Configure Adaptive Security Appliance (ASA) DHCP Relay

Contents

Introduction

This document describes DHCP relay on Cisco ASA with the help of packet captures and debugs, and provides a configuration example.

Prerequisites

A Dynamic Host Configuration Protocol (DHCP) relay agent allows the security appliance to forward DHCP requests from clients to a router or other DHCP server connected to a different interface.

These restrictions apply only to the use of the DHCP relay agent:

- The relay agent cannot be enabled if the DHCP server feature is also enabled.
- You must be directly connected to the security appliance and cannot send requests through another relay agent or a router.
- For multiple context mode, you cannot enable DHCP relay, or configure a DHCP relay server, on an interface that is used by more than one context.

DHCP relay services are not available in transparent firewall mode. A security appliance in transparent firewall mode only allows Address Resolution Protocol (ARP) traffic through. All other traffic requires an Access Control List (ACL). In order to allow DHCP requests and replies through the security appliance in transparent mode, you must configure two ACLs:

- One ACL that allows DHCP requests from the inside interface to the outside.

- One ACL that allows the replies from the server in the other direction.

Requirements

Cisco recommends that you have a basic knowledge of ASA CLI and Cisco IOS® CLI.

Components Used

The information in this document is based on these software and hardware versions:

- ASA 5500-x Series Security Appliance Release 9.x or later
- Cisco 1800 Series Routers

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. If your network is live, ensure that you understand the potential impact of any command.

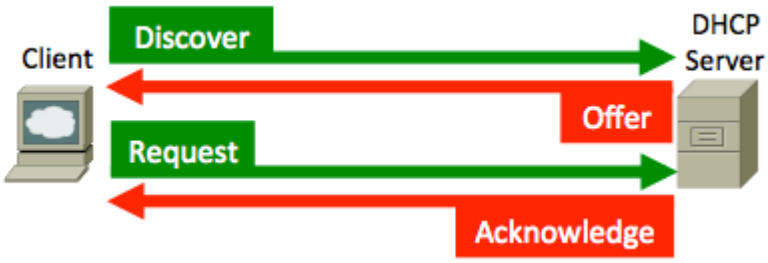
Background Information

The DHCP protocol supplies automatic configuration parameters, such as an IP address with a subnet mask, default gateway, DNS server address, and Windows Internet Name Service (WINS) address to hosts. Initially, DHCP clients have none of these configuration parameters. In order to obtain this information, they send a broadcast request for it. When a DHCP server sees this request, the DHCP server supplies the necessary information. Due to the nature of these broadcast requests, the DHCP client and server must be on the same subnet. Layer 3 devices such as routers and firewalls do not typically forward these broadcast requests by default.

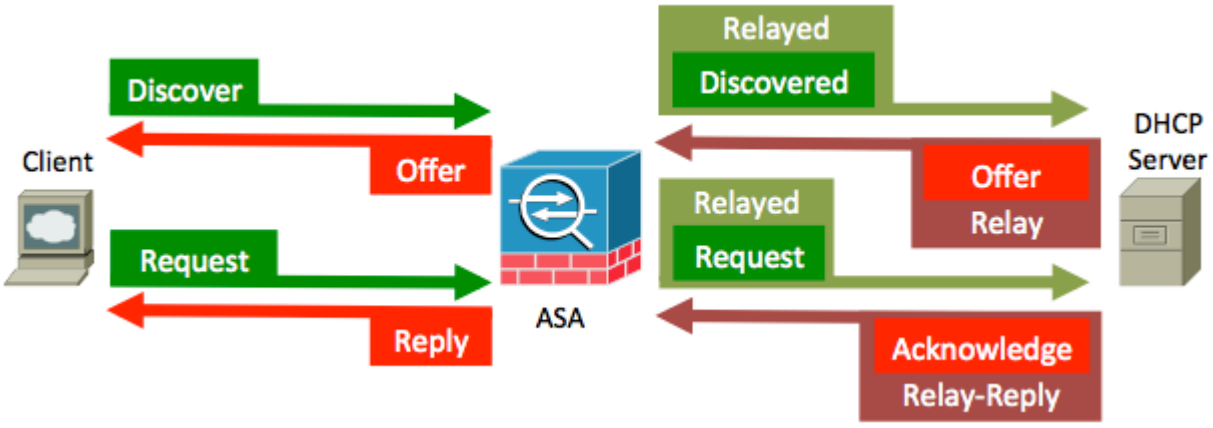
An attempt to locate DHCP clients and a DHCP server on the same subnet is not always convenient. In such a situation, you can use DHCP relay. When the DHCP relay agent on the security appliance receives a DHCP request from a host on an inside interface, it forwards the request to one of the specified DHCP servers on an outside interface. When the DHCP server replies to the client, the security appliance forwards that reply back. Thus, the DHCP relay agent acts as a proxy for the DHCP client in its conversation with the DHCP server.

