Dépannage du protocole DHCP (Dynamic Host Configuration Protocol) dans les commutateurs Catalyst ou les réseaux d'entreprise

Contenu

Introduction

Ce document décrit comment dépanner plusieurs problèmes courants avec le protocole DHCP (Dynamic Host Configuration Protocol) dans un réseau de commutateurs Cisco Catalyst.

Conditions préalables

Conditions requises

Aucune condition préalable spécifique n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

> **Note**: Seuls les clients Cisco enregistrés ont accès aux rapports de bogue internes.

Informations générales

DHCP fournit un mécanisme par lequel les ordinateurs qui utilisent le protocole TCP/IP (Transmission Control Protocol/Internet Protocol) peuvent obtenir des paramètres de configuration du protocole automatiquement via le réseau. DHCP est une norme ouverte développée par le Groupe dédié à la configuration des hôtes dynamiques (DHC-WG) du groupe de travail Internet Engineering Task Force (IETF).

DHCP est basé sur un paradigme client-serveur, dans lequel le client DHCP, par exemple un ordinateur de bureau, entre en contact avec un serveur DHCP pour obtenir des paramètres de configuration. Le serveur DHCP est en général situé dans un emplacement central et utilisé par l'administrateur réseau. Puisque le serveur est exécuté par un administrateur réseau, les clients DHCP peuvent être configurés de façon fiable et dynamique avec les paramètres appropriés pour l'architecture réseau actuelle.

La plupart des réseaux d'entreprise se composent de plusieurs sous-réseaux divisés à leur tour en sous-réseaux appelés LAN virtuels (VLAN), où les routeurs transfèrent les données entre les sous-réseaux. Étant donné que les routeurs ne transmettent pas les diffusions par défaut, un serveur DHCP est nécessaire sur chaque sous-réseau, sauf si les routeurs sont configurés pour transférer la diffusion DHCP avec la fonctionnalité d'agent de relais DHCP.

Concepts clés

Voici plusieurs concepts clés de DHCP :

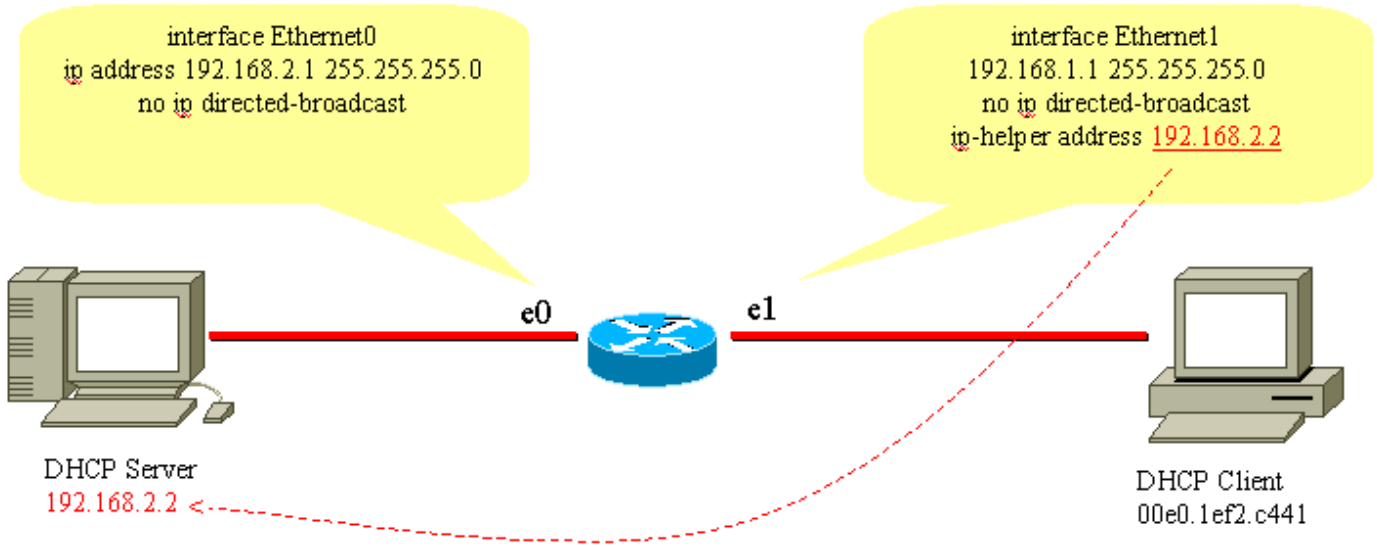
- Les clients DHCP n'ont initialement aucune adresse IP configurée et doivent donc envoyer une requête de diffusion pour obtenir une adresse IP d'un serveur DHCP.
- Par défaut, les routeurs ne transfèrent pas les diffusions. Il est nécessaire d'accueillir les demandes de diffusion du client DHCP si le serveur DHCP se trouve dans un autre domaine de diffusion (réseau de couche 3 (L3)). Cette opération est effectuée à l'aide d'un agent relais DHCP.
- La mise en œuvre du routeur Cisco du relais DHCP est réalisée par l'intermédiaire de commande **ip helper au niveau de l'interface.**

Exemples de scénarios

Scénario 1 : Routage de routeur Cisco entre les réseaux client et serveur DHCP

Comme configuré dans ce schéma, l’interface Ethernet1 transfère le message DHCPDISCOVER

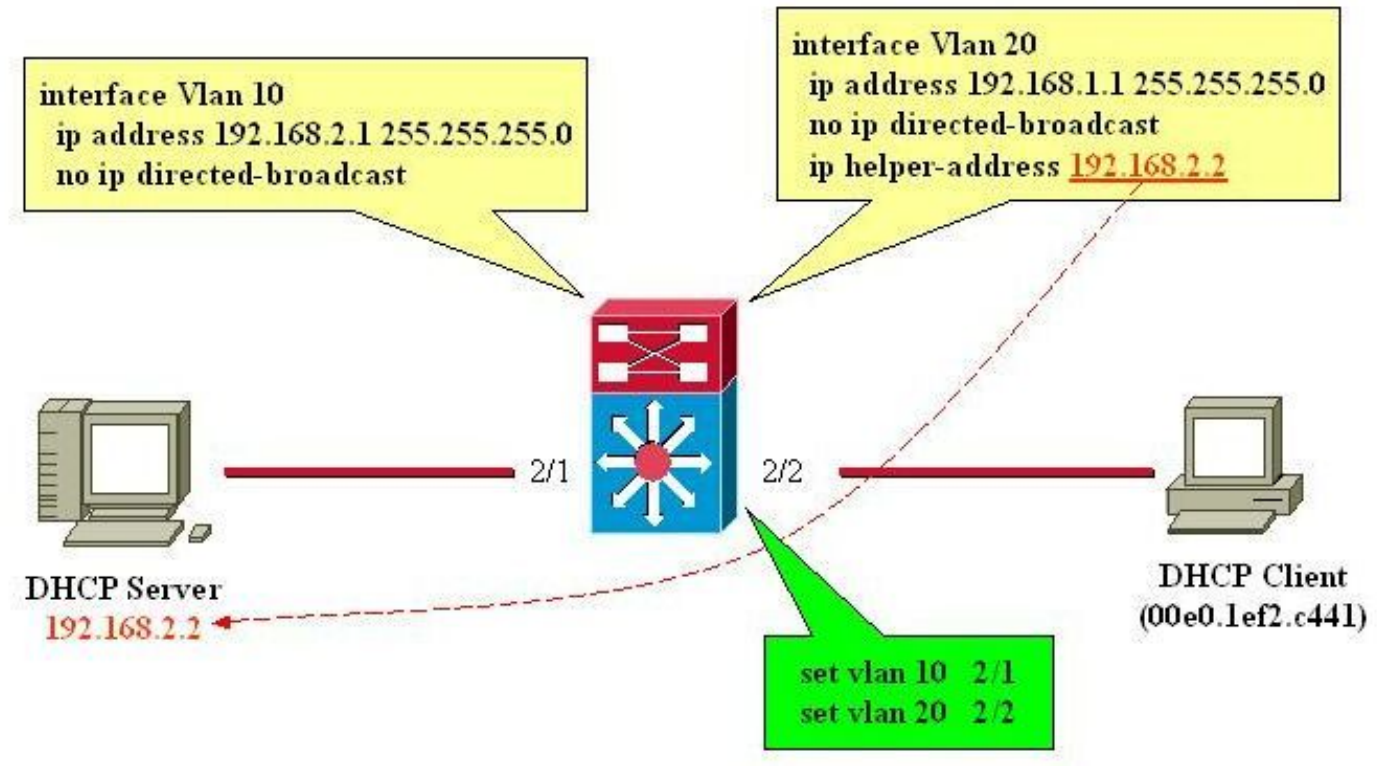
diffusé par le client vers 192.168.2.2 via l'interface Ethernet1. Le serveur DHCP exécute la requête par monodiffusion. Aucune autre configuration du routeur n'est nécessaire dans cet exemple.



Routage entre les réseaux client et serveur DHCP

Scénario 2 : Commutateur Cisco Catalyst avec routage de module L3 entre les réseaux client et serveur DHCP

Comme configuré dans le schéma, l'interface VLAN20 transfère le message DHCPDISCOVER diffusé par le client à l'adresse 192.168.2.2 via l'interface VLAN10. Le serveur DHCP exécute la requête par monodiffusion. Aucune autre configuration du routeur n'est nécessaire dans cet exemple. Les ports de commutateur doivent être configurés comme ports hôtes et avec STP (Spanning-Tree Protocol) portfast activé, et l'agrégation de liaison et l'acheminement désactivés.



Route du module L3 entre les réseaux client et serveur DHCP

Comprendre DHCP

DHCP a été défini à l'origine dans les RFC 1531 et a depuis été obsolète par la RFC 2131. DHCP est basé sur le protocole Bootstrap (BootP), qui est défini dans la RFC 951.

DHCP est utilisé par les postes de travail (hôtes) pour obtenir les informations de configuration initiale, telles qu'une adresse IP, un masque de sous-réseau et une passerelle par défaut au démarrage. Avec DHCP, vous n'avez pas besoin de configurer manuellement chaque hôte avec une adresse IP. En outre, si un hôte est déplacé vers un autre sous-réseau IP, il doit utiliser une autre adresse IP que celle précédemment utilisée. DHCP s'en charge automatiquement. Il permet également à l'hôte de choisir une adresse IP dans le sous-réseau IP correct.

