BTS SIO BLOC 2 Admin Sys	*DHCP* *L'exploitation du service DHCP* Sources : RFC 2131, RFC 2132 et Microsoft Learn	Fiche de synthèse N° 5

Ressources : protocole DHCPv4, options DHCP et documentation Windows Server.

Liens : rfc-editor.org/rfc/rfc2131 – learn.microsoft.com (DHCP)

I. Le rôle du service DHCP

DHCP signifie *Dynamic Host Configuration Protocol*. Il automatise la configuration réseau des clients et centralise sa gestion. Cette fiche porte principalement sur **DHCP pour IPv4** : adresse IP, masque, passerelle par défaut et serveurs DNS.

Le serveur attribue une adresse pour une durée appelée **bail**. Il conserve les attributions pour éviter de distribuer simultanément une même adresse à plusieurs clients. DHCP limite les erreurs de saisie et facilite les changements de configuration d'un parc.

DHCP prolonge BOOTP, notamment utilisé pour l'amorçage réseau. Les références de base sont les **RFC 2131** pour DHCPv4 et **2132** pour ses options. DHCP fournit la configuration ; DNS assure la résolution des noms.

II. Les étendues et les modes d'attribution

A- Le vocabulaire à connaître

Élément	Rôle
Étendue (scope)	Ensemble de paramètres et d'adresses destinés à un sous-réseau.
Plage d'adresses	Intervalle configuré pour les attributions aux clients.
Exclusion	Adresse ou intervalle de la plage non distribué par le serveur.
Réservation	Association d'une adresse à un client identifié, souvent par sa MAC.
Bail actif	Attribution en cours, avec un client et une date d'expiration.

B- Adresse statique ou réservation

Une **adresse statique** est configurée sur l'équipement : elle doit être hors de la plage distribuée ou exclue. Une **réservation** reste fournie par DHCP : le client doit donc être configuré en automatique et pouvoir joindre le service.

Une réservation **n'impose pas un bail illimité**. Pour les équipements d'infrastructure, notamment le serveur DHCP et les interfaces des routeurs, on privilégie une configuration statique documentée.

III. L'obtention d'une configuration : les échanges DORA

DHCPv4 fonctionne en mode **client-serveur** avec **UDP 67 côté serveur** et **UDP 68 côté client**. Lors d'une première attribution sur le réseau local, le client ne dispose pas encore d'une adresse IPv4 utilisable.

Étape	Échange et fonction
1. DHCPDISCOVER	Le client recherche un serveur. Il diffuse généralement depuis 0.0.0.0 vers 255.255.255.255.
2. DHCPOFFER	Un serveur propose une adresse, une durée de bail et des paramètres. Plusieurs serveurs peuvent répondre.
3. DHCPREQUEST	Le client choisit une offre et diffuse sa demande en indiquant le serveur retenu ; les autres serveurs sont informés du choix.
4. DHCPACK	Le serveur retenu confirme l'attribution et les paramètres. Le client peut configurer son interface après les vérifications nécessaires.

DORA = Discover, Offer, Request, Acknowledge. Toutes les trames ne sont pas systématiquement diffusées : OFFER et ACK peuvent être envoyés en unicast ou en broadcast selon la situation. Le choix de l'offre dépend du client ; la première reçue n'est pas une règle universelle.

Le client peut vérifier par ARP que l'adresse n'est pas déjà utilisée. En cas de conflit détecté, il avertit le serveur par **DHCPDECLINE** et recommence la recherche.

IV. Le bail DHCP et son renouvellement

A- Les échéances du bail

Le client ne possède pas définitivement son adresse. Il tente de la conserver par renouvellement. Sauf valeurs différentes fournies par le serveur, les échéances sont les suivantes :

Moment	Comportement du client
T1 : 50 % du bail	DHCPREQUEST en unicast vers le serveur d'origine pour renouveler.
T2 : 87,5 % du bail	Sans renouvellement, DHCPREQUEST en broadcast pour rechercher un serveur capable de prolonger le bail (rebinding).
Expiration : 100 %	Sans confirmation, arrêt de l'utilisation de l'adresse et nouvelle recherche DHCP.

