Configurazione dell'inoltro DHCP di Adaptive Security Appliance (ASA)

Sommario

Introduzione

In questo documento viene descritto il inoltro DHCP su Cisco ASA con l'aiuto di acquisizione e debug dei pacchetti e viene fornito un esempio di configurazione.

Prerequisiti

L'agente di inoltro DHCP (Dynamic Host Configuration Protocol) consente all'appliance di sicurezza di inoltrare le richieste DHCP dai client a un router o a un altro server DHCP connesso a un'interfaccia diversa.

Le restrizioni seguenti si applicano solo all'utilizzo dell'agente di inoltro DHCP:

- Impossibile abilitare l'agente di inoltro se è abilitata anche la funzionalità server DHCP.
- È necessario essere connessi direttamente all'appliance di sicurezza e non è possibile inviare richieste tramite un altro agente di inoltro o un router.

- Per la modalità a più contesti, non è possibile abilitare l'inoltro DHCP o configurare un server di inoltro DHCP su un'interfaccia utilizzata da più contesti.

I servizi di inoltro DHCP non sono disponibili in modalità firewall trasparente. Un'appliance di sicurezza in modalità firewall trasparente consente solo il passaggio del traffico ARP (Address Resolution Protocol). Per tutto il resto del traffico è necessario un Access Control List (ACL). Per consentire le richieste e le risposte DHCP tramite l'appliance di sicurezza in modalità trasparente, è necessario configurare due ACL:

- Un ACL che consente le richieste DHCP dall'interfaccia interna verso l'esterno.
- Un ACL che consente le risposte dal server nell'altra direzione.

Requisiti

Cisco consiglia di avere una conoscenza base di ASA CLI e Cisco IOS® CLI.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA serie 5500-x Security Appliance release 9.x o successive
- Cisco serie 1800 Router

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

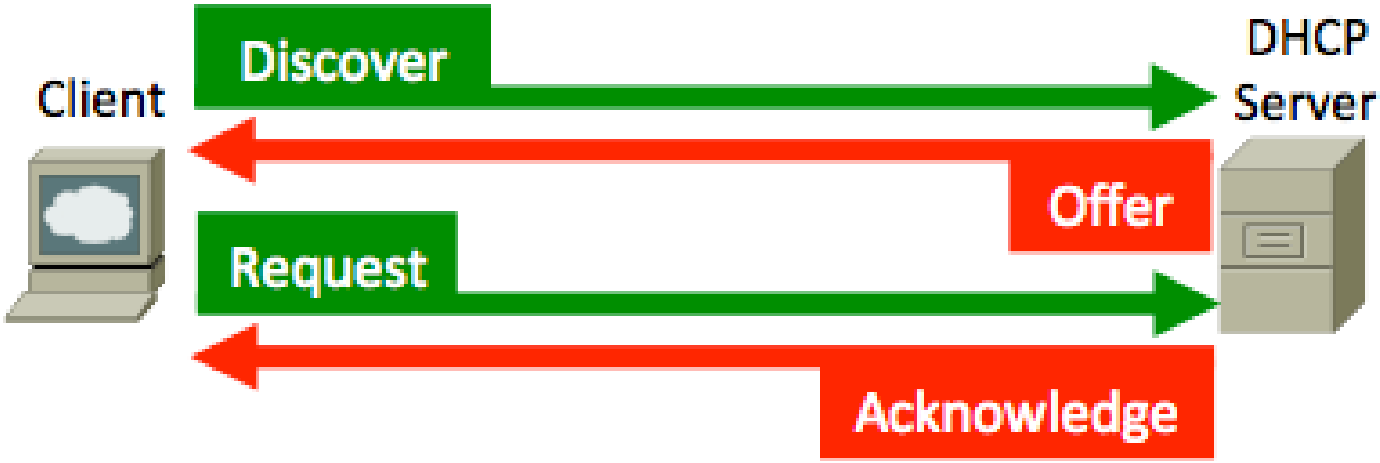
Premesse

Il protocollo DHCP fornisce agli host parametri di configurazione automatica, ad esempio un indirizzo IP con una subnet mask, un gateway predefinito, l'indirizzo del server DNS e l'indirizzo WINS (Windows Internet Name Service). Inizialmente, i client DHCP non hanno nessuno di questi parametri di configurazione. Per ottenere queste informazioni, inviano una richiesta di trasmissione. Quando un server DHCP riceve questa richiesta, fornisce le informazioni necessarie. A causa della natura di queste richieste di trasmissione, il client e il server DHCP devono trovarsi nella stessa subnet. I dispositivi di layer 3, quali router e firewall, in genere non inoltrano queste richieste di trasmissione per impostazione predefinita.

