

# 了解 Catalyst 交换机或企业网络中的 DHCP 以及故障排除

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[关键概念](#)

[示例情景](#)

[背景信息](#)

[了解 DHCP](#)

[当前的 DHCP RFC 参考](#)

[DHCP 消息表](#)

[续订租期](#)

[DHCP 数据包](#)

[客户端和 DHCP 服务器位于同一子网时的用于为客户端获得 DHCP 地址的客户端-服务器会话](#)

[DHCP/BootP 中继代理的角色](#)

[在 Cisco IOS 路由器上配置 DHCP/BootP 中继代理功能](#)

[设置手动绑定](#)

[如何使 DHCP 在备用 IP 分段工作](#)

[使用 DHCP 中继功能的 DHCP 客户端服务器会话](#)

[Pre-Execution Environment \(PXE\) 启动 DHCP 注意事项](#)

[使用嗅探器踪迹了解和排除 DHCP 故障](#)

[解码同一 LAN 段上的 DHCP 客户端和服务器的嗅探器踪迹](#)

[解码由配置 DHCP 中继代理的路由器分隔的 DHCP 客户端和服务器的嗅探器跟踪信息](#)

[排除客户端工作站无法获得 DHCP 地址时的 DHCP 故障](#)

[案例分析 1：DHCP 服务器与 DHCP 客户端位于同一个 LAN 分段或 VLAN 上](#)

[案例分析 2：DHCP 服务器与 DHCP 客户端被配置用于 DHCP/BootP 中继代理功能的路由器分隔](#)

[路由器上的 DHCP 服务器由于 POOL EXHAUSTED 错误而无法分配地址](#)

[DHCP 故障排除模块](#)

[了解何处可能出现 DHCP 问题](#)

[在 ip dhcp pool 命令选项 {option number} ASCII 后输入的关键字位于双引号中](#)

[附录 A：IOS DHCP 示例配置](#)

[相关信息](#)

## 简介

本文档包含了有关如何排除 Cisco Catalyst 交换机网络中可能发生的几个常见的动态主机配置协议

(DHCP) 问题的信息。本文档涉及对使用 Cisco IOS® DHCP/BootP 中继代理功能时出现的故障进行故障排除。

## 先决条件

### 要求

本文档没有任何特定的前提条件。

### 使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

### 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

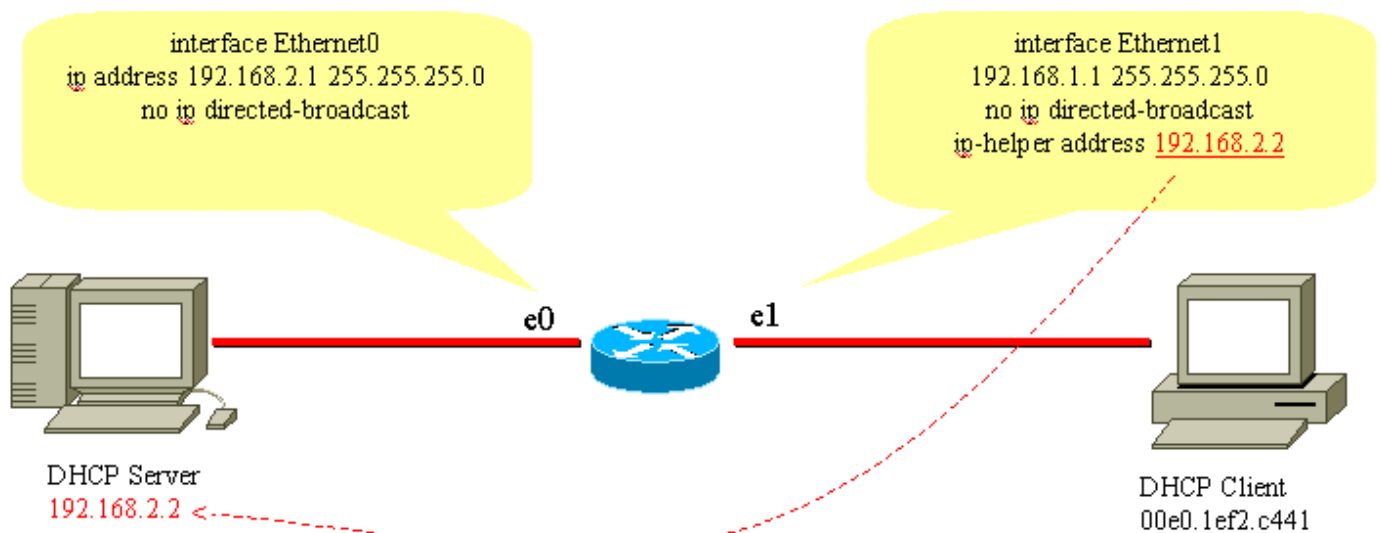
### 关键概念

以下是关于 DHCP 的一些关键概念：

- DHCP客户端最初没有配置IP地址，因此必须发送广播请求，从DHCP服务器获取IP地址。
- 默认情况下，路由器不转发广播。如果 DHCP 服务器在另一个广播域上（第 3 层 (L3) 网络），则必须能够处理客户端的 DHCP 广播请求。该功能需使用 DHCP 中继代理执行。
- Cisco 路由器实施 DHCP 中继需由接口级的 `ip helper` 命令来执行

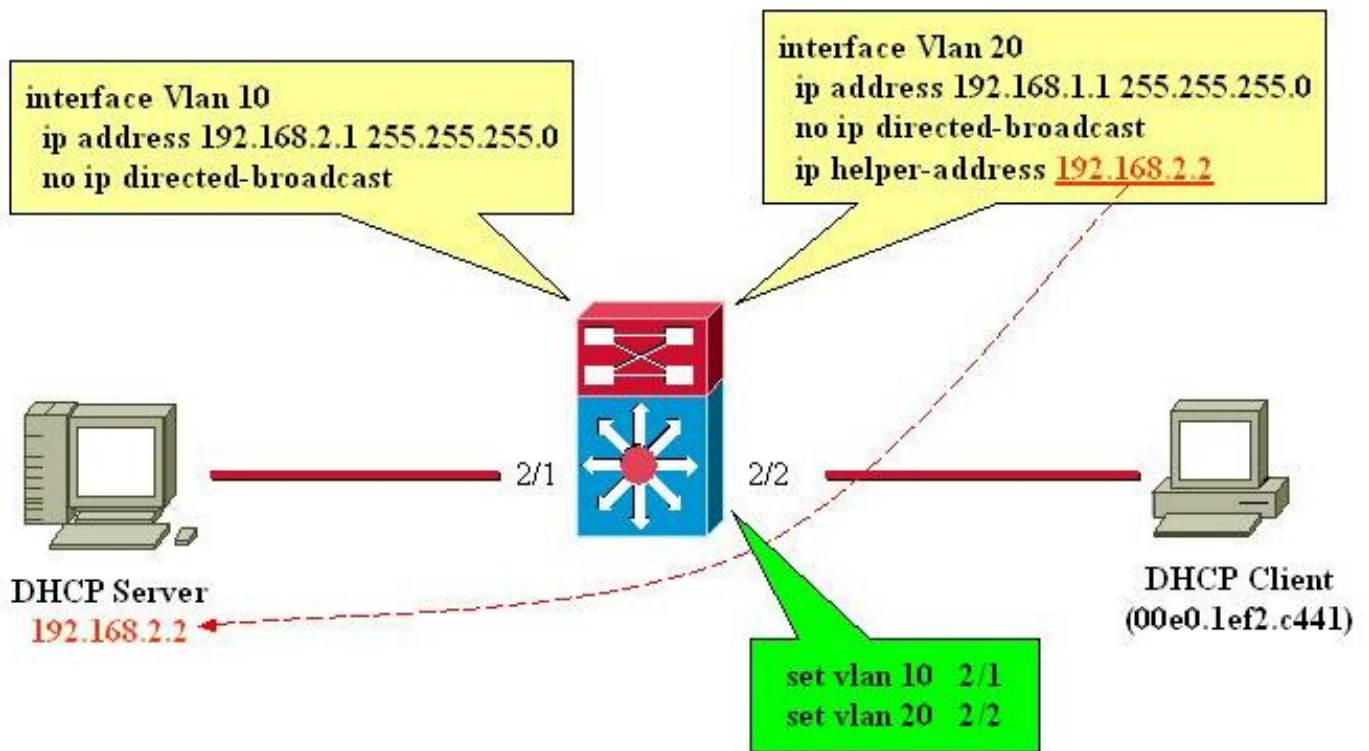
### 示例情景

**情形 1：** Cisco 路由器在 DHCP 客户端网络与 DHCP 服务器网络之间进行路由



如上图的配置所示，接口 Ethernet1 通过接口 Ethernet1 将客户端广播的 DHCPDISCOVER 转发到 192.168.2.2。DHCP 服务器通过单播满足请求。在本例中无需对路由器进行其他配置。

