Configuration du relais DHCP ASA (Adaptive Security Appliance)

Table des matières

Introduction

Ce document décrit le relais DHCP sur Cisco ASA à l'aide des captures de paquets et des débogages, et fournit un exemple de configuration.

Conditions préalables

Un agent de relais DHCP (Dynamic Host Configuration Protocol) permet au dispositif de sécurité de transférer les requêtes DHCP des clients à un routeur ou à un autre serveur DHCP connecté à une autre interface.

Ces restrictions s’appliquent seulement à l’utilisation de l’agent de relais DHCP :

- L’agent de relais ne peut pas être activé si la caractéristique de serveur DHCP est également activée.
- Vous devez être directement connecté aux dispositifs de sécurité et ne pouvez pas envoyer

des demandes par un autre agent de relais ou un routeur.
- Pour le mode de contexte multiple, vous ne pouvez pas activer le relais DHCP ou configurer un serveur de relais DHCP sur une interface utilisée par plusieurs contextes.

Les services de relais DHCP ne sont pas offerts dans le mode transparent du pare-feu. Des appareils de sécurité réglés au mode transparent du pare-feu permettent seulement le trafic du protocole ARP (Address Resolution Protocol). Tout autre trafic exige une liste de contrôle d'accès (ACL). Afin de permettre les requêtes DHCP et les réponses par les appareils de sécurité en mode transparent, vous devez configurer deux ACL :

- Une liste de contrôle d'accès qui autorise les requêtes DHCP de l'interface interne vers l'extérieur.
- Une liste de contrôle d'accès qui autorise les réponses du serveur dans l'autre direction.

Exigences

Cisco recommande que vous ayez une connaissance de base de l'interface de ligne de commande ASA et de l'interface de ligne de commande Cisco IOS®.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appareil de sécurité de la gamme ASA 5500-x, version 9.x ou ultérieure
- Routeurs de la gamme Cisco 1800

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

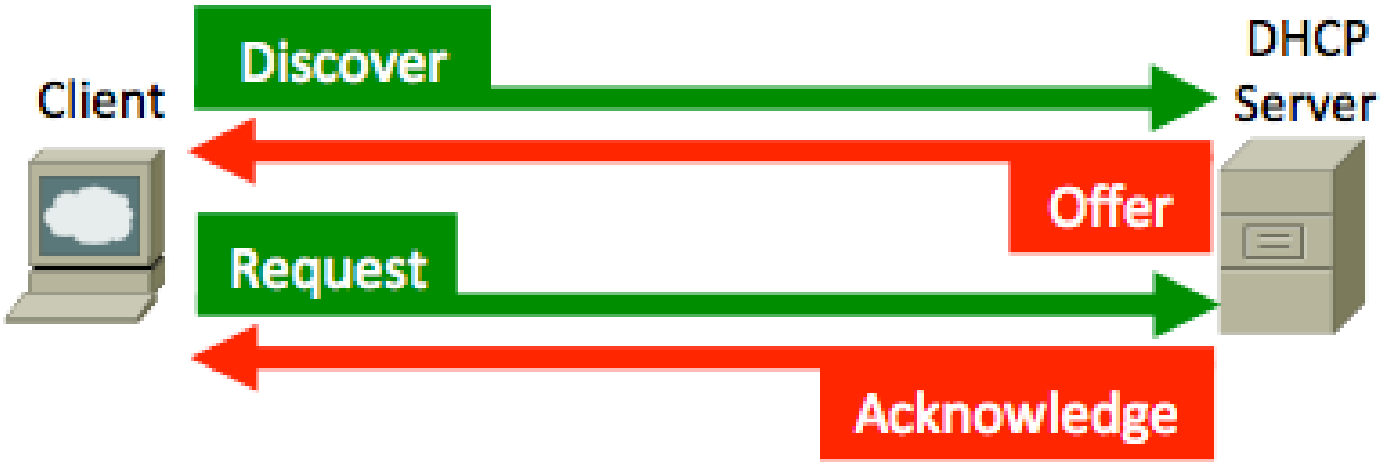
Le protocole DHCP fournit aux hôtes des paramètres de configuration automatique, tels qu'une adresse IP avec un masque de sous-réseau, une passerelle par défaut, une adresse de serveur de DNS et une adresse de serveur WINS (Windows Internet Name Service). Au départ, les clients DHCP n'ont aucun de ces paramètres de configuration. Pour obtenir ces renseignements, ils envoient une demande de diffusion. Lorsqu'un serveur DHCP voit cette demande, il fournit les renseignements nécessaires. Vu la nature de ces demandes de diffusion, le client et le serveur DHCP doivent être sur le même sous-réseau. Les périphériques de couche 3 comme les routeurs et les pare-feu ne transmettent généralement pas ces demandes de diffusion par défaut.

Une tentative de localisation des clients DHCP et d'un serveur DHCP sur le même sous-réseau n'est pas toujours pratique. Dans une telle situation, vous pouvez utiliser le relais DHCP. Lorsque l'agent de relais DHCP sur l'appareil de sécurité reçoit une requête DHCP d'un hôte sur une interface interne, il transmet celle-ci à un serveur DHCP donné sur une interface externe. Lorsque le serveur DHCP répond au client, l'appareil de sécurité répond en retour. Ainsi, l'agent de relais