Références RFC à DHCP actuelles

- RFC 2131 - DHCP
- RFC 2132 - Options DHCP et extensions fournisseur BootP
- RFC 1534 - Interopérabilité DHCP et BootP
- RFC 1542 - Clarifications et extensions pour BootP
- RFC 2241 - Options DHCP pour les services d'annuaire Novell
- RFC 2242 - Nom de domaine et informations Netware/IP
- RFC 2489 - Procédure de définition de nouvelles options DHCP

DHCP utilise un modèle client-serveur où un ou plusieurs serveurs (serveurs DHCP) allouent des adresses IP et d'autres paramètres de configuration facultatifs aux clients (hôtes) au démarrage du client. Ces paramètres de configuration sont loués par le serveur au client pour une durée spécifiée. À l'amorçage d'un hôte, la pile TCP/IP de l'hôte transmet un message de diffusion (DHCPDISCOVER) afin d'obtenir une adresse IP et un masque de sous-réseau, entre autres paramètres de configuration. Un échange est engagé entre le serveur DHCP et l'hôte. Au cours de cet échange, le client passe par ces états bien définis :

1. Initialisation
2. Sélection
3. Demande
4. Liaison
5. Renouvellement
6. Reliaison

Pour passer d'un état à l'autre, le client et le serveur peuvent échanger les types de messages répertoriés dans la table des messages DHCP.

Tableau des messages DHCP

Référence	Message	Description
0x01	DHCPDISCOVER	Le client recherche les serveurs DHCP disponibles.
0x02	DHCPOFFER	Réponse du serveur au paquet DHCPDISCOVER du client.
0x03	DHCPREQUEST	Le client diffuse au serveur, demande les paramètres offerts à un serveur en particulier, comme défini dans le paquet.
0x04	DHCPDECLINE	La communication client-serveur indique que l'adresse réseau est déjà utilisée.

0x05	DHCPACK	Communication serveur-client avec les paramètres de configuration, ainsi qu'une adresse réseau validée.
0x06	DHCPNAK	La communication serveur-client refuse la demande de paramètre de configurati
0x07	DHCPRELEASE	La communication client-serveur abandonne l'adresse réseau et annule le bail re
0x08	DHCPINFORM	La communication client-serveur ne demande que les paramètres de configuratio locale que le client a déjà configurés en externe comme adresse.

DHCPDISCOVER

Lors du premier démarrage du client, il est dit être à l'état d'initialisation, et transmet un message DHCPDISCOVER sur son sous-réseau physique local sur le port 67 UDP (User Datagram Protocol) (serveur BootP). Puisque le client n'a aucun moyen de connaître le sous-réseau auquel il appartient, DHCPDISCOVER est une diffusion de tous les sous-réseaux (adresse IP de destination 255.255.255.255), avec une adresse IP source 0.0.0.0. L'adresse IP source est 0.0.0.0 puisque le client n'a pas d'adresse IP configurée. Si un serveur DHCP existe sur ce sous-réseau local, est configuré et fonctionne correctement, le serveur DHCP entend la diffusion et répond avec un message DHCPOFFER. Si aucun serveur DHCP n'existe sur le sous-réseau local, un agent relais DHCP/BootP doit être présent sur ce sous-réseau local pour transférer le message DHCPDISCOVER à un sous-réseau qui contient un serveur DHCP.

Cet agent de relais peut être soit un hôte dédié (par exemple, Microsoft Windows Server), soit un routeur (par exemple, un routeur Cisco configuré avec des instructions IP helper de niveau interface).

DHCPOFFER

Un serveur DHCP qui reçoit un message DHCPDISCOVER peut répondre par un message DHCPOFFER sur le port UDP 68 (client BootP). Le client reçoit le message DHCPOFFER et passe à l'état Sélection. Ce message DHCPOFFER contient les informations de configuration initiale pour le client. Par exemple, le serveur DHCP remplit le champ yiaddr du message DHCPOFFER avec l'adresse IP demandée. Le masque de sous-réseau et la passerelle par défaut sont spécifiés dans le champ d'options, et les options de masque de sous-réseau et de routeur, respectivement. D'autres options communes dans le message DHCPOFFER sont la durée du bail de l'adresse IP, la date de renouvellement, le serveur de noms de domaine et le serveur de noms NetBIOS (WINS). Le serveur DHCP envoie le message DHCPOFFER à l'adresse de diffusion, mais inclut l'adresse matérielle du client dans le champ chaddr de l'offre, afin que le client sache qu'il s'agit de la destination prévue. Dans le cas où le serveur DHCP ne se trouve pas sur le sous-réseau local, le serveur DHCP renvoie le paquet DHCPOFFER, en tant que paquet de monodiffusion, sur le port UDP 67, à l'agent relais DHCP/BootP d'où provient le paquet DHCPDISCOVER. L'agent relais DHCP/BootP diffuse ou monodiffuse ensuite le message DHCPOFFER sur le sous-réseau local sur le port UDP 68, qui dépend de l'indicateur de diffusion défini par le client Boot.

DHCPREQUEST

Une fois que le client a reçu un message DHCPOFFER, il répond par un message

DHCPREQUEST et indique son intention d'accepter les paramètres du message DHCPOFFER, puis passe à l'état Demandeur. Le client peut recevoir plusieurs messages DHCPOFFER, un de chaque serveur DHCP qui a reçu le message DHCPDISCOVER d'origine. Le client choisit un message DHCPOFFER et répond uniquement à ce serveur DHCP et, implicitement, refuse tous les autres messages DHCPOFFER. Le client identifie le serveur sélectionné après avoir renseigné le champ d'option Server Identifier avec l'adresse IP du serveur DHCP. Le message DHCPREQUEST est également une diffusion, de sorte que tous les serveurs DHCP qui ont envoyé un message DHCPOFFER voient le message DHCPREQUEST, et chacun sait si son message DHCPOFFER a été accepté ou refusé. Toutes les options de configuration supplémentaires requises par le client sont incluses dans le champ d'options du message DHCPREQUEST. Bien qu'une adresse IP ait été proposée au client, celui-ci envoie le message DHCPREQUEST avec l'adresse IP source 0.0.0.0. À ce stade, le client n'a pas encore reçu la vérification qu'il est prêt à utiliser l'adresse IP.

DHCPACK

Une fois que le serveur DHCP a reçu le message DHCPREQUEST, il accuse réception de la demande avec un message DHCPACK, puis termine le processus d'initialisation. Le message DHCPACK a une adresse IP source du serveur DHCP, et l'adresse de destination est à nouveau une diffusion et contient tous les paramètres que le client a demandé dans le message DHCPREQUEST. Lorsque le client reçoit le message DHCPACK, il passe à l'état Liaison, et est alors libre d'utiliser l'adresse IP pour communiquer sur le réseau. Pendant ce temps, le serveur DHCP stocke le bail dans sa base de données et l'identifie de manière unique avec l'identifiant client ou chaddr, et l'adresse IP associée. Le client et le serveur utilisent tous deux cette combinaison d'identificateurs pour faire référence au bail. L'identificateur client est l'adresse MAC du périphérique plus le type de support.

Avant que le client DHCP commence à utiliser la nouvelle adresse, il doit calculer les paramètres de temps associés à une adresse louée, à savoir le temps de bail (LT), le temps de renouvellement (T1) et le temps de reconnexion (T2). Par défaut, LT est de 72 heures. Vous pouvez utiliser des durées de bail inférieures afin de conserver les adresses, si nécessaire.

DHCPNAK

Si le serveur sélectionné ne parvient pas à satisfaire le message DHCPREQUEST, le serveur DHCP répond avec un message DHCPNAK. Lorsque le client reçoit un message DHCPNAK ou ne reçoit pas de réponse à un message DHCPREQUEST, il redémarre le processus de configuration lorsqu'il passe à l'état Demandeur. Le client retransmet le message DHCPREQUEST au moins quatre fois dans les 60 secondes qui précèdent le redémarrage de l'état Initializing.

DHCPDECLINE

Le client reçoit le message DHCPACK et, éventuellement, effectue une vérification finale des paramètres. Le client exécute cette procédure lorsqu'il envoie des requêtes ARP (Address Resolution Protocol) pour l'adresse IP fournie dans le DHCPACK. Si le client détecte que l'adresse est déjà utilisée lorsqu'il reçoit une réponse à la requête ARP, il envoie un message DHCPDECLINE au serveur et redémarre le processus de configuration à l'état Demandeur.

DHCPINFORM

Si un client a obtenu une adresse réseau par un autre moyen ou a une adresse IP configurée manuellement, une station de travail client peut utiliser un message de requête DHCPINFORM pour obtenir d'autres paramètres de configuration locale, tels que le nom de domaine et les serveurs de noms de domaine (DNS). Lorsque les serveurs DHCP reçoivent un message DHCPINFORM, créez un message DHCPACK avec tous les paramètres de configuration locale appropriés pour le client sans nouvelle adresse IP. Ce DHCPACK est envoyé en monodiffusion au client.

DHCPRELEASE

Un client DHCP peut choisir de renoncer à son bail sur une adresse réseau lorsqu'il envoie un message DHCPRELEASE au serveur DHCP. Le client identifie le bail à libérer en utilisant le champ d'identification `du client` et l'adresse réseau dans le message DHCPRELEASE. Si vous devez étendre la plage actuelle du pool DHCP, supprimez le pool actuel d'adresses et spécifiez la nouvelle plage d'adresses IP sous le pool DHCP. Afin de supprimer des adresses IP spécifiques ou une plage d'adresses que vous voulez placer dans le pool DHCP, utilisez la commande **ip dhcp excluded-address**.

> **Note**: Si les périphériques utilisent le protocole BOOTP, les baux à durée indéfinie sont indiqués dans les liaisons DHCP des routeurs.

