Mécanismes de configuration automatique d'une interface réseau, aspects sécurité

B. Amedro, V. Bodnartchouk, V.Robitzer

Juin 2005
Université de Nice - Sophia-Antipolis
Licence d'informatique 3ème année

Présentation du sujet

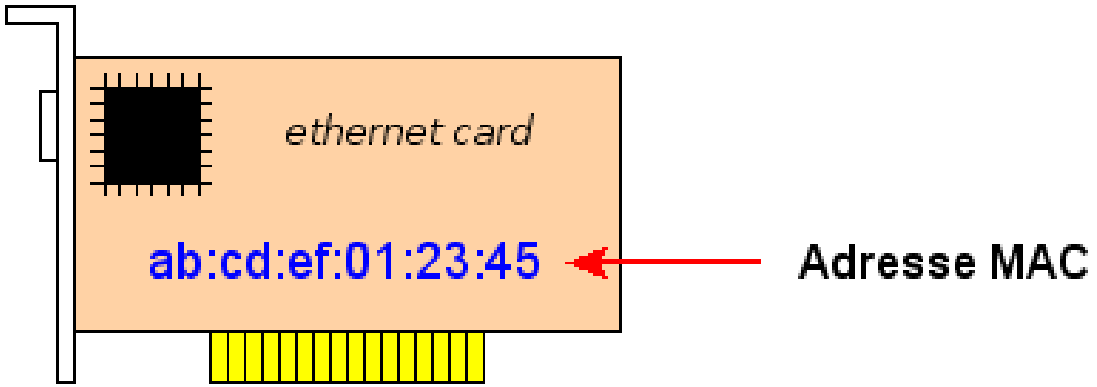
- Aujourd'hui, les réseaux constituent un domaine privilégié qui fournit à l'homme des services irremplaçables.
- Cependant, les mécanismes de configuration qui permettent à un ordinateur d'exister au sein d'un réseau, constituent une étape délicate, facilement exploitable par des utilisateurs malveillants.
- Il devient donc indispensable de compter sur des mécanismes entièrement automatisés et securisés.

Plan de la présentation

- Enjeux de la configuration (Vladimir)
- Protocoles existants (Vladimir)
- Le protocole DHCP (Vincent)
- Proposition d'un protocole securisé SDHCP (Brian)
- Conclusion (Vincent)

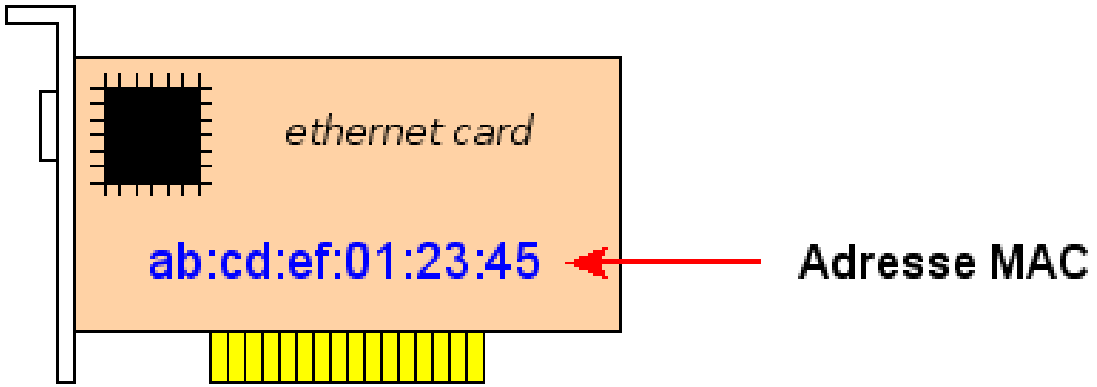
Pour exister dans un réseau :

- L'adresse physique (ou MAC)



Pour exister dans un réseau :

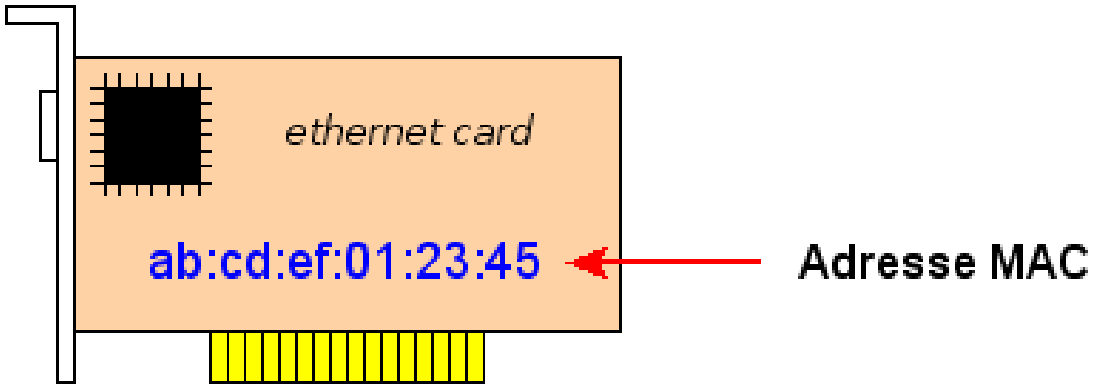
- L'adresse physique (ou MAC)



- L'adresse logique (ou IP)

Pour exister dans un réseau :

- L'adresse physique (ou MAC)



- L'adresse logique (ou IP)
- Autres paramètres (adresse de la passerelle ...)

La configuration manuelle

Le plus simple

Avoir toujours un technicien sous la main. (les côuts deviennent vite importants)

La configuration manuelle

Le plus simple

Avoir toujours un technicien sous la main. (les côuts deviennent vite importants)

Avant le déploiement

Une autre méthode est d'attribuer les paramètres avant le déploiement final du dispositif. (technique employée par "BeAtHome" pour des appareils ménagers commandés par Internet)

Problème dès qu'il y a déplacement de dispositif, nécessité d'automatisation.

Protocoles existants

Attribution statique :

- RARP
- BOOTP

Attribution dynamique :

- DHCP

Attribution automatique :

- AutoIP

Attribution statique d'adresses IP avec un serveur RARP

RARP (Reverse Address Resolution Protocol)
Historiquement, le premier protocole automatique permettant de retrouver une adresse.

Attribution statique d'adresses IP avec un serveur RARP

RARP (Reverse Address Resolution Protocol)
Historiquement, le premier protocole automatique permettant de retrouver une adresse.

