ASA(Adaptive Security Appliance) DHCP 릴레이 구성

목차

소개

이 문서에서는 패킷 캡처 및 디버그를 통한 Cisco ASA의 DHCP 릴레이에 대해 설명하고 컨피그레이션 예를 제공합니다.

사전 요구 사항

DHCP(Dynamic Host Configuration Protocol) 릴레이 에이전트를 사용하면 보안 어플라이언스가 클라이언트의 DHCP 요청을 라우터나 다른 인터페이스에 연결된 다른 DHCP 서버로 전달할 수 있습니다.

이러한 제한은 DHCP 릴레이 에이전트를 사용하는 경우에만 적용됩니다.

- DHCP 서버 기능도 활성화된 경우 릴레이 에이전트를 활성화할 수 없습니다.
- 보안 어플라이언스에 직접 연결해야 하며 다른 릴레이 에이전트 또는 라우터를 통해 요청을 보낼 수 없습니다.

- 다중 컨텍스트 모드에서는 둘 이상의 컨텍스트에서 사용하는 인터페이스에서 DHCP 릴레이를 활성화하거나 DHCP 릴레이 서버를 구성할 수 없습니다.

투명 방화벽 모드에서는 DHCP 릴레이 서비스를 사용할 수 없습니다. 투명 방화벽 모드의 보안 어플라이언스는 ARP(Address Resolution Protocol) 트래픽만 통과하도록 허용합니다. 다른 모든 트래픽에는 ACL(Access Control List)이 필요합니다. 투명 모드에서 DHCP 요청과 회신이 보안 어플라이언스를 통과하도록 허용하려면 두 개의 ACL을 구성해야 합니다.

- 내부 인터페이스에서 외부로의 DHCP 요청을 허용하는 하나의 ACL.
- 서버의 응답을 다른 방향으로 허용하는 하나의 ACL.

요구 사항

Cisco에서는 ASA CLI 및 Cisco IOS® CLI에 대한 기본 지식을 갖춘 것을 권장합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASA 5500-x Series Security Appliance 릴리스 9.x 이상
- Cisco 1800 Series 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

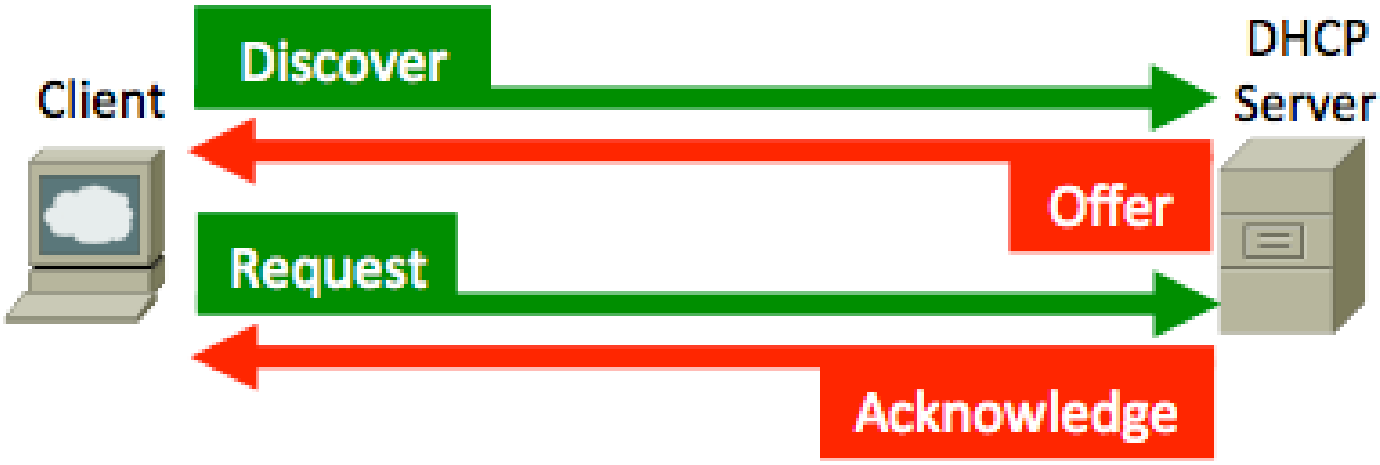
배경 정보

DHCP 프로토콜은 IP 주소(서브넷 마스크 포함), 기본 게이트웨이, DNS 서버 주소, WINS(Windows Internet Name Service) 주소 등의 자동 컨피그레이션 매개변수를 호스트에 제공합니다. 처음에 DHCP 클라이언트에는 이러한 컨피그레이션 매개변수가 없습니다. 이러한 정보를 얻기 위해 브로드캐스트 요청을 보냅니다. DHCP 서버가 이 요청을 발견하면 DHCP 서버는 필요한 정보를 제공합니다. 이러한 브로드캐스트 요청의 특성으로 인해 DHCP 클라이언트와 서버는 동일한 서브넷에 있어야 합니다. 라우터 및 방화벽과 같은 레이어 3 디바이스는 일반적으로 이러한 브로드캐스트 요청을 기본적으로 전달하지 않습니다.

