適応型セキュリティアプライアンス(ASA)DHCPリレーの設定

内容

はじめに

このドキュメントでは、パケットキャプチャとデバッグを使用したCisco ASAでのDHCPリレーについて説明し、設定例を示します。

前提条件

Dynamic Host Configuration Protocol(DHCP)リレーエージェントを使用すると、セキュリティアプライアンスはクライアントからのDHCP要求を、別のインターフェイスに接続されたルータまたは他のDHCPサーバに転送できます。

以下の制限事項は、DHCP リレー エージェントの使用にのみ適用されます。

- DHCP サーバ機能も有効になっている場合、リレー エージェントを有効にできません。
- 直接セキュリティ アプライアンスに接続されている必要があり、別のリレー エージェントやルータを経由して要求を送信できません。

- マルチコンテキストモードの場合、複数のコンテキストで使用されるインターフェイスでDHCPリレーを有効にしたり、DHCPリレーサーバを設定したりすることはできません。

トランスペアレント ファイアウォール モードでは、DHCP リレー サービスを使用できません。トランスペアレント ファイアウォール モードのセキュリティ アプライアンスでは、アドレス解決プロトコル（ARP）トラフィックのみが通過可能です。その他のトラフィックにはすべてアクセス コントロール リスト（ACL）が必要です。トランスペアレント モードでセキュリティ アプライアンスを通じて、DHCP 要求および応答を許可するには、以下の 2 つの ACL を設定する必要があります。

- 内部インターフェイスから外部インターフェイスへの DHCP 要求を許可する ACL.
- 他の方向のサーバからの応答を許可する ACL.

要件

ASA CLIおよびCisco IOS® CLIに関する基本的な知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ASA 5500-x シリーズ セキュリティ アプライアンス リリース 9.x 以降
- Cisco 1800 シリーズ ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

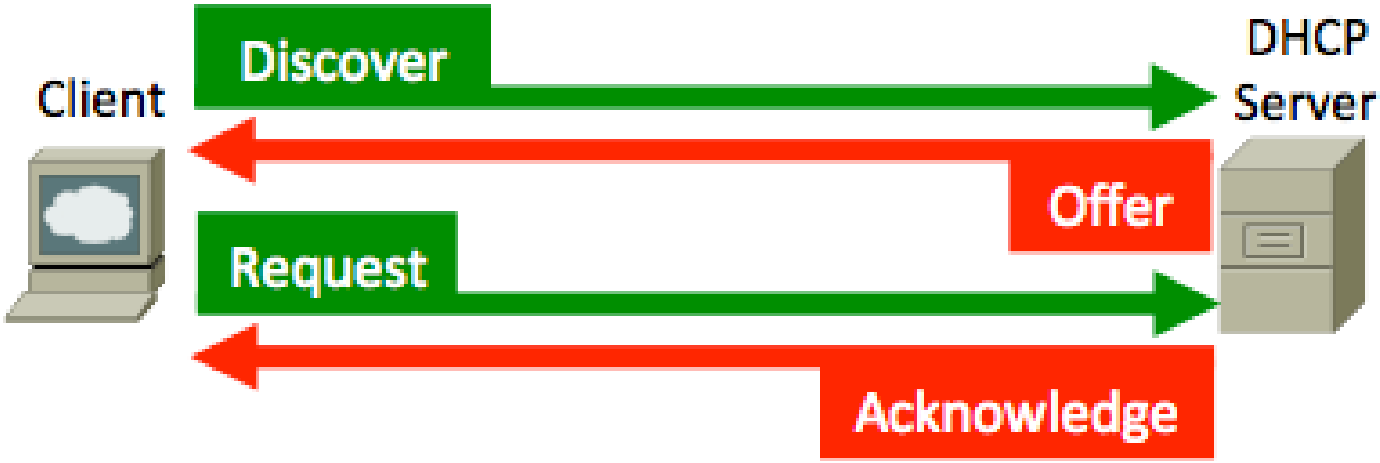
背景説明

DHCPプロトコルは、サブネットマスク付きのIPアドレス、デフォルトゲートウェイ、DNSサーバアドレス、Windows Internet Name Service(WINS)アドレスなどの自動設定パラメータをホストに提供します。最初は、DHCP クライアントにこれらの設定パラメータはありません。この情報を取得するために、クライアントからブロードキャスト要求が送信されます。DHCP サーバがこの要求を見て、必要な情報を提供します。このようなブロードキャスト要求の性質のため、DHCP クライアントとサーバは同じサブネット上にある必要があります。ルータやファイアウォールなどのレイヤ 3 デバイスは、一般に、デフォルトではこれらのブロードキャスト要求を転送しません。

