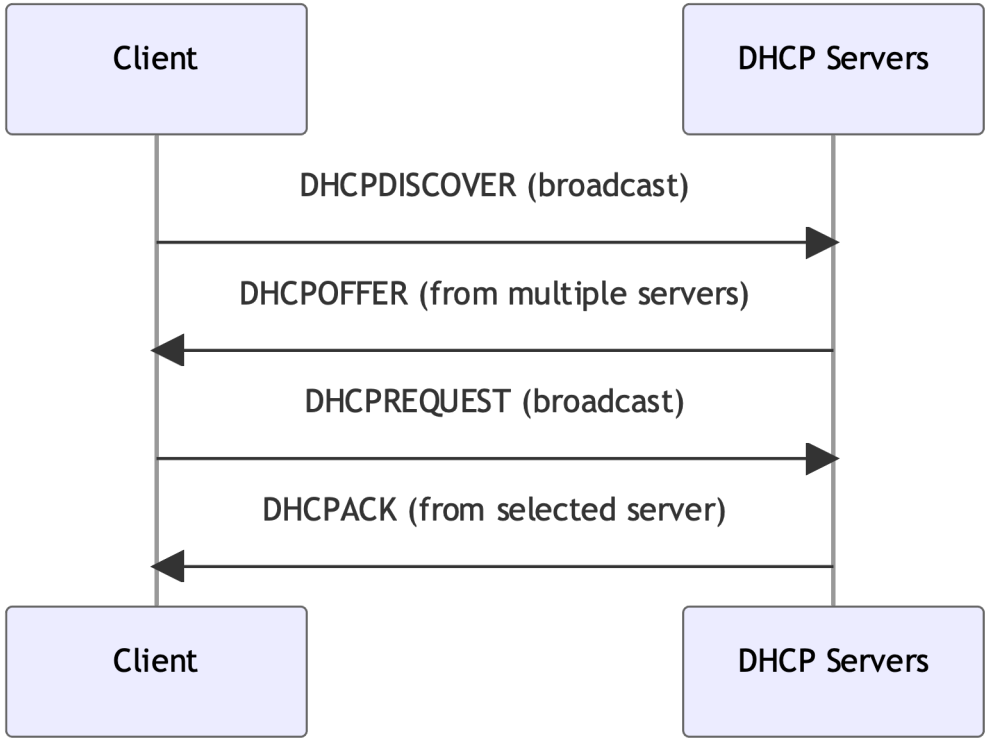
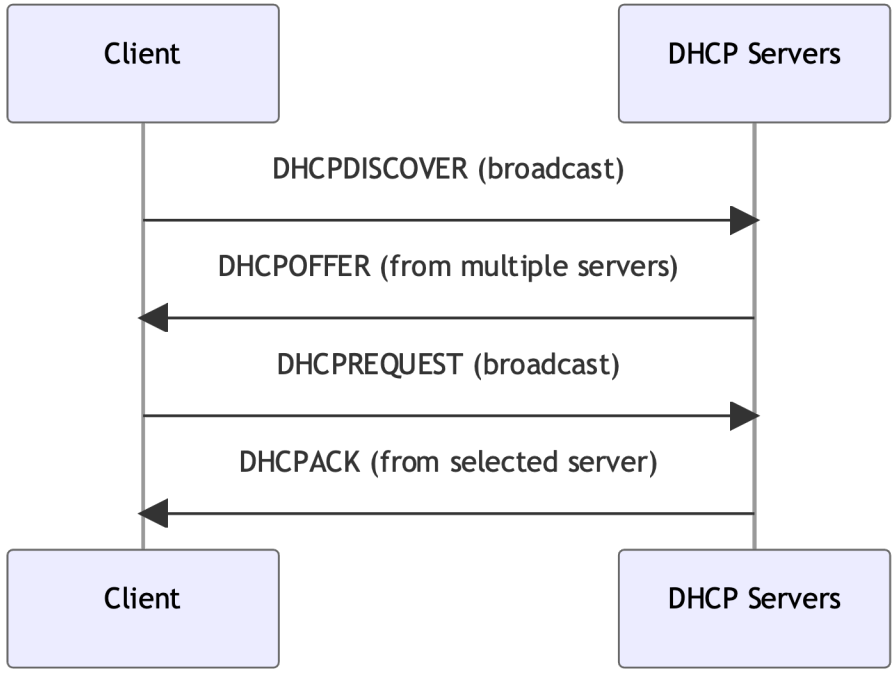
LE PROTOCOLE DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) est utilisé pour attribuer automatiquement des adresses IP et d'autres paramètres réseau à des dispositifs dans un réseau. Le processus DHCP se déroule en quatre étapes principales, souvent appelées DORA (pour Discover, Offer, Request, Acknowledge). Voici une explication détaillée de ces étapes :





1.Discover (Découverte) :

1. Lorsqu'un client souhaite obtenir une configuration réseau via DHCP, il commence par envoyer un paquet DHCPDISCOVER. Ce paquet est envoyé en broadcast, car le client ne connaît pas l'adresse du serveur DHCP.
2. Le paquet DHCPDISCOVER signale que le client recherche un serveur DHCP pour obtenir une adresse IP.

