了解和排除在Catalyst交换机或企业网络的DHCP故障

Contents

Introduction

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。

Prerequisites

Requirements

本文档没有任何特定的前提条件。

Components Used

This document is not restricted to specific software and hardware versions.

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。All of the devices used in this document started with a cleared (default) configuration.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。

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

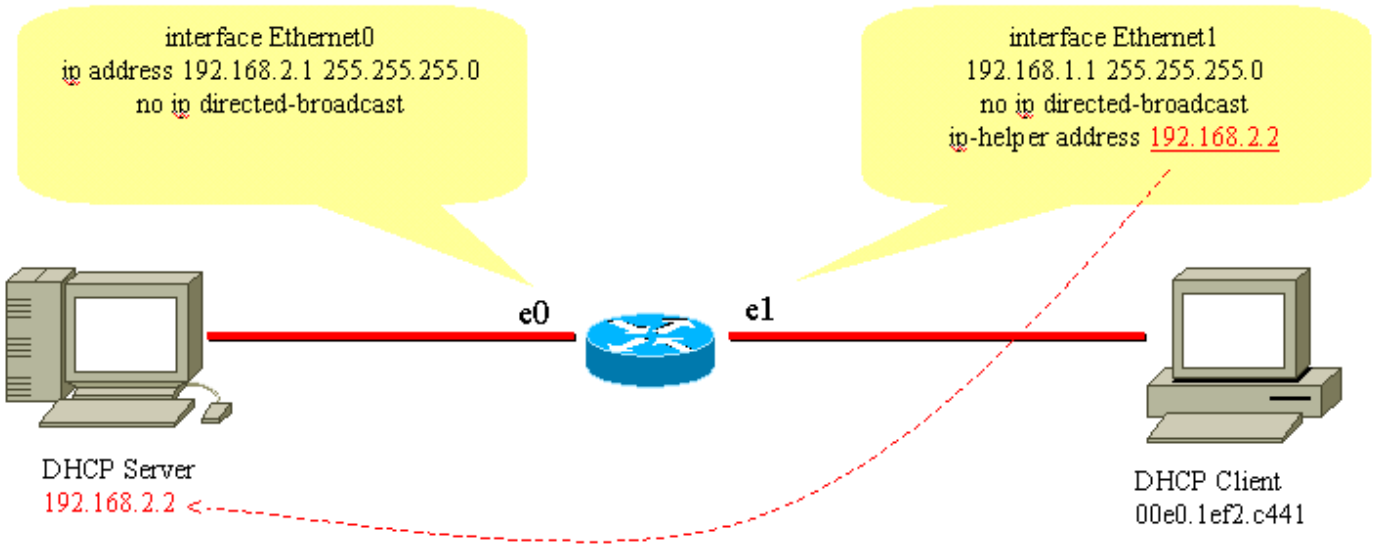
关键概念

这些是DHCP的几个关键概念：

- 因此DHCP客户端最初没有配置的IP地址，并且必须发送广播请求获得从DHCP服务器的一个IP地址。
- 路由器，默认情况下，不转送广播。适应客户端DHCP广播请求是必要的DHCP服务器是否在另一广播域(第3层(L3)网络)。这利用DHCP中继代理执行。
- DHCP中继Cisco路由器实施通过interface-level **IP辅助**命令提供

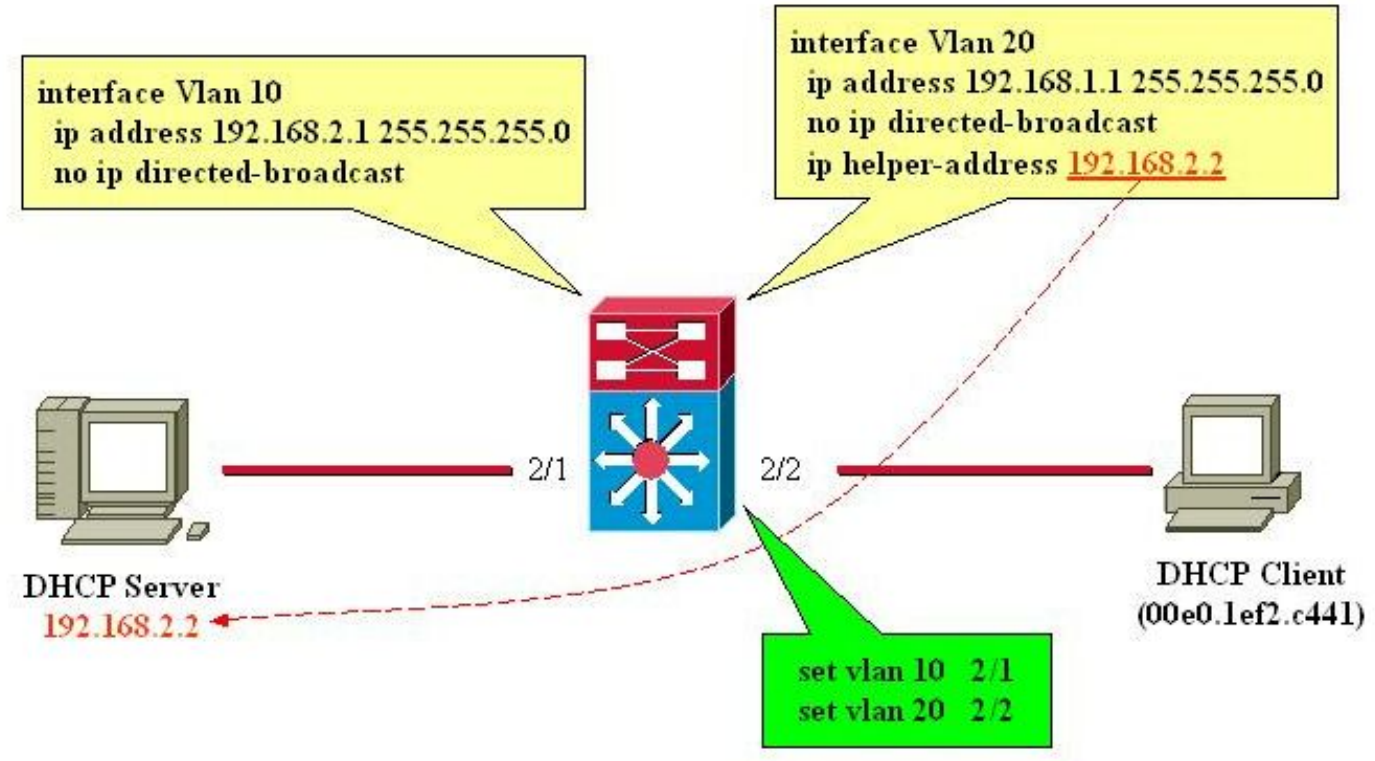
示例情景

情形 1：在DHCP客户端和服务器网络之间的Cisco路由器路由



如此图表所配置的一样，接口Ethernet 1转发客户端的被播放的DHCPDISCOVER到192.168.2.2通过接口Ethernet 1。DHCP服务器通过单播实现请求。对路由器的进一步配置在本例中不是必要的。

方案 2：有L3模块路由的Cisco Catalyst交换机在DHCP客户端和服务器网络之间



如图表所配置的一样，接口VLAN20转发客户端的被播放的DHCPDISCOVER到192.168.2.2通过接口VLAN10。DHCP服务器通过单播实现请求。对路由器的进一步配置在本例中不是必要的。作为主机端口将被配置的交换机端口和有生成树协议(STP)被启用的portfast和被禁用的建立中继和开辟信道。

背景信息

DHCP提供计算机使用传输控制协议/互联网协议的一个机制(TCP/IP)能通过网络自动地得到协议配置参数。DHCP是由互联网工程任务组(IETF)的动态主机配置工作组(DHC-WG)开发 的一个开放标

