

配置自適應安全裝置(ASA)DHCP中繼

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[封包流量](#)

[在ASA內部和外部介面上使用資料包捕獲功能的DHCP中繼](#)

[DHCP中繼事務的調試和系統日誌](#)

[設定](#)

[網路圖表](#)

[組態](#)

[使用CLI進行DHCP中繼配置](#)

[DHCP中繼最終配置](#)

[DHCP伺服器配置](#)

[使用多個DHCP伺服器的DHCP中繼](#)

[使用多個DHCP伺服器進行調試](#)

[使用多個DHCP伺服器捕獲](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔通過資料包捕獲和調試的幫助介紹Cisco ASA上的DHCP中繼，並提供配置示例。

必要條件

動態主機配置協定(DHCP)中繼代理允許安全裝置將DHCP請求從客戶端轉發到連線到不同介面的路由器或其他DHCP伺服器。

以下限制僅適用於使用DHCP中繼代理：

- 如果還啟用了DHCP伺服器功能，則無法啟用中繼代理。
- 您必須直接連線到安全裝置，並且不能通過其他中繼代理或路由器傳送請求。
- 對於多情景模式，不能在多個情景使用的介面上啟用DHCP中繼或配置DHCP中繼伺服器。

DHCP中繼服務在透明防火牆模式下不可用。處於透明防火牆模式的安全裝置僅允許地址解析協定(ARP)流量通過。所有其他流量需要存取控制清單(ACL)。為了在透明模式下允許通過安全裝置進行DHCP請求和回覆，您必須配置兩個ACL：

- 一個ACL，它允許從內部介面到外部的DHCP請求。
- 一個ACL，它允許從伺服器向另一個方向進行應答。

需求

Cisco建議您瞭解ASA CLI和Cisco IOS® CLI的基本知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA 5500-x系列安全裝置版本9.x或更高版本
- Cisco 1800系列路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

