



# Dynamic Host Configuration Protocol

## 2 problèmes de gestion avec IP

- La Gestion des adresses IP
  - Les adresses IP doivent être unique
  - Nécessité d'une liste d'ordinateurs avec leurs adresses IP respectives
- La Gestion des principaux paramètres IP
  - Masques de sous-réseaux
  - Adresses IP du gateway
  - Serveurs DNS

# DHCP ? (1)

- Dynamic Host Configuration Protocol
- Extension du protocole BOOTP
- Bâti sur un modèle client-serveur utilisant UDP
- Composé de deux parties :
  - Un protocole
  - Un mécanisme de création d'adresses

## DHCP ? (2)

- Permet :
  - Allocation dynamique des adresses IP et des noms d'hôte.
  - Utilisation automatique de la plupart des paramètres de réseau.
  - Maintenance des adresses IP en cours grâce au concept de « bail d'adresses IP ».
  - Aide à la récupération de paramètres de réseau valides sur un système déplacé d'un réseau géré par DHCP à un autre.

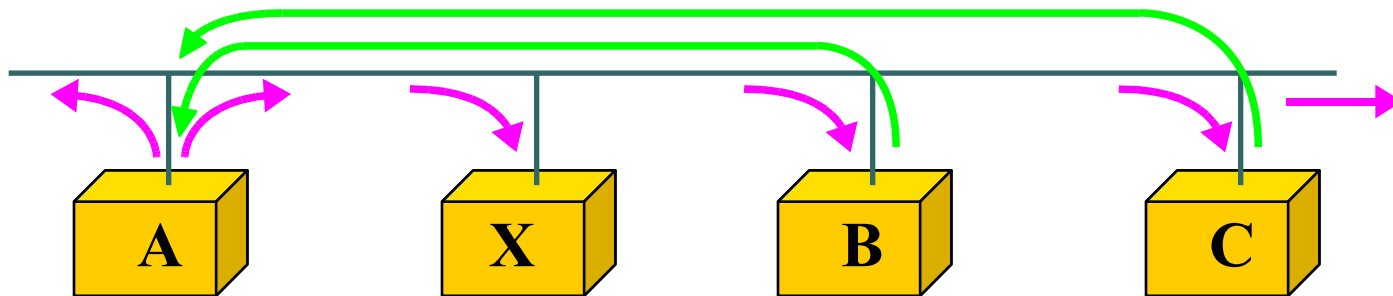


# Dynamic Host Configuration Protocol

D'autres mécanismes

# RARP

- Inverse de Adress Resolution Protocol
- But : Obtenir une @IP à partir d'une @MAC
- Nécessité d'une liste de couples : @MAC/@IP



- Pour connaître son @IP, A diffuse sur le réseau, une requête RARP
- Les Serveurs RARP (B et C) répondent à la requête.

# Inconvénients de RARP

- Opère à un niveau très bas
  - Difficile de programmer un tel service
- Réponse RARP ne contient qu'une petite quantité d'informations (une adresse IP)
  - Impossible de faire de la configuration automatique

# BootStrap Protocol (BOOTP)

- Protocole d'amorçage
- Défini par les RFCs :
  - RFC951            Bootpstrap Protocol
  - RFC1542        Clarifications and Extensions for Bootp
- Basé sur IP/UDP.
- Permet aux clients sans disque de démarrer et de se configurer automatiquement



# Caractéristiques de BOOTP

- Adresse IP attribuée jusqu'à la déconnection du client
  - Temps d'attribution non paramétrable
- Nécessité pour le serveur de connaître l'@MAC du client pour être autorisé à lui répondre et disposer de ses paramètres IP
- Renseignement **manuel** d'une table faisant correspondre à chaque client son @MAC et les paramètres IP associés

# Fonctionnement de BOOTP

- Le client émet par broadcast une trame de requête Bootp, contenant son adresse MAC pour obtenir sa configuration IP
- Le serveur du réseau reçoit ce broadcast; si l'@MAC du client est présente dans sa table Bootp, il envoie alors une réponse contenant les paramètres de configuration IP du client
- Le client reçoit la trame et initialise sa configuration IP
- Le client adresse ensuite au serveur une requête de transfert TFTP afin d'obtenir un fichier de démarrage

# Apport de DHCP par rapport à BOOTP

## → BOOTP:

- Pré-allocation manuelle d'adresses IP uniques.

