

Catalyst 스위치 또는 엔터프라이즈 네트워크의 동적 호스트 구성 프로토콜 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[주요 개념](#)

[예제 시나리오](#)

[DHCP 이해](#)

[현재 DHCP RFC 참조](#)

[DHCP 메시지 테이블](#)

[DHCPDISCOVER](#)

[DHCPOFFER](#)

[DHCPREQUEST](#)

[DHCPACK](#)

[DHCPNAK](#)

[DHCPDECLINE](#)

[DHCPINFORM](#)

[DHCPRELEASE](#)

[리스 갱신](#)

[DHCP 패킷 테이블](#)

[클라이언트와 DHCP 서버가 동일한 서브넷에 있는 DHCP 주소를 가져오는 클라이언트에 대한 클라이언트-서버 대화](#)

[DHCP/BootP 릴레이 에이전트의 역할](#)

[Cisco IOS® 라우터에서 DHCP/BootP 릴레이 에이전트 기능 구성](#)

[수동 바인딩 설정](#)

[보조 IP 세그먼트에서 DHCP가 작동하도록 하는 방법](#)

[DHCP 릴레이 기능을 사용한 DHCP 클라이언트-서버 대화](#)

[DHCP 클라이언트가 IP 주소를 가져오는 프로세스](#)

[PXE\(Pre-Execution Environment\) 부팅 DHCP 고려 사항](#)

[스니퍼 추적을 사용하여 DHCP 이해 및 문제 해결](#)

[동일한 LAN 세그먼트에서 DHCP 클라이언트 및 서버의 스니퍼 추적 디코딩](#)

[DHCP 클라이언트와 서버가 동일한 LAN 세그먼트에 상주하는 네트워크 토폴로지](#)

[DHCP 릴레이 에이전트로 구성된 라우터로 분리된 DHCP 클라이언트 및 서버의 스니퍼 추적 디코딩](#)

[스니퍼-B 추적](#)

[스니퍼-A 추적](#)

[클라이언트 워크스테이션이 DHCP 주소를 가져올 수 없을 때 DHCP 문제 해결](#)

[고객 사례 #1: DHCP 클라이언트와 동일한 LAN 세그먼트 또는 VLAN의 DHCP 서버](#)

[고객 사례 #2: DHCP 서버 및 DHCP 클라이언트는 DHCP/BootP 릴레이 에이전트 기능을 위해 구성된 라우터로 구분됩니다](#)

[DHCP Server on Router Fails Fails\(라우터의 DHCP 서버가 주소 할당에 실패함\) - POOL EXHAUSTED\(풀 사용\) 오류](#)

[DHCP 문제 해결 모듈](#)

[DHCP 문제가 발생할 수 있는 위치 이해](#)

[DHCP 문제의 가능한 원인 짧은 목록:](#)

[A. 물리적 연결 확인](#)

[C. 시작 문제로 확인](#)

[D. 스위치 포트 구성 확인\(STP Portfast 및 기타 명령\)](#)

[E. 알려진 NIC 카드 또는 Catalyst 스위치 문제 확인](#)

[F. DHCP 클라이언트가 DHCP 서버와 동일한 서브넷 또는 VLAN에서 IP 주소를 얻는지 여부를 구별합니다](#)

[G. 라우터 DHCP/BootP 릴레이 컨피그레이션 확인](#)

[H. 가입자 식별\(82\) 옵션 설정](#)

[I. DHCP 데이터베이스 에이전트 및 DHCP 충돌 로깅](#)

[J. IP 전화 연결에 대한 CDP 확인](#)

[K. Remove Down SVI Disrupts DHCP Snooping Operation\(SVI가 DHCP 스누핑 작업을 중단합니다\)](#)

[L. 제한된 브로드캐스트 주소](#)

[M. 라우터 디버그 명령을 사용하여 DHCP 디버그](#)

[샘플 출력](#)

[샘플 출력](#)

[부록 A: Cisco IOS DHCP 샘플 컨피그레이션](#)

[관련 정보](#)

소개

이 문서에서는 Cisco Catalyst 스위치 네트워크에서 DHCP(Dynamic Host Configuration Protocol)와 관련된 몇 가지 일반적인 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

참고: 등록된 Cisco 클라이언트만 내부 버그 보고서에 액세스할 수 있습니다.

배경 정보

DHCP는 TCP/IP(Transmission Control Protocol/Internet Protocol)를 사용하는 컴퓨터가 네트워크를 통해 프로토콜 구성 매개변수를 자동으로 얻을 수 있는 메커니즘을 제공합니다. DHCP는 IETF([Internet Engineering Task Force](#))의 DHC-WG([Dynamic Host Configuration-Working Group](#))에서 개발한 개방형 표준입니다.

DHCP는 클라이언트-서버 패러다임을 기반으로 합니다. 여기서 DHCP 클라이언트(예: 데스크톱 컴퓨터)는 구성 매개변수를 위해 DHCP 서버에 연결합니다. DHCP 서버는 일반적으로 네트워크 관리자가 중앙에 배치하고 운영합니다. 네트워크 관리자가 서버를 실행하므로 DHCP 클라이언트를 현재 네트워크 아키텍처에 적합한 매개변수로 안정적이고 동적으로 구성할 수 있습니다.

대부분의 엔터프라이즈 네트워크는 VLAN(Virtual LAN)이라고 하는 하위 네트워크로 구분되는 여러 서브넷으로 구성됩니다. 여기서 라우터는 하위 네트워크 간에 라우팅됩니다. 라우터는 기본적으로 브로드캐스트를 전달하지 않으므로 DHCP 릴레이 에이전트 기능을 사용하여 DHCP 브로드캐스트를 전달하도록 구성되지 않는 한 각 서브넷에 DHCP 서버가 필요합니다.

주요 개념

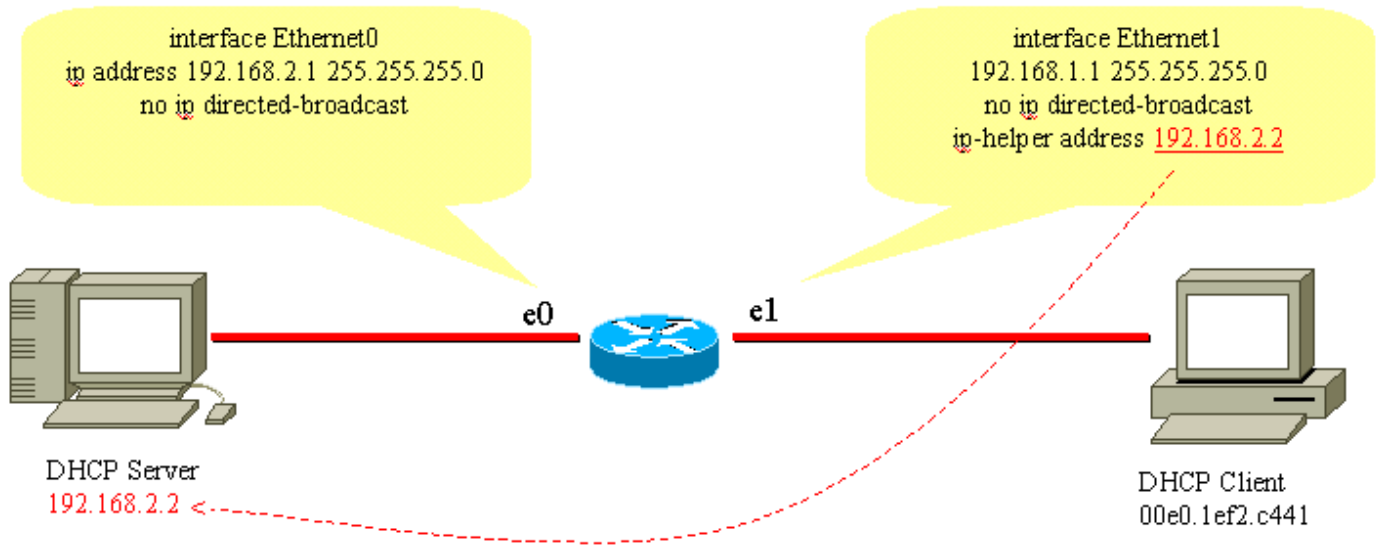
다음은 DHCP의 몇 가지 주요 개념입니다.

- DHCP 클라이언트는 처음에 구성된 IP 주소가 없으므로 DHCP 서버로부터 IP 주소를 얻기 위해 브로드캐스트 요청을 보내야 합니다.
- 기본적으로 라우터는 브로드캐스트를 전달하지 않습니다. DHCP 서버가 다른 브로드캐스트 도메인(레이어 3(L3) 네트워크)에 있는 경우 클라이언트 DHCP 브로드캐스트 요청을 수용해야 합니다. 이는 DHCP 릴레이 에이전트를 사용하여 수행됩니다.
- DHCP 릴레이의 Cisco 라우터 구현은 인터페이스 레벨 **ip 헬퍼** 명령을 통해 제공됩니다.

예제 시나리오

시나리오 1: DHCP 클라이언트와 서버 네트워크 간의 Cisco 라우터 라우팅

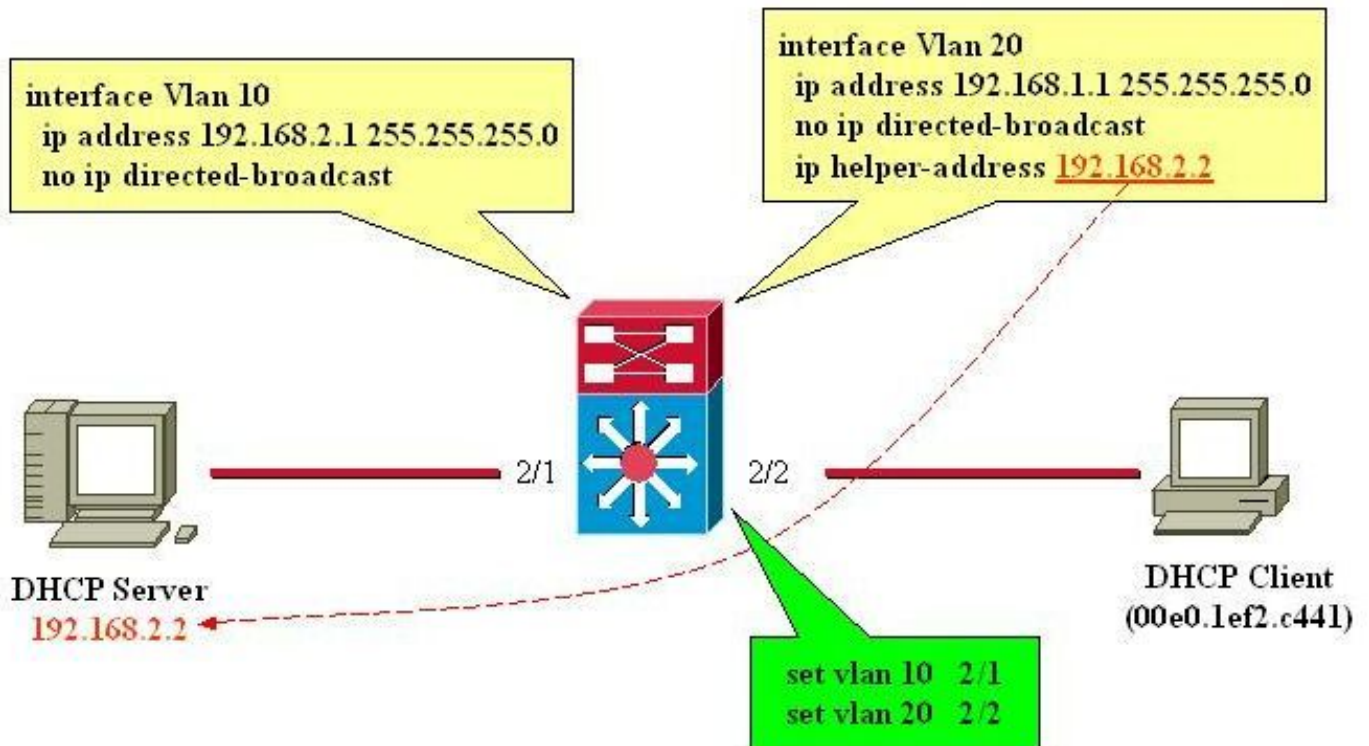
이 다이어그램에 구성된 대로, 인터페이스 Ethernet1은 클라이언트 브로드캐스트 DHCPDISCOVER를 인터페이스 Ethernet1을 통해 192.168.2.2로 전달합니다. DHCP 서버는 유니캐스트를 통해 요청을 이행합니다. 이 예에서는 라우터에 대한 추가 컨피그레이션이 필요하지 않습니다.



