

# Identificar e Solucionar Problemas do Dynamic Host Configuration Protocol no Catalyst Switch ou em Redes Corporativas

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Principais conceitos](#)

[Cenários de exemplo](#)

[Entender o DHCP](#)

[Referências RFC de DHCP atuais](#)

[Tabela de mensagens DHCP](#)

[DHCPDISCOVER](#)

[DHCPOFFER](#)

[DHCPREQUEST](#)

[DHCPACK](#)

[DHCPNAK](#)

[DHCPDECLINE](#)

[DHCPINFORM](#)

[DHCPRELEASE](#)

[Renove o leasing](#)

[Tabela de pacotes DHCP](#)

[Conversa o cliente-servidor para cliente que obt m o endere o DHCP onde o cliente e o servidor DHCP residem na mesma sub-rede](#)

[Fun o do agente de transmiss o de DHCP/BootP](#)

[Configurar o recurso DHCP/BootP Relay Agent no roteador Cisco IOS®](#)

[Definir Associa es Manuais](#)

[Como fazer com que o DHCP funcione em segmentos IP secund rios](#)

[Conversa entre cliente e servidor DHCP com a fun o DHCP Relay](#)

[Processo para um cliente DHCP obter um endere o IP](#)

[Considera es sobre DHCP de inicializa o do ambiente de pr -execu o \(PXE\)](#)

[Entender e solucionar problemas do DHCP com farejadores de rastreamento](#)

[Decodificar o farejador de rastreamento do cliente e servidor DHCP no mesmo segmento de LAN](#)

[Topologia de rede onde o cliente e o servidor DHCP residem no mesmo segmento de LAN](#)

[Decodificar farejador de rastreamento de cliente e servidor DHCP separados por um roteador configurado como agente de retransmiss o DHCP](#)

[Rastreamento do farejador B](#)

[Rastreamento Sniffer-A](#)

[Solucionar problemas do DHCP quando as estações de trabalho clientes não conseguem obter endereços DHCP](#)

[Casos Práticos 1: Servidor DHCP no mesmo segmento LAN ou VLAN em que se encontra o cliente DHCP](#)

[Casos Práticos 2: O servidor DHCP e o cliente DHCP são separados por um roteador configurado para a funcionalidade DHCP/BootP Relay Agent](#)

[O servidor DHCP no roteador falha ao atribuir o endereço com um erro POOL EXHAUSTED](#)

[Módulos de Troubleshooting de DHCP](#)

[Entender onde podem ocorrer problemas de DHCP](#)

[Lista breve com causas possíveis para os problemas de DHCP:](#)

[A. Verificar a conectividade física](#)

[C. Verifique o Problema como um Problema de Inicialização](#)

[D. Verifique a configuração da porta do Switch \(STP Portfast e outros comandos\)](#)

[E. Verifique se há problemas conhecidos de placa de rede ou switch Catalyst](#)

[F. Distinguir se os clientes DHCP obtêm o endereço IP na mesma sub-rede ou VLAN que o servidor DHCP](#)

[G. Verifique a configuração do roteador DHCP/BootP Relay](#)

[H. Opção Identificação Do Assinante \(82\) Ativada](#)

[I. Agente de banco de dados DHCP e registro de conflitos DHCP](#)

[J. Verifique o CDP para conexões de telefone IP](#)

[K. A remoção do SVI interrompe a operação de rastreamento de DHCP](#)

[L. Endereço de Broadcast Limitado](#)

[M. Debug DHCP With Router Debug Commands](#)

[Saída de exemplo](#)

[Saída de exemplo](#)

[Apêndice A: Exemplo de configuração do DHCP do Cisco IOS](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve como solucionar vários problemas comuns com o Dynamic Host Configuration Protocol (DHCP) em uma rede de switch Cisco Catalyst.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

**Note:** Somente clientes Cisco registrados têm acesso a relatórios de bugs internos.

## Informações de Apoio

O DHCP fornece um mecanismo pelo qual os computadores que usam o protocolo TCP/IP podem obter os parâmetros de configuração de protocolo automaticamente através da rede. [O DHCP é um padrão aberto que foi desenvolvido pelo Grupo de trabalho de configuração dinâmica de hosts \(DHC-WG\) da Internet Engineering Task Force \(IETF\)](#).

O DHCP é baseado em um paradigma cliente-servidor, em que o cliente DHCP, por exemplo, um computador desktop, entra em contato com um servidor DHCP para obter os parâmetros de configuração. O servidor DHCP normalmente está em uma localização central e é operado pelo administrador da rede. Como o servidor é executado por um administrador de rede, os clientes DHCP podem ser configurados com confiança e dinamicamente com os parâmetros adequados para a arquitetura de rede atual.

A maioria das redes corporativas consiste em várias sub-redes divididas em sub-redes denominadas VLANs (LANS virtuais), onde os roteadores fazem roteamento entre as sub-redes de comunicação. Como os roteadores não passam broadcasts por padrão, um servidor DHCP seria necessário em cada sub-rede, a menos que os roteadores estejam configurados para encaminhar o broadcast DHCP com o recurso DHCP Relay Agent.

## Principais conceitos

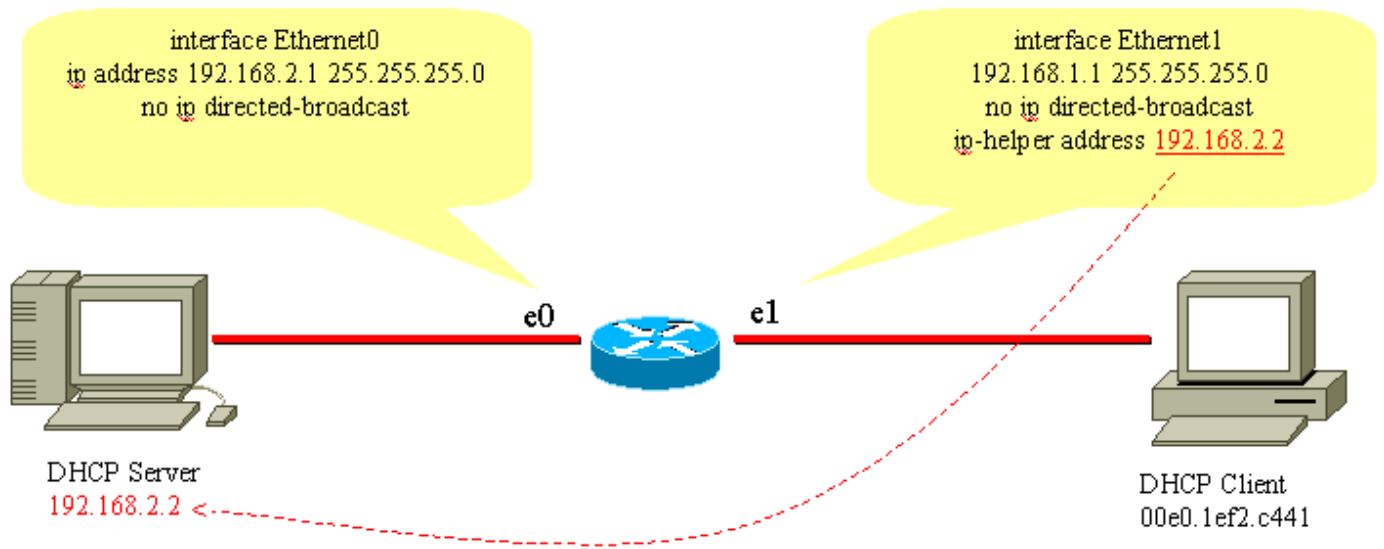
Esses são vários conceitos importantes do DHCP:

- Inicialmente, os clientes DHCP não têm endereço IP configurado e, portanto, devem enviar uma solicitação de broadcast para obter um endereço IP de um servidor DHCP.
- Por padrão, os roteadores não encaminham transmissões. Será necessário acomodar solicitações de broadcast DHCP clientes se o servidor DHCP estiver em outro domínio de broadcast (rede da Camada 3 (L3)). Isso é feito com o uso de um Agente de Retransmissão DHCP.
- A implementação do roteador Cisco do relé DHCP é fornecida através dos comandos **ip helper na interface**