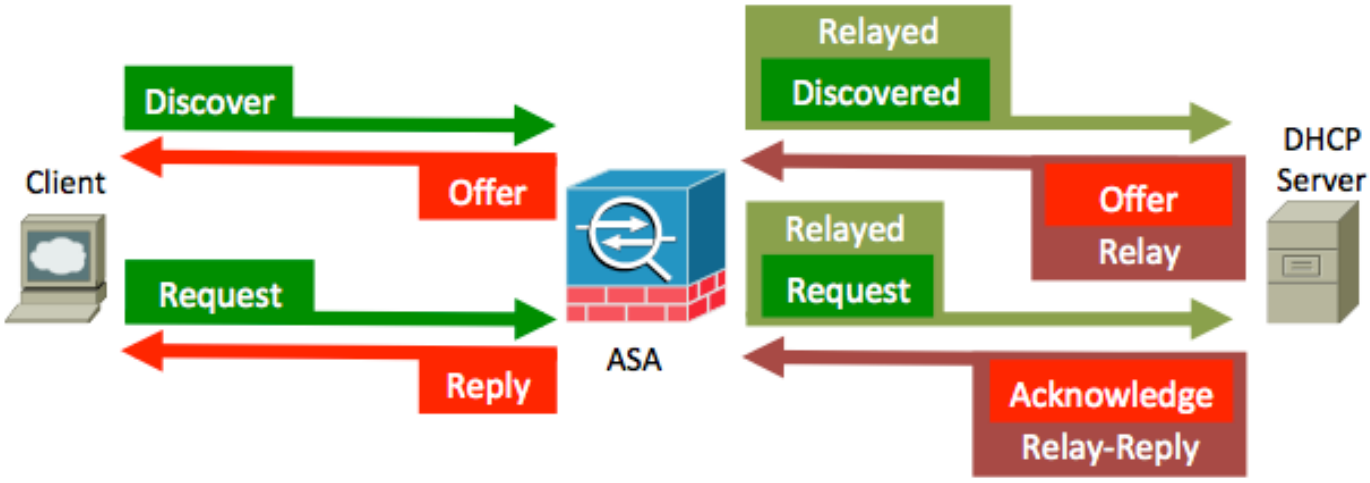
DHCP agit comme proxy pour le client DHCP dans sa conversation avec le serveur DHCP.

Flux des paquets

Cette image illustre le flux de paquets DHCP lorsqu'un agent de relais DHCP n'est pas utilisé :



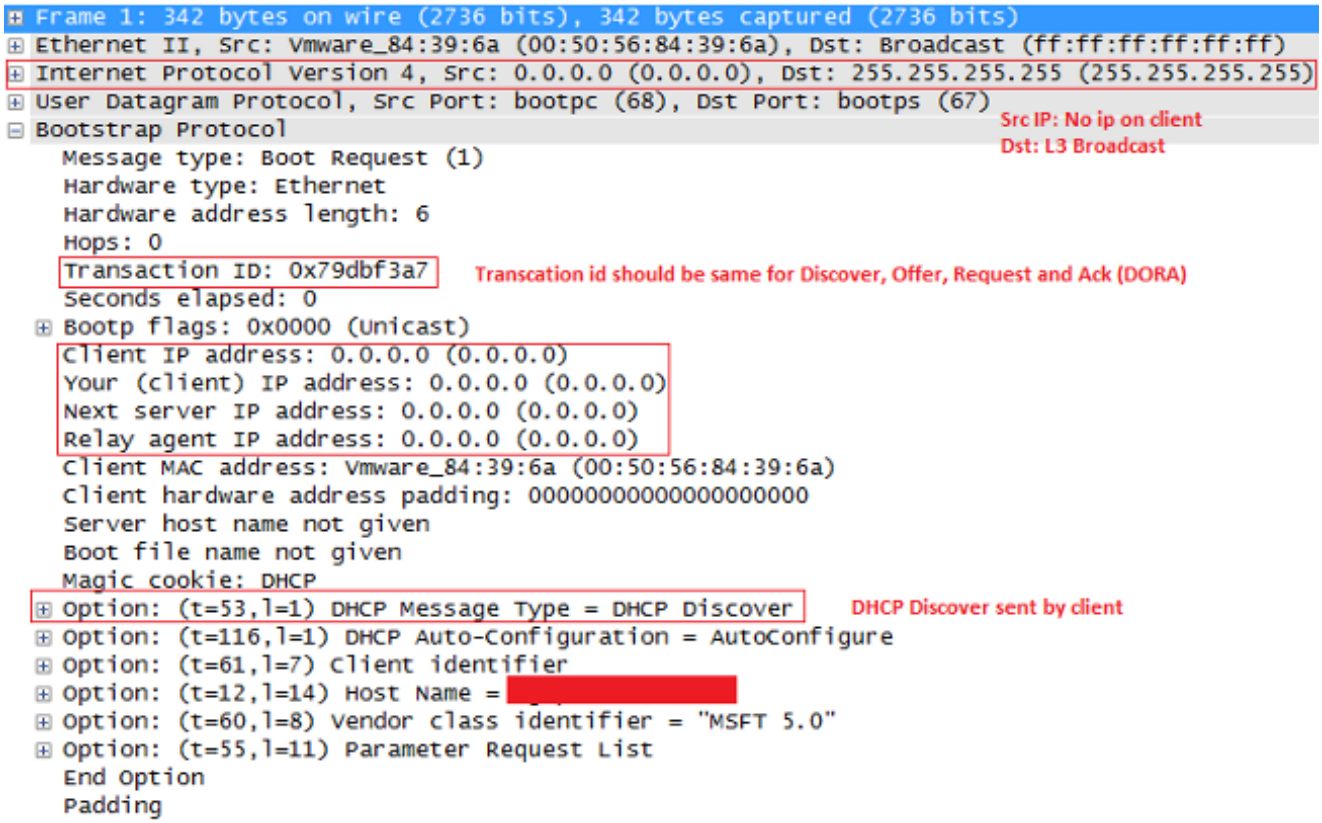
L'ASA intercepte ces paquets et les enveloppe dans le format de relais DHCP :