准 。

DHCP根据客户端服务器示例， DHCP客户端，例如，一部台式机，联系配置参数的一个DHCP服务器。网络管理员典型地在中央位于DHCP服务器并且管理。由于服务器由网络管理员负责，DHCP客户端可以可靠和动态地配置有参数适当对当前网络体系结构。

多数企业网络包括多个子网分开成指虚拟LAN子网络(VLAN)，其中在子网络之间的路由器路由。默认情况下因为路由器不通过广播， DHCP服务器在每个子网必要使用DHCP中继代理功能，除非配置路由器转送DHCP广播。

了解DHCP

DHCP在RFC最初被定义了(RFC) 1531 和从那以后是已废弃的由RFC 2131 。DHCP根据Bootstrap协议(BootP)，在RFC 951被定义 。

工作站用于DHCP (主机)获得初始配置信息，例如IP地址、子网掩码和默认网关启动后。因为每台主机在IP网络需要IP地址沟通， DHCP减轻手工配置每台主机管理负担用IP地址。此外，如果主机移动向一个不同的IP子网，它比那个它以前使用了必须使用一个不同的IP地址。DHCP自动地照料此。它允许主机选择在正确的IP子网的一个IP地址。

当前DHCP RFC参考

- RFC 2131 - DHCP
- RFC 2132 - DHCP选项和BootP供应商扩展名
- RFC 1534 -在DHCP和BootP之间的配合动作
- RFC 1542 -说明和扩展BootP的
- RFC 2241 - Novell目录服务的DHCP选项
- RFC 2242 - Netware/IP域名和信息
- RFC 2489 -定义新的DHCP选项方法

DHCP使用一个或更多服务器的一个客户服务器模型(DHCP服务器)分配IP地址和其他可选配置参数到客户端(主机)在客户端启动。这些配置参数由对客户端的服务器出租某指定的时间的。当主机启动时，在主机的TCP/IP协议栈传送广播(DHCPDISCOVER)消息为了获取一个IP地址和子网掩码，在其他配置参数中。这起动在DHCP服务器和主机之间的交换。在此交换期间，客户端穿过如下所示的几个明确定义的状态：

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

在移动在以上所列的状态之间，客户端和服务器可能交换在下面DHCP信息表里列出的消息类型。

DHCP信息表

参考	消息	请使用
0x	DHCPDISCOVER	客户端寻找可用的DHCP服务器。

01		
0x02	DHCPOFFER	对客户端DHCPDISCOVER的服务器响应。
0x03	DHCPREQUEST	客户端对服务器散播，特定请求从一个服务器的提供的参数，如对信息包定义。
0x04	DHCPDECLINE	客户端服务器通信，表明网络地址已经是在使用中的。
0x05	DHCPACK	与配置参数的服务器到客户通信，包括做的网络地址。
0x06	DHCPNAK	服务器到客户通信，拒绝要求配置参数。
0x07	DHCPRELEASE	客户端服务器通信，放弃网络地址和取消剩余的租赁。
0x08	DHCPINFORM	客户端服务器通信，请求仅本地配置参数客户端外部已经配置了作为地址。

DHCPDISCOVER

当客户端第一次时启动，它在初始化状态被认为，并且传输一个DHCPDISCOVER信息在其在用户数据报协议(UDP)端口67 (BOOTP服务器)的内部物理子网。因为客户端没办法认识它属于的子网，DHCPDISCOVER是所有子网广播(目的地IP地址255.255.255.255)，用0.0.0.0的IP原地址。因为客户端没有一个配置的IP地址， IP原地址是0.0.0.0。如果DHCP服务器在此本地子网存在并且是被配置和正确地运行， DHCP服务器将听到广播并且回应DHCPOFFER信息。如果DHCP服务器在本地子网不存在，必须有在转发DHCPDISCOVER信息的此本地子网的一个DHCP/bootp中继代理到包含一个DHCP服务器的子网。

此中继代理可以是一台专用的主机(例如，微软视窗服务器)，或者路由器(例如，与界面水平IP辅助语句的一Cisco路由器上配置)。

DHCPOFFER

接受一个DHCPDISCOVER信息的DHCP服务器可能回应一个DHCPOFFER信息在UDP端口68 (BOOTP客户端)。客户端接受DHCPOFFER并且搬入选择的状态。此DHCPOFFER信息包含客户端初始配置信息。例如， DHCP服务器用申请的IP地址将填写yiaddr字段DHCPOFFER信息。子网掩码和默认网关在选项域、子网掩码和路由器选项指定，分别。在DHCPOFFER信息的其他普通的

选项包括IP地址租用时间、更新时间、域名服务器和NetBIOS名称服务器(WINS)。DHCP服务器在chaddr将发送DHCPOFFER到广播地址，但是包括客户端硬件地址提供领域，因此客户端知道它是有意目的地。在DHCP服务器不在本地子网情况下， DHCP服务器将送回DHCPOFFER，作为一个单播信息包，在UDP端口67，到DHCPDISCOVER来自的DHCP/bootp中继代理。DHCP/bootp中继代理根据BOOTP客户端设置的广播标志位然后将播放或单播在本地子网的DHCPOFFER在UDP端口68。

DHCPREQUEST

在客户端接受DHCPOFFER后，回应DHCPREQUEST信息，指示其目的接受在DHCPOFFER的参数和移动到请求的状态。客户端可能从接受DHCPDISCOVER信息的原始的每个DHCP服务器收到多个DHCPOFFER消息，一个。客户端选择一个DHCPOFFER并且回应仅该DHCP服务器，隐含地拒绝其他DHCPOFFER消息。客户端通过填充Server Identifier选项字段鉴别所选服务器用DHCP服务器IP地址。DHCPREQUEST也是广播，那么发送DHCPOFFER将看到DHCPREQUEST，并且中的每一个知道的所有DHCP服务器其DHCPOFFER是否被接受了或被拒绝了。客户端需要的所有更多的配置选项在选项域将包括的DHCPREQUEST信息。即使提供了客户端一个IP地址，将发送DHCPREQUEST信息用0.0.0.0的IP原地址。此时，客户端未接受验证使用IP地址是确切的。

DHCPACK

在DHCP服务器接受DHCPREQUEST后，承认与DHCPACK信息的请求，因而完成初始化进程。DHCPACK信息有DHCP服务器的一个IP原地址，并且目的地地址再次是广播并且包含客户端在DHCPREQUEST信息要求的所有参数。当客户端接受DHCPACK时，在网络加入限制状态，并且当前是自由的使用IP地址沟通。同时，使用客户端标识符或chaddr， DHCP服务器在其数据库存储租赁和独特识别它和相关的IP地址。两客户端和服务器将使用标识的此组合是指租赁。客户端标识符是设备的MAC地址加上媒体类型。

在DHCP客户端开始使用新的地址前， DHCP客户端必须计算与一个被出租的地址产生关联的时间参数，是租用时间(IT)、更新时间(T1)和重新绑定时间(T2)。典型的默认LT是72小时。若需要您能花更短的租赁时间保存地址。

DHCPNAK

如果所选服务器无法满足DHCPREQUEST信息， DHCP服务器将回应DHCPNAK信息。当客户端接受一个DHCPNAK信息或者不收到对DHCPREQUEST信息时的答复，客户端通过进入重新启动配置流程请求的状态。客户端在重新启动初始化状态前在60秒以内将重新传输DHCPREQUEST至少四次。

DHCPDECLINE

客户端接受DHCPACK，并且可选地执行在参数的一个最终检查。客户端通过发送地址解析服务(ARP)要求执行此程序IP地址提供在DHCPACK。如果客户端发现地址通过收到给ARP请求的一个回复已经是在使用中，客户端将发送一个DHCPDECLINE信息到服务器并且通过进入重新启动配置流程请求的状态。