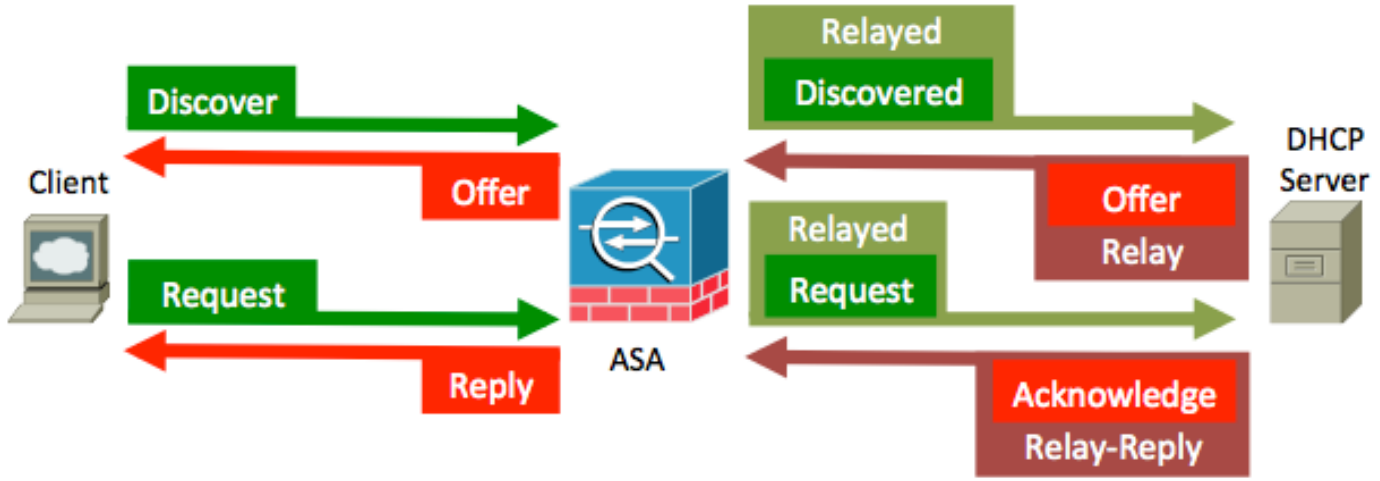
Un tentativo di individuare i client DHCP e un server DHCP nella stessa subnet non è sempre conveniente. In questa situazione, è possibile utilizzare l'inoltro DHCP. Quando l'agente di inoltro DHCP sull'appliance di sicurezza riceve una richiesta DHCP da un host su un'interfaccia interna, inoltra la richiesta a uno dei server DHCP specificati su un'interfaccia esterna. Quando il server DHCP risponde al client, l'appliance di sicurezza inoltra la risposta. Pertanto, l'agente di inoltro DHCP funge da proxy per il client DHCP nella conversazione con il server DHCP.

Flusso dei pacchetti

Nell'immagine viene mostrato il flusso del pacchetto DHCP quando non si usa un agente di inoltro DHCP:



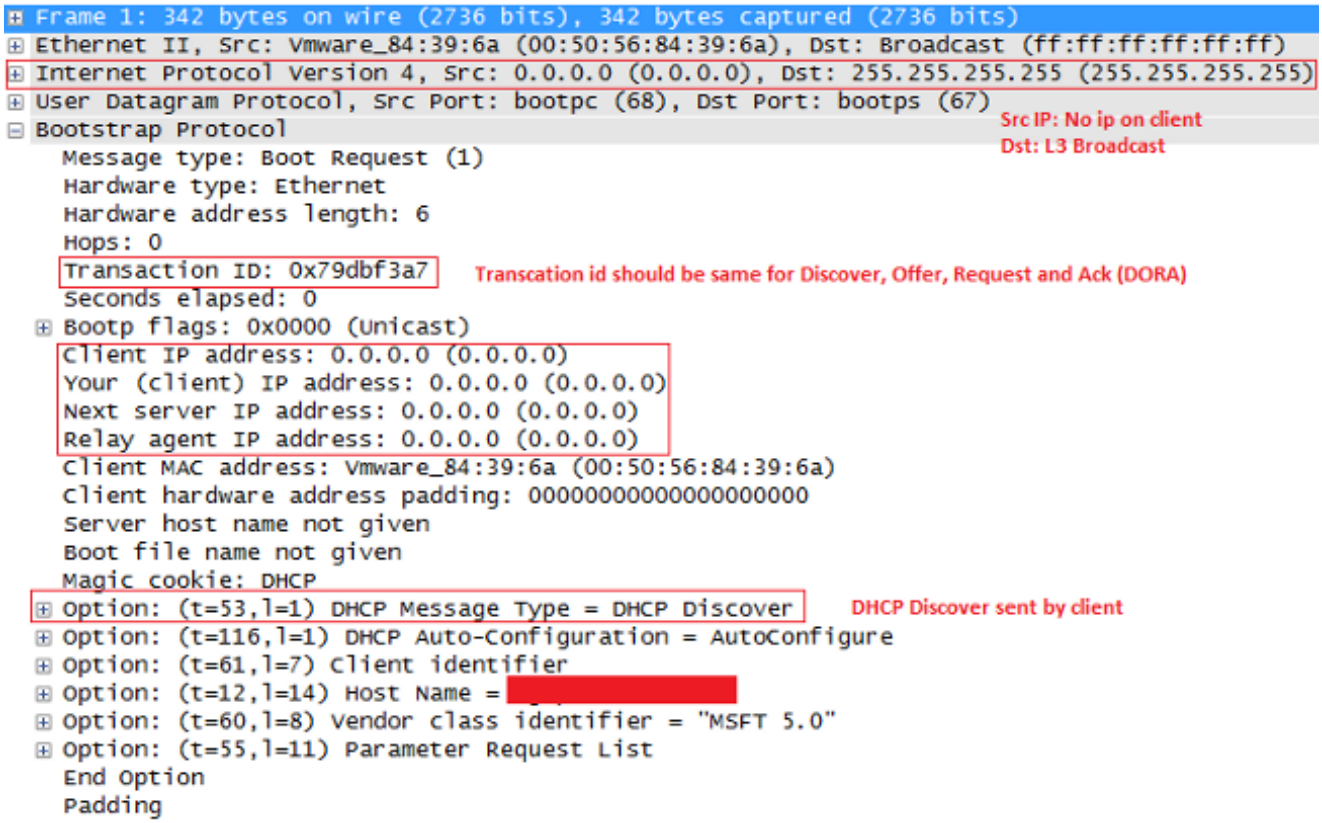
L'ASA intercetta questi pacchetti e li incapsula nel formato di inoltro DHCP:



Inoltro DHCP con acquisizioni di pacchetti sull'interfaccia ASA interna ed esterna

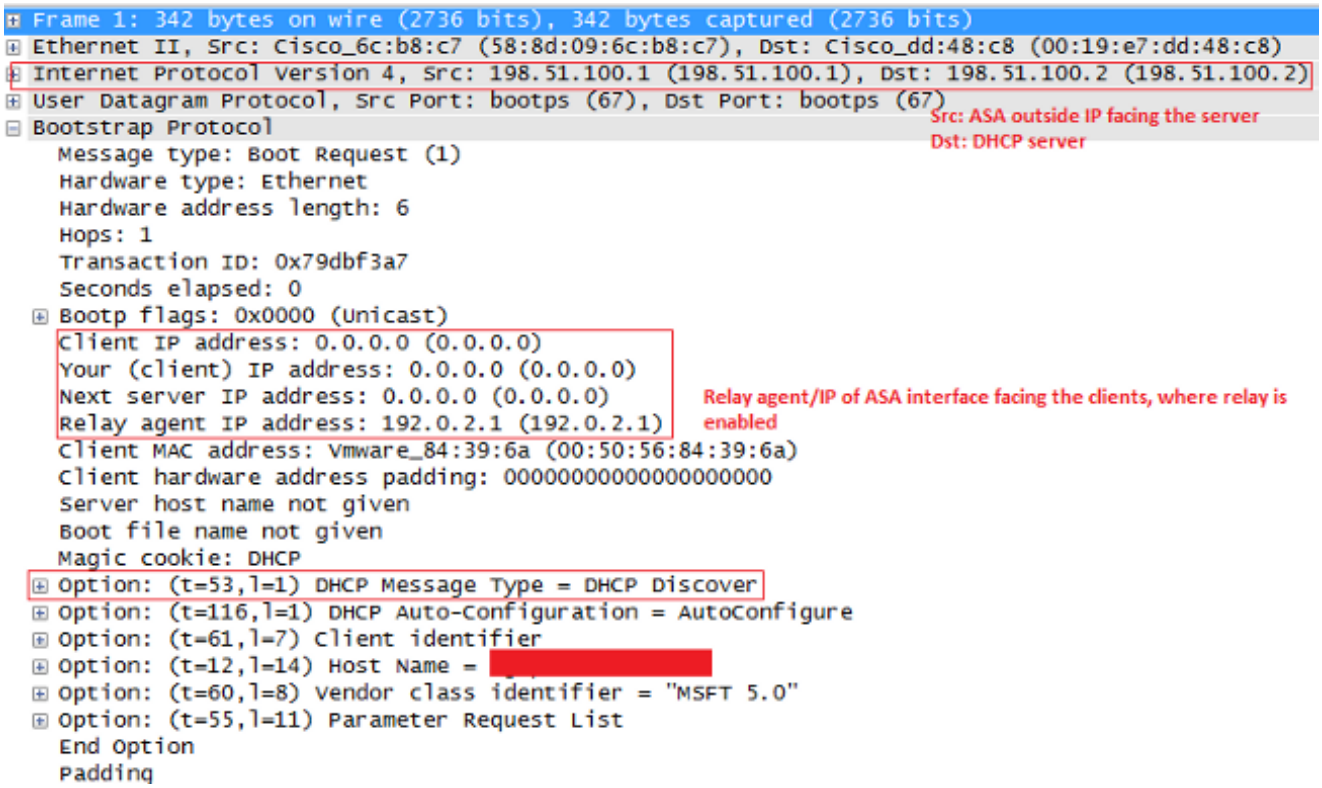
Prendere nota del contenuto evidenziato in ROSSO, perché è così che l'appliance ASA modifica i vari campi.

1. Per avviare il processo DHCP, avviare il sistema e inviare un messaggio broadcast (DHCP DISCOVER) all'indirizzo di destinazione 255.255.255.255 - porta UDP 67.