## Cenários de exemplo

### Cenário 1: Roteamento do roteador Cisco entre redes cliente e servidor DHCP

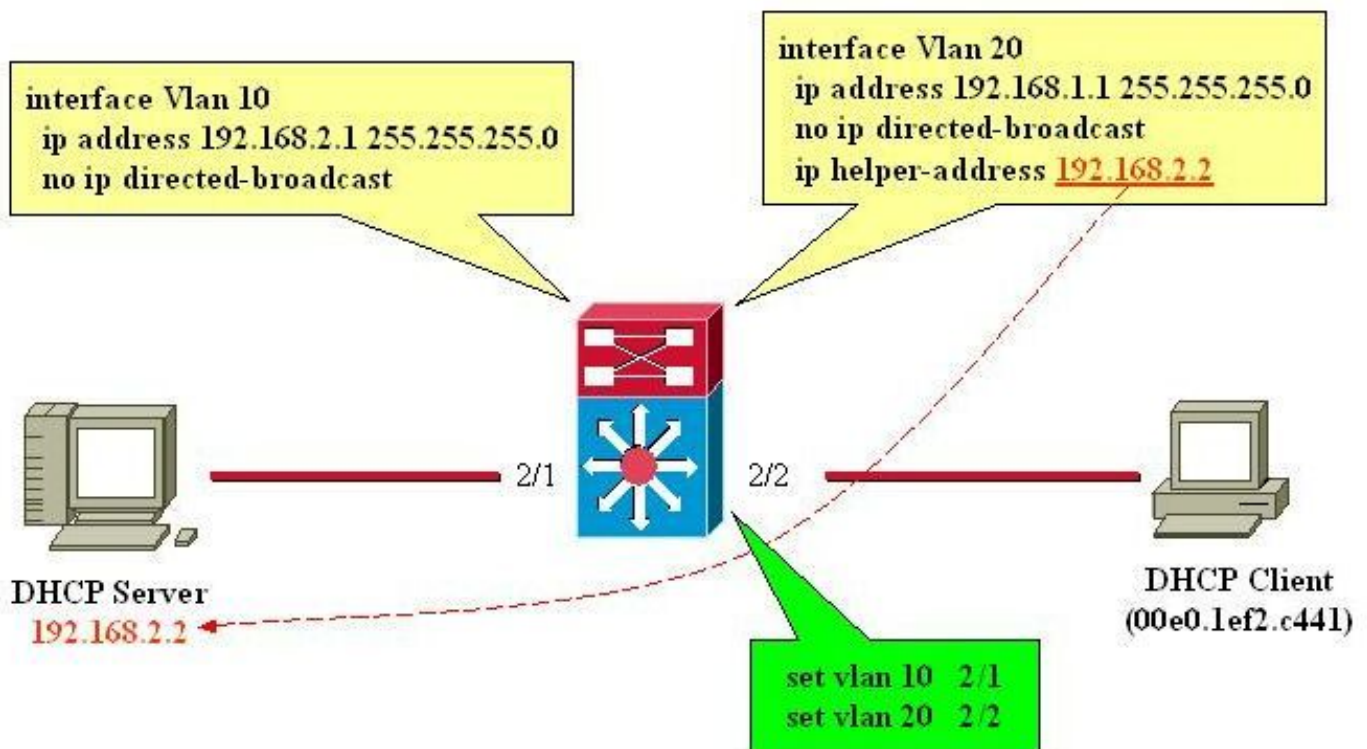
Conforme configurado neste diagrama, a interface Ethernet1 encaminha o cliente transmitiu DHCPDISCOVER para 192.168.2.2 através da interface Ethernet1. O servidor DHCP preenche a solicitação através de unicast. Nenhuma outra configuração para o roteador é necessária neste exemplo.



Roteamento entre redes cliente e servidor DHCP

## Cenário 2: Switch Cisco Catalyst com Módulo L3 Roteamento entre Redes de Cliente e Servidor DHCP

Conforme configurado no diagrama, a interface VLAN20 encaminha o cliente transmitiu DHCPDISCOVER para 192.168.2.2 através da interface VLAN10. O servidor DHCP preenche a solicitação através de unicast. Nenhuma outra configuração para o roteador é necessária neste exemplo. As portas do switch precisam ser configuradas como portas de host e ter PortFast STP (Spanning-Tree Protocol) ativado e entroncamento e canalização desativados.



Rota do módulo L3 entre redes cliente e servidor DHCP

## Entender o DHCP

O DHCP foi originalmente definido em [Requests for Comments \(RFCs\) 1531](#) e desde então está

obsoleto pelo [RFC 2131](#). O DHCP é baseado no Protocolo de Bootstrap (BootP), que é definido no [RFC 951](#).

O DHCP é usado pelas estações de trabalho (hosts) para obter informações de configuração inicial, como um endereço IP, uma máscara de sub-rede e um gateway padrão durante a inicialização. Com o DHCP, não é necessário configurar manualmente cada host com um endereço IP. Além disso, se um host for movido para uma sub-rede IP diferente, ele deve usar um endereço IP diferente do anterior. O DHCP faz disso automaticamente. Ele permite que o host escolha um endereço IP na sub-rede IP correta.

## Referências RFC de DHCP atuais

- RFC 2131 - DHCP
- Opções DHCP do RFC2132 e Extensões do Fornecedor do BootP
- RFC 1534 - Interoperação entre DHCP e BootP
- RFC 1542 - Esclarecimentos e Extensões para o Protocolo BootP
- RFC 2241 – Opções DHCP para Novell Directory Services
- RFC 2242 - Netware/IP Domain Name and Information
- RFC 2489 - Procedimento para definir novas opções de DHCP

O DHCP usa um modelo de cliente e servidor, em que um ou mais servidores (servidores DHCP) alocam endereços IP e outros parâmetros de configuração opcionais a clientes (hosts) após a inicialização de clientes. Esses parâmetros de configuração são usados do servidor para o cliente por um determinado tempo. Quando um host é inicializado, a pilha TCP/IP no host transmite uma mensagem de transmissão (DHCPDISCOVER) para obter um endereço IP e uma máscara de sub-rede, entre outros parâmetros de configuração. Isso inicia uma troca entre o servidor DHCP e o host. Durante essa troca, o cliente passa por esses estados bem definidos:

1. Inicializando
2. Seleção
3. Solicitação
4. Limite
5. Renovando
6. Religação

Para se mover entre esses estados, o cliente e o servidor podem trocar os tipos de mensagens listados na Tabela de Mensagens DHCP.

## Tabela de mensagens DHCP

Referência	Mensagem	Descrição
0x01	DHCPDISCOVER	O cliente procura os servidores DHCP disponíveis.
0x02	DHCPOFFER	A resposta do servidor para o cliente DHCPDISCOVER.
0x03	DHCPREQUEST	O cliente envia broadcasts para o servidor, solicita parâmetros oferecidos de um servidor especificamente, conforme definido no pacote.
0x04	DHCPDECLINE	A comunicação cliente-servidor indica que o endereço de rede já está em uso.
0x05	DHCPACK	A comunicação servidor-cliente com parâmetros de configuração, juntamente com endereço de rede comprometido.

0x06	DHCPNAK	A comunicação servidor-cliente recusa a solicitação do parâmetro de configuração.
0x07	DHCPRELEASE	A comunicação cliente-servidor renuncia o endereço de rede e cancela o aluguel restante.
0x08	DHCPINFORM	A comunicação cliente-servidor solicita somente parâmetros de configuração local que o cliente já tenha configurado externamente como um endereço.

## DHCPDISCOVER

Quando um cliente é inicializado pela primeira vez, diz-se que ele está no estado inicializando, e transmite uma mensagem DHCPDISCOVER em sua sub-rede física local pela porta 67 de UDP (servidor de BootP). Como o cliente não tem como saber a sub-rede à qual pertence, o DHCPDISCOVER é um broadcast de todas as sub-redes (endereço IP de destino 255.255.255.255), com um endereço IP de origem 0.0.0.0. O endereço IP de origem é 0.0.0.0 já que o cliente não tem um endereço IP configurado. Se um servidor DHCP existir nesta sub-rede local e estiver configurado e operar corretamente, o servidor DHCP ouvirá o broadcast e responderá com uma mensagem DHCPOFFER. Se um servidor de DHCP não existe na sub-rede local, ela deve conter um agente de transmissão de DHCP/BootIP para encaminhar a mensagem DHCPDISCOVER para uma sub-rede que contenha um servidor de DHCP.

Esse agente de retransmissão pode ser um host dedicado (por exemplo, o Microsoft Windows Server) ou um roteador (por exemplo, um roteador Cisco configurado com instruções IP helper no nível da interface).

## DHCPOFFER

Um servidor DHCP que recebe uma mensagem DHCPDISCOVER pode responder com uma mensagem DHCPOFFER na porta UDP 68 (cliente BootP). O cliente recebe o DHCPOFFER e vai para o estado Seleção. Essa mensagem DHCPOFFER contém informações de configuração inicial para o cliente. Por exemplo, o servidor DHCP preenche o campo yiaddr da mensagem DHCPOFFER com o endereço IP solicitado. A máscara da sub-rede e o gateway padrão estão especificados no campo de opções, nas opções de máscara de sub-rede e roteador, respectivamente. Outras opções comuns na mensagem DHCPOFFER incluem o tempo de concessão de Endereço IP, tempo de renovação, servidor de nome de domínio e servidor de nomes NetBIOS (WINS). O servidor DHCP envia o DHCPOFFER para o endereço de broadcast, mas inclui o endereço de hardware do cliente no campo chaddr da oferta, para que o cliente saiba que é o destino pretendido. Caso o servidor DHCP não esteja na sub-rede local, o servidor DHCP enviará o DHCPOFFER, como um pacote unicast, na porta UDP 67, de volta ao Agente de Transmissão DHCP/BootP do qual veio o DHCPDISCOVER. O Agente de Transmissão DHCP/BootP envia ou envia por unicast o DHCPOFFER na sub-rede local na porta UDP 68, que depende do flag de Transmissão definido pelo cliente Bootp.

