Présentation et dépannage du protocole DHCP dans les commutateurs Catalyst ou les réseaux d'entreprise

Contenu

Introduction

Ce document contient des informations sur le dépannage de plusieurs problèmes courants de DHCP (Dynamic Host Configuration Protocol) qui peuvent se produire dans un réseau commuté Cisco Catalyst. Ce document inclut le dépannage de l'utilisation de la fonctionnalité d'agent relais DHCP/BootP du logiciel Cisco IOS®.

Conditions préalables

Conditions requises

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

Composants utilisés

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

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

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

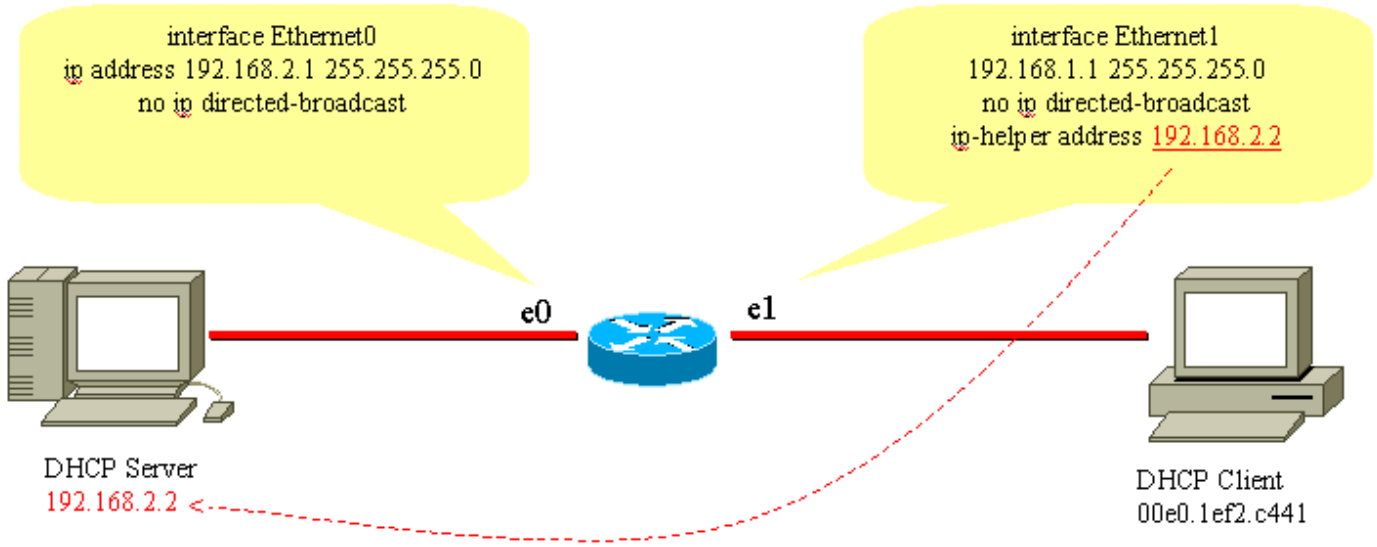
Concepts clés

Voici plusieurs concepts clés de DHCP :

- Àla base, aucune adresse IP n'est configurée pour les clients DHCP ; ces derniers doivent donc envoyer une demande de diffusion pour obtenir une adresse IP auprès 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.

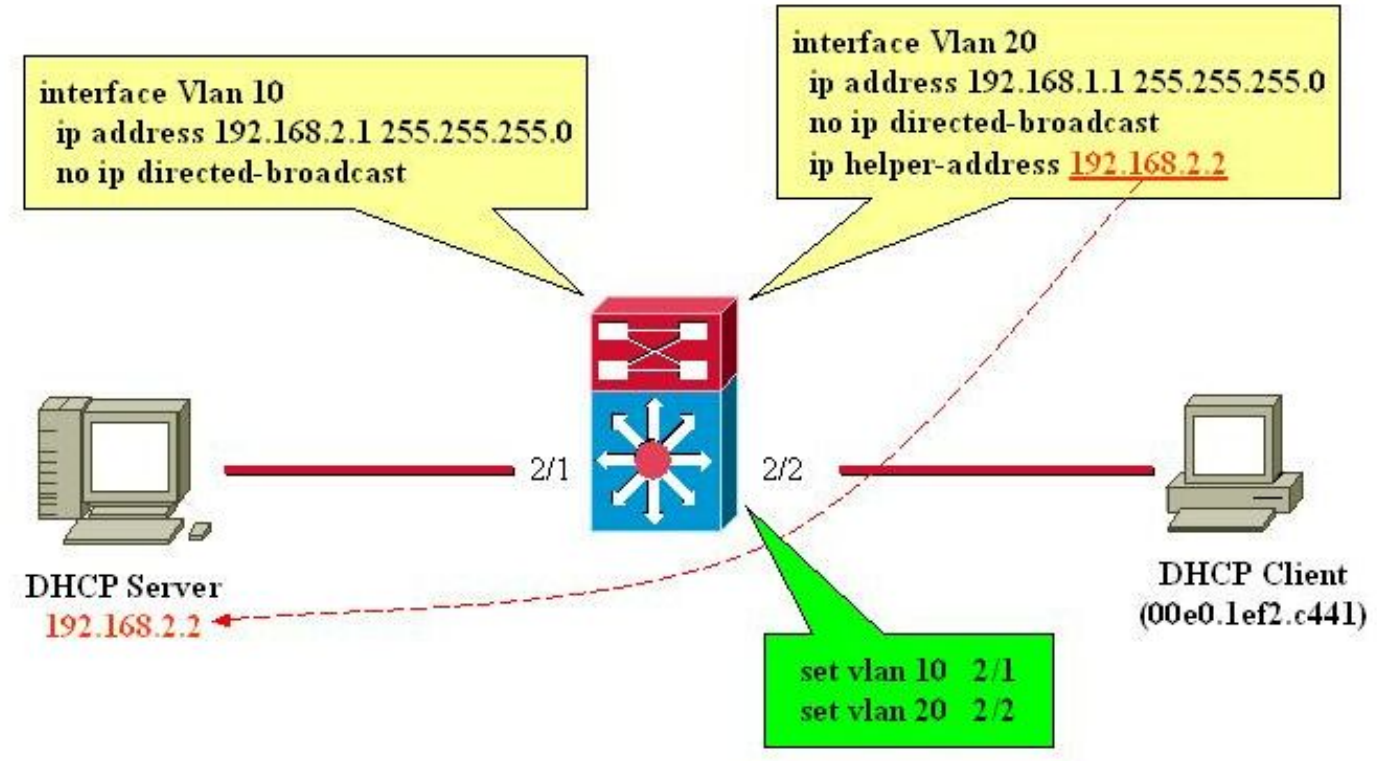
Exemples de scénarios

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



Comme l'illustre la configuration dans ce schéma, l'interface Ethernet1 transfère le paquet DHCPDISCOVER diffusé du client à 192.168.2.2 via l'interface Ethernet1. Le serveur DHCP satisfait la demande grâce à la monodiffusion. Aucune autre configuration du routeur n'est nécessaire dans cet exemple.