Renouveler le bail

Puisque l'adresse IP est seulement louée auprès du serveur, le bail doit être renouvelé de temps en temps. Lorsque la moitié du bail a expiré (T1=0,5 x LT), le client tente de renouveler le bail. Le client passe à l'état Renouvellement et envoie un message DHCPREQUEST au serveur, qui détient le bail en cours. Le serveur répond à la demande de renouvellement par un message DHCPACK s'il accepte de renouveler le bail. Le message DHCPACK contient le nouveau bail et tous les nouveaux paramètres de configuration, au cas où des modifications seraient apportées au serveur au cours du bail précédent. Si le client ne parvient pas à joindre le serveur lorsqu'il conserve le bail pour une raison quelconque, il tente de renouveler l'adresse à partir de n'importe quel serveur DHCP après que le serveur DHCP d'origine n'a pas répondu aux demandes de renouvellement dans un délai T2. La valeur par défaut de T2 est (7/8 x LT). Cela signifie que T1 < T2< LT.

Si le client avait précédemment une adresse IP attribuée par DHCP et qu'il est redémarré, le client demande spécifiquement l'adresse IP précédemment louée dans un paquet DHCPREQUEST. Cette requête DHCPREQUEST a toujours l'adresse IP source comme 0.0.0.0 et la destination comme adresse de diffusion IP 255.255.255.255.

Lorsqu'un client envoie un message DHCPREQUEST au cours d'un redémarrage, il ne doit pas remplir le champ d'identification du serveur, mais le champ d'option de l'adresse IP demandée. Seuls les clients compatibles RFC remplissent le champ ciaddr avec l'adresse demandée au lieu du champ d'option DHCP. Le serveur DHCP accepte l'une ou l'autre méthode. Le comportement du serveur DHCP dépend d'un certain nombre de facteurs, tels que, dans le cas des serveurs DHCP Windows NT, la version du système utilisée, ainsi que d'autres facteurs, tels que l'étendue globale. Si le serveur DHCP détermine que le client peut toujours utiliser l'adresse IP demandée, il reste silencieux ou envoie un message DHCPACK pour le message DHCPREQUEST. Si le serveur détermine que le client ne peut pas utiliser l'adresse IP demandée, il renvoie un message DHCPNACK au client. Le client passe ensuite à l'état Initializing (Initialisation) et envoie un message DHCPDISCOVER.

Note: Le serveur DHCP assigne la dernière adresse IP d'un pool d'adresses IP aux clients DHCP. Lorsque le bail de la dernière adresse expire, elle est assignée à un autre client si elle est demandée. Vous ne pouvez apporter aucune modification à l'ordre dans lequel les adresses DHCP sont assignées.

Table des paquets DHCP

Le message DHCP est de longueur variable et se compose des champs répertoriés dans la table des paquets DHCP.

Note: Ce paquet est une version modifiée du paquet BootP initial.

Champ	Octets	Name (nom)	Description
op	1	OpCode	Identifie le paquet en tant que requête ou réponse : 1=BOOTREQUEST 2=BOOTREPLY
htype	1	Type de matériel	Spécifie le type d'adresse du matériel réseau.
hlen	1	Longueur de matériel	Spécifie la longueur de l'adresse du matériel réseau.
hops	1	Tronçons	Le client définit la valeur à zéro et les incréments de valeur si la demand transférée via un routeur.
xid	4	ID de transaction	Nombre aléatoire choisi par le client. Tous les message DHCP échangé pour une transaction DHCP donnée utilise l'ID (xid).
secs	2	Secondes	Spécifie le nombre de secondes depuis le début du processus DHCP.
indicatifs	2	Indicatifs	Indique si le message est diffusé ou monodiffusé.
ciaddr	4	Adresse IP du client	Utilisé uniquement lorsque le client connaît son adresse IP, par exemple le cas des états Liaison, Renouvellement ou Nouvelle liaison.
yiaddr	4	Votre adresse IP	Si l'adresse IP du client est 0.0.0.0, le serveur DHCP place l'adresse IP client offerte dans ce champ.
siaddr	4	Adresse IP du serveur	Si le client connaît l'adresse IP du serveur DHCP, ce champ est renseig avec l'adresse du serveur DHCP. Sinon, elle est utilisée dans les messa DHCPOFFER et DHCPACK du serveur DHCP.
giaddr	4	Adresse IP du routeur (GI ADDR)	Adresse IP de passerelle, renseignée par l'agent relais DHCP/BootP.
chaddr	16	Adresse MAC du client	Adresse MAC du client DHCP.
sname	64	Nom de serveur	Nom d'hôte de serveur facultatif.
fichier	128	Nom du fichier de démarrage	Nom du fichier de démarrage.
options	variable	Paramètres d'option	Paramètres facultatifs qui peuvent être fournis par le serveur DHCP. RF 2132 donne toutes les options possibles.

Conversation client-serveur pour le client qui obtient une adresse DHCP où le client et le serveur DHCP résident sur le même sous-réseau

Description du paquet	Adr MAC source	Adr MAC de destination	Adr IP source	Adr IP de destination
DHCPDISCOVER	Client	Diffusion	0.0.0.0	255.255.255.255
DHCPOFFER	DHCPServer	Diffusion	DHCPServer	255.255.255.255

DHCPREQUEST	Client	Diffusion	0.0.0.0	255.255.255.255
DHCPACK	DHCPServer	Diffusion	DHCPServer	255.255.255.255

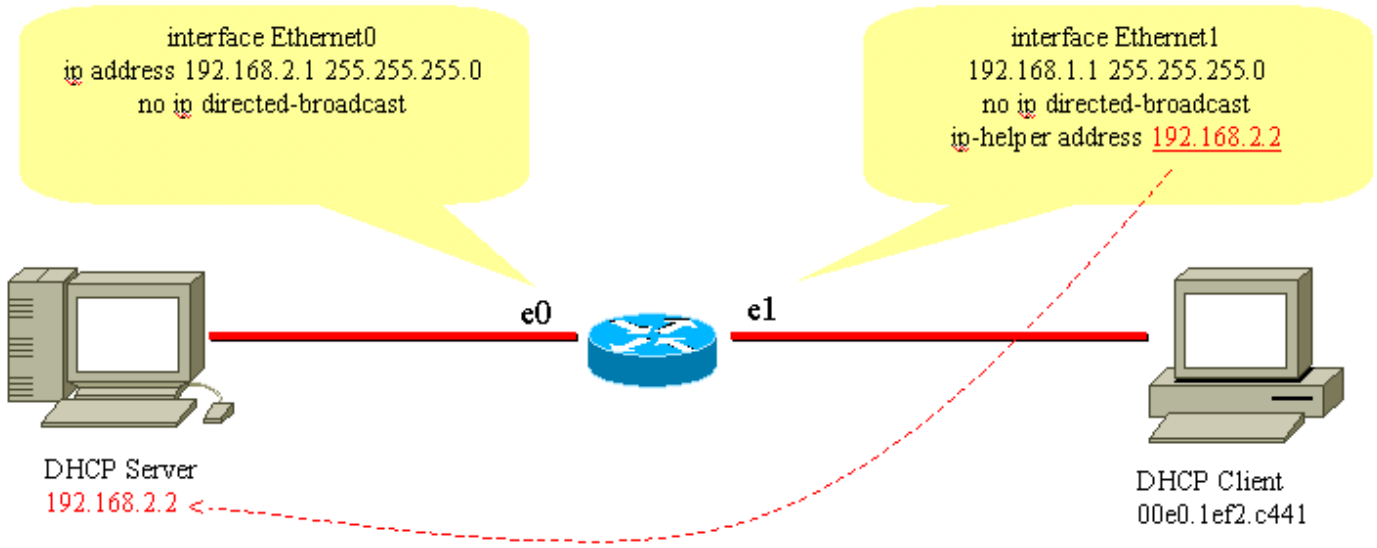
Rôle de l'agent relais DHCP/BootP

Par défaut, les routeurs ne transmettent pas les paquets de diffusion. Étant donné que les messages des clients DHCP utilisent l'adresse IP de destination 255.255.255.255 (tous les réseaux diffusés), les clients DHCP ne peuvent pas envoyer de requêtes à un serveur DHCP sur un sous-réseau différent à moins que l'agent de relais DHCP/BootP ne soit configuré sur le routeur. L'agent relais DHCP/BootP transfère les requêtes DHCP au nom d'un client DHCP au serveur DHCP. L'agent relais DHCP/BootP ajoute sa propre adresse IP à l'adresse IP source des trames DHCP qui accèdent au serveur DHCP. Ceci permet au serveur DHCP de répondre par monodiffusion à l'agent relais DHCP/BootP. L'agent relais DHCP/BootP renseigne également le champ d'adresse IP de passerelle avec l'adresse IP de l'interface sur laquelle le message DHCP est reçu du client. Le serveur DHCP utilise le champ d'adresse IP de passerelle pour déterminer de quel sous-réseau provient le message DHCPDISCOVER, DHCPREQUEST ou DHCPINFORM.

Configuration de la fonction Agent de relais DHCP/BootP sur le routeur Cisco IOS®

Le processus de configuration d'un routeur Cisco pour transférer des requêtes BootP ou DHCP est simple. Il vous suffit de configurer une adresse IP d'assistance qui pointe vers le serveur DHCP/BootP ou vers l'adresse de diffusion de sous-réseau du réseau sur lequel se trouve le serveur.

Exemple de réseau :



Agent de relais DHCP/BootP

Pour transférer la requête BootP/DHCP du client au serveur DHCP, **la** commande **ip helper-address interface** est utilisée. L'adresse IP auxiliaire peut être configurée pour transférer n'importe quelle diffusion UDP basée sur le numéro de port UDP. Par défaut, l'adresse IP helper-address transmet ces diffusions UDP :

- Trivial File Transfer Protocol (TFTP) (port 69)

- DNS (port 53), service horaire (port 37)
- Serveur de noms NetBIOS (port 137)
- Serveur de datagramme NetBIOS (port 138)
- Datagrammes de client et serveur du protocole de démarrage (DHCP/BootP) (ports 67 et 68)
- Service TACACS (Terminal Access Control Access Control System) (port 49)
- Service de noms IEN-116 (port 42)

Les adresses IP d'assistance peuvent diriger les diffusions UDP vers une adresse IP de monodiffusion ou de diffusion.Cependant, n'utilisez pas l'adresse IP d'assistance pour transférer les diffusions UDP d'un sous-réseau vers l'adresse de diffusion d'un autre sous-réseau, en raison de la grande quantité de diffusion qui peut se produire. Plusieurs entrées d'adresse d'assistance IP sur une seule interface sont également prises en charge :

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
!
!
interface Ethernet0
ip address 192.168.2.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet1
ip address 192.168.1.1 255.255.255.0
ip helper-address 192.168.2.2
ip helper-address 192.168.2.3

!--- IP helper-address pointing to DHCP server

no ip directed-broadcast
!
!
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

Les routeurs Cisco ne prennent pas en charge l'équilibrage de charge des serveurs DHCP qui sont configurés comme agents relais DHCP. Les routeurs Cisco transfèrent le message DHCPDISCOVER à toutes les adresses auxiliaires mentionnées pour cette interface. L'utilisation de deux serveurs DHCP ou plus pour servir un sous-réseau augmente uniquement le trafic DHCP, car les messages DHCPDISCOVER, DHCPOFFER et DHCPREQUEST / DHCPDECLINE sont échangés entre chaque paire de client et de serveur DHCP.