## DHCPREQUEST

Depois que o cliente recebe um DHCPOFFER, ele responde com uma mensagem DHCPREQUEST, indica sua intenção de aceitar os parâmetros no DHCPOFFER e entra no estado Requesting (Solicitando). O cliente pode receber várias mensagens DHCPOFFER, uma de cada servidor DHCP que recebeu a mensagem original DHCPDISCOVER. O cliente escolhe

um DHCPOFFER e responde somente a esse servidor DHCP e, implicitamente, recusa todas as outras mensagens DHCPOFFER. O cliente identifica o servidor selecionado depois de preencher o campo de opção Identificador do servidor com o endereço IP do servidor DHCP. O DHCPREQUEST também é um broadcast, portanto todos os servidores DHCP que enviaram um DHCPOFFER veem o DHCPREQUEST, e cada um sabe se o DHCPOFFER foi aceito ou recusado. Quaisquer opções de configuração adicionais que o cliente exigir serão incluídas no campo de opções da mensagem DHCPREQUEST. Mesmo que o cliente tenha recebido um endereço IP, ele envia a mensagem DHCPREQUEST com um endereço IP de origem 0.0.0.0. Neste momento, o cliente ainda não recebeu a verificação de que está claro para usar o endereço IP.

## **DHCPACK**

Depois que o servidor DHCP recebe o DHCPREQUEST, ele confirma a solicitação com uma mensagem DHCPACK e conclui o processo de inicialização. A mensagem DHCPACK tem o endereço IP de origem do servidor DHCP e o endereço de destino é mais uma vez uma transmissão e contém todos os parâmetros que o cliente solicitou na mensagem DHCPREQUEST. Quando o cliente recebe o DHCPACK, ele entra no estado Bound (Vinculado) e agora fica livre para usar o endereço IP para se comunicar com a rede. Enquanto isso, o servidor DHCP armazena o aluguel em seu banco de dados e o identifica exclusivamente com o identificador do cliente ou chaddr e o endereço IP associado. O cliente e o servidor usam essa combinação de identificadores para fazer referência ao aluguel. O identificador de cliente é o endereço MAC do dispositivo mais o tipo de mídia.

Antes de o cliente DHCP começar a usar o novo endereço, ele deve calcular os parâmetros de tempo associados a um endereço alugado, que são Tempo de concessão (LT), Tempo de renovação (T1) e Tempo de reassociação (T2). O LT de padrão típico é 72 horas. Você pode usar tempos de arrendamento mais curtos para conservar endereços, se for necessário.

## **DHCPNAK**

Se o servidor selecionado não puder atender à mensagem DHCPREQUEST, o servidor DHCP responderá com uma mensagem DHCPNAK. Quando o cliente recebe uma mensagem DHCPNAK ou não recebe uma resposta a uma mensagem DHCPREQUEST, ele reinicia o processo de configuração quando entra no estado Requesting (Solicitando). O cliente retransmite o DHCPREQUEST pelo menos quatro vezes em 60 segundos antes de reiniciar o estado de Inicialização.

## **DHCPDECLINE**

O cliente recebe o DHCPACK e, opcionalmente, executa uma verificação final nos parâmetros. O cliente executa esse procedimento quando envia as solicitações do Address Resolution Protocol (ARP) para o endereço IP fornecido no DHCPACK. Se o cliente detectar que o endereço já está em uso quando receber uma resposta à solicitação ARP, ele enviará uma mensagem DHCPDECLINE ao servidor e reiniciará o processo de configuração no estado Requesting (Solicitando).

## **DHCPINFORM**

Se um cliente tiver obtido um endereço de rede por algum outro meio ou tiver um endereço IP configurado manualmente, uma estação de trabalho cliente poderá usar uma mensagem de

solicitação DHCPINFORM para obter outros parâmetros de configuração local, como o nome de domínio e os Domain Name Servers (DNSs). Quando os servidores DHCP recebem uma mensagem DHCPINFORM, construa uma mensagem DHCPACK com qualquer parâmetro de configuração local apropriado para o cliente sem um novo endereço IP. Esse DHCPACK é enviado por unicast ao cliente.

## DHCPRELEASE

Um cliente DHCP pode optar por ceder seu aluguel em um endereço de rede quando envia uma mensagem DHCPRELEASE ao servidor DHCP. O cliente identifica o aluguel a ser liberado com o uso do campo `identificador de cliente` e o endereço de rede na mensagem DHCPRELEASE. Se precisar estender o intervalo atual do pool DHCP, remova o pool atual de endereços e especifique o novo intervalo de endereços IP no pool DHCP. Para remover endereços IP específicos ou um intervalo de endereços que você deseja que estejam no pool DHCP, use o comando `ip dhcp excluded-address`.

**Note:** Se os dispositivos usarem BOOTP, as concessões de comprimento infinito serão mostradas nos vínculos de DHCP dos roteadores.

## Renove o leasing

Como o endereço IP é concedido somente a partir do servidor, a concessão deve ser renovada periodicamente. Quando metade do tempo de aluguel expira ( $T1=0,5 \times LT$ ), o cliente tenta renovar o aluguel. O cliente entra no estado de Renewing e envia uma mensagem DHCPREQUEST para o servidor, que mantém a licença atual. O servidor responde à solicitação de renovação com uma mensagem DHCPACK se concordar em renovar o aluguel. A mensagem DHCPACK contém o novo aluguel e quaisquer novos parâmetros de configuração, caso quaisquer alterações sejam feitas no servidor durante o tempo do aluguel anterior. Se o cliente não conseguir acessar o servidor quando ele mantiver o aluguel por algum motivo, ele tentará renovar o endereço de qualquer servidor DHCP depois que o servidor DHCP original não tiver respondido às solicitações de renovação em um tempo  $T2$ . O valor padrão de  $T2$  é  $(7/8 \times LT)$ . Isso significa  $T1 < T2 < LT$ .

Se o cliente tiver anteriormente um endereço IP atribuído por DHCP e ele for reiniciado, ele solicitará especificamente o endereço IP anteriormente concedido em um pacote DHCPREQUEST. Esse DHCPREQUEST ainda tem o endereço IP origem como tem 0.0.0.0 e o destino como o endereço de broadcast IP 255.255.255.255.

Quando um cliente envia um DHCPREQUEST durante uma reinicialização, ele não deve preencher o campo de identificador do servidor e deve preencher o campo de opção de endereço IP solicitado. Somente clientes compatíveis com RFC preenchem o campo `ciaddr` com o endereço solicitado em vez do campo de opção DHCP. O servidor DHCP aceita qualquer um dos métodos. O comportamento do servidor DHCP depende de uma série de fatores, como no caso dos servidores DHCP do Windows NT, a versão do sistema que é usada, além de outros fatores, como o superescopo. Se o servidor DHCP determinar que o cliente ainda pode usar o endereço IP solicitado, ele permanecerá em silêncio ou enviará um DHCPACK para o DHCPREQUEST. Se o servidor determinar que o cliente não pode usar o endereço IP solicitado, ele enviará um DHCPNACK de volta ao cliente. Em seguida, o cliente passa para o estado Inicializando e envia uma mensagem DHCPDISCOVER.



**Note:** O servidor DHCP atribui o endereço IP inferior de um pool de endereços IP aos clientes DHCP. Quando o lease do endereço inferior expirar, ele será atribuído a outro cliente se for solicitado. Você não pode fazer alterações na ordem em que os endereços DHCP estão atribuídos.

## Tabela de pacotes DHCP

A mensagem DHCP tem comprimento variável e consiste em campos listados na Tabela de Pacotes DHCP.

**Note:** Esse pacote é uma versão modificada do pacote BootP original.

Campo	Bytes	Nome	Descrição
op	1	Opcode	Identifica o pacote como uma solicitação ou resposta: 1 = BOOTREQUEST, 2 = BOOTREPLY
htype	1	Tipo de hardware	Especifica o tipo de endereço de hardware de rede.
hlen	1	Tamanho do hardware	Especifica a extensão do endereço de hardware.
saltos	1	Saltos	O cliente define o valor como zero e, se a solicitação for encaminhada através de um roteador, o valor será incrementado.
xid	4	ID de transação	Um número aleatório selecionado pelo cliente. Todas as mensagens DHCP trocadas em uma determinada transação DHCP usam o ID (xid).
segundos	2	Segundos	Especifica o número de segundos desde o início do processo de DHCP.
flags	2	Flags	Indica se a mensagem é broadcast ou unicast.
ciaddr	4	Endereço IP do cliente	Utilizado apenas se o cliente sabe seu endereço IP, como no caso dos estados Bound, Renew ou Rebinding.
yiaddr	4	Seu endereço IP	Se o endereço IP do cliente for 0.0.0.0, o servidor DHCP colocará o endereço IP do cliente oferecido nesse campo.
siaddr	4	Endereço IP do servidor	Se o cliente souber o endereço IP do servidor DHCP, este campo será preenchido com o endereço do servidor DHCP. Caso contrário, ele será usado em DHCPDISCOVER e DHCPACK a partir do servidor DHCP.
giaddr	4	Endereço IP do roteador (GI ADDR)	O endereço IP de porta de comunicação, preenchido pelo agente do roteador DHCP/BootP.
chaddr	16	Endereço MAC cliente	O endereço MAC do cliente DHCP.
sname	64	Nome do servidor	O nome do host do servidor opcional.
arquivo	128	nome do arquivo de inicialização	O nome do arquivo de inicialização.
opções	variável	Parâmetros de opção	Os parâmetros opcionais que o servidor de DHCP pode fornecer. A RFC 2132 oferece todas as opções possíveis.