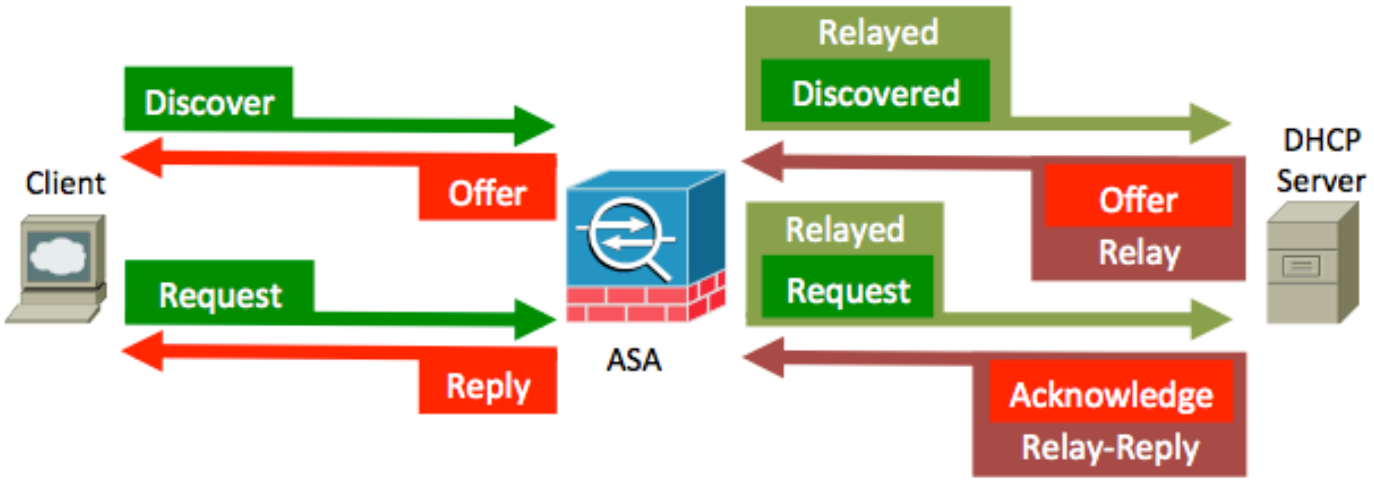
동일한 서브넷에서 DHCP 클라이언트와 DHCP 서버를 찾으려는 시도가 항상 편리한 것은 아닙니다. 이러한 상황에서는 DHCP 릴레이를 사용할 수 있습니다. 보안 어플라이언스의 DHCP 릴레이 에이전트는 내부 인터페이스의 호스트에서 DHCP 요청을 수신하면 외부 인터페이스의 지정된 DHCP 서버 중 하나로 요청을 전달합니다. DHCP 서버가 클라이언트에 회신하면 보안 어플라이언스는 해당 회신을 다시 전달합니다. 따라서 DHCP 릴레이 에이전트는 DHCP 서버와의 대화에서 DHCP 클라이언트를 위한 프록시 역할을 합니다.

패킷 플로우

이 그림에서는 DHCP 릴레이 에이전트를 사용하지 않는 경우의 DHCP 패킷 흐름을 보여 줍니다.



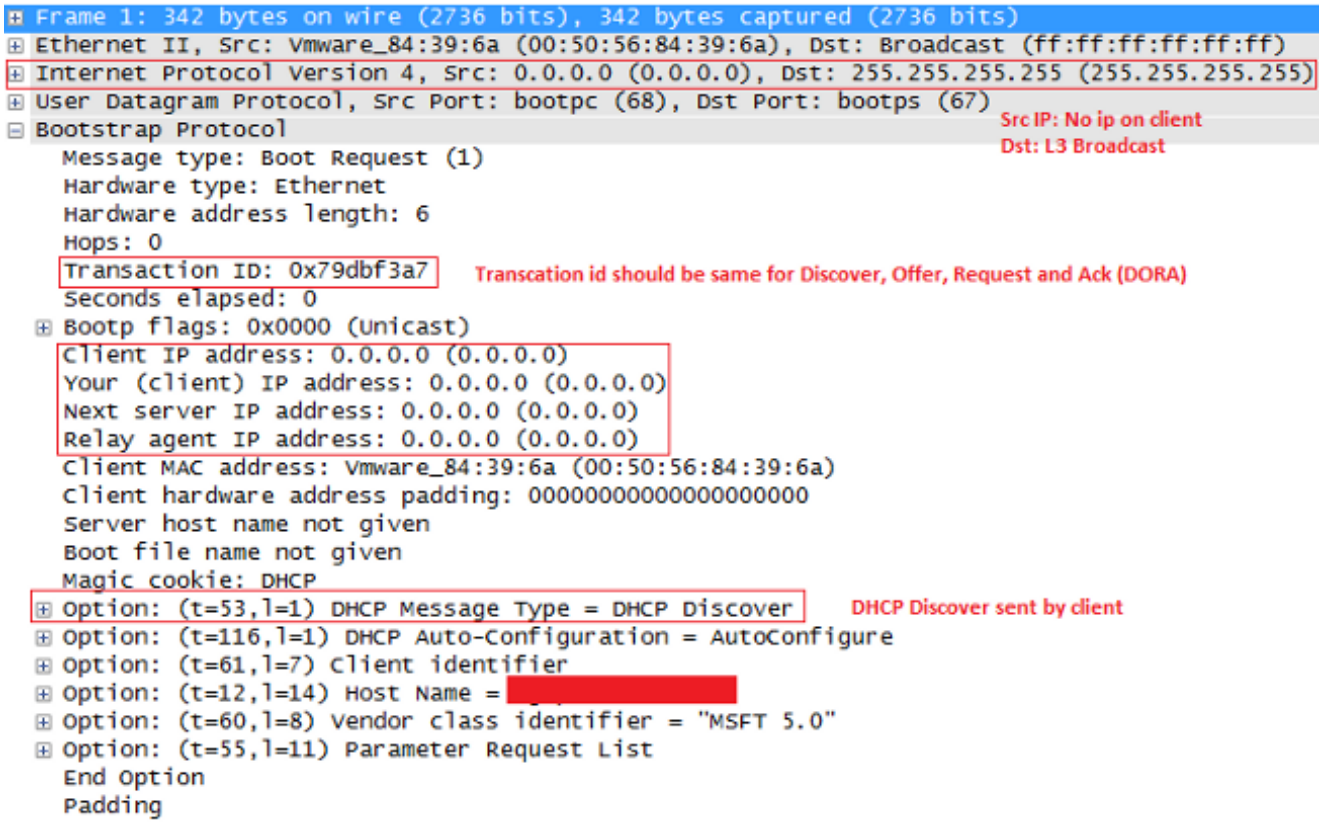
ASA는 이러한 패킷을 인터셉트하여 DHCP 릴레이 형식으로 래핑합니다.