Relais DHCP avec capture de paquets sur les interfaces ASA interne et externe

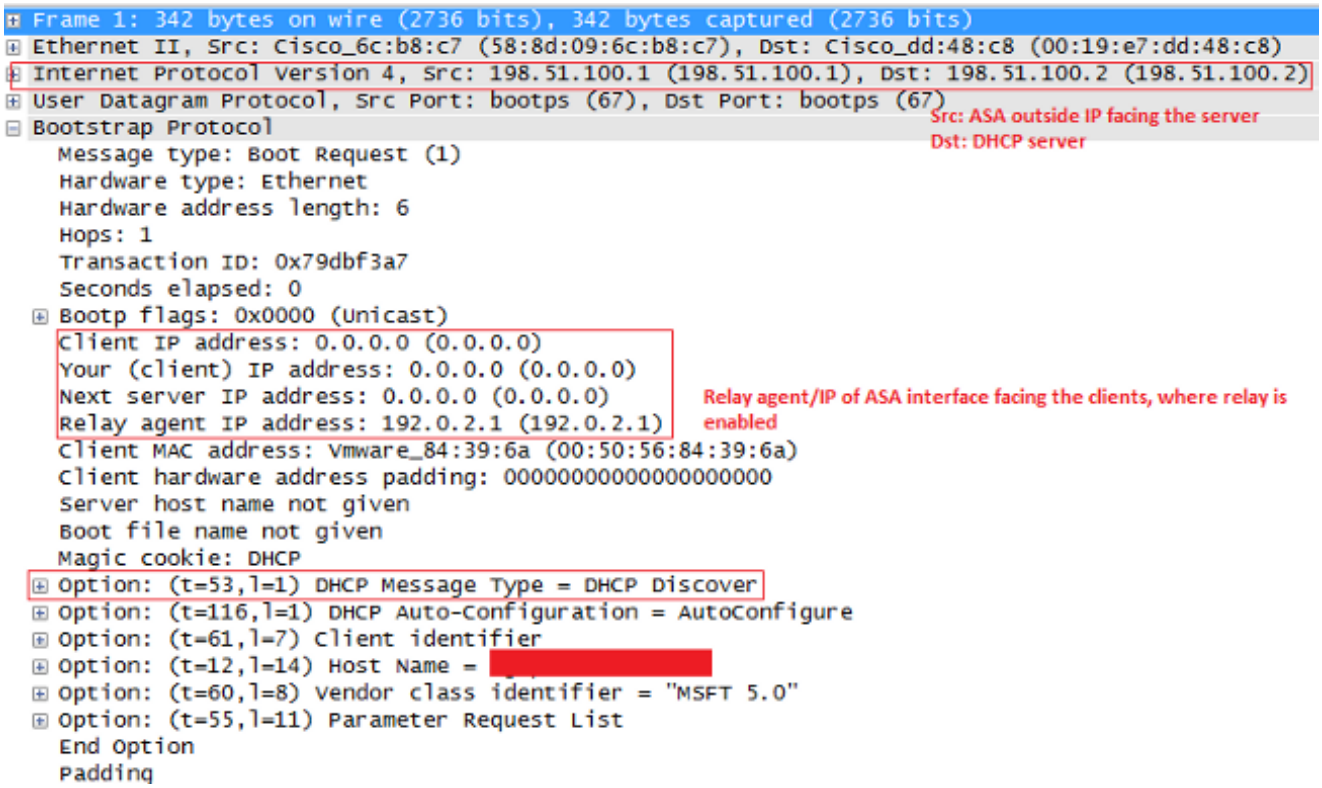
Notez le contenu surligné en ROUGE, car c'est ainsi que l'ASA modifie les divers champs.

1. Afin de démarrer le processus DHCP, démarrez le système et envoyez un message de diffusion (DHCPDISCOVER) à l'adresse de destination 255.255.255.255 – port UDP 67.



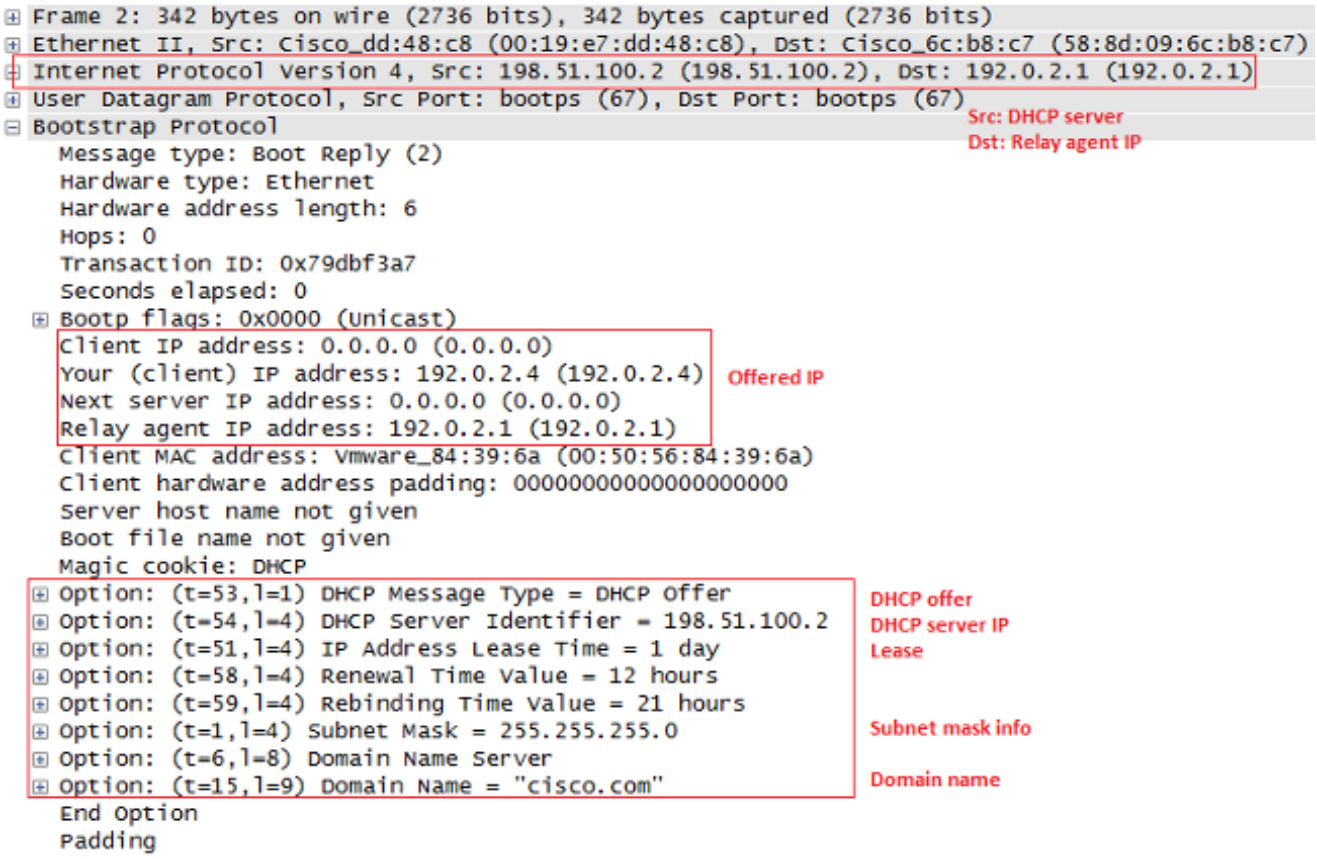
> Remarque : si un client VPN demande une adresse IP, l'adresse IP de l'agent de relais est la première adresse IP utilisable définie par la commande dhcp-network-scope, sous la stratégie de groupe.