Packet Flow

This image illustrates the DHCP packet flow when a DHCP relay agent is not used:



The ASA intercepts these packets and wraps them into DHCP relay format:



DHCP Relay with Packet Captures on the ASA Inside and Outside Interface

Make a note of content highligted in RED, because that is how the ASA modifies various fields.

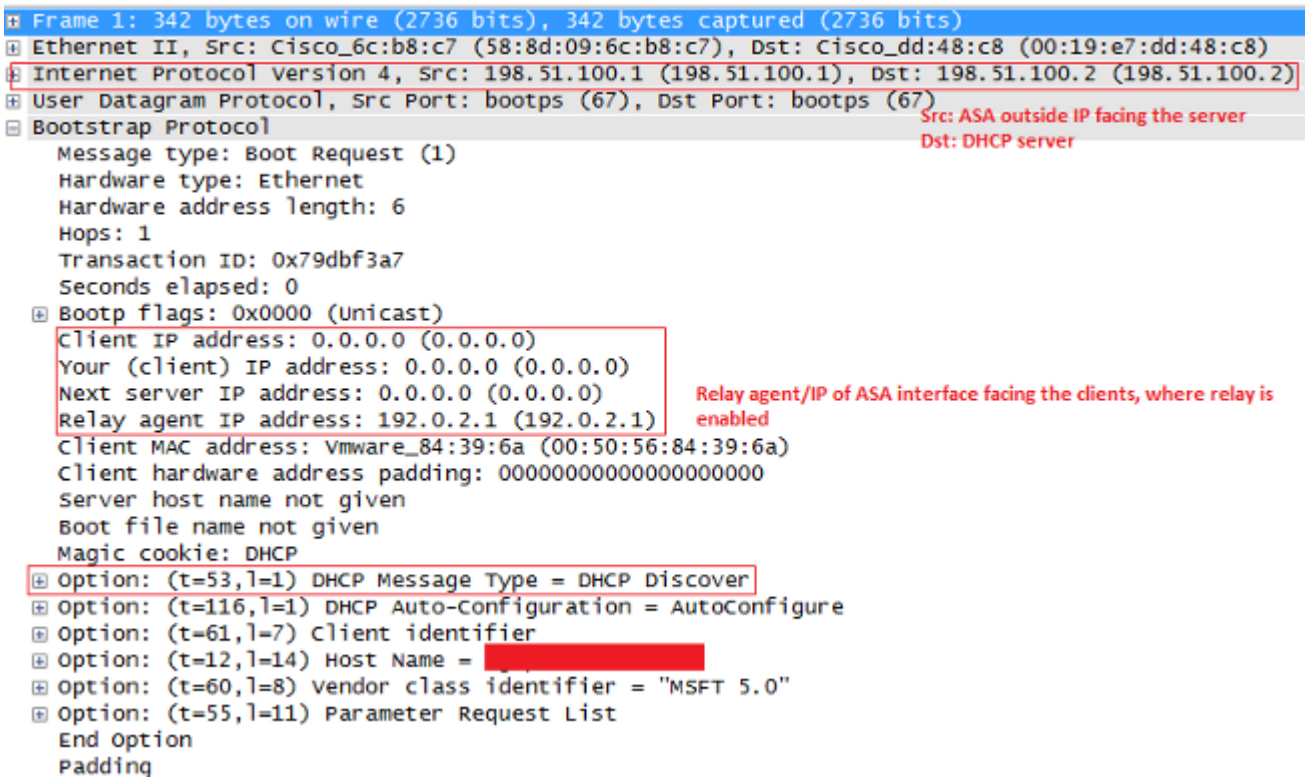
1. In order to start the DHCP process, boot the system and send a broadcast message (DHCPDISCOVER) to the destination address 255.255.255.255 - UDP port 67.

```
⊞ 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                                   Src IP: No ip on client
                                                       Dst: L3 Broadcast
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x79dbf3a7     Transcation id should be same for Discover, Offer, Request and Ack (DORA)
    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     DHCP Discover sent by client
  ⊞ Option: (t=116,l=1) DHCP Auto-Configuration = AutoConfigure
  ⊞ Option: (t=61,l=7) Client identifier
  ⊞ Option: (t=12,l=14) Host Name = [redacted]
  ⊞ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  ⊞ Option: (t=55,l=11) Parameter Request List
    End Option
    Padding
```

> **Note**: If a VPN client requests an IP address, the relay-agent IP address is the first usable IP address that is defined by the dhcp-network-scope command, under the group-policy.