Scénario 2 : Routage du commutateur Cisco Catalyst avec module L3 entre les réseaux du client et du serveur DHCP



Comme l'illustre la configuration dans le schéma, l'interface VLAN20 transfère le paquet DHCPDISCOVER diffusé du client à 192.168.2.2 via l'interface VLAN10. Le serveur DHCP

satisfait la demande grâce à la 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.

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. Puisque 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 à l'aide de la fonctionnalité d'agent relais DHCP.

Présentation de DHCP

DHCP a été initialement défini dans le document RFC 1531 , qui ont depuis été remplacés par le document RFC 2131 . DHCP est basé sur le protocole de démarrage (BootP), qui est défini dans le document 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. Puisque chaque hôte a besoin d'une adresse IP pour communiquer dans un réseau IP, DHCP allège la charge administrative liée à la configuration manuelle d'une adresse IP pour chaque hôte. 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. Lors de cet échange, le client passe par plusieurs états bien définis, listés ci-dessous :

1. Initialiser
2. Sélectionner
3. Demande
4. Limite
5. Renouveler
6. Se relier de nouveau

En passant de l'un à l'autre des états mentionnés ci-dessus, le client et le serveur peuvent échanger les types de messages repris dans la table des messages DHCP ci-dessous.

Tableau des messages DHCP

Référence	Message	Utilisation
0x01	DHCPDISCOVER	Le client recherche les serveurs DHCP disponibles.
0x02	DHCPOFFER	Réponse du serveur au paquet DHCPDISCOVER du client.
0x03	DHCPREQUEST	Le client envoie une diffusion au serveur, demandant les paramètres offerts d'un serveur spécifique, comme défini dans le paquet.
0x04	DHCPDECLINE	Communication client-serveur, indiquant que l'adresse de réseau est déjà utilisée.
0x05	DHCPACK	Communication serveur-client avec des paramètres de configuration, y compris l'adresse de réseau validée.
0x06	DHCPNAK	Communication serveur-client, refusant la demande de paramètre de configuration.
0x07	DHCPRELEASE	Communication client-serveur, abandonnant l'adresse de réseau et annulant le bail restant.
0x08	DHCPINFORM	Communication client-serveur, demandant seulement les paramètres de configuration locale que le client a déjà configurés en externe en tant qu'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 ne peut pas connaître le sous-réseau auquel il appartient, le message DHCPDISCOVER est une diffusion pour tous les sous-réseaux (adresse IP de destination 255.255.255.255), avec l'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, qu'il est configuré et fonctionne correctement, le serveur DHCP entend la diffusion et répond avec 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 relais peut être un hôte dédié (par exemple Microsoft Windows Server) ou un routeur (par exemple, un routeur Cisco configuré avec des déclarations auxiliaires IP au niveau de l'interface).

DHCPOFFER

Un serveur DHCP qui reçoit un message DHCPDISCOVER peut répondre avec un message DHCPOFFER sur le port 68 UDP (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 renseigne 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 des clients dans le champ chaddr de l'offre, ainsi le client connaît la destination prévue. Si le serveur DHCP n'est pas sur le sous-réseau local, le serveur DHCP renvoie le message DHCPOFFER, comme paquet de monodiffusion, sur le port 67 UDP, à l'agent relais DHCP/BootP qui lui avait envoyé le message DHCPDISCOVER. L'agent relais DHCP/BootP envoie alors par diffusion ou monodiffusion le message DHCPOFFER sur le sous-réseau local sur le port 68 UDP, selon l'indicateur de diffusion défini par le client BootP.

DHCPREQUEST

Après avoir reçu un message DHCPOFFER, le client répond avec un message DHCPREQUEST, indiquant son intention d'accepter les paramètres du message DHCPOFFER et passe à l'état Demande. Le client peut recevoir plusieurs messages DHCPOFFER, un de chaque serveur DHCP qui a reçu le message DHCPDISCOVER initial. Le client choisit un message DHCPOFFER et répond à ce serveur DHCP uniquement, implicitement refusant tous les autres messages DHCPOFFER. Le client identifie le serveur sélectionné en renseignant le champ d'option Server Identifier avec l'adresse IP du serveur DHCP. Le message DHCPREQUEST est également une diffusion. Tous les serveurs DHCP qui ont envoyé un message DHCPOFFER voient donc le message DHCPREQUEST, et chacun sait si son message DHCPOFFER a été accepté ou refusé. Toutes les options de configuration supplémentaires demandées par le client sont incluses dans le champ d'options du message DHCPREQUEST. Bien que le client ait reçu une adresse IP, il envoie le message DHCPREQUEST avec l'adresse IP source 0.0.0.0. Le client n'a alors pas encore reçu la confirmation qu'il peut utiliser l'adresse IP.

DHCPACK

Une fois que le serveur reçoit le message DHCPREQUEST, il confirme avoir reçu la demande avec un message DHCPACK, finalisant ainsi 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. En attendant, le serveur DHCP enregistre le bail dans sa base de données et l'identifie de façon unique à l'aide de l'identificateur client ou chaddr, et de l'adresse IP associée. Le client et le serveur utilisent tous les deux cette combinaison des 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, le client DHCP doit calculer les paramètres temporels associés à l'adresse louée, qui sont la durée du bail (LT), la date de renouvellement (T1) et la date de nouvelle liaison (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 peut pas satisfaire le message DHCPREQUEST, le serveur DHCP répond avec un message DHCPNAK. Quand le client reçoit un message DHCPNAK, ou qu'il ne reçoit pas de réponse à un message DHCPREQUEST, il relance le processus de configuration en passant à l'état Demande. Le client retransmet le message DHCPREQUEST au moins quatre fois en 60 secondes avant de reprendre l'état Initialisation.

DHCPDECLINE

Le client reçoit le message DHCPACK et exécute éventuellement une vérification finale des paramètres. Le client exécute cette procédure en envoyant des demandes de protocole de résolution d'adresse (ARP) pour l'adresse IP fournie dans le message DHCPACK. Si le client détecte que l'adresse est déjà utilisée en recevant une réponse à la requête ARP, il envoie un message DHCPDECLINE au serveur et redémarre le processus de configuration en passant à l'état Demande.

