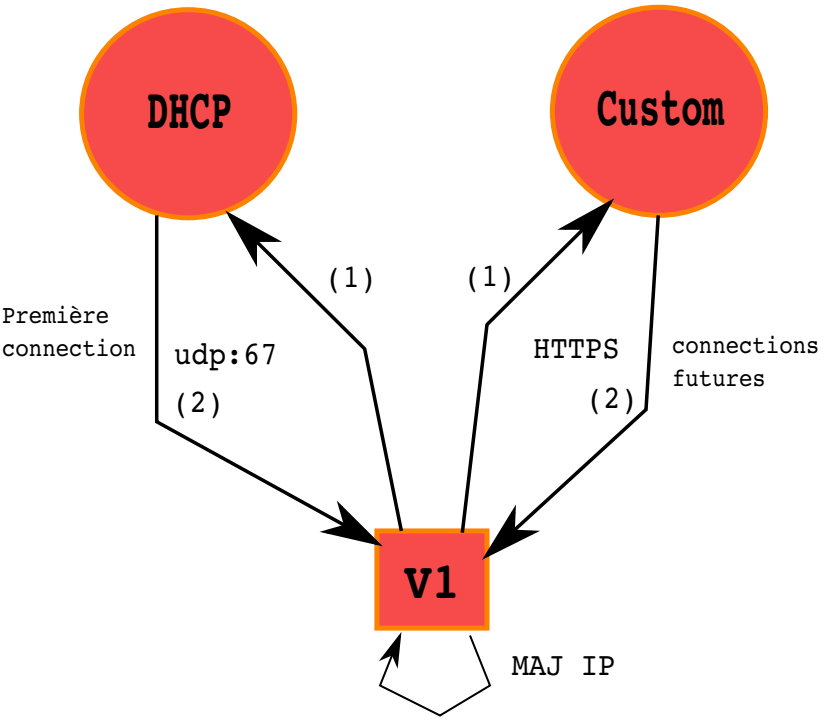
Personne connecté sur le réseau =
- Une voiture légitime.
- Une voiture légitime d'un attaquant avec un "sniffer" de réseau interceptant toutes les communications.

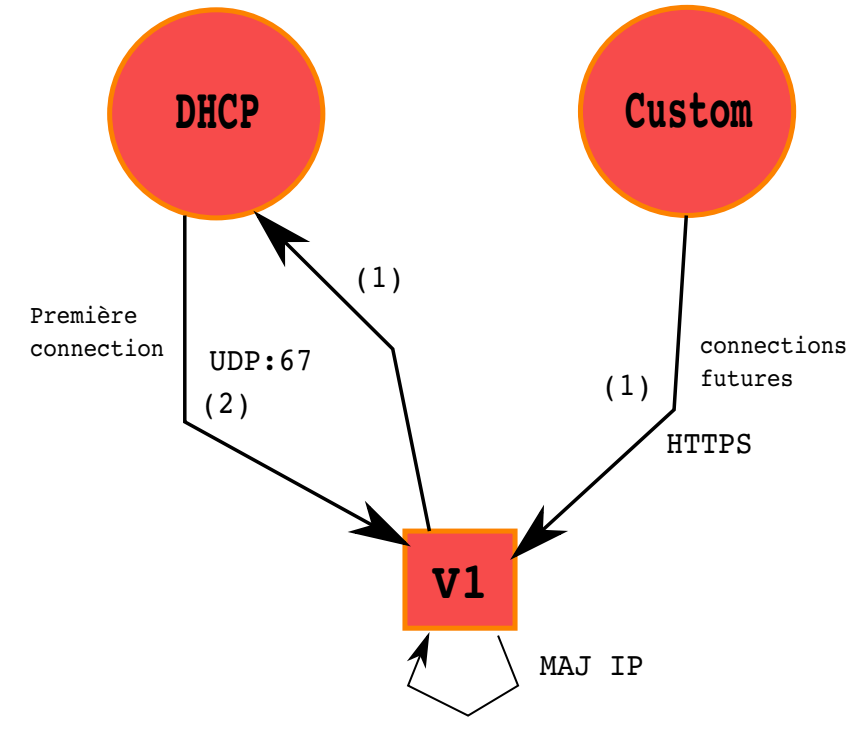


Possible si méchanismes de demande de changement d'addresse IP.
(Pour l'instant pas existant et pas testable)

Première connection (allumage de la voiture):

- Communication non cryptée (**HTTP**) avec le serveur DHCP pour obtenir une première adresse IP.
- Visible de toute personne connectée sur le réseau

Renouvellement adresse IP (apres X temps) :
- Communication crypté (**HTTPS**) pour réclamer une nouvelle adresse au serveur DHCP.
- Le serveur communique une nouvelle adresse de façon crypté lui aussi.
- Mise à jour en dur dans le système de la nouvelle adresse.



Mise a jour de la durée de vie d'une adresse dans le serveur dhcp pour être fixe petite, utilie au MTD et viable dans le réseau.
Déjà existant

visible et testable,
openstack et wireshark

Première connection (allumage de la voiture):

- Communication non cryptée (**HTTP**) avec le serveur DHCP pour obtenir une première adresse IP.
- Visible de toute personne connectée sur le réseau

Renouvellement adresse IP (après fin de vie de l'adresse IP) :
- Le serveur cherche, trouve et attribue une nouvelle adresse
- Le serveur communique une nouvelle adresse de façon crypté (**HTTPS**) à la voiture.
- Mise à jour (en dur?) dans le système de la nouvelle adresse.