## Conversação cliente-servidor para cliente que obtém o endereço DHCP onde o cliente e o servidor DHCP residem na mesma sub-rede

Descrição do pacote	Endereço MAC de Origem	Endereço MAC de destino	Endereço IP de origem	End IP de destino
DHCPDISCOVER	Cliente	Broadcast	0.0.0.0	255.255.255.255

DHCPOFFER	DHCP Server	Broadcast	DHCP Server	255.255.255.255
DHCPREQUEST	Cliente	Broadcast	0.0.0.0	255.255.255.255
DHCPACK	DHCP Server	Broadcast	DHCP Server	255.255.255.255

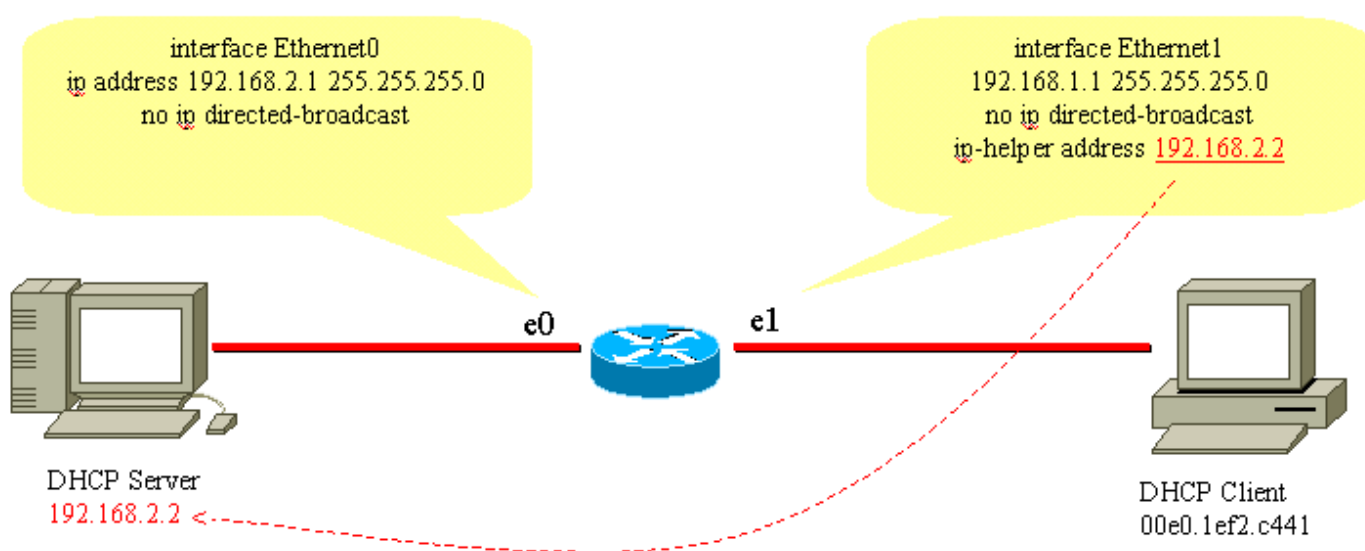
## Função do agente de transmissão de DHCP/BootP

Os roteadores, por padrão, não encaminham pacotes de broadcast. Como as mensagens do cliente DHCP usam o endereço IP de destino 255.255.255.255 (all NetBroadcast), os clientes DHCP não podem enviar solicitações a um servidor DHCP em uma sub-rede diferente, a menos que o Agente de Transmissão DHCP/BootP esteja configurado no roteador. O Agente de Transmissão DHCP/BootP encaminha solicitações DHCP em nome de um cliente DHCP para o servidor DHCP. O Agente de Transmissão DHCP/BootP anexa seu próprio endereço IP ao endereço IP origem dos quadros DHCP que vão para o servidor DHCP. Isso permite que o servidor DHCP responda via unicast para o agente de transmissão de DHCP/BootP. O Agente de Transmissão DHCP/BootP também preenche o campo Endereço IP do Gateway com o endereço IP da interface na qual a mensagem DHCP é recebida do cliente. O servidor DHCP usa o campo de endereço IP do gateway para determinar a sub-rede de origem das mensagens DHCPDISCOVER, DHCPREQUEST ou DHCPINFORM.

## Configurar o recurso DHCP/BootP Relay Agent no roteador Cisco IOS®

O processo para configurar um roteador Cisco para encaminhar solicitações BootP ou DHCP é simples. Basta configurar um endereço IP auxiliar que aponte para o servidor DHCP/BootP ou para o endereço de broadcast da sub-rede da rede em que o servidor está.

Exemplo de rede:



Agente de retransmissão DHCP/BootP

Para encaminhar a solicitação BootP/DHCP do cliente para o servidor DHCP, o comando **ip helper-address interface** é usado. O endereço do auxiliar IP pode ser configurado de forma a encaminhar apenas a transmissão UDP com base no número da porta UDP. Por padrão, o IP helper-address encaminha estes broadcasts UDP:

- TFTP (Protocolo de Transferência de Arquivo Trivial) (porta 69)
- DNS (porta 53), serviço de tempo (porta 37)
- Servidor de nomes NetBIOS (porta 137)
- Servidor de datagramas NetBIOS (porta 138)
- Datagramas de cliente e servidor do protocolo de inicialização (DHCP/BootP) (portas 67 e 68)
- Serviço do TACACS (Sistema de controle de acesso do controlador de acesso do terminal) (porta 49)
- Serviço de nome IEN-116 (porta 42)

Os endereços auxiliares IP podem direcionar broadcasts UDP para um endereço IP unicast ou de broadcast. No entanto, não use o endereço auxiliar IP para encaminhar broadcasts UDP de uma sub-rede para o endereço de broadcast de outra sub-rede, devido à grande quantidade de inundação de broadcast que pode ocorrer. Várias entradas de endereço IP auxiliar em uma única interface também são suportadas:

```

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

```

Os roteadores Cisco não são compatíveis com balanceamento de carga de servidores DHCP configurados como agentes de relé de DHCP. Os roteadores Cisco encaminham a mensagem DHCPDISCOVER para todos os endereços do helper mencionados para essa interface. O uso de dois ou mais servidores DHCP para servir uma sub-rede somente aumenta o tráfego DHCP à medida que as mensagens DHCPDISCOVER, DHCPOFFER e DHCPREQUEST / DHCPDECLINE são trocadas entre cada par de cliente e servidor DHCP.

## Definir Associações Manuais

Há duas maneiras de configurar vínculos manuais; uma é para o host do Windows e a outra é para os hosts que não são do Windows. Há dois comandos diferentes usados para configurar; um é para clientes DHCP da Microsoft e o outro é para clientes DHCP não Microsoft: **DHCPclient-identifier** (ligação manual - clientes DHCP da Microsoft) e **DHCPhardware-address** (ligação manual - clientes DHCP não Microsoft). A razão para dois comandos diferentes é que um PC executado com o Windows modifica seus MACs e um **01** é adicionado no início do endereço. Estas são as configurações de exemplo:

- Esta é uma configuração para clientes DHCP da Microsoft:

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

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

- Esta é uma configuração para clientes DHCP não Microsoft:

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

!--- xxxxxx represents 48 bit MAC address

## Como fazer com que o DHCP funcione em segmentos IP secundários

Por padrão, o DHCP tem uma limitação em que os pacotes de resposta são enviados somente se a solicitação for recebida da interface configurada com o endereço IP primário. O tráfego DHCP usa o endereço de transmissão. Quando a solicitação de DHCP é recebida pela interface do roteador, ela a encaminha para o servidor DHCP (quando o IP helper-address está configurado) com um endereço IP de origem primário configurado na interface, para permitir que o servidor DHCP saiba qual pool de IP deve ser usado (para o cliente) no pacote de resposta de DHCP.

Não há como o roteador saber se a solicitação de transmissão DHCP vem de um dispositivo que está na rede IP secundária configurada na interface. Como uma solução alternativa, a configuração de subinterface (desde que o dispositivo conectado ao roteador ofereça suporte à marcação de dot1q) para separar as duas sub-redes podem ser configuradas, então ambas recebem os endereços IP correspondentes corretamente.

Se o endereço secundário for o caminho preferido, há outra solução alternativa, que é ativar o **comando de** configuração global **dhcp smart-relay**. Isso tem uma limitação, pois só usa o IP secundário para retransmitir a solicitação de DHCP se não houver resposta do servidor DHCP após três solicitações consecutivas para o pool de endereços primário.

## Conversa entre cliente e servidor DHCP com a função DHCP Relay

A tabela a seguir ilustra o processo para um cliente DHCP obter um endereço IP de um servidor DHCP. Esta tabela é modelada após o diagrama de rede anterior do recurso Configurar DHCP/BootP Relay Agent. Cada valor numérico no diagrama representa um pacote que é descrito nesta próxima tabela. Use esta tabela para entender o fluxo de pacotes da conversação cliente-servidor DHCP. Também ajuda a determinar onde os problemas ocorrem.