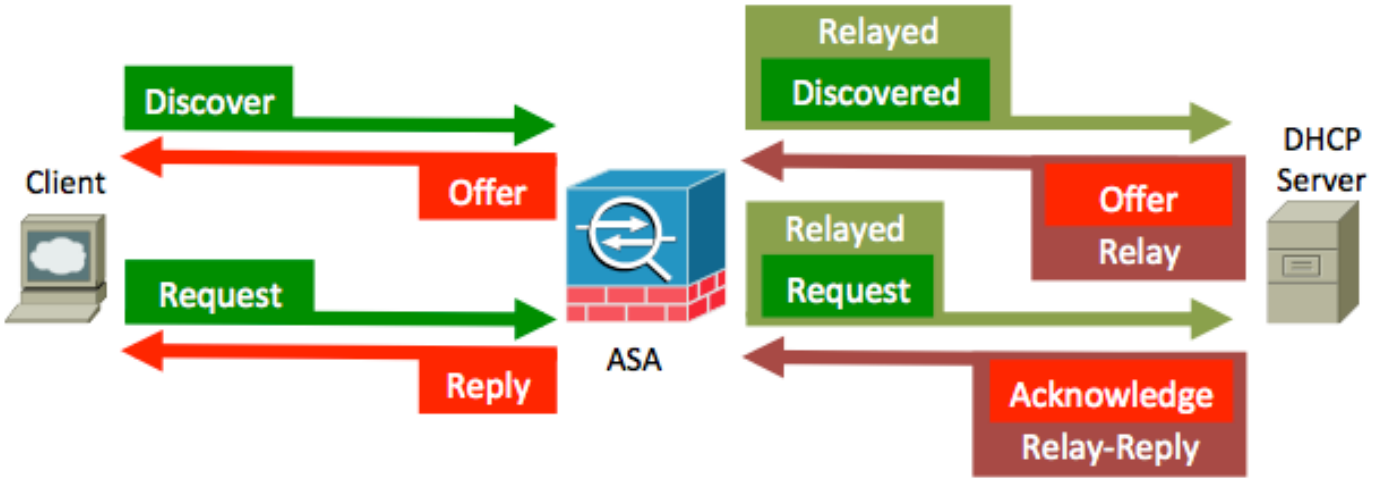
DHCPクライアントとDHCPサーバを同じサブネット上に配置する試みは、常に便利とは限りません。そのような配置が適さない場合には、DHCP リレーを使用できます。セキュリティ アプライアンス上の DHCP リレー エージェントが内部インターフェイスのホストからの DHCP 要求を受け取ると、その要求を外部インターフェイスの指定された DHCP サーバのいずれかに転送します。DHCP サーバがクライアントに返信すると、セキュリティ アプライアンスが返信を転送します。このため、DHCP リレー エージェントは DHCP サーバとのやり取りにおいて、DHCP クライアントのプロキシの役割を果たします。

パケット フロー

次の図は、DHCP リレー エージェントが使用されない場合の DHCP パケット フローを示しています。



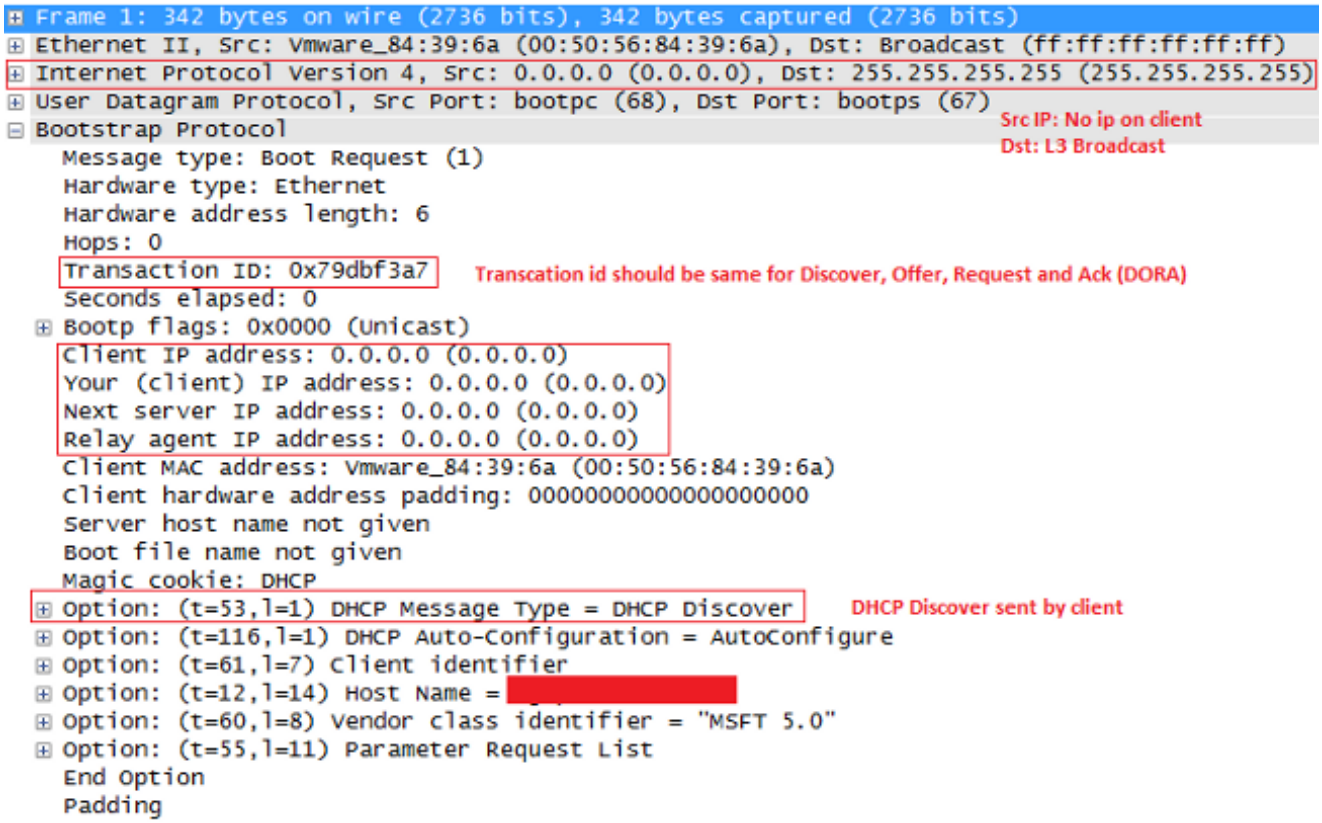
ASA はこれらのパケットを代行受信し、DHCP リレー フォーマットにラップします。