2. Normally, ASA would drop the broadcast, but because it is configured to act as a DHCP relay, it

forwards the DHCPDISCOVER message as a unicast packet to the DHCP server's IP sourcing from the interface IP that faces the server. In this case, it is the outside interface IP address. Notice the change in the IP header and relay agent field:



Note: Due to the fix incorporated in Cisco bug ID CSCuo89924, ASA in Versions 9.1(5.7), 9.3(1), and later can forward the unicast packets to the DHCP server's IP sourcing from the interface IP address that faces the client (giaddr) where the dhcprelay is enabled. In this case, it can be the inside interface IP address.

---

3. The server sends back a DHCPOFFER message as a unicast packet to the ASA, destined to the relay agent IP set up in DHCPDISCOVER- UDP port 67. In this case, it is the IP address of the inside interface (giaddr), where dhcprelay is enabled. Notice the destination IP in the layer 3 header:

```
⊞ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊞ Ethernet II, Src: Cisco_dd:48:c8 (00:19:e7:dd:48:c8), Dst: Cisco_6c:b8:c7 (58:8d:09:6c:b8:c7)
⊞ Internet Protocol Version 4, Src: 198.51.100.2 (198.51.100.2), Dst: 192.0.2.1 (192.0.2.1)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootps (67)
⊟ 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)
    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 Offer
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 1 day
  ⊞ 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
  ⊞ Option: (t=6,l=8) Domain Name Server
  ⊞ Option: (t=15,l=9) Domain Name = "cisco.com"
    End Option
    Padding
```

Src: DHCP server
Dst: Relay agent IP

Offered IP

DHCP offer
DHCP server IP
Lease

Subnet mask info

Domain name

4. ASA sends this packet out of the inside interface - UDP port 68. Notice the change in the IP header while the packet leaves the inside interface:

```
⊞ Frame 2: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits)
⊞ Ethernet II, Src: Cisco_6c:b8:c6 (58:8d:09:6c:b8:c6), Dst: Vmware_84:39:6a (00:50:56:84:39:6a)
⊞ Internet Protocol Version 4, Src: 192.0.2.1 (192.0.2.1), Dst: 192.0.2.4 (192.0.2.4)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ 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)
    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 Offer
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 1 day
  ⊞ 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
  ⊞ Option: (t=6,l=8) Domain Name Server
  ⊞ Option: (t=15,l=9) Domain Name = "cisco.com"
  ⊞ Option: (t=3,l=4) Router = 192.0.2.1
    End Option
    Padding
```