DHCP 클라이언트와 서버 네트워크 간 라우팅

시나리오 2: DHCP 클라이언트와 서버 네트워크 간의 L3 모듈 라우팅을 지원하는 Cisco Catalyst 스위치

다이어그램에 구성된 대로 인터페이스 VLAN20은 클라이언트 브로드캐스트 DHCPDISCOVER를 인터페이스 VLAN10을 통해 192.168.2.2로 전달합니다. DHCP 서버는 유니캐스트를 통해 요청을 이행합니다. 이 예에서는 라우터에 대한 추가 컨피그레이션이 필요하지 않습니다. 스위치 포트는 호스트 포트로 구성해야 하며 STP(Spanning-Tree Protocol) 포트패스트가 활성화되고 트렁킹 및 채널링이 비활성화됩니다.



DHCP 클라이언트와 서버 네트워크 간의 L3 모듈 경로

DHCP 이해

DHCP는 원래 RFC([Requests for Comments](#)) 1531에 정의되었으며 이후 RFC 2131에 의해 폐기되

있습니다. DHCP는 RFC 951에 정의된 BootP(부트스트랩 프로토콜)를 기반으로 [합니다](#).

DHCP는 워크스테이션(호스트)에서 부팅 시 IP 주소, 서브넷 마스크, 기본 게이트웨이와 같은 초기 컨피그레이션 정보를 가져오는 데 사용됩니다. DHCP를 사용하면 각 호스트를 수동으로 구성할 필요가 없습니다. 또한 호스트가 다른 IP 서브넷으로 이동하는 경우 이전에 사용한 것과 다른 IP 주소를 사용해야 합니다. DHCP는 자동으로 이 작업을 처리합니다. 호스트가 올바른 IP 서브넷에서 IP 주소를 선택할 수 있습니다.

현재 DHCP RFC 참조

- RFC 2131 - DHCP
- RFC 2132 - DHCP 옵션 및 BootP 벤더 확장
- RFC 1534 - DHCP와 BootP 간의 상호 운용
- RFC 1542 - BootP용 설명 및 확장
- RFC 2241 - Novell 디렉터리 서비스에 대한 DHCP 옵션
- RFC 2242 - Netware/IP 도메인 이름 및 정보
- RFC 2489 - 새 DHCP 옵션 정의 절차

DHCP는 하나 이상의 서버(DHCP 서버)가 클라이언트 부팅 시 클라이언트(호스트)에 IP 주소 및 기타 선택적 구성 매개변수를 할당하는 클라이언트-서버 모델을 사용합니다. 이러한 컨피그레이션 매개변수는 서버가 지정된 시간 동안 클라이언트에 임대합니다. 호스트가 부팅되면 호스트의 TCP/IP 스택은 IP 주소 및 서브넷 마스크, 기타 컨피그레이션 매개변수를 얻기 위해 브로드캐스트 (DHCPDISCOVER) 메시지를 전송합니다. 이렇게 하면 DHCP 서버와 호스트 간의 교환이 시작됩니다. 이 교환 과정에서 클라이언트는 다음과 같이 잘 정의된 상태를 통과합니다.

1. 초기화 중
2. 선택
3. 요청
4. 경계
5. 갱신
6. 다시 바인딩

이러한 상태 간에 이동하려면 클라이언트와 서버는 DHCP Message Table(DHCP 메시지 테이블)에 나열된 메시지 유형을 교환할 수 있습니다.

DHCP 메시지 테이블

참조	메시지	설명
0x01	DHCPDISCOVER	클라이언트가 사용 가능한 DHCP 서버를 찾습니다.
0x02	DHCPOFFER	클라이언트 DHCPDISCOVER에 대한 서버 응답입니다.
0x03	DHCPREQUEST	클라이언트는 서버로 브로드캐스트하고, 패킷에 정의된 대로 한 서버에서 제공된 변수를 요청합니다.
0x04	DHCPDECLINE	클라이언트-서버 통신 - 네트워크 주소가 이미 사용 중임을 나타냅니다.
0x05	DHCPACK	컨피그레이션 매개변수와 커밋된 네트워크 주소를 사용하는 서버-클라이언트 통신.
0x06	DHCPNAK	서버-클라이언트 통신에서 컨피그레이션 매개변수에 대한 요청을 거부합니다.
0x07	DHCPRELEASE	클라이언트-서버 통신에서 네트워크 주소를 해제하고 나머지 임대를 취소합니다.

0x08 DHCPINFORM

클라이언트-서버 통신에서는 클라이언트가 이미 외부로 주소로 구성된 로컬 컨피이션 매개변수만 요청합니다.

DHCPDISCOVER

클라이언트가 처음 부팅할 때 초기화 상태라고 하며 로컬 물리적 서브넷에서 UDP(User Datagram Protocol) 포트 67(BootP 서버)을 통해 DHCPDISCOVER 메시지를 전송합니다. 클라이언트는 자신이 속한 서브넷을 알 수 없으므로 DHCPDISCOVER는 소스 IP 주소가 0.0.0.0인 모든 서브넷 브로드캐스트(대상 IP 주소 255.255.255.255)입니다. 클라이언트에 구성된 IP 주소가 없으므로 소스 IP 주소는 0.0.0.0입니다. DHCP 서버가 이 로컬 서브넷에 있고 구성되어 있고 올바르게 작동하는 경우, DHCP 서버는 브로드캐스트를 듣고 DHCPPOFFER 메시지로 응답합니다. DHCP 서버가 로컬 서브넷에 없는 경우 DHCP 서버가 포함된 서브넷에 DHCPDISCOVER 메시지를 전달하려면 이 로컬 서브넷에 DHCP/BootP 릴레이 에이전트가 있어야 합니다.

이 릴레이 에이전트는 전용 호스트(예: Microsoft Windows Server) 또는 라우터(예: 인터페이스 레벨 IP 헬퍼 명령문으로 구성된 Cisco 라우터)일 수 있습니다.

DHCPOFFER

DHCPDISCOVER 메시지를 수신하는 DHCP 서버는 UDP 포트 68(BootP 클라이언트)에서 DHCPOFFER 메시지로 응답할 수 있습니다. 클라이언트가 DHCPOFFER를 받고 Selecting(선택) 상태로 이동합니다. 이 DHCPOFFER 메시지는 클라이언트에 대한 초기 컨피그레이션 정보를 포함합니다. 예를 들어 DHCP 서버는 DHCPOFFER 메시지의 yiaddr 필드에 요청된 IP 주소를 채웁니다. 서브넷 마스크 및 기본 게이트웨이는 각각 options 필드, subnet mask 및 라우터 옵션에 지정됩니다. DHCPOFFER 메시지의 다른 일반적인 옵션으로는 IP 주소 임대 시간, 갱신 시간, 도메인 이름 서버, WINS(NetBIOS Name Server)가 있습니다. DHCP 서버는 브로드캐스트 주소로 DHCPOFFER를 전송하지만, 서비스의 chaddr 필드에 클라이언트 하드웨어 주소를 포함하므로, 클라이언트는 자신이 의도된 대상임을 알 수 있습니다. DHCP 서버가 로컬 서브넷에 없는 경우 DHCP 서버는 유니캐스트 패킷인 DHCPOFFER를 UDP 포트 67에서 DHCPDISCOVER가 온 DHCP/BootP 릴레이 에이전트로 다시 보냅니다. 그러면 DHCP/BootP 릴레이 에이전트는 UDP 포트 68의 로컬 서브넷에서 DHCPOFFER를 브로드캐스트하거나 유니캐스트하며, 이는 Bootp 클라이언트에서 설정한 브로드캐스트 플래그에 따라 달라집니다.

DHCPREQUEST

클라이언트가 DHCPOFFER를 수신하면 DHCPREQUEST 메시지로 응답하고 DHCPOFFER의 매개변수를 수락할 의도를 나타내며 Requesting 상태로 이동합니다. 클라이언트는 원래 DHCPDISCOVER 메시지를 받은 각 DHCP 서버에서 하나씩 여러 DHCPOFFER 메시지를 받을 수 있습니다. 클라이언트는 하나의 DHCPOFFER를 선택하고 해당 DHCP 서버에만 응답하며 암시적으로 다른 모든 DHCPOFFER 메시지를 거부합니다. 클라이언트는 Server Identifier(서버 식별자) 옵션 필드를 DHCP 서버 IP 주소로 채운 후 선택한 서버를 식별합니다. DHCPREQUEST는 브로드캐스트이기도 하므로 DHCPOFFER를 보낸 모든 DHCP 서버가 DHCPREQUEST를 보고, 각 서버가 DHCPOFFER의 수락 또는 거부 여부를 알 수 있습니다. 클라이언트에 필요한 추가 컨피그레이션 옵션은 DHCPREQUEST 메시지의 options 필드에 포함됩니다. 클라이언트가 IP 주소를 제공받더라도 소스 IP 주소가 0.0.0.0인 DHCPREQUEST 메시지를 전송합니다. 현재 클라이언트는 IP 주소를 사용하는 것이 분명하다는 확인을 아직 받지 못했습니다.

DHCPACK

DHCP 서버는 DHCPREQUEST를 받은 후 DHCPACK 메시지로 요청을 승인하고 초기화 프로세스를 완료합니다. DHCPACK 메시지는 DHCP 서버의 소스 IP 주소를 가지며, 대상 주소는 다시 한 번 브로드캐스트이며 클라이언트가 DHCPREQUEST 메시지에서 요청한 모든 매개 변수를 포함합니다. 클라이언트가 DHCPACK을 수신하면 Bound(바인딩된) 상태가 되고 이제 네트워크에서 IP 주소를 사용하여 자유롭게 통신할 수 있습니다. 한편, DHCP 서버는 임대를 데이터베이스에 저장하고 클라이언트 식별자 또는 chaddr 및 관련 IP 주소로 임대차를 고유하게 식별합니다. 클라이언트와 서버 모두 이 식별자 조합을 사용하여 임대를 참조합니다. 클라이언트 식별자는 장치의 MAC 주소와 미디어 유형입니다.

DHCP 클라이언트가 새 주소를 사용하기 전에 DHCP 클라이언트는 임대 주소와 관련된 시간 매개 변수인 LT(임대 시간), T1(갱신 시간) 및 T2(리바인드 시간)를 계산해야 합니다. 일반적인 기본 LT는 72시간입니다. 필요한 경우 더 짧은 임대 시간을 사용하여 주소를 보존할 수 있습니다.

DHCPNAK

선택한 서버가 DHCPREQUEST 메시지를 충족할 수 없는 경우 DHCP 서버는 DHCPNAK 메시지로 응답합니다. 클라이언트가 DHCPDNK 메시지를 받거나 DHCPREQUEST 메시지에 대한 응답을 받지 못한 경우, 클라이언트는 요청 상태가 되면 컨피그레이션 프로세스를 다시 시작합니다. 클라이언트는 초기화 상태를 다시 시작하기 전에 60초 이내에 DHCPREQUEST를 4번 이상 재전송합니다.

DHCPDECLINE

클라이언트는 DHCPACK을 수신하고 선택적으로 매개 변수에 대한 최종 검사를 수행합니다. 클라이언트는 DHCPACK에 제공된 IP 주소에 대한 ARP(Address Resolution Protocol) 요청을 전송할 때 이 절차를 수행합니다. 클라이언트가 ARP 요청에 대한 응답을 수신할 때 주소가 이미 사용 중임을 감지하면 클라이언트는 서버에 DHCPDENT 메시지를 전송하고 요청 상태에서 컨피그레이션 프로세스를 다시 시작합니다.

DHCPINFORM

클라이언트가 다른 방법을 통해 네트워크 주소를 얻었거나 수동으로 구성된 IP 주소가 있는 경우, 클라이언트 워크스테이션은 DHCPINFORM 요청 메시지를 사용하여 도메인 이름 및 DNS(Domain Name Server)와 같은 다른 로컬 구성 매개 변수를 얻을 수 있습니다. DHCP 서버가 DHCPINFORM 메시지를 수신하면 새 IP 주소 없이 클라이언트에 적합한 로컬 구성 매개 변수를 사용하여 DHCPACK 메시지를 작성합니다. 이 DHCPACK은 클라이언트에 유니캐스트로 전송됩니다.