ASA 내부 및 외부 인터페이스에서 패킷 캡처를 사용하는 DHCP 릴레이

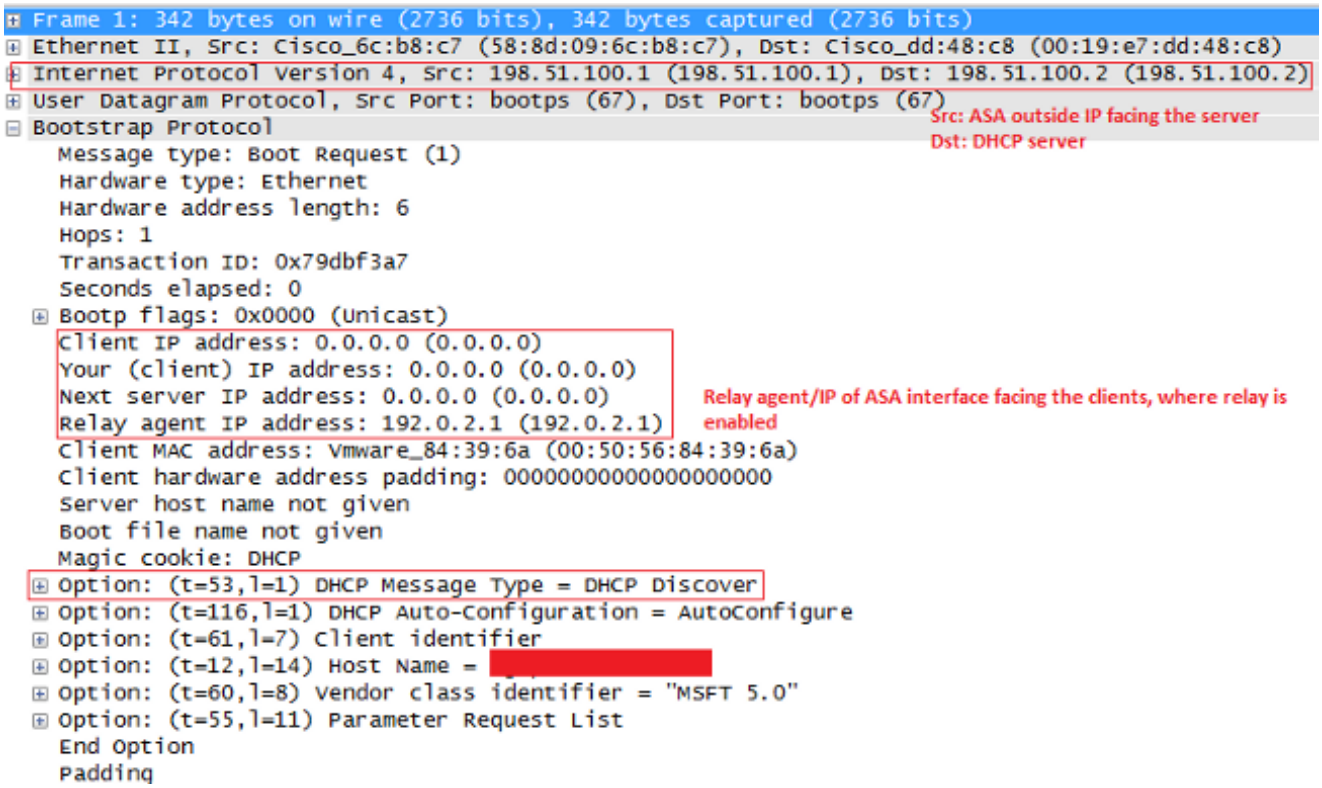
ASA에서 다양한 필드를 수정하는 방식이므로 빨간색으로 강조 표시된 내용을 기록해 둡니다.