DHCPINFORM

Si un client a obtenu une adresse de réseau d'un autre moyen ou qu'il dispose d'une adresse IP configurée manuellement, un poste de travail client peut utiliser un message de demande DHCPINFORM pour obtenir d'autres paramètres de configuration locale, tels que le nom de domaine et les serveurs de noms de domaine (DNS). Les serveurs DHCP qui reçoivent un message DHCPINFORM créent un message DHCPACK avec les paramètres de configuration locale appropriés pour le client sans allouer de nouvelle adresse IP. Ce message DHCPACK envoie une monodiffusion au client.

DHCPRELEASE

Un client DHCP peut choisir d'abandonner son bail sur une adresse de réseau en envoyant un message DHCPRELEASE au serveur DHCP. Le client identifie le bail à libérer à l'aide du champ client identifier et de l'adresse de réseau dans le message DHCPRELEASE. Si vous devez étendre la plage de pool DHCP actuelle, supprimez le pool d'adresses actuel et spécifiez la nouvelle plage d'adresses IP dans 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.

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

Renouvellement du bail

Puisque l'adresse IP est seulement louée auprès du serveur, le bail doit être renouvelé de temps en temps. Lorsque la première moitié de la durée du bail a expiré (T1=0,5 x LT), le client essaie 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 est d'accord de renouveler le bail. Le message DHCPACK contient le nouveau bail et tous les nouveaux paramètres de configuration, au cas où une modification serait apportée au serveur pendant la durée du bail précédent. Si le client ne peut pas atteindre le serveur qui détient le bail pour quelque raison que ce soit, il essaie de renouveler l'adresse de tout serveur DHCP après que le serveur DHCP d'origine n'a pas répondu aux demandes de renouvellement avec une durée 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 DHCP assignée et qu'il est redémarré, le client demande spécifiquement l'adresse IP louée précédemment dans un paquet DHCPREQUEST. Ce paquet DHCPREQUEST a toujours l'adresse IP source 0.0.0.0, et l'adresse IP de diffusion 255.255.255.255 comme destination.

Un client qui envoie un message DHCPREQUEST lors d'un redémarrage ne doit pas renseigner le champ d'identificateur du serveur, et doit à la place renseigner le champ d'option d'adresse IP demandée. Les clients strictement conformes aux documents RFC renseignent le champ ciaddr avec l'adresse demandée au lieu du champ d'option DHCP. Le serveur DHCP accepte les deux méthodes. Le comportement du serveur DHCP dépend d'un certain nombre de facteurs, comme les serveurs DHCP Windows NT et la version du système d'exploitation utilisée, ainsi que d'autres facteurs, tels que le superscoping. Si le serveur DHCP détermine que le client peut encore utiliser l'adresse IP demandée, il reste silencieux ou envoie un message DHCPACK pour le paquet 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 alors à l'état Initialisation, et envoie un message DHCPDISCOVER.

Remarque: 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.

Paquet DHCP

Le message DHCP est de longueur variable et se compose des champs mentionnés dans le tableau ci-dessous.

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

Champ	Octets	Nom	Description
op	1	OpCo	Identifie le paquet en tant que

		de	demande 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.
sauts	1	Sauts	Le client définit la valeur à zéro et les incréments de valeur si la demande est transférée via un routeur.
xid	4	ID de transaction	Nombre aléatoire choisi par le client. Tous les message DHCP échangés pour une transaction DHCP donnée utilise l'ID (xid).
sec	2	Secondes	Spécifie le nombre de secondes depuis le début du processus DHCP.
indicateurs	2	Indicateurs	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 dans 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 renseigné avec l'adresse du serveur DHCP. Sinon, elle est utilisée dans les messages DHCPOFFER et DHCPACK du serveur DHCP.
giaddr	4	Adresse IP du routeur (GIADDR)	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 serve	Nom d'hôte de serveur facultatif.

		ur	
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. RFC 2132 donne toutes les options possibles.

Conversation client-serveur pour un client obtenant une adresse DHCP lorsque 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	Émission	0.0.0.0	255.255.255.255
DHCPOFFER	DHCPServer	Émission	DHCPServer	255.255.255.255
DHCPREQUEST	Client	Émission	0.0.0.0	255.255.255.255
DHCPACK	DHCPServer	Émission	DHCPServer	255.255.255.255

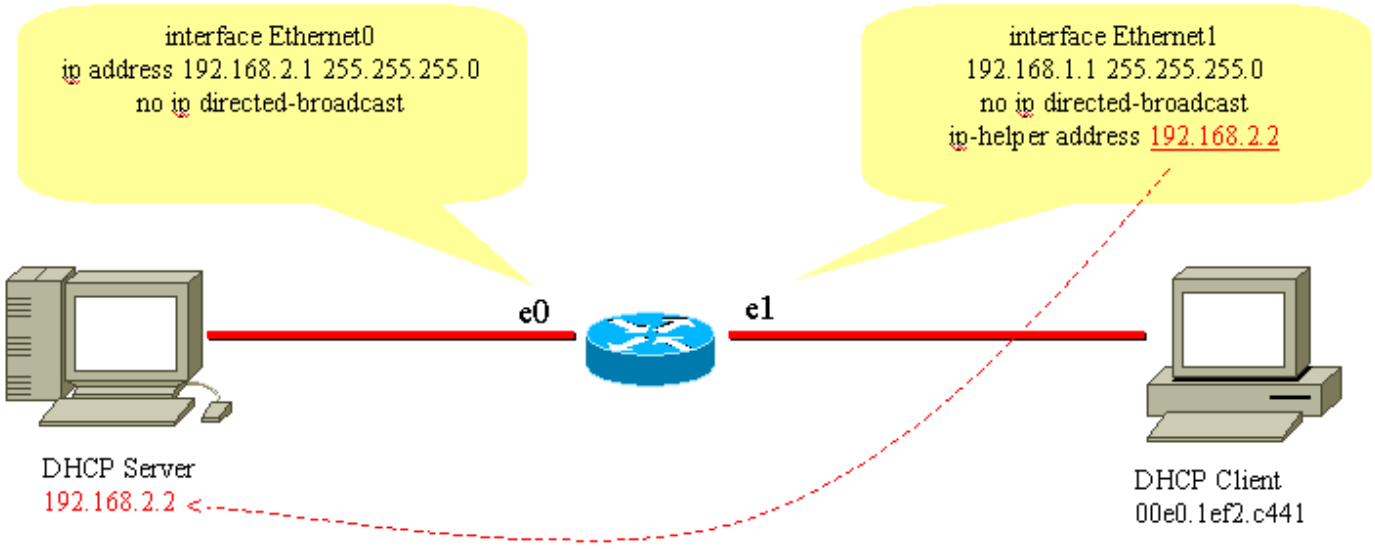
Rôle de l'agent relais DHCP/BootP

Par défaut, les routeurs ne transfèrent pas les paquets de diffusion. Puisque les messages du client DHCP utilisent l'adresse IP de destination 255.255.255.255 (toutes les diffusions de réseau), les clients DHCP ne peuvent pas envoyer de demandes à un serveur DHCP sur un autre sous-réseau sauf si l'agent relais DHCP/BootP est configuré sur le routeur. L'agent relais DHCP/BootP transfère les demandes 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 à destination du 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 du client est reçu. 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 fonctionnalité de l'agent relais DHCP/BootP sur le routeur Cisco IOS