Src: ASA interface/Relay agent IP
Dst: Offered IP

Offered IP

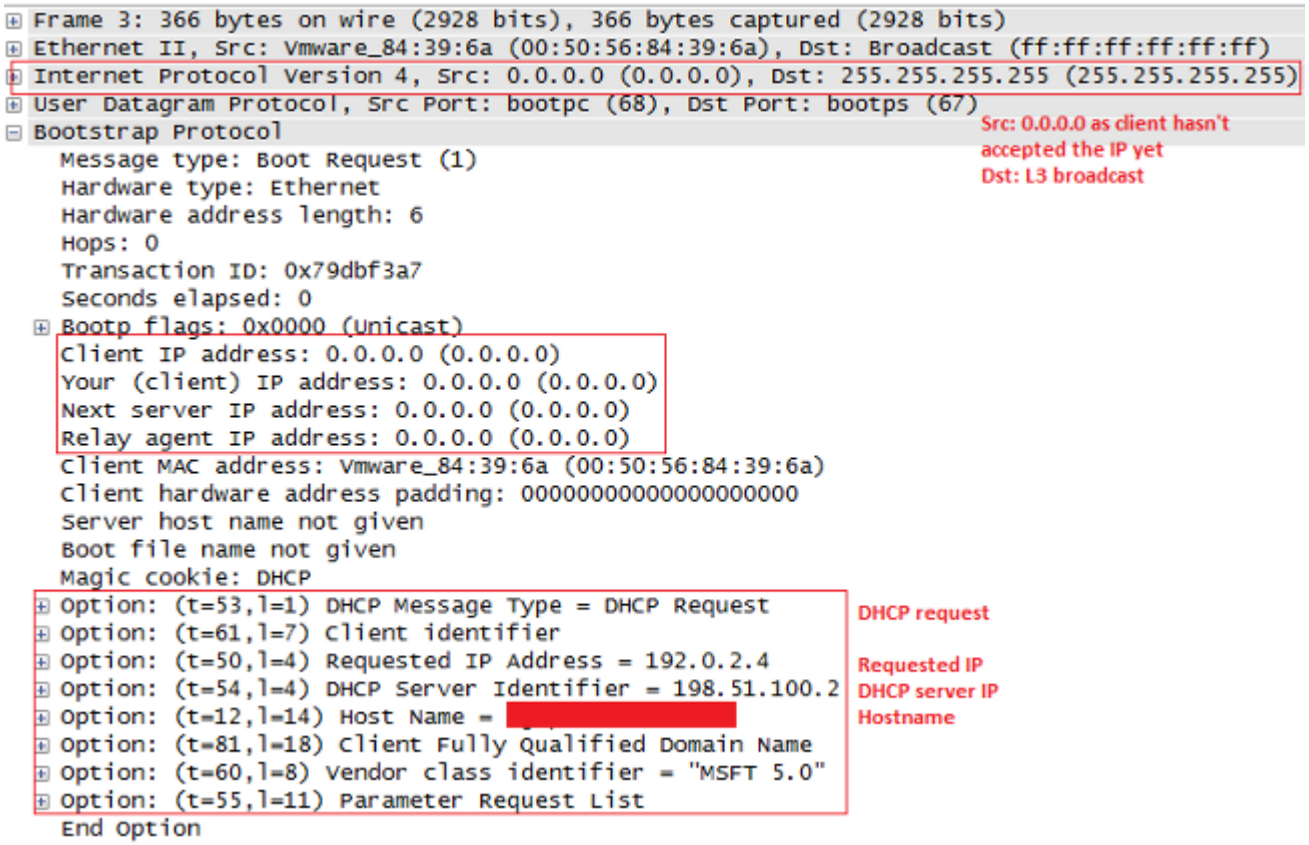
ASA interface IP

DHCP Offer
DHCP server IP
Lease

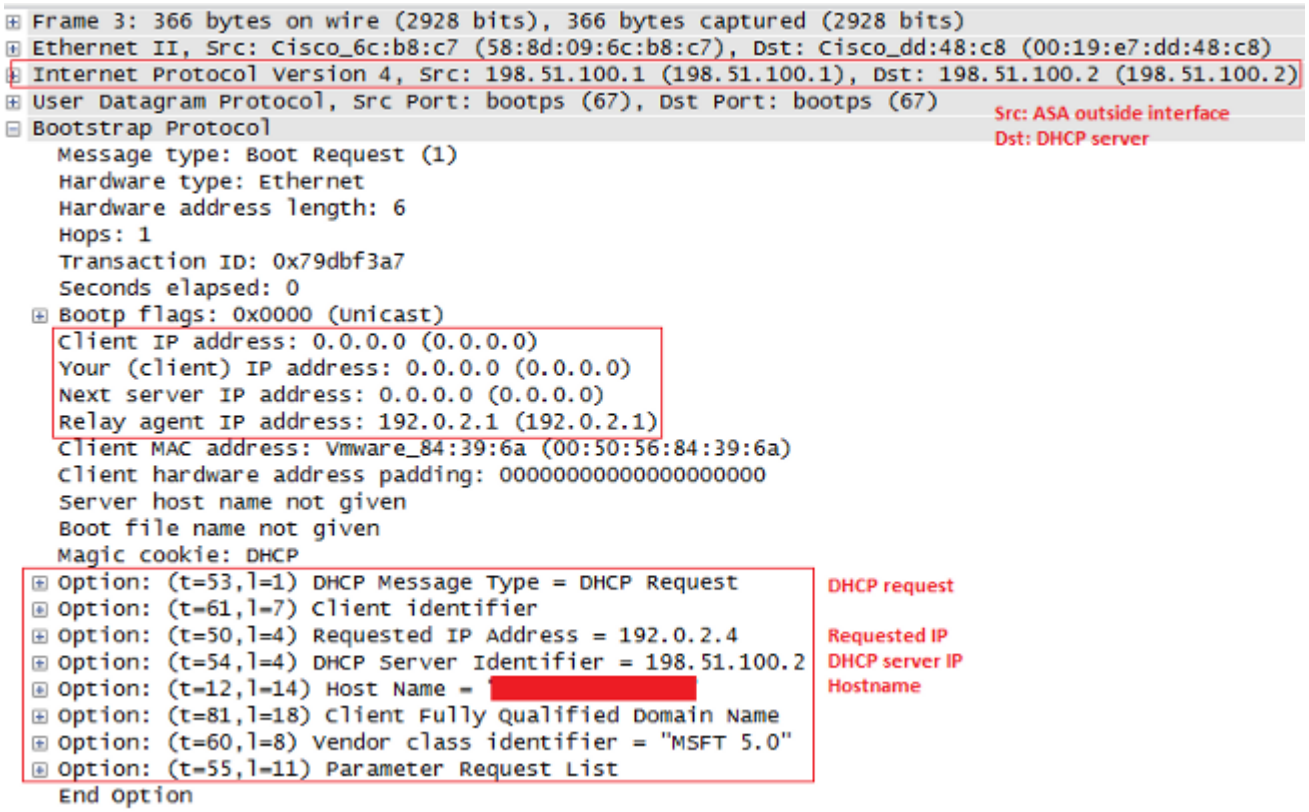
Subnet mask info