DHCPINFORM

如果客户端通过一些其它方法获得了一个网络地址或有一个手工配置的IP地址，客户端工作站可能使用Request信息的DHCPINFORM得到其他本地配置参数，例如域名和域名服务器(DNSs)。接受DHCPINFORM信息构建的DHCP服务器一个DHCPACK信息与任何本地配置参数适当为客户端，不

用分配一个新的IP地址。此DHCPACK将被发送单播到客户端。

DHCPRELEASE

DHCP客户端可能选择通过发送DHCPRELEASE信息放弃其在网络地址的租赁到DHCP服务器。客户端识别将发布的租赁使用字段和网络地址在DHCPRELEASE信息。如果需要扩大当前DHCP池范围，请去除当前地址池并且指定IP地址的新的范围在DHCP池下。为了取消您希望在DHCP池的特定IP地址或地址范围，请使用ip dhcp excluded-address命令。

Note: 如果设备使用BOOTP，无限长度租赁在路由器DHCP捆绑显示。

更新租赁

因为IP地址从服务器只被租用，必须时常更新租赁。当租用时间一半的到期了(T1=0.5 x LT)，客户端将设法更新租赁。客户端进入更新的状态并且发送DHCPREQUEST信息到服务器，拿着当前租赁。如果同意更新租赁，切断将回复请求更新与DHCPACK信息。在早先租赁期间情况下，在任何变动做对服务器DHCPACK信息将包含新的租赁和所有新的配置参数。由于某种原因如果客户端无法到达拿着租赁的服务器，将尝试更新从所有DHCP服务器的地址，在原始DHCP服务器未回答在时间T2内后的更新请求。DEFAULT值T2是(7/8 x LT)。这意味着T1 < T2< LT。

如果客户端以前有一个DHCP指定的IP地址，并且被重新启动，客户端特定将请求在DHCPREQUEST信息包的以前被租用的IP地址。此DHCPREQUEST将有IP原地址作为0.0.0.0和目的地作为IP广播地址255.255.255.255。

发送DHCPREQUEST的客户端在重新启动期间不能填写服务器indentifier领域，并且必须填写Option字段的申请的IP地址。RFC兼容客户端将严格填充与地址的ciaddr字段被请求而不是DHCP选项字段。DHCP服务器将接受任一个方法。DHCP服务器的工作情况取决于一定数量的要素，例如一旦Windows NT DHCP服务器，版本的操作系统使用，以及其他要素，例如superscoping。如果DHCP服务器确定客户端能仍然使用申请的IP地址，它将保持无声或发送DHCPREQUEST的DHCPACK。如果服务器确定客户端不能使用申请的IP地址，将送回DHCPNACK到客户端。客户端然后将迁移向初始化状态，并且发送DHCPDISCOVER信息。

Note: DHCP服务器分配从IP地址池的底下IP地址到DHCP客户端。当底下地址的租赁到期时，分配到另一个客户端，如果被请求。您不能做在命令DHCP地址的任何变动分配。

DHCP信息包

DHCP信息依长度而变并且包括在下表列出的字段。

Note: 此信息包是原始BOOTP信息包的一个修正的版本。

字段	字节	名字	说明
操作	1	操作码	识别信息包作为请求或回复：1=BOOTREQUEST， 2=BOOTREPLY
htype	1	硬件类型	指定网络硬件地址类型。

hlen	1	硬件长度	指定长度硬件地址长度。
跳跃	1	跳跃	如果请求在路由器间，转发客户端调整值到零和值增量。
XID	4	交易ID	由客户端选择的随机数。为特定DHCP处理使用交换的所有DHCP消息ID (XID)。
秒	2	秒钟	因为DHCP进程开始了，指定秒钟的编号。
标志位	2	标志位	指示消息是否将是广播或单播。
ciaddr	4	客户端IP地址	只使用，当客户端认识其IP地址和一旦区域时，请更新或者REBINDING状态。
yiaddr	4	您的IP地址	如果客户端IP地址是0.0.0.0， DHCP服务器在此字段将安置提供的客户端IP地址。
siaddr	4	服务器IP地址	如果客户端认识DHCP服务器的IP地址，此字段将带有DHCP服务器地址。否则，用于DHCPOFFER和DHCPACK从DHCP服务器。
giaddr	4	路由器IP地址(GIADDR)	网关IP地址，填写由DHCP/bootp中继代理。
chaddr	16	客户端MAC地址	DHCP客户端MAC地址。
sname	64	服务器名	可选的服务器主机主机名。
文件	128	引导程序文件名	引导程序文件名。

选项	可选择变参数	可以由DHCP服务器提供的可选参数。RFC 2132给出所有可能的选项。

获得客户端和DHCP服务器在相同子网驻留的DHCP地址的客户端的客户端服务器会话

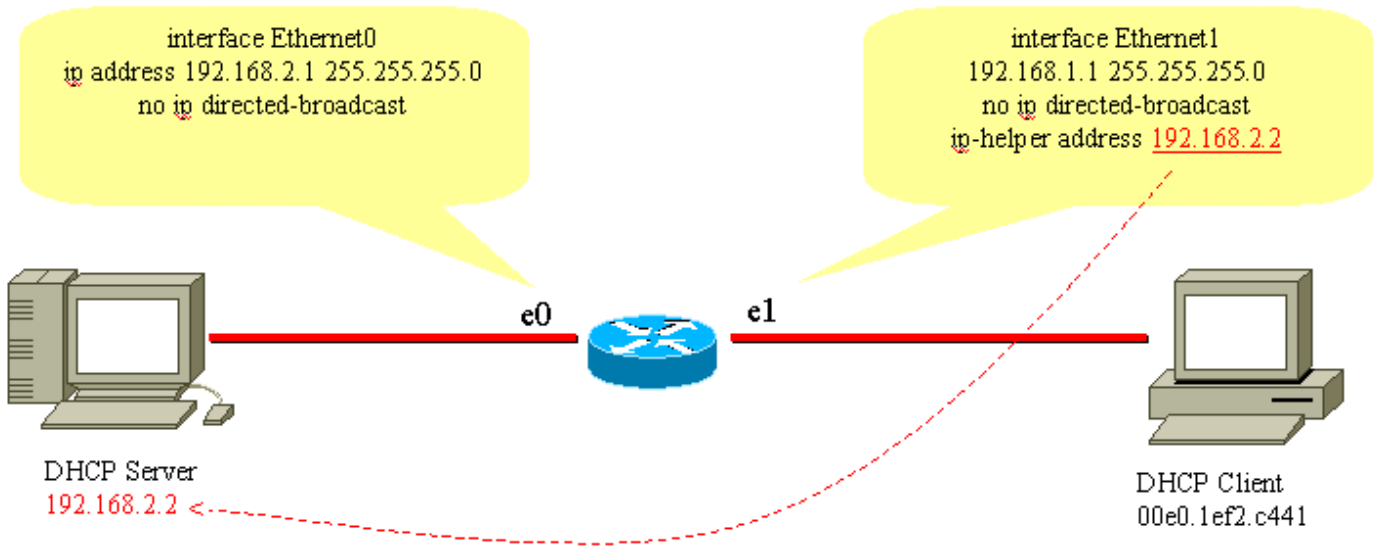
信息包说明	源MAC地址	目的地MAC地址	来源IP地址	目的地IP地址
DHCPDISCOVER	客户端	广播	0.0.0.0	255.255.255.255
DHCPOFFER	DHCPServer	广播	DHCPServer	255.255.255.255
DHCPREQUEST	客户端	广播	0.0.0.0	255.255.255.255
DHCPACK	DHCPServer	广播	DHCPServer	255.255.255.255