**方案 2：带有 L3 模块的 Cisco Catalyst 交换机在 DHCP 客户端网络与 DHCP 服务器网络之间路由**



如上图的配置所示，接口 VLAN20 通过接口 VLAN10 将客户端广播的 DHCPDISCOVER 转发到 192.168.2.2。DHCP 服务器通过单播满足请求。在本例中无需对路由器进行其他配置。需要将交换机端口配置为主机端口，然后启用生成树协议 (STP) Portfast，并禁用中继和信道。

## 背景信息

DHCP 提供一种机制，通过这种机制，使用传输控制协议/互联网协议 (TCP/IP) 的计算机能够通过网络自动获取协议配置参数。DHCP 是由 [互联网工程任务组 \(IETF\)](#) 的 [动态主机配置工作组 \(DHCP-WG\)](#) 开发的开放标准。

DHCP 基于客户端-服务器模式，在该模式中，DHCP 客户端（例如台式机）联系 DHCP 服务器以获得配置参数。DHCP 服务器一般位于中心位置，并且由网络管理员进行操作。由于服务器由网络管理员负责运行，因此 DHCP 客户端可以可靠、动态地配置适合当前网络体系结构的参数。

多数企业网络由多个子网组成，这些网络分成称为虚拟 LAN (VLAN) 的多个子网络，路由器在子网络之间路由。由于默认情况下路由器不转发广播，所以每个子网中都要有 DHCP 服务器，除非将路由器配置为使用 DHCP 中继代理功能转发 DHCP 广播。

## 了解 DHCP

DHCP 最初在 [请求注解 \(RFC\) 1531](#) 中进行了定义，但该定义已经过时，最新的定义可在 [RFC 2131](#) 中找到。DHCP 基于 [RFC 951](#) 中定义的引导协议 (BootP)。

工作站（主机）在启动时使用 DHCP 获取初始配置信息，例如 IP 地址、子网掩码和默认网关。由于每台主机都需要拥有 IP 地址才能在 IP 网络中通信，所以 DHCP 减轻了为每台主机手动配置 IP

地址的管理负担。此外，如果主机移至其他 IP 子网，它使用的 IP 地址不得与先前使用的 IP 地址相同。DHCP 会自动处理此问题。它允许主机在正确的 IP 子网中选择 IP 地址。

## 当前的 DHCP RFC 参考

- RFC 2131 - DHCP
- RFC 2132 - DHCP 选项和 BootP 厂商扩展
- RFC 1534 - DHCP 和 BootP 之间的互操作
- RFC 1542 - BootP 的说明与扩展
- RFC 2241 - Novell 目录服务的 DHCP 选项
- RFC 2242 - Netware/IP 域名和信息
- RFC 2489 - 定义新 DHCP 选项的步骤

DHCP 采用客户端-服务器模式，在该模式下，一个或多个服务器（DHCP 服务器）在客户端启动时将 IP 地址和其他可选配置参数分配给客户端（主机）。在指定时间内，服务器将这些配置参数租给客户端。主机启动时，主机中的 TCP/IP 协议栈将传输广播 (DHCPDISCOVER) 消息，以获取 IP 地址和子网掩码以及其他配置参数。DHCP 服务器与主机间的交换过程随之启动。在此交换过程中，客户端将经历下列几个定义状态：

1. 正在初始化
2. 选择
3. 请求
4. 区域
5. 更新
6. 重新绑定

在上面所列的状态之间进行转换时，客户端和服务器可能会交换以下 DHCP 消息表中列出的消息类型。

## DHCP 消息表

参考	消息	请使用
0 x 0 0 1	DHCPDISCOVER	客户端正在查找可用的 DHCP 服务器。
0 x 0 0 2	DHCPDISCOVER	服务器响应客户端的 DHCPDISCOVER。
0 x 0 0 3	DHCPREQUEST	客户端向服务器广播数据包，根据数据包中的定义请求从特定的服务器获得参数。
0 x 0 0 4	DHCPDECLINE	客户端-服务器通信，指示网络地址已在使用中。
0 x 0 0 x	DHCPACK	包含配置参数的服务器-客户端通信，包括承诺的网络地址。

0 5		
0 x 0 6	DHCPN AK	服务器-客户端通信，拒绝有关配置参数的请求。
0 x 0 7	DHCPR ELEASE	客户端-服务器通信，放弃网络地址且取消剩余租期。
0 x 0 8	DHCP INFORM	客户端-服务器通信，只请求获取本地配置参数（客户端已将这些配置参数配置为外部地址）。

## DHCPDISCOVER

当客户端第一次启动时，我们认为它处在初始化状态，它通过用户数据报协议 (UDP) 端口 67 ( BootP 服务器 ) 在本地物理子网上传输 DHCPDISCOVER 消息。由于客户端无法知道自己属于哪个子网，因此 DHCPDISCOVER 是一个全子网广播 ( 目标 IP 地址为 255.255.255.255 ) ，源 IP 地址为 0.0.0.0。因客户端未配置 IP 地址，所以源 IP 地址为 0.0.0.0。如果本地子网中存在 DHCP 服务器，并且该 DHCP 服务器配置和运行正常，则该 DHCP 服务器将听到广播并使用 DHCP OFFER 消息进行响应。如果本地子网中没有 DHCP 服务器，则该本地子网中必须要有 DHCP/BootP 中继代理以将 DHCPDISCOVER 消息转发到包含 DHCP 服务器的子网。

此中继代理可以是一台专用主机 ( 例如 Microsoft Windows Server ) 或路由器 ( 例如使用接口级 IP helper 语句配置的 Cisco 路由器 ) 。

## DHCPOFFER

收到 DHCPDISCOVER 消息的 DHCP 服务器可能在 UDP 端口 68 ( BootP 客户端 ) 上使用 DHCP OFFER 消息进行响应。客户端接收到 DHCP OFFER，并进入选择状态。此 DHCP OFFER 消息包含客户端的初始配置信息。例如，DHCP 服务器会将请求的 IP 地址填入 DHCP OFFER 消息的 yiaddr 字段。选项域、子网掩码和路由器选项分别指定了子网掩码和默认网关。DHCP OFFER 消息中的其他常用选项包括 IP 地址租用时间、续订时间、域名服务器和 NetBIOS 名称服务器 (WINS)。DHCP 服务器会将 DHCP OFFER 发送到广播地址，它会在 DHCP OFFER 的 chaddr 字段中包含客户端硬件地址，从而使客户端知道自己是预定目标。如果 DHCP 服务器不在本地子网上，则 DHCP 服务器会通过 UDP 端口 67 将 DHCP OFFER 作为单播数据包发送回 DHCPDISCOVER 所来自的 DHCP/BootP 中继代理。然后，DHCP/BootP 中继代理会通过 UDP 端口 68 在本地子网上广播或单播 DHCP OFFER，这取决于 Bootp 客户端设置的广播标志位。

## DHCPREQUEST

客户端收到 DHCP OFFER 之后，用 DHCPREQUEST 消息进行响应 ( 表示其愿意接受 DHCP OFFER 中的参数 ) 并转换到请求状态。客户端可能收到多条 DHCP OFFER 信息，该信息源自收到原始 DHCPDISCOVER 信息的每台 DHCP 服务器。客户端选择一个 DHCP OFFER，并且只回应该 DHCP 服务器，隐含拒绝其他所有 DHCP OFFER 信息。客户端通过用 DHCP 服务器的 IP 地址填充 Server Identifier 选项字段来标识选中的服务器。DHCPREQUEST 也是广播，所以发送 DHCP OFFER 的所有 DHCP 服务器都将看到 DHCPREQUEST，从而每台服务器都可知道自己发送的 DHCP OFFER 是被接受还是被拒绝。客户端要求的所有其他配置选项都将包括在

DHCPREQUEST 消息的选项字段中。尽管客户端已经分配到一个 IP 地址，它发送的 DHCPREQUEST 消息所包含的源 IP 地址仍然为 0.0.0.0。此时，客户端还没有收到使用 IP 地址的明确确认。

## DHCPACK

DHCP 服务器收到 DHCPREQUEST 之后，它将通过 DHCPACK 消息确认该请求，从而完成初始化过程。DHCPACK 消息包含 DHCP 服务器的源 IP 地址，且其目标地址也是广播地址。DHCPACK 消息包含客户端在 DHCPREQUEST 消息中请求的所有参数。客户端收到 DHCPACK 后将进入已绑定状态，此时可以自由使用 IP 地址在网络上进行通信。同时，DHCP 服务器会将租期信息存储在数据库中，并使用客户端标识符（或 chaddr）和相关 IP 地址对租期进行唯一标识。客户端和服务器都将使用此标识符组合来引用租期信息。客户端标识符是设备的 MAC 地址加上介质类型。