2. Offer (Offre) :

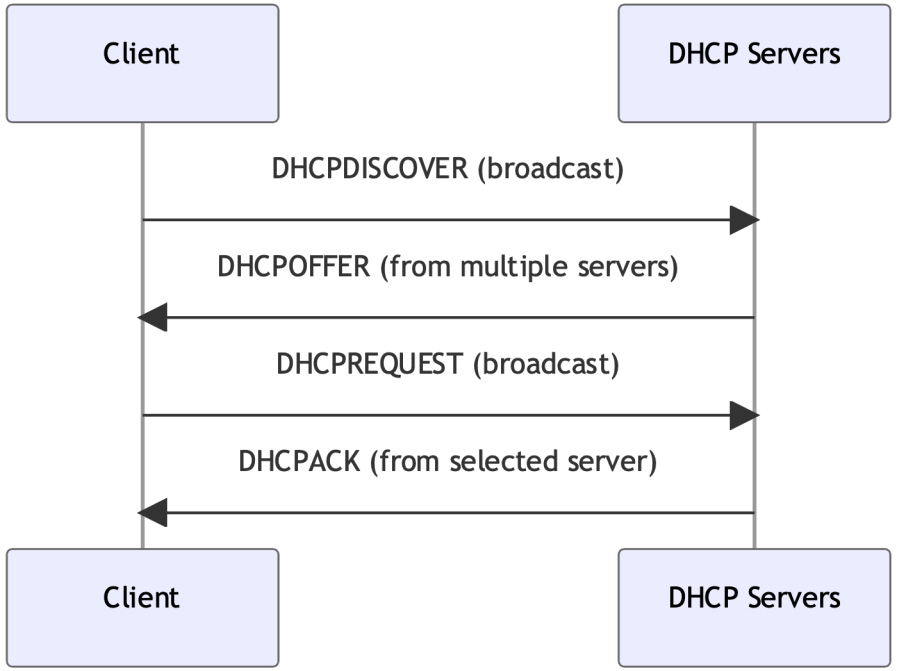
1. Tous les serveurs DHCP qui reçoivent le paquet DHCPDISCOVER répondent avec un paquet DHCPOFFER. Ce paquet contient une adresse IP que le serveur propose d'attribuer au client, ainsi que d'autres paramètres de configuration tels que le masque de sous-réseau, la passerelle par défaut et les serveurs DNS.
2. Si plusieurs serveurs DHCP sont présents sur le réseau, le client peut recevoir plusieurs offres. Dans ce cas, le client choisit généralement la première offre qu'il reçoit.

3. Request (Demande) :

1. Une fois qu'une offre a été choisie, le client envoie un paquet DHCPREQUEST en broadcast pour informer tous les serveurs DHCP qu'il accepte une offre spécifique. Ce paquet contient l'adresse IP de l'offre acceptée.
2. Les serveurs DHCP qui ont fait des offres non acceptées retirent simplement leurs offres et retournent les adresses IP proposées dans le pool d'adresses disponibles.

4. Acknowledge (Accusé de réception) :

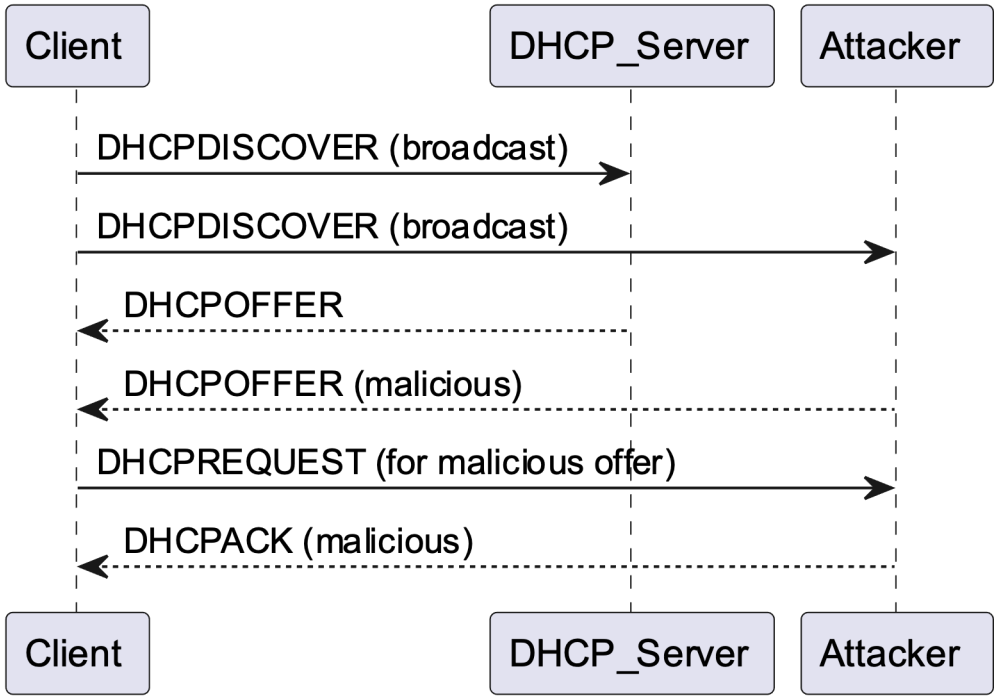
1. Le serveur DHCP qui a fait l'offre acceptée répond avec un paquet DHCPACK, confirmant que le client peut utiliser l'adresse IP proposée. Ce paquet contient également la durée de bail de l'adresse IP, c'est-à-dire la durée pendant laquelle le client peut utiliser cette adresse.
2. Si, pour une raison quelconque, l'adresse IP proposée n'est plus valide ou si l'offre a été retirée, le serveur peut envoyer un paquet DHCPNAK (Negative Acknowledgment) pour informer le client que l'adresse ne peut pas être utilisée.