1. DHCP 프로세스를 시작하려면 시스템을 부팅하고 브로드캐스트 메시지 (DHCPDISCOVER)를 대상 주소 255.255.255.255 - UDP 포트 67로 보냅니다.



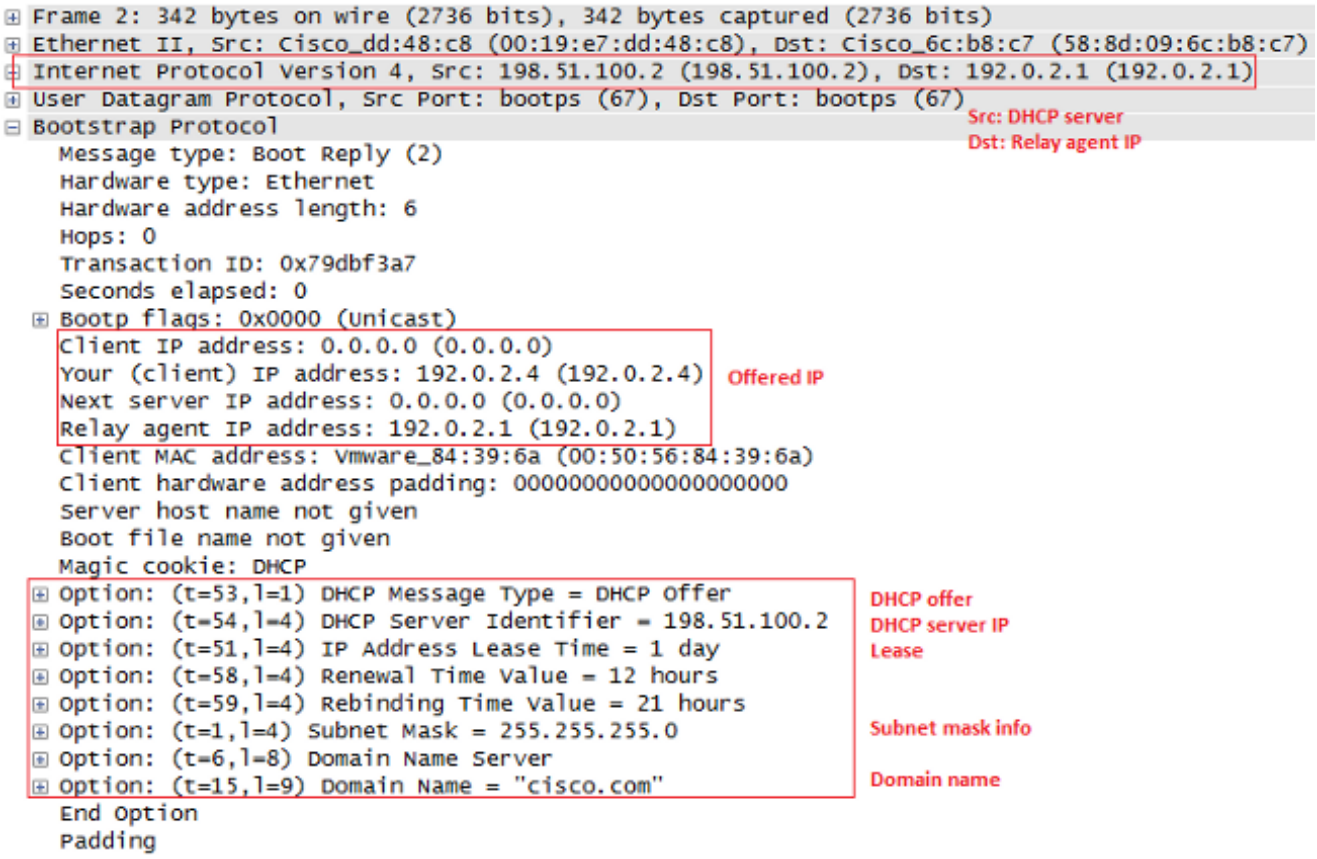
참고: VPN 클라이언트에서 IP 주소를 요청할 경우 릴레이 에이전트 IP 주소는 group-policy에서 dhcp-network-scope 명령으로 정의된 첫 번째 사용 가능한 IP 주소입니다.

2. 일반적으로 ASA는 브로드캐스트를 삭제하지만 DHCP 릴레이의 역할을 하도록 구성되어 있으므로 DHCP 릴레이 역할을 하는 DHCP 서버는 DHCP 서버의 IP 소싱에 유니캐스트 패킷으로 DHCPDISCOVER 메시지를 전달합니다. 인터페이스 IP는 서버에 전달됩니다. 이 경우 외부 인터페이스 IP 주소입니다. IP 헤더 및 릴레이 에이전트 필드의 변경 사항을 확인합니다.