DHCP 客户端开始使用新的地址之前必须计算与所租用地址相关的时间参数，即租用时间 (LT)、续订时间 (T1) 和重新绑定时间 (T2)。一般默认的 LT 是 72 个小时。如果需要，您也可以使用较短的租用时间，以便节约地址资源。

## DHCPNAK

如果所选服务器不能满足 DHCPREQUEST 消息的要求，则该 DHCP 服务器将以 DHCPNAK 消息进行响应。若客户端收到 DHCPNAK 消息，或者若客户端没有收到对 DHCPREQUEST 消息的任何响应，则客户端会进入请求状态，重新启动配置过程。在重新启动初始化状态之前，客户端将在 60 秒内至少重新发出四次 DHCPREQUEST。

## DHCPDECLINE

客户端接收到 DHCPACK，并可以选择对参数执行最终检查。客户端执行此过程的方法是针对 DHCPACK 中提供的 IP 地址发送地址解析协议 (ARP) 请求。如果客户端收到对该 ARP 请求的响应，发现该地址已在使用中，则客户端将向服务器发送 DHCPDECLINE 消息，并且进入请求状态，重新启动配置过程。

## DHCPINFORM

如果客户端已通过其他一些方法获得网络地址或者手动配置了 IP 地址，则客户端工作站可能会使用 DHCPINFORM 请求消息来获得其他本地配置参数，例如域名和域名服务器 (DNS)。在没有分配新 IP 地址的情况下，接收 DHCPINFORM 信息的 DHCP 服务器采用适合客户端的本地配置参数构建 DHCPACK 信息。此 DHCPACK 将单播至客户端。

## DHCPRELEASE

DHCP 客户端可能会选择通过向 DHCP 服务器发送 DHCPRELEASE 消息来放弃它对某个网络地址的租用权。客户端在 DHCPRELEASE 消息中使用 client identifier 字段和网络地址来标识要释放的租期。如果需要扩大当前 DHCP 池范围，应删除当前地址池并在 DHCP 池内指定新的 IP 地址范围。[若要删除您想放置在 DHCP 池中的特定 IP 地址或特定 IP 地址范围，请使用 ip dhcp excluded-address 命令。](#)

**注意：** 如果设备使用的是 BOOTP，路由器的 DHCP 绑定将显示无限租期。

## [续订租期](#)

由于 IP 地址只是从服务器租用的，因此必须时常续订租期。当租用时间过半 ( $T1=0.5 \times LT$ ) 时，客户端将尝试续订租期。客户端将进入续订状态，并向保有当前租用信息的服务器发送 DHCPREQUEST 消息。如果服务器同意续订租期，它将以 DHCPACK 消息响应续订请求。DHCPACK 消息将包含新的租期，如果在早先的租用期间服务器发生任何更改，则 DHCPACK 消息还将包含所有新的配置参数。如果由于某种原因，客户端无法访问保有租期信息的服务器，则当该原始 DHCP 服务器没有在时间  $T2$  内响应续订请求时，客户端将尝试向任意 DHCP 服务器续订 IP 地址。 $T2$  的默认值是  $(7/8 \times LT)$ 。也就是说  $T1 < T2 < LT$ 。

如果客户端先前有一个由 DHCP 分配的 IP 地址并且该客户端已重新启动，则该客户端将在 DHCPREQUEST 数据包中请求租用先前租用的 IP 地址。此 DHCPREQUEST 包含的源 IP 地址仍然为 0.0.0.0，而其目标 IP 地址仍然为 IP 广播地址 255.255.255.255。

重新启动过程发送 DHCPREQUEST 的客户端，不必一定填写服务器标识符字段，但必须填写被请求的 IP 地址选项字段。严格遵守 RFC 的客户端将使用所请求的地址填充 ciaddr 字段，而不是填充 DHCP 选项字段。DHCP 服务器对两种方法均可接受。DHCP 服务器的工作情况取决于一系列因素，例如，对于 Windows NT DHCP 服务器，其工作情况取决于使用的操作系统版本以及其他因素（例如超级作用域）。如果 DHCP 服务器确定客户端仍然可以使用所请求的 IP 地址，则它将保持沉默或发送 DHCPACK 以响应 DHCPREQUEST。如果服务器确定客户端不可继续使用所请求的 IP 地址，则它将向客户端发送 DHCPNACK。客户端将进入初始化状态，并且发送 DHCPDISCOVER 消息。

**注意：** DHCP 服务器将 IP 地址池的底部 IP 地址分配给 DHCP 客户端。在底部地址租期过期后，如果此地址再次被请求，则其将会被分配给另一客户端。您不能更改 DHCP 地址的分配顺序。

## DHCP 数据包

DHCP 消息的长度是可变的，它由下表列出的字段组成。

**注意：** 此数据包是原始 BootP 数据包的修订版本。

字段	字节	名称	说明
操作	1	操作码	确定数据包是请求还是回复 : 1=BOOTREQUEST、2=BOOTREPLY
htype	1	硬件类型	指定网络硬件地址类型。
hlen	1	硬件地址长度	指定硬件地址的长度。
跳	1	跳	客户端将该值设置为零，如果通过路由器转发请求，则该值会递增。
XID	4	事务 ID	客户端随机选取的数值。所有针对特定 DHCP 事务交换的 DHCP 消息都使用此 ID (xid)。
秒	2	秒钟	指定自 DHCP 过程开始后的秒数。
标志	2	标志	指示是广播还是单播消息。
ciaddr	4	客户端 IP 地址	只有当客户端知道其 IP 地址时（例如客户端处于已绑定、续订或重新绑定状态时）才能使用。
yiaddr	4	您的	如果客户端 IP 地址是 0.0.0.0，则 DHCP

ddr		IP 地址	服务器将把提供的客户端 IP 地址放在该字段中。
sia dd r	4	服务器 IP 地址	如果客户端知道 DHCP 服务器的 IP 地址，则将使用 DHCP 服务器地址填充此字段。否则，它将用在 DHCP 服务器的 DHCPOFFER 和 DHCPACK 中。
gia dd r	4	路由器 IP 地址 (GI ADDR)	由 DHCP/BootP 中继代理填写的网关 IP 地址。
ch ad dr	1 6	客户端 MAC 地址	DHCP 客户端的 MAC 地址。
sn a m e	6 4	服务器名称	可选的服务器主机名。
文件	1 2 8	引导文件名称	引导文件的名称。
选项	变量	选项参数	可由 DHCP 服务器提供的选项参数。RFC 2132 给出了所有可能的选项。

## 客户端和 DHCP 服务器位于同一子网时的用于为客户端获得 DHCP 地址的客户端-服务器会话

数据包描述	源 MAC 地址	目标 MAC 地址	源 IP 地址	目标 IP 地址
DHCPDISCOVER	客户端	广播	0.0.0.0	255.255.255.255
DHCPOFFER	DHCPServer	广播	DHCPServer	255.255.255.255
DHCPREQUEST	客户端	广播	0.0.0.0	255.255.255.255
DHCPACK	DHCPServer	广播	DHCPServer	255.255.255.255