ASA の内部および外部インターフェイスのパケット キャプチャによる DHCP リレー

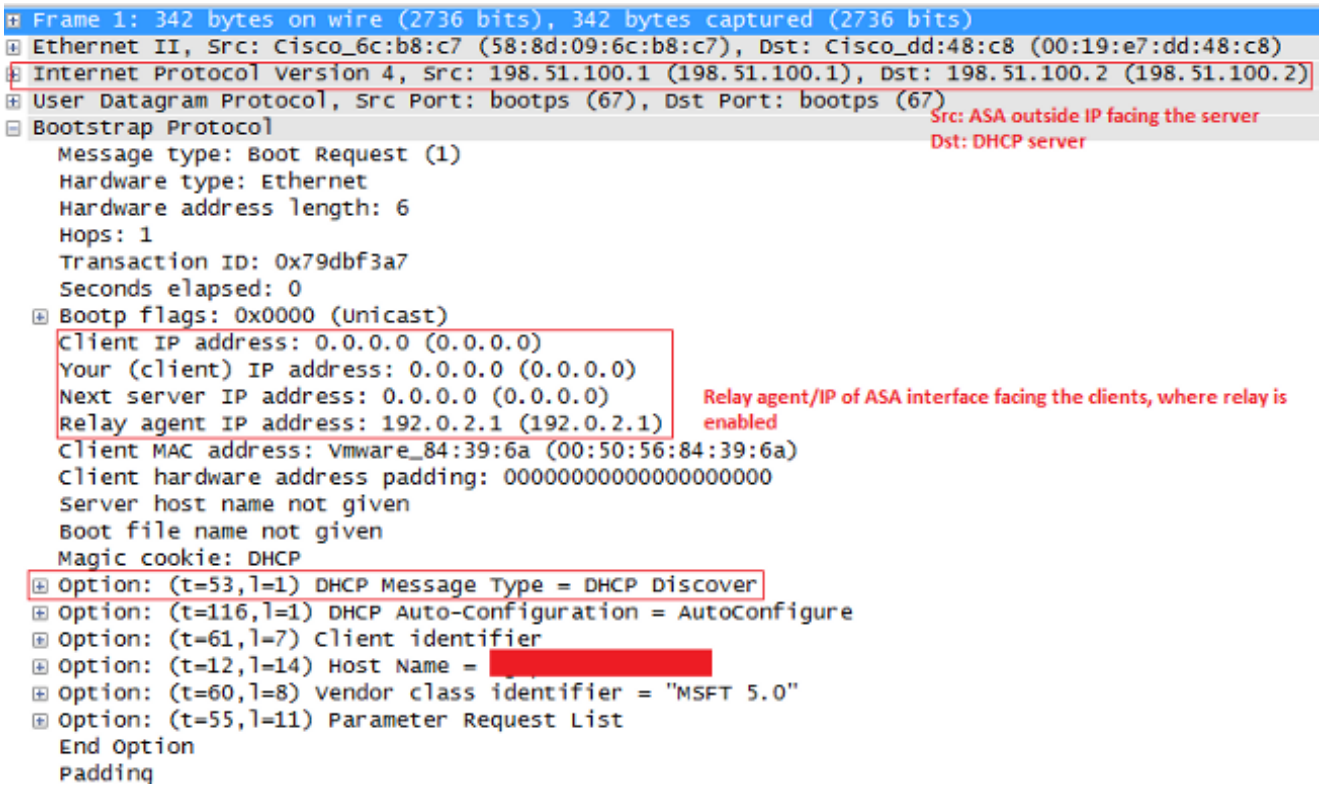
赤で強調されている部分は、ASA が各種フィールドを変更する方法を示しているので、内容をメモしてください。

