DHCP l'outil confortable pour l'administrateur

Le Dynamic Host Configuration Protocol (DHCP) facilite la configuration du réseau : aujourd'hui, plutôt que de configurer individuellement chaque client, PC, smartphone ou appareil compatible, on préfère généralement faire appel au DHCP. Les différents participants au réseau obtiennent leur adresse IP, les masques de sous-réseau et d'autres informations via un serveur. Cela permet non seulement de faciliter le **travail avec de vastes réseaux**, mais aussi de réduire les sources d'erreur : l'attribution des adresses s'effectuant de façon dynamique, il est impossible que deux appareils se voient attribuer la même adresse IP. Cela réduit également l'espace d'adressage nécessaire : si l'appareil se déconnecte du réseau, l'adresse IP peut être automatiquement libérée pour un nouveau participant au réseau.

Malheureusement, ce raccourci constitue également une **porte d'entrée pour les cybercriminels**. Lorsque l'on compte sur quelqu'un d'autre pour faire le travail, on perd en contrôle. Certaines choses, dont on n'a absolument pas conscience, peuvent alors se dérouler en arrière-plan. Il en va de même pour le DHCP. Fort heureusement, il existe une solution : il est possible de lutter contre cette utilisation abusive du DHCP avec le DHCP snooping.

1. Exemples d'attaques par DHCP

L'objectif d'une attaque par insuffisance de resources DHCP est de créer un déni de service (DoS) pour connecter les clients. Les attaques par insuffisance des ressources DHCP reposent sur un outil d'attaque, par exemple, Gobbler. Rappelez-vous que les attaques d'insuffisance DHCP peuvent être efficacement atténuées en utilisant **la sécurité des ports** car Gobbler utilise une adresse MAC source unique pour chaque demande DHCP envoyée.

Cependant, l'atténuation des attaques d'usurpation DHCP nécessite plus de protection. Gobbler peut être configuré pour utiliser l'adresse MAC de l'interface réelle comme adresse Ethernet source, mais indiquer une adresse Ethernet différente dans la charge utile DHCP. Cela rendrait la sécurité du port inefficace car l'adresse MAC source serait légitime.

Les attaques d'usurpation DHCP peuvent être atténuées en utilisant **l'espionnage DHCP** sur les ports approuvés.

2. Espionnage (snooping) DHCP

2.1. À quoi sert le DHCP snooping ?

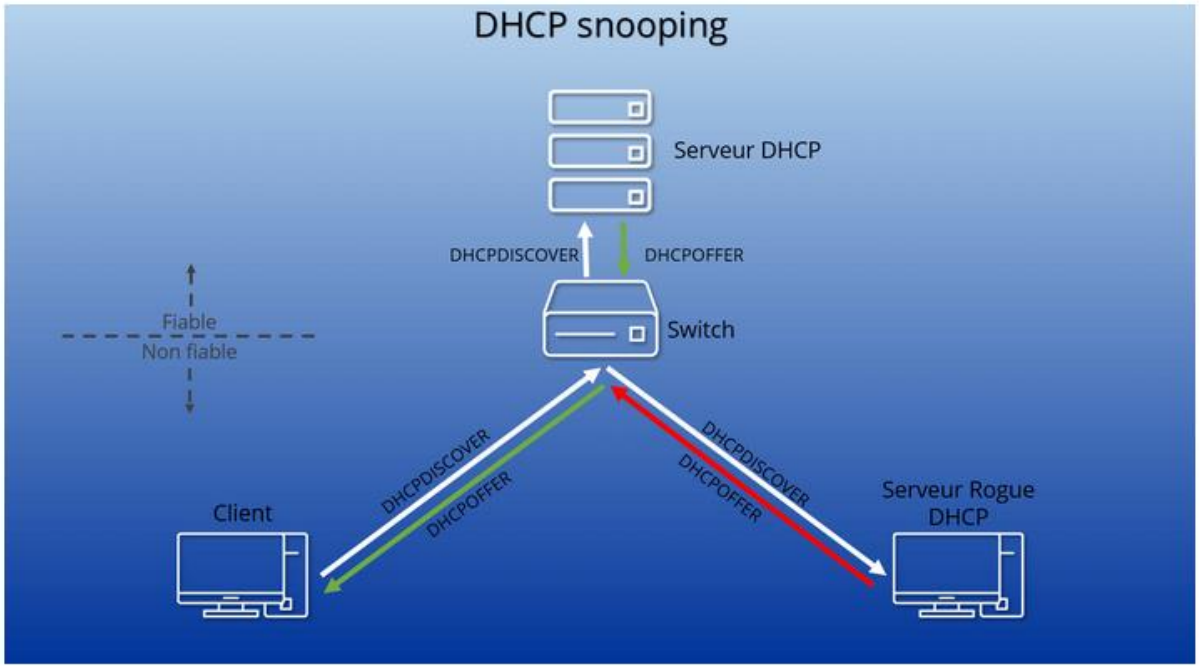
Le **DHCP snooping** est une fonction de sécurité intervenant au deuxième niveau du modèle OSI. Cette fonction est intégrée dans le commutateur connectant les clients aux serveurs **DHCP**. En d'autres termes, il s'agit d'un protocole qui contrôle tout d'abord l'ensemble des informations **DHCP** passant par le commutateur.