## DHCP/BootP 中继代理的角色

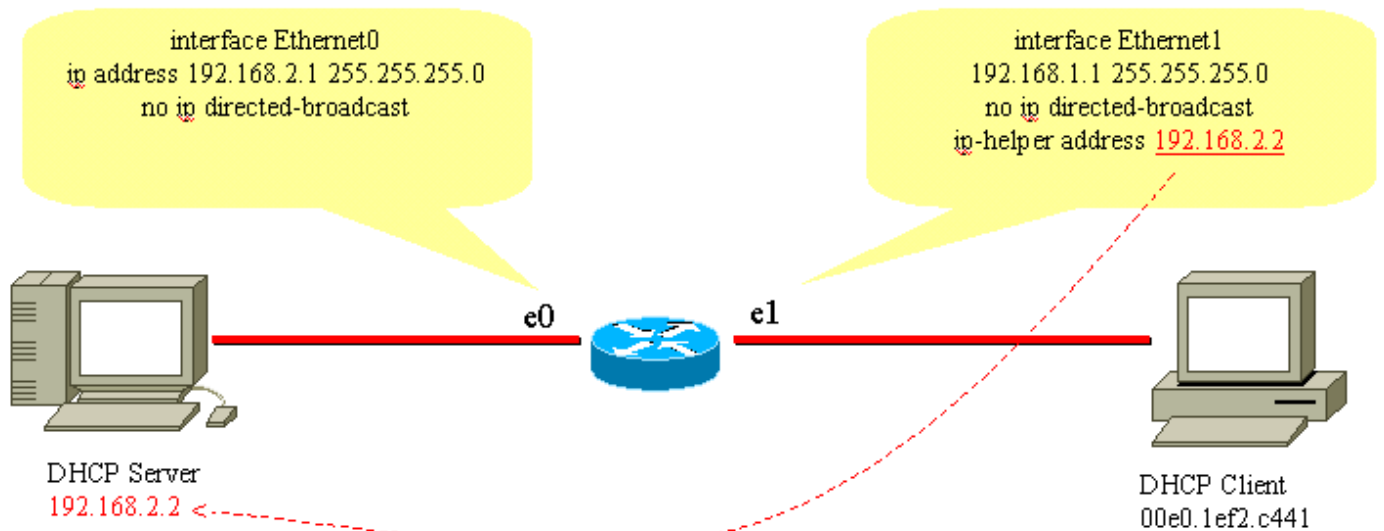
默认情况下，路由器不转发广播数据包。由于 DHCP 客户端消息在使用了目的地 IP 地址 255.255.255.255 (所有网络广播)，DHCP 客户端无法将请求发送到不同子网上的 DHCP 服务器，除非路由器上配置了 DHCP /BootP Relay Agent。DHCP/BootP 中继代理将代表 DHCP 客户端将 DHCP 请求转发到 DHCP 服务器。DHCP/BootP 中继代理将自己的 IP 地址附加到进入 DHCP 服务器的 DHCP 帧的源 IP 地址。这使得 DHCP 服务器可以通过单播响应 DHCP/BootP 中继代理。



DHCP/BootP 中继代理还将使用接收来自客户端的 DHCP 消息的接口的 IP 地址填充网关 IP 地址字段。DHCP 服务器使用网关 IP 地址字段确定 DHCPDISCOVER、DHCPREQUEST 或 DHCPINFORM 消息所来自的子网。

## 在 Cisco IOS 路由器上配置 DHCP/BootP 中继代理功能

将思科路由器配置为转发 BootP 或 DHCP 请求很简单 - 只需配置指向 DHCP/BootP 服务器或指向服务器所在网络的子网广播地址的 IP 帮助地址。例如，请考虑以下网络图：



要将 BootP/DHCP 请求从客户端转发到 DHCP 服务器，可使用 ip helper-address interface 命令。可配置 IP 帮助地址以根据 UDP 端口号转发所有 UDP 广播。默认情况下，IP 帮助地址将转发以下 UDP 广播：

- 简单文件传输协议 (TFTP) ( 端口 69 )
- DNS ( 端口 53 )、时间服务 ( 端口 37 )
- NetBIOS 名称服务器 ( 端口 137 )
- NetBIOS 数据报服务器 ( 端口 138 )
- 引导协议 (DHCP/BootP) 客户端和服务器数据报 ( 端口 67 和 68 )
- 终端访问控制器访问控制系统 (TACACS) 服务 ( 端口 49 )
- IEN-116 名称服务 ( 端口 42 )

IP 帮助地址能将 UDP 广播转发到单播/广播 IP 地址。但不建议使用 IP 帮助地址将 UDP 广播从一个子网转发到另一个子网的广播地址，因为这有可能会产生大规模的广播泛洪。此外，也支持单个接口上存在多个 IP 帮助地址条目，如下所示：

```
!  
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 路由器不支持在已配置为 DHCP 中继代理的 DHCP 服务器上实现负载平衡。Cisco 路由器会将 DHCPDISCOVER 消息转发到所提及的该接口的所有帮助地址。如果一个子网包含两个或多个 DHCP 服务器，则 DHCP 流量会增加，因为要在每一对 DHCP 客户端与服务器间交换 DHCPDISCOVER、DHCP OFFER 和 DHCPREQUEST/DHCPDECLINE 等消息。

## 设置手动绑定

有两种方式可设置手动绑定；一种适用于 Windows 主机，另一种适用于非 Windows 主机。有两种不同的用来配置的命令；一种适用于 Microsoft DHCP 客户端，另一种适用于非 Microsoft DHCP 客户端：[DHCP client-identifier \(手动绑定 - Microsoft DHCP 客户端\)](#) 和 [DHCP hardware-address \(手动绑定 - 非 Microsoft DHCP 客户端\)](#)。采用两种不同的命令是因为运行 Windows 的计算机修改本机的 MAC 地址，即在地址的起始处加上 01。以下为示例配置：

- 以下是 Microsoft DHCP 客户端的配置

```
configuration terminal
ip dhcp pool new_pool host ip_address subnet_mask client-identifier 01XXXXXXXXXXXXX !---
xxxxxx represents 48 bit MAC address prepended with 01
```

- 以下是非 Microsoft DHCP 客户端的配置