DHCPRELEASE

DHCP 클라이언트는 DHCP 서버에 DHCPRELEASE 메시지를 보낼 때 네트워크 주소에서 임대를 포기할 수 있습니다. 클라이언트는 DHCPRELEASE 메시지의 클라이언트 식별자 필드와 네트워크 사용하여 릴리스할 리스를 식별합니다. 현재 DHCP 풀 범위를 확장해야 하는 경우 현재 주소 풀을 제거하고 DHCP 풀 아래에서 새 IP 주소 범위를 지정합니다. DHCP 풀에 포함할 특정 IP 주소 또는 주소 범위를 제거하려면 `ip dhcp excluded-address` 명령을 사용합니다.

참고: 디바이스에서 BOOTP를 사용하는 경우 라우터의 DHCP 바인딩에 무제한 길이 임대가 표시됩니다.

리스 갱신

IP 주소는 서버에서만 임대 기간이 만료된 경우(T1=0.5 x LT) 클라이언트는 임대 갱신을 시도합니다. 클라이언트가 Renewing(갱신) 상태로 들어가서 현재 리스를 보유한 서버에 DHCPREQUEST 메시지를 전송합니다. 서버는 임대 갱신에 동의하는 경우 DHCPACK 메시지로 갱신 요청에 응답합니다. DHCPACK 메시지에는 이전 임대 기간 동안 서버가 변경된 경우 새 임대 및 새 컨피그레이션 매개변수가 포함됩니다. 클라이언트가 어떤 이유로 임대를 보유할 때 서버에 연결할 수 없는 경우, 원래 DHCP 서버가 T2 시간 내에 갱신 요청에 응답하지 않은 후 임의의 DHCP 서버에서 주소를 갱신하려고 시도합니다. 기본값 T2는 (7/8 x LT)입니다. 이는 T1 < T2 < LT를 의미합니다.

클라이언트가 이전에 DHCP에 할당된 IP 주소를 가지고 있었고 다시 시작된 경우, 클라이언트는 특별히 이전에 임대된 IP 주소를 DHCPREQUEST 패킷에서 요청합니다. 이 DHCPREQUEST에는 소스 IP 주소가 0.0.0.0으로, 대상이 IP 브로드캐스트 주소 255.255.255.255로 남아 있습니다.

재부팅 과정에서 클라이언트가 DHCPREQUEST를 전송할 경우 서버 식별자 필드에 입력하지 말고 요청된 IP 주소 옵션 필드에 입력해야 합니다. RFC 호환 클라이언트만 ciaddr 필드에 DHCP 옵션 필드 대신 요청된 주소를 채웁니다. DHCP 서버는 두 방법 중 하나를 수락합니다. DHCP 서버의 동작은 Windows NT DHCP 서버의 경우, 사용되는 시스템의 버전뿐만 아니라 다른 요인(예: 슈퍼대처)과 같은 여러 요인에 따라 달라집니다. DHCP 서버는 클라이언트가 요청된 IP 주소를 계속 사용할 수 있다고 판단할 경우, 무음으로 유지되거나 DHCPREQUEST를 위해 DHCPACK을 전송합니다. 서버는 클라이언트가 요청한 IP 주소를 사용할 수 없다고 판단하면 DHCPNACK을 클라이언트로 다시 전송합니다. 그런 다음 클라이언트는 Initializing(초기화) 상태로 이동하고 DHCPDISCOVER 메시지를 전송합니다.

참고: DHCP 서버는 IP 주소 풀의 하위 IP 주소를 DHCP 클라이언트에 할당합니다. 하위 주소의 임대가 만료되면 요청된 경우 다른 클라이언트에 할당됩니다. DHCP 주소가 할당된 순서는 변경할 수 없습니다.

DHCP 패킷 테이블

DHCP 메시지는 길이가 가변적이며 DHCP 패킷 테이블에 나열된 필드로 구성됩니다.

참고: 이 패킷은 원래 BootP 패킷의 수정된 버전입니다.

필드	바이트	이름	설명
운영	1	운영 코드	패킷을 요청 또는 회신으로 식별합니다. 1=BOOTREQUEST, 2=BOOTREPL
htype	1	하드웨어 유형	네트워크 하드웨어 주소 유형을 지정합니다.
hlen	1	하드웨어 길이	하드웨어 주소 길이의 길이를 지정합니다.
hlen	1	hlen	클라이언트는 값을 0으로 설정하고 요청이 라우터 전체에 전달될 경우 값이 증가합니다.
XID	4	거래 ID	클라이언트가 선택한 난수입니다. 지정된 DHCP 트랜잭션과 교환되는 모든 DHCP 메시지는 ID(xid)를 사용합니다.
초	2	초	DHCP 프로세스가 시작된 이후 시간(초)을 지정합니다.
플래그	2	플래그	메시지가 브로드캐스트인지 유니캐스트인지를 나타냅니다.
ciaddr	4	클라이언트 IP 주소	Bound, Renew 또는 Rebinding 상태의 경우와 마찬가지로 클라이언트가 IP 주소를 알고 있는 경우에만 사용됩니다.
이주소	4	IP 주소	클라이언트 IP 주소가 0.0.0.0이면 DHCP 서버는 제공된 클라이언트 IP 주소로 서버에 배치합니다.
주소	4	서버 IP 주소	클라이언트가 DHCP 서버의 IP 주소를 알고 있는 경우 이 필드는 DHCP 서버 주소로 채워집니다. 그렇지 않으면 DHCP 서버의 DHCP OFFER 및 DHCPACK에서

됩니다.

주소	4	라우터 IP 주소(GI 주소)	DHCP/BootP 릴레이 에이전트가 입력한 게이트웨이 IP 주소.
주소	16	클라이언트 MAC 주소	DHCP 클라이언트 MAC 주소.
성	64	서버 이름	선택적 서버 호스트 이름입니다.
파일	128	부팅 파일 이름	부트 파일 이름.
옵션	변수	옵션 매개변수	DHCP 서버에서 제공할 수 있는 선택적 매개변수. RFC 2132는 가능한 모든 옵션을 제공합니다.

클라이언트와 DHCP 서버가 동일한 서브넷에 있는 DHCP 주소를 가져오는 클라이언트에 대한 클라이언트-서버 대화

패킷 설명	소스 MAC 주소	대상 MAC 주소	소스 IP 주소	대상 IP 주소
DHCPDISCOVER	클라이언트	브로드캐스트	0.0.0.0	255.255.255.255
DHCPOFFER	DHCPServer	브로드캐스트	DHCPServer	255.255.255.255
DHCPREQUEST	클라이언트	브로드캐스트	0.0.0.0	255.255.255.255
DHCPACK	DHCPServer	브로드캐스트	DHCPServer	255.255.255.255

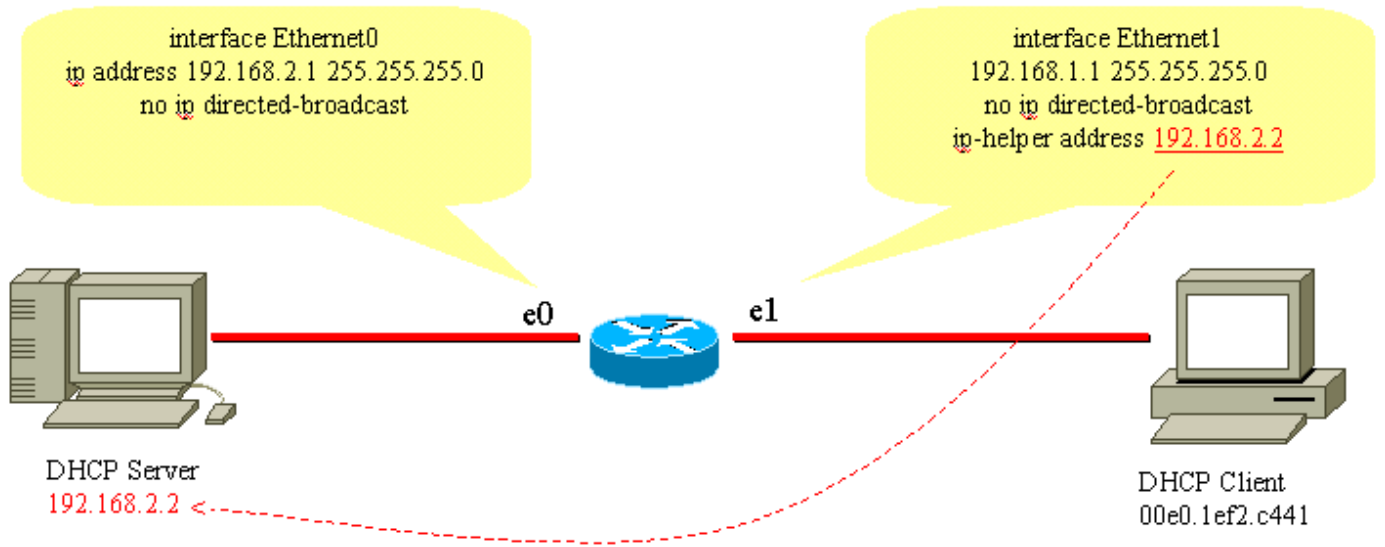
DHCP/BootP 릴레이 에이전트의 역할

기본적으로 라우터는 브로드캐스트 패킷을 전달하지 않습니다. DHCP 클라이언트 메시지는 255.255.255.255(모든 네트워크 브로드캐스트)의 대상 IP 주소를 사용하므로 DHCP 클라이언트는 라우터에 DHCP/BootP 릴레이 에이전트가 구성되어 있지 않으면 다른 서브넷의 DHCP 서버에 요청을 보낼 수 없습니다. DHCP/BootP 릴레이 에이전트는 DHCP 클라이언트를 대신하여 DHCP 요청을 DHCP 서버에 전달합니다. DHCP/BootP 릴레이 에이전트는 DHCP 서버로 이동하는 DHCP 프레임의 소스 IP 주소에 자체 IP 주소를 추가합니다. 이렇게 하면 DHCP 서버가 유니캐스트를 통해 DHCP/BootP 릴레이 에이전트에 응답할 수 있습니다. DHCP/BootP 릴레이 에이전트는 Gateway IP address 필드에도 클라이언트로부터 DHCP 메시지를 받은 인터페이스의 IP 주소를 채웁니다. DHCP 서버는 게이트웨이 IP 주소 필드를 사용하여 DHCPDISCOVER, DHCPREQUEST 또는 DHCPINFORM 메시지가 시작되는 서브넷을 결정합니다.

Cisco IOS® 라우터에서 DHCP/BootP 릴레이 에이전트 기능 구성

BootP 또는 DHCP 요청을 전달하도록 Cisco 라우터를 구성하는 프로세스는 간단합니다. DHCP/BootP 서버 또는 서버가 있는 네트워크의 서브넷 브로드캐스트 주소를 가리키는 IP 도우미 주소만 구성하면 됩니다.

네트워크 예:



DHCP/BootP 릴레이 에이전트

클라이언트에서 DHCP 서버로 BootP/DHCP 요청을 전달하려면 **ip helper-address interface** 명령을 사용합니다. IP helper-address는 UDP 포트 번호를 기반으로 임의의 UDP 브로드캐스트를 전달하도록 구성할 수 있습니다. 기본적으로 IP helper-address는 다음 UDP 브로드캐스트를 전달합니다.