Domain name
Default Gateway for client

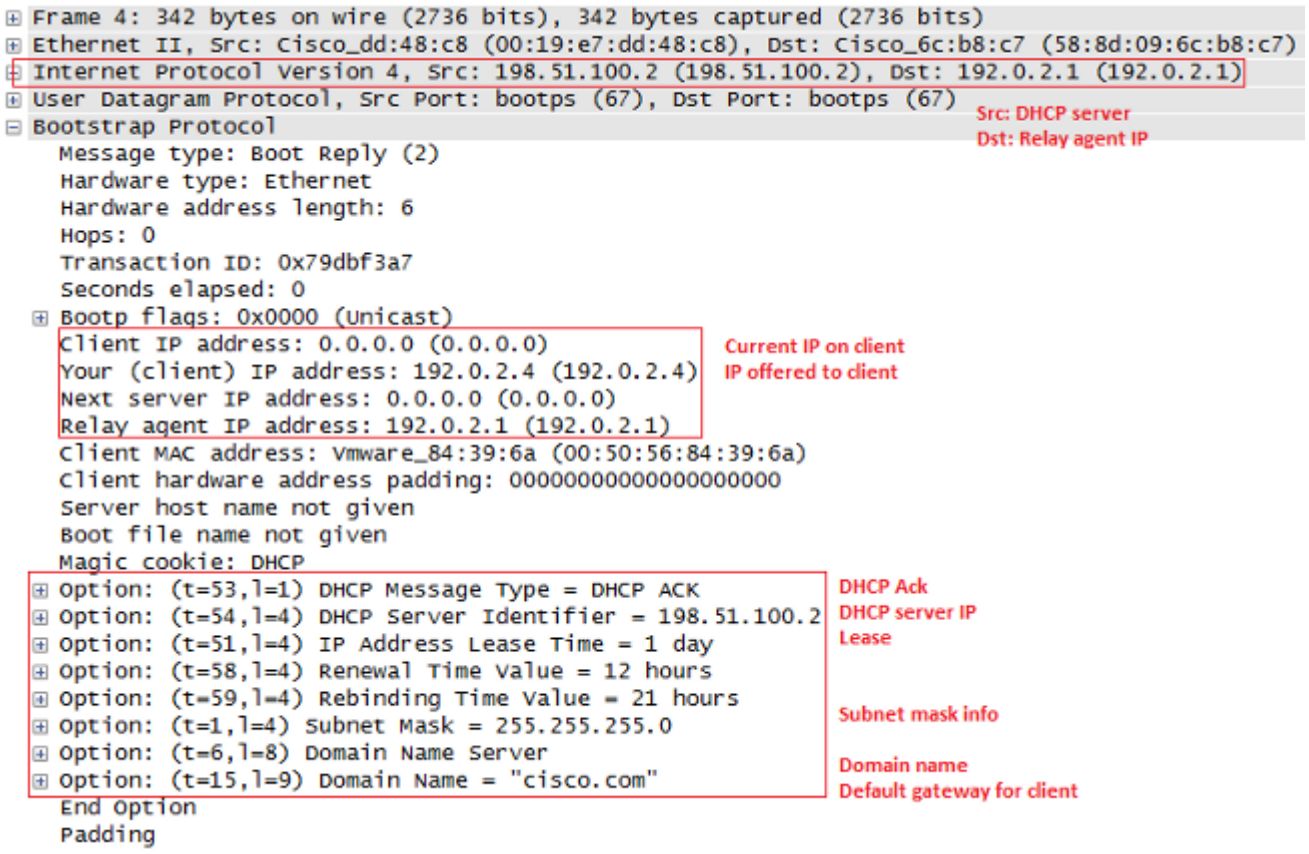
5. Once you receive the DHCPOFFER message, send a DHCPREQUEST message in order to indicate that you accept the offer.