```
configuration terminal
ip dhcp pool new_pool host ip_address subnet_mask hardware-address XXXXXXXXXXXXX !--- xxxxxx
represents 48 bit MAC address
```

## 如何使 DHCP 在备用 IP 分段工作

默认情况下，DHCP 对发送应答数据包有所限制，只有当接收的请求是来自配置有主 IP 地址的接口时，才会发送应答数据包。DHCP 数据流使用广播地址。路由器接口接收到 DHCP 请求后，会将其转发到具有该接口上配置的主 IP 地址的源地址的 DHCP 服务器（已配置 IP 帮助地址），使 DHCP 服务器知道在 DHCP 应答数据包中必须使用哪一个 IP 池（分配给客户端）。

路由器无法判断 DHCP 广播请求是否来自接口上配置的备用 IP 网络上的设备。应急方案是，通过配置子接口配置（前提是连接到路由器的设备支持 dot1q 标记）来分开两个子网，这样二者都可正常地获得它们各自的 IP 地址。

[如果想要首选备用地址，还有另一个应急方案，就是启用全局配置命令 ip dhcp smart-relay。](#)这个方法有所限制，即只有在对主地址池进行三次连续的请求而 DHCP 服务器均无响应的情况下，才使用备选 IP 来中继 DHCP 请求。

## 使用 DHCP 中继功能的 DHCP 客户端服务器会话

下表说明了 DHCP 客户端从 DHCP 服务器获取 IP 地址的过程。下表是根据上面的[网络图](#)而建立的。图中各个数值分别代表下面所述的数据包。此表作为了解 DHCP 客户端-服务器会话的数据包流的参考依据。此表也可用于确定 DHCP 问题可能发生在什么地方。

数据包	客户端 IP 地址	服务器 IP 地址	GI 地址	数据包的源 MAC 地址	数据包的源 IP 地址	数据包的目标 MAC 地址	数据包的目标 IP 地址
1. 客户端发送 DHCPDISCOVER。	0.0 .0. 0	0.0 .0. 0	0.0 .0. 0	0005. DCC 9.C6 40	0.0 .0. 0	ffff.ffff .ffff (广播)	255. 255. 255. 255
2. 路由器通过 E1 接口接收 DHCPDISCOVER。路由器识别出此数据包为 DHCP UDP 广播。路由器此时将作为 DHCP/BootP 中继代理，使用传入接口的 IP 地址填写网关 IP 地址字段，将源 IP 地址更改为传入接口的 IP 地址，并将请求直接转发到 DHCP 服务器。	0.0 .0. 0	0.0 .0. 0	19 2.1 68. 1.1	E2 接口的 MAC 地址	19 2.1 68. 1.1	DHCP 服务器的 MAC 地址	192. 168. 2.2
3. DHCP 服务器已接收 DHCPDISCOVER，并正在向 DHCP 中继代理发送 DHCPPOFFER。	19 2.1 68. 1.2	19 2.1 68. 2.2	19 2.1 68. 1.1	DHCP 服务器的 MAC 地址	19 2.1 68. 2.2	E2 接口的 MAC 地址	192. 168. 1.1
4. DHCP 中继代理接收到 DHCPPOFFER，并将在本地 LAN 上转发 DHCPPOFFER 广播。	19 2.1 68. 1.2	19 2.1 68. 2.2	19 2.1 68. 1.1	E1 接口的 MAC 地址	19 2.1 68. 1.1	ffff.ffff .ffff (广播)	255. 255. 255. 255
5. 客户端发送 DHCPREQUEST。	0.0 .0. 0	0.0 .0. 0	0.0 .0. 0	0005. DCC 9.C6 40	0.0 .0. 0	ffff.ffff .ffff (广播)	255. 255. 255. 255
6. 路由器通过 E1 接口接收 DHCPREQUEST。	0.0 .0. 0	0.0 .0. 0	19 2.1 68.	E2 接口的 MAC 地址	19 2.1 68.	DHCP 服务器	192. 168. 2.2

T. 路由器识别出此数据包为 DHCP UDP 广播。路由器此时将作为 DHCP 中继代理，使用传入接口的 IP 地址填写网关 IP 地址字段，将源 IP 地址更改为传入接口的 IP 地址，并将请求直接转发到 DHCP 服务器。			1.1	地址	1.1	的 MAC 地址	
7. DHCP 服务器已接收 DHCPREQUEST，并正在向 DHCP/BootP 中继代理发送 DHCPACK。	19 2.1 68. 1.2	19 2.1 68. 2.2	19 2.1 68. 1.1	DHC P 服 务器 的 MAC 地址	19 2.1 68. 2.2	E2 接 口的 MAC 地址	192. 168. 1.1
8. DHCP/BootP 中继代理接收到 DHCPACK，并将在本地 LAN 上转发 DHCPACK 广播。客户端将接受 ACK 并且使用客户端 IP 地址。	19 2.1 68. 1.2	19 2.1 68. 2.2	19 2.1 68. 1.1	E1 接 口的 MAC 地址	19 2.1 68. 1.1	ffff.ffff .ffff ( 广播 )	255. 255. 255. 255

## [Pre-Execution Environment \(PXE\) 启动 DHCP 注意事项](#)

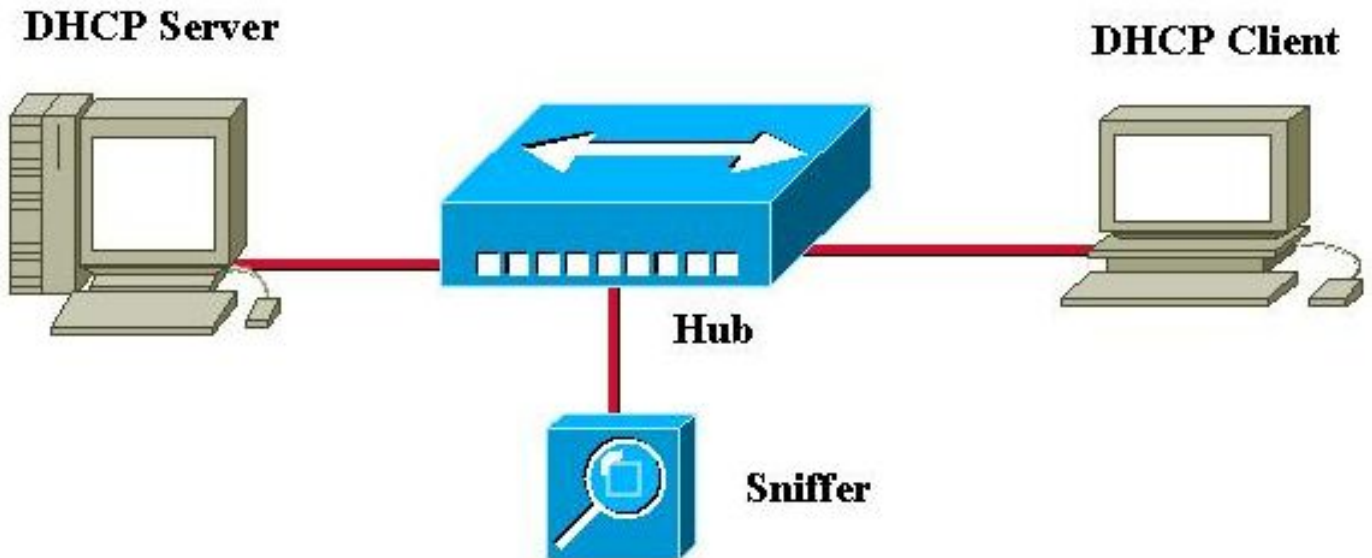
Pre-Execution Environment (PXE) 允许在启动本地硬盘操作系统之前启动一个网络上的一台服务器的工作站。网络管理员无需实际接触特定工作站并手动启动该工作站。可以通过网络将操作系统和其他软件（例如诊断程序）从服务器加载到设备上。PXE 环境使用 DHCP 配置 IP 地址。

如果 DHCP 服务器位于网络的另一个路由段上，则必须在路由器上执行 DHCP/BootP 中继代理配置。[必须对本地路由器接口的 ip helper-address 命令进行配置。](#)参见本文在 Cisco IOS 路由器上配置 DHCP / BOOTP 中继代理程序功能章节，了解相关的配置信息。

## [使用嗅探器踪迹了解和排除 DHCP 故障](#)

### [解码同一 LAN 段上的 DHCP 客户端和服务器的嗅探器踪迹](#)

## Network Topology where DHCP Client and Server Reside on Same LAN Segment



以下的嗅探器踪迹包括六个帧。这六个帧演示了 DHCP 的一个工作情景，在该情景中，DHCP 客户端和服务端驻留在同一个物理或逻辑网段上。排除 DHCP 故障时，重要的是让您的嗅探器踪迹与下面所示的踪迹相匹配。您的嗅探器踪迹与下面的踪迹相比可能有一些差别，但总体的数据包流应该完全相同。数据包踪迹符合之前有关 DHCP 如何工作的讨论内容。

```
----- 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 1 arrived 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 = 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 = 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 FFFFFFFF, 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:

```

- - - - - **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 -----

```

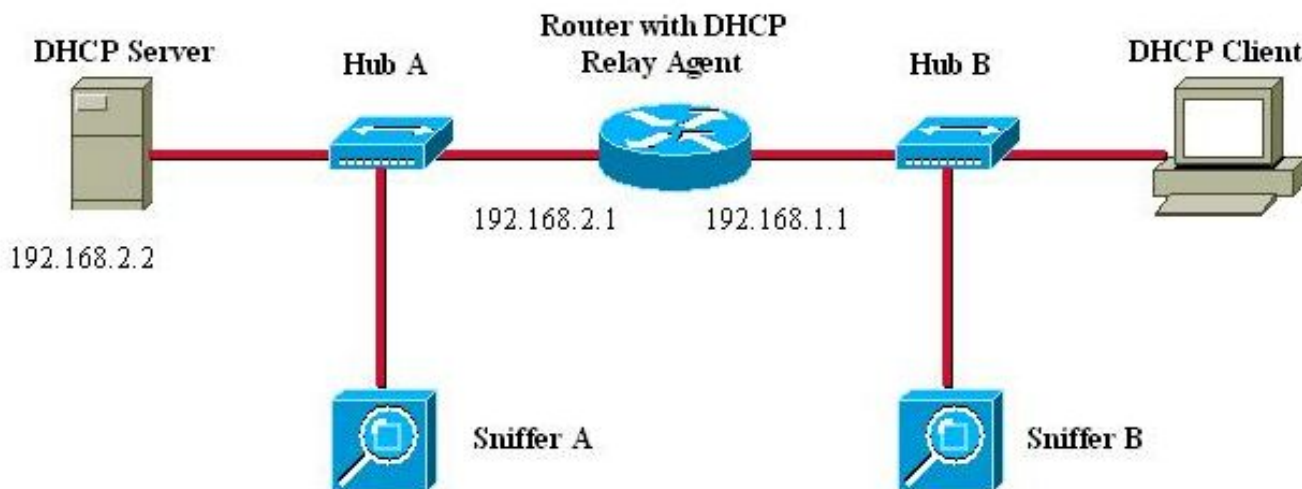
```

DLC:
DLC: Frame 59 arrived at 11:52:04.3557; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, 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:

```

**解码由配置 DHCP 中继代理的路由器分隔的 DHCP 客户端和服务器的嗅探器跟踪信息**

**DHCP Client and Server separated by router configured as DHCP Relay Agent**



**嗅探器 B 踪迹**

```

----- 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:
```

### 嗅探器 A 踪迹

----- **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 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:
```

## [排除客户端工作站无法获得 DHCP 地址时的 DHCP 故障](#)

### [案例分析 1：DHCP 服务器与 DHCP 客户端位于同一个 LAN 分段或 VLAN 上](#)

当 DHCP 服务器和客户端驻留在同一个 LAN 分段或 VLAN 上时，如果客户端无法从 DHCP 服务器获得 IP 地址，则该 DHCP 问题不太可能是由本地路由器导致的。该问题很可能与连接 DHCP 服务器和 DHCP 客户端的设备有关。但是，这个问题也可能是 DHCP 服务器或客户端造成的。根据以下排除故障的模块，应该就能确定是什么设备导致此问题。

**注意：**要基于每个 VLAN 配置 DHCP 服务器，需为向客户端提供 DHCP 地址的每个 VLAN 定义不同的 DHCP 池。

### [案例分析 2：DHCP 服务器与 DHCP 客户端被配置用于 DHCP/BootP 中继代理功能的路由器分隔](#)

当 DHCP 服务器和客户端驻留在不同的 LAN 分段或 VLAN 上时，路由器将充当 DHCP/BootP 中继代理，负责将 DHCPREQUEST 转发到 DHCP 服务器。要对 DHCP/BootP 中继代理、DHCP 服务器和客户端进行故障排除，还需要使用其他故障排除步骤。根据以下排除故障的模块，应该就能确定是哪一个设备导致此问题。

## [路由器上的 DHCP 服务器由于 POOL EXHAUSTED 错误而无法分配地址](#)

有些地址虽然已被从池中释放，但可能仍然被客户端占用。这可以通过 `show ip dhcp conflict` 命令的输出进行验证。当两台主机使用相同的 IP 地址时，就会产生地址冲突。进行地址分配时，DHCP 会通过 ping 和无故 ARP 来检查是否存在冲突。

如果检测到冲突，就会将相关地址从池中删除。直到管理员解决该冲突问题，该地址才会被分配。配置 `ip dhcp conflict logging` 以解决此问题。

## [DHCP 故障排除模块](#)

### [了解何处可能出现 DHCP 问题](#)

DHCP 问题可能有多种起因。最常见的起因就是配置问题。然而，许多 DHCP 问题可能由路由器上运行的操作系统、网络接口卡 (NIC) 驱动程序或 DHCP/BootP 中继代理中的软件缺陷引起。鉴于可能发生问题的地方有多处，因此需要采取系统化的方法来排除故障。

可能造成 DHCP 问题的原因简表：

- Catalyst 交换机的默认配置
- DHCP/BootP 中继代理的配置
- NIC 兼容问题或 DHCP 功能问题
- NIC 故障或 NIC 驱动程序安装不正确
- 因频繁的生成树计算导致的间歇性网络中断
- 操作系统的行为或软件缺陷
- DHCP 服务器的范围配置或软件缺陷
- Cisco Catalyst 交换机或 IOS DHCP/BootP 中继代理的软件缺陷
- 因在非预计接口接收到 DHCP offer，造成单播反向路径转发 (uRPF) 检查失败。当接口启用反向路径转发 (RPF) 功能时，Cisco 路由器会丢弃源地址为 0.0.0.0 以及目标地址为 255.255.255.255 的动态主机配置协议 (DHCP) 和引导协议 (BOOTP) 数据包。路由器也会在接口上丢弃所有含组播目标 IP 地址的 IP 数据包。此问题记录在 [CSCdw31925](#) ( [仅限注册用户](#) ) 中。
- 未使用 DHCP 数据库代理，但未禁用 DHCP 冲突日志记录

本文将使用以下故障排除模块，确定根本原因，如上表所示。

### [A. 验证物理连接](#)

本过程适用于所有案例研究。

首先，验证 DHCP 客户端和服务器的物理连接。如果连接到 Catalyst 交换机，请验证 DHCP 客户端和服务器与交换机之间的物理连接。

对于 Catalyst CatOS 交换机 ( 例如 2948G、4000、5000 和 6000 系列交换机 )，请使用 `show`

`port <mod#>/<port_range>` 命令显示端口状态。如果端口未处于 `connected` 状态，则端口不会传输任何数据流，包括 DHCP 客户端请求。命令的输出如下：

```
Switch (enable) show port 5/1
Port Name Status Vlan Duplex Speed Type
```

```
-----
5/1 connected 1 a-full a-100 10/100BaseTX
```

对于基于 IOS 的交换机（如 Catalyst 2900XL/3500XL/2950/3550），与 `show port status` 等效的命令是 `show interface <interface>`。如果接口是除 `<interface>` 处于 UP 状态的任何状态，且路由协议处于 UP 状态，那么端口不会通过数据流，包括 DHCP 客户端请求。命令的输出如下：