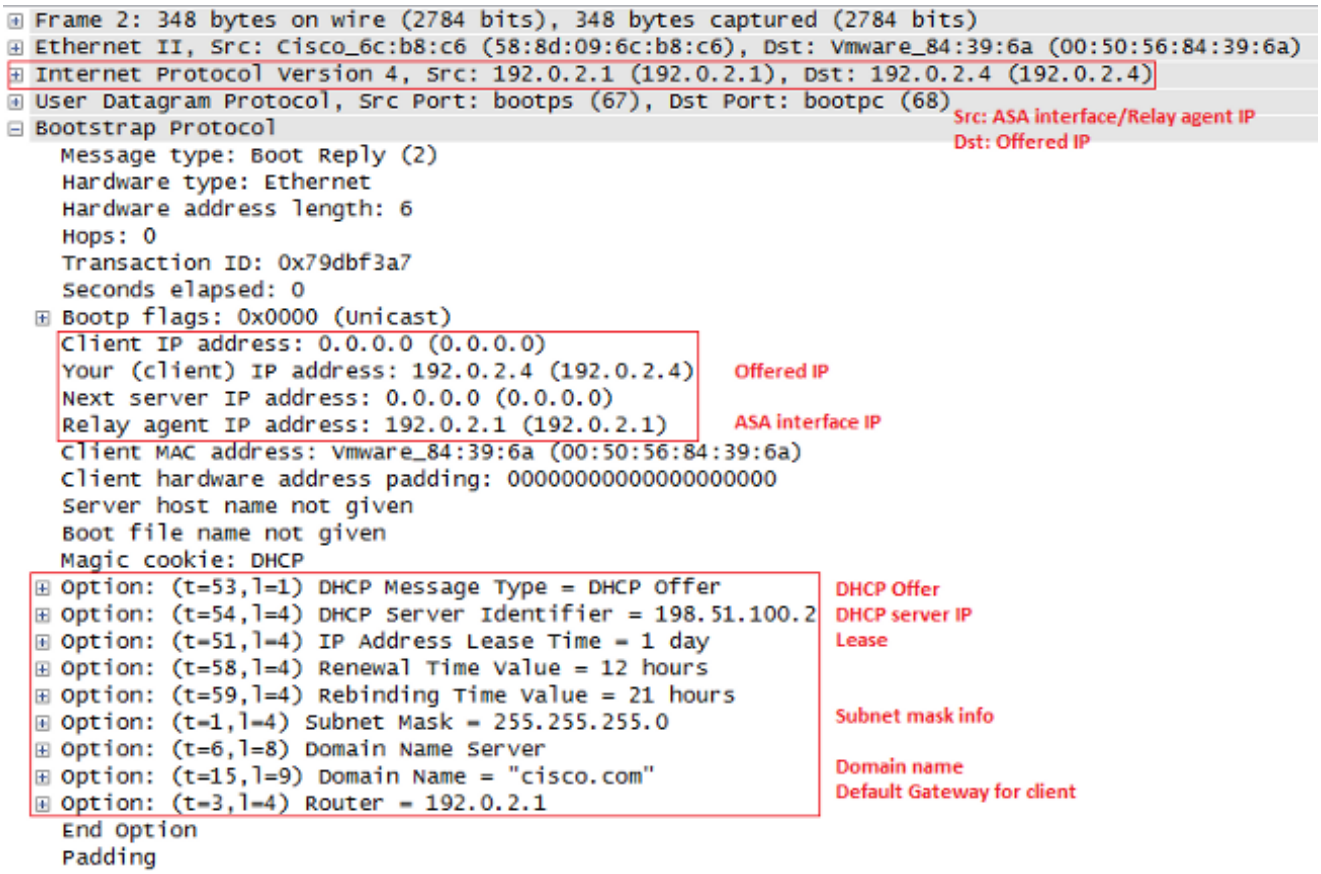


> 참고: Cisco 버그 ID CSCuo89924에 통합된 수정 사항으로 인해 버전 9.1(5.7), 9.3(1) 이상에서 ASA는 dhcprelay가 활성화된 클라이언트(gipaddr)를 향하는 인터페이스 IP 주소에서 DHCP 서버의 IP 소싱으로 유니캐스트 패킷을 전달할 수 있습니다. 이 경우 내부 인터페이스 IP 주소일 수 있습니다.

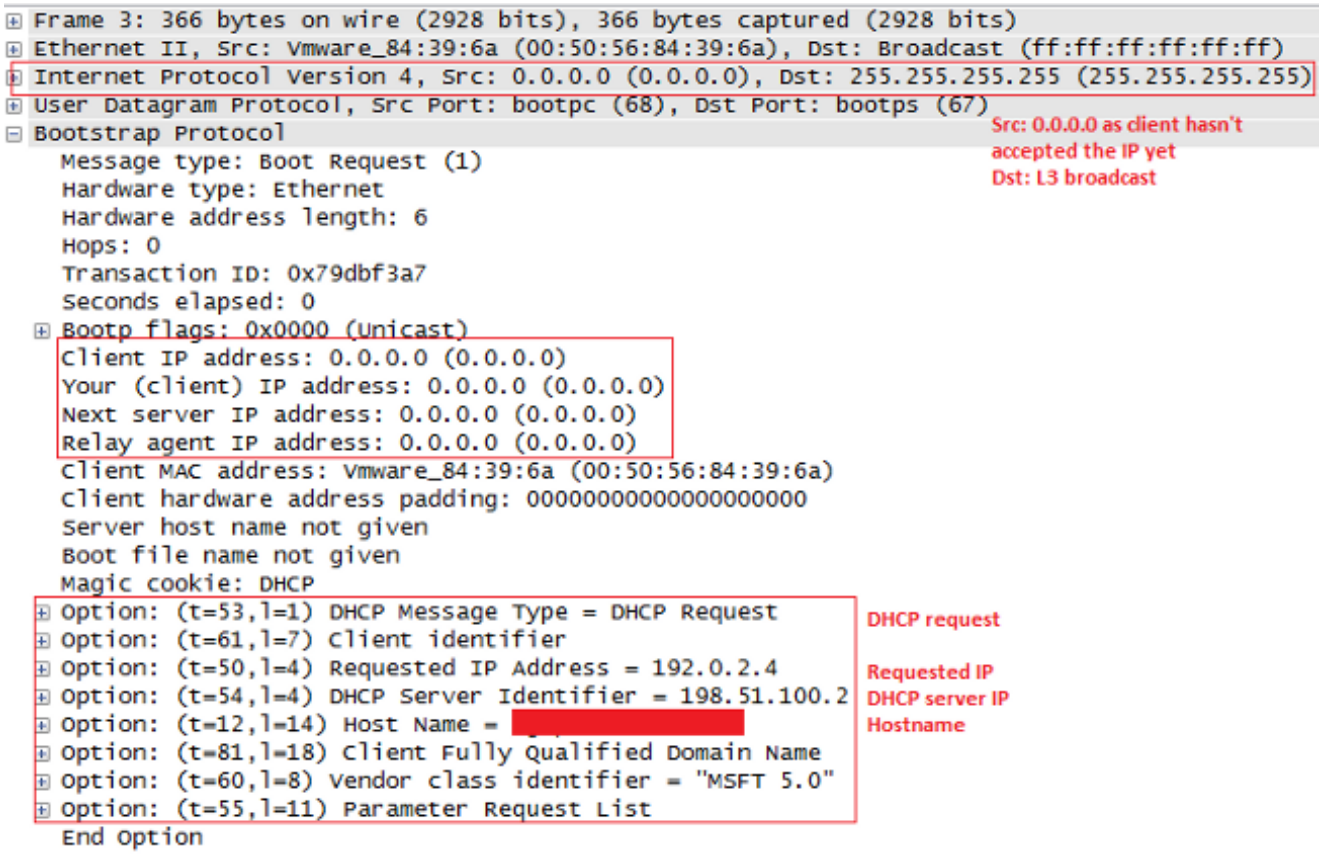
3. 서버는 DHCPDISCOVER- UDP 포트 67에 설정된 릴레이 에이전트 IP를 대상으로 DHCPOFFER 메시지를 유니캐스트 패킷으로 ASA에 다시 전송합니다. 이 경우 dhcprelay가 활성화된 내부 인터페이스(giaddr)의 IP 주소입니다. 레이어 3 헤더의 목적지 IP를 확인합니다
.