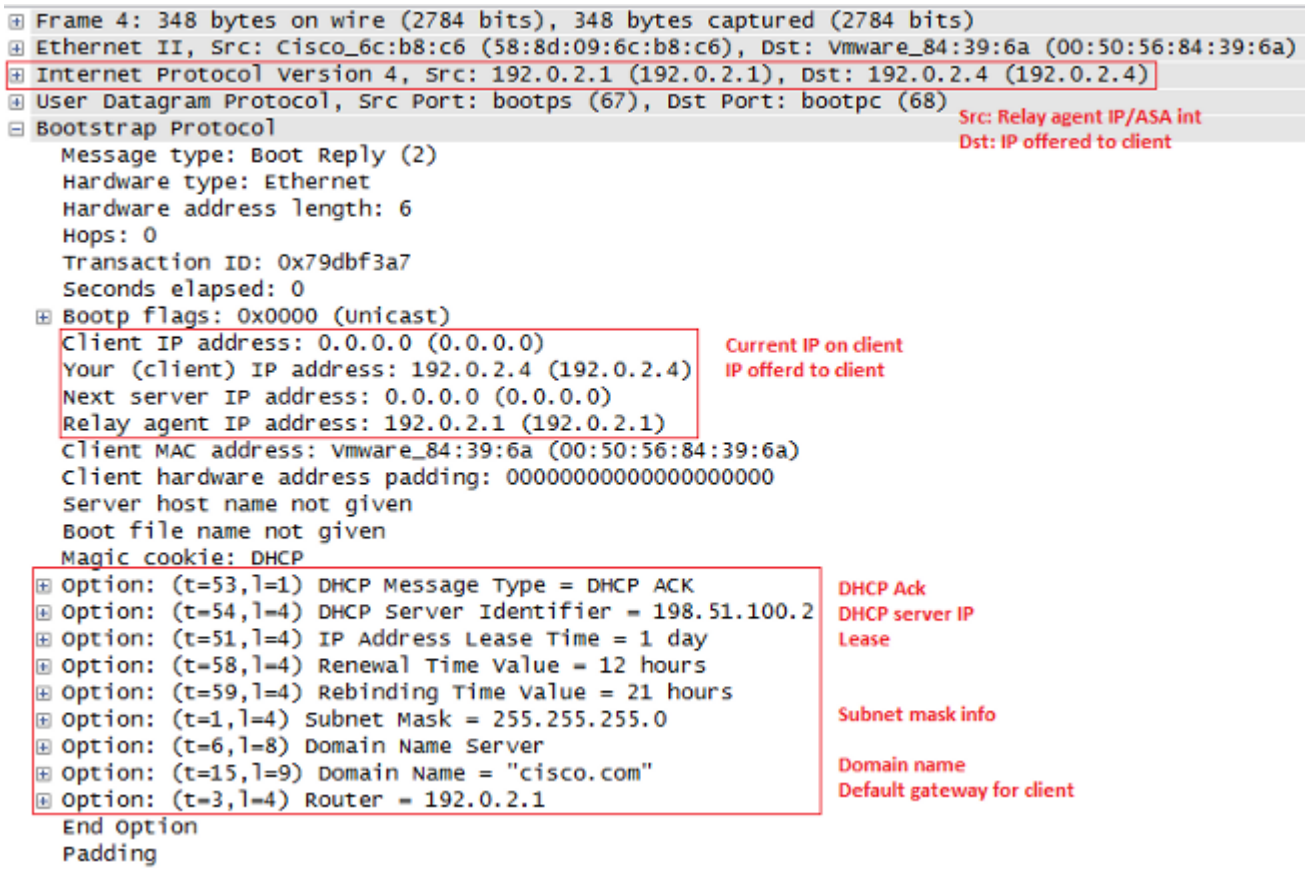
6. ASA passes the DHCPREQUEST to the DHCP server.