Principe Le serveur fourni une IP si l'adresse MAC de le client est connue du serveur.

Attribution statique d'adresses IP avec un serveur RARP

RARP (Reverse Address Resolution Protocol)
Historiquement, le premier protocole automatique permettant de retrouver une adresse.

Principe Le serveur fourni une IP si l'adresse MAC de le client est connue du serveur.

Qualités Simplicité d'implémentation et d'utilisation.

Attribution statique d'adresses IP avec un serveur RARP

RARP (Reverse Address Resolution Protocol)
Historiquement, le premier protocole automatique permettant de retrouver une adresse.

Principe Le serveur fourni une IP si l'adresse MAC de le client est connue du serveur.

Qualités Simplicité d'implémentation et d'utilisation.

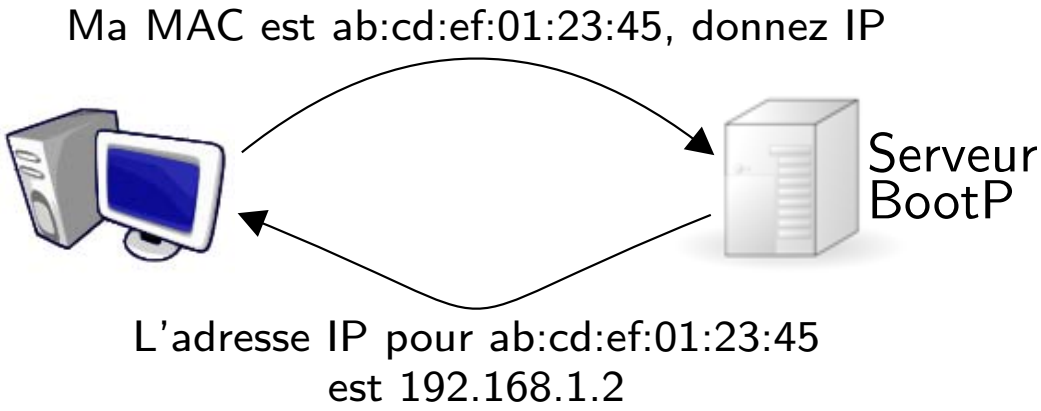
Inconvénients Permet uniquement de fournir l'adresse IP mais pas le masque de sous-réseau ni l'adresse de la passerelle.

Attribution statique d'adresses IP avec un serveur BOOTP

BOOTP (Bootstrap Protocol) Évolution de RARP, permet de configurer la passerelle et le sous-réseau. Conçu pour l'amorçage de terminaux sans disque dur.

Attribution statique d'adresses IP avec un serveur BOOTP

BOOTP (Bootstrap Protocol) Évolution de RARP, permet de configurer la passerelle et le sous-réseau. Conçu pour l'amorçage de terminaux sans disque dur.



Principe

Le client envoie un datagramme UDP au serveur, qui réponds avec les paramètres de configuration spécifiques du client.

Attribution statique d'adresses IP avec un serveur BOOTP

Qualités Peut fonctionner sur de grands réseaux grâce à l'Agent Relais BootP supporté par les routeurs. Peut inclure des infos spécifiques du fournisseur (typiquement sur la configuration du serveur proxy).

Attribution statique d'adresses IP avec un serveur BOOTP

Qualités Peut fonctionner sur de grands réseaux grâce à l'Agent Relais BootP supporté par les routeurs. Peut inclure des infos spécifiques du fournisseur (typiquement sur la configuration du serveur proxy).

Inconvénients Gaspillage d'adresses IP !

Attribution dynamique d'adresses IP avec le serveur DHCP

DHCP (Dynamic Host Configuration Protocol)
Évolution de BOOTP. Mécanisme de crédit-bail qui permet de contrôler le cycle de vie des adresses IP.

Attribution dynamique d'adresses IP avec le serveur DHCP

DHCP (Dynamic Host Configuration Protocol)
Évolution de BOOTP. Mécanisme de crédit-bail qui permet de contrôler le cycle de vie des adresses IP.

Principe L'administrateur doit attribuer un intervalle d'adresses IP exploitables.
Sera vu en détails par Vincent.

Attribution automatique d'adresses IP privées

Convention Les extensions du DHCP décrivent de nouvelles méthodes d'attribution d'adresses IP même si il n'y a pas de serveur.

Attribution automatique d'adresses IP privées

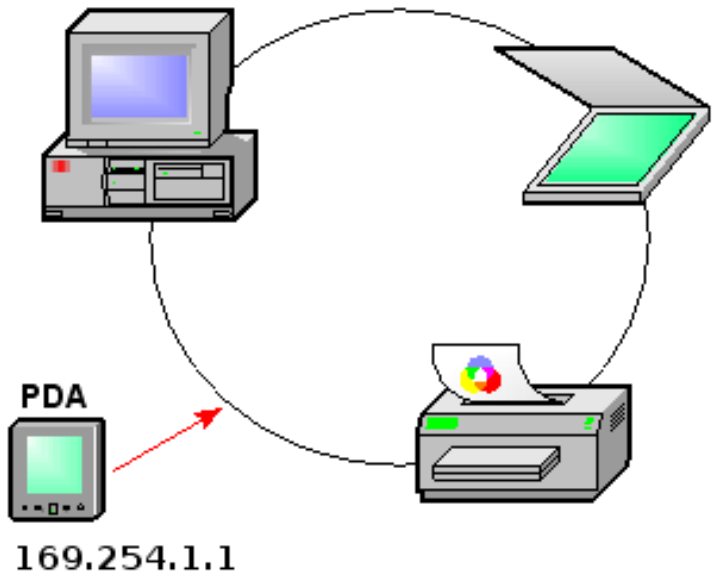
Convention Les extensions du DHCP décrivent de nouvelles méthodes d'attribution d'adresses IP même si il n'y a pas de serveur.

- Autonet
- Auto-IP Configuration
- Automatic Private IP Addressing (APIPA) par Microsoft

Plus simplement AutoIP.

Attribution automatique d'adresses IP privées

Contexte



Principe Si le serveur DHCP n'est pas disponible, l'AutoIP sélectionne une adresse aléatoire dans l'intervalle 169.254.0.1 - 169.254.255.254 (réservé par l'IANA). S'assure qu'il n'y a pas duplication.

Attribution automatique d'adresses IP privées

Qualités Simplicité d'utilisation, pas d'administrateur.

Inconvénients Restreint à de petits réseaux.