### Processo para um cliente DHCP obter um endereço IP

Pacote	Endereço IP do cliente	Endereço IP do Servidor	Endereço GI	Endereço MAC de origem do pacote	Endereço IP de origem do pacote	Endereço MAC de destino do pacote	Endereço de destino do pacote
1. DHCPDISCOVER é enviado do cliente.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.ffff (transmissão)	255.255.255.255
2. O roteador recebe o DHCPDISCOVER na interface E1. O roteador reconhece que esse pacote é um broadcast DHCP UDP. O roteador agora atua como um agente de transmissão de DHCP/BootP e preenche o campo de endereço IP do gateway com o endereço IP da interface de entrada, altera o endereço IP de origem para um endereço IP da interface de entrada e encaminha a solicitação diretamente para o servidor DHCP.	0.0.0.0	0.0.0.0	192.168.1.1	Endereço E2 MAC da interface	192.168.1.1	Endereço MAC do servidor de DHCP	192.168.1.1
3. O servidor DHCP recebeu o DHCPDISCOVER e envia um DHCPOFFER ao Agente de Retransmissão DHCP.	192.168.1.2	192.168.2.2	192.168.1.1	Endereço MAC do servidor de DHCP	192.168.2.2	Endereço E2 MAC da interface	192.168.2.2
4. O Agente de Retransmissão DHCP recebe um DHCPOFFER e encaminha o broadcast de DHCPOFFER na LAN local.	192.168.1.2	192.168.2.2	192.168.1.1	Endereço MAC da interface E1	192.168.1.1	ffff.ffff.ffff (broadcast)	255.255.255.255

5. DHCPREQUEST enviado do cliente.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.ffff (transmissão)	255
6. O roteador recebe o DHCPREQUEST na interface E1. O roteador reconhece que este pacote é a difusão UDP do DHCP. O roteador agora atua como um agente de retransmissão DHCP e preenche o campo de endereço IP do gateway com o endereço IP da interface enviada, altera o endereço IP de origem para um endereço IP da interface de entrada e encaminha a solicitação diretamente ao servidor DHCP.	0.0.0.0	0.0.0.0	192.168.1.1	Endereço E2 MAC da interface	192.168.1.1	Endereço MAC do servidor de DHCP	192
7. O servidor DHCP recebeu o DHCPREQUEST e envia um DHCPACK ao Agente de Transmissão DHCP/BootP.	192.168.1.2	192.168.2.2	192.168.1.1	Endereço MAC do servidor de DHCP	192.168.2.2	Endereço E2 MAC da interface	192
8. O Agente de Transmissão DHCP/BootP recebe o DHCPACK e encaminha o broadcast DHCPACK na LAN local. O cliente aceita o ACK e usa o endereço IP do	192.168.1.2	192.168.2.2	192.168.1.1	Endereço MAC da interface E1	192.168.1.1	ffff.ffff.ffff (broadcast)	255

cliente.

## Considerações sobre DHCP de inicialização do ambiente de pré-execução (PXE)

O Ambiente de pré-execução (PXE) permite que uma estação de trabalho seja inicializada a partir de um servidor em uma rede antes da inicialização do sistema no disco rígido local. Um administrador de rede não precisa visitar fisicamente a estação de trabalho específica e inicializá-la manualmente. O SO e outros softwares, como programas de diagnóstico, podem ser carregados no dispositivo a partir de um servidor na rede. O ambiente PXE usa DHCP para configurar seu endereço IP.

A configuração do agente de relé DHCP/BootP deve ser feita no roteador, se o servidor DHCP estiver localizado em outro segmento roteado da rede. O comando `ip helper-address` na interface do roteador local deve ser configurado. Consulte [a seção Configurar o Recurso de Agente de Retransmissão DHCP/BootP no Cisco IOS](#) Router deste documento para obter informações de configuração.

## Entender e solucionar problemas do DHCP com farejadores de rastreamento

### Decodificar o farejador de rastreamento do cliente e servidor DHCP no mesmo segmento de LAN

Topologia de rede onde o cliente e o servidor DHCP residem no mesmo segmento de LAN

O exemplo do farejador de rastreamento é composto de seis quadros. Esses seis quadros ilustram um cenário no qual o cliente e o servidor DHCP residem no mesmo segmento físico ou lógico. Use o próximo exemplo de código para solucionar problemas de DHCP. É importante associar o farejador de rastreamento aos rastreamentos neste exemplo. Pode haver algumas diferenças em comparação com os próximos rastreamentos ilustrados, mas o fluxo geral de pacotes deve ser exatamente o mesmo. O rastreamento de pacote segue as discussões anteriores sobre o funcionamento do DHCP.

```
----- Frame 1 - DHCPDISCOVER -----  
-----  
Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary  
1[0.0.0.0] [255.255.255.255] 618 0:01:26.810 0.575.244 05/07/2001 11:52:03 AM DHCP: Request,  
Message type: DHCP Discover  
DLC: ----- DLC Header -----  
DLC:  
DLC: Frame larrived at 11:52:03.8106; frame size is 618 (026A hex) bytes.  
DLC: Destination = BROADCAST FFFFFFFF, Broadcast  
DLC: Source = Station 0005DCC9C640  
DLC: Ethertype = 0800 (IP)  
DLC:  
IP: ----- IP Header -----  
IP:  
IP: Version = 4, header length = 20 bytes  
IP: Type of service = 00
```

IP: 000. .... = routine  
IP: ...0 .... = normal delay  
IP: .... 0... = normal throughput  
IP: .... .0.. = normal reliability  
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit  
IP: .... ...0 = CE bit - no congestion  
IP: Total length = 604 bytes  
IP: Identification = 9  
IP: Flags = 0X  
IP: .0.. .... = may fragment  
IP: ..0. .... = last fragment  
IP: Fragment offset = 0 bytes  
IP: Time to live = 255 seconds/hops  
IP: Protocol = 17 (UDP)  
IP: Header checksum = B988 (correct)  
IP: **Source address = [0.0.0.0]**  
IP: **Destination address = [255.255.255.255]**  
IP: No options  
IP:  
UDP: ----- UDP Header -----  
UDP:  
UDP: **Source port = 68 (BootPc/DHCP)**  
UDP: **Destination port = 67 (BootPs/DHCP)**  
UDP: Length = 584  
UDP: No checksum  
UDP: [576 byte(s) of data]  
UDP:  
DHCP: ----- DHCP Header -----  
DHCP:  
DHCP: Boot record type = 1 (Request)  
DHCP: Hardware address type = 1 (10Mb Ethernet)  
DHCP: Hardware address length = 6 bytes  
DHCP:  
DHCP: Hops = 0  
DHCP: **Transaction id = 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 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:

## Decodificar farejador de rastreamento de cliente e servidor DHCP separados por um roteador configurado como agente de retransmissão DHCP

### Rastreamento do farejador B

- - - - - **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:

## Rastreamento Sniffer-A

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

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary  
118 [192.168.1.1] [192.168.2.2] 618 0:00:51.212 0.489.912 05/31/2001 07:02:54 AM DHCP: Request,  
Message type: DHCP Discover  
DLC: ----- DLC Header -----  
DLC:  
DLC: Frame 118 arrived at 07:02:54.7463; frame size is 618 (026A hex) bytes.  
DLC: **Destination = Station 0005DC0BF2F4**  
DLC: **Source = Station 003094248F72**  
DLC: Ethertype = 0800 (IP)  
DLC:  
IP: ----- IP Header -----  
IP:  
IP: Version = 4, header length = 20 bytes  
IP: Type of service = 00  
IP: 000. .... = routine  
IP: ...0 .... = normal delay  
IP: .... 0... = normal throughput  
IP: .... .0.. = normal reliability  
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit  
IP: .... ...0 = CE bit - no congestion  
IP: Total length = 604 bytes  
IP: Identification = 52  
IP: Flags = 0X  
IP: .0.. .... = may fragment  
IP: ..0. .... = last fragment  
IP: Fragment offset = 0 bytes  
IP: Time to live = 255 seconds/hops  
IP: Protocol = 17 (UDP)

```

IP: Header checksum = 3509 (correct)
IP: Source address = [192.168.1.1]
IP: Destination address = [192.168.2.2]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: Checksum = 0A19 (correct)
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 1
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload = 3 (File and Sname fields hold options)
DHCP:

```

```

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

```

```

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2 [192.168.2.2] [192.168.1.1] 347 0:00:51.214 0.002.133 05/31/2001 07:02:54 AM DHCP: Request,
  Message type: DHCP Offer
DLC: ----- DLC Header -----
DLC:
DLC: Frame 119 arrived at 07:02:54.7485; frame size is 347 (015B hex) bytes.
DLC: Destination = Station 003094248F72
DLC: Source = Station 0005DC0BF2F4
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:

```

IP: Version = 4, header length = 20 bytes  
IP: Type of service = 00  
IP: 000. .... = routine  
IP: ...0 .... = normal delay  
IP: .... 0... = normal throughput  
IP: .... .0.. = normal reliability  
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit  
IP: .... ...0 = CE bit - no congestion  
IP: Total length = 333 bytes  
IP: Identification = 41  
IP: Flags = 0X  
IP: .0.. .... = may fragment  
IP: ..0. .... = last fragment  
IP: Fragment offset = 0 bytes  
IP: Time to live = 255 seconds/hops  
IP: Protocol = 17 (UDP)  
IP: Header checksum = 3623 (correct)  
IP: **Source address = [192.168.2.2]**  
IP: **Destination address = [192.168.1.1]**  
IP: No options  
IP:  
UDP: ----- UDP Header -----  
UDP:  
UDP: **Source port = 67 (BootPs/DHCP)**  
UDP: **Destination port = 67 (BootPs/DHCP)**  
UDP: Length = 313  
UDP: Checksum = A1F8 (correct)  
UDP: [305 byte(s) of data]  
UDP:  
DHCP: ----- DHCP Header -----  
DHCP:  
DHCP: Boot record type = 2 (Request)  
DHCP: Hardware address type = 1 (10Mb Ethernet)  
DHCP: Hardware address length = 6 bytes  
DHCP:  
DHCP: Hops = 0  
DHCP: Transaction id = 000005F4  
DHCP: Elapsed boot time = 0 seconds  
DHCP: Flags = 8000  
DHCP: 1... .... .... = Broadcast IP datagrams  
DHCP: Client self-assigned IP address = [0.0.0.0]  
DHCP: Client IP address = [192.168.1.2]  
DHCP: Next Server to use in bootstrap = [0.0.0.0]  
**DHCP: Relay Agent = [192.168.1.1]**  
**DHCP: Client hardware address = 0005DCF2C441**  
DHCP:  
DHCP: Host name = ""  
DHCP: Boot file name = ""  
DHCP:  
DHCP: Vendor Information tag = 63825363  
DHCP: Message Type = 2 (DHCP Offer)  
DHCP: Server IP address = [192.168.2.2]  
DHCP: Request IP address lease time = 172571 (seconds)  
DHCP: Address Renewal interval = 86285 (seconds)  
DHCP: Address Rebinding interval = 150999 (seconds)  
DHCP: Subnet mask = [255.255.255.0]  
DHCP: **Domain Name Server address = [192.168.10.1]**  
DHCP: **Domain Name Server address = [192.168.10.2]**  
DHCP: **NetBIOS Server address = [192.168.10.1]**  
DHCP: **NetBIOS Server address = [192.168.10.3]**  
DHCP: **Domain name = "cisco.com"**  
DHCP:

- - -

```
Frame 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:
```

## Solucionar problemas do DHCP quando as estações de trabalho clientes não conseguem obter endereços DHCP

### Casos Práticos 1: Servidor DHCP no mesmo segmento LAN ou VLAN em que se encontra o cliente DHCP

Quando o servidor e o cliente DHCP residem no mesmo segmento de LAN ou VLAN e o cliente não consegue obter um endereço IP de um servidor DHCP. Mas é improvável que o roteador local cause um problema de DHCP. O problema está relacionado aos dispositivos que conectam o servidor DHCP e o cliente DHCP. No entanto, o problema pode estar no servidor DHCP ou no próprio cliente. Esses módulos ajudam a solucionar problemas e determinar qual dispositivo causa um problema.

**Note:** Para configurar o servidor DHCP em uma base por vlan, defina pools DHCP diferentes para cada VLAN que serve endereços DHCP aos seus clientes.

### Casos Práticos 2: O servidor DHCP e o cliente DHCP são separados por um roteador configurado para a funcionalidade DHCP/BootP Relay Agent

Quando o servidor e o cliente DHCP residem nos diferentes segmentos da LAN ou VLANs, o roteador funciona como um agente de transmissão de DHCP/BootP que é responsável por encaminhar o DHCPREQUEST ao servidor DHCP. Etapas adicionais são necessárias para solucionar problemas do Agente de Transmissão DHCP/BootP, bem como do servidor e cliente DHCP. Se você seguir esses módulos, poderá determinar qual dispositivo causa os problemas.



## O servidor DHCP no roteador falha ao atribuir o endereço com um erro POOL EXHAUSTED

É possível que alguns endereços ainda sejam mantidos pelos clientes, mesmo que sejam liberados do pool. Isso pode ser verificado pela saída `show ip dhcp conflict`. Um conflito de endereços ocorre quando dois hosts usam o mesmo endereço IP. Na atribuição de endereço, o DHCP verifica se há conflitos com o ping e o ARP gratuito.

Se um conflito for detectado, o endereço será removido do pool. O endereço é atribuído até que o administrador resolva o conflito. **Configure o log de conflitos ip dhcp** para resolver esse problema.

## Módulos de Troubleshooting de DHCP

### Entender onde podem ocorrer problemas de DHCP

Os problemas de DHCP podem surgir devido a várias razões. As razões mais comuns são problemas de configuração. No entanto, muitos problemas de DHCP podem ser causados por defeitos de software em sistemas, drivers de NIC (Network Interface Card, placa de interface de rede) ou agentes de transmissão de DHCP/BootP executados em roteadores. Devido ao número de áreas potencialmente problemáticas, é necessária uma abordagem sistemática para solucionar problemas.

### Lista breve com causas possíveis para os problemas de DHCP:

- Configuração Padrão do Catalyst 2960
- Configuração de agente de relé DHCP/BootP
- Questão de compatibilidade de NIC ou questão de característica DHCP.
- Instalação de driver de NIC incorreta ou NIC com defeito
- Quedas de rede intermitentes devido a cálculos de Spanning Tree frequentes
- Comportamento do sistema operacional ou software com defeito
- Defeito do software ou da configuração do escopo do servidor DHCP
- Defeito do switch Cisco Catalyst ou do software Cisco IOS DHCP/BootP Relay Agent
- Falha na verificação de encaminhamento de caminho unicast (uRPF) porque a oferta DHCP foi recebida em uma interface diferente da esperada. Quando o recurso Reverse Path Forwarding (RPF) está habilitado em uma interface, um roteador Cisco pode descartar pacotes Dynamic Host Configuration Protocol (DHCP) e BOOTstrap Protocol (BOOTP) que tenham endereços de origem 0.0.0.0 e endereços de destino 255.255.255.255. O roteador também pode descartar todos os pacotes IP que tenham um destino IP multicast na interface. Este problema está documentado na ID de bug Cisco [CSCdw31925](#)

Observação Apenas clientes Cisco registrados podem acessar relatórios de bugs.

- O agente de banco de dados DHCP não é usado, mas o log de conflitos DHCP não está desabilitado

### A. Verificar a conectividade física

Esse procedimento se aplica a todos os estudos de caso.

Primeiro, verifique a conectividade física de um DHCP de cliente e de servidor. Se estiver conectado a um switch Catalyst, verifique se o cliente e o servidor DHCP têm conectividade física. Para switches com base no Cisco IOS, como o Catalyst 2900XL/3500XL/2950/3550, o comando equivalente **para mostrar o status da porta** mostra a interface <interface>. Se o estado da interface for qualquer outro diferente de <interface> está ativo, o protocolo de linha está ativo, a porta não transmite tráfego, nem mesmo solicitações de cliente DHCP. A saída dos comandos:

```
Switch#show interface fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0030.94dc.ac1 (bia 0030.94dc.ac1)
```

Se a conexão física tiver sido verificada e de fato não houver link entre o switch Catalyst e o cliente DHCP, use [a seção Troubleshooting de Compatibilidade entre Switches Cisco Catalyst e NIC](#) para solucionar problemas relacionados à conectividade da camada física.

Erros excessivos de enlace de dados fazem com que as portas em alguns switches Catalyst entrem em um estado desabilitado por erro. Para obter mais informações, consulte [Errdisable Port State Recovery on the Cisco IOS Platforms](#), que descreve o estado errdisable, explica como se recuperar dele e fornece exemplos de recuperação desse estado.

## B. Configurar a Estação de Trabalho Cliente e o IP Estático para Testar a Conectividade da Rede

Esse procedimento se aplica a todos os estudos de caso.

Ao solucionar qualquer problema de DHCP, é importante configurar um endereço IP estático em uma estação de trabalho cliente para verificar a conectividade da rede. Se a estação de trabalho não puder acessar os recursos da rede apesar de ter um endereço IP configurado estaticamente, a causa raiz do problema não é o DHCP. Neste ponto, você será solicitado a solucionar problemas de conectividade de rede.

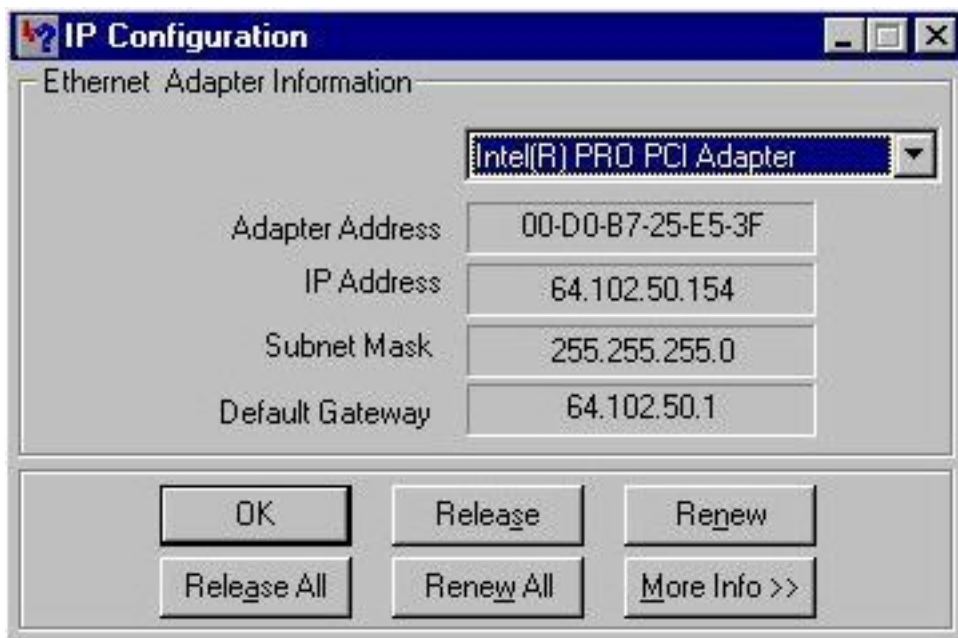
## C. Verifique o Problema como um Problema de Inicialização

Esse procedimento se aplica a todos os estudos de caso.