1. DHCP プロセスを開始するには、システムを起動して、ブロードキャスト メッセージ（DHCPDISCOVER）を宛先アドレス 255.255.255.255（UDP ポート 67）に送信します。



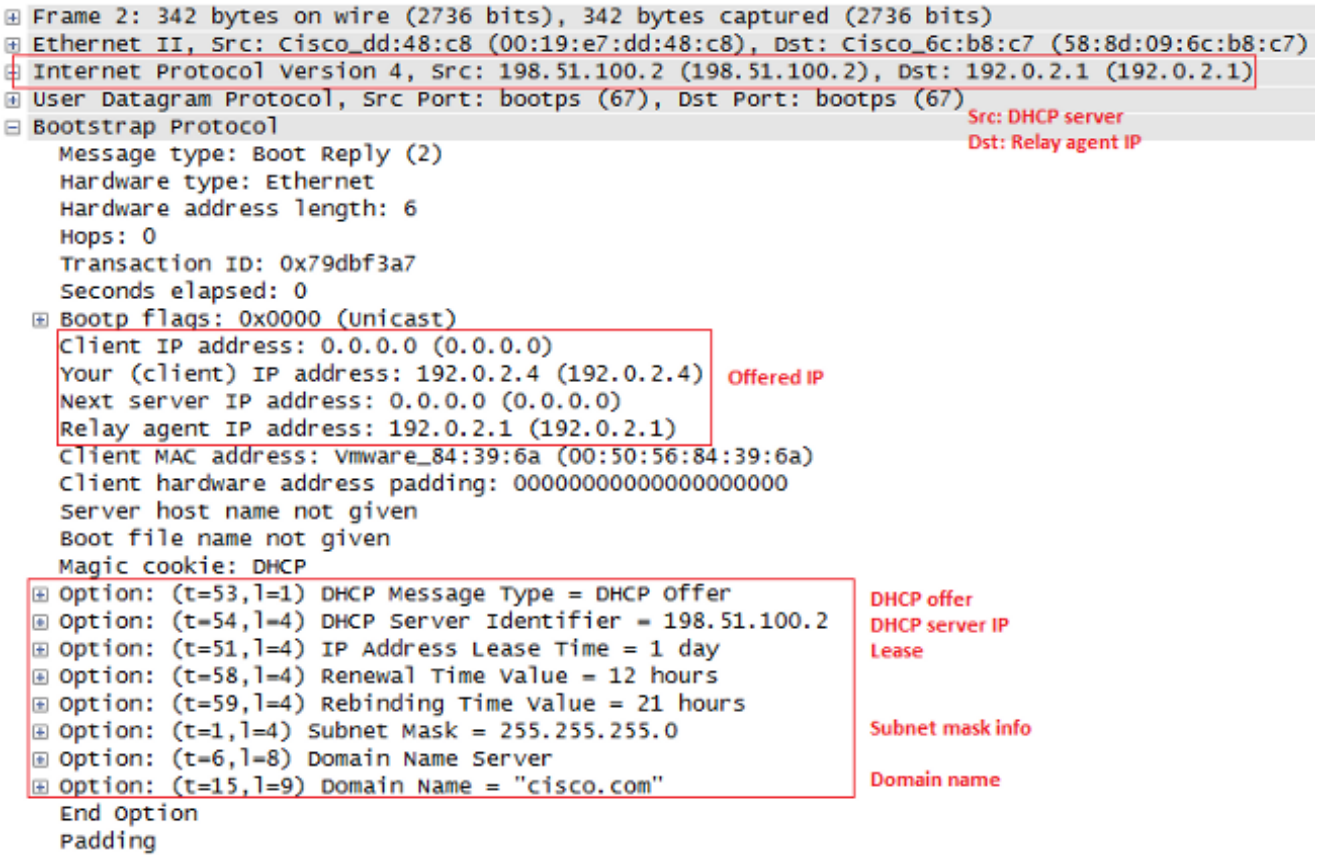
注:VPNクライアントがIPアドレスを要求する場合、グループポリシーでdhcp-network-scopeコマンドによって定義された、最初に使用できるIPアドレスがリレーエージェントのIPアドレスになります。

2. 通常 ASA はブロードキャストを廃棄しますが、DHCP リレーとして機能するように設定されているため、サーバ側のインターフェイス IP から DHCP サーバの IP 送信元に、ユニキャスト パケットとして DHCPDISCOVER メッセージを転送します。この場合は外部インターフェイスの IP アドレスです。IP ヘッダーとリレー エージェント フィールドの変更点に注目してください。