Attribution automatique d'adresses IP privées

Qualités Simplicité d'utilisation, pas d'administrateur.

Inconvénients Restreint à de petits réseaux.

Une variante de ce mécanisme est proposée en tant qu'alternative au DHCP avec Agent Relais dans de grands réseaux industriels.

Le protocole DHCP

Le principe

Quand une machine est démarrée, elle n'a aucune information sur sa configuration réseau, et surtout, l'utilisateur ne doit rien faire de particulier pour trouver une adresse IP.
Le serveur doit attribuer à chaque nouveau client un minimun d'information sur la configuration du réseau pour que celui-ci puisse communiquer.

- Il doit founir : adresse IP et masque de sous-réseau

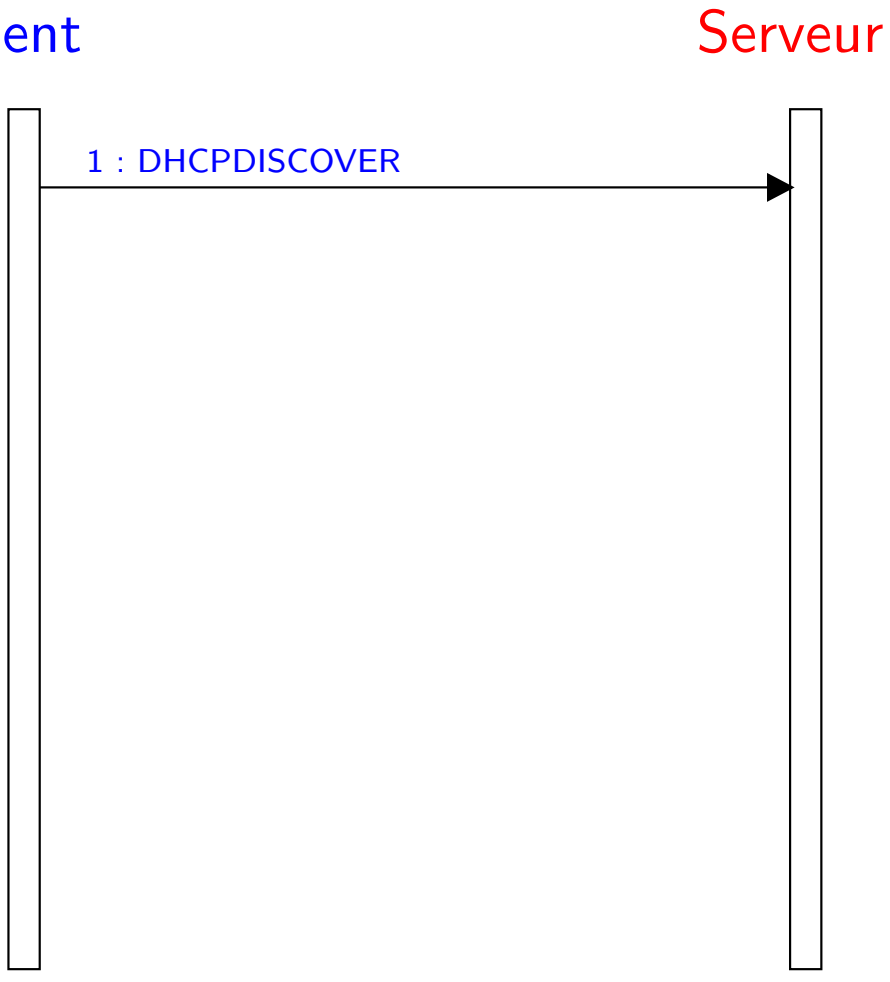
Le principe

Quand une machine est démarrée, elle n'a aucune information sur sa configuration réseau, et surtout, l'utilisateur ne doit rien faire de particulier pour trouver une adresse IP.
Le serveur doit attribuer à chaque nouveau client un minimun d'information sur la configuration du réseau pour que celui-ci puisse communiquer.

- Il doit founir : adresse IP et masque de sous-réseau
- Il peut founir : l'adresse du serveur DNS, WINS, ou encore la passerelle internet.

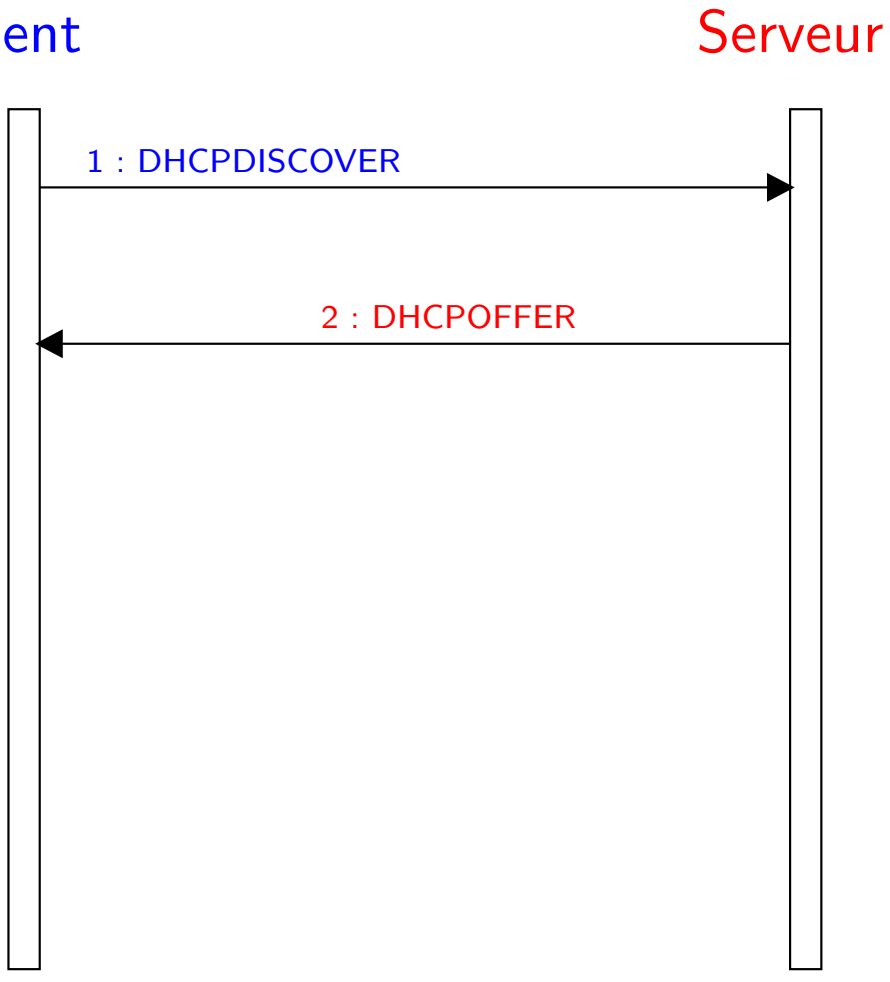
Les messages permettant la configuration d'un client

Lorsqu'un client souhaite obtenir les paramètres de configuration, il diffuse le message *DHCPDISCOVER* pour localiser les serveurs disponibles.