Définir les liaisons manuelles

Les liaisons manuelles peuvent être définies de deux façons ; l'une est pour l'hôte Windows, et l'autre est pour les hôtes non-Windows. Deux commandes différentes sont utilisées pour la

configuration ; l'une concerne les clients DHCP Microsoft, et l'autre concerne les clients DHCP non-Microsoft : **DHCPclient-identifier** (liaison manuelle - clients DHCP Microsoft) **et DHCPhardware-address** (liaison manuelle - clients DHCP non-Microsoft). La raison de deux commandes différentes est qu'un PC qui fonctionne avec Windows modifie ses adresses MAC, et a**01** est ajouté au début de l'adresse. Voici des exemples de configuration :

- Voici une configuration pour les clients DHCP Microsoft :

```
configure terminal
ip dhcp pool new_pool
host ip_address subnet_mask
client-identifier 01XXXXXXXXXXXX

!--- xxxxxx represents 48 bit MAC address prepended with 01
```

- Il s'agit d'une configuration pour les clients DHCP non-Microsoft :

```
configure terminal
ip dhcp pool new_pool
host ip_address subnet_mask
hardware-address XXXXXXXXXXXX

!--- xxxxxx represents 48 bit MAC address
```

Comment faire fonctionner DHCP sur les segments secondaires

Par défaut, DHCP est limité en ce que les paquets de réponse sont envoyés uniquement si la demande est reçue de l'interface configurée avec l'adresse IP principale. Le trafic DHCP utilise l'adresse de diffusion. Lorsque la requête DHCP est reçue par l'interface du routeur, elle la transfère au serveur DHCP (lorsqu'une adresse IP auxiliaire est configurée) avec comme adresse source l'adresse IP principale configurée sur l'interface, afin d'indiquer au serveur DHCP quel pool d'IP il doit utiliser (pour le client) dans le paquet de réponse DHCP.

Le routeur n'a aucun moyen de savoir si la demande de diffusion DHCP provient d'un périphérique qui se trouve sur le réseau IP secondaire configuré sur l'interface. Pour contourner le problème, une sous-interface (à condition que le périphérique connecté au routeur prenne en charge l'étiquetage dot1q) peut être configurée pour séparer les deux sous-réseaux, de sorte qu'ils obtiennent leurs adresses IP respectives correctement.

Si l'adresse secondaire est la méthode préférée, il y a une autre solution de contournement, qui est d'activer la commande de configuration globale **dhcp smart-relay**. Cette solution est limitée en ce qu'elle utilise uniquement l'adresse IP secondaire pour transmettre la demande DHCP si le serveur DHCP ne répond pas à trois demandes consécutives du pool d'adresses principal.

Conversation client-serveur DHCP avec la fonction de relais DHCP

Le tableau suivant illustre le processus permettant à un client DHCP d'obtenir une adresse IP d'un serveur DHCP. Ce tableau est calqué sur le schéma de réseau précédentConfiguration de la fonctionnalité de l'agent relais DHCP/BootP. Chaque valeur numérique du schéma représente un paquet décrit dans le tableau suivant. Utilisez ce tableau pour comprendre le flux de paquets de la conversation client-serveur DHCP. Il vous aide également à déterminer où les problèmes se produisent.

Processus permettant à un client DHCP d'obtenir une adresse IP

Paquet	Adresse IP du client	Adresse IP du serveur	Adresse interne globale	Adresse MAC source du paquet	Adresse IP source du paquet	Adresse MAC de destination du paquet	Adress destina paque
1. DHCPDISCOVER est envoyé à partir du client.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.ffff (diffusion)	255.25
2. Le routeur reçoit le message DHCPDISCOVER sur l’interface E1. Le routeur identifie ce paquet comme diffusion UDP DHCP. Le routeur agit désormais en tant qu'agent relais DHCP/BootP et renseignez le champ d'adresse IP de passerelle avec l'adresse IP d'interface entrante, remplacez l'adresse IP source par une adresse IP d'interface entrante et transférez la requête directement au serveur DHCP.	0.0.0.0	0.0.0.0	192.168.1.1	Adresse MAC d'interface E2	192.168.1.1	Adresse MAC du serveur DHCP	192.16
3. Le serveur DHCP a reçu le message DHCPDISCOVER et envoie un message DHCPOFFER à l’agent de relais DHCP.	192.168.1.2	192.168.2.2	192.168.1.1	Adresse MAC du serveur DHCP	192.168.2.2	Adresse MAC d'interface E2	192.16
4. L’agent de relais DHCP reçoit un message DHCPOFFER et transfère la diffusion	192.168.1.2	192.168.2.2	192.168.1.1	Adresse MAC d'interface E1	192.168.1.1	ffff.ffff.ffff (diffusion)	255.25

DHCPOFFER sur le réseau local.							
5. DHCPREQUEST envoyé par le client.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.ffff (diffusion)	255.25
6. Le routeur reçoit le message DHCPREQUEST sur l’interface E1. Le routeur identifie ce paquet comme diffusion UDP DHCP. Le routeur agit désormais en tant qu'agent de relais DHCP et remplit le champ d'adresse IP de passerelle avec l'adresse IP d'interface envoyée, remplace l'adresse IP source par une adresse IP d'interface entrante et transfère la requête directement au serveur DHCP.	0.0.0.0	0.0.0.0	192.168.1.1	Adresse MAC d'interface E2	192.168.1.1	Adresse MAC du serveur DHCP	192.16
7. Le serveur DHCP a reçu le message DHCPREQUEST et envoie un message DHCPACK à l’agent relais DHCP/BootP.	192.168.1.2	192.168.2.2	192.168.1.1	Adresse MAC du serveur DHCP	192.168.2.2	Adresse MAC d'interface E2	192.16
8. L’agent relais DHCP/BootP reçoit le message DHCPACK et transfère la diffusion DHCPACK sur le réseau local. Le client accepte l’accusé de	192.168.1.2	192.168.2.2	192.168.1.1	Adresse MAC d'interface E1	192.168.1.1	ffff.ffff.ffff (diffusion)	255.25

réception et
utilise l'adresse
IP du client.

Considérations DHCP de démarrage de l'environnement de préexécution (PXE)

L'environnement PXE (Pre-Execution Environment) permet à une station de travail de démarrer à partir d'un serveur sur un réseau avant le démarrage du système sur le disque dur local. Un administrateur réseau ne doit pas manipuler physiquement le poste de travail ni le démarrer manuellement. Le système d'exploitation et d'autres logiciels, tels que les programmes de diagnostic, peuvent être chargés sur le périphérique à partir d'un serveur sur le réseau. L'environnement PXE utilise DHCP pour configurer son adresse IP.

La configuration de l'agent relais DHCP/BootP doit être effectuée sur le routeur sur le serveur DHCP se trouve sur un autre segment routé du réseau. **La** commande **eip helper-address** sur l'interface du routeur local doit être configurée. Référez-vous à la sectionConfiguration de la fonctionnalité d'agent relais DHCP/BootP sur le routeur Cisco IOS de ce document pour des informations de configuration.

Comprendre et dépanner le protocole DHCP avec Sniffer Traces

Décodage de la trace du renifleur du client et du serveur DHCP sur le même segment LAN

Topologie réseau dans laquelle le client et le serveur DHCP résident sur le même segment LAN

L'exemple de trace d'analyseur se compose de six trames. Ces six trames illustrent un scénario dans lequel le client et le serveur DHCP résident sur le même segment physique ou logique. Utilisez l'exemple de code suivant pour dépanner DHCP. Il est important de faire correspondre la trace de votre analyseur aux traces de cet exemple. Il peut y avoir quelques différences par rapport aux traces illustrées ci-dessous, mais le flux général de paquets doit être exactement le même. Le tracé de paquets correspond aux considérations précédentes sur le fonctionnement de DHCP.

```
- - - - - - - - - - - - - - - - - - - - - - Frame 1 - DHCPDISCOVER - - - - - - - - - - - - - - - - - - - -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
1[0.0.0.0] [255.255.255.255] 618 0:01:26.810 0.575.244 05/07/2001 11:52:03 AM DHCP: Request,
 Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame 1arrived at 11:52:03.8106; frame size is 618 (026A hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
```

IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 9
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B988 (correct)
IP: **Source address = [0.0.0.0]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 68 (BootPc/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: **Message Type = 1 (DHCP Discover)**
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303030352E646363392E633634302D564C31**
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 2 - DHCPOFFER** -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2[192.168.1.1] [255.255.255.255] 331 0:01:26.825 0.015.172 05/07/2001 11:52:03 AM DHCP: Reply,
Message type: **DHCP Offer**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 2 arrived at 11:52:03.8258; frame size is 331 (014B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC42484**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 317 bytes
IP: Identification = 5
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F901 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = **67 (BootPs/DHCP)**
UDP: Destination port = **68 (BootPc/DHCP)**
UDP: Length = 297
UDP: No checksum
UDP: [289 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:

DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Address Renewal interval = 42767 (seconds)
DHCP: Address Rebinding interval = 74843 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.1.3]**
DHCP: **Domain Name Server address = [192.168.1.4]**
DHCP: **Gateway address = [192.168.1.1]**
DHCP:

- **Frame 3 - DHCPREQUEST** - - - - - - - - - - - - - - - - - -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3[0.0.0.0] [255.255.255.255] 618 0:01:26.829 0.003.586 05/07/2001 11:52:03 AM DHCP: Request,
Message type: **DHCP Request**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 56 arrived at 11:52:03.8294; frame size is 618 (026A hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC9C640**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 10
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B987 (correct)
IP: **Source address = [0.0.0.0]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 68 (BootPc/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**

DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303030352E646363392E633634302D564C31**
DHCP: **Server IP address = [192.168.1.1]**
DHCP: **Request specific IP address = [192.168.1.2]**
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 4 - DHCPACK** -
-

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4[192.168.1.1] [255.255.255.255] 331 0:01:26.844 0.014.658 05/07/2001 11:52:03 AM DHCP: Reply,
 Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 57 arrived at 11:52:03.8440; frame size is 331 (014B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC42484**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 317 bytes
IP: Identification = 6
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F900 (correct)
IP: **Source address = [192.168.1.1]**

IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 68 (BootPc/DHCP)**
UDP: Length = 297
UDP: No checksum
UDP: [289 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 86400 (seconds)
DHCP: Address Renewal interval = 43200 (seconds)
DHCP: Address Rebinding interval = 75600 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.1.3]**
DHCP: **Domain Name Server address = [192.168.1.4]**
DHCP: **Gateway address = [192.168.1.1]**
DHCP:

- **Frame 5 - ARP** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 0005DCC9C640 Broadcast 60 0:01:26.846 0.002.954 05/07/2001 11:52:03 AM ARP: R PA=[192.168.1.2]
 HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 58 arrived at 11:52:03.8470; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]

```
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:

- - - - - - - - - - - - - - - - - - - - - - - - Frame 6 - ARP - - - - - - - - - - - - - - - - - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
6 0005DCC9C640 Broadcast 60 0:01:27.355 0.508.778 05/07/2001 11:52:04 AM ARP: R PA=[192.168.1.2]
 HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 59 arrived at 11:52:04.3557; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

Décoder la trace de l'analyseur du client et du serveur DHCP séparés par un routeur configuré comme agent de relais DHCP

Tracé analyseur-B

```
- - - - - - - - - - - - - - - - - - - - - - - - Frame 1 - DHCPDISCOVER - - - - - - - - - - - - - - - - - -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
1 [0.0.0.0] [255.255.255.255] 618 0:02:05.759 0.025.369 05/31/2001 06:53:04 AM DHCP: Request,
 Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame 124 arrived at 06:53:04.2043; frame size is 618 (026A hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCF2C441
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
```

```
IP: Total length = 604 bytes
IP: Identification = 183
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B8DA (correct)
IP: Source address = [0.0.0.0]
IP: Destination address = [255.255.255.255]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 68 (BootPc/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 00001425
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:
```

- **Frame 2 - DHCPOFFER** -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summaryr
125 [192.168.1.1] [255.255.255.255] 347 0:02:05.772 0.012.764 05/31/2001 06:53:04 AM DHCP:
Reply,
 Message type: **DHCP Offer**

DLC: ----- DLC Header -----
DLC:
DLC: Frame 125 arrived at 06:53:04.2171; frame size is 347 (015B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF, Broadcast**
DLC: **Source = Station 003094248F71**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 45
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F8C9 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 68 (BootPc/DHCP)**
UDP: Length = 313
UDP: Checksum = 8517 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 99471 (seconds)
DHCP: Address Renewal interval = 49735 (seconds)
DHCP: Address Rebinding interval = 87037 (seconds)

DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.10.1]**
DHCP: **Domain Name Server address = [192.168.10.2]**
DHCP: **NetBIOS Server address = [192.168.10.1]**
DHCP: **NetBIOS Server address = [192.168.10.3]**
DHCP: **Domain name = "cisco.com"**
DHCP:

- **Frame 3 - DHCPREQUEST** -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3 [0.0.0.0] [255.255.255.255] 618 0:02:05.774 0.002.185 05/31/2001 06:53:04 AM DHCP: Request,
Message type: **DHCP Request**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 126 arrived at 06:53:04.2193; frame size is 618 (026A hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF, Broadcast**
DLC: **Source = Station Cisc14F2C441**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 184
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B8D9 (correct)
IP: **Source address = [0.0.0.0]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 68 (BootPc/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]

DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30**
DHCP: **Server IP address = [192.168.2.2]**
DHCP: **Request specific IP address = [192.168.1.2]**
DHCP: Request IP address lease time = 99471 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 4 - DHCPACK** -
-

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4 [192.168.1.1] [255.255.255.255] 347 0:02:05.787 0.012.875 05/31/2001 06:53:04 AM DHCP: Reply,
 Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 127 arrived at 06:53:04.2321; frame size is 347 (015B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF, Broadcast**
DLC: **Source = Station 003094248F71**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 47
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F8C7 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----

```
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 68 (BootPc/DHCP)
UDP: Length = 313
UDP: Checksum = 326F (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 00001425
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172800 (seconds)
DHCP: Address Renewal interval = 86400 (seconds)
DHCP: Address Rebinding interval = 151200 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:

- - - - - - - - - - - - - - - - - - - - Frame 5 - ARP - - - - - - - - - - - - - - - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 Cisc14F2C441 Broadcast 60 0:02:05.798 0.011.763 05/31/2001 06:53:04 AM ARP: R PA=[192.168.1.2]
 HA=Cisc14F2C441 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 128 arrived at 06:53:04.2439; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station Cisc14F2C441
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 00E01EF2C441
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
```

```
ARP:
ARP: 18 bytes frame padding
ARP:

- - - - - - - - - - - - - - - - - - - - - - Frame 6 - ARP - - - - - - - - - - - - - - - - - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 Cisc14F2C441 Broadcast 60 0:02:05.798 0.011.763 05/31/2001 06:53:04 AM ARP: R PA=[192.168.1.2]
 HA=Cisc14F2C441 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 128 arrived at 06:53:04.2439; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station Cisc14F2C441
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 00E01EF2C441
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

Tracé Analyseur-A

```
- - - - - - - - - - - - - - - - - - - - - - Frame 1 - DHCPDISCOVER - - - - - - - - - - - - - - - - -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
118 [192.168.1.1] [192.168.2.2] 618 0:00:51.212 0.489.912 05/31/2001 07:02:54 AM DHCP: Request,
 Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame 118 arrived at 07:02:54.7463; frame size is 618 (026A hex) bytes.
DLC: Destination = Station 0005DC0BF2F4
DLC: Source = Station 003094248F72
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 52
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
```

IP: Protocol = 17 (UDP)
IP: Header checksum = 3509 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [192.168.2.2]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: Checksum = 0A19 (correct)
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 1
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 2 - DHCPOFFER** -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2 [192.168.2.2] [192.168.1.1] 347 0:00:51.214 0.002.133 05/31/2001 07:02:54 AM DHCP: Request,
 Message type: **DHCP Offer**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 119 arrived at 07:02:54.7485; frame size is 347 (015B hex) bytes.
DLC: **Destination = Station 003094248F72**
DLC: **Source = Station 0005DC0BF2F4**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----

```
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 41
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3623 (correct)
IP: Source address = [192.168.2.2]
IP: Destination address = [192.168.1.1]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 313
UDP: Checksum = A1F8 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172571 (seconds)
DHCP: Address Renewal interval = 86285 (seconds)
DHCP: Address Rebinding interval = 150999 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:
```

- **Frame 3 - DHCPREQUEST** -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3 [192.168.1.1] [192.168.2.2] 618 0:00:51.240 0.025.974 05/31/2001 07:02:54 AM DHCP: Request,
 Message type: DHCP Request
DLC: ----- DLC Header -----
DLC:
DLC: Frame 120 arrived at 07:02:54.7745; frame size is 618 (026A hex) bytes.
DLC: **Destination = Station 0005DC0BF2F4**
DLC: **Source = Station 003094248F72**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 54
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3507 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [192.168.2.2]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: Checksum = 4699 (correct)
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 1
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:

DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30**
DHCP: Server IP address = [192.168.2.2]
DHCP: Request specific IP address = [192.168.1.2]
DHCP: Request IP address lease time = 172571 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 4 - DHCPACK** -
-

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4 [192.168.2.2] [192.168.1.1] 347 0:00:51.240 0.000.153 05/31/2001 07:02:54 AM DHCP: Request,
 Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 121 arrived at 07:02:54.7746; frame size is 347 (015B hex) bytes.
DLC: **Destination = Station 003094248F72**
DLC: **Source = Station 0005DC0BF2F4**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 42
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3622 (correct)
IP: **Source address = [192.168.2.2]**
IP: **Destination address = [192.168.1.1]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 313
UDP: Checksum = 7DF6 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----

```
DHCP:
DHCP: Boot record type = 2 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172800 (seconds)
DHCP: Address Renewal interval = 86400 (seconds)
DHCP: Address Rebinding interval = 151200 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:
```

Dépannage de DHCP lorsque les stations de travail clientes ne parviennent pas à obtenir des adresses DHCP

Étude de cas #1 : Serveur DHCP résidant sur le même segment LAN ou VLAN que le client DHCP

Lorsque le serveur et le client DHCP résident sur le même segment LAN ou VLAN et que le client ne parvient pas à obtenir une adresse IP d'un serveur DHCP. Mais il est peu probable que le routeur local cause un problème DHCP. Le problème est lié aux périphériques qui connectent le serveur DHCP et le client DHCP. Cependant, le problème peut être lié au serveur DHCP ou au client lui-même. Ces modules permettent de dépanner et de déterminer le périphérique à l'origine du problème.

> **Note**: Pour configurer le serveur DHCP par VLAN, définissez différents pools DHCP pour chaque VLAN qui fournit des adresses DHCP à vos clients.

Étude de cas #2 : Le serveur et le client DHCP sont séparés par un routeur configuré pour la fonctionnalité d'agent relais DHCP/BootP

Lorsque le serveur DHCP et le client résident sur les différents segments LAN ou VLAN, le routeur fonctionne comme un agent relais DHCP/BootP qui est responsable du transfert de DHCPREQUEST au serveur DHCP. Des étapes supplémentaires sont nécessaires pour dépanner l'agent relais DHCP/BootP, ainsi que le serveur et le client DHCP. Si vous suivez ces modules,

vous pouvez déterminer quel périphérique est à l'origine des problèmes.

