# DHCP sous windows 2000

## *Généralités*

DHCP est l'abréviation de « Dynamic Host Configuration Protocol). Ce protocole permet à un ordinateur (client DHCP) d'obtenir sa configuration IP du réseau. Nous parlerons du service DHCP présent sous windows 2000 server qui permet à un ordinateur windows 2000 server de jouer le rôle d'un serveur DHCP et de fournir leur configuration TCP/IP à des clients DHCP.

DHCP permet de simplifier et de centraliser la gestion des paramètres TCP/IP des machines du réseau. C'est un protocole qui est largement utilisé de nos jours. Les routeurs ADSL destinés au marché résidentiel hébergent tous des serveurs DHCP et tous ce qui a vocation à avoir une configuration TCP/IP (ordinateurs, imprimantes, ...) peut être configuré via DHCP. DHCP est conçu de façon à ce que les ordinateurs clients DHCP conservent autant que possible la même adresse en cas de reboot,  renouvellement de bail, ...

DHCP permet aussi à un ordinateur qui a son adresse IP configurée d'obtenir les paramètres réseau locaux (passerelle, ...) via le message DHCPInform.

Le service DHCP de windows 2000 est conforme aux RFC 2131 et RFC 2132. Le service DHCP peut donc interagir avec des clients DHCP non microsoft.

Quelques termes et situation à ne pas confondre:

- Adresse IP statique : configurée manuellement sur l'ordinateur
- Adresse IP dynamique: adresse obtenue par DHCP
- Adresse IP Fixe: adresse qui ne change pas quelque soit son mode d'obtention (statique ou dynamique)

## *DHCP: processus, gestion des conflits d'adresses, APIPA*

## Processus

Le processus peut être sommairement résumé de la façon suivante :

1. un ordinateur (client DHCP) sans adresse IP diffuse une demande d'adresse IP sur le réseau (DHCPDiscover ou message de découverte). Ce message contient l'adresse MAC de l'ordinateur;
2. Tous les serveurs DHCP qui voient passer ce message répondent en proposant une adresse IP à l'ordinateur client (message d'offre ou DHCPOffer);
3. Le client indique qu'il accepte l'une de ces offres en diffusant un message de demande (DHCPRequest) contenant notamment l'adresse IP et le serveur DHCP sélectionnés. Cette diffusion indique aux serveurs lequel a été retenu. Le client peut choisir parmi les DHCPOffer reçu. Le client DHCP windows prend le premier reçu.
4. Le serveur accuse réception à l'aide d'un message DHCPAck (accusé de réception) qui peut contenir d'autres options de configuration.