Les messages permettant la configuration d'un client

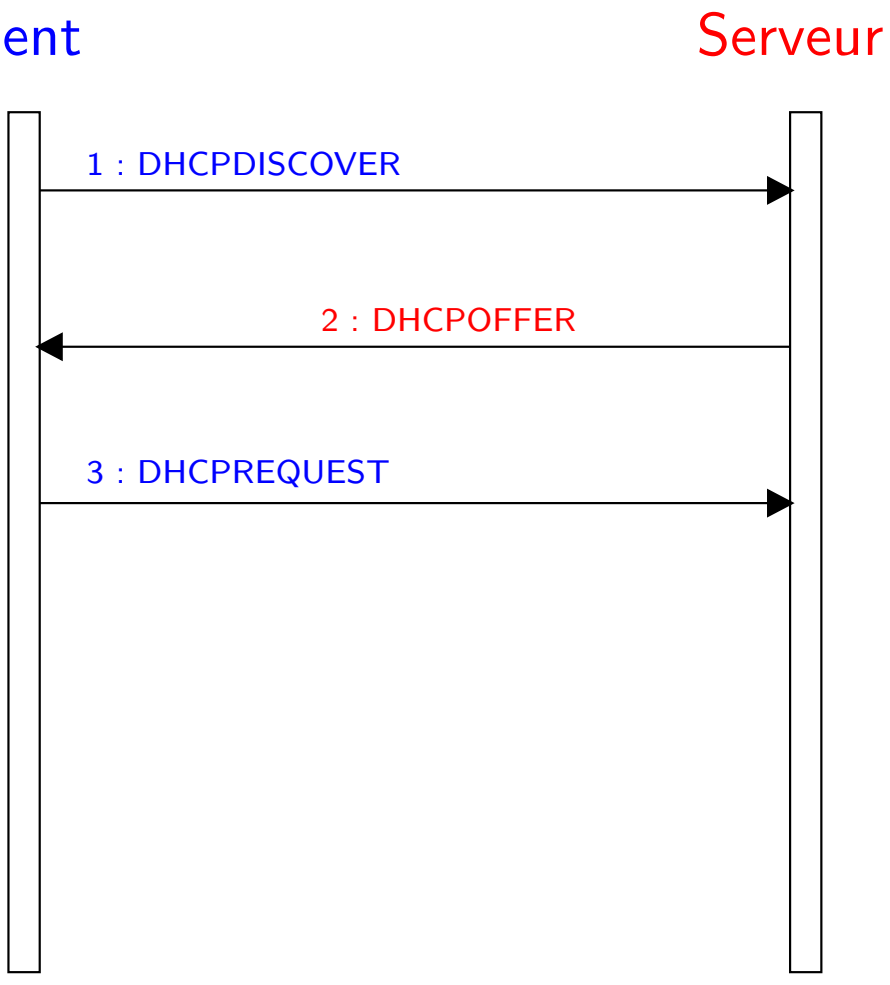
Le serveur répond avec les paramètres de configuration par le message *DHCPOFFER*. Ce message est un paquet unicast car le serveur a reçu l'adresse MAC du client.



Les messages permettant la configuration d'un client

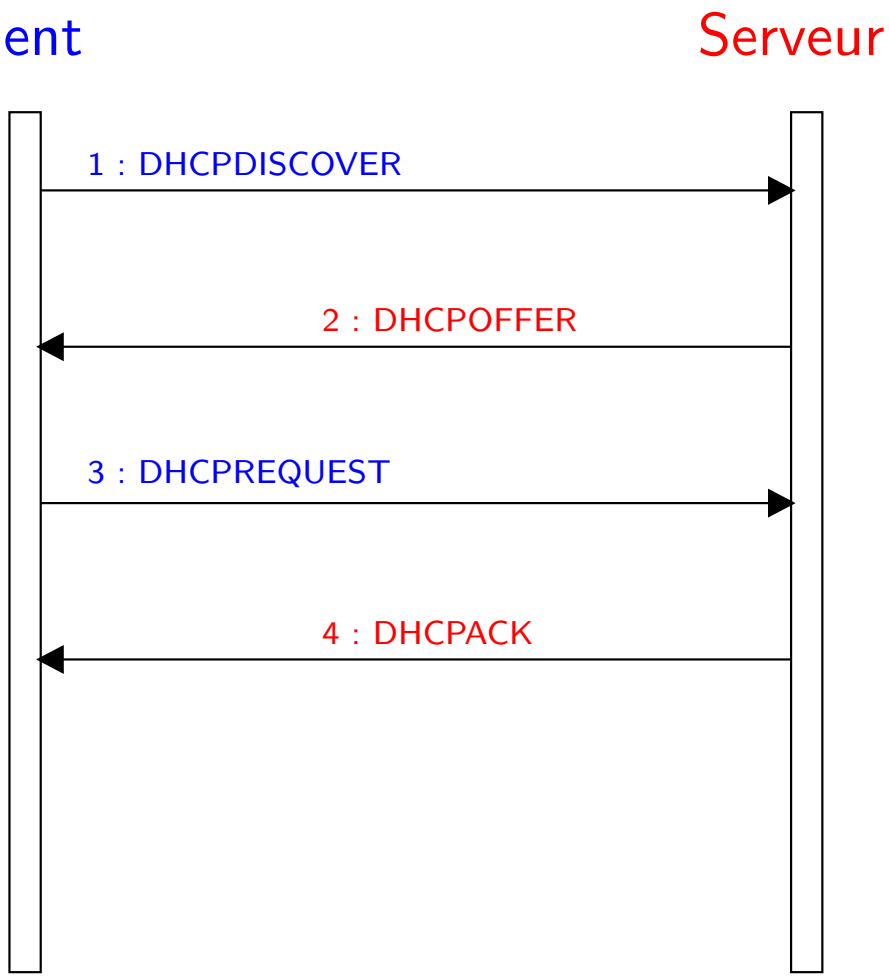
Le client accepte cette configuration par le message *DHCPREQUEST*.
Ce message peut servir aussi à :

- prolonger le bail
- confirmer la validité de cette configuration



Les messages permettant la configuration d'un client

Le serveur valide la configuration de ce client par le message *DHCPACK* en incluant l'adresse du réseau déjà attribuée.
Le client peut utiliser la configuration fournie.