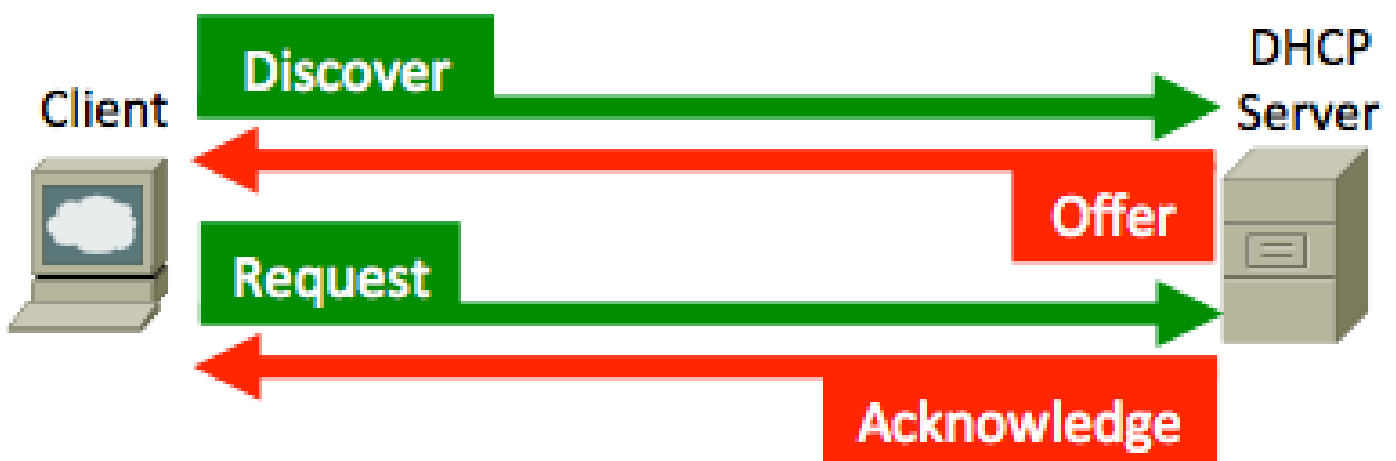
背景資訊

DHCP協定向主機提供自動配置引數，如帶有子網掩碼的IP地址、預設網關、DNS伺服器地址和Windows Internet名稱服務(WINS)地址。最初，DHCP客戶端沒有這些配置引數。為了獲取此資訊，它們會傳送廣播請求。當DHCP伺服器看到此請求時，DHCP伺服器會提供必需的資訊。由於這些廣播請求的性質，DHCP客戶端和伺服器必須位於同一子網中。預設情況下，第3層裝置（如路由器和防火牆）通常不會轉發這些廣播請求。

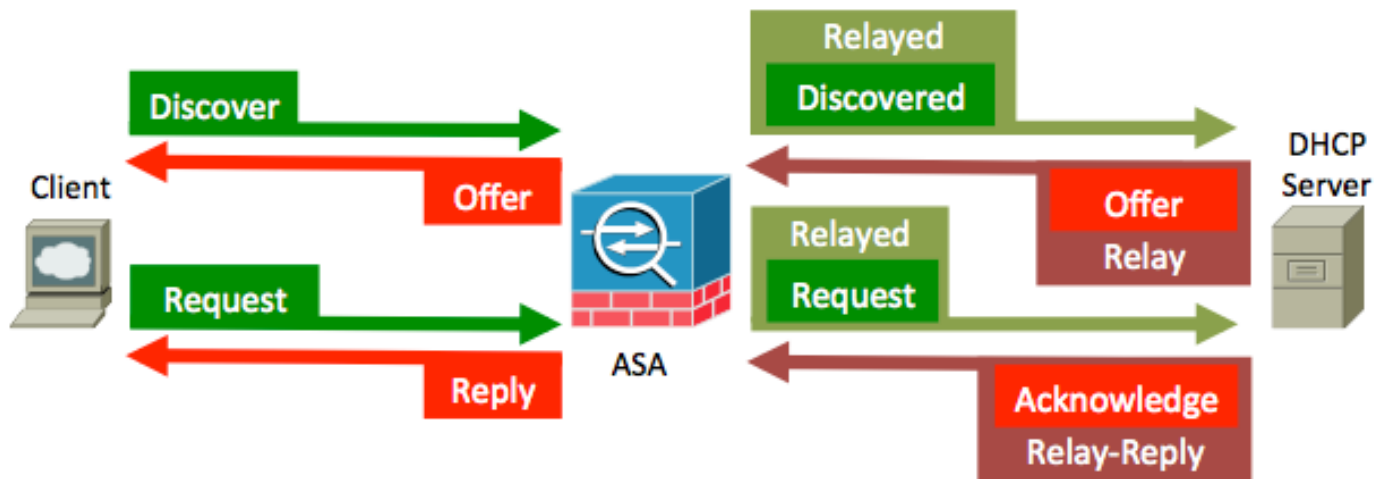
嘗試在同一子網中查詢DHCP客戶端和DHCP伺服器並不總是方便的。在這種情況下，您可以使用DHCP中繼。安全裝置上的DHCP中繼代理收到來自內部介面上的主機的主機DHCP請求時，會將該請求轉發到外部介面上的指定DHCP伺服器之一。當DHCP伺服器回覆客戶端時，安全裝置會將該回覆轉發回來。因此，DHCP中繼代理在與DHCP伺服器的會話中充當DHCP客戶端的代理。