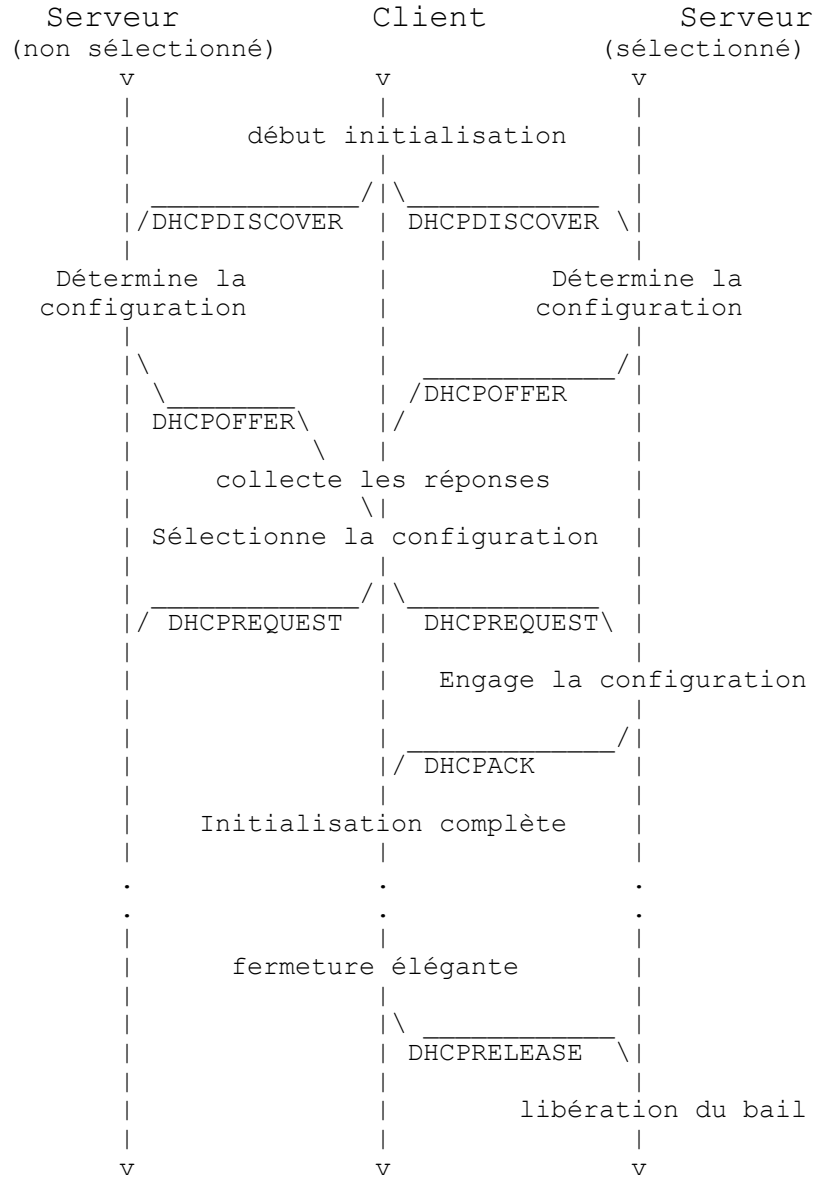
Il arrive qu'un serveur réponde négativement à l'étape 4 (DHCPNak, accusé de réception négatif). Le client doit alors reprendre le processus à l'étape 1.

L'ensemble des informations obtenues par le client DHCP est appelé un **bail**[1]. Ce nom est justifié par le fait que les informations reçues sont valables pour une durée appelée **durée du bail**. La durée du bail est présente dans les deux réponses du serveur (DHCPOffer et DHCPAck). Elle indique pendant combien de temps l'adresse IP et les informations complémentaires pourront être utilisées par le client.

Arrivé à la moitié de la durée du bail, le client DHCP demande la prolongation du bail à son serveur DHCP à l'aide d'un message DHCPRequest. S'il n'y a pas eu de renouvellement après la fin du bail, le serveur DHCP considère que l'adresse est libre et il peut éventuellement la réaffecter à un autre client.

Lors que le serveur et le client sont sur le même sous-réseau, les messages sont envoyés via le contrôle d'accès au media (MAC). S'ils sont sur des sous-réseaux différents, il faut que les passerelles intermédiaires puissent jouer le rôle d'agent relais DHCP.

Diagramme temporel du processus (recopié de la rfc 2131) :




## Gestion des conflits d'adresses

Une adresse IP ne doit pas être affectée à deux machines différentes. Ce cas de figure peut se produire si une adresse gérée par un serveur DHCP a été configurée statiquement

[1] Rappel grammatical: un bail, des baux

sur une machine ou si cette adresse est gérée par un autre serveur DHCP qui l'a déjà attribuée à une machine du réseau. Deux mécanismes permettent d'éviter les conflits:

***détection des conflits côté serveur:***

Le serveur DHCP peut détecter les conflits en testant les adresses IP par ping avant de les proposer aux clients. Si le serveur reçoit une réponse à son ping, il désactive l'adresse IP qui ne sera plus proposée à aucun client. Le serveur ne teste que les adresses allouées à des nouveaux clients (DHCPDiscover) mais pas celles des baux renouvelés (DHCPRequest).

Cette fonctionnalité augmente le temps de réponse des serveurs car ils doivent attendre une éventuelle réponse à son ping.

La RFC 2131 conseille cette fonctionnalité mais elle est désactivée par défaut sur les serveurs windows 2000 et doit être activée explicitement par l'administrateur du serveur. Elle s'applique au niveau d'un serveur et ne peut être paramétrée étendue par étendue.