DHCP/bootp中继代理的角色

路由器，默认情况下，不会转发广播包。因为DHCP客户端消息使用255.255.255.255 (所有网广播)的目的地IP地址， DHCP客户端不能发送请求到在一个不同的子网的一个DHCP服务器，除非DHCP/bootp中继代理在路由器被配置。DHCP/bootp中继代理代表DHCP客户端将转发DHCP请求到DHCP服务器。DHCP/bootp中继代理将添附其自己的IP地址对去DHCP服务器的DHCP帧的IP原地址。这允许DHCP服务器通过单播回应DHCP/bootp中继代理。DHCP/bootp中继代理也将填充网关IP Address字段用DHCP信息从客户端被接受接口的IP地址。DHCP服务器使用IP Address字段的网关确定DHCPDISCOVER， DHCPREQUEST或者DHCPINFORM信息产生的子网。

配置DHCP/bootp在Cisco IOS路由器的中继代理功能

配置Cisco路由器转发BootP或DHCP请求是简单的-请配置指向DHCP/bootp服务器的一个IP辅助工具地址，或者指向网络的子网广播地址服务器打开。例如，请考虑以下网络图：



要转发自客户端的BootP/DHCP请求到DHCP服务器，使用ip helper-address interface命令。可以配置IP辅助工具地址转送根据UDP端口号的所有UDP广播。默认情况下， IP辅助工具地址将转送以下UDP广播：

- 简单文件传输协议(TFTP) (端口69)
- DNS (端口53)，时钟服务(端口37)
- NetBIOS名称服务器(端口137)
- NetBIOS数据报服务器(端口138)
- 引导程序协议(DHCP/bootp)客户端和服务器数据包(端口67和68)
- 终端存取控制访问控制系统(TACACS)服务(端口49)
- IEN-116域名服务(端口42)

IP辅助工具地址能处理UDP广播到单播或播放IP地址。**然而，没有推荐使用IP辅助工具地址转送从一个子网的UDP广播到另一个子网广播地址，由于可能发生的很多广播泛滥。**多个IP在单个接口的辅助地址条目支持，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路由器不支持的DHCP服务器负载均衡被配置作为DHCP中继代理。Cisco路由器寄DHCPDISCOVER信息给为该接口提及的所有帮助地址。当DHCPDISCOVER、DHCPOFFER和DHCPREQUEST/DHCPDECLINE消息被交换在每个对DHCP客户端和服务器之间，有服务两个或多个的DHCP服务器子网只增加DHCP流量。

设置手工的捆绑

有两种方式设置手工的捆绑;一是为Windows主机，并且其他是为非Windows主机。有两个不同的命令用于配置;一是为Microsoft DHCP客户端，并且其他是为非Microsoft DHCP客户端：client-identifier **DHCP** (手工的捆绑- Microsoft DHCP客户端)和**DHCP硬件地址**(手工的捆绑-非Microsoft DHCP客户端)。两个不同的命令的原因是以Windows运行的PC修改其橡皮防水布，并且**01**在地址初加。以下为示例配置：

- 下列是Microsoft DHCP客户端的配置

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

- 下列是非Microsoft DHCP客户端的配置

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

如何做DHCP工作在附属IP分段

默认情况下， DHCP有一个限制因为发送回复信息包，只有当请求从接口收到配置有主要IP地址。DHCP流量使用广播地址。当DHCP请求由路由器接口时收到，寄它给DHCP服务器(当配置IP辅助工具地址)时有在接口配置的主要IP的源地址的告诉DHCP服务器哪个IP池在DHCP回复信息包必须使用(为客户端)。

没有办法知道的路由器DHCP广播请求是否来自在接口配置的第二IP网络的设备。作为解决方法，可以配置(在设备被连接到路由器支持dot1q标记)条件下分离两个子网的子接口配置，因此他们两个适当地获得他们对应的IP地址。

如果备用地址是首选的方法，有另一个解决方法，是对enable (event) global configuration命令ip dhcp聪明中继。这有一个限制因为只使用第二IP传递DHCP请求，如果没有自DHCP服务器的无响应在三个连续的要求以后主要的地址池。

DHCP客户端与DHCP中继功能的服务器会话

下面的表说明DHCP客户端的进程能获得从DHCP服务器的一个IP地址。此表在网络以上图表以后被模拟。每个数值在图表中表示下述的信息包。此表是参考点了解的DHCP客户端服务器会话信息包流。此表为确定DHCP问题哪里也是有用的可能发生。

信息包	客户端IP地址	服务器IP地址	GI地址	信息包源MAC地址	信息包源IP地址	信息包目的地MAC地址	信息包目的地IP地址
1. DHCPDISCOVER从客户端被发送。	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.ffff (广播)	255.255.255.255
2. 路由器接受在E1接口的DHCPDISCOVER。路由器认为此信息包是DHCP UDP广播。路由器作为DHCP/bootp中继代理并且填装IP Address字段的网关用流入的端口IP地址，当前更改IP原地址到一个流入的端口IP地址，并且转发请求直接地到DHCP服务器。	0.0.0.0	0.0.0.0	192.168.1.1	接口E2 MAC地址	192.168.1.1	DHCP服务器MAC地址	192.168.2.2

			1				
3. DHCP服务器接受了DHCPDISCOVER和发送DHCPOFFER到DHCP中继代理。	192.168.1.2	192.168.2.2	192.168.1.1	DHCP服务器MAC地址	192.168.2.2	接口E2 MAC地址	192.168.1.1
4. DHCP中继代理接受DHCPOFFER和转送在本地LAN的DHCPOFFER广播。	192.168.1.2	192.168.2.2	192.168.1.1	接口E1 MAC地址	192.168.1.1	ffff.ffff.ffff (广播)	255.255.255.255
5. 从客户端发送的DHCPREQUEST。	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.ffff (广播)	255.255.255.255
6. 路由器接受在E1接口的DHCPREQUEST。路由器认为此信息包是DHCP UDP广播。路由器作为DHCP中继代理并且填装IP Address字段的网关用流入的端口IP地址，当前更改IP原地址到一个流入的端口IP地址，并且转发请求直接地到DHCP服务器。	0.0.0.0	0.0.0.0	192.168.1.1	接口E2 MAC地址	192.168.1.1	DHCP服务器MAC地址	192.168.2.2
7. DHCP服务器接受了DHCPREQUEST和发送DHCPACK到DHCP/bootp中继代理。	192.168.1.2	192.168.2.2	192.168.1.1	DHCP服务器MAC地址	192.168.2.2	接口E2 MAC地址	192.168.1.1

8. DHCP/bootp中继代理接受DHCPACK和转送在本地LAN的DHCPACK广播。客户端将接受ACK并且使用客户端IP地址。	192.168.1.2	192.168.2.2	192.168.1.1	接口E1 MAC地址	192.168.1.1	ffff.ffff.ffff (广播)	255.255.255.255