Se o cliente DHCP não conseguir obter um endereço IP do servidor DHCP na inicialização, você poderá forçar manualmente o cliente a enviar uma solicitação DHCP. Execute as próximas etapas para obter manualmente um endereço IP de um servidor DHCP para o SO listado.

### Microsoft Windows 95/98/ME:

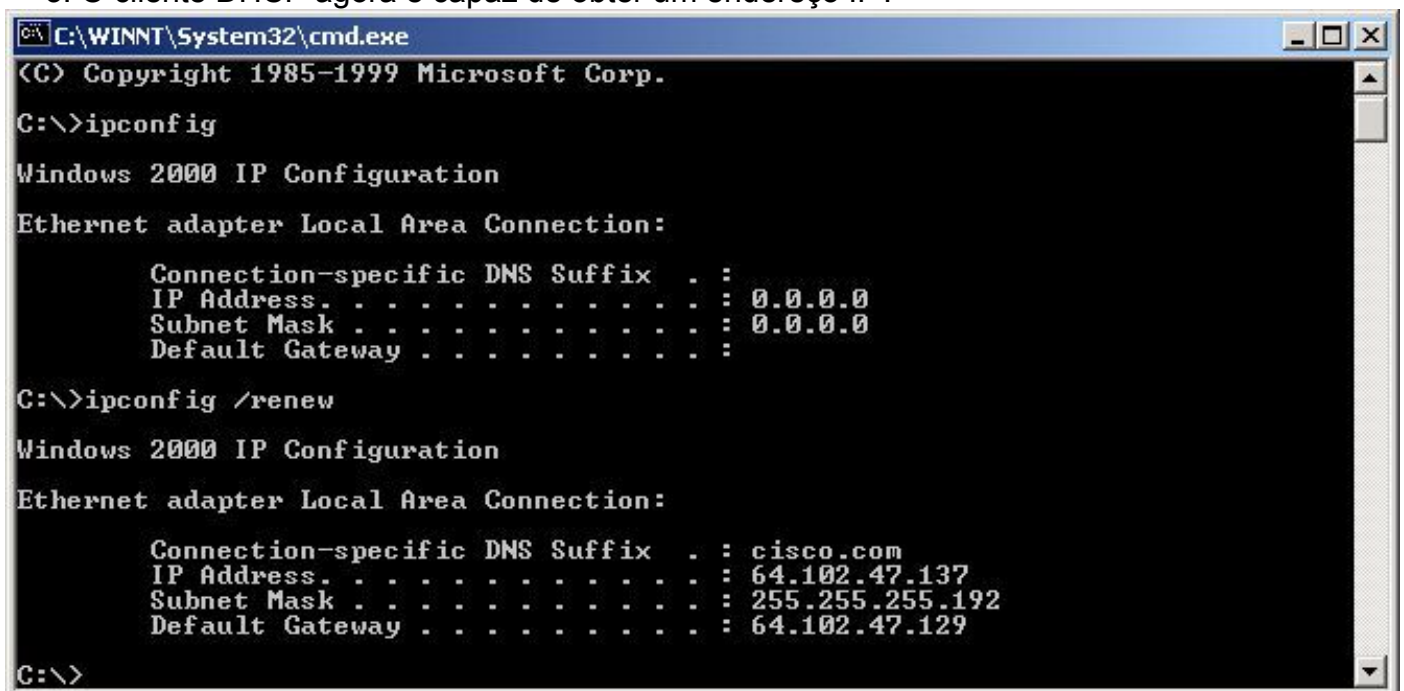
1. Clique no botão Iniciar e execute o programa WINIPCFG.exe.
2. Clique no **botão Release All**, seguido pelo botão **Renew All**.
3. Agora, o cliente DHCP consegue obter um endereço IP?



Janela de configuração de IP

### Microsoft Windows NT/2000:

1. Insira cmdin no campo Iniciar/Executar para abrir uma janela de prompt de comando.
2. Emita o comando **commandipconfig/Renein** na janela do prompt de comando.
3. O cliente DHCP agora é capaz de obter um endereço IP?



Prompt da linha de comando

Se o cliente DHCP for capaz de obter um endereço IP com uma renovação manual do endereço IP depois que o PC tiver concluído o processo de inicialização, o problema muito provavelmente é de inicialização do DHCP. Se o cliente DHCP estiver conectado a um switch Cisco Catalyst, o problema é provavelmente devido a um problema de configuração que lida com portfast STP e/ou canalização e entroncamento. Outras possibilidades incluem problemas de placa NIC e problemas de inicialização da porta do switch. Revise as Etapas D e E para descartar problemas de configuração de porta do switch e da placa de rede como a causa raiz do problema de DHCP.

### D. Verifique a configuração da porta do Switch (STP Portfast e outros comandos)

Se o switch for um Catalyst 2900/4000/5000/6000, verifique se a porta tem o STP PortFast ativado e o entroncamento/canalização desativado. A configuração padrão é STP portfast desabilitada e truncamento/canalização automático, se aplicável. Para os switches 2900XL/3500XL/2950/3550, o STP PortFast é a única configuração necessária. Essas alterações de configurações resolvem os problemas mais comuns dos clientes DHCP que ocorrem com uma instalação inicial de um switch Catalyst.

Para obter mais documentação sobre os requisitos de configuração de porta do switch necessários para que o DHCP funcione corretamente quando conectado aos switches Catalyst, consulte [Using Portfast and Other Commands to Fix Workstation Startup Connectivity Delays](#).

Depois de revisar esse documento, você poderá continuar a solucionar esses problemas.

## E. Verifique se há problemas conhecidos de placa de rede ou switch Catalyst

Se a configuração do switch Catalyst estiver correta, é possível que um problema de compatibilidade de software possa existir no switch Catalyst ou na placa de rede do cliente DHCP que possa causar os problemas de DHCP. A próxima etapa para fazer Troubleshooting é rever [Troubleshooting de Cisco Catalyst Switches para Problemas de Compatibilidade de NIC](#) e descartar quaisquer problemas de software com o Catalyst Switch ou NIC que contribuam para o problema.

O conhecimento do sistema operacional do cliente DHCP, bem como informações específicas da placa de rede, como fabricante, modelo e versão do driver, é necessário para descartar qualquer problema de compatibilidade.

## F. Distinguir se os clientes DHCP obtêm o endereço IP na mesma sub-rede ou VLAN que o servidor DHCP

É importante distinguir se o DHCP está ou não funcionando corretamente quando o cliente está na mesma sub-rede ou VLAN que o servidor DHCP. Se o DHCP não funcionar corretamente na mesma sub-rede ou VLAN que o servidor DHCP, o problema de DHCP será causado principalmente pelo agente de transmissão de DHCP/BootP. Se o problema persistir mesmo quando você testar o DHCP na mesma sub-rede ou VLAN que o servidor DHCP, o problema pode realmente ser com o servidor DHCP.

## G. Verifique a configuração do roteador DHCP/BootP Relay

Para verificar a configuração:

1. Quando você configura a retransmissão de DHCP em um roteador, verifique se o comando **ip helper-address** está localizado na interface correta. O comando **ip helper-address** deve estar presente na interface de entrada das estações de trabalho clientes DHCP e deve ser direcionado para o servidor DHCP correto.
2. Verifique se o comando global configuration **no service dhcp** não está presente. Esse parâmetro de configuração desativa toda a funcionalidade de retransmissão e servidor DHCP no roteador. A configuração padrão, `service dhcp`, não aparece na configuração e é o comando de configuração padrão. Se o **serviço dhcp** não estiver habilitado, os clientes não receberão os endereços IP do servidor DHCP. **Note:** Nos roteadores que executam versões mais antigas do Cisco IOS, o comando `ip bootp server` processa a função de agente de relé

DHCP em vez do comando **service dhcp**. Por causa disso, o comando **ip bootp server** precisa ser ativado nesses roteadores se o comando **ip helper-address** estiver configurado para encaminhar difusões UDP de DHCP e agir corretamente como um agente de relé DHCP em nome do cliente DHCP.

3. Quando você usa os comandos **ip helper-address** para encaminhar broadcasts UDP para um endereço de broadcast de sub-rede, verifique se no `ip directed-broadcast` não está configurado em nenhuma interface de saída que os pacotes de broadcast UDP precisam atravessar. O `no ip directed-broadcast` bloqueia qualquer tradução de um broadcast direcionado para broadcasts físicos. Essa configuração de interface é a configuração padrão nas versões de software 12.0 e posterior.
4. Quando os broadcasts DHCP são encaminhados para o endereço de broadcast da sub-rede do servidor DHCP, pode surgir um problema de software. Ao solucionar problemas do DHCP, tente encaminhar broadcasts UDP do DHCP para o endereço IP do servidor DHCP:

## H. Opção Identificação Do Assinante (82) Ativada

O recurso de informações do agente de relé DHCP (opção 82) permite que os agentes de relé DHCP (switches Catalyst) incluam informações sobre si mesmo e o cliente conectado, quando ele encaminha as solicitações de DHCP de um cliente DHCP para um servidor DHCP.