La configuration d'un routeur Cisco pour qu'il transfère les demandes BootP ou DHCP est simple : configurez une adresse IP auxiliaire qui pointe vers le serveur DHCP/BootP, ou vers l'adresse de

diffusion du sous-réseau du réseau sur lequel le serveur réside. Par exemple, observez le schéma de réseau suivant :



Pour transférer la demande 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 auxiliaire transfère les diffusions UDP suivantes :

- 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 auxiliaires peuvent diriger des diffusions UDP vers une adresse IP de monodiffusion ou diffusion. **Cependant, il n'est pas recommandé d'utiliser l'adresse IP auxiliaire pour transférer des diffusions UDP d'un sous-réseau à l'adresse de diffusion d'un autre sous-réseau, en raison du grand nombre de diffusions pouvant se produire**. Plusieurs entrées d'adresses IP auxiliaires sur une interface unique sont également prises en charge, comme illustré ci-dessous :

```
!
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. Le fait d'avoir plusieurs serveurs DHCP qui gèrent un sous-réseau augmente le trafic DHCP car les messages DHCPDISCOVER, DHCPOFFER et DHCPREQUEST/DHCPDECLINE sont échangés entre chaque paire de client-serveur DHCP.

Définition de 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 pour les clients DHCP Microsoft, et l'autre pour les clients DHCP non-Microsoft : DHCP client-identifier (liaison manuelle - Clients DHCP Microsoft) et DHCP hardware-address (liaison manuelle - clients DHCP non-Microsoft). La raison pour laquelle il existe deux commandes différentes est qu'un ordinateur qui exécute Windows modifie ses adresses MAC, et que **01** est ajouté au début de l'adresse. Voici des exemples de configuration :

- Configuration pour les clients DHCP Microsoft
  ```
  configuration terminal
  ip dhcp pool new_pool host ip_address subnet_mask client-identifier 01XXXXXXXXXXX !---
  xxxxxx represents 48 bit MAC address prepended with 01
  ```
- Configuration pour les clients DHCP non-Microsoft
  ```
  configuration terminal
  ip dhcp pool new_pool host ip_address subnet_mask hardware-address XXXXXXXXXXX !--- 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 existe une autre solution de contournement, qui consiste à activer la commande de configuration globale ip 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 ci-dessous illustre le processus pour qu'un client DHCP obtienne une adresse IP d'un serveur DHCP. Ce tableau repose sur le schéma de réseau ci-dessus. Chaque valeur numérique dans le schéma représente un paquet décrit ci-dessous. Ce tableau est un point de référence pour comprendre le flux de paquets de la conversation client-serveur DHCP. Ce tableau permet également de déterminer où les problèmes DHCP peuvent se produire.

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	Adresse IP de destination du paquet
1. DHCPDISCOVER est envoyé 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)	255.255.255.255
2. Le routeur reçoit le message DHCPDISCOVER sur l'interface E1. Le routeur identifie ce paquet comme diffusion UDP DHCP. Le routeur agit à présent en tant qu'agen	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	192.168.2.2

t relais DHCP/ BootP et renseigne le champ d'adresse IP de passerelle avec l'adresse IP d'interface entrante, modifie l'adresse IP source en interface IP d'interface entrante, et transfère la demande directement au serveur DHCP.							
3. Le serveur DHCP a reçu le message DHCPDISCOVER et envoie un message DHCPOFFER à	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	192.168.1.1

l'agent relais DHCP.							
4. L'agent relais DHCP reçoit un message DHCPOFFER, et transfère la diffusion DHCPOFFER sur le réseau local.	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)	255.255.255.255
5. DHCPREQUEST envoyé 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)	255.255.255.255
6. Le routeur reçoit le message DHCPREQUEST sur l'interface E1. Le routeur identifie ce paquet comme diffusion UDP DHCP. Le routeur agit à	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	192.168.2.2

présent en tant qu'agent relais DHCP et renseigne le champ d'adresse IP de passerelle avec l'adresse IP d'interface entrante, modifie l'adresse IP source en interface IP d'interface entrante, et transfère la demande directement au serveur DHCP.							
7. Le serveur DHCP a reçu le message DHCPREQUEST et envoie un message	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	192.168.1.1

DHCPACK à l'agent relais DHCP/BootP.							
8. L'agent relais DHCP/BootP reçoit le message DHCPACK, et transfère la diffusion DHCPACK sur le réseau local. Le client accepte le paquet ACK et utilise l'adresse IP du client.	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)	255.255.255.255

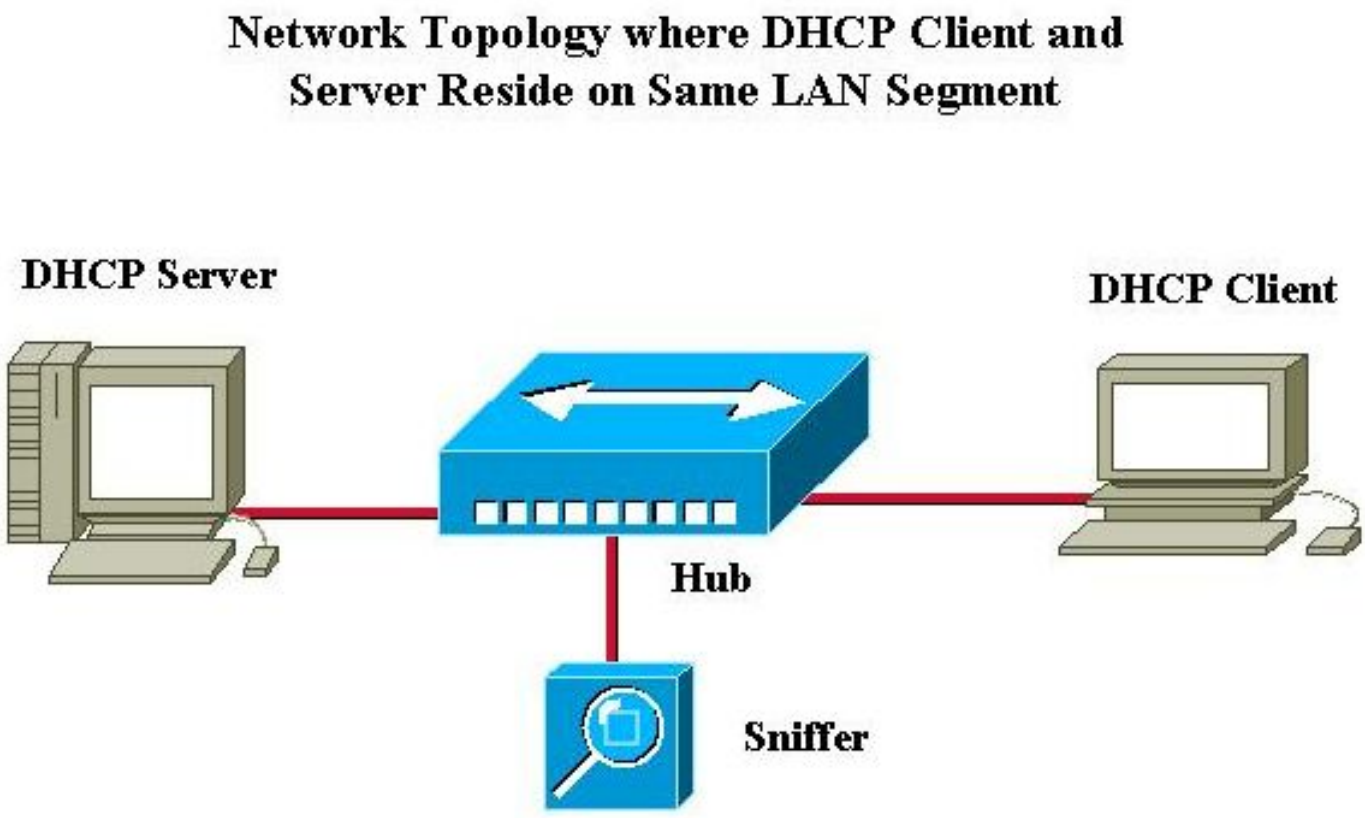
Considérations DHCP de démarrage d'environnement de pré-exécution (PXE)