## → DHCP:

- Allocation automatique d'adresses IP permanentes
- Allocation dynamique d'adresses uniques réutilisables
- Possibilités de conserver les paramètres du client après redémarrage de celui-ci



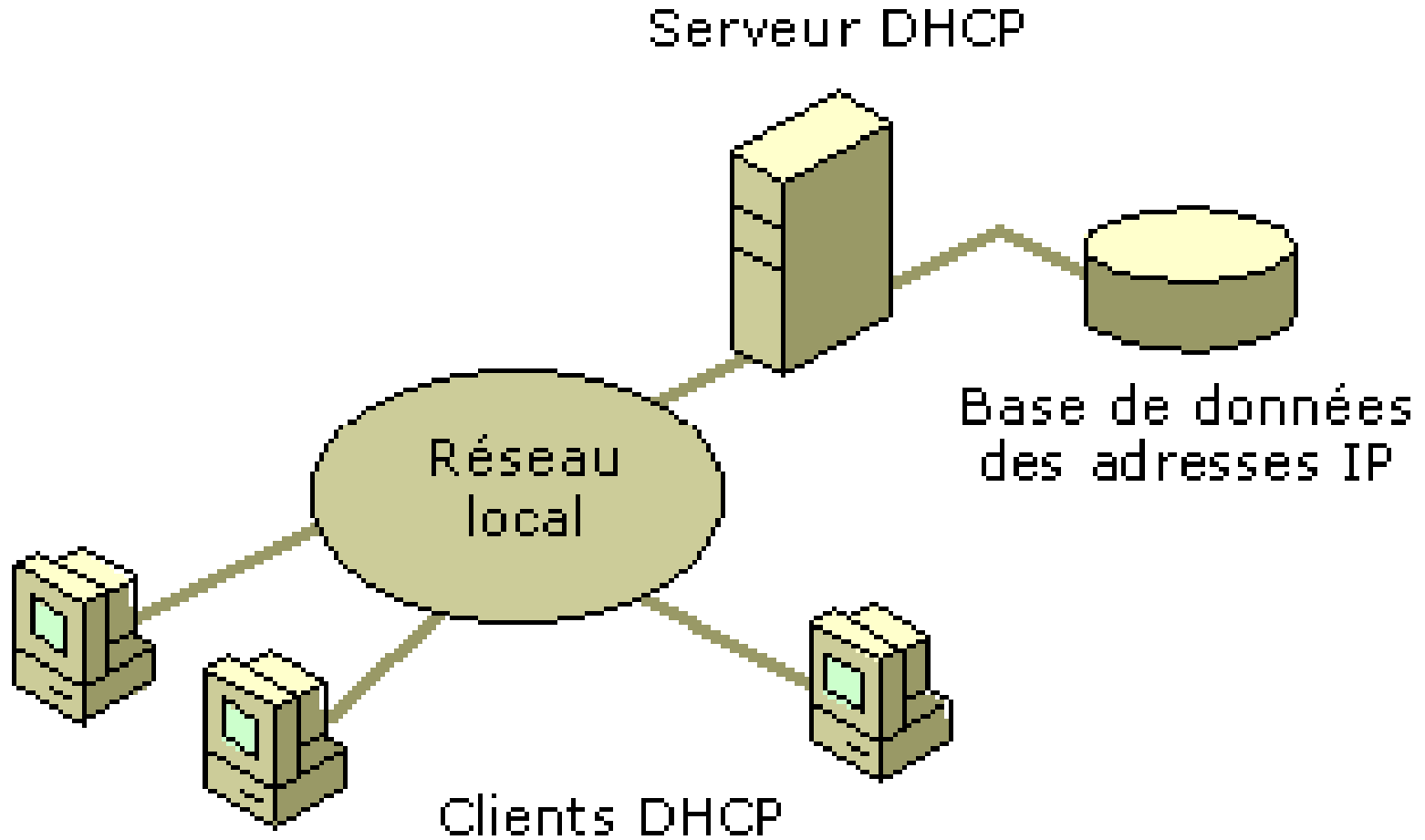
# Dynamic Host Configuration Protocol

Le fonctionnement

# Définition

- Dynamic Host Configuration Protocol
- Standard TCP/IP conçu pour simplifier la gestion de la configuration d'IP hôte
- Réduit la complexité et la quantité de travail de l'administrateur réseaux
- Méthode de gestion d'affectation dynamique d'adresses IP et d'autres paramètres de configuration

# Schéma classique



# Fonctionnement

- Modèle client-serveur
- Le client :
  - Vient de démarrer et réclame sa configuration.
- Le serveur :
  - détient la politique d'attribution des configurations IP.
  - envoie une configuration donnée pour une durée donnée, appelé bail à un client donné

# Le Bail ?

- Définit par le serveur DHCP
- C'est l'intervalle de temps pendant lequel un client peut utiliser une adresse IP qui lui a été affectée
- Demande de renouvellement de l'adresse IP à  $T1=1/2*Bail$ 
  - Si échec du renouvellement, nouvelle demande à  $T2=0.875*Bail$
  - Si nouvelle échec, à expiration du bail, le client libère l'adresse IP attribué