封包流量

此圖說明未使用DHCP中繼代理時的DHCP資料包流：



ASA會攔截這些資料包並將其封裝為DHCP中繼格式：




在ASA內部和外部介面上使用資料包捕獲功能的DHCP中繼

記下以紅色突出顯示的內容，因為ASA就是這樣修改各個欄位的。


1. 要啟動DHCP進程，請啟動系統並向目標地址255.255.255.255 - UDP埠67傳送廣播消息 (DHCPDISCOVER)。

```
Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: Vmware_84:39:6a (00:50:56:84:39:6a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x79dbf3a7
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 0.0.0.0 (0.0.0.0)
  Client MAC address: Vmware_84:39:6a (00:50:56:84:39:6a)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (t=53,l=1) DHCP Message Type = DHCP Discover
  Option: (t=116,l=1) DHCP Auto-Configuration = AutoConfigure
  Option: (t=61,l=7) client identifier
  Option: (t=12,l=14) Host Name =
  Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  Option: (t=55,l=11) Parameter Request List
  End Option
  Padding
```

 註：如果VPN客戶端請求IP地址，則中繼代理IP地址是通過dhcp-network-scope命令在group-policy下定義的第一個可用IP地址。

- 通常，ASA會丟棄廣播，但由於它被配置為充當DHCP中繼，因此它會將DHCPDISCOVER消息作為單播資料包轉發到DHCP伺服器的IP源，該源來自面向伺服器的介面IP。在本例中，它是外部介面IP地址。請注意IP報頭和中繼代理欄位的變化：

```
Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: Cisco_6c:b8:c7 (58:8d:09:6c:b8:c7), Dst: Cisco_dd:48:c8 (00:19:e7:dd:48:c8)
Internet Protocol Version 4, Src: 198.51.100.1 (198.51.100.1), Dst: 198.51.100.2 (198.51.100.2)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootps (67)
Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x79dbf3a7
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 192.0.2.1 (192.0.2.1)
  Client MAC address: vmware_84:39:6a (00:50:56:84:39:6a)
  Client hardware address padding: 00000000000000000000
  server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (t=53,l=1) DHCP Message Type = DHCP Discover
  Option: (t=116,l=1) DHCP Auto-Configuration = AutoConfigure
  Option: (t=61,l=7) client identifier
  Option: (t=12,l=14) Host Name = 
  Option: (t=60,l=8) vendor class identifier = "MSFT 5.0"
  Option: (t=55,l=11) Parameter Request List
  End Option
  Padding
```

 註：由於Cisco錯誤ID [CSCuo89924](#)中引入的修復程式，版本9.1(5.7)、9.3(1)及更高版本的ASA可以將單播資料包轉發到DHCP伺服器的IP源，該源地址來自啟用了dnhcprelay的客戶端(giaddr)。在這種情況下，可以是內部介面IP地址。

- 伺服器將DHCP OFFER消息作為單播資料包發回ASA，目的地為在DHCPDISCOVER - UDP埠67中設定的中繼代理IP。在本例中，它是內部介面(giaddr)的IP地址，在該介面上啟用了dnhcprelay。請注意第3層報頭中的目標IP：

```

④ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
④ Ethernet II, Src: Cisco_dd:48:c8 (00:19:e7:dd:48:c8), Dst: Cisco_6c:b8:c7 (58:8d:09:6c:b8:c7)
④ Internet Protocol Version 4, Src: 198.51.100.2 (198.51.100.2), Dst: 192.0.2.1 (192.0.2.1)
④ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootps (67)
④ Bootstrap Protocol
    Src: DHCP server
    Dst: Relay agent IP
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x79dbf3a7
    Seconds elapsed: 0
④ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.0.2.4 (192.0.2.4) Offered IP
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 192.0.2.1 (192.0.2.1)
    Client MAC address: vmware_84:39:6a (00:50:56:84:39:6a)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
④ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
    DHCP offer
④ Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2
    DHCP server IP
④ Option: (t=51,l=4) IP Address Lease Time = 1 day
    Lease
④ Option: (t=58,l=4) Renewal Time Value = 12 hours
④ Option: (t=59,l=4) Rebinding Time Value = 21 hours
④ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
    Subnet mask info
④ Option: (t=6,l=8) Domain Name Server
④ Option: (t=15,l=9) Domain Name = "cisco.com"
    Domain name
    End option
    Padding