- TFTP(Trivial File Transfer Protocol)(포트 69)
- DNS(포트 53), 시간 서비스(포트 37)
- NetBIOS 이름 서버(포트 137)
- NetBIOS 데이터그램 서버(포트 138)
- 부트 프로토콜(DHCP/BootP) 클라이언트 및 서버 데이터그램(포트 67 및 68)
- TACACS(Terminal Access Control Access Control Control System) 서비스(포트 49)
- IEN-116 이름 서비스(포트 42)

IP 헬퍼 주소는 유니캐스트 또는 브로드캐스트 IP 주소로 UDP 브로드캐스트를 전달할 수 있습니다. 그러나 발생할 수 있는 브로드캐스트 플러딩의 양이 많기 때문에 IP 헬퍼 주소를 사용하여 한 서브넷에서 다른 서브넷의 브로드캐스트 주소로 UDP 브로드캐스트를 전달하지 마십시오. 단일 인터페이스에서 여러 IP 헬퍼 주소 항목도 지원됩니다.

```

version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
!
interface Ethernet0
ip address 192.168.2.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet1
ip address 192.168.1.1 255.255.255.0
ip helper-address 192.168.2.2
ip helper-address 192.168.2.3

!--- IP helper-address pointing to DHCP server

```

```

no ip directed-broadcast
!
!
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
end

```

Cisco 라우터는 DHCP 릴레이 에이전트로 구성된 DHCP 서버의 로드 밸런싱을 지원하지 않습니다. Cisco 라우터는 해당 인터페이스에 대해 언급된 모든 헬퍼 주소에 DHCPDISCOVER 메시지를 전달합니다. 둘 이상의 DHCP 서버를 사용하여 서브넷을 제공하면 DHCPDISCOVER, DHCPOFFER 및 DHCPREQUEST/DHCPDENT 메시지가 각 쌍의 DHCP 클라이언트와 서버 간에 교환되므로 DHCP 트래픽만 증가합니다.

수동 바인딩 설정

수동 바인딩을 설정하는 방법에는 두 가지가 있습니다. 하나는 Windows 호스트용이고 다른 하나는 Windows 이외의 호스트용입니다. 구성하는 데 사용되는 두 가지 명령이 있습니다. 하나는 Microsoft DHCP 클라이언트용이고 다른 하나는 비 Microsoft DHCP 클라이언트용입니다. DHCPclient **-identifier**(manual binding - Microsoft DHCP clients) 및 DHCP**hardware-address**(manual binding - non-Microsoft DHCP clients). 두 가지 명령이 다른 이유는 Windows로 실행되는 PC가 MAC을 수정하고 주소 시작 부분에 01이 추가되기 때문입니다. 다음은 샘플 컨피그레이션입니다.

- Microsoft DHCP 클라이언트를 위한 컨피그레이션입니다.

```

configure terminal
ip dhcp pool new_pool
host ip_address subnet_mask
client-identifier 01XXXXXXXXXXXX

```

!--- xxxxxx represents 48 bit MAC address prepended with 01

- 비 Microsoft DHCP 클라이언트를 위한 컨피그레이션입니다.

```

configure terminal
ip dhcp pool new_pool
host ip_address subnet_mask
hardware-address XXXXXXXXXXXX

```

!--- xxxxxx represents 48 bit MAC address

보조 IP 세그먼트에서 DHCP가 작동하도록 하는 방법

기본적으로 DHCP는 기본 IP 주소로 구성된 인터페이스에서 요청을 받은 경우에만 응답 패킷이 전송된다는 제한이 있습니다. DHCP 트래픽은 브로드캐스트 주소를 사용합니다. 라우터 인터페이스에서 DHCP 요청을 받으면 DHCP 서버에 전달합니다(IP 헬퍼 주소가 구성된 경우). 이때 인터페이스에 기본 IP의 소스 주소가 구성되어 DHCP 서버가 DHCP 응답 패킷에서 (클라이언트에) 사용할 IP 풀을 알 수 있도록 합니다.

라우터가 DHCP 브로드캐스트 요청이 인터페이스에 구성된 보조 IP 네트워크에 있는 디바이스에서

오는 것인지 알 수 있는 방법은 없습니다. 이를 해결하려면 두 서브넷을 분리하기 위한 하위 인터페이스 컨피그레이션(라우터에 연결된 디바이스가 dot1q 태깅을 지원하는 경우)을 구성할 수 있으므로 두 디바이스 모두 해당 IP 주소를 올바르게 가져옵니다.

보조 주소가 기본 설정인 경우 다른 해결 방법이 있습니다. 이 방법은 전역 환경 설정 명령 `dhcp smart-relay`를 활성화하는 것입니다. 이는 기본 주소 풀에 대한 3회 연속 요청 후 DHCP 서버의 응답이 없는 경우 보조 IP만 사용하여 DHCP 요청을 릴레이한다는 제한점이 있습니다.

DHCP 릴레이 기능을 사용한 DHCP 클라이언트-서버 대화

다음 표에서는 DHCP 클라이언트가 DHCP 서버에서 IP 주소를 가져오는 프로세스를 보여줍니다. 이 테이블은 이전 Configure DHCP/BootP Relay Agent Feature 네트워크 다이어그램을 모델링한 것입니다. 다이어그램의 각 숫자 값은 다음 표에 설명된 패킷을 나타냅니다. 이 표를 사용하여 DHCP 클라이언트-서버 대화의 패킷 흐름을 이해할 수 있습니다. 또한 문제가 발생하는 위치를 확인하는 데 도움이 됩니다.

DHCP 클라이언트가 IP 주소를 가져오는 프로세스

패킷	클라이언트 IP 주소	서버 IP 주소	GI 주소	패킷 소스 주소	패킷 소스 MAC 주소	패킷 대상 IP 주소	패킷 대상 MAC 주소
1. DHCPDISCOVER가 클라이언트에서 전송됩니다.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640		0.0.0.0	ffff.ffff.ffff(브로드캐스트)
2. 라우터가 E1 인터페이스에서 DHCPDISCOVER를 수신합니다. 라우터는 이 패킷이 DHCP UDP 브로드캐스트임을 인식합니다. 이제 라우터가 DHCP/BootP 릴레이 에이전트 역할을 하며 게이트웨이 IP 주소 필드에 수신 인터페이스 IP 주소를 입력하고 소스 IP 주소를 수신 인터페이스 IP 주소로 변경한 다음 DHCP 서버에 직접 요청을 전달합니다.	0.0.0.0	0.0.0.0	192.168.1.1	인터페이스 E2 MAC 주소		192.168.1.1	DHCP 서버의 MAC 주소
3. DHCP 서버가 DHCPDISCOVER를 수신하고 DHCP 릴레이 에이전트에 DHCPOFFER를 보냅니다.	192.168.1.2	192.168.2.2	192.168.1.1	DHCP 서버의 MAC 주소		192.168.2.2	인터페이스 E2 주소
4. DHCP 릴레이 에이전트는 DHCPOFFER를 수	192.168.1.2	192.168.2.2	192.168.1.1	인터페이스 E1 MAC 주소		192.168.1.1	ffff.ffff.ffff(브로드캐스트)

신하고 로컬 LAN에서 DHCP OFFER 브로드캐스트를 전달합니다.

5. 고객으로부터 발송된

0.0.0.0 0.0.0.0 0.0.0.0 0005.DCC9.C640 0.0.0.0 ffff.ffff.ffff(브로드캐스트)

DHCPREQUEST

6. 라우터가 E1 인터페이스에서

DHCPREQUEST를 수신합니다. 라우터는 이 패킷이 DHCP UDP 브로드캐스트임을 인식합니다. 이제 라우터가 DHCP 릴레이 에이전트 역할을 하며 게이트웨이 IP 주소 필드에 보낸 인터페이스 IP 주소를 입력하고 소스 IP 주소를 들어오는 인터페이스 IP 주소로 변경한 다음 DHCP 서버에 직접 요청을 전달합니다.

0.0.0.0 0.0.0.0 192.168.1.1 인터페이스 E2 MAC 주소 192.168.1.1 DHCP 서버의 MAC 주소

7. DHCP 서버가 DHCPREQUEST를 받고 DHCP/BootP 릴레이 에이전트에 DHCPACK을 보냅니다.

192.168.1.2 192.168.2.2 192.168.1.1 DHCP 서버의 MAC 주소 192.168.2.2 인터페이스 E2 주소

8. DHCP/BootP 릴레이 에이전트는

DHCPACK을 수신하고 로컬 LAN에서 DHCPACK 브로드캐스트를 전달합니다. 클라이언트는 ACK를 수락하고 클라이언트 IP 주소를 사용합니다.

192.168.1.2 192.168.2.2 192.168.1.1 인터페이스 E1 MAC 주소 192.168.1.1 ffff.ffff.ffff(브로드캐스트)

PXE(Pre-Execution Environment) 부팅 DHCP 고려 사항

PXE(Pre-Execution Environment)를 사용하면 워크스테이션이 로컬 하드 드라이브에서 시스템을 부팅하기 전에 네트워크의 서버에서 부팅할 수 있습니다. 네트워크 관리자는 특정 워크스테이션을 직접 방문하여 수동으로 부팅할 필요가 없습니다. OS 및 기타 소프트웨어(예: 진단 프로그램)는 네트워크를 통해 서버에서 디바이스로 로드할 수 있습니다. PXE 환경은 DHCP를 사용하여 IP 주소를 구성합니다.

DHCP 서버가 네트워크의 다른 라우티드 세그먼트에 있는 경우 라우터에서 DHCP/BootP 릴레이 에이전트 컨피그레이션을 수행해야 합니다. 로컬 라우터 인터페이스에서 helper-address 명령을 구

성해야 합니다. 구성 정보는 [이 문서의 Cisco IOS 라우터에 DHCP/BootP 릴레이 에이전트 기능 구성 섹션을 참조하십시오.](#)

스니퍼 추적을 사용하여 DHCP 이해 및 문제 해결

동일한 LAN 세그먼트에서 DHCP 클라이언트 및 서버의 스니퍼 추적 디코딩

DHCP 클라이언트와 서버가 동일한 LAN 세그먼트에 상주하는 네트워크 토폴로지

스니퍼 추적 예는 6개의 프레임으로 구성됩니다. 이 6개의 프레임은 DHCP 클라이언트와 서버가 동일한 물리적 또는 논리적 세그먼트에 상주하는 시나리오를 보여줍니다. DHCP 문제를 해결하려면 다음 코드 예를 사용합니다. 스니퍼 추적을 이 예의 추적과 일치시키는 것이 중요합니다. 다음 그림에 표시된 추적과 비교하면 몇 가지 차이점이 있을 수 있지만, 일반적인 패킷 흐름은 정확히 동일해야 합니다. 패킷 추적은 DHCP가 작동하는 방식에 대한 이전 논의를 따릅니다.

```
----- Frame 1 - DHCPDISCOVER -----  
-----  
Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary  
1[0.0.0.0] [255.255.255.255] 618 0:01:26.810 0.575.244 05/07/2001 11:52:03 AM DHCP: Request,  
Message type: DHCP Discover  
DLC: ----- DLC Header -----  
DLC:  
DLC: Frame larrived at 11:52:03.8106; frame size is 618 (026A hex) bytes.  
DLC: Destination = BROADCAST FFFFFFFF, Broadcast  
DLC: Source = Station 0005DCC9C640  
DLC: Ethertype = 0800 (IP)  
DLC:  
IP: ----- IP Header -----  
IP:  
IP: Version = 4, header length = 20 bytes  
IP: Type of service = 00  
IP: 000. .... = routine  
IP: ...0 .... = normal delay  
IP: .... 0... = normal throughput  
IP: .... .0.. = normal reliability  
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit  
IP: .... ...0 = CE bit - no congestion  
IP: Total length = 604 bytes  
IP: Identification = 9  
IP: Flags = 0X  
IP: .0.. .... = may fragment  
IP: ..0. .... = last fragment  
IP: Fragment offset = 0 bytes  
IP: Time to live = 255 seconds/hops  
IP: Protocol = 17 (UDP)  
IP: Header checksum = B988 (correct)  
IP: Source address = [0.0.0.0]  
IP: Destination address = [255.255.255.255]  
IP: No options  
IP:  
UDP: ----- UDP Header -----  
UDP:  
UDP: Source port = 68 (BootPc/DHCP)  
UDP: Destination port = 67 (BootPs/DHCP)  
UDP: Length = 584  
UDP: No checksum
```

```

UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 0000882
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: Client hardware address = 0005DCC9C640
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303030352E646363392E633634302D564C31
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload = 3 (File and Sname fields hold options)
DHCP:

```

- - - - - **Frame 2 - DHCP OFFER** - - - - -

```

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2[192.168.1.1] [255.255.255.255] 331 0:01:26.825 0.015.172 05/07/2001 11:52:03 AM DHCP: Reply,
Message type: DHCP Offer
DLC: ----- DLC Header -----
DLC:
DLC: Frame 2 arrived at 11:52:03.8258; frame size is 331 (014B hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station 0005DCC42484
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 317 bytes
IP: Identification = 5
IP: Flags = 0X

```

IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F901 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = **67 (BootPs/DHCP)**
UDP: Destination port = **68 (BootPc/DHCP)**
UDP: Length = 297
UDP: No checksum
UDP: [289 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Address Renewal interval = 42767 (seconds)
DHCP: Address Rebinding interval = 74843 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.1.3]**
DHCP: **Domain Name Server address = [192.168.1.4]**
DHCP: **Gateway address = [192.168.1.1]**
DHCP:

- - - - - **Frame 3 - DHCPREQUEST** - - - - -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3[0.0.0.0] [255.255.255.255] 618 0:01:26.829 0.003.586 05/07/2001 11:52:03 AM DHCP: Request,
Message type: **DHCP Request**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 56 arrived at 11:52:03.8294; frame size is 618 (026A hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC9C640**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----

IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 10
IP: Flags = 0X
IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B987 (correct)
IP: **Source address = [0.0.0.0]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 68 (BootPc/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303030352E646363392E633634302D564C31**
DHCP: **Server IP address = [192.168.1.1]**
DHCP: **Request specific IP address = [192.168.1.2]**
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server

DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- - - - - **Frame 4 - DHCPACK** - - - - -
-

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4[192.168.1.1] [255.255.255.255] 331 0:01:26.844 0.014.658 05/07/2001 11:52:03 AM DHCP: Reply,

Message type: **DHCP Ack**

DLC: ----- DLC Header -----

DLC:

DLC: Frame 57 arrived at 11:52:03.8440; frame size is 331 (014B hex) bytes.