# Différences entre DHCP et BOOTP (1)

- **1 – Affectation de paramètre réseau:**
  - Fournir un espace de mémorisation des paramètres réseau pour les clients du sous-réseau
  - Basé sur la mémorisation (dans une base de données) d'une valeur clé pour chaque client => identifiant unique
  - Possibilité de récupération des paramètres de configuration précédemment utilisés après le redémarrage du client ou du serveur

## Différences entre DHCP et BOOTP (2)

- **2 - Allocation dynamique des adresses réseaux:**
  - Utilise automatiquement une adresse qui n'est plus utilisée.
  - Adresse allouée pour une durée déterminée (ou infinie): le bail.
  - Utilité:
    - Connexion temporaire au réseau.
    - Partage d'une liste limitée d'adresses IP.



# Dynamic Host Configuration Protocol

Les messages échangés

# Les messages transmis

- Plusieurs types de messages DHCP transmis via UDP
- Spécifié dans l'option 'type du message DHCP' de la trame DHCP
- Comme un seul « aller-retour » n'est pas suffisant pour une configuration complète
  - Plusieurs messages sont nécessaires pour une configuration
- Le client utilise le port 68, le serveur le port 67

# Mécanisme d'une allocation d'adresse

- Recherche d'un serveur DHCP:
  - Broadcast d'un message DHCPDISCOVER sur son réseau local physique.
  - Peut utiliser les options 50 et 51 qui suggèrent des valeurs pour son @IP et sa durée du bail.

# Les différents messages

- **DHCPDISCOVER (1)**
  - Diffusion du client pour localiser les serveurs disponibles.
  - Demande une première configuration.

# Mécanisme d'une allocation d'adresse

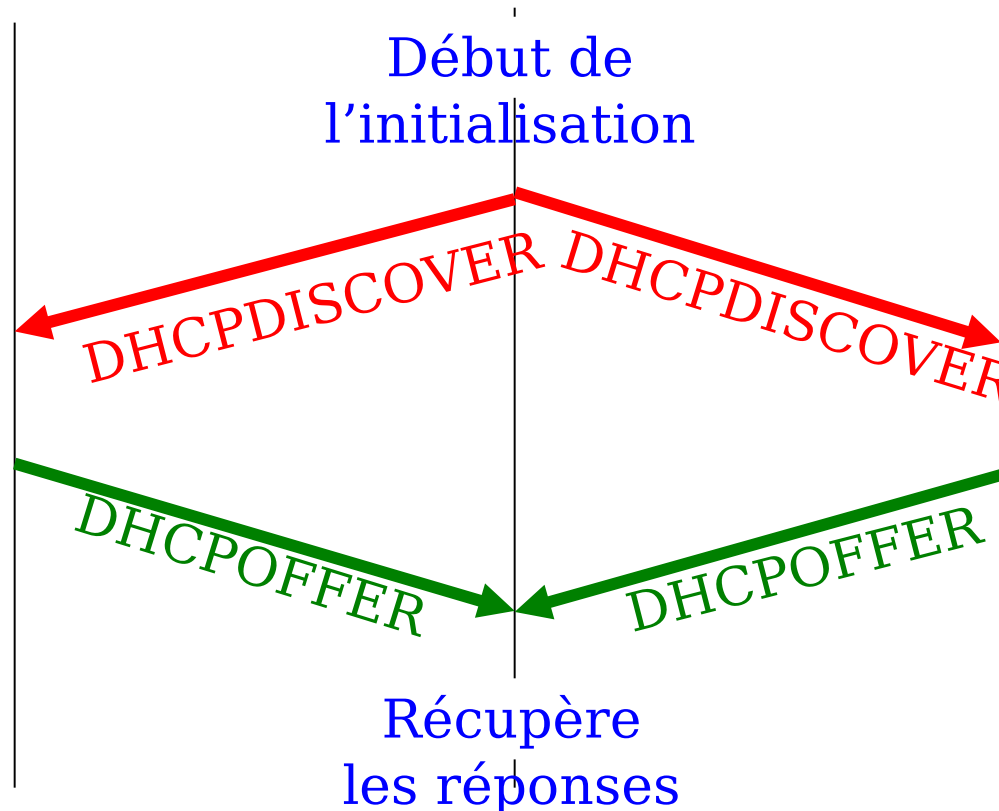
Serveur  
(non sélectionné)

Client

Serveur  
(sélectionné)

Détermine la  
configuration

Détermine la  
configuration



# Mécanisme d'une allocation d'adresse

- **Détermination de la configuration:**
  - Envoie d'un message DHCPOFFER en réponse au DHCPDISCOVER
  - Adresse réseau valide dans un champ appelé 'yiaddr'
  - Réponse aux différentes options demandées
- **Remarque:**
  - Si le client ne reçoit pas le DHCPOFFER au bout d'un délai d'attente, il retransmet son DHCPDISCOVER