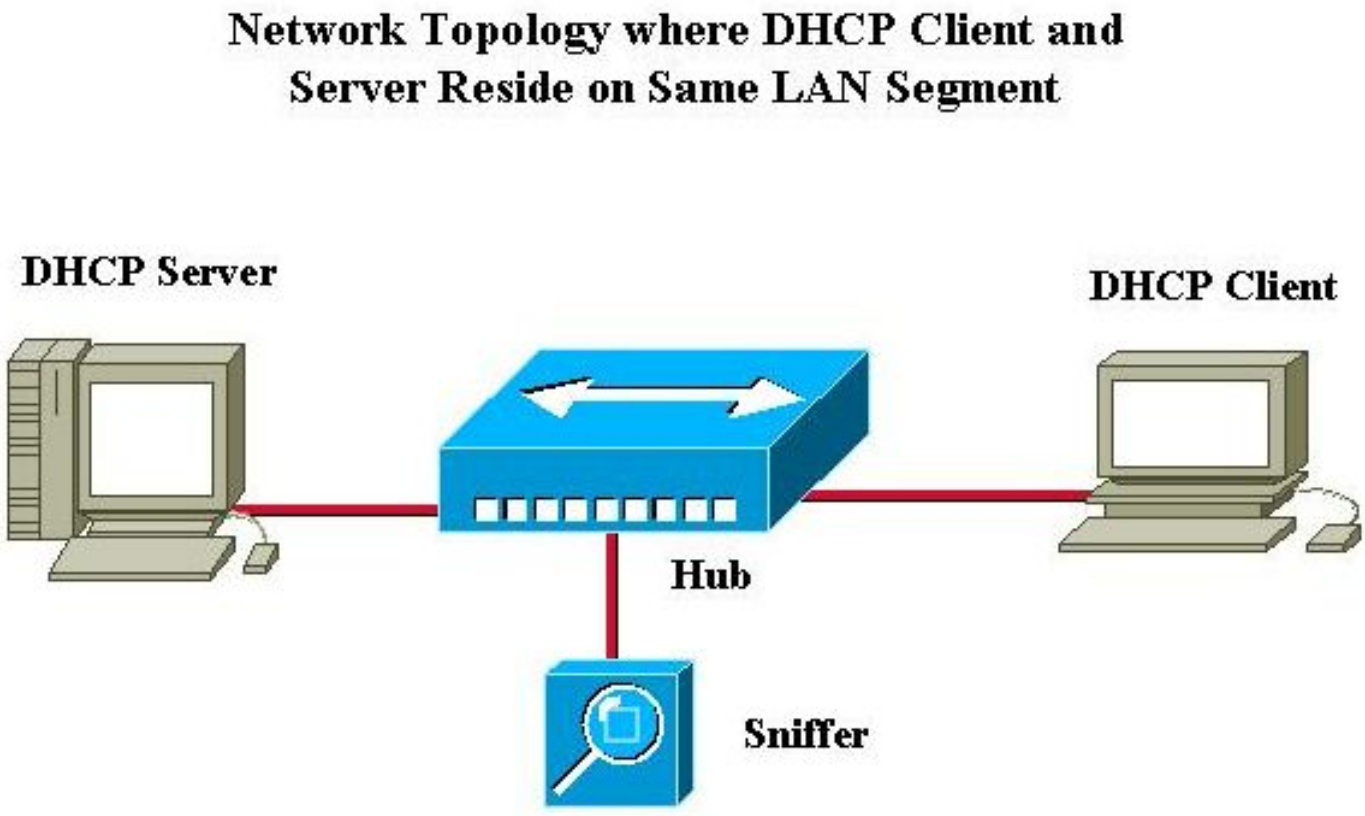
Pre-Execution Environment (PXE)启动DHCP考虑

Pre-Execution Environment (PXE)允许工作站从在网络的一个服务器引导在引导操作系统之前在本地硬盘驱动器。网络管理员不物理的必须访问特定工作站和手工引导它。操作系统和其它软件，例如诊断程序，可以被装载在设备上从一个服务器在网络。PXE环境配置它的用途DHCP是IP地址。

如果DHCP服务器位于网络的另一个路由段，在路由器必须执行DHCP/bootp中继代理配置。必须配置在本地路由器接口的ip helper-address命令。请参见在本文的Cisco IOS路由器部分的配置的DHCP/bootp中继代理功能配置信息。

了解和排除DHCP故障使用嗅探器跟踪

DHCP客户端和服务器解码嗅探器跟踪在同一LAN段



下面的嗅探器跟踪包括六个帧。这六个帧说明DHCP的一个工作的方案， DHCP客户端和服务器在同一个物理或逻辑分段驻留。当排除DHCP故障时，匹配您的嗅探器跟踪到下面跟踪是重要的。也许有一些区别与下面跟踪比较，但是一般信息包流应该正确地是相同的。信息包踪影跟随早先讨论关于DHCP如何工作。

```
- - - - - - - - - - - - - - - - - - - - - - - - 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 1arrived at 11:52:03.8106; frame size is 618 (026A hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, 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 - DHCPOFFER** -
- -

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 FFFFFFFFFFFF**, 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 Renewel 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 FFFFFFFFFFFF**, 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

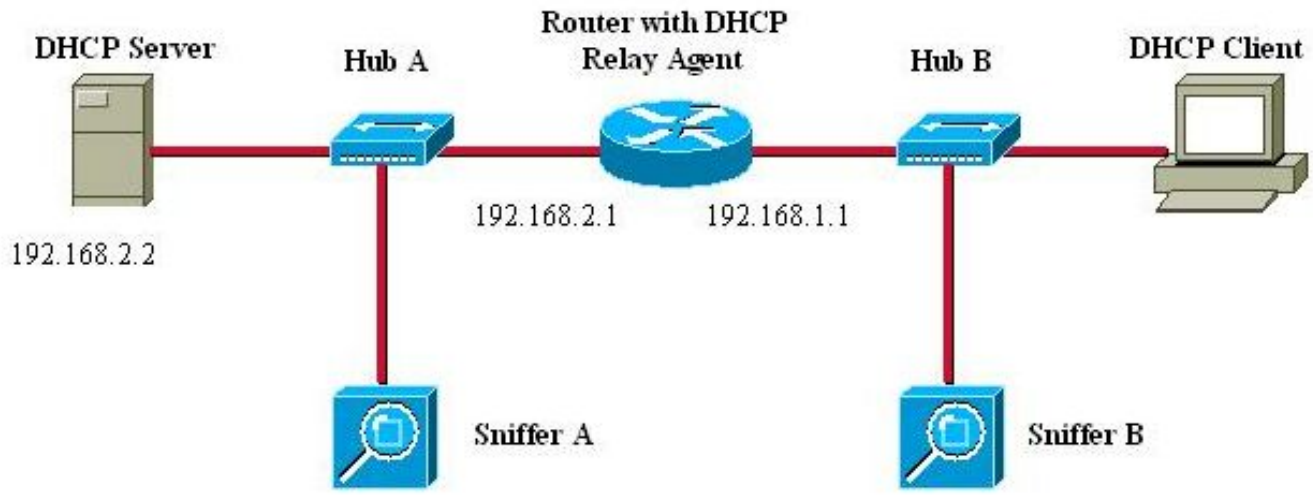
```
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B987 (correct)
IP: Source address = [0.0.0.0]
IP: Destination address = [255.255.255.255]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 68 (BootPc/DHCP)
UDP: Destination 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 FFFFFFFFFFFF**, 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 Renewel 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 FFFFFFFFFFFF, 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 = FFFFFFFFFFFF
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 FFFFFFFFFFFF, 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 = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

DHCP客户端解码嗅探器跟踪和服务器由被配置作为DHCP中继代理的路由器分离了

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



sniffer-b跟踪

```
- - - - - - - - - - - - - - - - - - - - - - - - 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 FFFFFFFFFFFF, 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 - DHCPOFFER** -

```
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 FFFFFFFFFFFF, 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 Renewel 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 FFFFFFFFFFFF, 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 FFFFFFFFFFFF, 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 Renewel 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 FFFFFFFFFFFF, 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 = FFFFFFFFFFFF
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 FFFFFFFFFFFF, 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 = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