***Détection des conflits côté client:***

Les ordinateurs windows 98, 2000, ... vérifient si l'adresse qui leur a été communiquée par le serveur est déjà utilisée sur le réseau grace à un requète ARP. Si c'est le cas, ils envoient un message DHCPDecline au lieu du message DHCPRequest d'acceptation d'adresse IP et recommence la demande bail au début. Ce cas étant un cas anormal, le serveur doit signaler le problème à son administrateur.

## Automatic Private IP Adressing (APIPA)

APIPA est un mécanisme conçu pour gérer le cas où aucun serveur DHCP ne répond. Dans une telle situation, le client DHCP d'un ordinateur windows NT 4 se contenait d'essayer périodiquement de contacter un serveur DHCP mais ne prenait aucune adresse IP.

Les ordinateurs windows 98, 2000, ... réagissent différemment : si aucun serveur DHCP ne répond, l'ordinateur prend une adresse IP sur la classe privée 169.254/16 (classe privée affectée à microsoft), vérifie que l'adresse n'est pas utilisée et l'utilise si c'est le cas. Si l'adresse choisit est utilisée, l'ordinateur choisit une autre adresse. Il peut ainsi tenter d'utiliser jusqu'à 10 adresses.

On peut ainsi avoir des machines non configurées qui arrivent néanmoins à communiquer. Les autres informations (passerelle, serveur DNS, ...) n'étant pas configurées, APIPA n'est pas une solution viable dans une entreprise. Ce mécanisme peut par contre rendre service chez un particulier qui ne sait pas configurer les paramètres réseau de ses ordinateurs.

Le client DHCP tente de contacter un serveur DHCP toutes les 5 minutes. En cas de succès, les données reçues du serveur remplaceront les données autoconfigurées avec APIPA.

## Mécanisme utilisé en cas de renouvellement de bail :

- Demande de renouvellement de bail
- en cas d'échec et si la durée du bail n'est pas dépassée :
  - l'ordinateur tente de contacter la passerelle indiquée dans le bail
    - Si il y arrive, il suppose que les informations de configuration TCP/IP du bail sont encore valides et il les utilise
    - si la passerelle ne répond pas, il utilise APIPA pour obtenir une adresse IP.

Le client DHCP microsoft enregistre localement le bail ce qui permet au client de tenter un renouvellement de bail lors du redémarrage. Si aucun serveur DHCP ne répond, le client peut alors utiliser le mécanisme décrit ci-dessus pour utiliser les informations du bail sauvé s'il n'est pas expiré.

Ces comportement sont conformes à la RFC 2131 qui précise que le serveur DHCP doit faire en sorte de redonner la même adresse IP à une machine cliente lors d'un renouvellement de bail ou d'un redémarrage.

## Message DHCP

Les messages DHCP (rfc2131) :

| **Message** | **Utilisation** |
|---|---|
| DHCPDISCOVER | Diffusion du client pour localiser les serveurs disponibles |
| DHCPOFFER | Du serveur au client pour répondre au DHCPDISCOVER avec les paramètres de configuration. |
| DHCPREQUEST | Message client aux serveurs soit (a) qui demande les paramètres à un serveur et décline implicitement les offres de tous les autres, (b) qui confirme la validité des adresses précédemment allouées, par ex : un redémarrage système, ou (c) qui étend le bail sur une adresse réseau en particulier. |
| DHCPACK | Du serveur au client avec les paramètres de configuration et qui inclut l'adresse réseau déjà attribuée. |
| DHCPNAK | Du serveur au client indiquant que la notion d'un client pour les adresses réseau est incorrecte. (par ex : si un client est déplacé sur un nouveau sous réseau) ou que le bail du client a expiré. |
| DHCPDECLINE | Client vers serveur indiquant que l'adresse réseau est déjà utilisée. |
| DHCPRELEASE | Client vers serveur libérant l'adresse réseau et annulant le bail. |
| DHCPINFORM | Client vers serveur, demandant seulement les paramètres de configuration locaux ; le client possède déjà une adresse réseau attribuée de manière externe. |

## *Les nouveautés de windows 2000*

## Mise à jour automatique du dns

Si le serveur dns supporte les mises à jour dynamiques ce qui est le cas du serveur dns de windows 2000, le serveur DHCP ou le client DHCP W2K peuvent mettre à jour l'entrée d'un ordinateur dans le DNS de façon à ce que l'adresse qu'il vient de lui affecter soit associée à l'ordinateur demandeur.