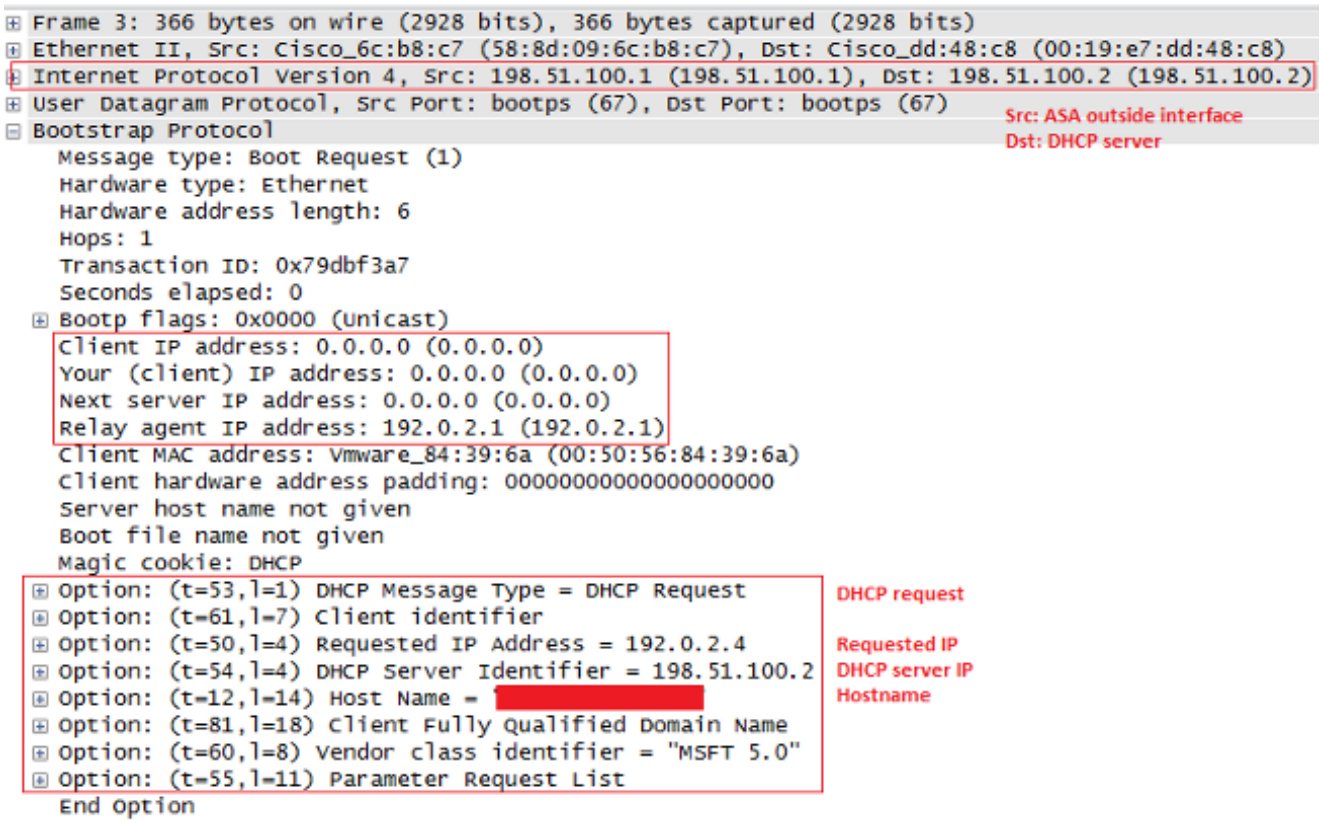
4. ASA는 내부 인터페이스(UDP 포트 68)에서 이 패킷을 전송합니다. 패킷이 내부 인터페이스를 떠나는 동안 IP 헤더가 변경된 것을 확인합니다.