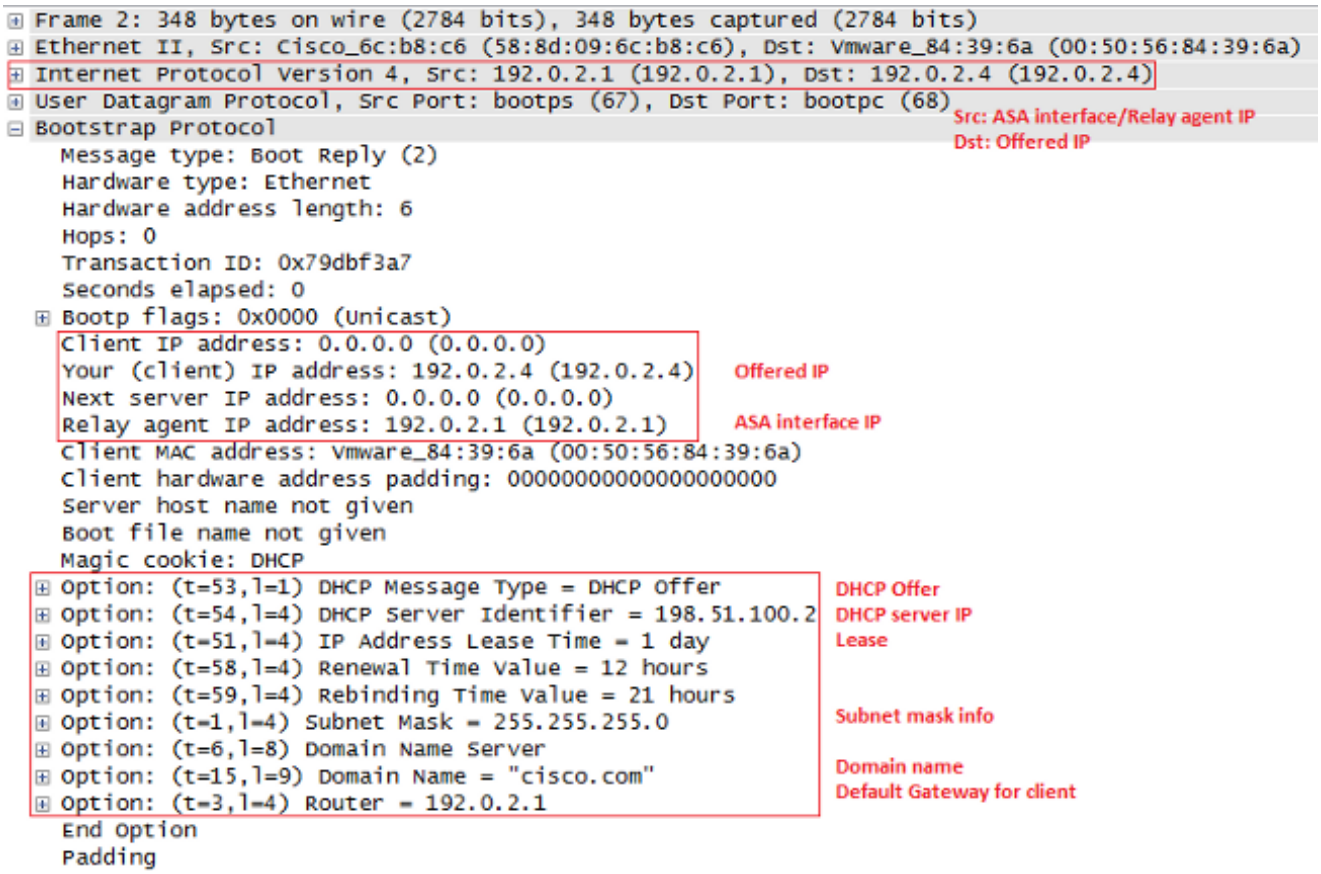


> 注:Cisco Bug ID CSCuo89924に組み込まれている修正により、バージョン9.1(5.7)、9.3(1)以降のASAは、dhcprelayが有効になっているクライアント(giaddr)側のインターフェイスIPアドレスから、DHCPサーバのIP送信元にユニキャストパケットを転送できます。この場合は、内部インターフェイスのIPアドレスにすることができます。

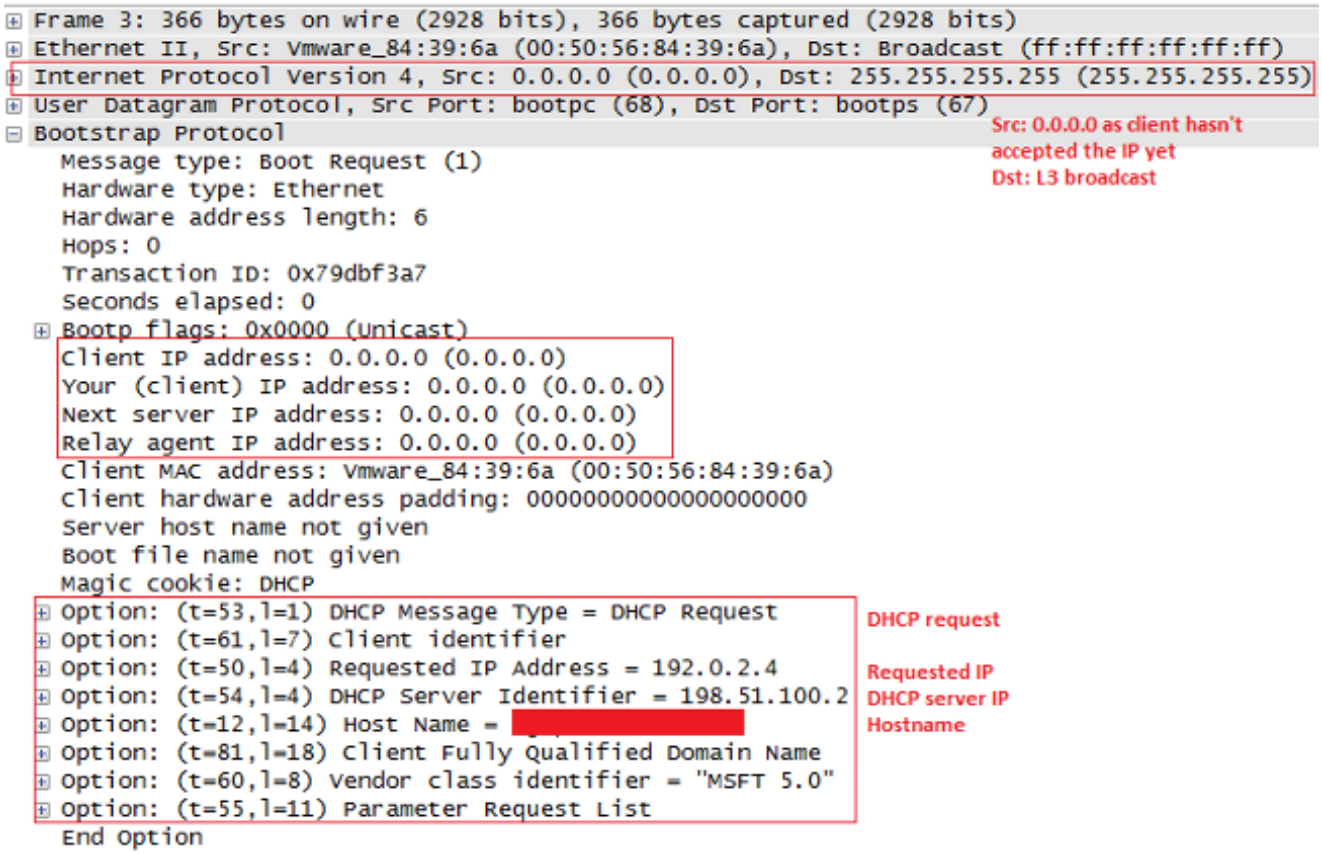
3. サーバは、DHCPDISCOVER（UDP ポート 67）で設定されたリレー エージェントの IP を宛先とする ASA に、ユニキャスト パケットとして DHCPOFFER メッセージを返信します。この場合は、dhcprelay が有効になっている内部インターフェイスの IP アドレス（giaddr）です。レイヤ 3 ヘッダーの宛先 IP に注目してください。