```

4. ASA將此資料包傳送到內部介面 — UDP埠68。請注意，當封包離開內部介面時，IP標頭會有所變更：


```

④ Frame 2: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits)
④ Ethernet II, Src: Cisco_6c:b8:c6 (58:8d:09:6c:b8:c6), Dst: Vmware_84:39:6a (00:50:56:84:39:6a)
④ Internet Protocol Version 4, Src: 192.0.2.1 (192.0.2.1), Dst: 192.0.2.4 (192.0.2.4)
④ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
④ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x79dbf3a7
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.0.2.4 (192.0.2.4)    Offered IP
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 192.0.2.1 (192.0.2.1)    ASA interface IP
    Client MAC address: vmware_84:39:6a (00:50:56:84:39:6a)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (t=53,l=1) DHCP Message Type = DHCP Offer    DHCP Offer
    Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2    DHCP server IP
    Option: (t=51,l=4) IP Address Lease Time = 1 day    Lease
    Option: (t=58,l=4) Renewal Time Value = 12 hours
    Option: (t=59,l=4) Rebinding Time Value = 21 hours
    Option: (t=1,l=4) Subnet Mask = 255.255.255.0    Subnet mask info
    Option: (t=6,l=8) Domain Name Server
    Option: (t=15,l=9) Domain Name = "cisco.com"    Domain name
    Option: (t=3,l=4) Router = 192.0.2.1    Default Gateway for client
    End option
    Padding
  
```

5. 收到DHCP OFFER消息後，傳送DHCP REQUEST消息以指示您接受該提議。

```

④ Frame 3: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits)
④ Ethernet II, Src: Vmware_84:39:6a (00:50:56:84:39:6a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
④ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
④ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
④ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x79dbf3a7
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: vmware_84:39:6a (00:50:56:84:39:6a)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (t=53,l=1) DHCP Message Type = DHCP Request    DHCP request
    Option: (t=61,l=7) Client identifier
    Option: (t=50,l=4) Requested IP Address = 192.0.2.4    Requested IP
    Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2    DHCP server IP
    Option: (t=12,l=14) Host Name = ████████████████████    Hostname
    Option: (t=81,l=18) Client Fully Qualified Domain Name
    Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
    Option: (t=55,l=11) Parameter Request List
    End option
  
```

6. ASA將DHCPREQUEST傳遞到DHCP伺服器。

```
Frame 3: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits)
Ethernet II, Src: Cisco_6c:b8:c7 (58:8d:09:6c:b8:c7), Dst: Cisco_dd:48:c8 (00:19:e7:dd:48:c8)
Internet Protocol Version 4, Src: 198.51.100.1 (198.51.100.1), Dst: 198.51.100.2 (198.51.100.2)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootps (67)
Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x79dbf3a7
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 192.0.2.1 (192.0.2.1)
  Client MAC address: Vmware_84:39:6a (00:50:56:84:39:6a)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (t=53,l=1) DHCP Message Type = DHCP Request
  Option: (t=61,l=7) Client identifier
  Option: (t=50,l=4) Requested IP Address = 192.0.2.4
  Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2
  Option: (t=12,l=14) Host Name = ████████████████████
  Option: (t=81,l=18) Client Fully Qualified Domain Name
  Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  Option: (t=55,l=11) Parameter Request List
  End option
```