DLC: **Destination = BROADCAST FFFFFFFF**, Broadcast

DLC: **Source = Station 0005DCC42484**

DLC: Ethertype = 0800 (IP)

DLC:

IP: ----- IP Header -----

IP:

IP: Version = 4, header length = 20 bytes

IP: Type of service = 00

IP: 000. = routine

IP: ...0 = normal delay

IP: 0... = normal throughput

IP:0.. = normal reliability

IP:0. = ECT bit - transport protocol will ignore the CE bit

IP:0 = CE bit - no congestion

IP: Total length = 317 bytes

IP: Identification = 6

IP: Flags = 0X

IP: .0.. = may fragment

IP: ..0. = last fragment

IP: Fragment offset = 0 bytes

IP: Time to live = 255 seconds/hops

IP: Protocol = 17 (UDP)

IP: Header checksum = F900 (correct)

IP: **Source address = [192.168.1.1]**

IP: **Destination address = [255.255.255.255]**

IP: No options

IP:

UDP: ----- UDP Header -----

UDP:

UDP: **Source port = 67 (BootPs/DHCP)**

UDP: **Destination port = 68 (BootPc/DHCP)**

UDP: Length = 297

UDP: No checksum

UDP: [289 byte(s) of data]

UDP:

DHCP: ----- DHCP Header -----

DHCP:

DHCP: Boot record type = 2 (Reply)

DHCP: Hardware address type = 1 (10Mb Ethernet)

DHCP: Hardware address length = 6 bytes

DHCP:

DHCP: Hops = 0

DHCP: **Transaction id = 00000882**

DHCP: Elapsed boot time = 0 seconds

DHCP: Flags = 8000

DHCP: 1... = Broadcast IP datagrams

DHCP: Client self-assigned IP address = [0.0.0.0]

DHCP: **Client IP address = [192.168.1.2]**

DHCP: Next Server to use in bootstrap = [0.0.0.0]

DHCP: Relay Agent = [0.0.0.0]

DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 86400 (seconds)
DHCP: Address Renewal interval = 43200 (seconds)
DHCP: Address Rebinding interval = 75600 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.1.3]**
DHCP: **Domain Name Server address = [192.168.1.4]**
DHCP: **Gateway address = [192.168.1.1]**
DHCP:

- - - - - **Frame 5 - ARP** - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 0005DCC9C640 Broadcast 60 0:01:26.846 0.002.954 05/07/2001 11:52:03 AM ARP: R PA=[192.168.1.2]
HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 58 arrived at 11:52:03.8470; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:

- - - - - **Frame 6 - ARP** - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
6 0005DCC9C640 Broadcast 60 0:01:27.355 0.508.778 05/07/2001 11:52:04 AM ARP: R PA=[192.168.1.2]
HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 59 arrived at 11:52:04.3557; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640

ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:

DHCP 릴레이 에이전트로 구성된 라우터로 분리된 DHCP 클라이언트 및 서버의 스니퍼 추적 디코딩

스니퍼-B 추적

```
----- Frame 1 - DHCPDISCOVER -----  
-----  
Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary  
1 [0.0.0.0] [255.255.255.255] 618 0:02:05.759 0.025.369 05/31/2001 06:53:04 AM DHCP: Request,  
Message type: DHCP Discover  
DLC: ----- DLC Header -----  
DLC:  
DLC: Frame 124 arrived at 06:53:04.2043; frame size is 618 (026A hex) bytes.  
DLC: Destination = BROADCAST FFFFFFFF, Broadcast  
DLC: Source = Station 0005DCF2C441  
DLC: Ethertype = 0800 (IP)  
DLC:  
IP: ----- IP Header -----  
IP:  
IP: Version = 4, header length = 20 bytes  
IP: Type of service = 00  
IP: 000. .... = routine  
IP: ...0 .... = normal delay  
IP: .... 0... = normal throughput  
IP: .... .0.. = normal reliability  
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit  
IP: .... ...0 = CE bit - no congestion  
IP: Total length = 604 bytes  
IP: Identification = 183  
IP: Flags = 0X  
IP: .0.. .... = may fragment  
IP: ..0. .... = last fragment  
IP: Fragment offset = 0 bytes  
IP: Time to live = 255 seconds/hops  
IP: Protocol = 17 (UDP)  
IP: Header checksum = B8DA (correct)  
IP: Source address = [0.0.0.0]  
IP: Destination address = [255.255.255.255]  
IP: No options  
IP:  
UDP: ----- UDP Header -----  
UDP:  
UDP: Source port = 68 (BootPc/DHCP)  
UDP: Destination port = 67 (BootPs/DHCP)  
UDP: Length = 584  
UDP: No checksum  
UDP: [576 byte(s) of data]  
UDP:  
DHCP: ----- DHCP Header -----  
DHCP:  
DHCP: Boot record type = 1 (Request)  
DHCP: Hardware address type = 1 (10Mb Ethernet)  
DHCP: Hardware address length = 6 bytes
```

```

DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 00001425
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload = 3 (File and Sname fields hold options)
DHCP:

```

- - - - - **Frame 2 - DHCP OFFER** - - - - -
- -

```

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summaryr
125 [192.168.1.1] [255.255.255.255] 347 0:02:05.772 0.012.764 05/31/2001 06:53:04 AM DHCP:
Reply,

```

```

  Message type: DHCP Offer
DLC: ----- DLC Header -----
DLC:
DLC: Frame 125 arrived at 06:53:04.2171; frame size is 347 (015B hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station 003094248F71
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 45
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F8C9 (correct)

```

IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 68 (BootPc/DHCP)**
UDP: Length = 313
UDP: Checksum = 8517 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 99471 (seconds)
DHCP: Address Renewal interval = 49735 (seconds)
DHCP: Address Rebinding interval = 87037 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.10.1]**
DHCP: **Domain Name Server address = [192.168.10.2]**
DHCP: **NetBIOS Server address = [192.168.10.1]**
DHCP: **NetBIOS Server address = [192.168.10.3]**
DHCP: **Domain name = "cisco.com"**
DHCP:

----- **Frame 3 - DHCPREQUEST** -----

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3 [0.0.0.0] [255.255.255.255] 618 0:02:05.774 0.002.185 05/31/2001 06:53:04 AM DHCP: Request,
Message type: **DHCP Request**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 126 arrived at 06:53:04.2193; frame size is 618 (026A hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFF, Broadcast**
DLC: **Source = Station Cisc14F2C441**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine

IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 184
IP: Flags = 0X
IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B8D9 (correct)
IP: **Source address = [0.0.0.0]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 68 (BootPc/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30**
DHCP: **Server IP address = [192.168.2.2]**
DHCP: **Request specific IP address = [192.168.1.2]**
DHCP: Request IP address lease time = 99471 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload = 3 (File and Sname fields hold options)
DHCP:

- - - - - **Frame 4 - DHCPACK** - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4 [192.168.1.1] [255.255.255.255] 347 0:02:05.787 0.012.875 05/31/2001 06:53:04 AM DHCP: Reply,
Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 127 arrived at 06:53:04.2321; frame size is 347 (015B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFF, Broadcast**
DLC: **Source = Station 003094248F71**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 47
IP: Flags = 0X
IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F8C7 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 68 (BootPc/DHCP)**
UDP: Length = 313
UDP: Checksum = 326F (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""

DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172800 (seconds)
DHCP: Address Renewal interval = 86400 (seconds)
DHCP: Address Rebinding interval = 151200 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.10.1]**
DHCP: **Domain Name Server address = [192.168.10.2]**
DHCP: **NetBIOS Server address = [192.168.10.1]**
DHCP: **NetBIOS Server address = [192.168.10.3]**
DHCP: **Domain name = "cisco.com"**
DHCP:

- - - - - **Frame 5 - ARP** - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 Cisc14F2C441 Broadcast 60 0:02:05.798 0.011.763 05/31/2001 06:53:04 AM ARP: R PA=[192.168.1.2]
HA=Cisc14F2C441 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 128 arrived at 06:53:04.2439; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station Cisc14F2C441
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 00E01EF2C441
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:

- - - - - **Frame 6 - ARP** - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 Cisc14F2C441 Broadcast 60 0:02:05.798 0.011.763 05/31/2001 06:53:04 AM ARP: R PA=[192.168.1.2]
HA=Cisc14F2C441 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 128 arrived at 06:53:04.2439; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station Cisc14F2C441
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 00E01EF2C441
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFF

ARP: Target protocol address = [192.168.1.2]

ARP:

ARP: 18 bytes frame padding

ARP:

스니퍼-A 추적

- - - - - **Frame 1 - DHCPDISCOVER** - - - - -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
118 [192.168.1.1] [192.168.2.2] 618 0:00:51.212 0.489.912 05/31/2001 07:02:54 AM DHCP: Request,
Message type: DHCP Discover

DLC: ----- DLC Header -----

DLC:

DLC: Frame 118 arrived at 07:02:54.7463; frame size is 618 (026A hex) bytes.

DLC: **Destination = Station 0005DC0BF2F4**

DLC: **Source = Station 003094248F72**

DLC: Ethertype = 0800 (IP)

DLC:

IP: ----- IP Header -----

IP:

IP: Version = 4, header length = 20 bytes

IP: Type of service = 00

IP: 000. = routine

IP: ...0 = normal delay

IP: 0... = normal throughput

IP:0.. = normal reliability

IP:0. = ECT bit - transport protocol will ignore the CE bit

IP:0 = CE bit - no congestion

IP: Total length = 604 bytes

IP: Identification = 52

IP: Flags = 0X

IP: .0.. = may fragment

IP: ..0. = last fragment

IP: Fragment offset = 0 bytes

IP: Time to live = 255 seconds/hops

IP: Protocol = 17 (UDP)

IP: Header checksum = 3509 (correct)

IP: **Source address = [192.168.1.1]**

IP: **Destination address = [192.168.2.2]**

IP: No options

IP:

UDP: ----- UDP Header -----

UDP:

UDP: **Source port = 67 (BootPs/DHCP)**

UDP: **Destination port = 67 (BootPs/DHCP)**

UDP: Length = 584

UDP: Checksum = 0A19 (correct)

UDP: [576 byte(s) of data]

UDP:

DHCP: ----- DHCP Header -----

DHCP:

DHCP: Boot record type = 1 (Request)

DHCP: Hardware address type = 1 (10Mb Ethernet)

DHCP: Hardware address length = 6 bytes

DHCP:

DHCP: Hops = 1

DHCP: Transaction id = 000005F4

DHCP: Elapsed boot time = 0 seconds

DHCP: Flags = 8000

DHCP: 1... = Broadcast IP datagrams

DHCP: Client self-assigned IP address = [0.0.0.0]

DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload = 3 (File and Sname fields hold options)
DHCP:

- - - - - **Frame 2 - DHCP OFFER** - - - - -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2 [192.168.2.2] [192.168.1.1] 347 0:00:51.214 0.002.133 05/31/2001 07:02:54 AM DHCP: Request,
Message type: **DHCP Offer**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 119 arrived at 07:02:54.7485; frame size is 347 (015B hex) bytes.
DLC: **Destination = Station 003094248F72**
DLC: **Source = Station 0005DC0BF2F4**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 41
IP: Flags = 0X
IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3623 (correct)
IP: **Source address = [192.168.2.2]**
IP: **Destination address = [192.168.1.1]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**

```

UDP: Length = 313
UDP: Checksum = A1F8 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172571 (seconds)
DHCP: Address Renewal interval = 86285 (seconds)
DHCP: Address Rebinding interval = 150999 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:

```

- - - - - **Frame 3 - DHCPREQUEST** - - - - -

```

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3 [192.168.1.1] [192.168.2.2] 618 0:00:51.240 0.025.974 05/31/2001 07:02:54 AM DHCP: Request,
  Message type: DHCP Request
DLC: ----- DLC Header -----
DLC:
DLC: Frame 120 arrived at 07:02:54.7745; frame size is 618 (026A hex) bytes.
DLC: Destination = Station 0005DC0BF2F4
DLC: Source = Station 003094248F72
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 54
IP: Flags = 0X

```

```

IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3507 (correct)
IP: Source address = [192.168.1.1]
IP: Destination address = [192.168.2.2]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: Checksum = 4699 (correct)
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 1
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Server IP address = [192.168.2.2]
DHCP: Request specific IP address = [192.168.1.2]
DHCP: Request IP address lease time = 172571 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload = 3 (File and Sname fields hold options)
DHCP:

```

- - - - - **Frame 4 - DHCPACK** - - - - -

```

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4 [192.168.2.2] [192.168.1.1] 347 0:00:51.240 0.000.153 05/31/2001 07:02:54 AM DHCP: Request,
  Message type: DHCP Ack
DLC: ----- DLC Header -----

```

DLC:

DLC: Frame 121 arrived at 07:02:54.7746; frame size is 347 (015B hex) bytes.