# Mécanisme d'une allocation d'adresse

- **Récupération et choix de la configuration:**
  - Réception d'un ou plusieurs messages DHCPOFFER d'un ou plusieurs serveurs.
  - Choix du serveur pour ses paramètres
  - Diffusion d'un message DHCPREQUEST avec:
    - Option 'identifiant serveur',
    - Possibilité d'option spécifiant les valeurs de configuration désirées.
  - Relayé grâce à l'agent de relais

# Les différents messages

## → DHCPREQUEST (3)

- Message du client aux serveurs
- Qui demande les paramètres à un serveur et décline implicitement les offres de tous les autres,
- Qui confirme la validité des adresses précédemment alloués
- Qui étend le bail sur une adresse réseau en particulier

# Mécanisme d'une allocation d'adresse

- **Confirmation ou non de la configuration:**
  - Serveurs non sélectionnés par le message DHCPREQUEST: le client décline leur offre
  - Serveur sélectionné renvoie un DHCPACK qui contient la configuration pour le client demandeur.
  - Envoie de DHCPNAK si le serveur est indisponible (ex: @IP demandée déjà allouée)

# Les différents messages

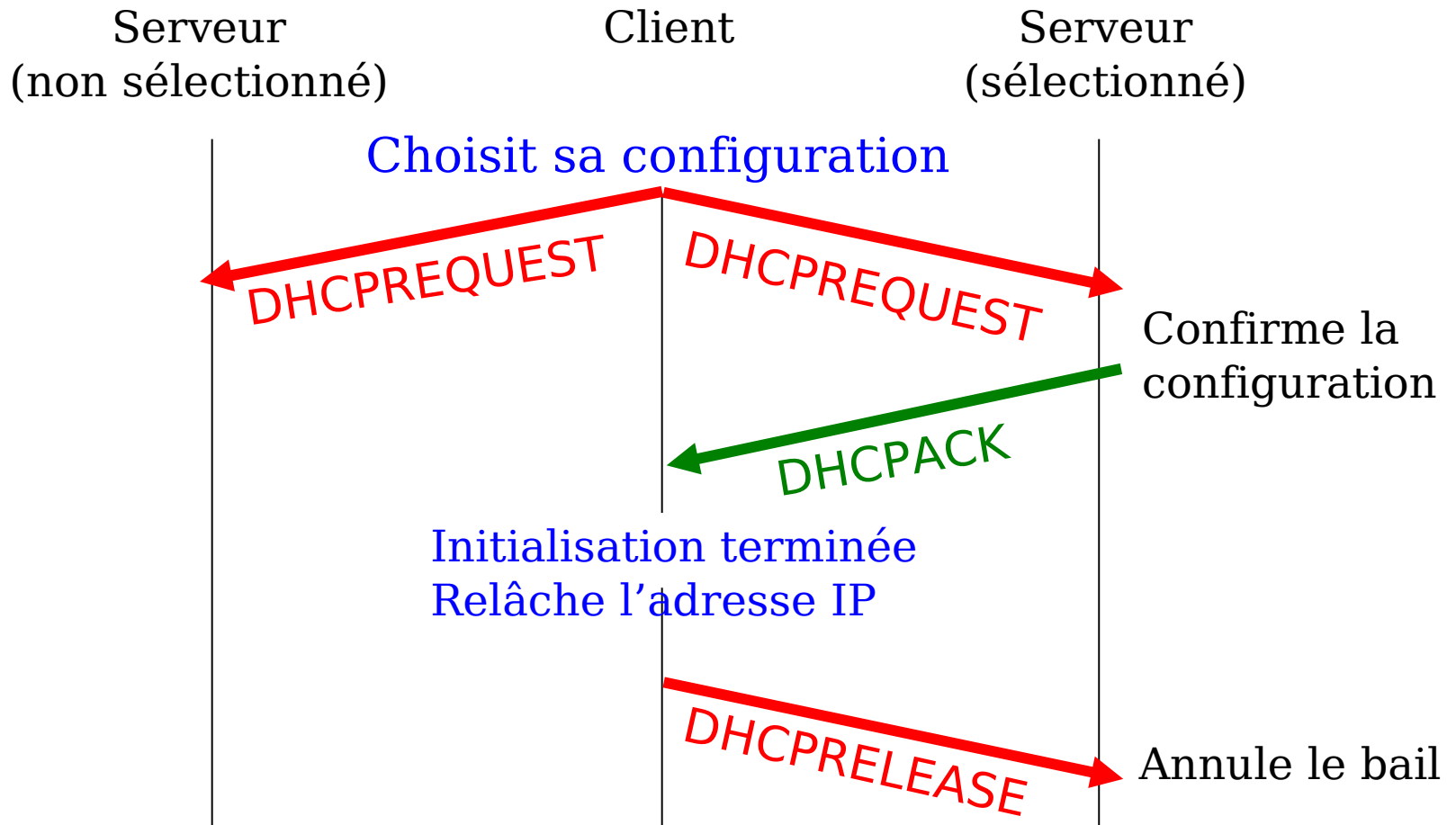
## → DHCPACK (5)

- Message du serveur au client
- Incluant les paramètres demandés dans le DHCPREQUEST.
- Incluant l'adresse IP déjà attribuée.