O servidor DHCP pode usar essas informações para atribuir endereços IP, realizar o controle de acesso e definir a qualidade de serviço (QoS) e as políticas de segurança (ou outras políticas de atribuição de parâmetros) para cada assinante de uma rede do provedor de serviços. Quando o rastreamento de DHCP está habilitado em um switch, ele habilita automaticamente a opção 82. Se o servidor DHCP não estiver configurado para manipular os pacotes com a opção 82, ele deixará de alocar o endereço para essa solicitação. Para resolver esse problema, desabilite a opção de identificação de assinante (82) nos switches (agentes de retransmissão) com o comando de configuração global **no ip dhcp relay information option**.

## I. Agente de banco de dados DHCP e registro de conflitos DHCP

Um agente de banco de dados DHCP é qualquer host — por exemplo, um servidor FTP, TFTP ou RCP, que armazena o banco de dados de associações DHCP. Você pode configurar vários agentes de banco de dados DHCP e pode configurar o intervalo entre atualizações de banco de dados e transferências para cada agente. Use o comando **ip dhcp database** para configurar um agente de banco de dados e parâmetros do agente de banco de dados.

Se você optar por não configurar um agente de banco de dados DHCP, desative a gravação de conflitos de endereço DHCP no servidor DHCP. Execute o comando **no ip dhcp conflict logging** para desativar o registro de conflitos de endereços DHCP. Limpe os conflitos registrados anteriormente com **clear ip dhcp conflict**.

Se isso não conseguir desativar o registro de conflitos, essa mensagem de erro será exibida:

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

## J. Verifique o CDP para conexões de telefone IP

Quando a switchport conectada ao Telefone IP Cisco tem o CDP (Cisco Discovery Protocol) desativado, o servidor DHCP não pode atribuir um endereço IP apropriado ao telefone. O servidor

DHCP tende a atribuir o endereço IP que pertence à VLAN/sub-rede de dados da switchport. Se o CDP estiver ativado, o switch poderá detectar que o Telefone IP Cisco solicita o DHCP e fornecer as informações de sub-rede corretas. O servidor DHCP pode alocar um endereço IP da VLAN/pool de sub-rede de voz. Não há etapas explícitas necessárias para vincular o serviço DHCP à VLAN de voz.

## K. A remoção do SVI interrompe a operação de rastreamento de DHCP

Nos switches Cisco Catalyst série 6500, uma SVI (no estado desligada) é criada automaticamente depois de configurar o DHCP para rastreamento para uma VLAN específica. A presença dessa SVI tem implicações diretas sobre a operação correta de snooping de DHCP.

O rastreamento de DHCP nos Cisco Catalyst 6500 Series Switches que executam o Cisco IOS Nativo é implementado principalmente no Route Processor (RP ou MSFC), não no Switch Processor (SP ou Supervisor). O Cisco Catalyst série 6500 intercepta pacotes em hardware com VACLs que fornecem os pacotes para uma lógica de destino local (LTL) inscrita pelo RP. Depois que os quadros entram no RP, eles primeiro precisam ser associados a um IDB da interface L3 (SVI) antes que possam ser transmitidos para a parte de snooping. Sem uma SVI, esse IDB não existe e os pacotes são descartados no RP.

## L. Endereço de Broadcast Limitado

Quando um cliente DHCP define o bit de transmissão em um pacote DHCP, o servidor DHCP e o agente de relé enviam mensagens de DHCP para os clientes com o endereço de broadcast de todas as conexões (255.255.255.255). Se o comando **ip broadcast-address** tiver sido configurado para enviar um broadcast de rede, o broadcast all-ones enviado pelo DHCP será substituído. Para corrigir essa situação, use o comando **eip dhcp limited-broadcast-address** para garantir que um broadcast de rede configurado não substitua o comportamento padrão do DHCP.

Alguns clientes DHCP só podem aceitar uma transmissão all-ones (somente com um) e não podem adquirir um endereço DHCP, a menos que esse comando seja configurado na interface do roteador conectada ao cliente.

## M. Debug DHCP With Router Debug Commands

### Verificar se o roteador recebe a solicitação DHCP com comandos debug

Nos roteadores que suportam o software que processa pacotes DHCP, você pode verificar se um roteador recebe a solicitação DHCP do cliente. O processo DHCP falhará se o roteador não receber solicitações do cliente. Nesta etapa, configure uma lista de acesso para depurar a saída. Essa lista de acesso é usada apenas para depurar um comando e não é intrusiva para o roteador.

No modo de configuração global, digite esta lista de acesso:

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

No modo exec, insira este comando debug:

```
debug ip packet detail 100
```

### Saída de exemplo

```
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
```

A partir deste exemplo de saída, fica claro que o roteador recebe ativamente as solicitações DHCP do cliente. Essa saída mostra apenas um resumo do pacote, e não todo o pacote. Portanto, não é possível determinar se o pacote está correto. No entanto, o roteador recebeu um pacote de difusão com o IP de origem e de destino e portas corretos para DHCP.

### Verificar se o roteador recebe e encaminha a solicitação DHCP com o comando `debug ip udp`

O comando `debug ip udp` pode rastrear o caminho de uma solicitação DHCP através de um roteador. No entanto, essa depuração é intrusiva em um ambiente de produção, já que todos os pacotes UDP comutados processados são exibidos no console. Esse comando de depuração não deve ser usado na produção.

**aviso:** O comando `debug ip udp` é intrusivo e pode causar alta utilização da Unidade Central de Processamento (CPU).

No modo exec, insira este comando de depuração: `debug ip udp`

### Saída de exemplo

```
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 DHCP OFFER 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 DHCP OFFER 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 DHCP REQUEST 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.
```

## Verificar se o roteador recebe e encaminha a solicitação DHCP com o comando `debug ip dhcp server packet`

Se o roteador Cisco IOS for 12.0.x.T ou 12.1 e suportar a funcionalidade do servidor DHCP do Cisco IOS, você poderá usar o comando **debug ip dhcp server packet**. Essa depuração foi planejada para uso com o recurso de servidor DHCP do IOS e para solucionar problemas do recurso DHCP/BootP Relay Agent também. Como nas etapas anteriores, as depurações do roteador não fornecem uma determinação exata do problema, já que o pacote real não pode ser visualizado. No entanto, as depurações permitem que sejam feitas inferências com relação ao processamento DHCP. No modo exec, insira este comando de depuração:

### 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 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 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.

## Executar várias depurações simultaneamente

Quando você executa várias depurações simultaneamente, uma quantidade razoável de informações pode ser descoberta com relação à operação do agente de transmissão de DHCP/BootP e do servidor. Se você usar os tópicos anteriores para solucionar problemas, poderá fazer inferências sobre onde a funcionalidade do Agente de Transmissão DHCP/BootP não opera corretamente.

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

## Obter rastreamento do sniffer e determinar a causa raiz do problema de DHCP

Revise as seções [Decode Sniffer Trace of DHCP Client and Server on Same LAN Segment](#) e [Decode Sniffer Trace of DHCP Client and Server Separated by Router Configured as a DHCP Relay Agent](#)

para decifrar os rastreamentos de pacotes DHCP.

Para obter informações sobre como obter rastreamentos de farejador com o recurso Switched Port Analyzer (SPAN) nos switches Catalyst, consulte [Exemplo de Configuração do Catalyst Switched Port Analyzer \(SPAN\)](#).

## Método Alternativo de Decodificação de Pacotes com Depuração no Roteador

Com o comando **debug ip packet detail dump <acl>** em um roteador Cisco, é possível obter um pacote inteiro em hexadecimal exibido no registro do sistema ou na Interface de Linha de Comando (CLI). Revise [as seções Verificar se o roteador recebe a solicitação DHCP com os comandos debug](#) e Verificar se o roteador recebe a solicitação DHCP e encaminha a solicitação ao servidor DHCP com os comandos debug acima, junto com a palavra-chave dump adicionada à lista de acesso, para obter as mesmas informações de depuração, mas com os detalhes do pacote em hexadecimal. Para determinar o conteúdo do pacote, ele precisa ser convertido. Um exemplo é fornecido no Apêndice A.

## Apêndice A: Exemplo de configuração do DHCP do Cisco IOS

O banco de dados do servidor DHCP é organizado como uma árvore. A raiz da árvore é o pool de endereços para redes naturais, as ramificações são pools de endereços de sub-rede e as folhas são associações manuais aos clientes. As subredes herdaram os parâmetros da rede e os clientes herdaram os parâmetros da subrede. Portanto, os parâmetros comuns, por exemplo o nome de domínio, devem ser configurados no nível mais alto (rede ou sub-rede) da árvore.

Para obter mais informações sobre como configurar o DHCP e os comandos associados a ele, consulte a [Lista de tarefas de configuração do DHCP](#).

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

!--- Address range excluded from DHCP pools.

ip dhcp pool test_dhcp

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

network 10.10.1.0 255.255.255.0

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

```
default-router 10.10.1.1

!--- DHCP option for default gateway.

dns-server 10.30.1.1

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

netbios-name-server 10.40.1.1

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

lease 0 0 1

!--- Lease time.

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

## Informações Relacionadas

- [Ferramentas e recursos](#)
- [Suporte Técnico - Cisco Systems](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.