On peut ainsi garantir qu'un ordinateur aura toujours la bonne adresse IP associée à son nom dans le DNS quelque soit ses changements d'adresse IP.

## Autorisation des serveurs DHCP dans active directory

Les serveurs DHCP s'exécutant sur des ordinateurs appartenant à un domaine active directory vérifient avant de se lancer s'ils sont autorisés par le domaine. Si ce n'est pas le cas, le service DHCP est automatiquement arrêté.

Cette fonctionnalité a pour but d'éliminer les serveurs DHCP non autorisés qui pourraient envoyer des informations incorrectes aux ordinateurs clients DHCP.

Elle ne marche pas avec les serveur DHCP s'exécutant sous des versions plus anciennes de windows, sur les serveurs DHCP non microsoft et sur les serveurs DHCP des ordinateurs n'appartenant pas au domaine. C'est donc une fonctionnalité qui n'est utile que dans les réseau 100% microsoft et dont toutes les machines font partie d'un domaine.

## Accès en lecture seul possible pour certains utilisateurs

Les membres du groupe « utilisateurs DHCP » peuvent utiliser la console DHCP en lecture seule. Ils ont ainsi accès aux informations mais ne peuvent les modifier.

## classes d'options

Les classes d'options permettent de regrouper certains clients d'une étendue et de leur d'attribuer des paramètres spécifiques. Les clients peuvent être regroupés sur des critères liés aux fournisseur du client ou à des données utilisateurs.

On peut ainsi regrouper dans une classe toutes les machines d'un même type (terminaux X d'un modèle donné par exemple) ou toutes les machines d'un étage (sélection selon une donnée utilisateur).

## surveillance des performances

De nouveaux compteurs destinés au moniteur système ont été ajoutés dans windows 2000. Ils permettent de surveiller les performances des serveurs DHCP.

## Prise en charge améliorée des étendues de multidiffusion

Les étendues de multidiffusion permettent aux applications qui emploient la multidiffusion d'obtenir des adresses IP de classe D pour participer à des groupes de multidiffusion.

## Prise en charge des adresses dynamiques pour BOOTP

Le serveur DHCP microsoft peut affecter des adresses extraites d'un ensemble d'adresses à des client BOOTP. Les serveurs pré-windows 2000 imposait une réservation d'adresse obligatoire pour les clients BOOTP.

## *DHCP: mise en place d'un serveur*

Les opérations nécessaires pour mettre en service un serveur DHCP sont les suivantes :

1. installer le service DHCP s'il ne l'est pas
2. autoriser le serveur DHCP dans active directory
3. définir les étendues
4. activer les étendues

De façon optionnelles :

- définir des options DHCP et notamment : le DNS et la passerelle (ne pas le faire a peu de sens)
- définir des classes d'option si nécessaire.

Si un serveur DHCP a plusieurs cartes réseau, le serveur gérera les réseaux situés derrière chacune des cartes pour lesquelles l'adresse IP du serveur est configurée statiquement. Il est possible d'empêcher le serveur de gérer l'une des cartes en supprimant la liaison correspondante dans **Propriétés**/**Avancé/liaison** du serveur.

Nous allons détailler ces divers éléments:

## Étendue :

Une étendue est un ensemble d'adresse IP et de paramètres de configuration que le serveur va utiliser pour fournir des baux à ses clients. Une étendue est définie par :

- son nom;
- une plage d'adresse IP et un masque de sous-réseau;
- une valeur par défaut pour la durée du bail

Elle peut comporter aussi :

- des plages d'exclusion permettant d'exclure les adresses des ordinateurs configurés statiquement ou celle gérées par d'autres serveurs DHCP;
- des réservations qui permettant d'associer une adresse IP Fixe à certains ordinateurs (à leur adresse MAC en fait). Les imprimantes, passerelles, serveurs DNS, ... ont vocation à avoir une adresse IP Fixe.