## → DHCPNAK (6)

- Message du serveur au client
- La notion d'un client pour les adresses réseau est incorrecte (il a changé de sous-réseau)
- Ou le bail du client a expiré.

# Mécanisme d'une allocation d'adresse



# Les différents messages

## → DHCPDECLINE (4)

- Message du client vers le serveur
- Adresse réseau déjà utilisée.

## → DHCPRELEASE (7)

- Message du client vers le serveur
- Libère l'adresse réseau
- Annule le bail.

# Mécanisme d'une allocation d'adresse

- **Configuration ou relance:**
  - Réception de DHCPACK avec les paramètres de configuration
  - Vérification de l'adresse IP:
    - Utilisation de ARP
    - S'il constate que l'adresse est déjà utilisée, il envoie un message DHCPDECLINE au serveur
  - Le client est alors configuré.

# Mécanisme d'une allocation d'adresse

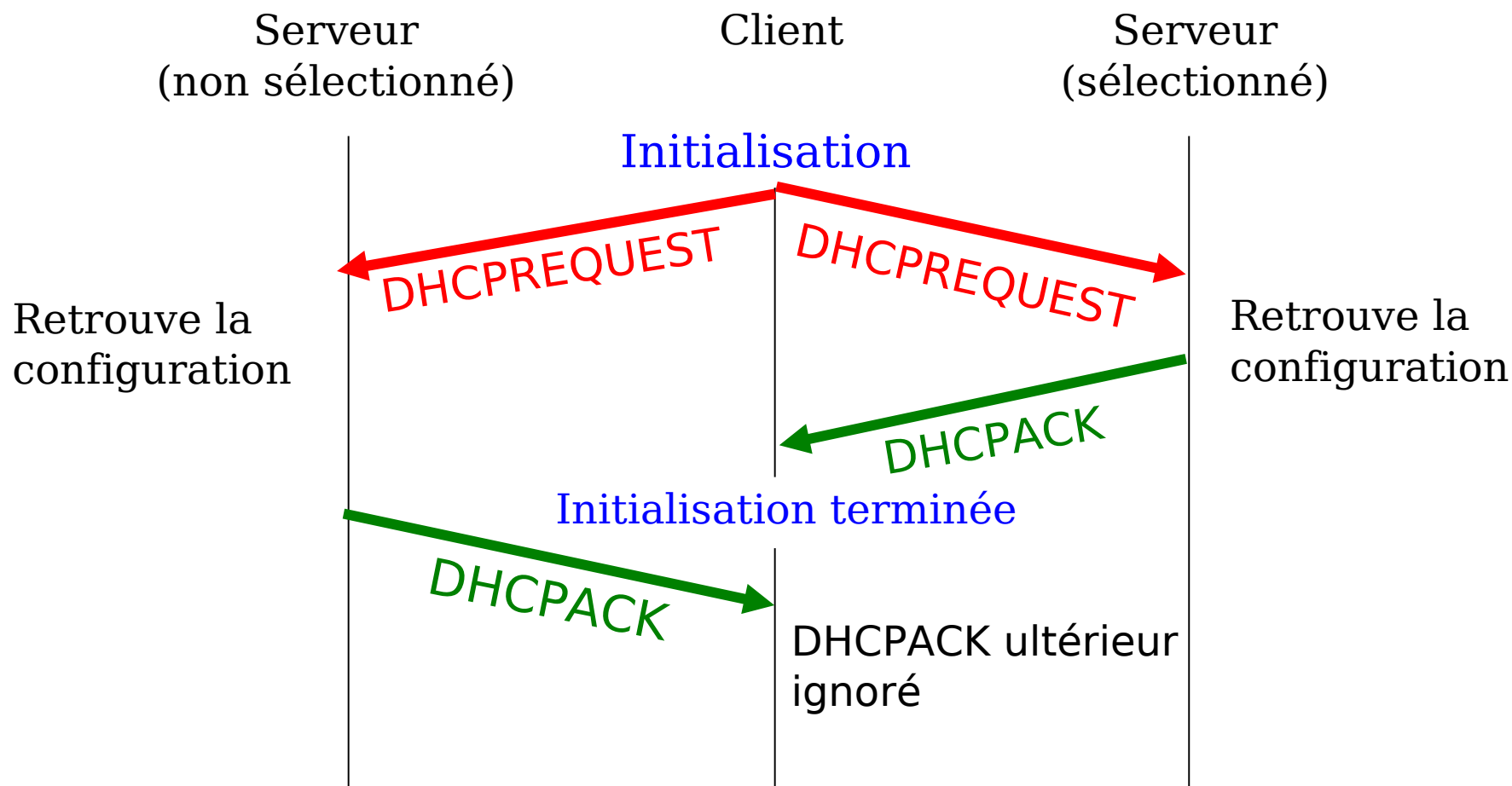
- **Configuration ou relance (suite):**
  - Réception d'un DHCPNAK,
    - le client relance la configuration.
  