Dans le cadre du DHCP, un serveur est chargé de la configuration des différents clients. Pour ce faire, le client envoie tout d'abord une requête au réseau par broadcast. Le participant au réseau entend ainsi déterminer quels serveurs DHCP sont disponibles et peuvent répondre. Tous les serveurs DHCP disponibles répondent à cette requête. Si plusieurs serveurs sont activés au sein du réseau, le client choisit **la première réponse qui lui est parvenue**. Le client procède ensuite à l'attribution des adresses à l'aide de ce serveur DHCP. C'est ici que se trouve le point faible du système, la porte d'entrée des cybercriminels.

Il est possible d'intégrer d'autres serveurs (qu'on appelle **serveur DHCP non autorisé**) dans le réseau. Lorsqu'un serveur de ce type parvient à répondre au client en premier, le participant au réseau reçoit les informations de configuration via le serveur nuisible. Le serveur DHCP non autorisé envoie alors des données erronées et manipulées. Le client est donc paramétré de façon erronée. Il est ainsi possible d'effectuer **un DHCP-Spoofing (« usurpation DHCP »)**, c'est-à-dire de piloter le client vers une fausse passerelle. À travers cette passerelle, les cybercriminels peuvent intercepter le transfert des données et obtenir des informations sensibles. Ce type d'attaque est surnommée **« man in the middle attack »** ou **attaque de l'homme du milieu**. Une attribution d'adresse erronée peut en revanche entraîner une **« Denial of service attack »** ou **attaque par déni de service (DoS ou Saturation du service)** : l'intégralité du réseau est alors paralysée. Le DHCP snooping empêche toute prise de contact avec des serveurs nuisibles.

2.2. Expliquons avec un schéma :

Un serveur DHCP non autorisé peut recevoir le paquet DHCPDISCOVER (la requête du client visant à obtenir un serveur DHCP) puisqu'il surveille le broadcast. Il peut aussi envoyer un paquet DHCPOFFER (la réponse à la recherche), mais ce paquet n'atteindra jamais le client. Placé dans le commutateur, le DHCP snooping identifie le fait que le paquet **ne provient pas d'un serveur digne de confiance** et contient de fausses informations et procède donc au blocage de la transmission.



Avec le DHCP snooping, le commutateur empêche toute participation d'un serveur DHCP non autorisé à l'attribution des adresses.