Src: ASA outside interface
Dst: DHCP server

DHCP request
Requested IP
DHCP server IP
Hostname

7. 伺服器收到DHCPREQUEST後，會傳送DHCPACK以確認提供的IP。

```

④ Frame 4: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
④ Ethernet II, Src: Cisco_dd:48:c8 (00:19:e7:dd:48:c8), Dst: Cisco_6c:b8:c7 (58:8d:09:6c:b8:c7)
④ Internet Protocol Version 4, Src: 198.51.100.2 (198.51.100.2), Dst: 192.0.2.1 (192.0.2.1)
④ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootps (67) Src: DHCP server
④ Bootstrap Protocol Dst: Relay agent IP
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x79dbf3a7
    Seconds elapsed: 0
④ Bootp flags: 0x0000 (unicast)
    Client IP address: 0.0.0.0 (0.0.0.0) Current IP on client
    Your (client) IP address: 192.0.2.4 (192.0.2.4) IP offered to client
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 192.0.2.1 (192.0.2.1)
    Client MAC address: vmware_84:39:6a (00:50:56:84:39:6a)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
④ Option: (t=53,l=1) DHCP Message Type = DHCP ACK DHCP Ack
④ Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2 DHCP server IP
④ Option: (t=51,l=4) IP Address Lease Time = 1 day Lease
④ Option: (t=58,l=4) Renewal Time value = 12 hours
④ Option: (t=59,l=4) Rebinding Time Value = 21 hours
④ Option: (t=1,l=4) subnet Mask = 255.255.255.0 Subnet mask info
④ Option: (t=6,l=8) Domain Name Server Domain name
④ Option: (t=15,l=9) Domain Name = "cisco.com" Default gateway for client
    End option
    Padding

```

8. ASA將DHCPACK從DHCP伺服器傳送給您，從而完成事務。

```

④ Frame 4: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits)
④ Ethernet II, Src: Cisco_6c:b8:c6 (58:8d:09:6c:b8:c6), Dst: Vmware_84:39:6a (00:50:56:84:39:6a)
④ Internet Protocol Version 4, Src: 192.0.2.1 (192.0.2.1), Dst: 192.0.2.4 (192.0.2.4)
④ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) Src: Relay agent IP/ASA int
④ Bootstrap Protocol Dst: IP offered to client
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x79dbf3a7
    Seconds elapsed: 0
④ Bootp flags: 0x0000 (unicast)
    Client IP address: 0.0.0.0 (0.0.0.0) Current IP on client
    Your (client) IP address: 192.0.2.4 (192.0.2.4) IP offered to client
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 192.0.2.1 (192.0.2.1)
    Client MAC address: vmware_84:39:6a (00:50:56:84:39:6a)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
④ Option: (t=53,l=1) DHCP Message Type = DHCP ACK DHCP Ack
④ Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2 DHCP server IP
④ Option: (t=51,l=4) IP Address Lease Time = 1 day Lease
④ Option: (t=58,l=4) Renewal Time value = 12 hours
④ Option: (t=59,l=4) Rebinding Time Value = 21 hours
④ Option: (t=1,l=4) Subnet Mask = 255.255.255.0 Subnet mask info
④ Option: (t=6,l=8) Domain Name Server Domain name
④ Option: (t=15,l=9) Domain Name = "cisco.com" Default gateway for client
④ Option: (t=3,l=4) Router = 192.0.2.1
    End option
    Padding

```


DHCP中繼事務的調試和系統日誌

這是轉發到DHCP伺服器介面198.51.100.2的DHCP請求：

```
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
```

從DHCP伺服器收到回覆後，安全裝置會將其轉發到MAC地址為0050.5684.396a的DHCP客戶端，並將網關地址更改為自己的內部介面。

```
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.
```