7. Once the server gets the DHCPREQUEST, it sends the DHCPACK back in order to confirm the offered IP.



8. ASA passes the DHCPACK from the DHCP server to you, and that completes the transaction.



Debugs and Syslogs for DHCP Relay Transactions

This is a DHCP request forwarded to DHCP server interface 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
```

After the reply is received from the DHCP server, the security appliance forwards it to the DHCP client with MAC address 0050.5684.396a, and changes the gateway address to its own inside interface.

```
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.
```

The same transaction shows up in the syslogs as well:

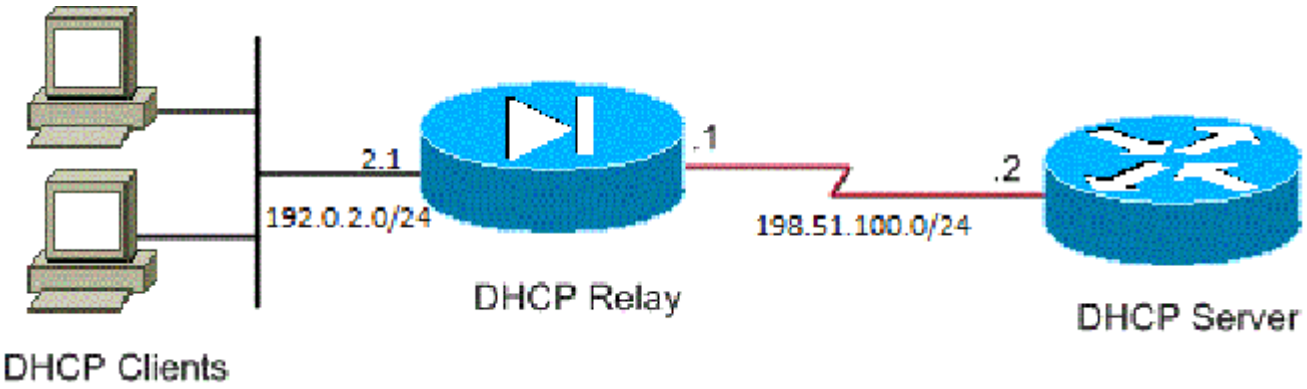
```
%ASA-7-609001: Built local-host inside:0.0.0.0
%ASA-7-609001: Built local-host identity:255.255.255.255
%ASA-6-302015: Built inbound UDP connection 13 for inside:
 0.0.0.0/68 (0.0.0.0/68) to identity:255.255.255.255/67 (255.255.255.255/67)
%ASA-7-609001: Built local-host identity:198.51.100.1
%ASA-7-609001: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

Configure

In this section, you are presented with the information used to configure the features described in this document.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- DHCP Relay Configuration with Use of the CLI
- DHCP Relay Final Configuration
- DHCP Server Configuration

DHCP Relay Configuration with Use of the CLI

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

DHCP Relay Final Configuration

```
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 Server Configuration

```
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
```

DHCP Relay with Multiple DHCP Servers

You can define up to ten DHCP servers. When a client sends a DHCP *Discover* packet, it is forwarded to all of the DHCP servers.

Here is an example:

```
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
```

Debugs with Multiple DHCP Servers

Here are some example debugs when multiple DHCP servers are used:

```
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 with Multiple DHCP Servers

Here is an example packet capture when multiple DHCP servers are used:

```
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
```

Verify

Use this section in order to confirm that your configuration works properly.

In order to view the statistical information about the DHCP relay services, enter the **show dhcprelay statistics** command on the ASA CLI:

```
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
```

This output provides information on several DHCP message types, such as DHCPDISCOVER, DHCP REQUEST, DHCP OFER, DHCP RELEASE, and DHCP ACK.

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

Troubleshoot

This section provides information you can use in order to troubleshoot your 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
```

You can also use these debug commands:

- **debug dhcprelay packet**
- **debug dhcprelay event**
- **Captures**
- **Syslogs**

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Related Information

- **Captures on ASA**
- **Technical Support & Documentation - Cisco Systems**