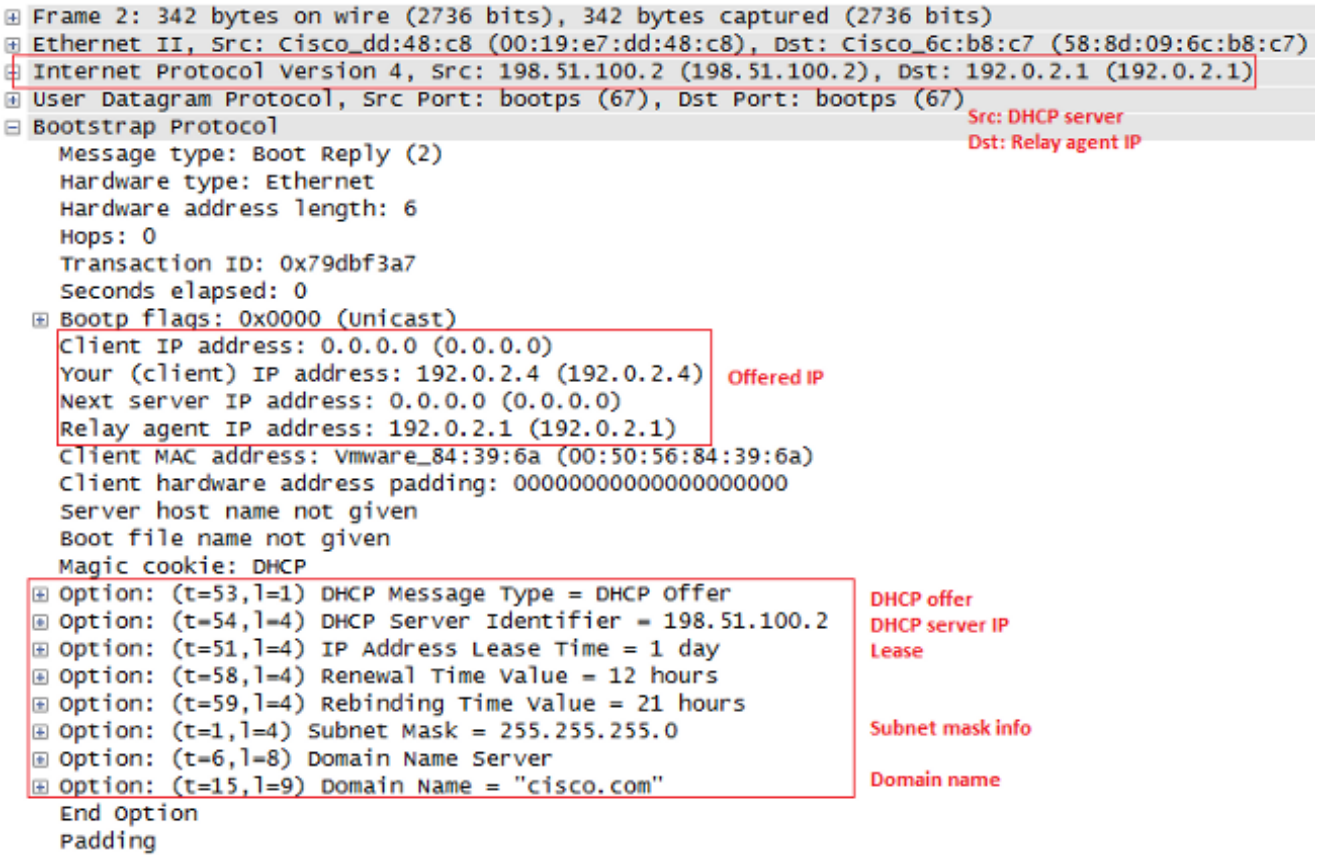
Nota: se un client VPN richiede un indirizzo IP, l'indirizzo IP dell'agente di inoltro è il primo indirizzo IP utilizzabile definito dal comando dhcp-network-scope nell'ambito dei criteri di gruppo.

2. Normalmente, l'ASA rifiuta la trasmissione, ma poiché è configurata per funzionare come inoltro DHCP, inoltra il messaggio DHCPDISCOVER come pacchetto unicast all'IP del server DHCP che proviene dall'IP dell'interfaccia rivolta al server. In questo caso, è l'indirizzo IP dell'interfaccia esterna. Si noti la modifica nel campo dell'intestazione IP e dell'agente di inoltro:

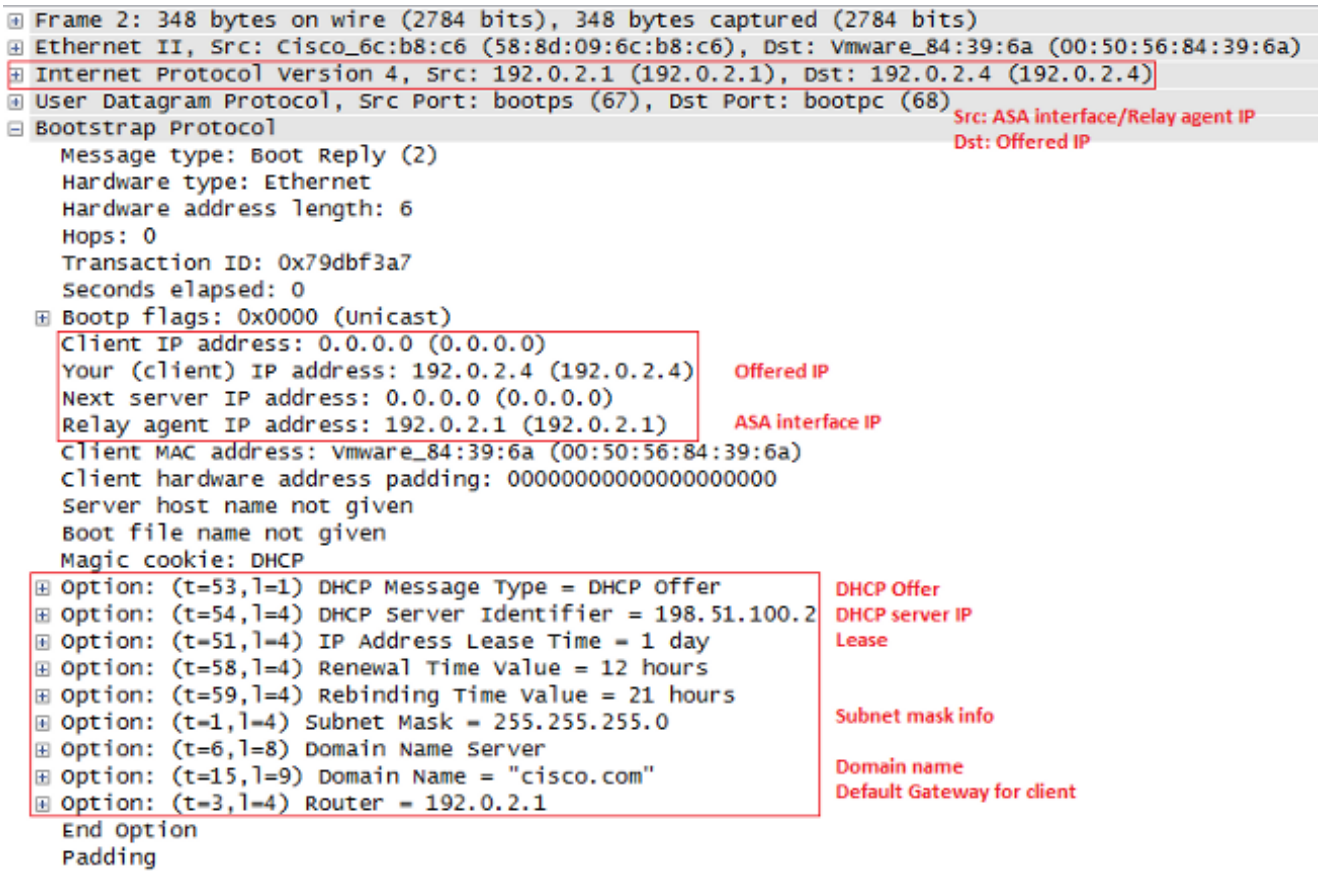


> Nota: a causa della correzione incorporata nell'ID bug Cisco CSCuo89924, l'appliance ASA nelle versioni 9.1(5.7), 9.3(1) e successive può inoltrare i pacchetti unicast all'origine IP del server DHCP dall'indirizzo IP dell'interfaccia rivolta al client (giaddr) su cui è abilitato dhcprelay. In questo caso, può essere l'indirizzo IP dell'interfaccia interna.

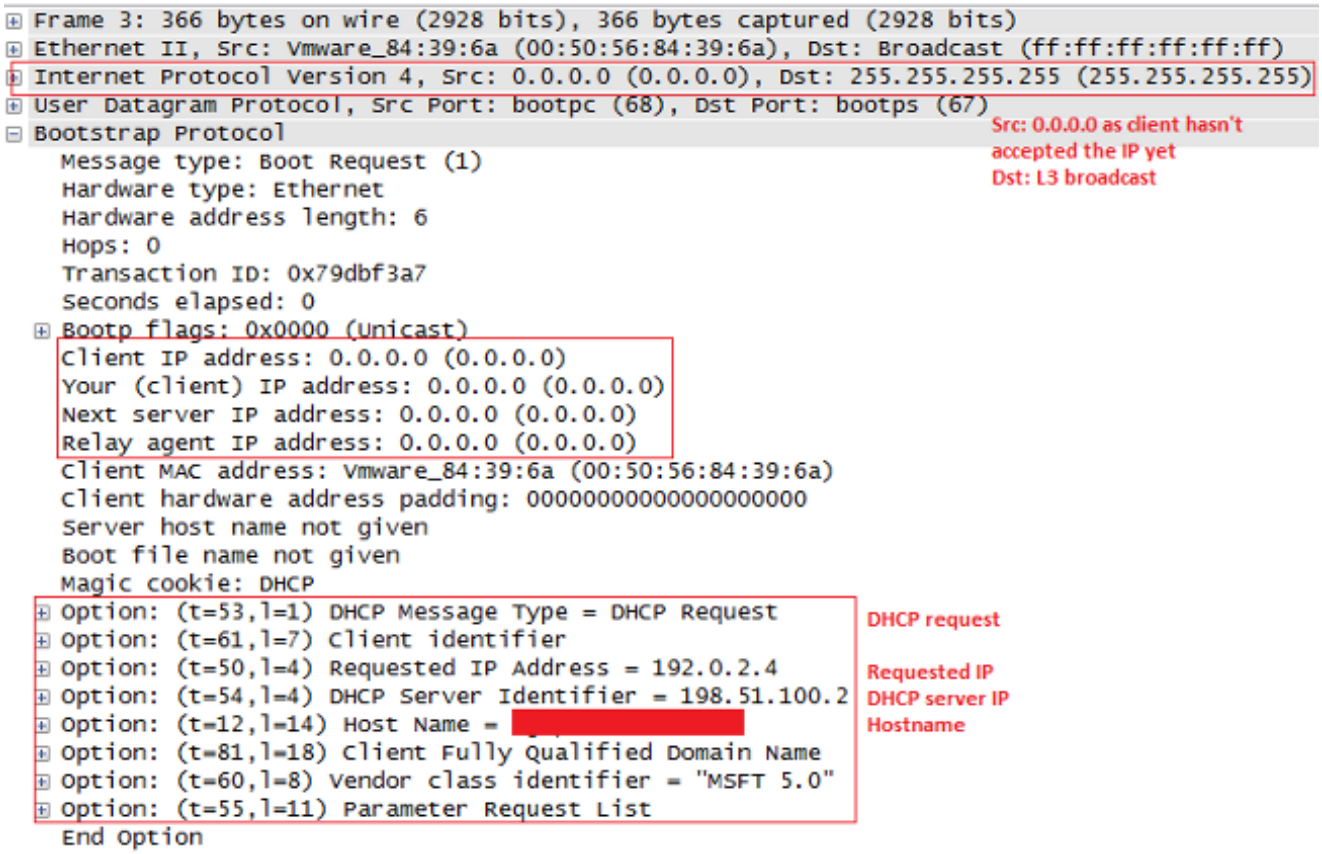
3. Il server invia un messaggio DHCP come pacchetto unicast all'ASA, destinato all'indirizzo IP dell'agente di inoltro configurato nella porta DHCP DISCOVER- UDP 67. In questo caso, si tratta dell'indirizzo IP dell'interfaccia interna (giaddr), dove dhcprelay è abilitato. Notare l'indirizzo IP di destinazione nell'intestazione di layer 3:



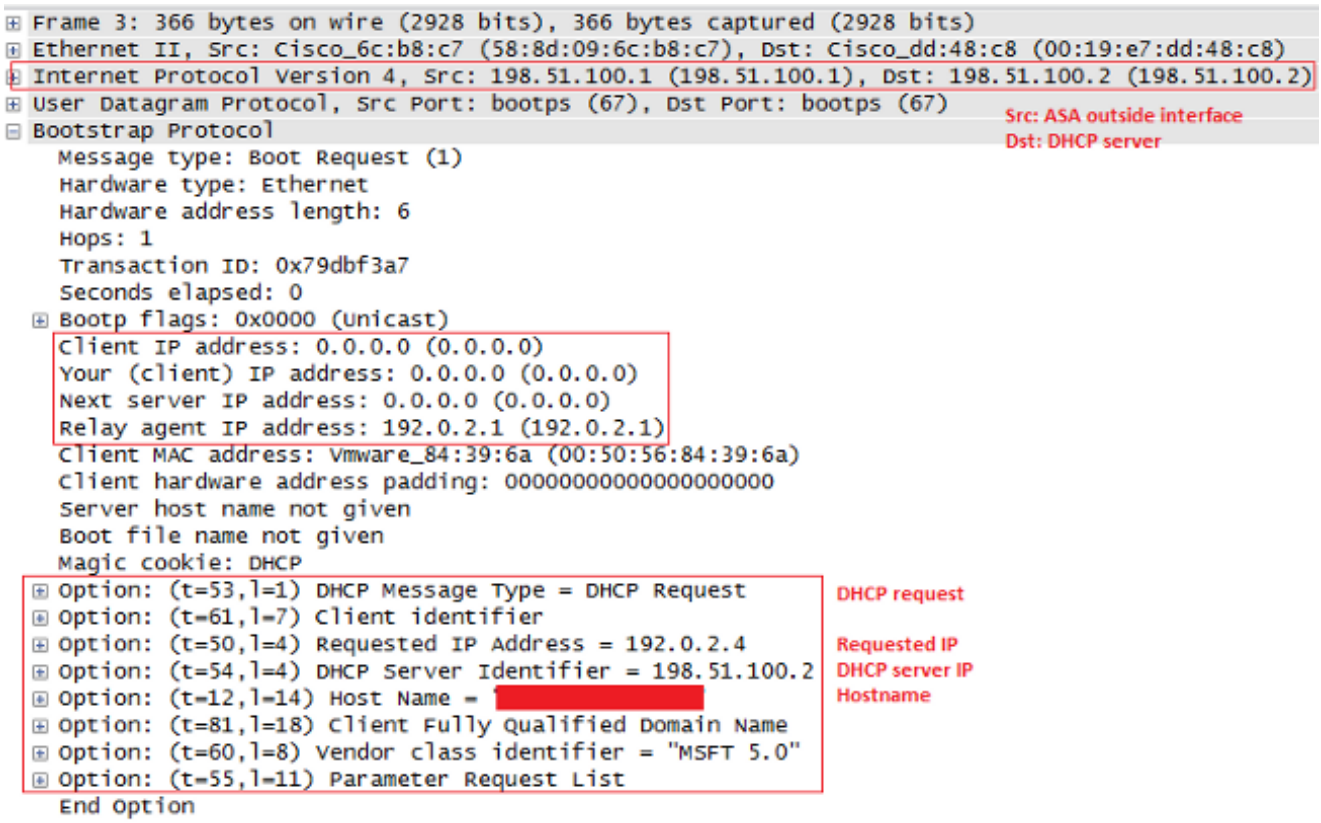
4. L'ASA invia questo pacchetto dall'interfaccia interna - porta UDP 68. Notare la modifica nell'intestazione IP mentre il pacchetto esce dall'interfaccia interna:



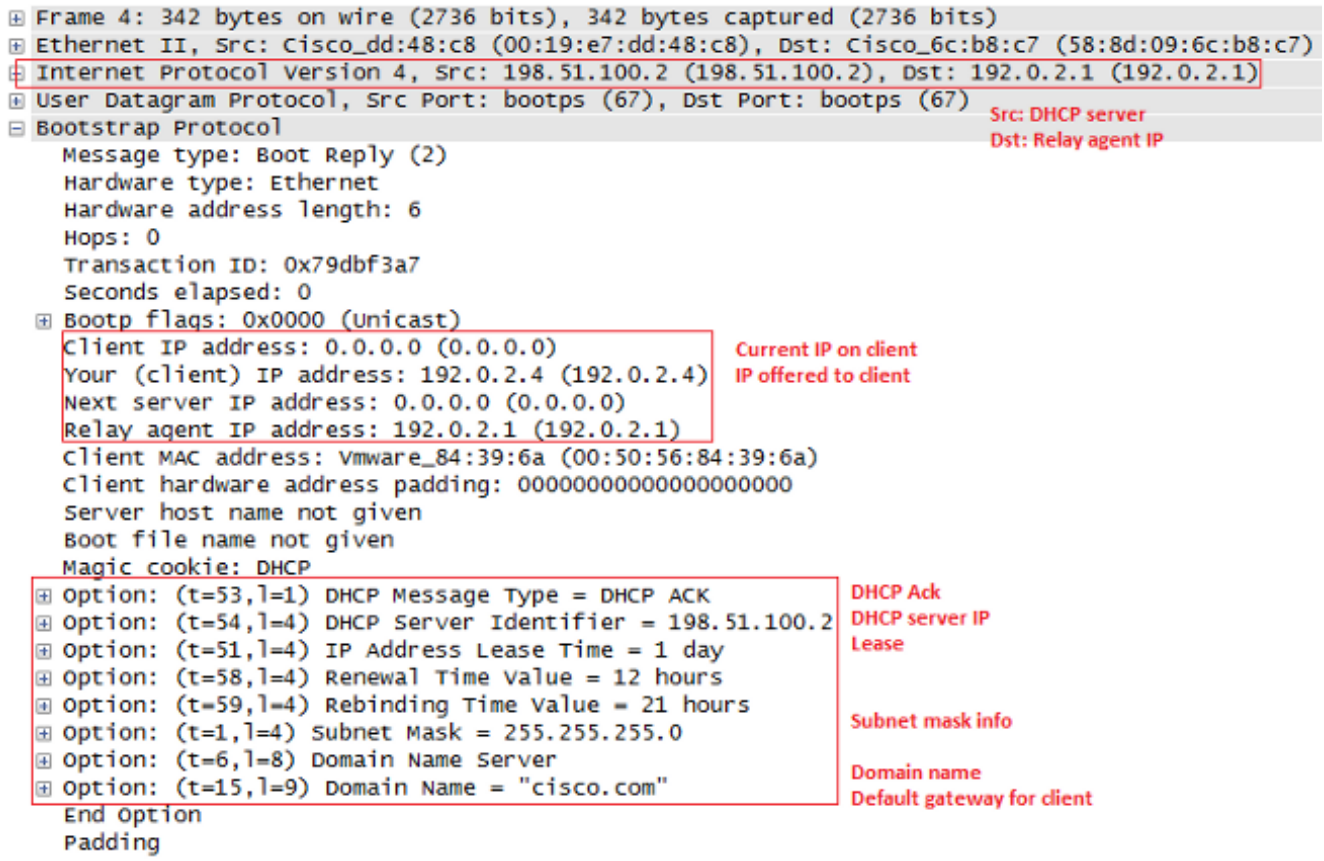
5. Dopo aver ricevuto il messaggio DHCPOFFER, inviare un messaggio DHCPREQUEST per indicare che si accetta l'offerta.



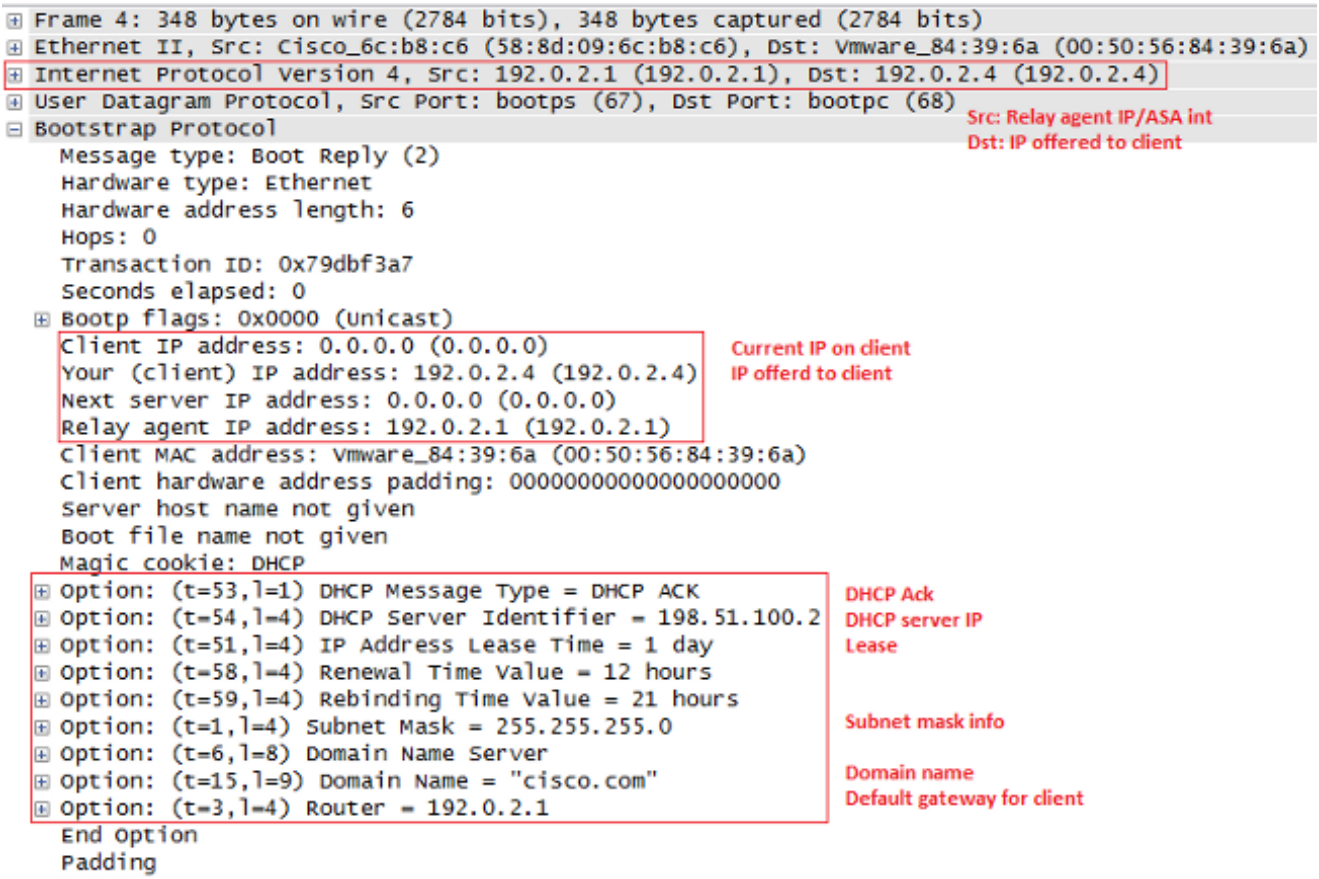
6. L'appliance ASA passa la richiesta DHCP al server DHCP.