系統日誌中也顯示相同的事務：

```
%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)

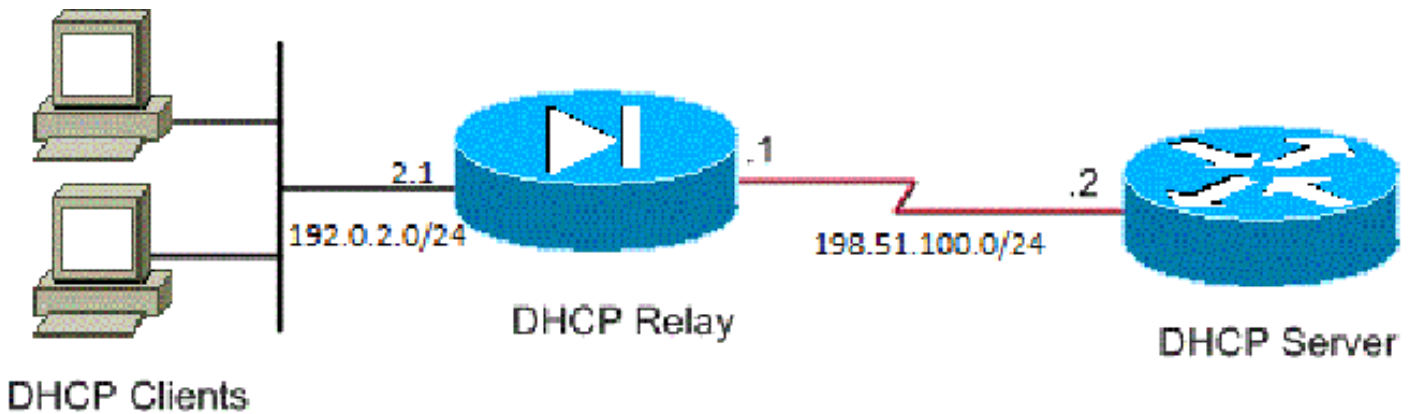
%ASA-7-609001: Built local-host inside:192.0.2.4
%ASA-6-302020: Built outbound ICMP connection for
  faddr 192.0.2.4/0 gaddr 198.51.100.2/1 laddr 198.51.100.2/1
%ASA-7-609001: Built local-host identity:192.0.2.1
%ASA-6-302015: Built inbound UDP connection 16 for outside:
  198.51.100.2/67 (198.51.100.2/67)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

本節提供用於設定本檔案中所述功能的資訊。

網路圖表

此文件使用以下網路設定：



組態

本檔案會使用以下設定：

- 使用CLI進行DHCP中繼配置
- DHCP中繼最終配置
- DHCP伺服器配置

使用CLI進行DHCP中繼配置

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

DHCP中繼最終配置

```
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伺服器配置

```
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 CISC01811W-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

```

使用多個DHCP伺服器的DHCP中繼

最多可以定義10個DHCP伺服器。當客戶端傳送DHCP Discover資料包時，該資料包將轉發到所有DHCP伺服器。

以下是範例：

```

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

```

使用多個DHCP伺服器進行調試

以下是使用多個DHCP伺服器時的一些調試示例：

```
DHCP: Received a BOOTREQUEST from interface 2 (size = 300)
DHCPR: relay binding found for client 000c.291c.34b5.
DHCPR: 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.
```

使用多個DHCP伺服器捕獲

以下是使用多個DHCP伺服器時的封包擷取範例：

```
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
```

驗證

使用本節內容，確認您的組態是否正常運作。

要檢視有關DHCP中繼服務的統計資訊，請在ASA CLI上輸入show dhcprelay statistics命令：

```
ASA# show dhcprelay statistics
```

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

```
Packets Relayed
```

```
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPRREQUEST         1
DHCPRDECLINE         0
DHCPRRELEASE        0
DHCPRINFORM          0

BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPRNAK             0
```

此輸出提供有關幾種DHCP消息型別的資訊，例如DHCPDISCOVER、DHCP REQUEST、DHCP OFFER、DHCP RELEASE和DHCP ACK。

- 顯示ASA CLI上的dhcprelay狀態
- show ip dhcp server statistics on router CLI

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

```
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
DHCPRREQUEST         1
DHCPCDECLINE         0
DHCPRELEASE          0
DHCPINFORM           0

Message               Sent
BOOTREPLY            0
DHCPPOFFER           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
```

您還可以使用以下debug指令：

- debug dhcprelay packet
- debug dhcprelay event
- 擷取
- 系統日誌



附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

相關資訊

- [在ASA上捕獲](#)

- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。