  - Ni DHCPACK, ni DHCPNAK,
    - Il attend,
    - Il effectue un processus de retransmission de DHCPREQUEST jusqu'à 4 fois en 60 secondes.
    - Au bout d'un certain temps sans réponse, il relance l'initialisation



# Mécanisme d'une allocation d'adresse

- **Relâche de son adresse IP:**
  - Peut choisir de renoncer à son bail sur une adresse réseau => Envoi de DHCPRELEASE
  - Bail identifié grâce à ('identifiant client' ou 'chaddr') et l'adresse réseau
  - Mémorisation locale de son adresse réseau.
  - Le client ne renonce pas à son bail lors d'un arrêt normal

# Réutilisation d'une adresse



# Réutilisation d'une adresse

- ➔ **Demande de réutilisation d'une adresse:**
  - ➔ Diffusion d'un message DHCPREQUEST sur le sous-réseau du client avec son adresse réseau dans l'option 'adresse IP demandée'.
  - ➔ Les agents de relais transmettent le message au serveur DHCP si celui-ci n'est pas sur le même sous réseau.
  - ➔ Utilisation du même 'identifiant client'.

# Les différents messages

- Si le client possède déjà une adresse réseau attribuée de manière externe, il doit compléter sa configuration:
  - **DHCPINFORM(8)**
    - Message du client vers le serveur
    - Récupère les paramètres de configuration locaux

# Réutilisation d'une adresse

- Localisation de la configuration:
  - Les serveurs qui connaissent les paramètres de configuration du client lui répondent avec un DHCPACK.
  - Pas de vérification de l'adresse IP du client.
  - Diffusion du DHCPACK par un broadcast.
  - Si le client et le serveur ne sont pas sur même sous-réseau => Envoi d'un message DHCPACK à l'adresse de l'agent de relais, comme enregistré dans le champ 'giaddr'.

# Réutilisation d'une adresse

- **Vérification finale des paramètres:**
  - Si OK, configuration terminée.
  - Sinon doit relancer une nouvelle configuration:
    - Si @IP utilisée, le client envoie DHCPDECLINE.
    - Si réception d'un DHCPNAK
- Algorithme de retransmission si non réception de DHCPACK ou DHCPNAK.

# Adresse configurée extérieurement

- Adresse réseau obtenue grâce à d'autres moyens (ex:config. manuelle)
- Utilisation d'une requête DHCPINFORM pour obtenir des paramètres de configuration locaux
- Le serveur répond:
  - Sans allouer l'adresse réseau
  - Sans inclure les durées de bail
  - Sans vérifier de lien

# La trame DHCP (1)

0	8	16	24
Type du message (op)	Type de l'@MAC (htype)	Longueur de l'@MAC (hlen)	(hops)
Identifiant de la transaction choisi aléatoirement (xid)			
Temps écoulé depuis le debut de la transaction (secs)		(flags)	
@IP du client (ciaddr)			
@IP du client renvoyée par le serveur DHCP (yiaddr)			
@IP du serveur à utiliser pour le processus de démarrage (siaddr)			
@IP de l'agent de relais DHCP (giaddr)			
@MAC du client (chaddr)			
@ optionnelle d'un serveur (sname)			
Nom de fichier de démarrage (file)			
(options)			



## La trame DHCP (2)

Type du message ( <b>op</b> )	Type de l'@MAC ( <b>htype</b> )	Longueur de l'@MAC ( <b>hlen</b> )	( <b>hops</b> )
-------------------------------	---------------------------------	------------------------------------	-----------------

- **op** (1 octet):
  - 1 = BOOTREQUEST, 2 = BOOTREPLY
- **htype** (1 octet):
  - Ex: 1 = Ethernet 10Mb/s
- **hlen** (1 octet):
  - Ex: '6' pour une @Ethernet 10Mb
- **hops** (1 octet):
  - Permet de compter le nombre de sauts de la source au destinataire