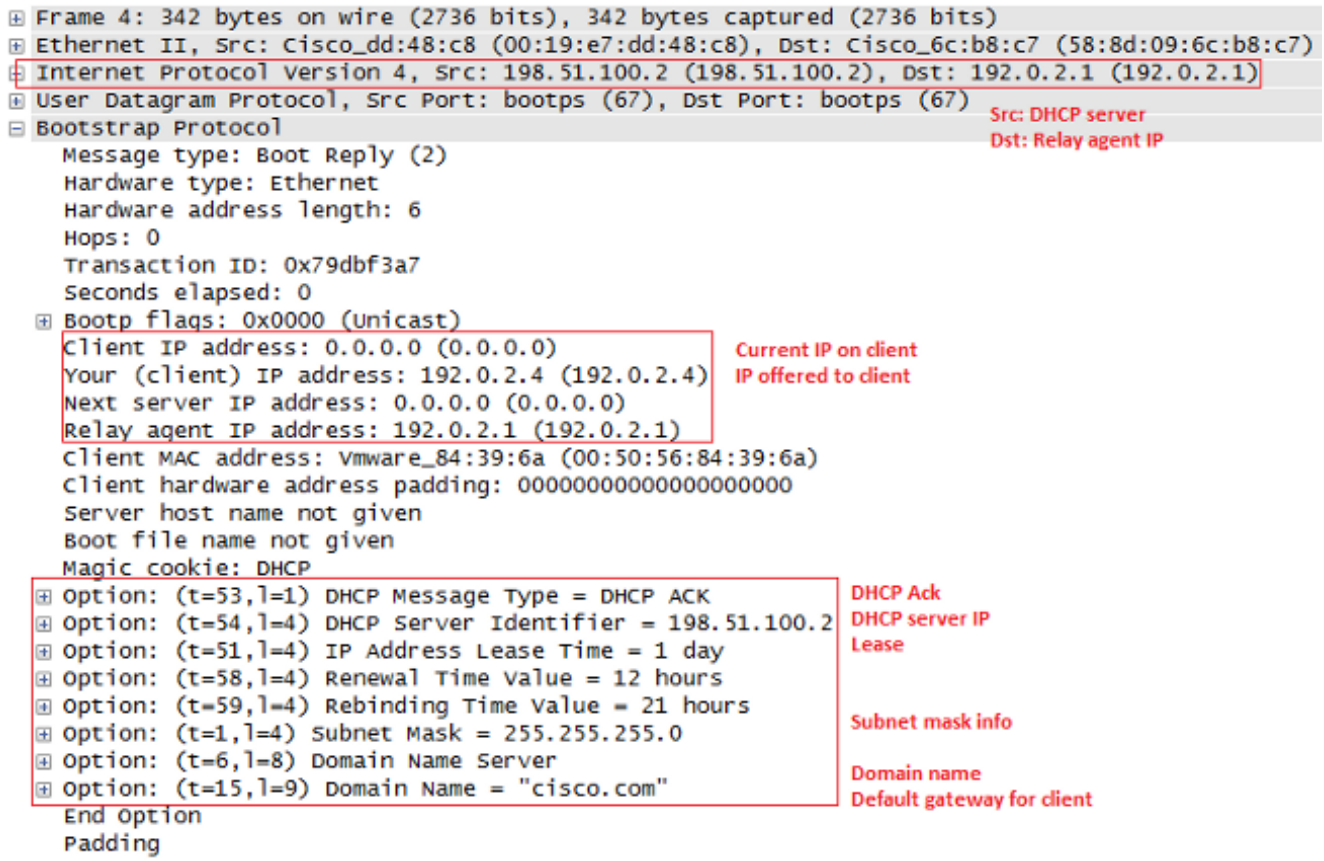
5. DHCPOFFER 메시지를 수신하면 DHCPREQUEST 메시지를 보내 제안을 수락함을 알립니다.



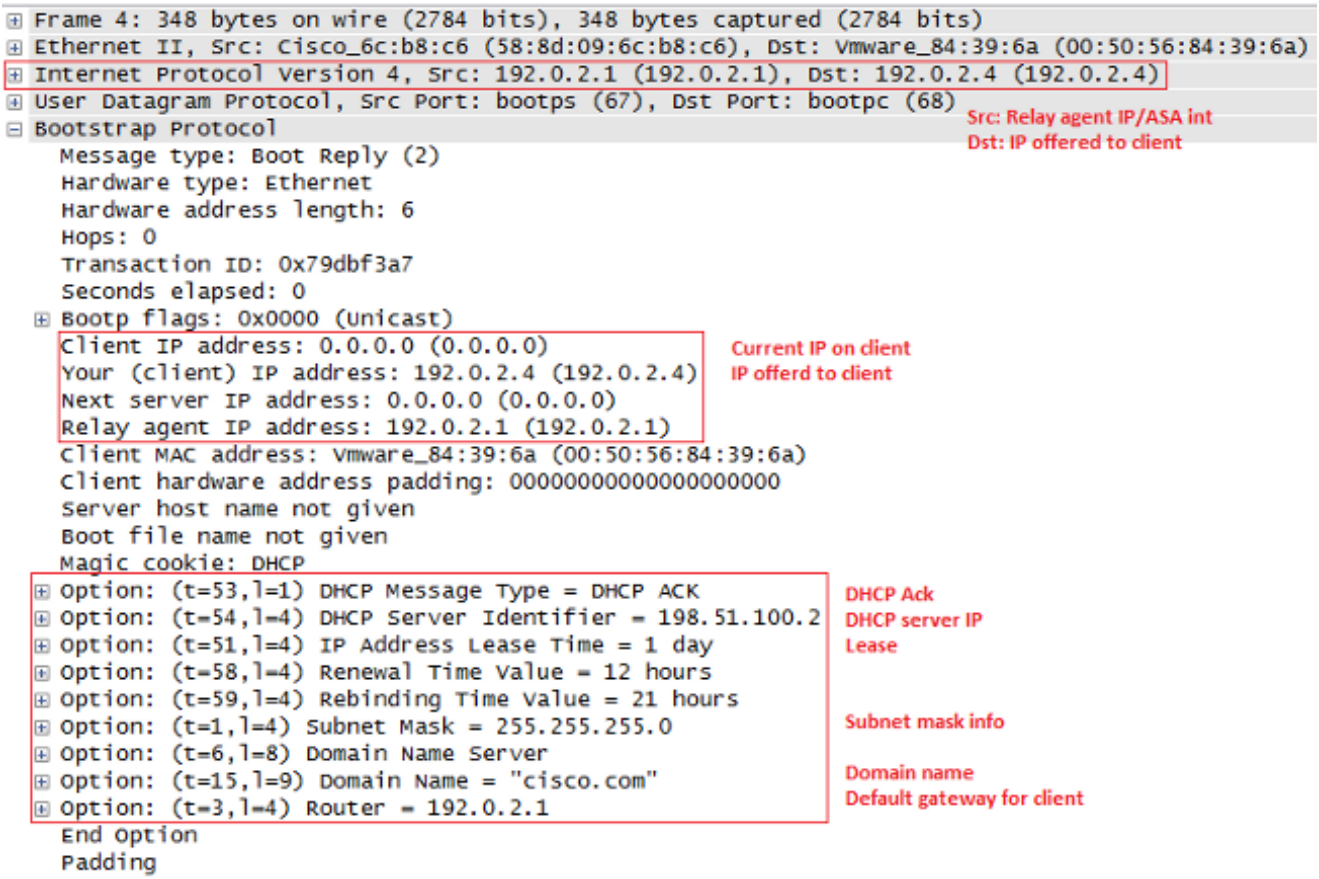
6. ASA는 DHCP 서버에 DHCPREQUEST를 전달합니다.