Sniffer-A跟踪

```
- - - - - - - - - - - - - - - - - - - - - - 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 - DHCPOFFER - - - - - - - - - - - - - - - - - - -
- -

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 Renewel 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 Renewel 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DHCP故障，当客户端工作站无法获得DHCP地址

案例分析 1：在同一LAN段的DHCP服务器或VLAN作为DHCP客户端

当DHCP服务器和客户端在同一LAN段时驻留或VLAN和客户端无法获得从DHCP服务器的一个IP地址，不太可能本地路由器引起DHCP问题。问题很可能与连接DHCP服务器和DHCP客户端的设备有关。然而，问题可能是DHCP服务器或客户端。在下面排除模块故障之后应该确定什么设备导致问题。

Note: 要配置在a的DHCP服务器每个VLAN基础，请定义服务DHCP地址的每个VLAN的不同的DHCP池对您的客户端。

案例分析 2：DHCP服务器和DHCP客户端由为DHCP/bootp中继代理功能配置的路由器分离

当DHCP服务器和客户端在不同的LAN分段或VLAN时驻留，功能作为DHCP/bootp中继代理的路由器对转发DHCPREQUEST负责到DHCP服务器。要求另外的故障排除步骤排除DHCP/bootp中继代理故障、以及DHCP服务器和客户端。在下面排除模块故障之后应该确定哪个设备导致问题。

在路由器的DHCP服务器不能分配与池用尽的错误的Adresses

很可能，一些地址由客户端仍然暂挂，即使他们从池发布。这可以由**显示IP DHCP冲突**输出验证。当两台主机使用同样IP地址，地址冲突发生。在地址分配， DHCP检查冲突与ping和无偿ARP。

如果发现冲突，地址从池被去除。地址分配，直到管理员解决冲突。请勿配置**ip dhcp conflict logging**解决此问题。

DHCP排除模块故障

了解DHCP问题哪里能发生

DHCP问题能出现由于一许多原因。多数常见原因是配置问题。然而，许多DHCP问题可以由软件缺陷引起的操作系统、网络接口卡(NIC)驱动程序或者运行在路由器的DHCP/bootp中继代理。由于

潜在有问题的区域的数量，对排除故障需要一个系统的方法。

DHCP问题的可能的原因最后的名单：

- Catalyst交换机默认配置
- DHCP/bootp中继代理配置
- NIC兼容性问题或DHCP的特点问题
- 有故障的NIC或不正确的网卡驱动程序安装
- 由于断断续续的网络中断常去生成树计算
- 操作系统的工作情况或软件缺陷
- DHCP服务器范围配置或软件缺陷
- Cisco Catalyst交换机或IOS DHCP/bootp中继代理软件缺陷
- 单播逆向路径转发(URPF)检查失败，因为DHCP提供在一个不同的接口比预计被接受。当反向路径转发(RPF)时功能在接口被启用， Cisco路由器能丢弃有0.0.0.0源地址和255.255.255.255的目的地地址的动态主机配置协议(DHCP)和Bootstrap协议(BOOTP)信息包。路由器能也丢弃有一个组播IP目的地在接口的所有IP信息包。此问题在CSCdw31925 (仅限注册用户)描述。
- 没有使用DHCP数据库代理，但是DHCP冲突记录不是失效的

本文将使用下面排除模块故障如上面列表所示确定根本原因。

A. 验证物理连接

此程序是可适用的对所有案例研究。

首先，请验证DHCP客户端和服务器的物理连接性。如果连接到Catalyst交换机，请验证DHCP客户端和服务器有物理连接性。

对于Catalyst CatOS交换机例如2948G， 4000， 5000和6000系列交换机，使用**show port <mod->/<port_range>命令**注释端口状态。除如果端口状态是任何，端口不会通过任何数据流，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IOS基本交换机例如Catalyst 2900XL/3500XL/2950/3550，对**show port status的**等效命令是**show interface <interface>**。如果接口的状态是任何除<interface>之外是UP，线路通信协议是UP，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)
```

如果物理连接被验证了，并且的确没有Catalyst交换机和DHCP客户端之间的链路，请参见排除Cisco Catalyst交换机故障对NIC另外的故障排除的兼容性问题文件关于物理层连通性问题。

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。参考恢复从在CatOS平台的错误禁用端口状态，并且在Cisco IOS平台的错误禁用端口状态恢复，描述errDisable状态，解释如何从它恢复，并且提供恢复示例从此状态的。

B. 测试网络连接通过配置客户端工作站用静态IP地址

此程序是可适用的对所有案例研究。

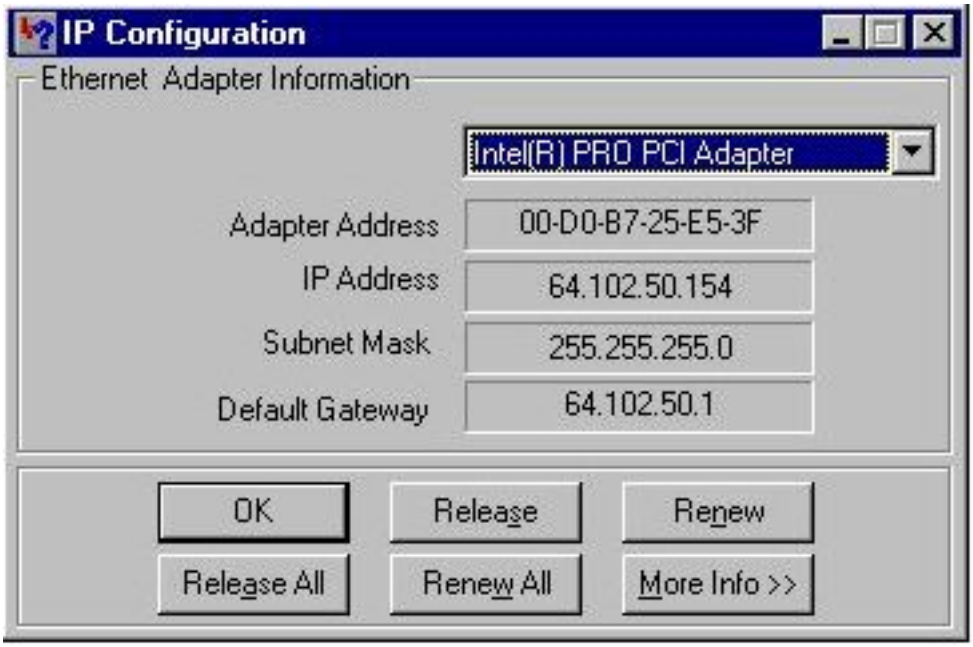
当排除所有DHCP问题故障时，通过配置在客户端工作站的一个静态IP地址验证网络连通性是重要的。如果工作站无法到达尽管有一个静态配置的IP地址的网络资源，问题的根本原因不是DHCP。这时，需要网络连通性故障排除。