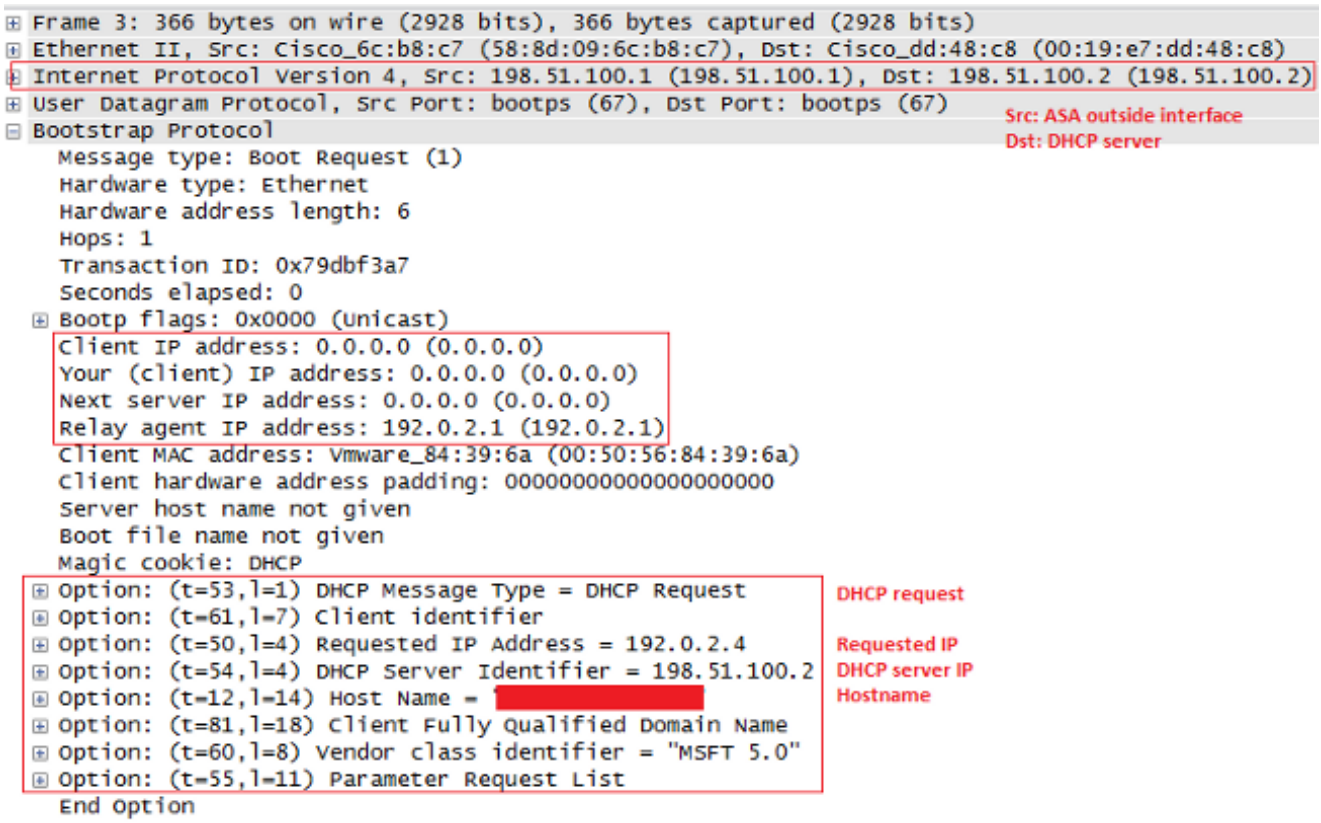
4. ASA は、このパケットを内部インターフェイス（UDP ポート 68）から送信します。パケットが内部インターフェイスから送信されるときの IP ヘッダーの変更点に注目してください。