## La trame DHCP (3)

Identifiant de la transaction choisi aléatoirement ( <b>xid</b> )	
Temps écoulé depuis le debut de la transaction ( <b>secs</b> )	<b>(flags)</b>

- **xid** (4 octets):
  - Identifiant de la transaction choisi aléatoirement
- **secs** (2 octets):
  - Temps écoulé depuis le debut de la transaction
- **Flags** (2 octets):
  - Le bit le plus à gauche est appelé « Flag de diffusion »

## La trame DHCP (4)

@IP du client (**ciaddr**)

@IP du client renvoyée par le serveur DHCP (**yiaddr**)

- **ciaddr** (4 octets):
  - @IP des clients, rempli seulement si le client est dans un état AFFECTE, RENOUELEMENT ou REAFFECTATION et peut répondre aux requêtes ARP.
- **yiaddr** (4 octets):
  - @IP du client (renvoyée par le serveur)

## La trame DHCP (5)

@IP du serveur à utiliser pour le processus de démarrage (**siaddr**)

@IP de l'agent de relais DHCP (**giaddr**)

- **siaddr** (4 octets):
  - @IP du prochain serveur à utiliser pour le processus de démarrage. (renseigné dans les messages DHCP OFFER et DHCPACK).
- **giaddr** (4 octets):
  - @IP de l'agent de relais, utilisée pour démarrer via un agent de relais.

## La trame DHCP (6)

@MAC du client (chaddr)
@ optionnelle d'un serveur (sname)
Nom de fichier de démarrage (file)

- **chaddr** (16 octets):
  - @MAC du client
- **sname** (64 octets):
  - Nom d'hôte du serveur optionnel
- **file** (128 octets):
  - Nom du fichier de démarrage

# La trame DHCP (7)

(options)

- Une option est composée de:
  - Un identifiant (code de l'option)
  - La longueur des données
  - La valeur de l'option
- De longueur variable entre 312 et 340 octets.
- Option obligatoire de taille fixe:
  - 'end' pour terminer la liste des options, code 255.
  - 'pad' pour le remplissage, code 0.

# Options spécifiques à DHCP (1)

- Adresse IP demandée:
  - Code 50, longueur 4
  - Permet au client de demander l'affectation d'une @IP particulière.
- Durée de bail de l'adresse IP:
  - Code 51, longueur 4
  - Client -> Serveur: Permet de demander une durée de bail pour l'@IP.
  - Serveur -> Client: Utilise cette option pour spécifier la durée du bail qu'il est disposé à offrir.

## Options spécifiques à DHCP (2)

- **Taille maximum des messages:**
  - Code 57, longueur 2
  - Spécifie la taille maximum d'un message DHCP(min 576o)
- **Utilisation des champs « file » / « sname »:**
  - Code 52, longueur 1
  - Indique que les champs DHCP 'sname' ou 'file' sont utilisés pour transporter des options.

1	Le champ 'file' est utilisé pour contenir des options
2	Le champ 'sname' est utilisé pour contenir des options
3	Les deux champs sont utilisés



## Options spécifiques à DHCP (3)

- **Type du message DHCP:**
  - Code 53, longueur 1
  - Utilisée pour transporter le type du message DHCP (valeur de 1 à 8).
- **Liste des paramètres requis:**
  - Code 55, longueur de 1 à n
  - Utilisée par un client DHCP pour demander des valeurs de paramètres de configuration spécifique.

# Options spécifiques à DHCP (4)

- **Identifiant serveur:**
  - Code 54, longueur 4
  - Adresse IP du serveur sélectionné
  
- **Identifiant client:**
  - Code 61, longueur 2
  - Utilisée par les clients DHCP pour spécifier leur identifiant unique.
  - Utilisée par les serveurs dans leur base de données pour l'affectation des adresses.