C. 验证问题作为启动问题

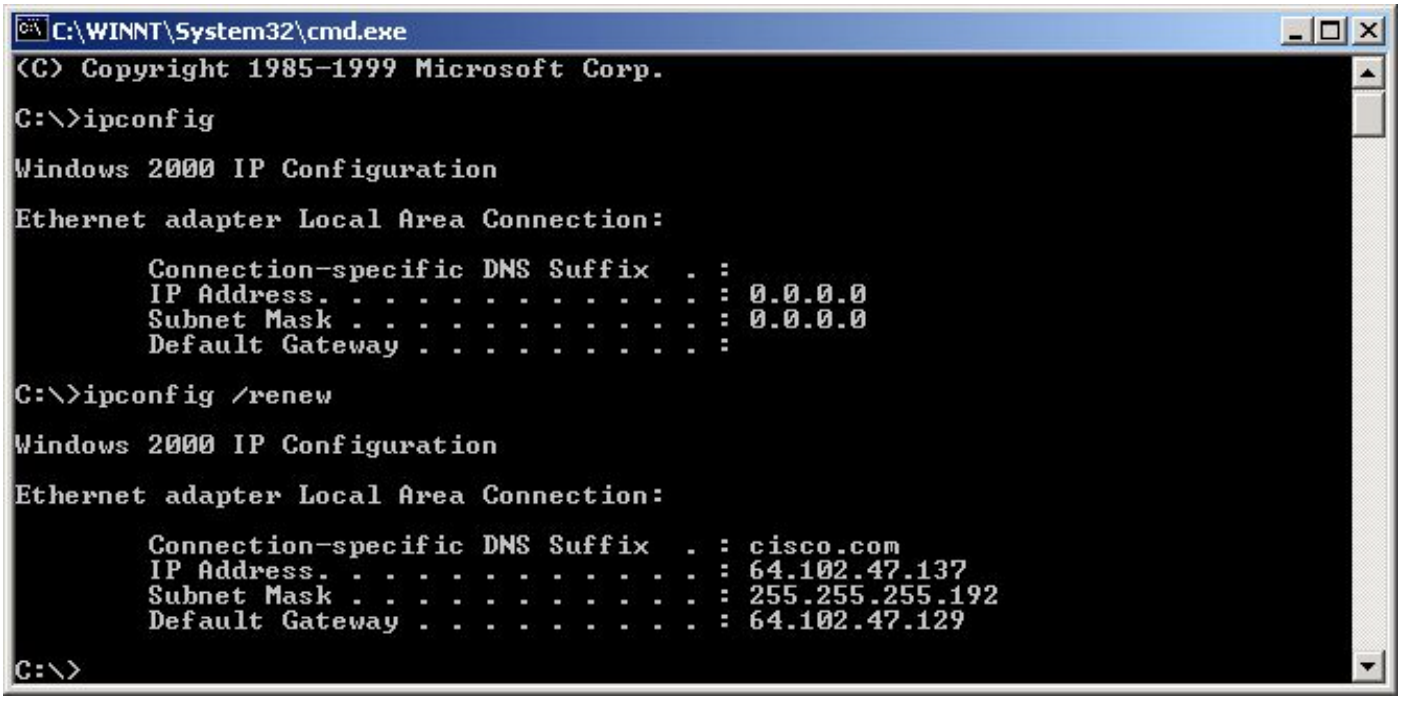
此程序是可适用的对所有案例研究。

如果DHCP客户端无法获得从DHCP服务器的一个IP地址在启动，请尝试通过手工迫使客户端发送DHCP请求获得从DHCP服务器的一个IP地址。发布以下步骤手工获得从一个DHCP服务器的一个IP地址的操作系统如下所示。

Microsoft Windows 95/98/me ：点击**开始按钮**，并且运行WINIPCFG.exe程序。点击ReleaseAll**按钮**，跟随由RenewAll**按钮**。当前DHCP客户端能获得IP地址？



Microsoft Windows NT/2000 ：通过键入在**Start/Run**字段的**cmd**打开命令提示符窗口。发出在命令提示符窗口的ipconfig/renew命令，如下所示。当前DHCP客户端能获得IP地址？



如果DHCP客户端能通过手工更新IP地址获得IP地址，在PC完成了启动流程后，问题是很可能DHCP启动问题。如果DHCP客户端连接Cisco Catalyst交换机，问题很可能归结于涉及STP portfast并且/或者开辟信道和建立中继的配置问题。其他可能性包括NIC卡问题和交换端口启动问题。应该检查故障排除步骤D和E排除交换机端口配置和NIC卡问题作为DHCP问题的根本原因。

D. 验证交换机端口配置(STP Portfast和其他命令)

如果交换机是Catalyst 2900/4000/5000/6000，请验证端口有STP portfast被启用和Trunking/开辟信道被禁用。默认配置是STP portfast被禁用的和Trunking/开辟的自动，如果适用。对于2900XL/3500XL/2950/3550交换机， STP portfast是唯一的必需的配置。这些配置更改解决发生在Catalyst交换机的一次初始安装的最普通的DHCP客户端问题。

对于关于必要的交换机端口配置需求的更多文档的DHCP正常运行，当连接到Catalyst交换机，请查看以下文件：

使用Portfast和其他命令修正工作站启动连通性延迟

在查看在以上的本文的配置指南以后，请回到另外的故障排除的本文。

E. 检查已知NIC卡或Catalyst交换机问题

如果Catalyst交换机配置是正确的，很可能，软件兼容性问题在可能导致DHCP问题的Catalyst交换机或DHCP客户端的NIC可能存在。在排除故障的下一步是查看以下文件和排除与可能造成问题的Catalyst交换机或NIC的所有软件问题：

排除对NIC兼容性问题的Cisco Catalyst交换机故障

DHCP客户端的操作系统以及特定NIC信息知识例如制造商、型号和驱动版本将是需要的适当地排除所有兼容性问题。

F. 区分DHCP客户端是否获得在相同子网的IP地址或VLAN作为DHCP服务器

区分是重要的DHCP是否正确地作用，当客户端是在相同子网或VLAN作为DHCP服务器时。如果DHCP在相同子网或VLAN正确地运作作为DHCP服务器， DHCP问题可能是DHCP/bootp中继代理。如果问题持续甚而与测试在相同子网的DHCP或VLAN作为DHCP服务器，问题可能实际上是DHCP服务器。

G. 验证路由器DHCP/bootp中继配置

发布下面步骤验证配置：

1. 当配置在路由器时的DHCP中继，请验证**ip helper-address命令**位于正确的接口。**ip helper-address命令**一定是存在DHCP客户端工作站的Inbound接口，并且必须处理到正确的DHCP服务器。
2. 验证全局配置no service dhcp命令不存在。此配置参数将禁用在路由器的所有DHCP服务器和中继功能。默认配置， `service dhcp`，不会出现于配置，并且default configuration命令。如果service dhcp不是启用的，客户端从DHCP服务器不收到IP地址。**Note:** 在运行更旧的Cisco IOS的路由器中发布， ip bootp server命令运用DHCP中继代理功能而不是**service dhcp命令**。因此， **ip bootp server命令**需要被启用在这些路由器，如果配置**ip helper-address命令**转送DHCP UDP广播和适当地作为DHCP中继代理代表DHCP客户端。
3. 当适用**IP辅助工具地址时**发出命令转送UDP广播到子网广播地址，验证`no ip directed-broadcast`在UDP广播信息包需要横断的任何出局接口没有被配置。no ip directed-broadcast在定向广播的所有转换将阻拦对物理广播。此接口配置是在软件版本12.0及以上版本的默认配置。
4. 转送DHCP广播到DHCP服务器的子网广播地址是一个偶尔的软件问题。当排除DHCP故障时，总是请尝试转送DHCP UDP广播到DHCP服务器IP地址，如下所示：

H. 用户标识(82)选项打开

DHCP relay agent information (选项82)功能enable (event)包括关于本身和连接的客户端的信息的DHCP中继代理(Catalyst交换机)，当转发自DHCP客户端的DHCP请求到DHCP服务器。

DHCP服务器能使用此信息分配IP地址，进行访问控制和为服务提供商网络的每个订户设置服务质量(QoS)和安全策略(或其他参数分配策略)。

当监听的DHCP在交换机被启用，自动它enable (event)选项82。

如果没有配置DHCP服务器处理与选项82的信息包，停止分配地址到该请求。

为了解决此问题，请禁用用户标识选项(82)在交换机(中继代理)用全局配置命令， **no ip dhcp relay信息选项**。

I. DHCP数据库代理和DHCP冲突记录

DHCP数据库代理是该所有的主机—例如， FTP、TFTP或者RCP服务器—存储DHCP约束数据库。您能配置多个DHCP数据库代理程序，并且您能配置在数据库更新和转移之间的间隔每个代理程序的。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，请禁用DHCP地址冲突记录在DHCP服务器的。执行**没有**ip dhcp conflict logging命令禁用DHCP地址冲突记录。清除与清楚的IP DHCP冲突的以前被记录的冲突。