Autres messages échangés entre le client et le serveur

Au client

- Le serveur peut envoyer un message *DHCPNACK* indiquant que les paramètres réseau sont incorrects.

Autres messages échangés entre le client et le serveur

Au client

- Le serveur peut envoyer un message *DHCPNACK* indiquant que les paramètres réseau sont incorrects.

Au serveur

- le client peut indiquer au serveur que l'adresse réseau est déjà attribuée par le message *DHCPDECLINE*.
- le client peut libérer l'adresse réseau et annuler son bail par le message *DHCPRELEASE*.
- le client peut demander au serveur seulement les paramètres de configuration locaux par le message *DHCPINFORM*.

Liste des adresses IP que peut fournir le serveur DHCP à ses clients

Adresse IP	Adresse MAC	Bail (date d'expiration)
192.168.1.0	?	?
192.168.1.1	01-10-B5-86-D1-AA	30 juin 2005
192.168.1.2	?	?
192.168.1.3	?	?
....	...	...
192.168.1.100	?	?

Avantages et Inconvénients

Avantages

- configuration centralisée
- bail

Avantages et Inconvénients

Avantages

- configuration centralisée
- bail

Inconvénients

- difficile à implanter à travers un réseau routé
- possibilité de mauvais fonctionnement du réseau si il y a plusieurs serveur DHCP
- **non sécurisé**

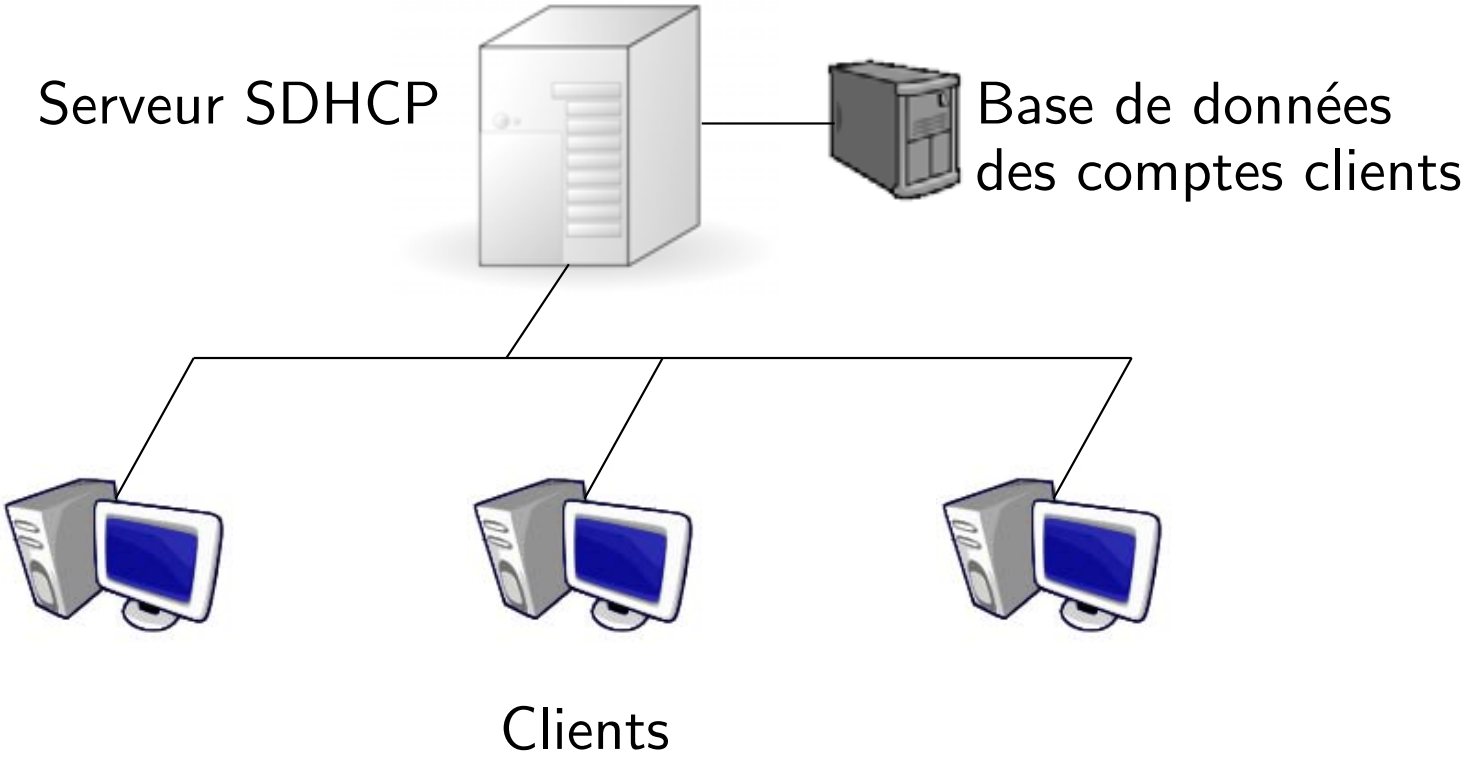
Proposition d'un protocole sécurisé : SDHCP

Contraintes lors de l'élaboration de ce protocole

Pour être valable, ce protocole doit se plier à certaines contraintes de sécurité :

- Le serveur doit être certain de la personne à qui il envoie des paramètres de configuration.
- Le client doit avoir confiance en les paramètres qu'il reçoit. En particulier, ces derniers ne peuvent être ni lus ni modifiés par un tiers.

Principe de fonctionnement



Le serveur SDHCP s'appuie sur une base de données de comptes clients, lesquels devront donc s'identifier avec un login et un mot de passe pour obtenir leur configuration réseau.

