller dans "Propriétés" → "Avancé" → Modifier l'adresse MAC.

C'est aussi simple que ça… ce qui montre pourquoi **les réseaux doivent se méfier des adresses MAC**.

Comment se protéger contre le spoofing MAC ?

Les administrateurs réseau ont plusieurs options pour empêcher ou détecter ce genre de manipulation :

Filtrage MAC avancé

- Bloquer les adresses MAC suspectes ou restreindre l'accès à une liste d'adresses MAC autorisées; c'est ce qu'on appelle un *white list* (même si ça peut être contourné);
- Surveillance du réseau (ARP *Monitoring*);
- Utiliser des outils comme ***ARPwatch*** pour détecter des changements suspects d'adresses MAC sur un réseau.

Utiliser le 802.1X et l'authentification réseau

Ce protocole oblige les appareils à s'authentifier avant d'accéder au réseau, rendant le spoofing plus difficile. Ça permet d'aider à détecter des adresses MAC clonées. Certains systèmes d'analyse réseau peuvent identifier si plusieurs appareils utilisent la même adresse MAC sur le réseau. Activer le port *security* sur les switches peut également aider.

Sur des réseaux professionnels, des commutateurs peuvent limiter le nombre d'adresses MAC par port, limitant les possibilités d'usurpation.

Conclusion : une question d'identification et de sécurité

Les **adresses IP et MAC** sont essentielles pour la communication des appareils sur un réseau, mais elles ne sont pas infaillibles. L'**usurpation d'adresse MAC (MAC *spoofing*)** est une technique courante utilisée pour contourner certaines restrictions ou mener des attaques malveillantes. Heureusement, il existe des solutions pour limiter ces risques et aider à sécuriser les réseaux.

Que vous soyez un passionné de cybersécurité ou un simple curieux, retenir ces concepts vous aidera à mieux comprendre comment fonctionne Internet… et à éviter quelques pièges !

Tous droits réservés – https://29a.ca – Patrick Sentinel @ 2025