2.3. Ports dignes de confiance

Pour garantir que seuls les serveurs fiables puissent intervenir dans l'attribution d'informations de configuration, le DHCP snooping procède en plusieurs étapes. Dans un premier temps, il détermine un port de confiance pour le serveur ou les serveurs propres. **Tous les autres appareils essayant d'accéder au réseau via un autre port sont considérés comme non dignes de confiance**. Tous les clients en font également partie. Cela implique donc qu'un hôte sur lequel tourne un serveur DHCP mais qui n'est pas approuvé par l'administrateur sera considéré comme non digne de confiance. Mais si un paquet DHCP ne pouvant être envoyé que par un serveur (DHCPOFFER, DHCPACK, DHCPMAK) arrive par le biais d'un

port qui n'est pas digne de confiance, **le commutateur bloque la transmission**. Le client ne recevra pas l'information.

2.4. La DHCP snooping Binding Database

Néanmoins, un hacker peut également essayer de détruire le réseau en se faisant passer pour l'un des clients existants et en rejetant ces offres du serveur DHCP. C'est pourquoi le DHCP snooping utilise une **base de données créée et actualisée de façon autonome par le système**. Le protocole lit toutes les informations DHCP (mais pas les données effectives après la réussite de la connexion) et en extrait des détails pour la DHCP snooping Binding Database.

Le système enregistre dans la base de données tous les hôtes ne passant pas par un port digne de confiance. Les informations accumulées comprennent l'**adresse MAC**, l'**adresse IP** attribuée, le **port du commutateur** utilisé, le sous-réseau logique (**VLAN**) et la durée du **Lease Time**. Le DHCP snooping peut ainsi garantir que seuls les clients originaux ayant participé à la communication peuvent envoyer des ordres au serveur, car l'adresse MAC et le port du commutateur de l'appareil ne coïncident avec les informations enregistrées dans la base de données que pour ces clients originaux.

2.5. Fichiers journaux

Certains périphériques réseau peuvent par ailleurs établir un rapport sur le processus de défense dans le cadre du DHCP. Il est possible de se faire envoyer les fichiers journaux (logs) et de les analyser. La procédure **distingue deux erreurs dans cette documentation** : d'une part, le décalage entre l'adresse MAC actuelle et les informations enregistrées dans la base de données et, d'autre part, les paquets de serveur envoyés via un port qui n'est pas digne de confiance.

Le premier type de messages d'erreur provient la plupart du temps d'une mise en œuvre erronée de certains aspects du réseau dans un appareil client et ne constitue pas, en général, une source d'inquiétude. Le second type de messages d'erreur **renvoie quant à lui aux intentions criminelles** : quelqu'un a délibérément tenté d'infiltrer le réseau avec un serveur DHCP non autorisé. Comme le DHCP snooping enregistre tout, il est possible de procéder à des enquêtes ciblées sur de tels incidents de sécurité.

Attention :

Des serveurs DHCP peuvent s'infiltrer dans le réseau sans que vous en ayez connaissance. Ces faux serveurs DHCP (les « spurious DHCP serveur ») peuvent cependant être détectés par un raté sous la forme du paquet DHCPDISCOVER, car le serveur nuisible répond à la requête et se dévoile de cette façon.

Remarque :