Les choix techniques

Les échanges sécurisés s'appuient principalement sur deux systèmes :

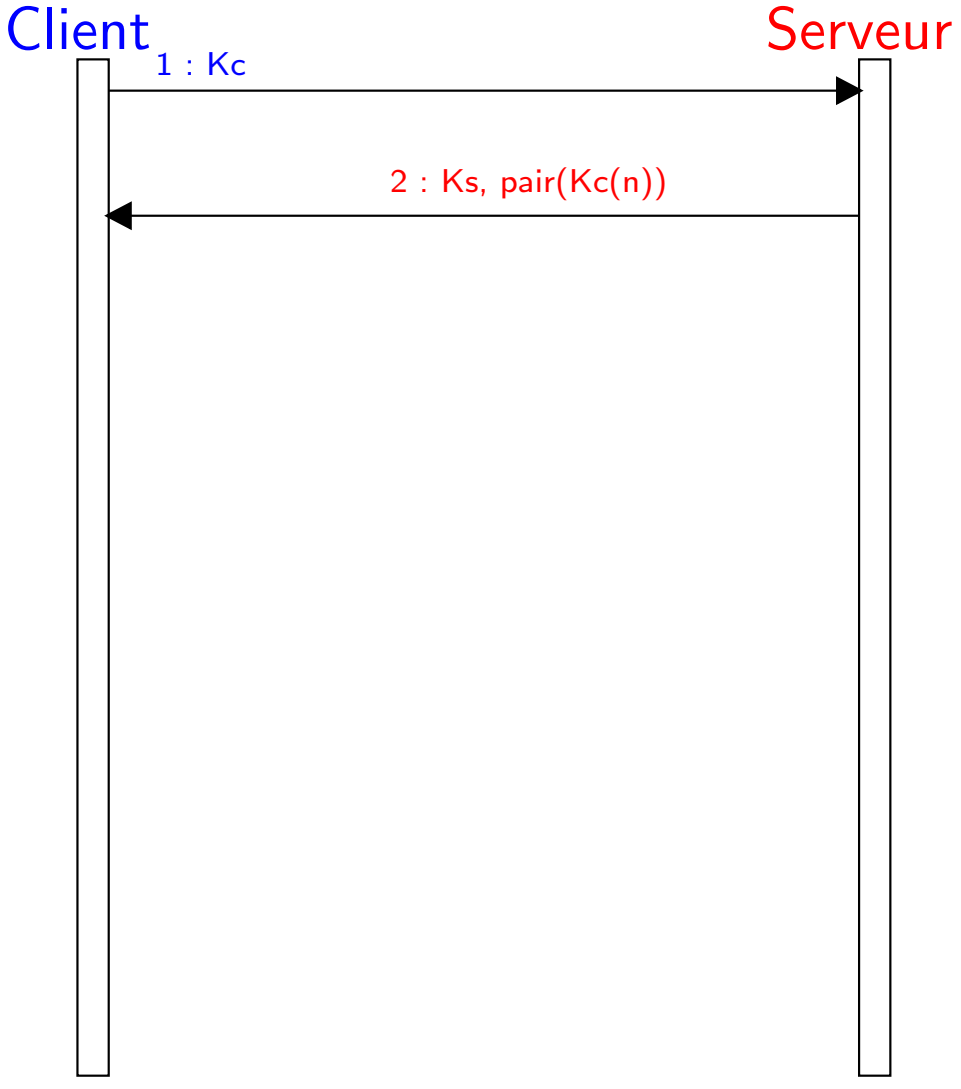
RSA Système de cryptage à clé publique.
On crypte avec la clé publique, et on décrypte avec la clé privée. Après s'être échangés leurs clés, les deux parties pourront donc s'envoyer des messages cryptés.

SHA Fonction de hachage, pour le calcul d'empreinte.
On utilise ce système pour l'authentification d'un client. En effet, pour des soucis de sécurité, on n'envoie jamais un mot de passe directement à un serveur. On lui fait parvenir une empreinte de ce dernier, qui prouvera la connaissance du vrai mot de passe.

Le Protocole

Une session SDHCP s'effectue avec 8 échanges au lieu de 4 pour DHCP

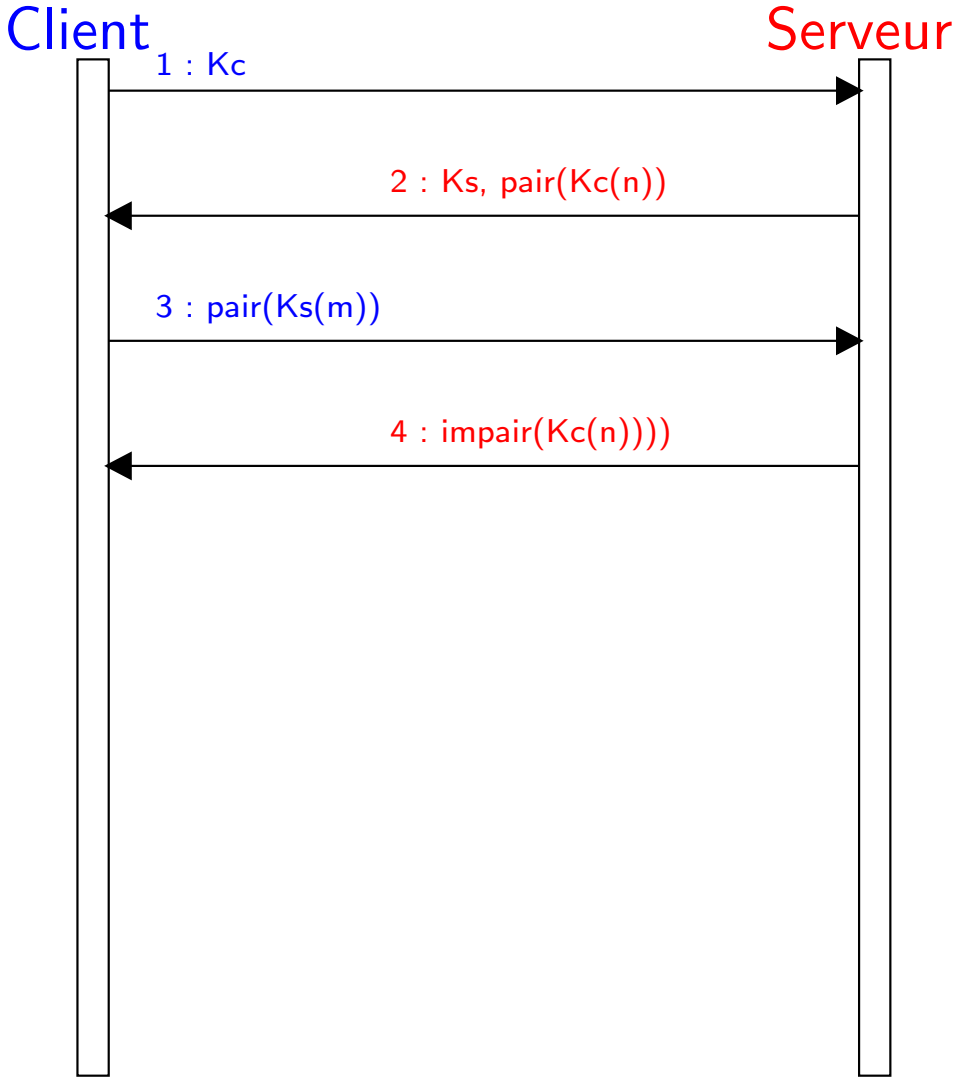
- Client et serveur s'échangent leurs clés publiques.