7. 서버는 DHCPREQUEST를 받으면 제공된 IP를 확인하기 위해 DHCPACK을 다시 보냅니다.



8. ASA가 DHCP 서버에서 DHCPACK을 사용자에게 전달하면 트랜잭션이 완료됩니다.



DHCP 릴레이 트랜잭션을 위한 디버깅 및 Syslog

DHCP 서버 인터페이스 198.51.100.2에 전달된 DHCP 요청입니다.

```
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
```

DHCP 서버에서 응답을 받으면 보안 어플라이언스는 MAC 주소가 0050.5684.396a인 DHCP 클라이언트에 회신을 전달하고 게이트웨이 주소를 자체 내부 인터페이스로 변경합니다.

```
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.
```

syslog에도 동일한 트랜잭션이 표시됩니다.

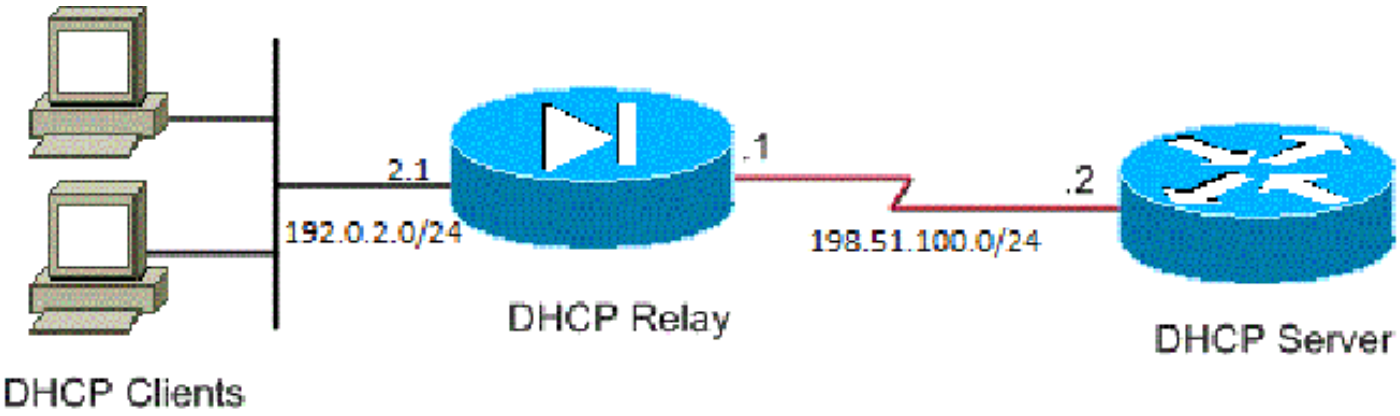
```
%ASA-7-609001: Built local-host inside:0.0.0.0
%ASA-7-609001: Built local-host identity:255.255.255.255
%ASA-6-302015: Built inbound UDP connection 13 for inside:
 0.0.0.0/68 (0.0.0.0/68) to identity:255.255.255.255/67 (255.255.255.255/67)
%ASA-7-609001: Built local-host identity:198.51.100.1
%ASA-7-609001: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

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 데 사용되는 정보를 제공합니다.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



설정

이 문서에서는 다음 설정을 사용합니다.

- CLI를 사용하는 DHCP 릴레이 컨피그레이션
- DHCP 릴레이 최종 컨피그레이션
- DHCP 서버 컨피그레이션

CLI를 사용하는 DHCP 릴레이 컨피그레이션

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

DHCP 릴레이 최종 컨피그레이션

```
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 서버 컨피그레이션

```
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
```

여러 DHCP 서버를 사용하는 DHCP 릴레이

최대 10개의 DHCP 서버를 정의할 수 있습니다. 클라이언트가 DHCP Discover 패킷을 전송하면 모든 DHCP 서버에 전달됩니다.

예를 들면 다음과 같습니다.

```
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
```

여러 DHCP 서버로 디버깅

다음은 여러 DHCP 서버가 사용될 때 디버깅하는 예입니다.

```
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.
```

여러 DHCP 서버를 사용한 캡처

다음은 여러 DHCP 서버가 사용되는 경우의 패킷 캡처 예입니다.

```
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
```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

DHCP 릴레이 서비스에 대한 통계 정보를 보려면 ASA CLI에서 show dhcprelay statistics 명령을 입력합니다.

```
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
```

이 출력은 DHCPDISCOVER, DHCP REQUEST, DHCP OFER, DHCP RELEASE 및 DHCP ACK와 같은 여러 DHCP 메시지 유형에 대한 정보를 제공합니다.

- asa CLI에 dhcprelay 상태 표시
- 라우터 CLI에서 ip dhcp 서버 통계 표시

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

```
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
```

다음 debug 명령을 사용할 수도 있습니다.

- dhcprelay 패킷 디버그
- dhcprelay 이벤트 디버그
- 캡처
- Syslog

참고: debug 명령을 사용하기 전에 Debug 명령에 대한 중요 정보를 참조하십시오.

관련 정보

- ASA의 캡처
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.