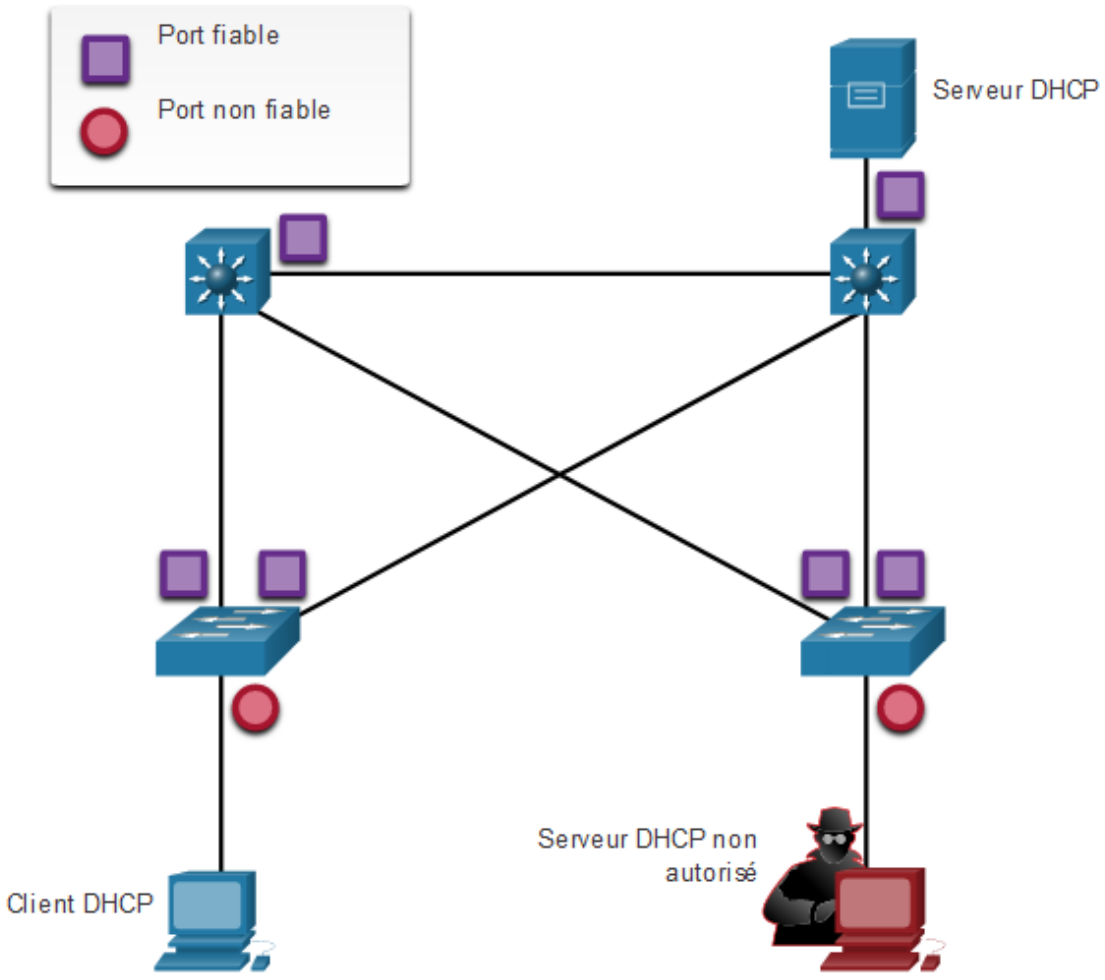
Dans la plupart des réseaux domestiques (LAN ou WLAN), la fonction de serveur DHCP est assumée par un routeur. Cela ne nous prémunit pas contre le danger que représente le DHCP-Spoofing, car chaque appareil peut en principe devenir un serveur DHCP. Les cybercriminels peuvent par exemple infiltrer un ordinateur portable dans le réseau local sans fil et contrôler l'attribution des adresses de cette façon.

Cependant le DHCP snooping ne protège pas uniquement des actes criminels, mais aussi des **sources d'erreur** causées par l'utilisation irréfléchie de routeurs supplémentaires. Si un nouveau routeur est intégré dans un réseau existant, il peut dérégler le DHCP : le nouveau routeur attribue alors des adresses qu'il ne devrait pas attribuer, pouvant ainsi entraîner des erreurs de connexion. Dans un contexte d'entreprise notamment, des problèmes peuvent survenir lorsque les employés intègrent leurs propres appareils dans le réseau sans en informer l'administrateur réseau.

3. Le DHCP snooping : de quoi s'agit-il ?

L'espionnage DHCP ne dépend pas des adresses MAC source. Au lieu de cela, l'espionnage DHCP détermine si les messages DHCP proviennent d'une source de confiance ou non approuvée configurée administrativement. Il filtre ensuite les messages DHCP et limite la fiabilité du trafic DHCP de sources qui ne sont pas approuvé.