```
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)
```

如果验证了物理连接，证实 Catalyst 交换机和 DHCP 客户端之间没有链路，则请参阅标题为 [排除 Cisco Catalyst 交换机的 NIC 兼容性问题](#) 的文档，以了解关于物理层连接问题的更多故障排除信息。

。

过多的数据链路错误导致某些 Catalyst 交换机上的端口进入 `errdisabled` state。请参阅 [在 CatOS 平台上恢复处于 errDisable 状态的端口](#) 以及 [Cisco IOS 平台的 errDisable 端口状态恢复](#)，二者描述了 `errDisable` 状态、说明了如何从此状态恢复，并且提供了从此状态恢复的示例。

## B. [测试网络连接通过配置有静态IP地址的客户端工作站](#)

本过程适用于所有案例研究。

排除任何 DHCP 问题时，重要的是通过在客户端工作站上配置静态 IP 地址来验证网络连通性。如果已配置了静态 IP 地址，工作站仍然无法访问网络资源，则问题的根本原因不在于 DHCP。此时，需要排除网络连接故障。

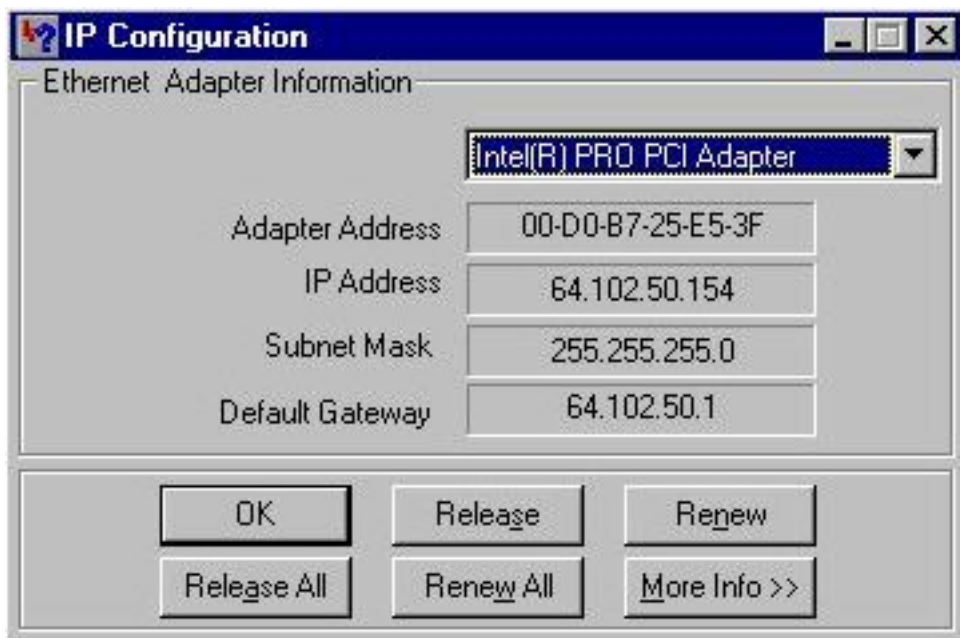
## C. [验证问题作为启动问题](#)

本过程适用于所有案例研究。

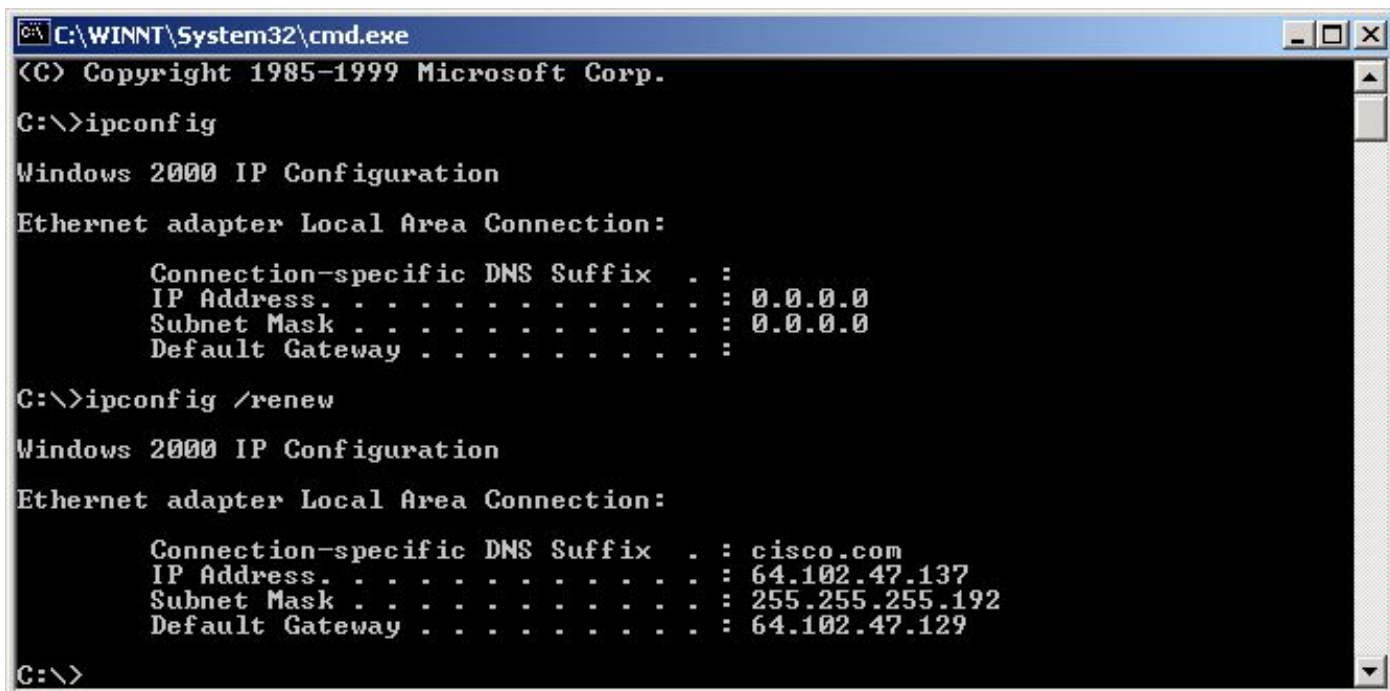
如果 DHCP 客户端在启动时无法从 DHCP 服务器获得 IP 地址，请尝试手动强制客户端发送 DHCP 请求，以从 DHCP 服务器获得 IP 地址。执行以下步骤，以从运行下列操作系统的 DHCP 服务器中手动获取 IP 地址。

**Microsoft Windows 95/98/ME**：单击“开始”按钮，并且运行 `WINIPCFG.exe` 程序。单击 **ReleaseAll** 按钮，跟随由 **RenewAll** 按钮。DHCP 客户端此时是否能获得 IP 地址？





Microsoft Windows NT/2000：在“开始/运行”字段中键入 `cmd` 以打开命令提示窗口。在命令提示窗口中发出 `ipconfig/renew` 命令，如下所示。DHCP 客户端此时是否能获得 IP 地址？



如果在 PC 完成启动过程后，DHCP 客户端能够通过手动更新 IP 地址来获得 IP 地址，则问题很可能属于 DHCP 启动问题。如果 DHCP 客户端连接到 Cisco Catalyst 交换机，则问题很可能源于与 STP portfast 以及/或信道和中继相关的配置问题。也有可能是 NIC 卡问题和交换机端口启动问题。应通过[故障排除步骤 D](#) 和 [E](#) 确定该 DHCP 问题的根本原因是否是交换机端口配置和 NIC 卡问题。

#### D. [检验交换机端口配置 \( STP Portfast 和其它命令 \)](#)

如果交换机是 Catalyst 2900/4000/5000/6000，请验证端口是否启用了 STP portfast，并禁用了中继/信道。默认配置是 STP portfast 为禁用，而中继/通道功能为自动（如果适用）。对于 2900XL/3500XL/2950/3550 交换机而言，STP Portfast 是唯一需要进行的配置。这些配置更改可以解决 Catalyst 交换机初始安装导致的最常见 DHCP 客户端问题。

如需了解有关 DHCP 客户端连接到 Catalyst 交换机时如何进行必要的交换机端口配置才能使

DHCP 正常运行的更多信息，请参阅以下文档：

### [使用 PortFast 和其他命令解决工作站启动连接延迟问题](#)

查看上文的配置指南后，回到本文获得其他排除故障的信息。

### E. [检查已知 NIC 卡或 Catalyst 交换机问题](#)

如果 Catalyst 交换机配置正确，则 Catalyst 交换机中或 DHCP 客户端的 NIC 中可能存在软件兼容性问题，这种软件兼容性问题可能导致了 DHCP 问题。故障排除的下一个步骤是查看以下文档并排除可能导致故障的与 Catalyst 交换机或 NIC 相关的软件问题：

### [排除 Cisco Catalyst 交换机的 NIC 兼容性问题](#)

要正确排除所有兼容性问题，需要了解 DHCP 客户端的操作系统及具体的 NIC 信息（例如制造商、型号和驱动程序版本等）。

### F. [辨别 DHCP 客户端在 DHCP 服务器所处的子网或 VLAN 上是否能获得 IP 地址](#)

当客户端和 DHCP 服务器位于同一子网或 VLAN 中时，辨别 DHCP 是否正常工作非常重要。如果 DHCP 在 DHCP 服务器所处的子网或 VLAN 中正常运行，则 DHCP 问题可能出在 DHCP/BootP 中继代理上。如果在 DHCP 服务器所处的子网或 VLAN 上测试 DHCP 后，问题仍然存在，则真正的问题可能出在 DHCP 服务器上。

### G. [验证路由器 DHCP/BootP 中继配置](#)

使用以下步骤以检验配置：

1. 在路由器上配置 DHCP 中继时，请验证 **ip helper-address** 命令是否位于正确的接口上。**ip helper-address** 命令必须位于 DHCP 客户端工作站的入站接口上，并且必须定向到正确的 DHCP 服务器。
2. 验证是否存在全局配置命令 **no service dhcp**。此配置参数会禁用路由器上的所有 DHCP 服务器和中继功能。此情况下，配置中不会出现默认配置命令 **service dhcp**。[如果未启用 service dhcp，则客户端无法从 DHCP 服务器获得 IP 地址。注意：在运行较早 Cisco IOS 版本的路由器中，处理 DHCP 中继代理功能的是 ip bootp server 命令而非 service dhcp 命令。](#)因此，如果将 **ip helper-address** 命令配置为转发 DHCP UDP 广播并作为代表 DHCP 客户端的 DHCP 中继代理，则需在路由器中启用 **ip bootp server** 命令。
3. 应用 **ip helper-address** 命令以向子网广播地址转发 UDP 广播时，请确认在 UDP 广播数据包需要穿过的任何出站接口上都未配置 **no ip directed-broadcast**。任何定向广播向物理广播的转换过程都将被 **no ip directed-broadcast** 阻止。在软件版本 12.0 及以上版本中，此接口配置为默认配置。
4. 将 DHCP 广播转发至 DHCP 服务器子网广播地址是一个偶发性的软件问题。排除 DHCP 故障时，请始终尝试将 DHCP UDP 广播转发到 DHCP 服务器的 IP 地址，如下所示：

### H. [用户标识\(82\)选项打开](#)

将 DHCP 请求从 DHCP 客户端转发到 DHCP 服务器时，DHCP 中继代理信息（选项 82）功能使得 DHCP 中继代理（Catalyst 交换机）可将有关其自身和所连接的客户端的信息包括在其中。

DHCP 服务器可利用该信息为服务提供商网络中的每个用户分配 IP 地址、执行访问控制并设置服务质量 (QoS) 和安全策略 (或其他参数分配策略)。

当在交换机中启用 DHCP 监听时，会自动启用选项 82。

如果未对 DHCP 服务器进行配置以使其可处理带选项 82 的数据包，则 DHCP 服务器会停止为该请求分配地址。

要解决此问题，请用全局配置命令 `no ip dhcp relay information option` 在交换机 (中继代理) 中禁用用户标识选项 (82)。

## I. [DHCP数据库代理和DHCP冲突记录日志](#)

DHCP 数据库代理是存储 DHCP 绑定数据库的任何主机，如 FTP、TFTP 或 RCP 服务器。您可以配置多个 DHCP 数据库代理，并且为每个代理配置每次数据库更新和转移之间的间隔。[请使用 `ip dhcp database` 命令配置数据库代理和数据库代理参数。](#)

如果选择不配置 DHCP 数据库代理，请在 DHCP 服务器上禁用 DHCP 地址冲突记录。[执行 `ip dhcp conflict logging` 命令以禁用 DHCP 地址冲突日志记录。可使用 `clear ip dhcp conflict` 清除已记录的冲突。](#)

如果以此方式禁用冲突日志记录失败，则会出现以下错误消息：