2. Normalement, l’ASA abandonnerait la diffusion, mais comme il est configuré pour agir comme un relais DHCP, il transmet le message DHCPDISCOVER en tant que paquet monodiffusion au fournisseur d’adresse IP du serveur DHCP à partir de l’adresse IP de l’interface qui fait face au serveur. Dans le présent cas, il s’agit de l’adresse IP de l’interface externe. Remarquez la modification dans le champ de l’en-tête IP et de l’agent de relais :

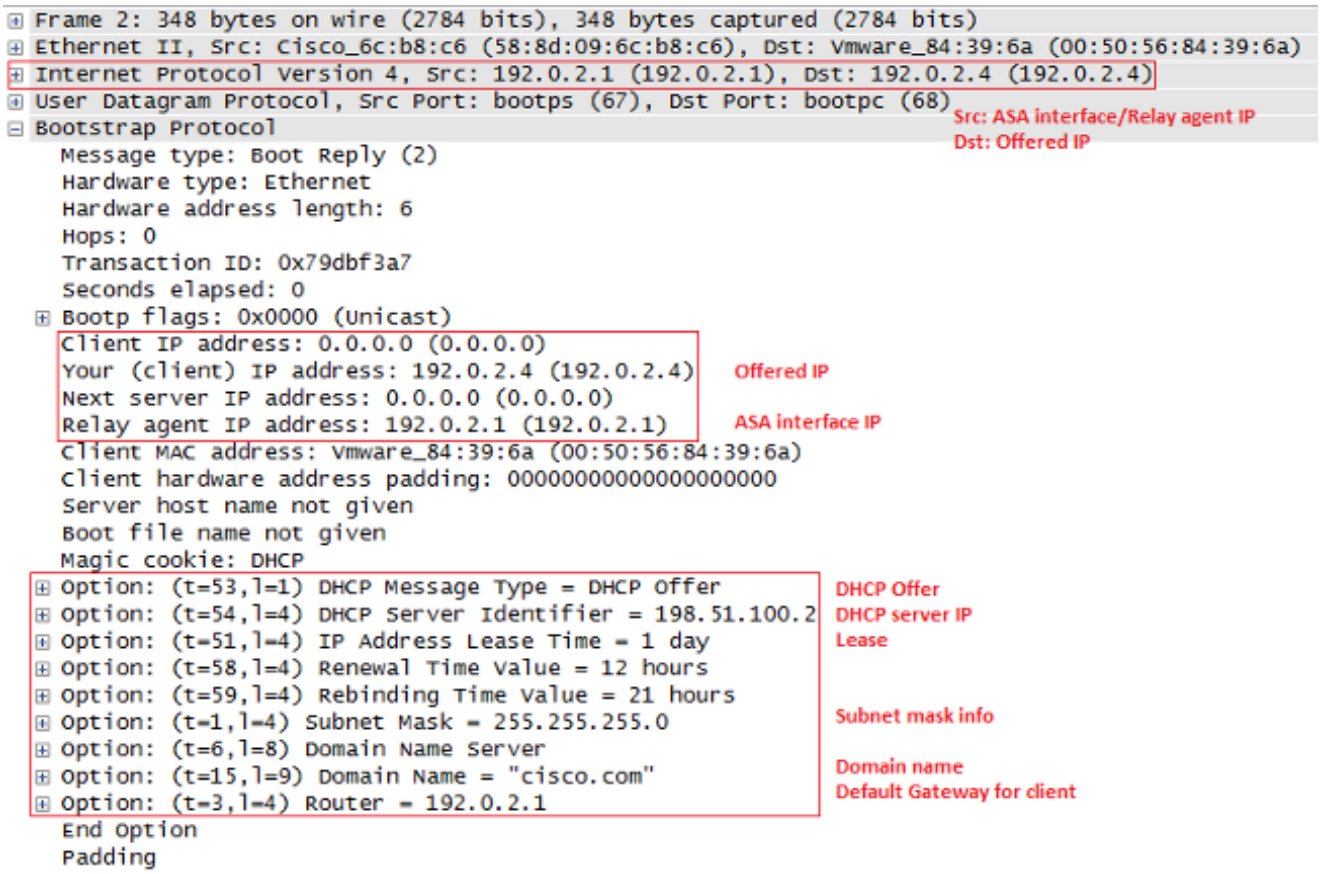


> Remarque : en raison du correctif incorporé dans l'ID de bogue Cisco CSCuo89924, ASA dans les versions 9.1(5.7), 9.3(1) et ultérieures peut transférer les paquets de monodiffusion à l'origine IP du serveur DHCP à partir de l'adresse IP de l'interface qui fait face au client (giaddr) où le dhcprelay est activé. Dans ce cas, il peut s'agir de l'adresse IP de l'interface interne.