Après avoir reçu le DHCPACK, le client configure son interface réseau avec l'adresse IP et les autres paramètres fournis. Lorsque la durée du bail est sur le point d'expirer, le client entame un nouveau processus DHCP pour renouveler ou obtenir une nouvelle adresse IP.

Il est à noter que le protocole DHCP contient d'autres messages et fonctionnalités (comme le renouvellement, la libération, etc.), mais les étapes DORA sont les étapes fondamentales pour obtenir une adresse IP via DHCP.

DHCP SPOOFING



Dans ce scénario, un attaquant (spoofing) répond à la requête DHCPDISCOVER du client avec une offre malveillante avant que le serveur DHCP légitime ne puisse répondre.

Le client accepte ensuite l'offre malveillante et l'attaquant confirme avec un DHCPACK malveillant.

DHCP SPOOFING

Le DHCP spoofing, également connu sous le nom de DHCP poisoning, est une attaque où un attaquant répond à des requêtes DHCP avec l'intention de fournir des adresses IP et d'autres configurations réseau malveillantes. Dans un scénario typique de DHCP spoofing, le DHCP OFFER malveillant est accepté par le client dans les situations suivantes :

Réponse la plus rapide : Si l'attaquant est physiquement plus proche du client ou si son réseau est plus rapide, sa réponse malveillante (DHCPOFFER) peut arriver au client avant la réponse du serveur DHCP légitime. Les clients DHCP acceptent généralement la première offre qu'ils reçoivent.

Inondation du réseau : L'attaquant peut inonder le réseau avec un grand nombre de requêtes DHCP, épuisant ainsi le pool d'adresses IP du serveur DHCP légitime. Une fois que toutes les adresses IP sont épuisées, le serveur DHCP légitime ne peut plus répondre aux nouvelles requêtes, permettant à l'attaquant de répondre à la place.

Désactivation du serveur DHCP légitime : Dans une attaque plus agressive, l'attaquant pourrait désactiver le serveur DHCP légitime, soit par une attaque DoS, soit en exploitant une vulnérabilité du serveur.

DHCP SPOOFING

Les conséquences d'une attaque MITM via DHCP spoofing peuvent être graves. L'attaquant peut rediriger le trafic vers des sites web malveillants, intercepter des informations sensibles, injecter du contenu malveillant dans les sessions de navigation, entre autres.

Pour se protéger contre les attaques MITM, il est recommandé d'utiliser des protocoles de communication sécurisés (comme HTTPS), d'activer des fonctionnalités de sécurité comme le DHCP snooping sur les équipements réseau, et d'éduquer les utilisateurs à reconnaître et à éviter les contenus et les sites web suspects.

DHCP SPOOFING

Le DHCP snooping est une fonctionnalité de sécurité disponible sur de nombreux commutateurs (switches) modernes. Elle permet de filtrer et de contrôler les réponses DHCP sur le réseau, empêchant ainsi les attaques DHCP spoofing. L'activation du DHCP snooping varie en fonction du fabricant et du modèle du commutateur. Voici une procédure générale pour activer le DHCP snooping sur un switch Cisco :

Activez le DHCP snooping globalement :

```
switch(config)# ip dhcp snooping
```

Configurez les interfaces de confiance : Les interfaces de confiance sont celles par lesquelles vous attendez des réponses DHCP légitimes (généralement, les interfaces connectées à vos serveurs DHCP). Sur ces interfaces, vous devez configurer le switch pour qu'il fasse confiance aux réponses DHCP entrantes.

```
switch(config)# interface [type numéro]
switch(config-if)# ip dhcp snooping trust
```

Enregistrez la configuration :

```
switch(config)# end
switch# write memory
```

Vérifiez la configuration : Pour vérifier que le DHCP snooping est correctement configuré, utilisez la commande :

```
switch# show ip dhcp snooping
```