Le serveur DHCP sur le routeur ne parvient pas à assigner d'adresses avec une erreur POOL EXHAUSTED

Il est possible que certaines adresses soient encore détenues par des clients, même si elles sont libérées du pool. Ceci peut être vérifié par **la sortie show ip dhcp** conflictuput. Un conflit d'adresses se produit lorsque deux hôtes utilisent la même adresse IP. Lors de l'affectation d'adresses, DHCP vérifie les conflits avec une commande ping et l'ARP gratuit.

Si un conflit est détecté, l'adresse est supprimée du pool. L'adresse est assignée jusqu'à ce que l'administrateur résolve le conflit. **Configurez no ip dhcp conflict** logging pour résoudre ce problème.

Dépannage des modules DHCP

Comprendre où les problèmes DHCP peuvent se produire

Les problèmes DHCP peuvent avoir une multitude de causes. Les causes les plus communes sont des problèmes de configuration. Cependant, de nombreux problèmes DHCP peuvent être causés par des défauts logiciels dans les systèmes, les pilotes de carte réseau ou les agents relais DHCP/BootP exécutés sur les routeurs. En raison du nombre de domaines potentiellement problématiques, une approche systématique du dépannage est requise.

Brève liste des causes possibles des problèmes DHCP :

- Configuration par défaut du commutateur Catalyst
- Configuration de l'agent relais DHCP/BootP
- Problème de compatibilité de la carte réseau ou de la fonctionnalité DHCP
- Carte réseau défectueuse ou mauvaise installation du pilote de carte réseau
- Pannes de réseau intermittentes en raison de calculs de spanning tree fréquents
- Erreur de comportement ou de logiciel du système d'exploitation
- Erreur de configuration de la portée ou du logiciel du serveur DHCP
- Défaut du logiciel du commutateur Cisco Catalyst ou de l'agent relais DHCP/BootP de Cisco IOS
- Échec de la vérification de retransmission par le chemin inverse d'Unicast (uRPF) car l'offre DHCP n'est reçue pas l'interface attendue. Lorsque la fonctionnalité Reverse Path Forwarding (RPF) est activée sur une interface, un routeur Cisco peut supprimer les paquets DHCP (Dynamic Host Configuration Protocol) et BOOTP (BOOTstrap Protocol) dont l'adresse source est 0.0.0.0 et l'adresse de destination 255.255.255.255. Le routeur peut également supprimer tous les paquets IP dont l'adresse IP de multidiffusion est destination sur l'interface. Ce problème est documenté dans l'ID de bogue Cisco CSCdw31925

Remarque Seuls les clients Cisco enregistrés peuvent accéder aux rapports de bogue.

- L'agent de base de données DHCP n'est pas utilisé, mais la journalisation des conflits DHCP n'est pas désactivée

A. Vérification de la connectivité physique

Cette procédure s'applique à toutes les études de cas.

Tout d'abord, vérifiez la connectivité physique d'un client et d'un serveur DHCP. Si vous êtes connecté à un commutateur Catalyst, vérifiez que le client et le serveur DHCP ont tous deux une connectivité physique. Pour les commutateurs basés sur Cisco IOS, tels que Catalyst 2900XL/3500XL/2950/3550, la commande équivalente **to show port status isshow interface <interface>**. Si l'état de l'interface est autre que <`interface`> is up, le protocole de ligne est up, le port ne transmet pas le trafic, pas même les requêtes du client DHCP. Le résultat des commandes :

```
Switch#show interface fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0030.94dc.acc1 (bia 0030.94dc.acc1)
```

Si la connexion physique a été vérifiée et qu'il n'y a en effet aucun lien entre le commutateur Catalyst et le client DHCP, utilisez la section Dépannage des problèmes de compatibilité entre les commutateurs Cisco Catalyst et les cartes réseau pour résoudre les problèmes liés à la connectivité de la couche physique.

Des erreurs de liaison de données excessives entraînent le passage des ports sur certains commutateurs Catalyst à un état errdisabled. Pour plus d'informations, référez-vous à Récupération d'état de port errdisable sur les plates-formes Cisco IOS, qui décrivent l'état errdisable, expliquent comment récupérer à partir de celui-ci, et fournissent des exemples de récupération à partir de cet état.

B. Configurer la station de travail cliente et l'IP statique pour tester la connectivité réseau

Cette procédure s'applique à toutes les études de cas.

Lorsque vous dépannez un problème DHCP, il est important de configurer une adresse IP statique sur un poste de travail client afin de vérifier la connectivité réseau. Si la station de travail ne parvient pas à atteindre les ressources réseau malgré une adresse IP configurée de manière statique, la cause principale du problème n'est pas DHCP. À ce stade, vous devez dépanner la connectivité réseau.

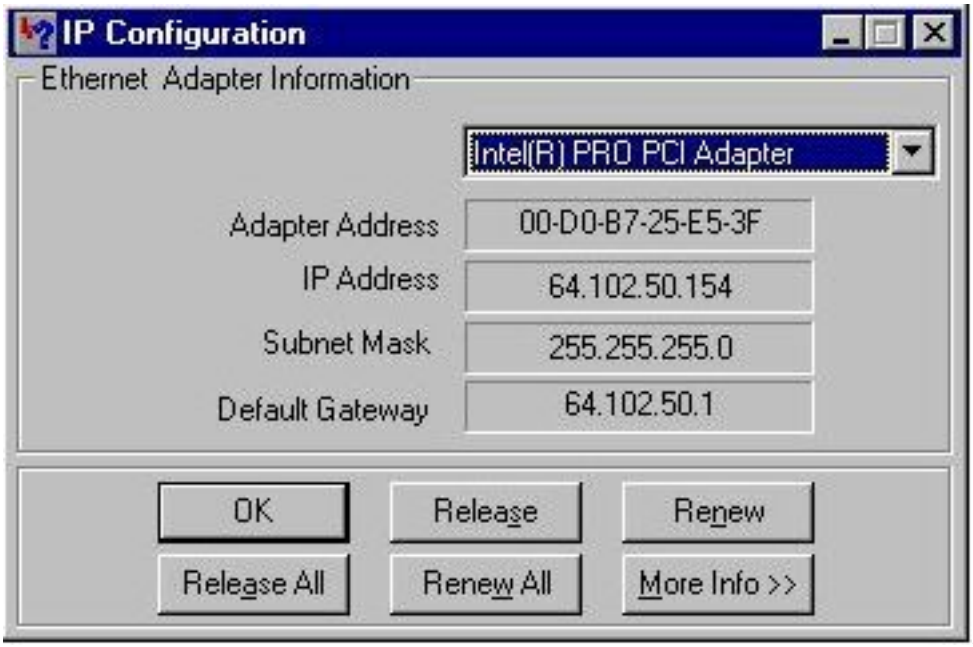
C. Vérification du problème en tant que problème de démarrage

Cette procédure s'applique à toutes les études de cas.

Si le client DHCP ne parvient pas à obtenir une adresse IP du serveur DHCP au démarrage, vous pouvez forcer manuellement le client à envoyer une requête DHCP. Exécutez les étapes suivantes pour obtenir manuellement une adresse IP d'un serveur DHCP pour le système d'exploitation indiqué.

Microsoft Windows 95/98/ME :

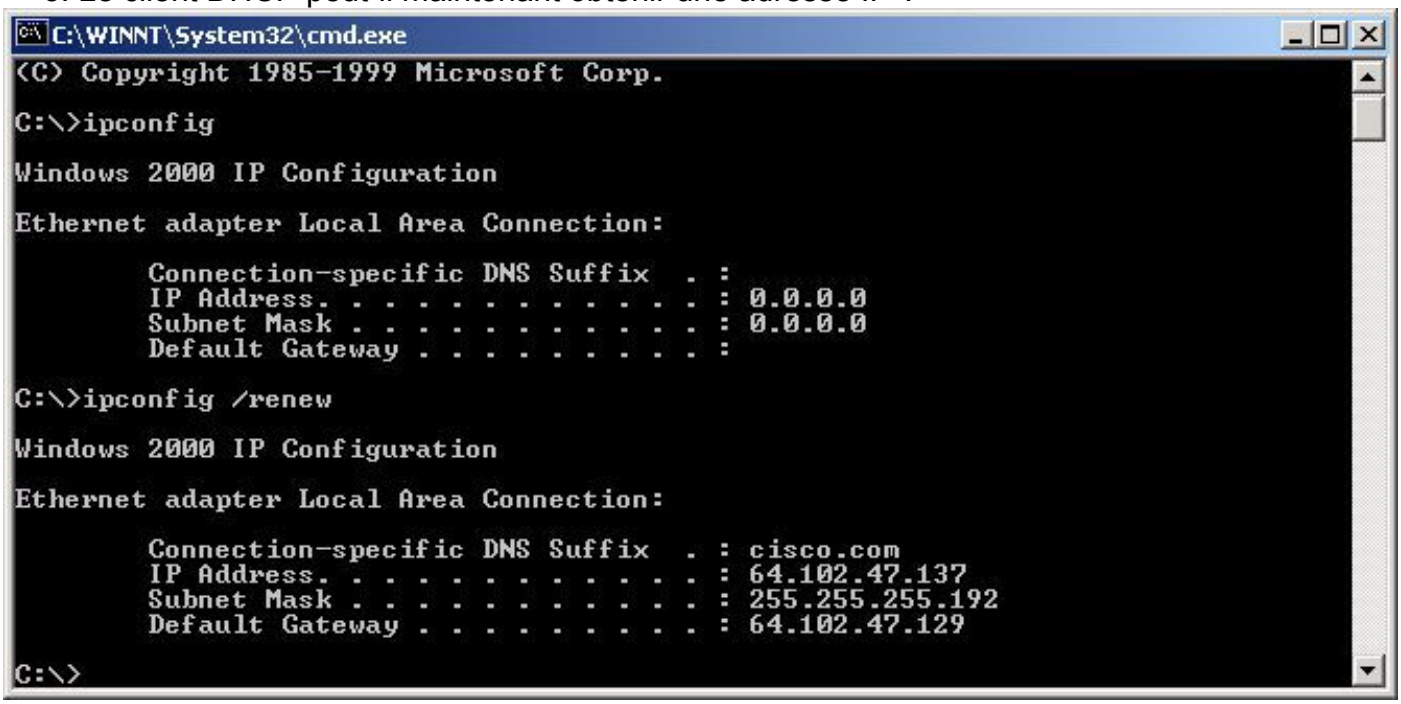
1. Cliquez sur le bouton Démarrer et exécutez le programme WINIPCFG.exe.
2. Cliquez sur **le** bouton **Libérer** tout, puis sur **le** bouton **Renouveler** tout.
3. Le client DHCP peut-il désormais obtenir une adresse IP?