```
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)
```

## J. [检查 CDP 以验证 IP 电话连接情况](#)

当与 Cisco IP 电话连接的交换端口禁用了 Cisco 设备发现协议 (CDP) 时，DHCP 服务器无法为电话分配合适的 IP 地址。DHCP 服务器倾向于分配属于数据 VLAN/交换端口子网的 IP 地址。如果已启用 CDP，则交换机能够检测到 Cisco IP 电话对 DHCP 的请求，并提供正确的子网信息。然后，DHCP 服务器可从语音 VLAN/子网池中分配一个 IP 地址。将 dhcp 服务绑定到语音 VLAN 并没有要求明确的步骤。

## K. [删除在SVI下打乱DHCP监听的](#)操作

在 Cisco Catalyst 6500 系列交换机上，将 DHCP 配置为监听特定 VLAN 后，将会自动创建 SVI (处于关闭状态)。此 SVI 的存在对于正确进行 DHCP 监听操作有直接影响。

运行本地 IOS 的 Cisco Catalyst 6500 系列交换机上的 DHCP 监听主要在路由处理器 (RP 或 MSFC) 上实现，而非在交换处理器 (SP 或 Supervisor) 上实现。Cisco Catalyst 6500 系列使用 VACL 拦截硬件中的数据包，VACL 将数据包提供给 RP 预定的本地目标逻辑 (LTL)。帧进入 RP 后，在被传送到监听部分前，首先需要与 L3 接口 (SVI) IDB 关联。如果 SVI 不存在，则 IDB 也将无法存在，数据包将在 RP 处被丢弃。

## L. [有限的广播地址](#)

当 DHCP 客户端在 DHCP 数据包内设置了广播位时，DHCP 服务器和中继代理会将 DHCP 消息发送到具有全 1 广播地址 (255.255.255.255) 的客户端。[如果 `ip broadcast-address` 命令被配置为发送网络广播，则会覆盖 DHCP 发送的全 1 广播。要解决此问题，请使用 `ip dhcp limited-broadcast-`](#)

## [address 命令来确保配置的网络广播不会覆盖默认 DHCP 行为。](#)

除非在连接到客户端的路由器接口上配置了此命令，否则某些 DHCP 客户端只能接受全 1 广播并且无法获得 DHCP 地址。

### [M. 使用路由器 debug 命令调试 DHCP](#)

#### **使用 debug 命令验证路由器是否在接收 DHCP 请求**

在支持软件处理 DHCP 信息包，您能验证的路由器上路由器是否接收从客户端的 DHCP 请求。如果路由器不接收来自客户端的请求，则 DHCP 过程会失败。此故障排除步骤涉及到配置访问列表以供调试输出使用。此访问控制列表只用于调试目的，不会干扰路由器。

在全局配置模式下输入以下访问列表：

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

在执行模式下，输入以下 debug 命令：

```
debug ip packet detail 100
```

输出示例：

```
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
```

以上输出很清楚地说明路由器正在接收来自客户端的 DHCP 请求。输出仅显示数据包总结信息，而不是数据包本身。因此，无法判断数据包是否正确。然而，路由器确实接收了包含正确的（对 DHCP 而言）源和目标 IP 和 UDP 端口的广播数据包。

#### **使用 debug 命令验证路由器是否在接收 DHCP 请求并将其转发至 DHCP 服务器**

可以添加访问列表中的其他条目，以查看路由器是否能与 DHCP 服务器成功通信。同样，这些 debug 输出不显示数据包本身的内容，但您可以确认 DHCP 中继代理是否正在向 DHCP 服务器转发请求。

在全局配置模式下创建以下访问列表：

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

```
access-list 100 permit udp host <dhcp_relay_agent> host <dhcp_server> eq 67
```

```
access-list 100 permit udp host <dhcp_server> host <dhcp_relay_agent> eq 67
```

例如：

```
access-list 100 permit ip host 0.0.0.0 host 255.255.255.0
```

```
access-list 100 permit udp host 192.168.1.1 host 192.168.2.2 eq 67
```

```
access-list 100 permit udp host 192.168.1.1 host 192.168.2.2 eq 68
```

```
access-list 100 permit udp host 192.168.2.2 host 192.168.1.1 eq 67
```

```
access-list 100 permit udp host 192.168.2.2 host 192.168.1.1 eq 68
```

在执行模式下，输入以下 debug 命令：

```
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
```

从以上输出很清楚地看到，路由器正在接收客户端发送的 DHCP 请求并正在按照 DHCP/BootP 中继代理配置向 DHCP 服务器转发请求。DHCP 服务器也对 DHCP/BootP 中继代理进行了直接应答。输出仅显示数据包总结信息，而不是数据包本身。因此，无法确定数据包是否正确或确定服务器是否在用 DHCPNAK 进行回复。然而，路由器确实接收了包含正确的（对 DHCP 而言）源和目标 IP 和 UDP 端口的广播数据包，且与 DHCP 服务器存在着双向通信。

**使用 debug ip udp 命令验证路由器是否在接收和转发 DHCP 请求**

[可以使用 debug ip udp 命令，通过路由器，追踪 DHCP 请求的路径。](#)然而，由于所有处理过的交换 UDP 数据包将显示在控制台中，所以此调试在生产环境中会产生干扰。在生产环境中不应使用此调试。

**警告：**因为 debug ip udp 命令会产生干扰，可能会导致中央处理器 (CPU) 的利用率很高。

在执行模式下，输入以下 debug 命令：

```
debug ip udp
```

输出示例：

```
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.
```

## 使用 debug ip dhcp server packet 命令验证路由器是否在接收和转发 DHCP 请求

如果路由器 IOS 是 12.0.x.T 或 12.1 并支持 IOS DHCP 服务器功能，可以使用 **debug ip dhcp server packet** 命令进行另外的调试。此调试主要用于 IOS DHCP 服务器功能，但也可以用于进行 DHCP/BootP 中继代理功能故障排除。与前面的故障排除步骤一样，由于无法查看实际的数据包，路由器调试输出不能确切地指出问题。但是，这些调试输出允许对 DHCP 处理进行某些推断。

在执行模式下，输入以下 debug 命令：

### debug ip dhcp server packet

```
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.
```

### 同时运行多个调试

同时运行多个调试时，可以发现关于 DHCP/BootP 中继代理和服务器运行情况的许多信息。使用上述故障排除概述，您可以推断 DHCP/BootP 中继代理功能的问题出在哪些地方。

```
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.
```

### 获取嗅探器踪迹并且确定 DHCP 问题的根本原因

使用路由器调试技术并不总是可以确定 DHCP 问题的确切的根本原因。解决 DHCP 问题的最后一步是获得嗅探器跟踪，并提醒进程没有正常操作。要对 DHCP 数据包踪迹进行解码，请参阅本文档的[解码同一 LAN 段上的 DHCP 客户端和服务器的嗅探器踪迹](#)和[解码由配置为 DHCP 中继代理的路由器分隔的 DHCP 客户端和服务器的嗅探器踪迹](#)部分。

有关使用 Catalyst 交换机的交换端口分析程序 (SPAN) 功能获取嗅探器踪迹的信息，请参阅以下文档：

- [配置 Catalyst 交换端口分析程序 \(SPAN\)](#)。

## 使用路由器上的 debug 命令进行数据包解码的其他方法

通过使用

[debug ip packet detail dump <acl>命令](#)在 Cisco 路由器，获得在系统日志或命令行界面 (CLI) 显示的十六进制的一整个数据包是可能的。使用上文中的[使用 debug 命令验证路由器是否在接收 DHCP 请求](#)和[使用 debug 命令验证路由器是否在接收 DHCP 请求并将其转发至 DHCP 服务器](#)部分以及添加到访问列表中的 dump 关键字可以得到相同的调试信息，但数据包的详细信息是以十六进制格式显示的。要确定数据包内容，需要将数据包进行转换。附录 A 中提供了相关示例。

## [在 ip dhcp pool 命令选项 {option\\_number} ASCII 后输入的关键字位于双引号中](#)

重新加载路由器后，任何在 `ip dhcp pool 命令选项 option_number ASCII` 后输入的关键字都在双引号内，这会导致带有配置了选项编号的 DHCP 选项的 Cisco 路由器在尝试解析 URL 时失败。这种情况在运行 IOS 12.4(17a) 的设备上是一个已知 Bug，该 Bug 记录在 [CSCsk96976](#) ( [仅限注册用户](#) ) 中。

此问题在 IOS 版本 12.4(17b)、12.4(18a) 及以上版本和 12.4(19)T1 中已经解决。

## [附录 A : IOS DHCP 示例配置](#)

DHCP 服务器数据库为树状结构。树根是自然网络的地址池，树枝是子网络地址池，树叶是客户端的手动绑定。子网继承网络参数，客户端继承子网参数。所以，应该在树的最高层(网络或子网络)配置共用参数，例如域名。

有关如何配置 DHCP 及其相关命令的详细信息，请参阅以下链接：

- [DHCP 配置任务列表](#)

```
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.
```

## [相关信息](#)

- [VPN 3000 集中器的 DHCP 中继功能的配置示例](#)
- [作为 DHCP 中继的 PIX/ASA 7.x 的配置示例](#)
- [工具和资源](#)
- [技术支持 - Cisco Systems](#)