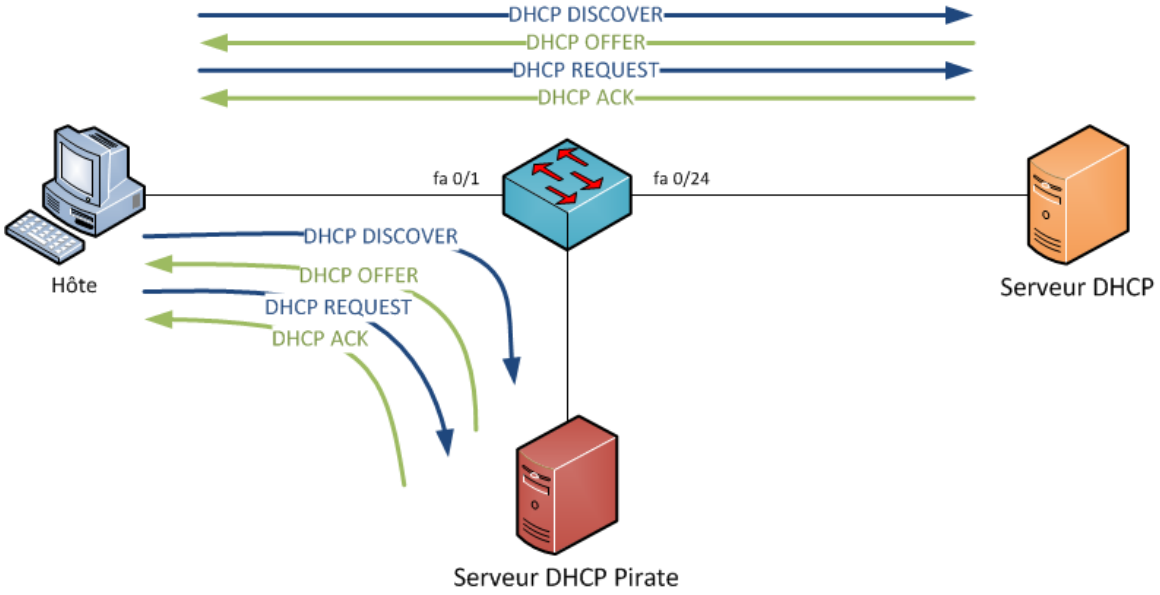
DHCP spoofing

DHCP Snooping : La parade au Spoofing DHCP

Vous avez dit DHCP Spoofing ?

Il s'agit d'**usurpation DHCP**. Le pirate informatique va tout simplement, au cours de la récupération d'une adresse IP, vous donner de mauvaises informations. Ceci va lui permettre, par exemple, de rediriger tout votre trafic vers sa machine *(afin de récupérer des informations sur vous comme vos coordonnées bancaires ou autre)* ou encore de rediriger le trafic de centaines de machines sur une seule et même cible *(dans le but de rendre non-fonctionnelle cette dernière)*.

Ajout d'un serveur DHCP Pirate. Lors du **DHCP Discover** de votre ordinateur celui-ci répond également ce qui le rend éligible entant que serveur, il pourrait donc fournir des données faussées à votre machine.



En mettant en place le DHCP Snooping vous pouvez limiter les attaques.

Afin d'empêcher le DHCP Spoofing, l'idée est de préciser où trouver les bons serveurs DHCP. Pour cela, nous allons travailler sur le **switch** *(= commutateur)* et préciser sur quelles interfaces trouver les serveurs DHCP authentiques. Sur l'exemple vu un peu plus haut on peut voir que le serveur DHCP est raccordé au port ***fa 0/24*** du switch. L'idée est de spécifier que cette interface est un port dit "**trusted**" *(= port de confiance)*. Ainsi, les ports "**trusted**" pourront emmètre des requêtes **DHCP Offer** et **DHCP Ack** alors que l'équipement du pirate informatique ne sera pas sur une interface de confiance *(= unstrusted)*. Ses requêtes seront alors ignorées.
Ce procédé est appelé **DHCP Snooping** *(= surveillance DHCP)*.

Mise en place sur des équipements CISCO

Le **DHCP Snooping** peut fonctionner de manière globale sur l'ensemble du switch *(et donc sur l'ensemble de ses ports)* mais aussi dans un **VLAN** particulier.
Voici la marche à suivre pour la mise en place sur des équipements de type CISCO :

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan X
Switch(config)# ip dhcp snooping information option
Switch(config)# interface fastethernet0/24
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate X
```

1. Mise en place du DHCP Snooping sur le switch *(de façon globale)*

Mise en place du DHCP Snooping sur un VLAN en particulier

---

2. Activation de l'**option 82**
3. On sélectionne l'interface fa 0/24 pour la configurer
4. On déclare le port en tant qu'interface de confiance
5. Permet de définir le maximum de requêtes que l'interface traitera *(en seconde)*

Quelques conseils en sécurité

Afin de garantir la sécurité sur votre réseau et éviter ce genre d'attaques voici quelques conseils :

- Restreindre le nombre d'adresses MAC autorisées par interface sur vos switch
- Désactiver les interfaces non utilisées sur vos équipements *(afin d'éviter que n'importe qui puisse se raccorder sur votre réseau)*
- Assigner des adresses IP fixes sur vos serveurs
- Si vous êtes sur un réseau à petite échelle, mettre l'ensemble du parc en IP fixe
- Différencier les services DHCP *(un dédié pour les clients Wifi, un pour le réseau classique...)*

Documentation Cisco

L'option 82

- When you enable the DHCP snooping information option 82 on the switch, this sequence of events occurs:
- • The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- • When the switch receives the DHCP request, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote-ID suboption) and the port identifier, **vlan-mod-port** from which the packet is received (the circuit-ID suboption).
- • If the IP address of the relay agent is configured, the switch adds the IP address in the DHCP packet.
- • The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
- • The DHCP server receives the packet. If the server is option-82 capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.
- • The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch verifies that it originally inserted

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface fastethernet0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```