L'environnement de pré-exécution (PXE) permet à un poste de travail de démarrer à partir d'un serveur sur un réseau avant de démarrer le système d'exploitation sur le disque dur local. Un administrateur réseau ne doit pas manipuler physiquement le poste de travail ni le démarrer manuellement. Des systèmes d'exploitation et autres logiciels, tel que des programmes de diagnostic, peuvent être chargés sur le périphérique d'un serveur sur un 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 de **helper-address d'IP** sur l'interface de routeur local doit être configurée. Référez-vous à la section Configuration de la fonctionnalité de l'agent relais DHCP/BootP sur le routeur Cisco IOS du présent document pour obtenir des informations de configuration.

Présentation et dépannage de DHCP à l'aide des tracés de l'analyseur de réseau

Décodage du tracé de l'analyseur de réseau d'un client et d'un serveur DHCP sur un même segment LAN



Le tracé de l'analyseur de réseau ci-dessous est composé de six trames. Ces six trames illustrent un scénario de travail pour DHCP, où le client et le serveur DHCP résident sur le même segment physique ou logique. En cas de dépannage de DHCP, il est important que le tracé de l'analyseur de réseau corresponde aux tracés ci-dessous. Quelques différences peuvent exister par rapport aux tracés ci-dessous, mais le flux de paquets général doit être identique. 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 Renewel 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 Renewel 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** -

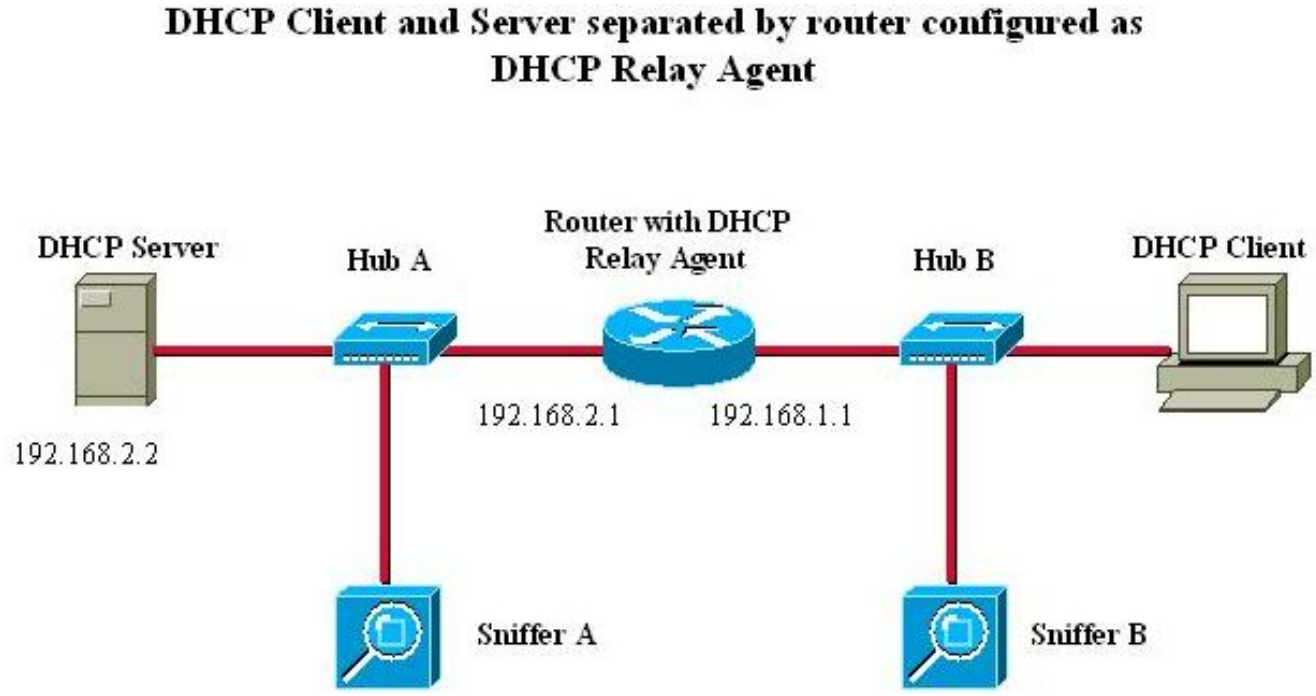
Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 0005DCC9C640 Broadcast 60 0:01:26.846 0.002.954 05/07/2001 11:52:03 AM ARP: R PA=[192.168.1.2]
 HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 58 arrived at 11:52:03.8470; frame size is 60 (003C 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:
```

Décodage du tracé de l'analyseur de réseau du client et du serveur DHCP séparé 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 Renewel 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 Renewel 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 Renewel 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 Renewel 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 postes de travail client ne peuvent pas obtenir d'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 de réseau local ou VLAN, et que le client ne peut pas obtenir l'adresse IP d'un serveur DHCP, il est peu probable que le routeur local soit la cause d'un problème DHCP. Le problème est très probablement lié aux périphériques qui se connectent au serveur DHCP ou au client DHCP. Cependant, le problème peut être causé par le serveur ou le client DHCP lui-même. Suivez les modules de dépannage ci-dessous pour déterminer quel périphérique cause le problème.

Remarque: Pour configurer le serveur DHCP par VLAN, définissez les différents pools DHCP pour tous les VLAN qui fournissent 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 et le client DHCP résident sur des différents segments LAN ou VLAN, le routeur qui agit en tant qu'agent relais DHCP/BootP est chargé du transfert du paquet DHCPREQUEST au serveur DHCP. Des étapes de dépannage supplémentaires sont requises pour dépanner l'agent relais DHCP/BootP, ainsi que le serveur et le client DHCP. Suivez les modules de dépannage ci-dessous pour déterminer quel périphérique cause le problème.

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 de la commande **show ip dhcp conflict**. 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.

Modules de dépannage de DHCP

Présentation des éventuels problèmes DHCP

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 provoqués par des défauts logiciels dans les systèmes d'exploitation, les pilotes de carte réseau (NIC), ou les agents relais DHCP/BootP exécutés sur les routeurs. En raison du nombre de points 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
- Erreur de logiciel du commutateur Cisco Catalyst ou de l'agent relais DHCP/BootP
- 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 de retransmission par le chemin inverse (RPF) est activée sur une interface, un routeur Cisco peut abandonner les paquets DHCP (Dynamic Host Configuration Protocol) ou BOOTP (BOOTstrap Protocol) dont l'adresse source est 0.0.0.0 et l'adresse de destination est 255.255.255.255. Le routeur peut également abandonner tous les paquets dotés d'une adresse IP de destination multicast à l'interface. Ce problème est documenté dans CSCdw31925 (clients enregistrés uniquement).
- L'agent de base de données DHCP n'est pas utilisé, mais la journalisation des conflits DHCP n'est *pas* désactivée.

Ce document utilise les modules de dépannage ci-dessous pour déterminer la cause initiale, comme indiqué dans la liste ci-dessus.

A. Vérifiez 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. En cas de connexion à un commutateur Catalyst, vérifiez que tant le client que le serveur DHCP sont connectés physiquement.

Pour les commutateurs Catalyst CatOS tels que les commutateurs de la gamme 2948G, 4000, 5000 et 6000, utilisez la commande **show port <mod#>/<port_range>** pour noter l'état du port. Si l'état du port est autre que connected, le port ne transmet pas de trafic, y compris les demandes de clients DHCP. La sortie des commandes est la suivante :