Une étendue inutilisée peut être désactivée. Le serveur DHCP agit ensuite comme si cette étendue n'existait pas.

## Étendue globale

Une étendue globale regroupe plusieurs étendues.

## Options DHCP

Les options DHCP sont des paramètres supplémentaires qui seront envoyés aux clients. On peut ainsi préciser les adresses IP de la passerelle, d'un serveur DNS, non de domaine DNS, adresse d'un serveur WINS, ...

Les options peuvent être définies :

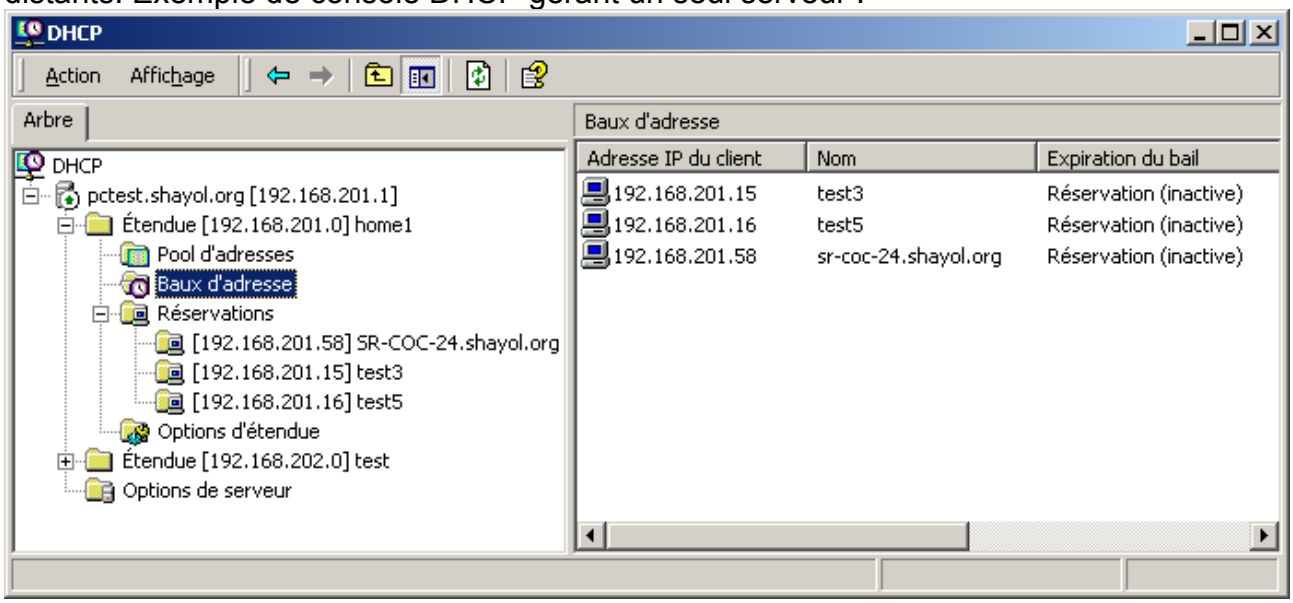
- globalement: elles s'appliquent à toutes les étendues du serveur
- au niveau d'une étendue: elles s'appliquent à tous les clients qui obtiennent un bail sur cette étendue;
- au niveau d'une classe: elle s'appliquent à tous les clients de la classe. On y accède via l'onglet avancé des options d'étendues;
- au niveau d'un client ayant une réservation: elle s'appliquent à ce client donné.

L'ordre de priorité est le suivant: les valeurs configurées statiquement sur le client l'emporte sur les informations transmises via DHCP, les options les plus locales sont les plus prioritaires. Ainsi, une options définie au niveau d'une étendue sera prioritaire par rapport à la même option définie au niveau globale.

### *Console de gestion DHCP*

La console de gestion DHCP est une console MMC qui peut être intégrée à une console personnalisée. Elle est disponible par défaut dans les Outils d'Administration.