DLC: **Destination = Station 003094248F72**

DLC: **Source = Station 0005DC0BF2F4**

DLC: Ethertype = 0800 (IP)

DLC:

IP: ----- IP Header -----

IP:

IP: Version = 4, header length = 20 bytes

IP: Type of service = 00

IP: 000. = routine

IP: ...0 = normal delay

IP: 0... = normal throughput

IP:0.. = normal reliability

IP:0. = ECT bit - transport protocol will ignore the CE bit

IP:0 = CE bit - no congestion

IP: Total length = 333 bytes

IP: Identification = 42

IP: Flags = 0X

IP: .0.. = may fragment

IP: ..0. = last fragment

IP: Fragment offset = 0 bytes

IP: Time to live = 255 seconds/hops

IP: Protocol = 17 (UDP)

IP: Header checksum = 3622 (correct)

IP: **Source address = [192.168.2.2]**

IP: **Destination address = [192.168.1.1]**

IP: No options

IP:

UDP: ----- UDP Header -----

UDP:

UDP: **Source port = 67 (BootPs/DHCP)**

UDP: **Destination port = 67 (BootPs/DHCP)**

UDP: Length = 313

UDP: Checksum = 7DF6 (correct)

UDP: [305 byte(s) of data]

UDP:

DHCP: ----- DHCP Header -----

DHCP:

DHCP: Boot record type = 2 (Request)

DHCP: Hardware address type = 1 (10Mb Ethernet)

DHCP: Hardware address length = 6 bytes

DHCP:

DHCP: Hops = 0

DHCP: Transaction id = 000005F4

DHCP: Elapsed boot time = 0 seconds

DHCP: Flags = 8000

DHCP: 1... = Broadcast IP datagrams

DHCP: Client self-assigned IP address = [0.0.0.0]

DHCP: Client IP address = [192.168.1.2]

DHCP: Next Server to use in bootstrap = [0.0.0.0]

DHCP: **Relay Agent = [192.168.1.1]**

DHCP: **Client hardware address = 0005DCF2C441**

DHCP:

DHCP: Host name = ""

DHCP: Boot file name = ""

DHCP:

DHCP: Vendor Information tag = 63825363

DHCP: Message Type = 5 (DHCP Ack)

DHCP: Server IP address = [192.168.2.2]

DHCP: Request IP address lease time = 172800 (seconds)

DHCP: Address Renewal interval = 86400 (seconds)

DHCP: Address Rebinding interval = 151200 (seconds)

DHCP: Subnet mask = [255.255.255.0]

DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:

클라이언트 워크스테이션이 DHCP 주소를 가져올 수 없을 때 DHCP 문제 해결

고객 사례 #1: DHCP 클라이언트와 동일한 LAN 세그먼트 또는 VLAN의 DHCP 서버

DHCP 서버와 클라이언트가 동일한 LAN 세그먼트 또는 VLAN에 있고 클라이언트가 DHCP 서버에서 IP 주소를 가져올 수 없는 경우. 그러나 로컬 라우터가 DHCP 문제를 일으킬 가능성은 낮습니다. 이 문제는 DHCP 서버와 DHCP 클라이언트를 연결하는 디바이스와 관련이 있습니다. 그러나 DHCP 서버 또는 클라이언트 자체에 문제가 있을 수 있습니다. 이러한 모듈은 문제를 해결하는 데 도움이 되며 어떤 장치에서 문제가 발생하는지 확인할 수 있습니다.

참고: VLAN별로 DHCP 서버를 구성하려면 클라이언트에 DHCP 주소를 제공하는 모든 VLAN에 대해 서로 다른 DHCP 풀을 정의합니다.

고객 사례 #2: DHCP 서버 및 DHCP 클라이언트는 DHCP/BootP 릴레이 에이전트 기능을 위해 구성된 라우터로 구분됩니다

DHCP 서버와 클라이언트가 서로 다른 LAN 세그먼트 또는 VLAN에 있는 경우 라우터는 DHCP 서버에 DHCPREQUEST를 전달하는 DHCP/BootP 릴레이 에이전트 역할을 합니다. DHCP/BootP 릴레이 에이전트 및 DHCP 서버와 클라이언트의 문제를 해결하려면 추가 단계가 필요합니다. 이러한 모듈을 따르는 경우 어떤 디바이스에서 문제가 발생하는지 확인할 수 있습니다.

DHCP Server on Router Fails Fails(라우터의 DHCP 서버가 주소 할당에 실패함) - POOL EXHAUSTED(풀 사용) 오류

풀에서 해제되더라도 일부 주소가 여전히 클라이언트에 보유될 수 있습니다. 이는 show ip dhcp conflictoutput으로 확인할 수 있습니다. 두 호스트가 동일한 IP 주소를 사용할 경우 주소 충돌이 발생합니다. 주소 할당 시 DHCP는 ping 및 불필요한 ARP와의 충돌을 확인합니다.

충돌이 감지되면 해당 주소가 풀에서 제거됩니다. 관리자가 충돌을 해결할 때까지 주소가 할당됩니다. 이 문제를 해결하려면 ip dhcp 충돌 로깅을 구성합니다.

DHCP 문제 해결 모듈

DHCP 문제가 발생할 수 있는 위치 이해

DHCP 문제는 많은 이유로 인해 발생할 수 있습니다. 가장 일반적인 이유는 구성 문제입니다. 그러나 많은 DHCP 문제는 시스템, NIC(Network Interface Card) 드라이버 또는 라우터에서 실행되는 DHCP/BootP 릴레이 에이전트의 소프트웨어 결함으로 인해 발생할 수 있습니다. 문제가 될 수 있는 영역의 수로 인해 체계적인 문제해결 접근이 필요하다.

DHCP 문제의 가능한 원인 짧은 목록:

- Catalyst 스위치 기본 컨피그레이션
- DHCP/BootP 릴레이 에이전트 구성
- NIC 호환성 문제 또는 DHCP 기능 문제
- NIC 오류 또는 잘못된 NIC 드라이버 설치
- 스페닝 트리의 잘못된 계산으로 인한 간헐적인 네트워크 중단
- 운영 체제 동작 또는 소프트웨어 결함
- DHCP 서버 범위 구성 또는 소프트웨어 결함
- Cisco Catalyst 스위치 또는 Cisco IOS DHCP/BootP Relay Agent 소프트웨어 결함
- DHCP 제안이 예상과 다른 인터페이스에서 수신되었기 때문에 uRPF(Unicast Reverse Path Forwarding) 확인에 실패했습니다. 인터페이스에서 RPF(Reverse Path Forwarding) 기능이 활성화된 경우 Cisco 라우터는 소스 주소가 0.0.0.0이고 목적지 주소가 255.255.255.255인 DHCP(Dynamic Host Configuration Protocol) 및 BOOTP(BOOTstrap Protocol) 패킷을 삭제할 수 있습니다. 또한 라우터는 인터페이스에 멀티캐스트 IP 대상이 있는 모든 IP 패킷을 삭제할 수 있습니다. 이 문제는 Cisco 버그 ID CSCdw에 [문서화되어 있습니다31925](#)

참고 등록된 Cisco 클라이언트만 버그 보고서에 액세스할 수 있습니다.

- DHCP 데이터베이스 에이전트는 사용되지 않지만 DHCP 충돌 로깅은 비활성화되지 않습니다

A. 물리적 연결 확인

이 절차는 모든 사례 연구에 적용됩니다.

먼저 DHCP 클라이언트 및 서버의 물리적 연결을 확인합니다. Catalyst 스위치에 연결된 경우 DHCP 클라이언트와 서버가 모두 물리적으로 연결되어 있는지 확인하십시오. Catalyst 2900XL/3500XL/2950/3550과 같은 Cisco IOS 기반 스위치의 경우 **포트 상태를 표시하는** 해당 명령 인터페이스 **<interface>**를 **표시합니다**. 인터페이스의 상태가 <interface>가 아닌 다른 경우 회선 프로토콜이 작동하면 포트가 트래픽을 전달하지 않고 DHCP 클라이언트 요청도 전달하지 않습니다. 명령의 출력:

```
Switch#show interface fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0030.94dc.acc1 (bia 0030.94dc.acc1)
```

물리적 연결이 확인되었고 Catalyst 스위치와 DHCP 클라이언트 간에 링크가 없는 경우 [Cisco Catalyst Switches to NIC Compatibility Issues](#)(Cisco Catalyst 스위치에서 [NIC 호환성 문제 해결](#)) [섹션](#)을 사용하여 물리적 레이어 연결 문제와 관련된 문제를 해결하십시오.

과도한 데이터 링크 오류로 인해 일부 Catalyst 스위치의 포트가 errdisabled 상태로 전환됩니다. 자세한 내용은 [errdisable 상태를 설명하는 Cisco IOS 플랫폼의 Errdisable Port State Recovery](#)를 참조하고, 이 상태에서 복구하는 방법을 설명하며, 이 상태로부터의 복구 예를 제공합니다.

B. 네트워크 연결을 테스트하도록 클라이언트 워크스테이션 및 고정 IP를 구성합니다

이 절차는 모든 사례 연구에 적용됩니다.

DHCP 문제를 해결할 때 네트워크 연결을 확인하려면 클라이언트 워크스테이션에서 고정 IP 주소를 구성하는 것이 중요합니다. 워크스테이션에 정적으로 구성된 IP 주소가 있지만 네트워크 리소스에 연결할 수 없는 경우 문제의 근본 원인은 DHCP가 아닙니다. 이때 네트워크 연결 문제를 해결해야 합니다.

C. 시작 문제로 확인

이 절차는 모든 사례 연구에 적용됩니다.

DHCP 클라이언트가 시작할 때 DHCP 서버에서 IP 주소를 가져올 수 없는 경우, 수동으로 클라이언트에 DHCP 요청을 보내도록 강제할 수 있습니다. 나열된 OS에 대해 DHCP 서버에서 IP 주소를 수동으로 가져오려면 다음 단계를 수행합니다.