```
Switch (enable) show port 5/1
Port Name Status Vlan Duplex Speed Type
----- ----------------- ---------- ---------- ------ ----- ------------
5/1 connected 1 a-full a-100 10/100BaseTX
```

Pour les commutateurs basés sur le logiciel IOS tels que les commutateurs Catalyst 2900XL/3500XL/2950/3550, la commande équivalente à **show port status** est **show interface <interface>**. Si l'état de l'interface n'est pas « <interface> is up, line protocol is up », le port ne transmet pas de trafic, y compris les demandes de clients DHCP. La sortie des commandes est la suivante :

```
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 aucune liaison entre le commutateur Catalyst et le client DHCP, consultez le document Dépannage des problèmes de compatibilité entre les commutateurs Cisco Catalyst et les NIC pour des informations de dépannage supplémentaires concernant les problèmes de connectivité de couche physique.

Des erreurs de liaison de données excessives provoquent la mise à l'état errdisabled des ports sur certains commutateurs Catalyst. Référez-vous à Récupération de l'état de port errDisable sur les plates-formes CatOS et Reprise d'état errdisable port sur les plates-formes d'IOS Cisco, qui décrivent l'état errdisable, expliquent comment récupérer de cet état, et fournissent des exemples de reprise de cet état.

B. [Connectivité du réseau de test en configurant le poste de travail de client avec l'adresse IP statique]

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

Lors du dépannage d'un problème DHCP, il est important de vérifier la connectivité réseau en configurant une adresse IP statique sur un poste de travail client. Si le poste de travail ne peut pas accéder aux ressources réseau bien qu'une adresse IP statique soit configurée, la cause du problème n'est pas DHCP. Le dépannage de connectivité réseau est alors requis.

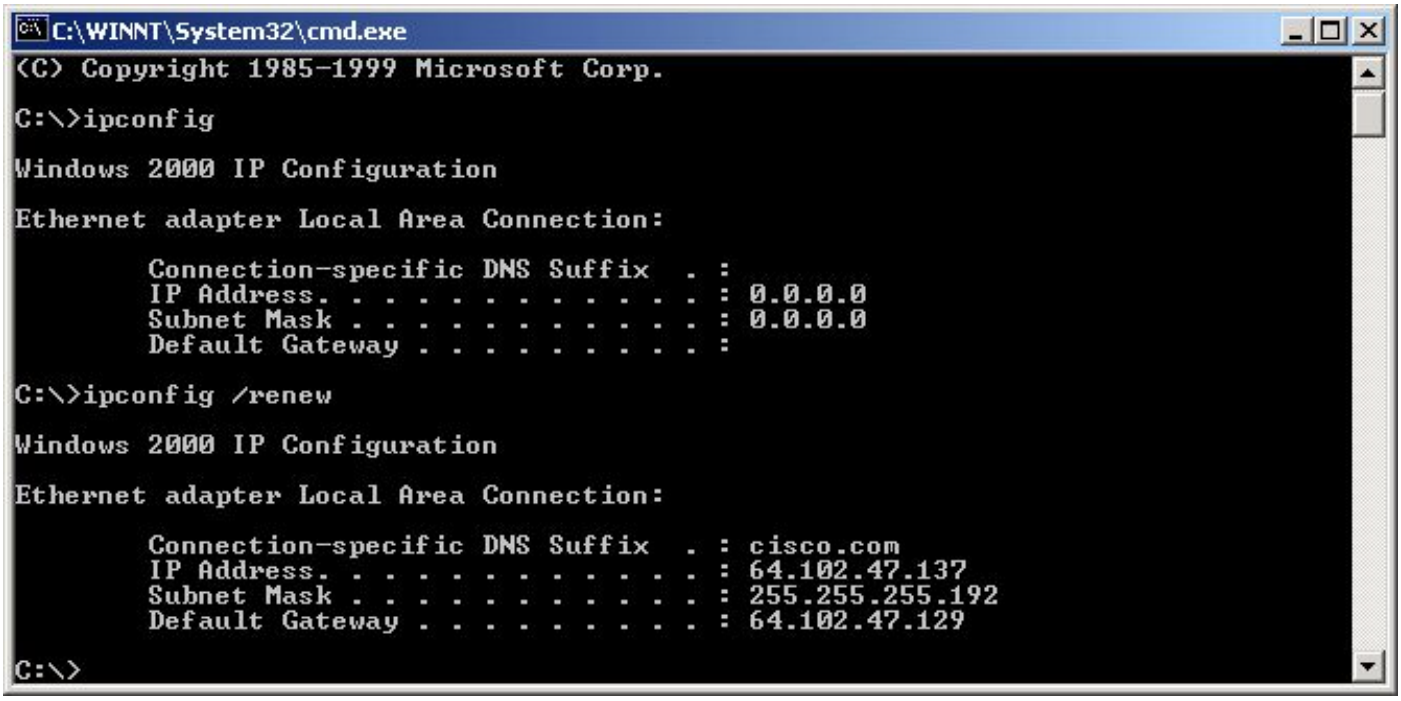
C. [Vérifiez la question comme problème de démarrage]