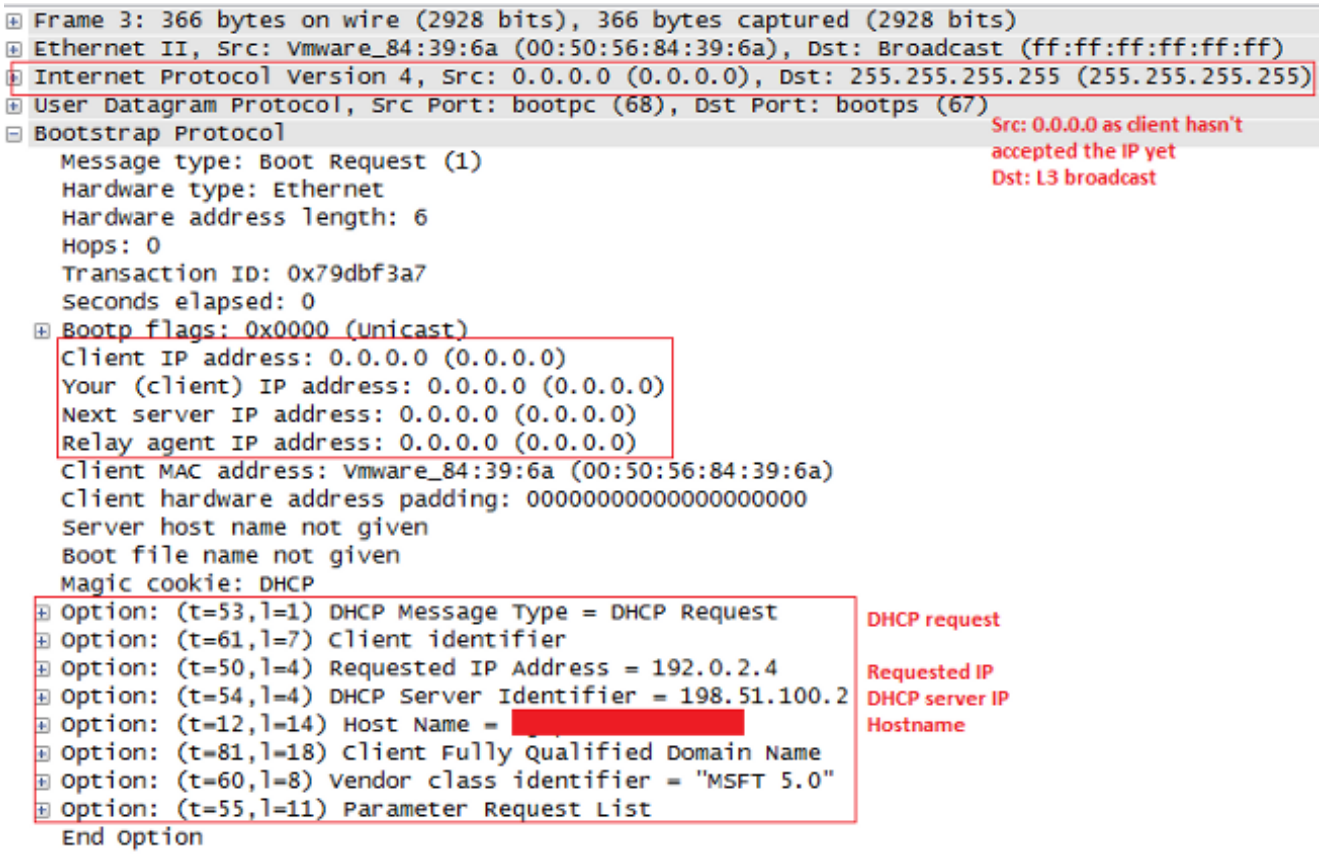
3. Le serveur renvoie un message DHCPOFFER en tant que paquet monodiffusion à l’ASA, destiné à l’adresse IP de l’agent de relais configuré dans le port DHCPDISCOVER-UDP 67. Dans ce cas, il s’agit de l’adresse IP de l’interface interne (giaddr), sur lequel dhcprelay est activé. Remarquez l’adresse IP de destination dans l’en-tête de couche 3 :



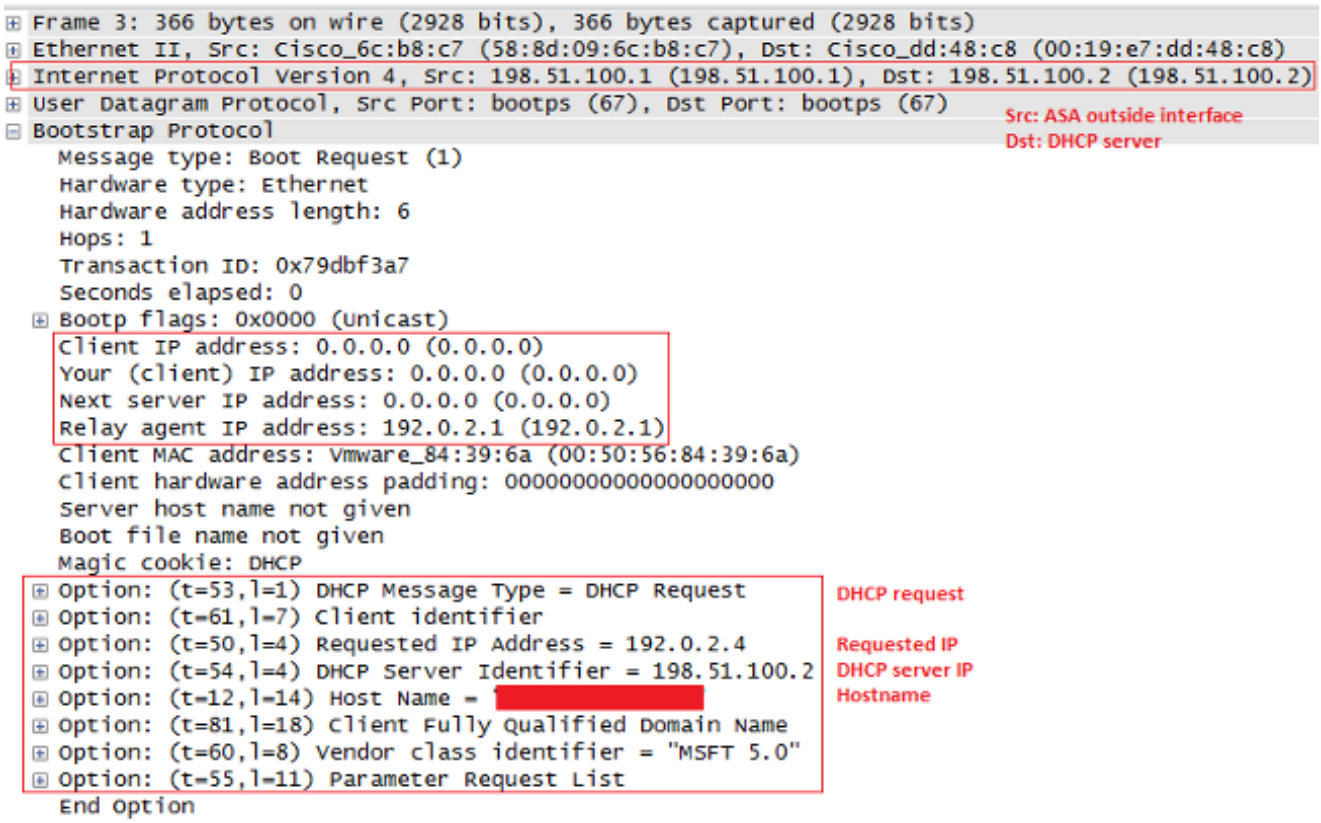
4. L'ASA envoie ce paquet par l'interface interne – port UDP 68. Remarquez la modification de l'en-tête IP pendant que le paquet quitte l'interface interne :