Microsoft Windows 95/98/ME:

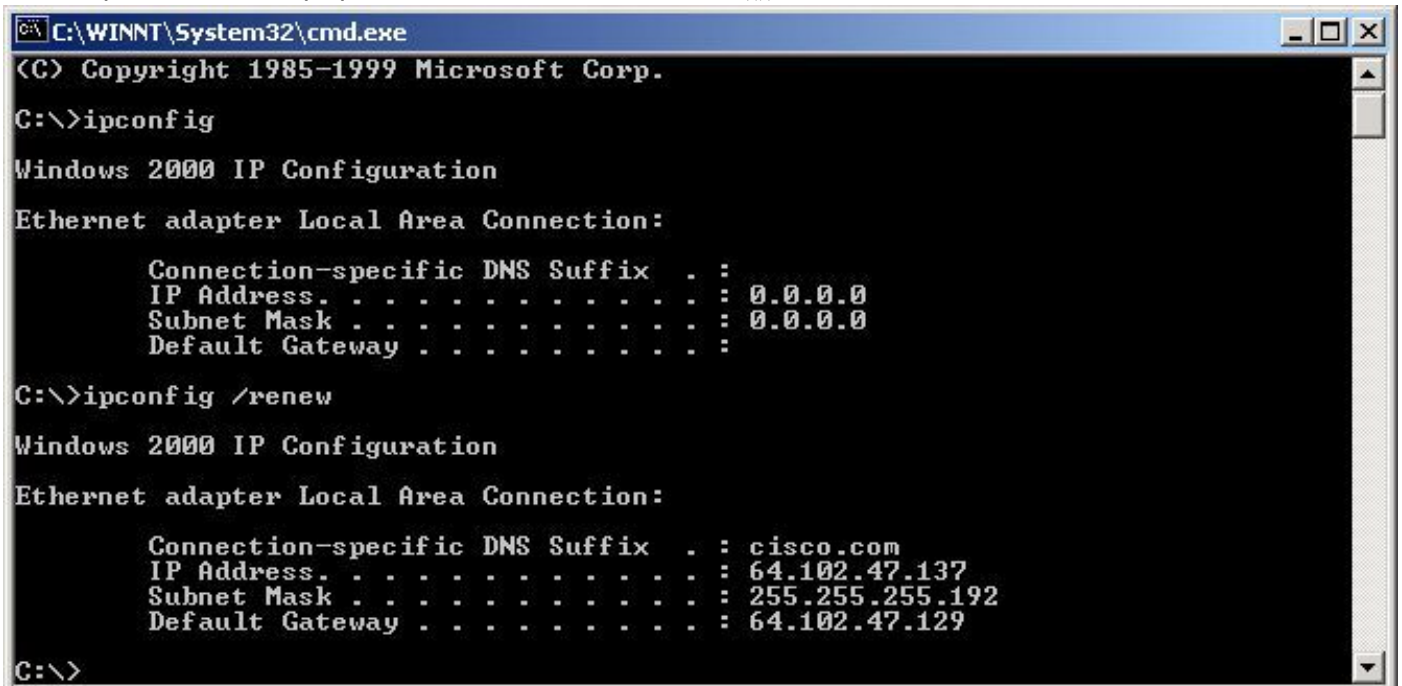
1. Startbutton을 클릭하고 WINIPCFG.exe 프로그램을 실행합니다.
2. Release Allbutton을 클릭한 다음 Renew Allbutton을 클릭합니다.
3. 이제 DHCP 클라이언트가 IP 주소를 가져올 수 있습니까?



IP Configuration(IP 컨피그레이션) 창

Microsoft Windows NT/2000:

1. 명령 프롬프트 창을 열려면 Start/Runfield 필드에 cmd를 입력합니다.
2. 명령 프롬프트 창에서 commandipconfig/renewal을 실행합니다.
3. 이제 DHCP 클라이언트가 IP 주소를 가져올 수 있습니까?



명령줄 프롬프트

PC가 부팅 프로세스를 완료한 후 DHCP 클라이언트가 IP 주소를 수동으로 갱신하여 IP 주소를 가져올 수 있는 경우, DHCP 시작 문제일 가능성이 높습니다. DHCP 클라이언트가 Cisco Catalyst 스위치에 연결된 경우 STP 포트패스트 및/또는 채널링 및 트렁킹을 처리하는 컨피그레이션 문제로 인해 문제가 발생할 가능성이 높습니다. 그 밖에도 NIC 카드 문제 및 스위치 포트 시작 문제가 발생할 수 있습니다. DHCP 문제의 근본 원인으로 스위치 포트 컨피그레이션 및 NIC 카드 문제를 배제하려면 D단계와 E단계를 검토하십시오.

D. 스위치 포트 구성 확인(STP Portfast 및 기타 명령)

스위치가 Catalyst 2900/4000/5000/6000인 경우, 이 포트에서 STP 포트패스가 활성화되고 트렁킹/채널링이 비활성화되었는지 확인합니다. 기본 컨피그레이션은 STP portfast disabled 및 자동 트렁킹/채널링입니다(해당되는 경우). 2900XL/3500XL/2950/3550 스위치의 경우 STP portfast가 유일한 필수 구성입니다. 이러한 컨피그레이션 변경은 Catalyst 스위치의 초기 설치에서 발생하는 가장 일반적인 DHCP 클라이언트 문제를 해결합니다.

Catalyst 스위치에 연결할 때 DHCP가 제대로 작동하는 데 필요한 스위치 포트 구성 요구 사항에 대한 자세한 내용은 Portfast [및 기타 명령을 사용하여 워크스테이션 시작 연결 지연을 해결하십시오.](#)

해당 문서를 검토한 후 계속해서 이러한 문제를 해결할 수 있습니다.

E. 알려진 NIC 카드 또는 Catalyst 스위치 문제 확인

Catalyst 스위치 컨피그레이션이 올바르면 Catalyst 스위치 또는 DHCP 클라이언트 NIC에 DHCP 문제를 일으킬 수 있는 소프트웨어 호환성 문제가 있을 수 있습니다. 트러블슈팅의 다음 단계는 Troubleshooting [Cisco Catalyst Switches to NIC Compatibility Issues\(Cisco Catalyst 스위치에서 NIC 호환성 문제](#)로 트러블슈팅)를 검토하고 문제의 원인이 되는 Catalyst 스위치 또는 NIC의 소프트웨어 문제를 배제하는 것입니다.

호환성 문제를 제대로 배제하려면 DHCP 클라이언트 OS는 물론 제조업체, 모델, 드라이버 버전과 같은 특정 NIC 정보를 알아야 합니다.

F. DHCP 클라이언트가 DHCP 서버와 동일한 서브넷 또는 VLAN에서 IP 주소를 얻는지 여부를 구별합니다

클라이언트가 DHCP 서버와 동일한 서브넷 또는 VLAN에 있을 때 DHCP가 올바르게 작동하는지 여부를 구분하는 것이 중요합니다. DHCP가 DHCP 서버와 동일한 서브넷 또는 VLAN에서 올바르게 작동하는 경우 DHCP 문제는 대부분 DHCP/BootP 릴레이 에이전트 때문에 발생합니다. DHCP 서버와 동일한 서브넷 또는 VLAN에서 DHCP를 테스트할 때도 문제가 지속되면 실제로 DHCP 서버에서 문제가 발생할 수 있습니다.

G. 라우터 DHCP/BootP 릴레이 컨피그레이션 확인

컨피그레이션을 확인하려면

1. 라우터에서 DHCP 릴레이를 구성할 때 **helper-addresscommand**가 올바른 인터페이스에 있는지 확인합니다. **Eip helper-addresscommand**는 DHCP 클라이언트 워크스테이션의 인바운드 인터페이스에 있어야 하며 올바른 DHCP 서버로 전달되어야 합니다.
2. 글로벌 컨피그레이션 명령 **no service dhcp**이 없는지 확인합니다. 이 컨피그레이션 매개변수는 라우터의 모든 DHCP 서버 및 릴레이 기능을 비활성화합니다. 기본 컨피그레이션, **service dhcp**는 컨피그레이션에 나타나지 않으며 기본 컨피그레이션 명령입니다. **서비스 dhcp**가 활성화

화되지 않으면 클라이언트는 DHCP 서버에서 IP 주소를 수신하지 않습니다.참고: 이전 Cisco IOS 릴리스를 실행하는 라우터에서 **ip bootp server** 명령은 **service dhcp** 명령 대신 DHCP 릴레이 에이전트 기능을 처리합니다. 따라서 **ip helper-address** 명령이 DHCP UDP 브로드캐스트를 전달하고 DHCP 클라이언트 대신 DHCP 릴레이 에이전트로 제대로 작동하도록 구성된 경우 이러한 라우터에서 **ip bootp server** 명령을 활성화해야 합니다.

3. **ip helper-address** 명령을 사용하여 UDP 브로드캐스트를 서브넷 브로드캐스트 주소로 전달할 경우 다음을 확인합니다. **no ip directed-broadcast** UDP 브로드캐스트 패킷이 통과해야 하는 아웃바운드 인터페이스에 구성되지 않았습니. 이 **no ip directed-broadcast** 물리적 브로드캐스트로 직접 브로드캐스트의 변환을 차단합니다. 이 인터페이스 컨피그레이션은 소프트웨어 버전 12.0 이상에서 기본 컨피그레이션입니다.
4. DHCP 브로드캐스트가 DHCP 서버 서브넷 브로드캐스트 주소로 전달되면 소프트웨어 문제가 발생할 수 있습니다. DHCP 문제를 해결할 때 DHCP UDP 브로드캐스트를 DHCP 서버 IP 주소로 전달하려고 합니다.

H. 가입자 식별(82) 옵션 설정

DHCP 릴레이 에이전트 정보(옵션 82) 기능을 사용하면 DHCP 릴레이 에이전트(Catalyst 스위치)가 DHCP 클라이언트에서 DHCP 서버로 DHCP 요청을 전달할 때 자신과 연결된 클라이언트에 대한 정보를 포함할 수 있습니다.

DHCP 서버는 이 정보를 사용하여 통신 사업자 네트워크의 각 가입자에 대해 IP 주소를 할당하고, 액세스 제어를 수행하고, QoS(Quality of Service) 및 보안 정책(또는 기타 매개변수 할당 정책)을 설정할 수 있습니다. 스위치에서 DHCP 스누핑이 활성화되면 옵션 82가 자동으로 활성화됩니다. DHCP 서버가 옵션 82로 패킷을 처리하도록 구성되지 않은 경우 해당 요청에 주소를 할당하는 것이 중단됩니다. 이 문제를 해결하려면 전역 구성 명령 **no ip dhcp relay information** 옵션을 사용하여 스위치(릴레이 에이전트)에서 가입자 식별 옵션 82를 비활성화하십시오.

I. DHCP 데이터베이스 에이전트 및 DHCP 충돌 로깅

DHCP 데이터베이스 에이전트는 DHCP 바인딩 데이터베이스를 저장하는 모든 호스트(예: FTP, TFTP 또는 RCP 서버)입니다. 여러 DHCP 데이터베이스 에이전트를 구성할 수 있으며, 각 에이전트에 대해 데이터베이스 업데이트와 전송 사이의 간격을 구성할 수 있습니다. **dhcp database** 명령을 사용하여 데이터베이스 에이전트 및 데이터베이스 에이전트 매개변수를 구성합니다.

DHCP 데이터베이스 에이전트를 구성하지 않도록 선택하는 경우 DHCP 서버에서 DHCP 주소 충돌의 기록을 비활성화합니다. **theno ip dhcp conflict logging** 명령을 실행하여 DHCP 주소 충돌 로깅을 비활성화합니다. **clear ip dhcp conflict(ip dhcp 충돌 지우기)**를 사용하여 이전에 로깅한 충돌을 지웁니다.

충돌 로깅을 비활성화하지 못하면 다음 오류 메시지가 나타납니다.

```
%DHCPD-4-DECLINE_CONFLICT: DHCP address conflict: client
```

J. IP 전화 연결에 대한 CDP 확인

Cisco IP Phone에 연결된 스위치 포트에서 CDP(Cisco Discovery Protocol)가 비활성화된 경우 DHCP 서버는 해당 IP 주소를 전화기에 할당할 수 없습니다. DHCP 서버는 스위치 포트의 데이터 VLAN / 서브넷에 속하는 IP 주소를 할당하는 경향이 있습니다. CDP가 활성화된 경우 스위치는 Cisco IP Phone에서 DHCP를 요청하는 것을 감지하고 올바른 서브넷 정보를 제공할 수 있습니다. 그러면 DHCP 서버가 음성 VLAN/서브넷 풀에서 IP 주소를 할당할 수 있습니다. 음성 VLAN에 **dhcp**

서비스를 바인딩하는 데 필요한 명시적 단계는 없습니다.

K. Remove Down SVI Disrupts DHCP Snooping Operation(SVI가 DHCP 스누핑 작업을 중단합니다)

Cisco Catalyst 6500 Series 스위치에서 특정 VLAN을 스누핑하도록 DHCP를 구성한 후 SVI(종료 상태)가 자동으로 생성됩니다. 이 SVI의 존재는 DHCP 스누핑의 올바른 작동에 직접적인 영향을 미칩니다.