Fenêtre IP Configuration

Microsoft Windows NT/2000 :

1. Entrez cmdin theStart/Runfield pour ouvrir une fenêtre d'invite de commandes.
2. Émettez la commande **commandipconfig/**renew dans la fenêtre d'invite de commande.
3. Le client DHCP peut-il maintenant obtenir une adresse IP ?



Invite de ligne de commande

Si le client DHCP est en mesure d'obtenir une adresse IP avec un renouvellement manuel de l'adresse IP après que le PC a terminé le processus de démarrage, le problème est très probablement un problème de démarrage DHCP. Si le client DHCP est connecté à un commutateur Cisco Catalyst, le problème est probablement dû à un problème de configuration qui traite de STP portfast et/ou de canalisation et d'agrégation. D'autres possibilités incluent des problèmes de cartes réseau ou de démarrage de port de commutateur. Passez en revue les étapes D et E pour exclure les problèmes de configuration des ports de commutation et de carte réseau comme cause principale du problème DHCP.

D. Vérification de la configuration des ports de commutation (commandes STP Portfast et autres)

Si le commutateur est un Catalyst 2900/4000/5000/6000, vérifiez que STP portfast est activé et l'agrégation de liaison/l'acheminement désactivés sur le port. La configuration par défaut est l'option STP portfast désactivée et l'agrégation de liaison/l'acheminement automatiques, le cas échéant. Pour les commutateurs 2900XL/3500XL/2950/3550, STP portfast est la seule configuration requise. Ces modifications de configuration résolvent les problèmes de client DHCP les plus courants qui se produisent avec une installation initiale d'un commutateur Catalyst.

Pour plus de documentation sur les exigences de configuration de port de commutateur nécessaires pour que DHCP fonctionne correctement lorsqu'il est connecté aux commutateurs Catalyst, référez-vous à Utilisation de Portfast et d'autres commandes pour corriger les retards de connectivité de démarrage de station de travail.

Après avoir examiné ce document, vous pouvez continuer à résoudre ces problèmes.

E. Recherchez les problèmes connus de carte réseau ou de commutateur Catalyst

Si la configuration du commutateur Catalyst est correcte, il est possible qu'un problème de compatibilité logicielle puisse exister sur le commutateur Catalyst ou la carte réseau du client DHCP qui pourrait causer les problèmes DHCP. L'étape suivante du dépannage consiste à examiner Dépannage des problèmes de compatibilité des commutateurs Cisco Catalyst avec les cartes réseau et à éliminer les problèmes logiciels du commutateur Catalyst ou de la carte réseau qui contribuent au problème.

Il est nécessaire de connaître le système d'exploitation du client DHCP ainsi que les informations spécifiques de la carte réseau, telles que le fabricant, le modèle et la version du pilote, pour éliminer correctement les problèmes de compatibilité.

F. Déterminer si les clients DHCP obtiennent une adresse IP sur le même sous-réseau ou VLAN que le serveur DHCP

Il est important de déterminer si DHCP fonctionne correctement lorsque le client se trouve sur le même sous-réseau ou VLAN que le serveur DHCP. Si le serveur DHCP fonctionne correctement sur le même sous-réseau ou VLAN que le serveur DHCP, le problème DHCP est principalement causé par l'agent relais DHCP/BootP. Si le problème persiste même lorsque vous testez DHCP sur le même sous-réseau ou VLAN que le serveur DHCP, le problème peut en fait se situer au niveau du serveur DHCP.

G. Vérification de la configuration du relais DHCP/BootP du routeur

Pour vérifier la configuration :

1. Lorsque vous configurez le relais DHCP sur un routeur, vérifiez que **la** commande **ip helper-**address se trouve sur la bonne interface. **La** commande **helper-**address **ip** doit être présente sur l'interface entrante des stations de travail clientes DHCP et doit être dirigée vers le serveur DHCP approprié.
2. Vérifiez que la commande de configuration globale **no service** dhcp n'est pas présente. Ce paramètre de configuration désactive toutes les fonctionnalités de serveur DHCP et de relais sur le routeur. La configuration par défaut, service dhcp, n'apparaît pas dans la configuration et est la commande de configuration par défaut. Si **le service dhcp** n'est pas activé, les clients ne reçoivent pas les adresses IP du serveur DHCP.**Note**: Sur les routeurs qui exécutent des

versions antérieures de Cisco IOS, la commande **ip bootp server gère la fonction d'agent relais DHCP à la place de la commande service dhcp.** Pour cette raison, la commande **ip bootp server doit être activée sur ces routeurs si la commande ip helper-address est configurée pour transférer les diffusions UDP DHCP et pour agir correctement en tant qu'agent relais DHCP au nom du client DHCP.**

3. Lorsque vous utilisez les commandes **ip helper-**address pour transférer des diffusions UDP à une adresse de diffusion de sous-réseau, vérifiez que no ip directed-broadcast n'est configuré sur aucune interface de sortie que les paquets de diffusion UDP doivent traverser. Les no ip directed-broadcast bloque toute traduction d'une diffusion dirigée vers des diffusions physiques. Cette configuration d'interface est la configuration par défaut dans les versions 12.0 et ultérieures du logiciel.
4. Lorsque les diffusions DHCP sont transmises à l'adresse de diffusion de sous-réseau du serveur DHCP, un problème logiciel peut se produire. Lorsque vous dépannez des problèmes DHCP, essayez de transférer les diffusions DHCP UDP à l'adresse IP du serveur DHCP :

H. Option D'Identification De L'Abonné (82) Activée

La fonctionnalité d'information d'agent relais DHCP (option 82) permet aux agents relais DHCP (commutateurs Catalyst) d'inclure des informations sur eux-mêmes et le client associé lors de la transmission de demandes DHCP d'un client DHCP à un serveur DHCP.

Le serveur DHCP peut utiliser ces informations pour assigner des adresses IP, effectuer le contrôle d'accès, et définir les stratégies de Qualité de service (QoS) et de sécurité (ou toute autre stratégie paramètre-affectation) pour chaque abonné d'un réseau de prestataire de services. Lorsque la surveillance DHCP est activée sur un commutateur, elle active automatiquement l'option 82. Si le serveur DHCP n'est pas configuré pour gérer les paquets avec l'option 82, il cesse d'allouer l'adresse à cette demande. Afin de résoudre ce problème, désactivez l'option d'identification d'abonné (82) dans les commutateurs (agents de relais) avec la commande de configuration globale, **no ip dhcp relay information option**.

I. Agent de base de données DHCP et journalisation des conflits DHCP

L'agent de base de données DHCP peut être n'importe quel hôte (par exemple, un serveur FTP, TFTP ou RCP) qui héberge la base de données de liaisons DHCP. Vous pouvez configurer plusieurs agents de base de données DHCP, et vous pouvez configurer l'intervalle entre les mises à jour de base de données et les transferts pour chaque agent. Utilisez **la commande ip dhcp database** pour configurer un agent de base de données et les paramètres de l'agent de base de données.

Si vous choisissez de ne pas configurer un agent de base de données DHCP, désactivez l'enregistrement des conflits d'adresses DHCP sur le serveur DHCP. Exécutez la commande **oip dhcp conflict logging** pour désactiver la journalisation des conflits d'adresses DHCP. Effacez les conflits précédemment enregistrés **avec clear ip dhcp conflict**.

Si cette opération ne désactive pas la journalisation des conflits, ce message d'erreur s'affiche :

```
%DHCPD-4-DECLINE_CONFLICT: DHCP address conflict: client
```

J. Vérifier les connexions de téléphone IP dans CDP

Lorsque le protocole CDP (Cisco Discovery Protocol) est désactivé sur le port de commutateur connecté au téléphone IP Cisco, le serveur DHCP ne peut pas assigner une adresse IP appropriée au téléphone. Le serveur DHCP tend à assigner l'adresse IP qui appartient au VLAN/sous-réseau de données du port de commutateur. Si CDP est activé, le commutateur peut détecter que le téléphone IP Cisco demande DHCP et peut fournir les informations de sous-réseau correctes. Le serveur DHCP peut alors allouer une adresse IP du pool du VLAN/sous-réseau de voix. Il n'existe aucune étape explicite requise pour relier le service DHCP au VLAN voix.

K. La suppression de l'interface SVI interrompt le fonctionnement de la surveillance DHCP

Sur les commutateurs de la gamme Cisco Catalyst 6500, une SVI (à l'arrêt) est créée automatiquement après que la surveillance DHCP a été configurée sur un VLAN spécifique. La présence de cette SVI a des implications directes sur le fonctionnement correct de la surveillance DHCP.

La surveillance DHCP sur les commutateurs de la gamme Cisco Catalyst 6500 qui exécutent la plate-forme logicielle Cisco IOS native est principalement implémentée sur le processeur de routage (RP ou MSFC), et non sur le processeur de commutation (SP ou Supervisor). Un commutateur Cisco Catalyst 6500 intercepte les paquets dans le matériel avec des VACL qui fournissent les paquets à une logique de cible locale (LTL) souscrite par le RP. Une fois que les trames entrent dans le RP, elles doivent tout d'abord être associées à un IDB d'interface (SVI) L3 avant de pouvoir être transmises à la partie surveillance. Sans SVI, cet IDB n'existe pas, et les paquets sont abandonnés dans le RP.

L. Adresse de diffusion limitée

Quand un client DHCP définit le bit de diffusion dans un paquet DHCP, le serveur DHCP et l'agent relais DHCP envoient les messages DHCP aux clients avec l'adresse de diffusion de 1 (255.255.255.255). Si **la commande ip broadcast-address** a été configurée pour envoyer une diffusion réseau, la diffusion « tous les uns » envoyée par DHCP est remplacée. Afin de remédier à cette situation, utilisez **la commande ip dhcp limited-broadcast-address** pour vous assurer qu'une diffusion réseau configurée ne remplace pas le comportement DHCP par défaut.