La console de gestion DHCP peut gérer le serveur DHCP local ou des serveurs DHCP distants. Exemple de console DHCP gérant un seul serveur :




### *Sauvegarde et procédure de reprise*

### *Outils en ligne de commande pour test et gestion du service DHCP*

## IPCONFIG

Ipconfig est un outil à utiliser sur le client :

- ipconfig /all permet d'obtenir notamment l'adresse ip, le serveur DHCP (s'il y en a un) ainsi que les valeurs couramment spécifiées par un serveur DHCP: passerelle, serveur DNS. On obtient aussi le nom de toutes les cartes de l'ordinateur (« Connexion au réseau local » est le nom de l'unique carte en général).
- Ipconfig /release: oblige le client DHCP à libérer son adresse IP actuelle.
- Ipconfig /renew: provoque un renouvellement (ou une demande initiale s'il n'y en avait pas) du bail
- ipconfig /showclassid IDCarte : affiche les ID de classes DHCP autorisées pour la carte.
- ipconfig /setclassid IDCarte : modifie l'ID de classe DHCP.

## NETSH DHCP

Netsh[2] est un outil en ligne de commande qui permet de réaliser des tâches de configuration réseau accessibles par des interfaces graphiques. Netsh possède toute une section concernant dhcp qui est consultable dans la documentation de la MMC DHCP. Il

[2] En fait, netsh est bien plus que cela puisque c'est un outil extensible extrêmement polyvalent.

est ainsi possible de créer des étendues, de créer des réservations, ...

C'est l'outil à utiliser si toutes les adresses des ordinateurs gérés par le serveur DHCP sont fixes (dont définies dans une réservation DHCP) et si l'on souhaite dupliquer la configuration d'un serveur : on peut ajouter une réservation en modifiant un script que l'on exécutera sur tous les serveurs DHCP concernés.

## *Sécurité*

DHCP utilise des paquets UDP : de/vers le port 68 du client et de/vers le port 67 du serveur. Il paraît un peu bizarre de parler d'UDP alors que le but du processus est d'obtenir les informations de configuration IP. On peut d'ailleurs noter que les messages DHCP diffusés par un client avant qu'il ait obtenu son adresse IP ont 0.0.0.0 comme adresse source. La RFC 2131 précise que pendant cette phase d'initialisation, les paquets correspondant adressé à l'adresse MAC de la machine doivent être passées à la couche IP pour y être traités comme des paquets UDP « normaux ».

DHCP a été conçu pour être compatible avec des protocoles conçus à une époque où la sécurité n'était pas considérée. DHCP fournit des informations critiques aux ordinateurs clients et notamment l'adresse de la passerelle, du serveur dns, ... Un serveur dhcp pirate pourrait fournir des informations erronées aux clients. Les conséquences possibles seraient notamment :

- déclaration d'une fausse passerelle : faire passer tout le trafic par une machine contrôlée par le pirate et déclarée comme passerelle par le serveur dhcp du pirate. Il est alors possible d'observer et de modifier le trafic passant par cette passerelle en l'envoyant ensuite à la passerelle légitime;
- déclaration d'un serveur dns: le serveur dns déclaré par le serveur dhcp du pirate pourra associé l'adresse IP d'une machine compromise à des noms de machines de l'entreprise et espionner le trafic entre le client et ces machines.

La RFC 3118 définit une méthode d'authentification permettant de supprimer ces failles. Elle a le défaut d'être complexe à mettre en oeuvre (il faut une clef unique par client) et, à l'heure actuelle, par encore disponible dans les implantations de DHCP.

## *Glossaire*

## *Bibliographie*


- Kit de ressources techniques windows 2000 server, tome 3 (Architecture TCP/IP), chapitre 4 (DHCP)
- Aide en ligne de la MMC DHCP
- RFC 2131: Dynamic Host Configuration Protocol (remplace le RFC 1541)
- RFC2132: DHCP Options et BOOTP vendors extensions.
- RFC 3118: Authentification for DHCP messages
- MISC No 4: Les failles du protocole DHCP: Spoof & Destroy