7. Una volta che il server ha ottenuto DHCPREQUEST, invia nuovamente il DHCPACK per confermare l'IP offerto.



8. L'appliance ASA trasmette il pacchetto DHCP dal server DHCP all'utente che ha completato la transazione.



Debug e syslog per le transazioni di inoltro DHCP

Questa è una richiesta DHCP inoltrata all'interfaccia del server 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
```

Dopo aver ricevuto la risposta dal server DHCP, l'appliance di sicurezza la inoltra al client DHCP con indirizzo MAC 0050.5684.396a e modifica l'indirizzo del gateway nella relativa interfaccia interna.

```
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 stessa transazione viene visualizzata anche nei syslog:

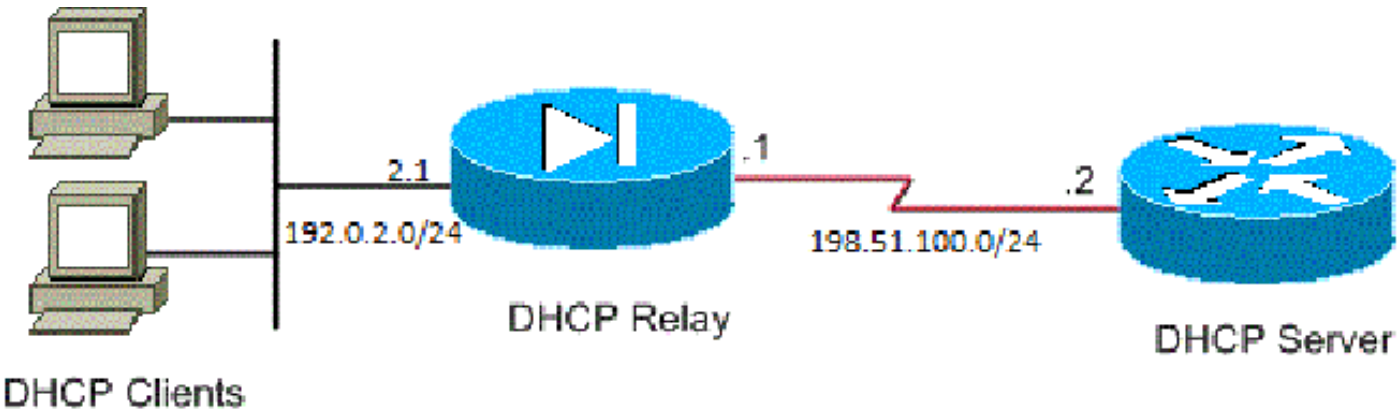
```
%ASA-7-609001: Built local-host inside:0.0.0.0
%ASA-7-609001: Built local-host identity:255.255.255.255
%ASA-6-302015: Built inbound UDP connection 13 for inside:
 0.0.0.0/68 (0.0.0.0/68) to identity:255.255.255.255/67 (255.255.255.255/67)
%ASA-7-609001: Built local-host identity:198.51.100.1
%ASA-7-609001: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

Configurazione

In questa sezione vengono presentate le informazioni utilizzate per configurare le funzionalità descritte più avanti nel documento.

Esempio di rete

Il documento usa la seguente configurazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- Configurazione dell'inoltro DHCP con uso della CLI
- Configurazione finale inoltro DHCP
- Configurazione server DHCP

Configurazione dell'inoltro DHCP con uso della CLI

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

Configurazione finale inoltro 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
```

Configurazione server 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
```

Inoltro DHCP con più server DHCP

È possibile definire fino a dieci server DHCP. Quando un client invia un pacchetto DHCP Discover, lo inoltra a tutti i server DHCP.

Di seguito è riportato un esempio:

```
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
```

Debug con più server DHCP

Di seguito sono riportati alcuni esempi di debug quando si utilizzano più server DHCP:

```
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.
```

Acquisizione con più server DHCP

Di seguito è riportato un esempio di acquisizione di pacchetti quando si utilizzano più server DHCP:

```
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
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Per visualizzare le informazioni statistiche sui servizi di inoltro DHCP, immettere il comando show dhcprelay statistics sulla CLI di 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
```

Questo output fornisce informazioni su diversi tipi di messaggi DHCP, ad esempio DHCP DISCOVER, DHCP REQUEST, DHCP OFER, DHCP RELEASE e DHCP ACK.

- show dhcprelay state sulla CLI di ASA
- show ip dhcp server statistics on router CLI

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

```
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
```

È inoltre possibile utilizzare i seguenti comandi di debug:

- debug dhcprelay packet
- debug dhcprelay, evento
- Clip
- Syslog

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di debug.

Informazioni correlate

- Acquisizioni sull'appliance ASA
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).