DHCP Dynamic Host Configuration Protocol

Le protocole DHCP est un protocole réseau utilisé pour attribuer automatiquement des adresses IP et d'autres informations de configuration réseau (comme une passerelle par défaut ou les serveurs DNS).

Le processus se fait en 4 étapes principales, appelé le **DORA** :

Discover : Le client envoie une requête pour trouver un serveur DHCP.

Offer : Le serveur DHCP répond avec une proposition d'adresse IP

Request : Le client accepte l'offre en envoyant une demande officielle.

Acknowledge : Le serveur confirme l'attribution de l'adresse IP.

Exemple : Un pc se connecte au réseau -> il n'a pas d'IP -> il envoie un DHCPDISCOVER -> le serveur propose une IP -> le pc accepte -> le serveur confirme -> le pc a une IP valide

Ce protocole a plusieurs avantages comme :

- La réduction des erreurs de configuration

- Gain de temps

- Permet une meilleure gestion des IP dans les grands réseaux et évite les conflits d'adresse

- Attribution automatique des adresses IP

- Il permet aussi le nom de domaine

Le DHCP peut fonctionner de 3 façons :

1. Dynamique : attribution automatique d'une IP à partir d'une plage.
2. Automatique : Attribution d'une IP fixe mémoriser pour un client
3. Manuelle : Attribution d'un IP précise en fonction de l'adresse MAC du client

Le serveur DHCP peut-être une box internet, un routeur, un serveur dédié, le port utilisé pour le serveur DHCP est **67** et le port du client DHCP **68**.

Les inconvénients sont que si le serveur est indisponible les clients n'ont plus d'IP et peut etre utilisé pour des attaques Rogue DHCP qui consiste à intégrer un faux serveur DHCP malveillant qui fonctionne sur un réseau. Il peut attribuer de fausses IP ou de mauvaises informations réseau aux clients. Quand un appareil se connecte il envoie une requête DHCP comme montré plus haut, si plusieurs serveurs répondent il peut accepter l'offre du serveur malveillant. Et la l'appareil est vulnérable à plusieurs attaques comme le phising, redirection, Man in the middle…

Pour s'en protéger il faut activer le DHCP Snooping sur les switchs managés (bloque les DHCP non autorisés).

Filtré les ports ou un DHCP ne doit pas apparaitre.

Et sur les grands réseaux n'autoriser qu'un seul serveur DHCP officielle.