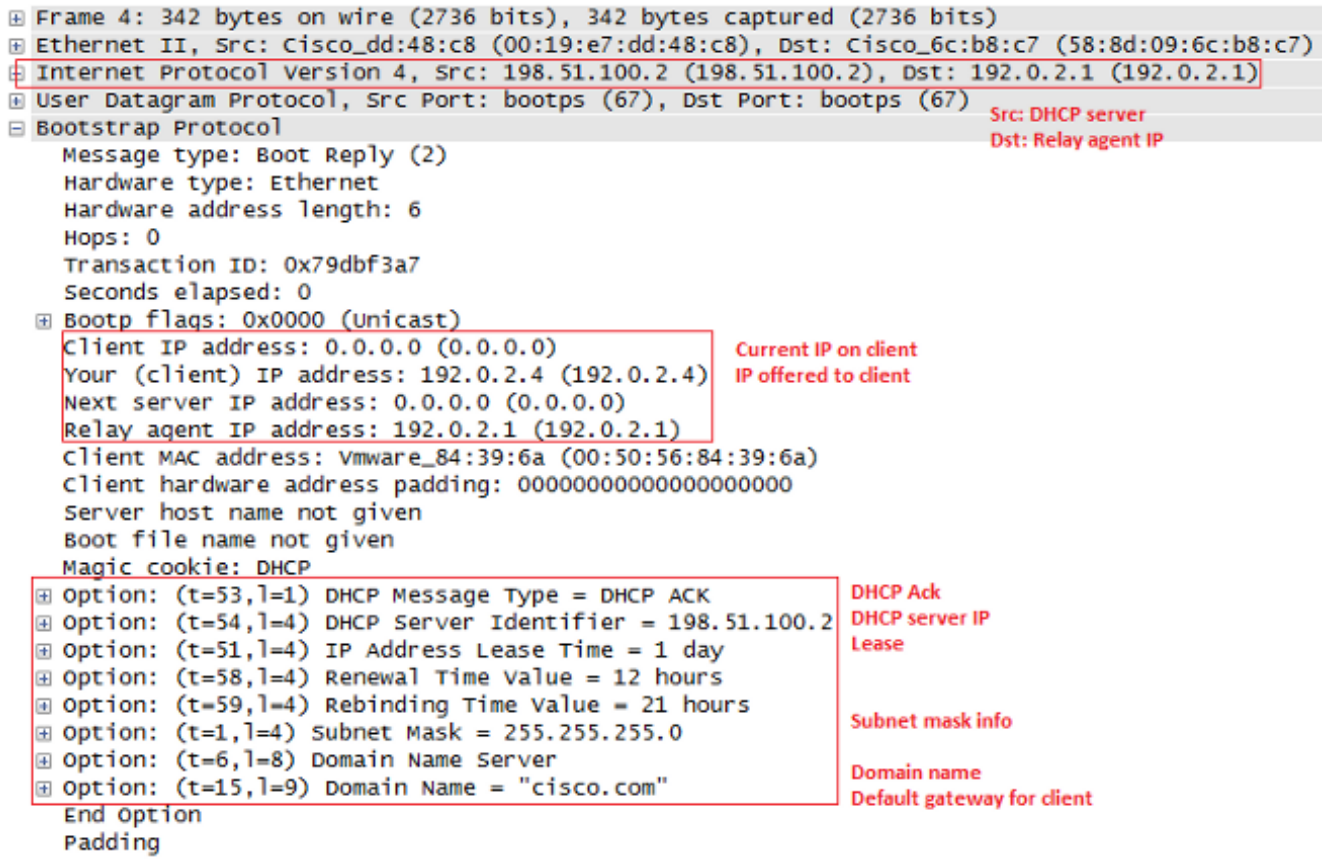
5. DHCPOFFER メッセージを受信したら、オファーを受け入れることを示すために DHCPREQUEST メッセージを送信します。