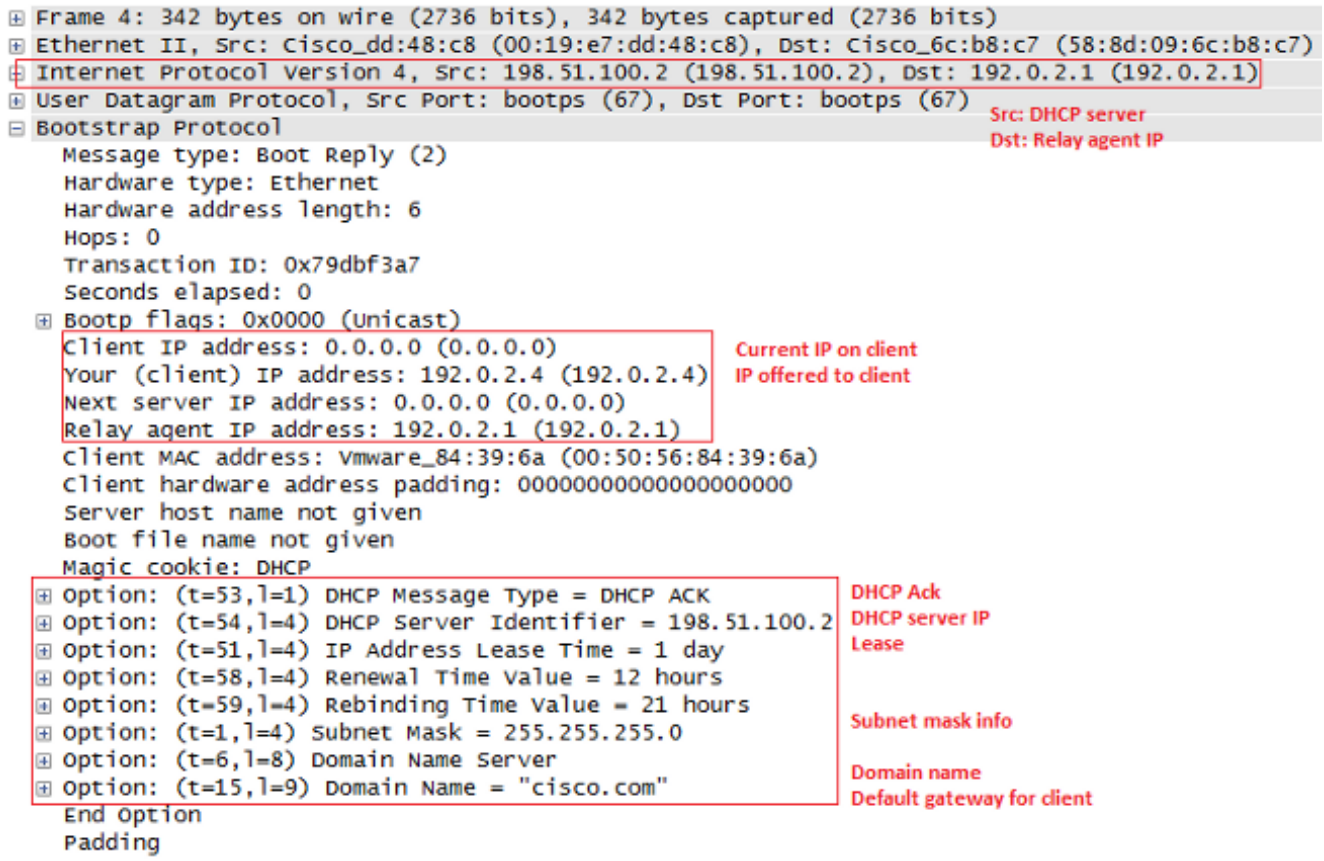
5. Lorsque vous recevez le message DHCPOFFER, envoyez un message DHCPREQUEST pour signaler que vous acceptez l’offre.



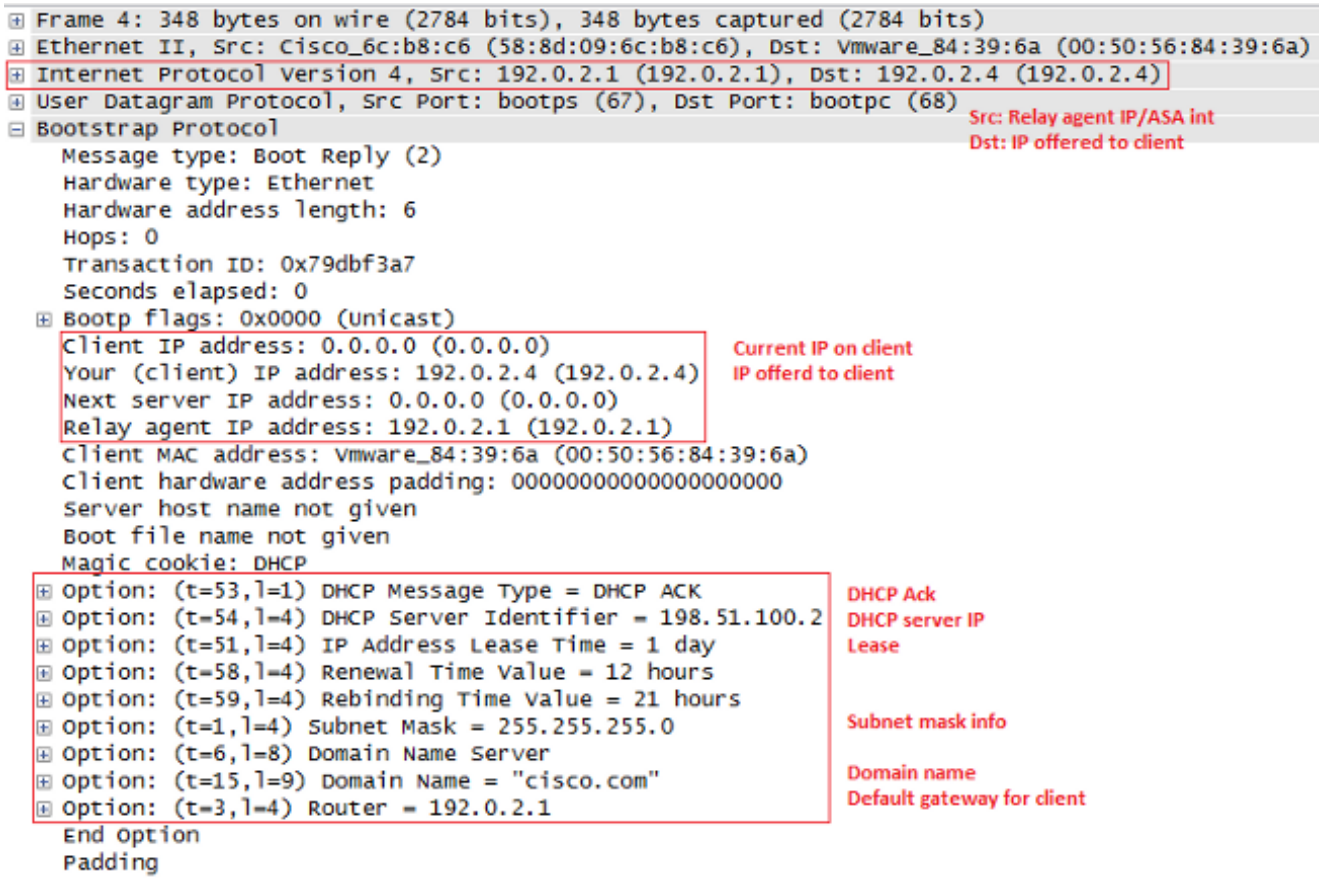
6. L’ASA transmet le message DHCPREQUEST au serveur DHCP.