Certains clients DHCP acceptent uniquement les diffusions de 1 et ne peuvent pas acquérir d'adresse DHCP, sauf si cette commande est configurée sur l'interface de routeur connectée au client.

M. Debug DHCP With Router Debug Commands

Vérifier que le routeur reçoit la requête DHCP avec les commandes debug

Sur les routeurs qui prennent en charge le logiciel qui traite les paquets DHCP, vous pouvez vérifier si un routeur reçoit la requête DHCP du client. Le processus DHCP échoue si le routeur ne reçoit pas de requêtes du client. Dans cette étape, configurez une liste d'accès pour déboguer la sortie. Cette liste d’accès est utilisée uniquement pour déboguer une commande et n’est pas intrusive pour le routeur.

En mode de configuration globale, entrez la liste de contrôle d’accès suivante :

access-list 100 permit ip host 0.0.0.0 host 255.255.255.255

En mode d’exécution, entrez la commande debug suivante :

debug ip packet detail 100

Exemple de sortie

```
Router#debug ip packet detail 100
IP packet debugging is on (detailed) for access list 100
Router#
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
```

Dans cet exemple de résultats, il est clair que le routeur reçoit activement les requêtes DHCP du client. Cette sortie montre uniquement un réseau du paquet, mais pas le paquet lui-même. Par conséquent, il n'est pas possible de déterminer si le paquet est correct. Néanmoins, le routeur a bien reçu un paquet de diffusion avec les adresses IP source et de destination et les ports UDP corrects pour DHCP.

Vérifier que le routeur reçoit et transfère la requête DHCP avec la commande debug ip udp

La commande **debug ip udp** peut tracer le chemin d’une requête DHCP via un routeur. Cependant, ce débogage est intrusif dans un environnement de production, puisque tous les paquets UDP commutés traités sont affichés sur la console. Cette commande debug ne doit pas être utilisée en production.

> **Avertissement :** La commande **debug ip udp** est intrusive et peut entraîner une utilisation élevée de l'unité centrale (UC).

En mode d'exécution, entrez cette commande debug : **debug ip udp**

Exemple de sortie

```
Router#debug ip udp
UDP packet debugging is on
Router#

00:18:48: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584

!--- Router receiving DHCPDISCOVER from DHCP client.

00:18:48: UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604

!--- Router forwarding DHCPDISCOVER unicast to DHCP server using DHCP/BootP Relay Agent source
IP address.

00:18:48: UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=313

!--- Router receiving DHCPOFFER from DHCP server directed to DHCP/BootP Relay Agent IP address.

00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=333
```

```
!--- Router forwarding DHCPOFFER from DHCP server to DHCP client via DHCP/BootP Relay Agent.

00:18:48: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584

!--- Router receiving DHCPREQUEST from DHCP client.

00:18:48: UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604

!--- Router forwarding DHCPDISCOVER unicast to DHCP server using DHCP/BootP Relay Agent source
IP address.

00:18:48: UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=313

!--- Router receiving DHCPACK (or DHCPNAK) from DHCP directed to DHCP/BootP Relay Agent IP
address.

00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=333

!--- Router forwarding DHCPACK (or DHCPNAK) to DHCP client via DHCP/BootP Relay Agent.

00:18:48: UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32

!--- DHCP client verifying IP address not in use by sending ARP request for its own IP address.

00:18:50: UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32

!--- DHCP client verifying IP address not in use by sending ARP request for its own IP address.
```

Vérifier que le routeur reçoit et transfère la requête DHCP avec la commande debug ip dhcp server packet

Si le routeur Cisco IOS est 12.0.x.T ou 12.1 et prend en charge la fonctionnalité de serveur DHCP de Cisco IOS, vous pouvez utiliser la commande **debug ip dhcp server packet**. Ce débogage a été conçu pour être utilisé avec la fonctionnalité de serveur DHCP IOS et pour dépanner également la fonctionnalité d'agent relais DHCP/BootP. Comme pour les étapes précédentes, les débogages de routeur ne permettent pas de déterminer précisément le problème, car le paquet réel ne peut pas être affiché. Toutefois, les débogages permettent d'établir des inférences en ce qui concerne le traitement DHCP. En mode d'exécution, entrez la commande debug suivante :

debug ip dhcp server packet

```
Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.

!--- Router received DHCPDISCOVER/REQUEST/INRORM and setting Gateway IP address to 192.168.1.1
for forwarding.

00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..

!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM.


!--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier.

00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441.

!--- BOOTREPLY includes DHCPOFFER and DHCPNAK.
```

```
!--- Client's MAC address is 00e0.1ef2.c441.

00:20:54: DHCPD: broadcasting BOOTREPLY to client 00e0.1ef2.c441.

!--- Router is forwarding DHCPOFFER or DHCPNAK broadcast on local LAN interface.

00:20:54: DHCPD: setting giaddr to 192.168.1.1.

!--- Router received DHCPDISCOVER/REQUEST/INFORM and set Gateway IP address to 192.168.1.1 for
forwarding.

00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..

!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM.


!--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier.

00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441.

!--- BOOTREPLY includes DHCPOFFER and DHCPNAK.


!--- Client's MAC address is 00e0.1ef2.c441.

00:20:54: DHCPD: broadcasting BOOTREPLY to client 00e0.1ef2.c441.

!--- Router is forwarding DHCPOFFER or DHCPNAK broadcast on local LAN interface.
```

Exécuter plusieurs débogages simultanément

Lorsque vous exécutez plusieurs débogages simultanément, une bonne quantité d'informations peuvent être découvertes concernant le fonctionnement de l'agent relais DHCP/BootP et du serveur. Si vous utilisez les plans précédents pour le dépannage, vous pouvez faire des inférences sur les points où la fonctionnalité de l'agent relais DHCP/BootP ne fonctionne pas correctement.

```
IP: s=0.0.0.0 (Ethernet0), d=255.255.255.255, len 604, rcvd 2
UDP src=68, dst=67
UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
DHCPD: setting giaddr to 192.168.1.1.
UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet1), len 604, sending
UDP src=67, dst=67
DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3030.302e.3030.3030.2e30.3030.312d.4574.30 forwarded
to 192.168.2.2.
IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
UDP src=67, dst=67
UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=308
DHCPD: forwarding BOOTREPLY to client 0000.0000.0001.
DHCPD: broadcasting BOOTREPLY to client 0000.0000.0001.
UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=328
IP: s=0.0.0.0 (Ethernet0), d=255.255.255.255, len 604, rcvd 2
UDP src=68, dst=67
UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
DHCPD: setting giaddr to 192.168.1.1.
UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet1), len 604, sending
UDP src=67, dst=67
```

```
DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3030.302e.3030.3030.2e30.3030.312d.4574.30 forwarded
to 192.168.2.2.
IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
UDP src=67, dst=67
UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=308
DHCPD: forwarding BOOTREPLY to client 0000.0000.0001.
DHCPD: broadcasting BOOTREPLY to client 0000.0000.0001.
UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=328.
```

Obtenir le tracé de l'analyseur de réseau et déterminer la cause des problèmes DHCP

Consultez les sections Decode Sniffer Trace of DHCP Client and Server on Same LAN Segment et Decode Sniffer Trace of DHCP Client and Server Separated by Router Configured as a DHCP Relay Agent

pour déchiffrer les traces de paquets DHCP.

Pour plus d'informations sur la façon d'obtenir des traces de renifleur avec la fonctionnalité SPAN (Switched Port Analyzer) sur les commutateurs Catalyst, référez-vous à Exemple de configuration de SPAN (Switched Port Analyzer) Catalyst.

Autre méthode de décodage de paquets avec débogage sur le routeur

Avec la commande **debug ip packet detail dump <acl>** sur un routeur Cisco, il est possible d'obtenir un paquet entier en hexadécimal affiché dans le journal système ou l'interface de ligne de commande (CLI). Passez en revue les sections Vérifier que le routeur reçoit la requête DHCP avec les commandes de débogage et Vérifier que le routeur reçoit la requête DHCP et transfère la requête au serveur DHCP avec les commandes de débogage ci-dessus, ainsi que le mot clé dump ajouté à la liste d'accès, pour obtenir les mêmes informations de débogage, mais avec les détails du paquet en hexadécimal. Pour déterminer le contenu du paquet, celui-ci doit être traduit. L'annexe A contient un exemple.

Annexe A : Exemple de configuration DHCP de Cisco IOS

La base de données du serveur DHCP est organisée sous forme arborescente. La racine de l'arborescence est un pool d'adresses pour les réseaux naturels, les branches sont les pools d'adresses de sous-réseaux, et les feuilles sont les liaisons manuelles aux clients. Les sous-réseaux héritent des paramètres de réseau et les clients héritent des paramètres de sous-réseau. Par conséquent, les paramètres courants, par exemple le nom de domaine, doivent être configurés au niveau le plus élevé (réseau ou sous-réseau) de l'arborescence.

Pour plus d'informations sur la façon de configurer DHCP et les commandes associées, référez-vous à la Liste des tâches de configuration DHCP.

```
version 12.1
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable password cisco
ip subnet-zero
no ip domain-lookup
```

```
ip dhcp excluded-address 10.10.1.1 10.10.1.199

!--- Address range excluded from DHCP pools.

ip dhcp pool test_dhcp

!--- DHCP pool (scope) name is test_dhcp.

network 10.10.1.0 255.255.255.0

!--- DHCP pool (address will be assigned in this range) for associated Gateway IP address.

default-router 10.10.1.1

!--- DHCP option for default gateway.

dns-server 10.30.1.1

!--- DHCP option for DNS server(s).

netbios-name-server 10.40.1.1

!--- DHCP option for NetBIOS name server(s) (WINS).

lease 0 0 1

!--- Lease time.

interface Ethernet0
description DHCP Client Network
ip address 10.10.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet1
description Server Network
ip address 10.10.2.1 255.255.255.0
no ip directed-broadcast
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
login
!
end
```

Informations connexes

- Outils et ressources
- Support technique - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.