如果这不能禁用冲突记录，此错误信息出现：

```
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 IP电话连接

当被连接到Cisco IP电话时的连接孔有思科设备发现协议(CDP)被禁用， DHCP服务器不能分配一个适当的IP地址到电话。DHCP服务器倾向于分配属于连接孔的数据VLAN/子网的IP地址。如果CDP是启用的，交换机能发现Cisco IP电话请求DHCP，并且能提供正确的子网信息。DHCP服务器然后能定量从语音VLAN/子网池的一个IP地址。没有明确步骤要求捆绑dhcp服务到语音VLAN。

K. 去除在SVI下打乱DHCP监听的操作

在Cisco Catalyst 6500 series switches， SVI (在关闭状态)自动地被创建，在配置DHCP为特定VLAN后监听。此SVI出现有在监听DHCP的正确的操作的直接暗示。

监听在Cisco Catalyst 6500 series switches的DHCP实现主要在路由处理器(运行本地IOS的RP或MSFC)，不在交换处理器(SP或Supervisor)。Cisco Catalyst 6500 series在硬件方面截断提供信息包给Local Target Logic (LTL)被预订由RP的信息包有VACLs的。一旦帧输入RP，他们首先需要与L3接口(SVI) IDB产生关联，在他们可以通过到监听的部分前。没有SVI，此IDB不存在，并且信息包在RP被撤销。

L. 有限的广播地址

当DHCP客户端设置在DHCP信息包时的广播位， DHCP服务器和中继代理传送DHCP信息到有全1广播地址的(255.255.255.255)客户端。如果配置ip broadcast-address命令发送网络广播，DHCP发送的全1广播被改写。为了修正此情况，请使用IP DHCP有限广播地址命令保证配置的网络广播不改写默认DHCP工作情况。

除非此命令在路由器接口被配置被连接到客户端，一些DHCP客户端能只接受全1广播并且不能获取DHCP地址。

M. 调试DHCP使用路由器调试指令

验证使用调试指令，路由器收到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从客户端收到DHCP请求。如果路由器从客户端，不收到请求DHCP进程将发生故障。此故障排除步骤包括配置调试输出的一访问列表。此访问列表只为调试目的是并且不是插入的对路由器。

在全局配置模式下，请进入以下访问列表：

access-list 100 permit ip主机0.0.0.0主机255.255.255.255

在exec模式下，请输入以下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
```

从以上输出，很清楚路由器从客户端收到DHCP请求。此输出只显示信息包而不是信息包的汇总。所以，确定是不可能的信息包是否是正确的。然而，路由器收到了有为DHCP是正确的来源和目的地IP和UDP端口的一个广播包。

验证使用调试指令，路由器收到DHCP请求和转发请求到DHCP服务器

在访问列表的其它条目可以被添加发现路由器是否与DHCP服务器成功通信。再次，这些调试不显出到信息包，但是您能确认DHCP中继代理是否是转发请求到DHCP服务器。

在全局配置模式下，请建立以下访问列表：

access-list 100 permit ip主机0.0.0.0主机255.255.255.255

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

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

例如：

access-list 100 permit ip主机0.0.0.0主机255.255.255.0

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

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

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

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

在exec模式下，请输入以下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，很清楚路由器从客户端收到DHCP请求并且转发请求，每种DHCP/bootp中继代理配置，到DHCP服务器。DHCP服务器也回复直接地DHCP/bootp中继代理。此输出只显示信息包而不是信息包的汇总。所以，确定是不可能的信息包是否是正确的或服务器是否回复以DHCPNAK。然而，路由器收到了有为DHCP是正确的来源和目的地IP和UDP端口的一个广播包，并且有双向通信用DHCP服务器。

验证路由器是收到和转发DHCP请求使用debug ip udp命令

debug ip udp命令可以用于通过路由器跟踪DHCP请求的路径。然而，因为所有被处理的交换式UDP信息包将显示给控制台，此调试是插入的在生产环境里。此调试不应该用于生产。

警告： debug ip udp命令是插入的，并且可能引起高中央处理器(CPU)利用率。

在exec模式下，请输入以下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 DHCPOFFER 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 DHCPOFFER 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.
```

验证路由器是收到和转发DHCP请求使用debug ip dhcp server packet命令

如果路由器IOS是12.0.x.T或12.1并且支持IOS DHCP服务器功能，使用**debug ip dhcp server packet命令，**另外的调试可以进行。此调试供与IOS DHCP服务功能的使用使用，但是可以用于排除DHCP/bootp中继代理功能故障。因为实际数据包不可能查看，如同早先故障排除步骤，路由器调试不提供问题的一个确切的确定。然而，调试允许推断关于dhcp处理做。

在exec模式下，请输入以下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/INRORM 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 DHCPOFFER and DHCPNAK. !-
-- Client's MAC address is 00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY to client
00e0.1ef2.c441. !--- Router is forwarding DHCPOFFER 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 DHCPOFFER and DHCPNAK. !--- Client's MAC address is 00e0.1ef2.c441. 00:20:54: DHCPD:
broadcasting BOOTREPLY to client 00e0.1ef2.c441. !--- Router is forwarding DHCPOFFER or DHCPNAK
broadcast on local LAN interface.
```

同时运行多个调试

当同时时运行多个调试，适当数量的信息可以关于DHCP/bootp中继代理和服务器的操作被发现。使用在故障排除分级显示之上，您能做的DHCP/bootp中继代理功能可能不正确地运行的推断关于。

```
Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
!--- Router received DHCPDISCOVER/REQUEST/INRORM 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 DHCPOFFER and DHCPNAK. !-
-- Client's MAC address is 00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY to client
00e0.1ef2.c441. !--- Router is forwarding DHCPOFFER 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 DHCPOFFER and DHCPNAK. !--- Client's MAC address is 00e0.1ef2.c441. 00:20:54: DHCPD:
broadcasting BOOTREPLY to client 00e0.1ef2.c441. !--- Router is forwarding DHCPOFFER or DHCPNAK
broadcast on local LAN interface.
```

获得嗅探器跟踪并且确定DHCP问题的根本原因

使用路由器调试技术永远不会确定DHCP问题的确切的根本原因。在解决DHCP问题的最后的步骤将获得嗅探器跟踪和注释进程哪里不正确地作用。DHCP信息包跟踪可以通过参考DHCP客户端解码在同一LAN段的嗅探器跟踪和路由器分离的服务器和解码DHCP客户端嗅探器跟踪解密和服务器被配置作为本文的DHCP中继代理部分。

关于获得嗅探器跟踪的信息使用在Catalyst交换机的交换端口分析器(SPAN)功能，请参见以下文件：

- 配置Catalyst Switched Port Analyzer (SPAN)。

数据包解码的其它方法使用在路由器的调试

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。使用验证路由器收到DHCP请求使用调试指令并且验证路由器收到DHCP请求，并且对DHCP服务器的转发请求使用调试指令部分以上，与dump关键字一起被添加到访问列表，将提供同样调试信息，但是关于在十六进制的信息包详细信息。要确定信息包的内容，信息包将需要转换。示例在附录A提供。

在ip dhcp pool命令选项{option_number} ASCII以后被输入的关键字在双引号

有一DHCP选项的一个Cisco路由器用选件编号配置能遇到故障，如果设法解析URL，因为任何关键字被输入，在**ip dhcp pool命令选项*选件编号***ASCII在双引号后，在路由器被重新载入后。此工作情

况在运行IOS 12.4(17a)，是一个已知Bug和描述在CSCsk96976的设备被看到(仅限注册用户)。

此问题在IOS版本12.4(17b)， 12.4(18a)及以后被解决和12.4(19)T1。

附录 A：IOS DHCP配置示例

DHCP服务器数据库被组织作为树。树的根是自然网络的地址池，分组是子网络地址池，并且分支是手工的捆绑给客户端。子网络继承网络参数，并且客户端继承子网络参数。例如所以，应该配置共用参数，域名，在树的最高的(网络或子网络)水平。

关于如何用它配置DHCP和associated命令的更多信息，请参见以下链接：

- DHCP配置任务表

```
Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
!--- Router received DHCPDISCOVER/REQUEST/INRORM 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
DHCPOFFER and DHCPNAK. !--- Client's MAC address is
00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY
to client 00e0.1ef2.c441. !--- Router is forwarding
DHCPOFFER 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
DHCPOFFER and DHCPNAK. !--- Client's MAC address is
00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY
to client 00e0.1ef2.c441. !--- Router is forwarding
DHCPOFFER or DHCPNAK broadcast on local LAN interface.
```

Related Information

- 在VPN 3000 Concentrator配置示例的DHCP中继功能
- PIX/ASA 7.x作为DHCP中继配置示例
- 工具和资源
- Technical Support - Cisco Systems