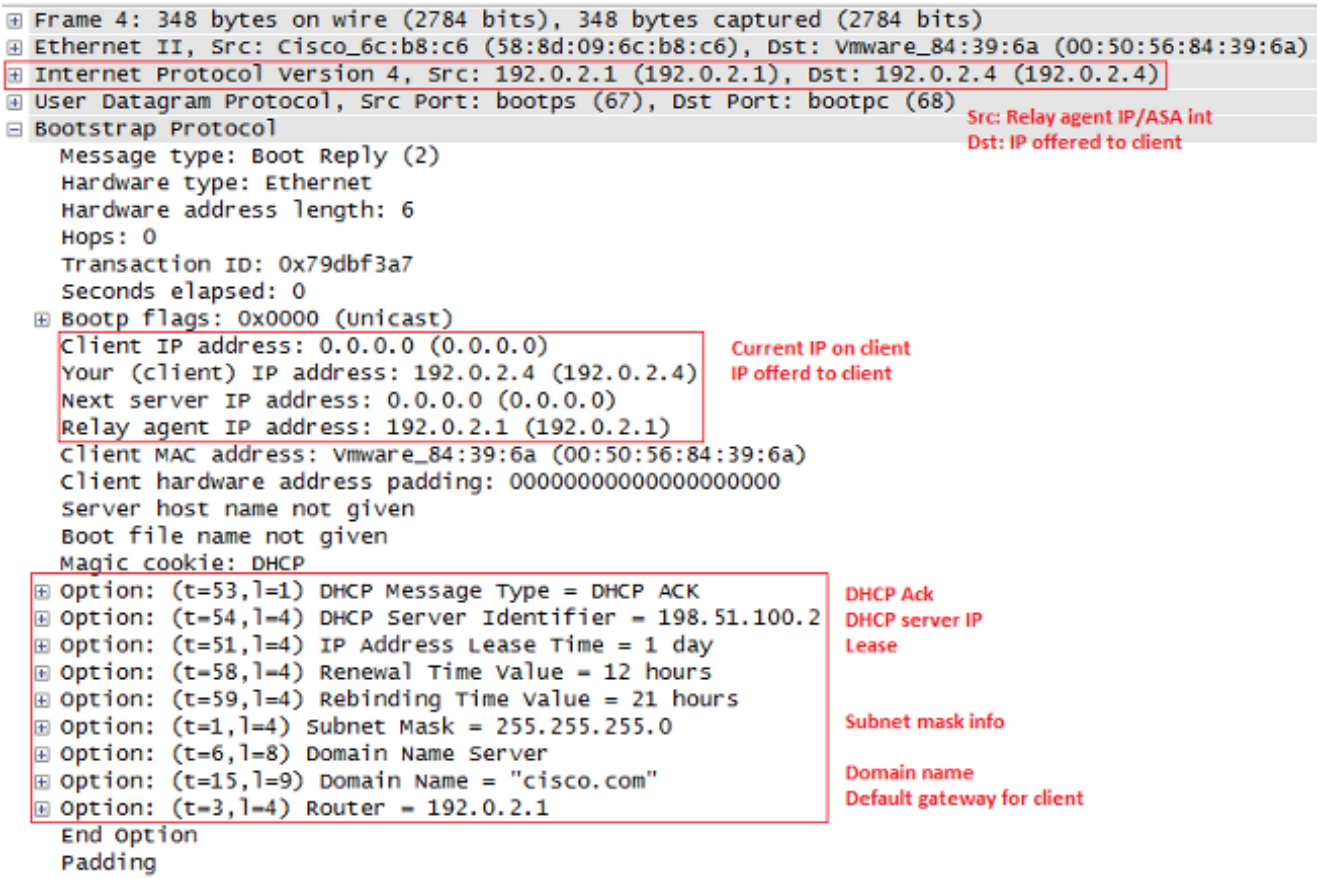
6. ASA が DHCP サーバに DHCPREQUEST を渡します。



7. サーバは DHCPREQUEST を受け取ると、オファーされた IP を確認するために DHCPACK を返信します。



8. ASA が DHCP サーバからの DHCPACK をユーザに渡して、トランザクションは完了します。



DHCP リレー トランザクションのデバッグおよび syslog

以下は、DHCP サーバ インターフェイス 198.51.100.2 に転送される DHCP 要求です。

```
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
```

応答が DHCP サーバから受信された後、セキュリティ アプライアンスが DHCP クライアント（MAC アドレスが 0050.5684.396a）に転送して、ゲートウェイ アドレスを自身の内部インターフェイスに変更します。

```
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.
```

同じトランザクションが syslog にも表示されます。

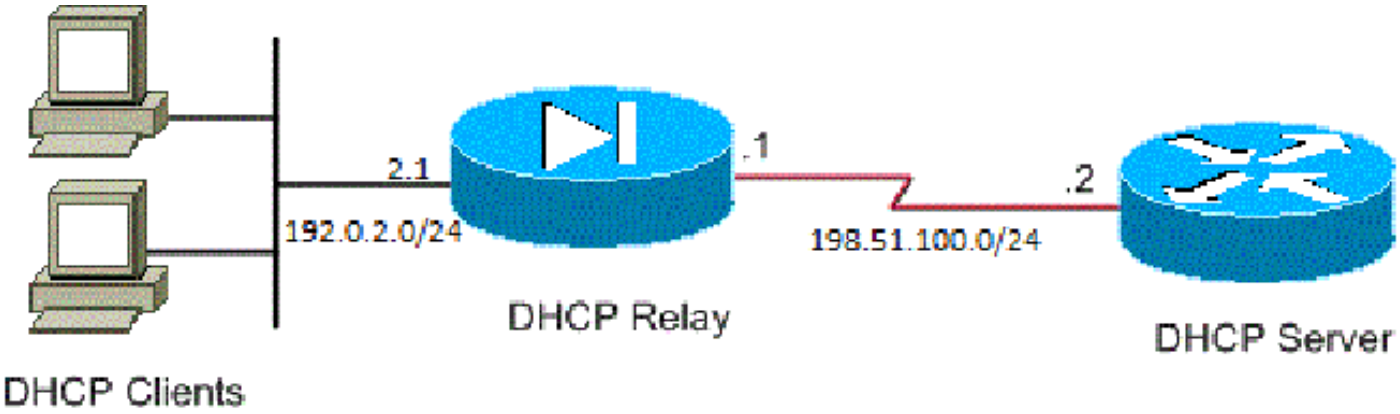
```
%ASA-7-609001: Built local-host inside:0.0.0.0
%ASA-7-609001: Built local-host identity:255.255.255.255
%ASA-6-302015: Built inbound UDP connection 13 for inside:
 0.0.0.0/68 (0.0.0.0/68) to identity:255.255.255.255/67 (255.255.255.255/67)
%ASA-7-609001: Built local-host identity:198.51.100.1
%ASA-7-609001: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

設定

このセクションでは、このドキュメントで説明する機能を設定するための情報を提供します。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



コンフィギュレーション

このドキュメントでは、次のコンフィギュレーションを使用します。

- CLI を使用した DHCP リレーの設定
- DHCP リレーの最終的な設定
- DHCP サーバの設定

CLI を使用した DHCP リレーの設定

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

DHCP リレーの最終的な設定

```
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
```

DHCP サーバの設定

```
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
```

複数のDHCPサーバを使用するDHCPリレー

最大10台のDHCPサーバを定義できます。クライアントがDHCP Discoverパケットを送信すると、そのパケットはすべてのDHCPサーバに転送されます。

ランダム データの例は次のとおりです。

```
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
```

複数のDHCPサーバでのデバッグ

複数のDHCPサーバを使用する場合のデバッグ例を次に示します。

```
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.
```

複数のDHCPサーバを使用したキャプチャ

複数のDHCPサーバを使用する場合のパケットキャプチャの例を次に示します。

```
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
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

DHCP リレー サービスに関する統計情報を表示するには、ASA CLI で show dhcprelay statistics コマンドを入力します。

```
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
```

この出力は、DHCPDISCOVER、DHCP REQUEST、DHCP OFER、DHCP RELEASE、および DHCP ACK などの複数の DHCP メッセージ タイプに関する情報を提供します。

- ASA CLI の show dhcprelay state
- ルータ CLI の show ip dhcp server statistics

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

```
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
```

次の debug コマンドも使用できます。

- debug dhcprelay packet
- debug dhcprelay event
- キャプチャ（Captures）
- Syslog

注：debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

関連情報

- ASA のキャプチャ
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。