Exemple : bail de 8 jours. T1 intervient après 4 jours, T2 après 7 jours, et l'expiration après 8 jours, si aucun renouvellement n'a abouti. Un DHCPACK renouvelle le bail et ses échéances.

B- Les autres situations à distinguer

DHCPNAK : le serveur refuse une configuration devenue invalide ; le client abandonne l'adresse et reprend l'initialisation. **DHCPRELEASE** : le client libère volontairement son bail. Un simple arrêt du poste ne garantit pas l'envoi d'un RELEASE.

Au redémarrage, un client peut demander la validation de son ancienne adresse directement par DHCPREQUEST. Il ne doit pas supposer qu'elle reste valable, notamment après un changement de réseau.

V. Les options DHCP et le fonctionnement entre VLAN

A- Les paramètres distribués

Option DHCPv4	Utilité et exemple
001 – Masque	Délimiter le sous-réseau : 255.255.255.0.
003 – Routeur	Indiquer la passerelle par défaut : 192.168.10.254.
006 – Serveurs DNS	Indiquer les résolveurs : 192.168.10.10.
015 – Nom de domaine	Fournir un suffixe DNS : entreprise.example.
051 – Durée du bail	Définir la durée de validité de l'attribution.
058 / 059 – T1 / T2	Préciser les délais de renouvellement et de rebinding.

L'adresse proposée figure dans le message DHCP ; elle n'est pas l'option « passerelle ». Les options doivent être cohérentes avec le réseau du client. Dans un domaine Active Directory, les clients utilisent les DNS capables de résoudre les enregistrements du domaine.

B- Le rôle du relais DHCP

Les routeurs ne transmettent normalement pas les diffusions DHCP d'un VLAN à un autre. Si le serveur est situé dans un autre sous-réseau, on configure un **agent relais DHCP** sur le routeur ou le commutateur de niveau 3 côté clients.

Le relais transmet les requêtes au serveur et renseigne notamment le champ **giaddr**, qui permet d'identifier le sous-réseau d'origine. Le serveur choisit l'étendue correspondante ; le relais remet ensuite la réponse au client.

Il faut donc une **étendue adaptée à chaque sous-réseau desservi**, un relais correctement configuré et des règles de routage et de filtrage autorisant les échanges. Un seul serveur peut ainsi desservir plusieurs VLAN.

Repère IPv6 : DHCPv6 est un protocole distinct. Le cycle DORA présenté ici ne s'y transpose pas tel quel ; la passerelle par défaut IPv6 est annoncée par les routeurs via les messages RA.

VI. L'exploitation du service

A- Préparer et mettre en service

1. Définir le plan d'adressage : sous-réseaux, plages, exclusions, réservations et options.
2. Configurer une adresse statique sur le serveur et installer le rôle DHCP.
3. Dans un environnement Active Directory, autoriser le serveur DHCP Windows dans l'annuaire avec les droits nécessaires.
4. Créer et activer les étendues ; vérifier les DNS, les passerelles et les relais.
5. Tester un client dans chaque VLAN et contrôler le bail côté serveur.

Un bail court récupère plus vite les adresses des équipements de passage, mais augmente les renouvellements. Un bail long convient davantage à un parc stable, mais immobilise plus longtemps les adresses après le départ de clients.

B- Contrôler un client Windows

Commande	Ce qu'elle permet de vérifier ou de faire
`ipconfig /all`	Voir DHCP activé, IP, masque, passerelle, DNS, serveur DHCP et dates du bail.
`ipconfig /release`	Abandonner le bail IPv4 ; la connexion réseau peut être interrompue.
`ipconfig /renew`	Demander une attribution ou renouveler la configuration DHCP.
`ping 192.168.10.254`	Tester la joignabilité de la passerelle ; un échec peut aussi venir du filtrage ICMP.
`nslookup nom-hote`	Tester la résolution DNS d'un nom connu du réseau.