7. Lorsque le serveur obtient le message DHCPREQUEST, il retourne le message DHCPACK pour confirmer l'adresse IP offerte.



8. L'ASA vous achemine le message DHCPACK du serveur DHCP, et voilà ce qui termine la transaction.



Débogage et SYSLOG pour les transactions de relais DHCP

Voici une requête DHCP acheminée à l'interface du serveur DHCP 198.51.100.2 :

```
DHCPRA: relay binding created for client 0050.5684.396a.DHCPD:
 setting giaddr to 192.0.2.1.

dhcpd_forward_request: request from 0050.5684.396a forwarded to 198.51.100.2.
DHCPD/RA: Punt 198.51.100.2/17152 --> 192.0.2.1/17152 to CP
DHCPRA: Received a BOOTREPLY from interface 2
DHCPRA: relay binding found for client 0050.5684.396a.
DHCPRA: Adding rule to allow client to respond using offered address 192.0.2.4
```

Une fois que la réponse est reçue du serveur DHCP, l'appareil de sécurité l'envoie au client DHCP avec l'adresse MAC 0050.5684.396a et change l'adresse de la passerelle pour son interface interne.

```
DHCPRA: forwarding reply to client 0050.5684.396a.
DHCPRA: relay binding found for client 0050.5684.396a.
DHCPD: setting giaddr to 192.0.2.1.
dhcpd_forward_request: request from 0050.5684.396a forwarded to 198.51.100.2.
DHCPD/RA: Punt 198.51.100.2/17152 --> 192.0.2.1/17152 to CP
DHCPRA: Received a BOOTREPLY from interface 2
DHCPRA: relay binding found for client 0050.5684.396a.
DHCPRA: exchange complete - relay binding deleted for client 0050.5684.396a.
```

```
DHCPD: returned relay binding 192.0.2.1/0050.5684.396a to address pool.
dhcpd_destroy_binding() removing NP rule for client 192.0.2.1
DHCPRA: forwarding reply to client 0050.5684.396a.
```

La même transaction apparaît également dans les journaux du système (SYSLOG) :

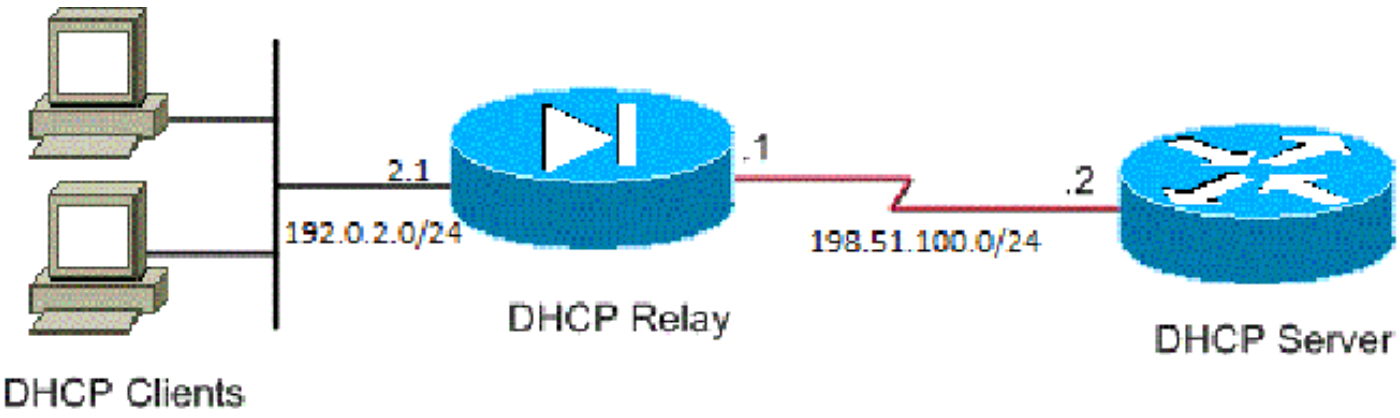
```
%ASA-7-609001: Built local-host inside:0.0.0.0
%ASA-7-609001: Built local-host identity:255.255.255.255
%ASA-6-302015: Built inbound UDP connection 13 for inside:
 0.0.0.0/68 (0.0.0.0/68) to identity:255.255.255.255/67 (255.255.255.255/67)
%ASA-7-609001: Built local-host identity:198.51.100.1
%ASA-7-609001: Built local-host outside:198.51.100.2
%ASA-6-302015: Built outbound UDP connection 14 for outside:
 198.51.100.2/67 (198.51.100.2/67) to identity:198.51.100.1/67 (198.51.100.1/67)

%ASA-7-609001: Built local-host inside:192.0.2.4
%ASA-6-302020: Built outbound ICMP connection for
 faddr 192.0.2.4/0 gaddr 198.51.100.2/1 laddr 198.51.100.2/1
%ASA-7-609001: Built local-host identity:192.0.2.1
%ASA-6-302015: Built inbound UDP connection 16 for outside:
 198.51.100.2/67 (198.51.100.2/67) to identity:192.0.2.1/67 (192.0.2.1/67)
%ASA-6-302015: Built outbound UDP connection 17 for inside:
 192.0.2.4/68 (192.0.2.4/68) to identity:192.0.2.1/67 (192.0.2.1/67)
%ASA-6-302021: Teardown ICMP connection for
 faddr 192.0.2.4/0 gaddr 198.51.100.2/1 laddr 198.51.100.2/1
```

Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- Configuration du relais DHCP au moyen de la CLI
- Configuration finale du relais DHCP
- Configuration du serveur DHCP

Configuration du relais DHCP au moyen de la CLI

```
dhcprelay server 198.51.100.2 outside
dhcprelay enable inside
dhcprelay setroute inside
dhcprelay timeout 60
```

Configuration finale du relais DHCP

```
show run
!
hostname ASA
names
!
interface Ethernet0/0
 nameif inside
 security-level 0
 ip address 192.0.2.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 100
 ip address 198.51.100.1 255.255.255.0
!
interface Ethernet0/2
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
no pager
logging enable
logging buffer-size 40960
logging buffered debugging
mtu inside 1500
```

```
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
timeout xlate 0:30:00
timeout pat-xlate 0:00:30
timeout conn 3:00:00 half-closed 0:30:00 udp 0:15:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 0:30:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0

dhcprelay server 198.51.100.2 Outside
dhcprelay enable inside
dhcprelay setroute inside

//Defining DHCP server IP and interface//
//Enables DHCP relay on inside/client facing interface//
//Sets ASA inside as DG for clients in DHCP reply packets//

dhcprelay timeout 60
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
!
!
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:7ae5f655ffe399c8a88b61cb13425972
: end
```

Configuration du serveur DHCP

```
show run
Building configuration...

Current configuration : 1911 bytes
!
! Last configuration change at 18:36:05 UTC Tue May 28 2013
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
logging buffered 4096
!
no aaa new-model
!
crypto pki token default removal timeout 0
!
!
dot11 syslog
ip source-route
!
ip dhcp excluded-address 192.0.2.1 192.0.2.2
ip dhcp excluded-address 192.0.2.10 192.0.2.254

//IP addresses exluded from DHCP scope//
!
ip dhcp pool pool1
 import all   network 192.0.2.0 255.255.255.0
   dns-server 192.0.2.10 192.0.2.11  domain-name cisco.com

//DHCP pool configuration and various parameters//
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1811W-AG-A/K9 sn FCTxxxx
!
!
!
interface Dot11Radio0
 no ip address
 shutdown
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role root
!
interface Dot11Radio1
 no ip address
 shutdown
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
```

```
!
interface FastEthernet0
 ip address 198.51.100.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!
interface FastEthernet3
 no ip address
!
interface FastEthernet4
 no ip address
!
interface FastEthernet5
 no ip address
!
interface FastEthernet6
 no ip address
!
interface FastEthernet7
 no ip address
!
interface FastEthernet8
 no ip address
!
interface FastEthernet9
 no ip address
!
interface Vlan1
 no ip address
!
interface Async1
 no ip address
 encapsulation slip
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 192.0.2.0 255.255.255.0 198.51.100.1

//Static route to ensure replies are routed to relay agent IP//
!
!
!
control-plane
!
!
line con 0
line 1
 modem InOut
 stopbits 1
 speed 115200
 flowcontrol hardware
```

```
line aux 0
line vty 0 4
 login
 transport input all
!
end
```

Relais DHCP avec plusieurs serveurs DHCP

Vous pouvez définir jusqu'à dix serveurs DHCP. Lorsqu'un client envoie un paquet DHCP Discover, celui-ci est transmis à tous les serveurs DHCP.

Voici un exemple :

```
dhcprelay server 198.51.100.2 outside
dhcprelay server 198.51.100.3 outside
dhcprelay server 198.51.100.4 outside
dhcprelay enable inside
dhcprelay setroute inside
```

Débogage avec plusieurs serveurs DHCP

Voici des exemples de débogage lorsque plusieurs serveurs DHCP sont utilisés :

```
DHCP: Received a BOOTREQUEST from interface 2 (size = 300)
DHCPRA: relay binding found for client 000c.291c.34b5.
DHCPRA: setting giaddr to 192.0.2.1.
dhcpd_forward_request: request from 000c.291c.34b5 forwarded to 198.51.100.2.
dhcpd_forward_request: request from 000c.291c.34b5 forwarded to 198.51.100.3.
dhcpd_forward_request: request from 000c.291c.34b5 forwarded to 198.51.100.4.
```

Captures avec plusieurs serveurs DHCP

Voici un exemple de capture de paquets lorsque plusieurs serveurs DHCP sont utilisés :

```
ASA# show cap out

3 packets captured

 1: 18:48:41.211628       192.0.2.1.67 > 198.51.100.2.67:  udp 300
 2: 18:48:41.211689       192.0.2.1.67 > 198.51.100.3.67:  udp 300
 3: 18:48:41.211704       192.0.2.1.67 > 198.51.100.4.67:  udp 300
```

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Afin de visualiser les renseignements statistiques sur les services de relais DHCP, saisissez la commande de statistiques show dhcprelay sur la CLI de l'ASA :

```
ASA# show dhcprelay statistics

DHCP UDP Unreachable Errors: 1
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          1
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              0
```

Cette sortie donne des renseignements sur plusieurs types de messages DHCP, p. ex., DHCPDISCOVER, DHCP REQUEST, DHCP OFER, DHCP RELEASE et DHCP ACK.

- Commande show dhcprelay state sur la CLI de l'ASA
- Commande show ip dhcp server statistics sur la CLI du routeur

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

```
Router#show ip dhcp server statistics

Memory usage         56637
Address pools        1
Database agents      0
Automatic bindings   1
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
```

```
DHCPREQUEST          1
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              0

ASA# show dhcprelay state
Context  Configured as DHCP Relay
Interface inside, Configured for DHCP RELAY SERVER
Interface outside, Configured for DHCP RELAY
```

Vous pouvez également utiliser ces commandes de débogage :

- debug dhcprelay packet
- debug dhcprelay event
- Captures
- SYSLOG

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de débogage.

Informations connexes

- Captures sur l'ASA
- Assistance et documentation techniques - Cisco Systems

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

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