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

Si le client DHCP ne peut pas obtenir une adresse IP du serveur DHCP au démarrage, essayez d'obtenir une adresse IP du serveur DHCP en forçant manuellement le client à envoyer une demande DHCP. Suivez les étapes suivantes pour obtenir manuellement une adresse IP d'un serveur DHCP pour les systèmes d'exploitation mentionnés ci-dessous.

Microsoft Windows 95/98/ME : Cliquez sur le **bouton Start**, et exécutez le programme WINIPCFG.exe. Cliquez sur le **bouton de** ReleaseAll, suivi du **bouton de** RenewAll. Le DHCP Client peut-il maintenant obtenir une adresse IP ?

Microsoft Windows NT/2000 : Ouvrez une fenêtre d'invite de commande en tapant **cmd** dans le champ **Start/Run**. Exécutez la commande **ipconfig/renew** dans la fenêtre d'invite de commande, comme montré ci-dessous. Le client DHCP peut-il maintenant obtenir une adresse IP ?



Si le client DHCP peut obtenir une adresse IP en renouvelant manuellement l'adresse IP après que l'ordinateur a terminé le processus de démarrage, le problème est probablement un problème de démarrage de DHCP. Si le client DHCP est associé à un commutateur Cisco Catalyst, le problème est très probablement dû à un problème de configuration lié à STP portfast et/ou l'acheminement et l'agrégation de liaison. D'autres possibilités incluent des problèmes de cartes réseau ou de démarrage de port de commutateur. Les étapes de dépannage D et E doivent être passées en revue pour éliminer les problèmes de la configuration du port de commutateur et de cartes réseau comme cause du problème DHCP.

D. Vérifiez la configuration de port de commutateur (STP Portfast et d'autres commandes)

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 d'informations concernant la configuration requise du port de commutateur pour que DHCP fonctionne correctement une fois connecté aux commutateurs Catalyst, consultez le document suivant :

>Utilisation de PortFast et d'autres commandes pour remédier aux délais de connectivité lors du démarrage de la station de travail

Après avoir examiné les directives de configuration dans le document ci-dessus, revenez à ce document pour plus d'informations de dépannage.

E. Vérifier les problèmes connus de cartes réseau et de commutateurs Catalyst

Si la configuration du commutateur Catalyst est correcte, il est possible qu'un problème de compatibilité logicielle existe sur le commutateur Catalyst ou la carte réseau du client DHCP qui pourrait entraîner des problèmes DHCP. L'étape de dépannage suivante consiste à examiner le

document suivant et à éliminer tous les problèmes logiciels du commutateur Catalyst ou de la carte réseau qui pourraient participer au problème :

Dépannage de problèmes de compatibilité des commutateurs Cisco Catalyst avec NIC

Des connaissances du système d'exploitation du client DHCP ainsi que des informations de la carte réseau, telles que le fabricant, le modèle ou la version du pilote, sont nécessaires pour éliminer correctement tous les problèmes de compatibilité.

F. Distinction si les clients DHCP obtiennent l'adresse IP sur le même sous-réseau ou le VLAN que le serveur DHCP

Il est important de déterminer si DHCP fonctionne correctement ou non lorsque le client est sur le sous-réseau ou VLAN que le serveur DHCP. Si DHCP fonctionne correctement sur le même sous-réseau ou VLAN que le serveur DHCP, le problème DHCP peut provenir de l'agent relais DHCP/BootP. Si le problème persiste après avoir tester DHCP sur le même sous-réseau ou VLAN que le serveur DHCP, le problème vient probablement du serveur DHCP.

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

Suivez les étapes ci-dessous pour vérifier la configuration :

1. Lors de la configuration du relais DHCP sur un routeur, vérifiez que la commande **ip helper-address** est sur la bonne interface. La commande **ip helper-address** doit être présente sur l'interface entrante des postes de travail de client 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 toute fonctionnalité 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 service dhcp n'est pas activé, les clients ne reçoivent pas les adresses IP du serveur DHCP.**Remarque:** 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. Lors de l'application des commandes **ip helper-address** pour transférer les diffusions UDP à une adresse de diffusion de sous-réseau, vérifiez que la commande no ip directed-broadcast n'est configurée sur aucune interface de sortie que les paquets de diffusion UDP doivent traverser. La commande no ip directed-broadcast bloque toute conversion d'une diffusion dirigée en diffusions physiques. Cette configuration d'interface est la configuration par défaut dans les versions 12.0 et ultérieure du logiciel.
4. La transmission des diffusions DHCP à l'adresse de diffusion de sous-réseau du serveur DHCP est un problème logiciel occasionnel. Lors du dépannage de DHCP, essayez toujours de transférer les diffusions UDP DHCP à l'adresse IP du serveur DHCP, comme indiqué ci-dessous :

H. Option de l'identification d'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 du trafic 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) sur les commutateurs (agents relais) avec la commande de configuration globale, **no ip dhcp relay information option**.

I. Agent de base de données DHCP et se connecter de conflit 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 des paramètres d'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 no ip dhcp conflict logging pour désactiver la journalisation des conflits d'adresses DHCP. Supprimez 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 :

```
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)
```

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. Retirer en bas du SVI perturbe l'exécution de 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 exécute le logiciel IOS natif est mise en œuvre principalement sur le processeur de routage (RP ou MSFC), pas sur le processeur du commutateur (SP ou superviseur). 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 limitée d'émission

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 de réseau, la diffusion de 1 envoyée par DHCP est remplacée. Afin de résoudre ce problème, utilisez la commande ip dhcp limited-broadcast-address pour vous assurer qu'une diffusion de 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. DHCP de débogage utilisant des commandes de débogage de routeur

Vérifier que le routeur reçoit la demande DHCP à l'aide des commandes de débogage

Sur les routeurs qui prennent en charge le traitement logiciel des paquets DHCP, vous pouvez vérifier si un routeur reçoit la demande DHCP du client. Le processus DHCP échoue si le routeur ne reçoit pas les demandes du client. Cette étape de dépannage implique de configurer une liste d'accès pour la sortie de débogage. Cette liste d'accès est uniquement destinée au débogage et n'est pas intrusive pour le routeur.