네이티브 Cisco IOS를 실행하는 Cisco Catalyst 6500 Series 스위치의 DHCP 스누핑은 스위치 프로세서(SP 또는 슈퍼바이저)가 아니라 주로 RP 또는 MSFC(Route Processor)에서 구현됩니다. Cisco Catalyst 6500 Series는 RP가 가입한 LTL(Local Target Logic)에 패킷을 제공하는 VACL을 사용하여 하드웨어에서 패킷을 가로챍니다. 프레임이 RP에 진입하면 먼저 SVI(L3 Interface) IDB와 연결해야 스누핑 부분으로 전달될 수 있습니다. SVI가 없으면 이 IDB가 없으며 패킷이 RP에서 삭제됩니다.

L. 제한된 브로드캐스트 주소

DHCP 클라이언트가 DHCP 패킷에서 브로드캐스트 비트를 설정하면 DHCP 서버 및 릴레이 에이전트는 올원 브로드캐스트 주소(255.255.255.255)를 사용하여 클라이언트에 DHCP 메시지를 보냅니다. 네트워크 브로드캐스트를 전송하도록 broadcast-address 명령을 구성한 경우 DHCP가 전송한 올원(all-one) 브로드캐스트가 재정의됩니다. 이 상황을 해결하려면 dhcp limited-broadcast-address 명령을 사용하여 구성된 네트워크 브로드캐스트가 기본 DHCP 동작을 재정의하지 않도록 합니다.

일부 DHCP 클라이언트는 올원 브로드캐스트만 수락할 수 있으며 이 명령이 클라이언트에 연결된 라우터 인터페이스에 구성되어 있지 않으면 DHCP 주소를 획득할 수 없습니다.

M. 라우터 디버그 명령을 사용하여 DHCP 디버그

라우터가 debug 명령을 사용하여 DHCP 요청을 수신하는지 확인

DHCP 패킷을 처리하는 소프트웨어를 지원하는 라우터에서 라우터가 클라이언트로부터 DHCP 요청을 받는지 확인할 수 있습니다. 라우터가 클라이언트로부터 요청을 받지 못하면 DHCP 프로세스가 실패합니다. 이 단계에서는 출력을 디버깅할 access-list를 구성합니다. 이 access-list는 명령을 디버깅하는 데만 사용되며 라우터에 침입하지 않습니다.

글로벌 컨피그레이션 모드에서 다음 access-list를 입력합니다.

```
access-list 100 permit ip host 0.0.0.0 host 255.255.255.255
```

exec 모드에서 다음 debug 명령을 입력합니다.

```
debug ip packet detail 100
```

샘플 출력

```
Router#debug ip packet detail 100
IP packet debugging is on (detailed) for access list 100
Router#
```

```
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
```

이 출력 예에서는 라우터가 클라이언트로부터 DHCP 요청을 능동적으로 수신한다는 것이 분명합니다. 이 출력은 패킷의 요약만 표시하고 패킷 자체는 표시하지 않습니다. 따라서 패킷이 정확한지 확인할 수 없습니다. 그럼에도 불구하고 라우터는 소스 및 대상 IP와 UDP 포트가 있는 브로드캐스트 패킷을 DHCP에 맞게 수신했습니다.

라우터가 debug ip udp 명령을 사용하여 DHCP 요청을 수신하고 전달하는지 확인

debug ip udp 명령은 라우터를 통해 DHCP 요청의 경로를 추적할 수 있습니다. 그러나 처리된 모든 스위치드 UDP 패킷이 콘솔에 표시되므로 프로덕션 환경에서는 이 디버그가 방해가 됩니다. 이 debug 명령은 프로덕션에서 사용할 수 없습니다.

경고: debug ip udp 명령은 침입적이며 CPU(Central Processing Unit) 사용률이 높을 수 있습니다.

exec 모드에서 debug 명령 debug ip udp를 입력합니다.

샘플 출력

```
Router#debug ip udp
UDP packet debugging is on
Router#

00:18:48: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584

!--- Router receiving DHCPDISCOVER from DHCP client.

00:18:48: UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604

!--- Router forwarding DHCPDISCOVER unicast to DHCP server using DHCP/BootP Relay Agent source IP address.

00:18:48: UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=313

!--- Router receiving DHCPPOFFER from DHCP server directed to DHCP/BootP Relay Agent IP address.

00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=333

!--- Router forwarding DHCPPOFFER from DHCP server to DHCP client via DHCP/BootP Relay Agent.

00:18:48: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584

!--- Router receiving DHCPREQUEST from DHCP client.

00:18:48: UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604

!--- Router forwarding DHCPDISCOVER unicast to DHCP server using DHCP/BootP Relay Agent source IP address.

00:18:48: UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=313

!--- Router receiving DHCPACK (or DHCPNAK) from DHCP directed to DHCP/BootP Relay Agent IP
```

address.

00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=333

!--- Router forwarding DHCPACK (or DHCPNAK) to DHCP client via DHCP/BootP Relay Agent.

00:18:48: UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32

!--- DHCP client verifying IP address not in use by sending ARP request for its own IP address.

00:18:50: UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32

!--- DHCP client verifying IP address not in use by sending ARP request for its own IP address.

라우터가 debug ip dhcp server packet 명령을 사용하여 DHCP 요청을 수신하고 전달하는지 확인

라우터 Cisco IOS가 12.0.x.T 또는 12.1이고 Cisco IOS DHCP 서버 기능을 지원하는 경우 debug ip dhcp server packet 명령을 사용할 수 있습니다. 이 디버그는 IOS DHCP 서버 기능과 함께 사용하고 DHCP/BootP 릴레이 에이전트 기능의 트러블슈팅도 수행하기 위한 것입니다. 이전 단계와 마찬가지로 라우터 디버그는 실제 패킷을 볼 수 없으므로 문제에 대한 정확한 결정을 제공하지 않습니다. 그러나 디버그를 사용하면 DHCP 처리와 관련하여 추론을 수행할 수 있습니다. EXEC 모드에서 다음 debug 명령을 입력합니다.

ip dhcp 서버 패킷 디버그

```
Router#debug ip dhcp server packet
```

```
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
```

```
!--- Router received DHCPDISCOVER/REQUEST/INFORM and setting Gateway IP address to 192.168.1.1 for forwarding.
```

```
00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..
```

```
!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM.
```

```
!--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier.
```

```
00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441.
```

```
!--- BOOTREPLY includes DHCPPOFFER and DHCPNAK.
```

```
!--- Client's MAC address is 00e0.1ef2.c441.
```

```
00:20:54: DHCPD: broadcasting BOOTREPLY to client 00e0.1ef2.c441.
```

```
!--- Router is forwarding DHCPPOFFER or DHCPNAK broadcast on local LAN interface.
```

```
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
```

```
!--- Router received DHCPDISCOVER/REQUEST/INFORM and set Gateway IP address to 192.168.1.1 for forwarding.
```

```
00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..
```

```
!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM.
```

```
!--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier.
00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441.
!--- BOOTREPLY includes DHCPPOFFER and DHCPNAK.

!--- Client's MAC address is 00e0.1ef2.c441.
00:20:54: DHCPD: broadcasting BOOTREPLY to client 00e0.1ef2.c441.
!--- Router is forwarding DHCPPOFFER or DHCPNAK broadcast on local LAN interface.
```

여러 디버그를 동시에 실행

여러 디버그를 동시에 실행할 경우 DHCP/BootP 릴레이 에이전트 및 서버의 작업과 관련하여 상당한 양의 정보를 검색할 수 있습니다. 이전 아웃라인을 사용하여 문제를 해결할 경우 DHCP/BootP 릴레이 에이전트 기능이 제대로 작동하지 않는 위치를 추론할 수 있습니다.

```
IP: s=0.0.0.0 (Ethernet0), d=255.255.255.255, len 604, rcvd 2
UDP src=68, dst=67
UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
DHCPD: setting giaddr to 192.168.1.1.
UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet1), len 604, sending
UDP src=67, dst=67
DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3030.302e.3030.3030.2e30.3030.312d.4574.30 forwarded
to 192.168.2.2.
IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
UDP src=67, dst=67
UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=308
DHCPD: forwarding BOOTREPLY to client 0000.0000.0001.
DHCPD: broadcasting BOOTREPLY to client 0000.0000.0001.
UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=328
IP: s=0.0.0.0 (Ethernet0), d=255.255.255.255, len 604, rcvd 2
UDP src=68, dst=67
UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
DHCPD: setting giaddr to 192.168.1.1.
UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet1), len 604, sending
UDP src=67, dst=67
DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3030.302e.3030.3030.2e30.3030.312d.4574.30 forwarded
to 192.168.2.2.
IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
UDP src=67, dst=67
UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=308
DHCPD: forwarding BOOTREPLY to client 0000.0000.0001.
DHCPD: broadcasting BOOTREPLY to client 0000.0000.0001.
UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=328.
```

스니퍼 추적을 가져오고 DHCP 문제의 근본 원인 확인

동일한 [LAN 세그먼트에 있는 DHCP 클라이언트 및 서버의 Decode Sniffer Trace\(스니퍼 추적 디코딩\)](#)와 DHCP [릴레이 에이전트 섹션으로 구성된 라우터로 구분된 DHCP 클라이언트 및 서버의 Decode Sniffer Trace\(스니퍼 추적 디코딩\)](#)을 검토합니다

- DHCP 패킷 추적을 해독합니다.

Catalyst 스위치에서 SPAN(Switched Port Analyzer) 기능을 사용하여 스니퍼 추적을 얻는 방법에 대한 자세한 내용은 [Catalyst SPAN\(Switched Port Analyzer\) 구성 예를 참조하십시오.](#)

라우터에서 디버깅으로 패킷 디코딩의 대체 방법

Cisco 라우터의 `debug ip packet detail dump <acl>` 명령을 사용하면 시스템 로그 또는 CLI(Command Line Interface)에 표시된 전체 패킷을 16진수로 가져올 수 있습니다. 디버그 명령을 사용하여 [DHCP 요청 수신 확인을 검토하고](#) 위의 [디버그 명령섹션과](#) 함께 [DHCP 요청 수신 확인](#) 및 DHCP 서버에 요청 전달을 수행하여 액세스 목록에 추가된 덤프 키워드와 함께 동일한 디버그 정보를 얻지만 패킷 세부사항이 16진수로 표시됩니다. 패킷의 내용을 확인하려면 패킷을 변환해야 합니다. 예는 부록 A에 나와 있습니다.

부록 A: Cisco IOS DHCP 샘플 컨피그레이션

DHCP 서버 데이터베이스는 트리로 구성됩니다. 트리의 루트는 자연 네트워크의 주소 풀이고, 브랜치는 하위 네트워크 주소 풀이며, 리프는 클라이언트에 대한 수동 바인딩입니다. 하위 네트워크는 네트워크 매개변수를 상속하고 클라이언트는 하위 네트워크 매개변수를 상속합니다. 따라서 공통 매개변수(예: 도메인 이름)는 트리의 최상위(네트워크 또는 서브네트워크) 레벨에서 구성해야 합니다.

DHCP를 구성하는 방법 및 이와 관련된 명령에 대한 자세한 내용은 DHCP 구성 [작업 목록을 참조하십시오](#).

```
version 12.1
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable password cisco
ip subnet-zero
no ip domain-lookup
ip dhcp excluded-address 10.10.1.1 10.10.1.199

!--- Address range excluded from DHCP pools.

ip dhcp pool test_dhcp

!--- DHCP pool (scope) name is test_dhcp.

network 10.10.1.0 255.255.255.0

!--- DHCP pool (address will be assigned in this range) for associated Gateway IP address.

default-router 10.10.1.1

!--- DHCP option for default gateway.

dns-server 10.30.1.1

!--- DHCP option for DNS server(s).

netbios-name-server 10.40.1.1

!--- DHCP option for NetBIOS name server(s) (WINS).

lease 0 0 1
```



```
!--- Lease time.
```

```
interface Ethernet0
description DHCP Client Network
ip address 10.10.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet1
description Server Network
ip address 10.10.2.1 255.255.255.0
no ip directed-broadcast
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
login
!
end
```

관련 정보

- [툴 및 리소스](#)
- [Technical Support - 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.