Le Protocole

Une session SDHCP s'effectue avec 8 échanges au lieu de 4 pour DHCP

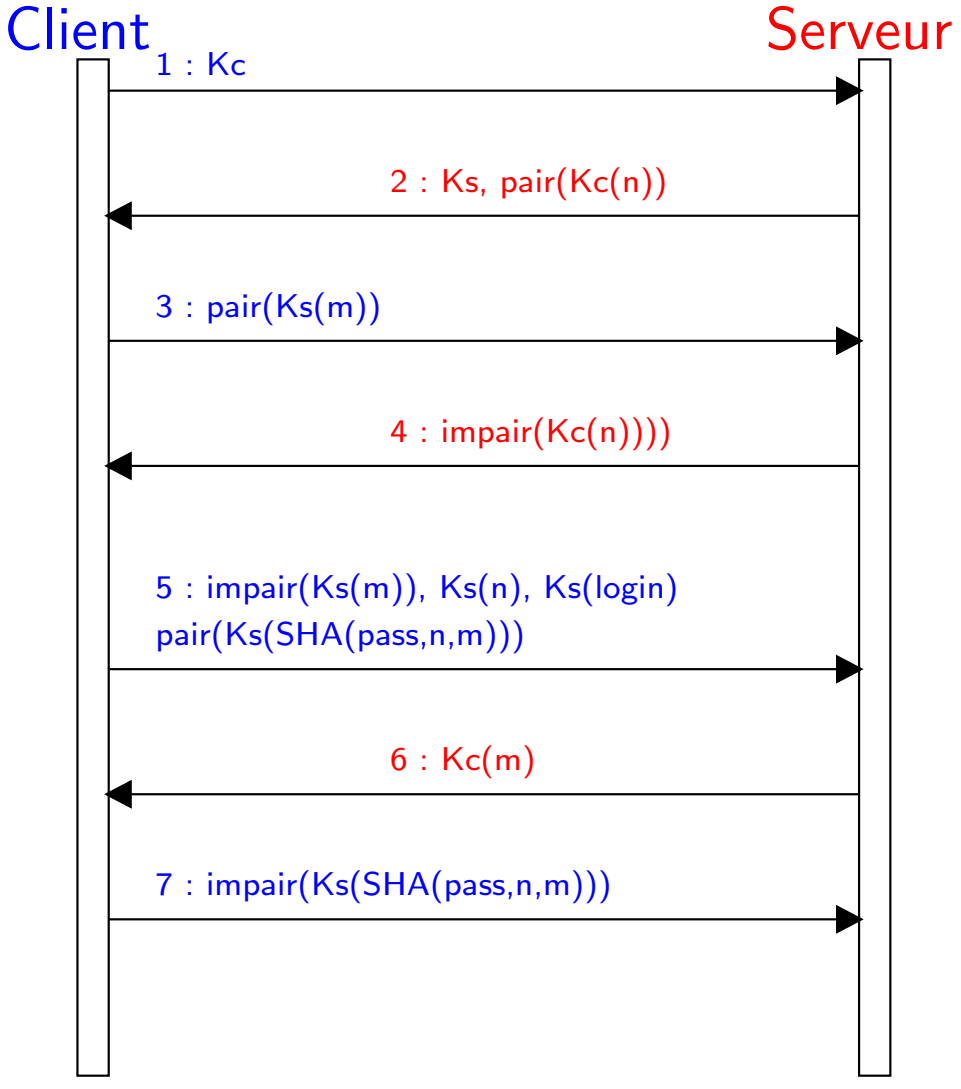
- Client et serveur s'échangent leurs clés publiques.
- Echange de deux nombres aléatoires pour le numéro de session.