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

access-list 100 permit ip host 0.0.0.0 host 255.255.255.255

Dans le mode exec, entrez la commande de débogage 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
```

Àpartir de la sortie ci-dessus, il est évident que le routeur reçoit les demandes 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 la demande DHCP et transfère les demandes au serveur DHCP à l'aide des commandes de débogage

Vous pouvez ajouter des entrées supplémentaires dans la liste d'accès pour voir si le routeur communique correctement avec le serveur DHCP. À nouveau, ces débogages ne regardent pas dans le paquet, mais vous pouvez vérifier si l'agent relais DHCP transfère les demandes au serveur DHCP.

En mode de configuration globale, créez la liste d'accès suivante :

access-list 100 permit ip host 0.0.0.0 host 255.255.255.255

access-list 100 permit udp host <agent_relais_dhcp> host <serveur_dhcp> eq 67

access-list 100 permit udp host <serveur_dhcp> host <agent_relais_dhcp> eq 67

Exemple :

access-list 100 permit ip host 0.0.0.0 host 255.255.255.0

access-list 100 permit udp host 192.168.1.1 host 192.168.2.2 eq 67

access-list 100 permit udp host 192.168.1.1 host 192.168.2.2 eq 68

access-list 100 permit udp host 192.168.2.2 host 192.168.1.1 eq 67

access-list 100 permit udp host 192.168.2.2 host 192.168.1.1 eq 68

Dans le mode exec, entrez la commande de débogage suivante :

```
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
```

Àpartir de la sortie ci-dessus, il est évident que le routeur reçoit les demandes DHCP du client et transfère la demande, conformément à la configuration d'agent relais DHCP/BootP, au serveur DHCP. Le serveur DHCP a également répondu directement à l'agent relais DHCP/BootP. 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 ou si le serveur répond avec un message DHCPNAK. 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 ; et la communication bidirectionnelle est établie avec le serveur DHCP.

Vérifier que le routeur reçoit et transfère la demande DHCP à l'aide de la commande debug ip udp

La commande debug ip udp peut être utilisée pour suivre le chemin d'une demande DHCP dans un routeur. Cependant, ce débogage est intrusif dans un environnement de production, puisque tous les paquets UDP commutés traités sont affichés dans la console. Ce débogage ne devrait pas être utilisé dans un environnement de production.

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

Dans le mode exec, entrez la commande de débogage suivante :

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 demande DHCP à l'aide de la commande debug ip dhcp server packet

Si l'IOS du routeur est de version 12.0.x.T ou 12.1 et prend en charge la fonctionnalité de serveur DHCP IOS, un débogage supplémentaire peut être effectué à l'aide de la commande **debug ip dhcp server packet**. Ce débogage est destiné à être utilisé avec la fonctionnalité de serveur DHCP IOS, mais peut être utilisé pour dépanner la fonctionnalité d'agent relais DHCP/BootP également. Comme pour les étapes de dépannage précédentes, les débogages de routeur ne permettent pas de déterminer précisément le problème puisque le paquet réel ne peut pas être affiché. Cependant, les débogages permettent d'effectuer des déductions concernant le traitement DHCP.

Dans le mode exec, entrez la commande de débogage 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.
```

Exécution de plusieurs débogages simultanés

Lors de l'exécution de plusieurs débogages simultanément, une certaine quantité d'informations peut être découverte quant au fonctionnement de l'agent relais et du serveur DHCP/BootP. À l'aide des directives de dépannage ci-dessus, vous pouvez faire des déductions quant aux éventuels problèmes de fonctionnalité d'agent relais DHCP/BootP.

```
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.
```

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

Les techniques de débogage de routeur ne permettent pas toujours de déterminer la cause exacte d'un problème DHCP. L'étape finale de résolution d'un problème DHCP est l'obtention d'un tracé de l'analyseur de réseau et la définition de la source du dysfonctionnement du processus. Les tracés de paquets DHCP peuvent être déchiffrés en se reportant aux sections Décodage du tracé de l'analyseur de réseau d'un client et d'un serveur DHCP sur un même segment de réseau local et Décodage du tracé de l'analyseur de réseau du client et du serveur DHCP séparé par un routeur configuré comme agent de relais DHCP de ce document.

Pour plus d'informations sur l'obtention des tracés de l'analyseur de réseau à l'aide de la fonctionnalité SPAN (Switched Port Analyzer) sur les commutateurs Catalyst, référez-vous au document suivant :

- Configuration de Catalyst Switched Port Analyzer (SPAN).

Autre méthode de décodage de paquets à l'aide du débogage du routeur

Àl'aide du

commande de **<acl> de** vidage mémoire de détail de debug ip packet sur un routeur de Cisco, il est possible d'obtenir un paquet entier dans l'hexa affiché dans le log système ou l'interface de ligne de commande (CLI). L'utilisation des sections Vérifier que le routeur reçoit la demande DHCP à l'aide des commandes de débogage et Vérifier que le routeur reçoit la demande DHCP et transfère les demandes au serveur DHCP à l'aide des commandes de débogage ci-dessus, ainsi que du mot clé de vidage ajouté à la liste d'accès, fournit les mêmes informations de débogage, mais avec les détails du paquet au format hex. Pour déterminer le contenu du paquet, le paquet doit être traduit. L'annexe A contient un exemple.

Les mots clés entrés après le code ASCII ip dhcp pool command option {numéro_option} sont entre guillemets doubles

Un routeur Cisco avec une option DHCP avec le numéro d'option configuré peut connaître une défaillance s'il essaie d'analyser l'URL car les mots clés entrés après que le code ASCII **ip dhcp pool command option option number** sont entre guillemets doubles après le rechargement du routeur. Ce comportement est présent sur les périphériques qui exécutent le logiciel IOS le 12.4(17a), et est un bogue connu et documenté dans CSCsk96976 (clients enregistrés uniquement).

Ce problème est résolu dans IOS versions 12.4(17b), 12.4(18a) et ultérieure, et 12.4(19)T1.

Annexe A : Exemple de configuration DHCP 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, des paramètres communs, par exemple le nom de domaine, doivent être configurés au niveau le plus élevé de l'arborescence (réseau ou sous-réseau).

Pour plus d'informations sur la configuration de DHCP et les commandes associées, référez-vous au lien suivant :

- Liste des tâches de configuration DHCP

```
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.
```

Informations connexes

- Exemple de configuration de la fonctionnalité de relais DHCP sur le concentrateur VPN 3000
- Exemple de configuration d'un dispositif PIX/ASA 7.x en tant que relais DHCP
- Outils et ressources
- Support technique - Cisco Systems