On commence par **observer** la configuration. La séquence release puis renew n'est pas un préalable systématique au diagnostic, en particulier lors d'une intervention à distance.

C- Contrôler un client Linux

Les noms d'interfaces et le gestionnaire réseau varient selon l'installation. Identifier d'abord l'interface avec `ip -br addr`, puis consulter les routes avec `ip route`. Avec NetworkManager, `nmcli device show` affiche les paramètres reçus.

Si le client **dhclient** est installé et utilisé pour gérer cette interface, les commandes suivantes libèrent puis demandent un bail. Remplacer `enp0s3` par le vrai nom :

```
sudo dhclient -r enp0s3
sudo dhclient enp0s3
```

Ne pas lancer un second client DHCP sur une interface déjà pilotée par un autre gestionnaire. Adapter l'action à NetworkManager, systemd-networkd ou à la configuration réellement utilisée.

D- Surveiller le serveur Windows

Dans la console DHCP, contrôler les baux actifs, les adresses libres, les réservations et les journaux. Avec le module PowerShell DhcpServer :

```
Get-DhcpServerv4Scope
Get-DhcpServerv4ScopeStatistics
Get-DhcpServerv4Lease -ScopeId 192.168.10.0
```

VII. Une méthode de diagnostic

Symptôme	Vérifications prioritaires
Pas d'adresse attendue / APIPA	Lien, VLAN, configuration automatique, service DHCP, étendue active, adresses libres, relais et pare-feu.
Adresse du mauvais réseau	VLAN d'accès, relais, choix de l'étendue et présence éventuelle d'un serveur DHCP non autorisé.
Réseau local accessible seulement	Masque, option 003, passerelle et routage.
Accès par IP mais pas par nom	Option 006, suffixe DNS et fonctionnement du serveur DNS.
Conflit d'adresses	Adresse statique dans la plage, exclusion manquante ou serveurs non coordonnés.

Sous Windows, une adresse automatique **169.254.x.x/16 (APIPA)** peut signaler l'absence de réponse DHCP. Elle permet éventuellement des échanges locaux avec d'autres hôtes compatibles, mais ne fournit pas la configuration habituelle du réseau.

Procéder dans l'ordre : **lien et VLAN → configuration IP → bail et options → passerelle → DNS**. Une capture des paquets UDP 67/68 permet de repérer l'étape DORA manquante. Comparer les observations côté client, relais et serveur avant de modifier la configuration.

VIII. Sécurité et disponibilité

A- Les risques à connaître

Un **serveur DHCP pirate (rogue DHCP)** peut fournir une fausse passerelle ou de faux DNS et favoriser un détournement du trafic. Une attaque de **DHCP starvation** cherche à épuiser la plage d'adresses par de nombreuses demandes.

Le **DHCP snooping**, sur un commutateur compatible, limite les réponses serveur aux ports de confiance. Il doit être configuré selon la topologie, avec une limitation de débit adaptée. L'autorisation dans Active Directory ne bloque pas à elle seule tout serveur pirate sur le réseau.

B- Assurer la continuité du service

Surveiller l'occupation des étendues, conserver des sauvegardes et tester la restauration. Documenter toute modification des plages, options et réservations. Deux serveurs indépendants ne doivent pas distribuer sans coordination les mêmes adresses.

Le **basculement DHCP (failover)** de Windows Server permet à deux partenaires de partager les informations de baux DHCPv4, en répartition de charge ou en secours. Après modification des paramètres d'une étendue, leur réplication vers le partenaire doit être déclenchée. Les clients doivent pouvoir joindre les deux serveurs.

Références officielles pour approfondir :
RFC 2131 – fonctionnement de DHCPv4 ; RFC 2132 – options DHCP.
Microsoft Learn – ipconfig ; Microsoft Learn – DHCP failover.