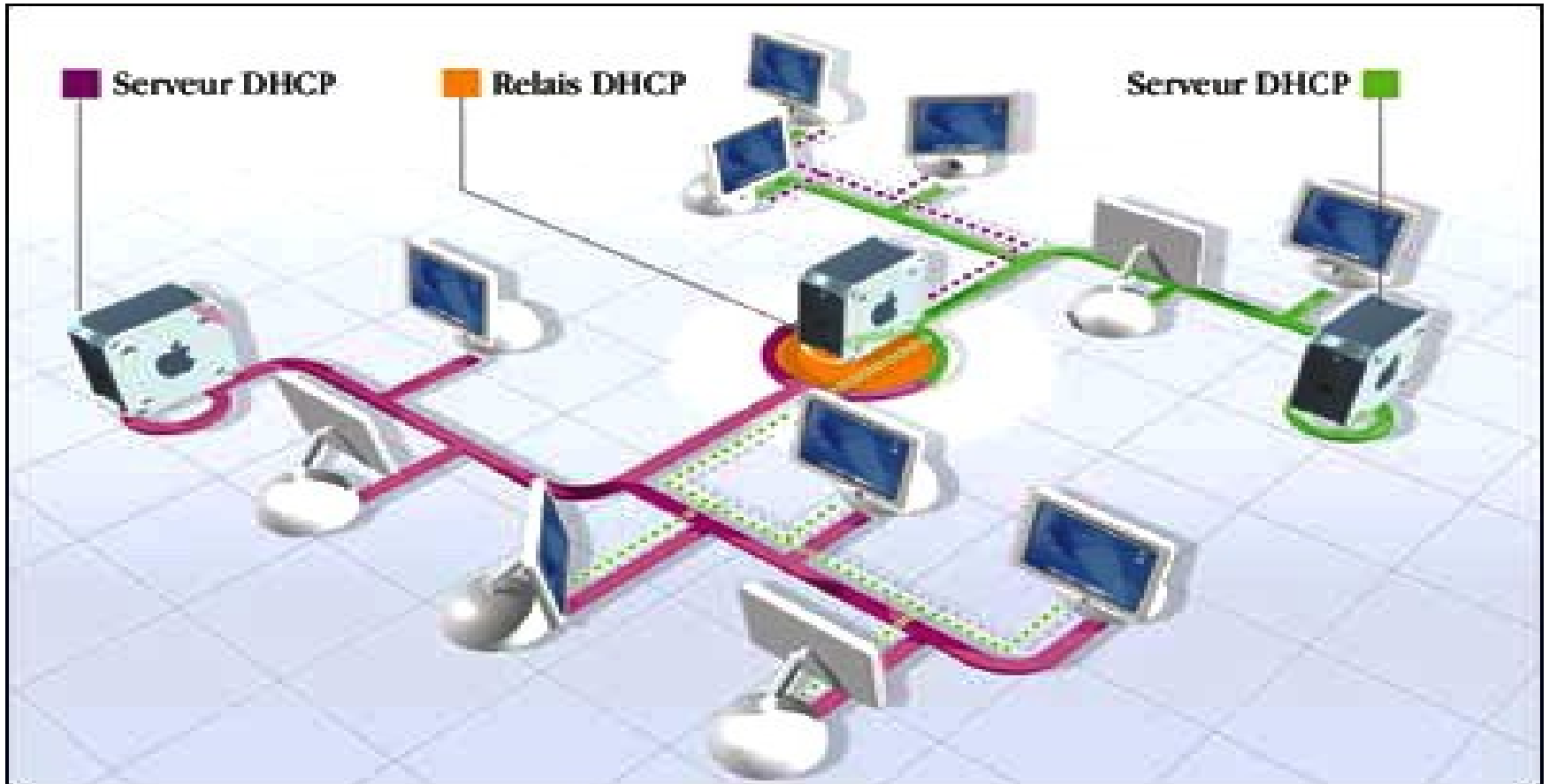
# Dynamic Host Configuration Protocol

La sécurité

# Sécurité

- Les failles de sécurité peuvent provenir des deux côtés du modèle client-serveur.
- Client pirate DHCP :
  - capable d'accéder à des ressources protégées si la protection ne repose que sur une identification de l'adresse IP, ce qu'il vaut donc mieux éviter.
  - pourra paralyser le serveur en consommant les adresses IP rapidement sans les libérer.

# Limiter les problèmes



# Agent de relais

- Une machine sur internet ou un routeur.
  - Transmet des messages entre clients et serveurs DHCP.
  - Incrémente le champ 'hops' de la trame DHCP.
  - Permet à un client d'interroger un serveur DHCP qui n'est pas sur le même sous-réseaux

# Sécurité

- Serveur parasite :
  - capable d'envoyer de fausses informations de configuration aux clients dont il acquittera les requêtes.
- Existence de logiciels capables:
  - de surveiller les paquets DHCP sur un réseau
  - de donner l'alerte s'ils en détectent qui ne proviennent pas de serveurs autorisés.

# Quand utiliser DHCP ?

- Pour obtenir ou vérifier une @IP et ses paramètres chaque fois que les paramètres locaux changent
- Si le client connaît une @IP et est incapable de se connecter à un serveur DHCP local, il peut continuer à utiliser cette @ jusqu'à expiration du bail.
- Après expiration du bail, le client ne peut plus utiliser cette adresse.





# Dynamic Host Configuration Protocol

Conclusion

# Conclusion

- Configuration sûre et fiable
  - Évite les erreurs dues à l'enregistrement manuel.
  - Empêche les conflits causés par l'utilisation double d'une même adresse.
- Réduction de la gestion de la configuration
  - Diminue le temps de configuration.
  - Renouvellement de bail automatique.
  - Possibilité de récupération des paramètres de configuration précédemment utilisés après le redémarrage du client ou du serveur.