Les périphériques sous contrôle administratif (par exemple, les commutateurs, les routeurs et les serveurs) sont des sources fiables. Tout appareil placé en dehors le pare-feu ou en dehors de votre réseau est une source non fiable. Par ailleurs, tous les ports d'accès sont généralement traités comme des sources non fiables. La figure montre un exemple de ports approuvés et non approuvés.



Notez que le serveur DHCP rouge serait sur un port non approuvé après avoir activé l'espionnage DHCP. Toutes les interfaces sont traitées comme non fiables par défaut. Les interfaces approuvées sont généralement des liaisons de trunc et des ports directement connectés à un serveur DHCP légitime. Ces interfaces doivent être explicitement configurées comme approuvées.

Une table DHCP est créée qui inclut l'adresse MAC source d'un périphérique sur un port non approuvé et l'adresse IP attribuée par le serveur DHCP à ce périphérique. L'adresse MAC et l'adresse IP sont liées ensemble. Par conséquent, cette table est appelé table de liaison d'espionnage DHCP.

4. Étapes pour implémenter l'espionnage DHCP

Utilisez les étapes suivantes pour activer l'espionnage DHCP (snooping):

Étape 1. Activez l'espionnage DHCP à l'aide de la commande de configuration globale **ip dhcp snooping**.

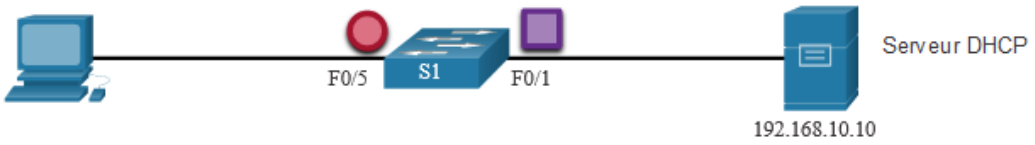
Étape 2. Sur les ports approuvés, configurez l'interface avec la commande **ip dhcp snooping trust**.

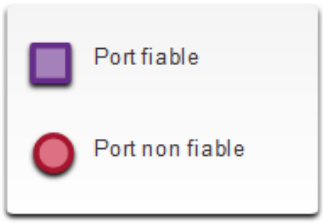
Étape 3: Limitez le nombre de messages de découverte DHCP pouvant être reçus par seconde sur les ports non approuvés à l'aide de la commande de configuration d'interface **ip dhcp snooping limit rate**.

Étape 4. Activez la surveillance DHCP par VLAN ou par une plage de VLAN à l'aide de la commande de configuration globale **ip dhcp snooping** *vlan*.

5. Exemple de configuration de l'espionnage DHCP:

La topologie de référence pour cet exemple d'espionnage DHCP est illustrée dans la figure. Notez que F0 / 5 est un port non approuvé car il se connecte à un PC. F0 / 1 est un port approuvé car il se connecte au serveur DHCP.





Voici un exemple de configuration de l'espionnage DHCP sur S1. Remarquez comment l'espionnage DHCP est activée pour la première fois. Alors l'interface en amont du serveur DHCP est explicitement approuvée. Ensuite, la gamma de ports FastEthernet de F0 / 5 à F0 / 24 n'est pas approuvée par défaut, donc une limite de débit est fixée à six paquets par seconde. Enfin, l'espionnage DHCP est activée sur les VLANS 5, 10, 50, 51 et 52.

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if-range)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

Utilisez la commande EXEC privilégiée **show ip dhcp snooping** pour vérifier la surveillance DHCP et **show ip dhcp snooping binding** pour afficher les clients qui ont reçu des informations DHCP, comme illustré dans l'exemple.

Remarque: l'espionnage DHCP est également requis par l'inspection ARP dynamique (DAI), qui est le sujet suivant

```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet0/1            yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/5            no         no              6
  Custom circuit-ids:
FastEthernet0/6            no         no              6
  Custom circuit-ids:
S1# show ip dhcp snooping binding
MacAddress         IpAddress       Lease(sec) Type          VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
00:03:47:B5:9F:AD  192.168.10.11   193185     dhcp-snooping 5    FastEthernet0/5
```