Le Protocole

Une session SDHCP s'effectue avec 8 échanges au lieu de 4 pour DHCP

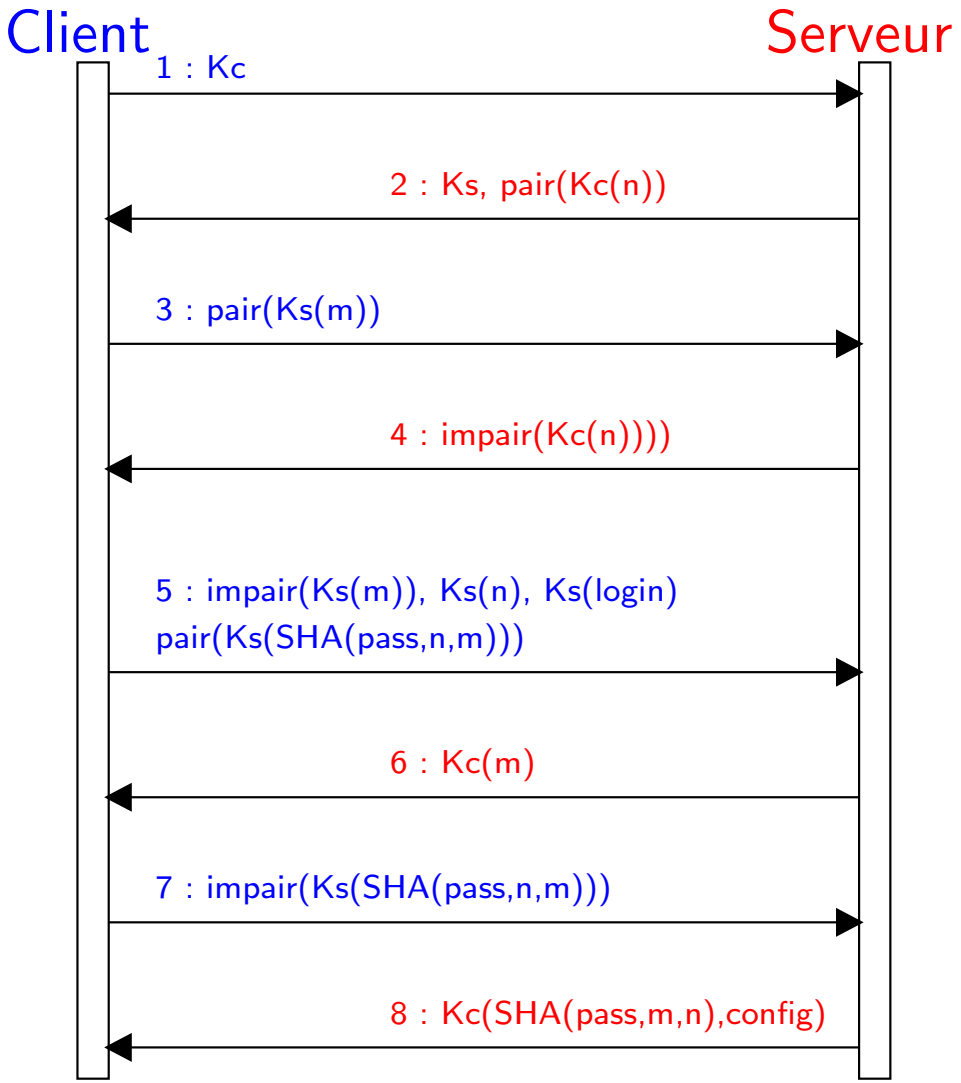
- Client et serveur s'échangent leurs clés publiques.
- Echange de deux nombres aléatoires pour le numéro de session.
- Le client envoie alors ses login et mot de passe.



Le Protocole

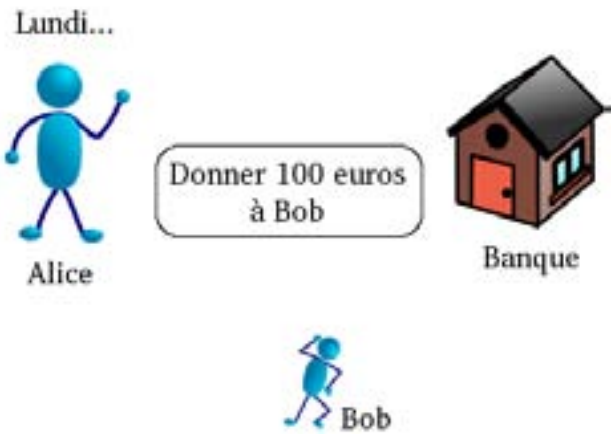
Une session SDHCP s'effectue avec 8 échanges au lieu de 4 pour DHCP

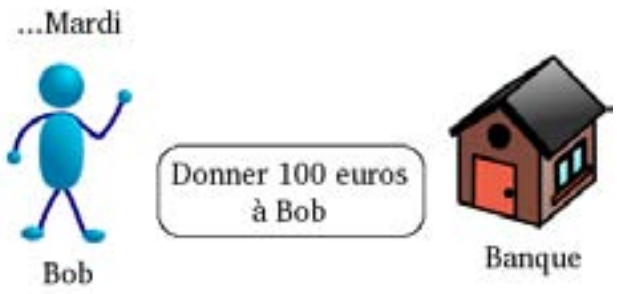
- Client et serveur s'échangent leurs clés publiques.
- Echange de deux nombres aléatoires pour le numéro de session.
- Le client envoie alors ses login et mot de passe.
- Pour finir, si tout va bien, le serveur retourne les paramètres de configuration du client.



Les attaques possibles, et comment s'en protéger

Le rejeu





Pour contrer ce type d'attaque, on marque les paquets d'un numéro de session.

Les attaques possibles, et comment s'en protéger

Le passeur de seau

Pat se fait passer pour Alice auprès de Bob et pour Bob auprès d'Alice :

Les attaques possibles, et comment s'en protéger

Le passeur de seau

Pat se fait passer pour Alice auprès de Bob et pour Bob auprès d'Alice :

Les attaques possibles, et comment s'en protéger

Le passeur de seau

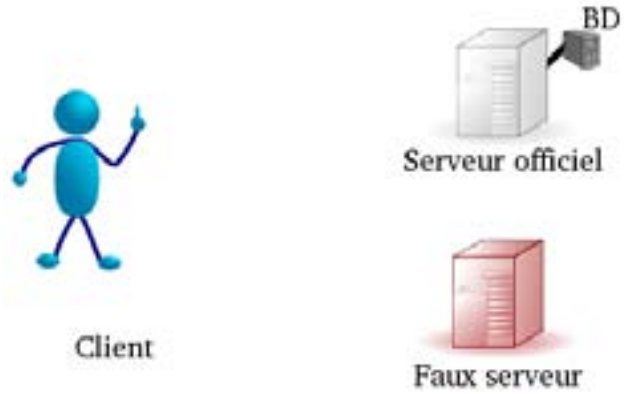
Pat se fait passer pour Alice auprès de Bob et pour Bob auprès d'Alice :

Pour se protéger de cette attaque, on utilise *un protocole imbriqué*, seule une moitié du message est envoyée à la fois, ce qui empêchera Pat de déchiffrer le message puis de le rechiffrer pour Alice.

Les attaques possibles, et comment s'en protéger

Le faux serveur

Il va tenter de donner des informations erronées aux clients par exemple pour détourner son trafic.



Pour déjouer une telle attaque, on retourne une information que seul le vrai serveur peut connaître. Par exemple, l'empreinte seule du mot de passe du client.

Conclusion sur SDHCP

Notre protocole respecte donc les trois grands principes d'un environnement sécurisé :

- Confidentialité
- Intégrité
- Confiance

... mais un protocole n'est jamais inviolable :)

Épilogue

L'homme a toujours imaginé des moyens pour simplifer les tâches à accomplir. Dans l'univers des réseaux, il a fallu implanter des mécanismes pour configurer les machines. Imaginez, si vous deviez configurer à la main les 200 machines qui constituent le réseau, c'est un travail laborieux.De nos jours le protocole DHCP est le plus répandu et permet cette configuration automatique.

Autrefois au second plan, la sécurité d'un système est aujourd'hui un point crucial, ce qui nous a poussé à imaginer SDHCP, un mécanisme simple et fiable.