

Compreensão e Troubleshooting DHCP no Catalyst Switch ou em Redes Corporativas

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Principais conceitos](#)

[Cenários de exemplo](#)

[Informações de Apoio](#)

[Compreendendo o DHCP](#)

[Referências RFC de DHCP atuais](#)

[Tabela de mensagens DHCP](#)

[Renovando a concessão](#)

[Pacote DHCP](#)

[Conversão entre cliente-servidor para cliente obtendo o endereço DHCP em que o cliente e o servidor DHCP residem na mesma sub-rede](#)

[Função do agente de transmissão de DHCP/BootP](#)

[Configurando o DHCP/BootP Relay Agent Feature no Cisco IOS Router](#)

[Ajustando emperramentos manuais](#)

[Como fazer o trabalho DHCP em segmentos IP secundários](#)

[Conversação cliente-servidor de DHCP com função de transmissão de DHCP](#)

[Considerações de DHCP de inicialização do ambiente da PRE-execução \(PXE\)](#)

[Compreendendo e Troubleshooting de DHCP usando Sniffer Traces](#)

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

[Decodificando o farejador de rastreamento do DHCP Client e Server separado por um roteador configurado como DHCP Relay Agent](#)

[Troubleshooting de DHCP Quando Estações de Trabalho Cliente Não Conseguem Obter DHCP Addresses](#)

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

[Casos Práticos 2: Servidor DHCP e Cliente DHCP são separados por um roteador configurado para a funcionalidade Agente de transmissão de DHCP/BootP](#)

[O servidor DHCP no roteador não atribui Adresses com um erro ESGOTADO POOL](#)

[Módulos de Troubleshooting de DHCP](#)

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

[As palavras-chaves incorporadas após a opção do comando ip dhcp pool {option number} ASCII estão nas aspas duplas](#)

Introdução

Este documento contém informações sobre como resolver problemas de vários problemas comuns do protocolo DHCP que podem surgir na rede de switch Cisco Catalyst. Este documento inclui Troubleshooting para o uso do recurso Cisco IOS® DHCP/BootP Relay Agent do Cisco IOS.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Convenções

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

Principais conceitos

Estes são diversos conceitos chaves do DHCP:

- Os clientes do DHCP não têm o endereço IP configurado inicialmente e por isso devem enviar uma requisição de transmissão para obter um endereço IP de um servidor de DHCP.
- O Roteadores, à revelia, não envia 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 de Cisco Router da transmissão de DHCP é fornecida através dos comandos **ip helper do relação-nível**

Cenários de exemplo

Cenário 1: Roteamento do roteador Cisco entre o DHCP Client e as redes do server

Como configurado neste diagrama, relação Ethernet1 para a frente o DHCPDISCOVER transmitido do cliente a 192.168.2.2 através da relação Ethernet1. O servidor DHCP cumpre o pedido com o unicast. Nenhuma outra configuração para o roteador é necessária neste exemplo.

Cenário 2: Interruptor do Cisco catalyst com roteamento de módulo I3 entre o DHCP Client e as redes do server

Como configurado no diagrama, relação VLAN20 para a frente o DHCPDISCOVER transmitido do cliente a 192.168.2.2 através da relação VLAN10. O servidor DHCP cumpre o pedido com o unicast. Nenhuma outra configuração para o roteador é necessária neste exemplo. As portas de switch precisam de ser configuradas como portas de host e têm a medida - portfast do protocolo de árvore (STP) permitido, e o entroncamento e a canalização desabilitadas.

Informações de Apoio

O DHCP fornece um mecanismo através de que os computadores que se usam o Protocolo de Controle de Transmissão/Protocolo de Internet (TCP/IP) podem obter parâmetros da configuração de protocolo automaticamente através da rede. O DHCP é um padrão aberto que seja desenvolvido pelo [Dynamic Host Configuration-Working Group](#) (DHC-WG) do [Internet Engineering Task Force](#) (IETF).

O DHCP é baseado em um paradigma do servidor cliente, em que o DHCP Client, por exemplo, um computador de área de trabalho, contacta um servidor DHCP para 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. Uma vez que os roteadores não passam broadcasts por padrão, um servidor de DHCP seria necessário em cada sub-rede a menos que os roteadores estejam configurados para encaminhar o broadcast de DHCP usando o recurso DHCP Relay Agent.

Compreendendo o DHCP

O DHCP foi definido originalmente nos [request for comments \(RFC\) 1531](#) , e desde obsoleted pelo [RFC 2131](#) . [O DHCP é baseado no protocolo de bootstrap \(BOOTP\), que é definido no RFC 951](#) .

O DHCP é usado por estações de trabalho (anfitriões) para obter a informação de configuração inicial, tal como um endereço IP de Um ou Mais Servidores Cisco ICM NT, uma máscara de sub-rede, e um gateway padrão em cima da inicialização. Uma vez que cada host necessita de um endereço IP para se comunicar em uma rede IP, o DHCP alivia a carga administrativa de configurar manualmente um endereço IP para cada host. Além disso, se um host se move para uma sub-rede diferente IP, deve usar um endereço IP de Um ou Mais Servidores Cisco ICM NT diferente do que esse ele se usou previamente. O DHCP toma deste automaticamente. Permite que o host escolha um endereço IP de Um ou Mais Servidores Cisco ICM NT na sub-rede correta IP.

Referências RFC de DHCP atuais

- RFC 2131 - DHCP
- Opções DHCP do RFC2132 e Extensões do Fornecedor do BootP
- RFC 1534 - Interoperação entre o DHCP e o 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 opções de DHCP novas

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 carrega acima, a pilha TCP/IP no host transmite uma mensagem de transmissão (DHCPDISCOVER) a fim ganhar um endereço IP de Um ou Mais Servidores Cisco ICM NT e uma máscara de sub-rede, entre outros parâmetros de configuração. Isto inicia uma troca entre o servidor DHCP e o host. Durante esta troca, o cliente passa através de diversos estados bem definidos alistados abaixo:

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

Ao se movimentar entre os estados listados acima, o cliente e o servidor poderão trocar os tipos de mensagens listados na Tabela de Mensagens DHCP, abaixo.

Tabela de mensagens DHCP

| Referência | Mensagem | Use |
|------------|--------------|--|
| 0x01 | DHCPDISCOVER | O cliente está procurando por servidores DHCP disponíveis. |
| 0x02 | DHCP OFFER | A resposta de servidor ao cliente DHCPDISCOVER. |
| 0x03 | DHCPREQUEST | As transmissões do cliente ao server, pedindo parâmetros oferecidos de um server especificamente, como definido no pacote. |
| 0x04 | DHCPDECLINE | A comunicação de cliente com servidor, indicando que o endereço de rede já está em uso. |
| 0x05 | DHCPACK | A comunicação de servidor com cliente com os parâmetros de configuração, incluindo o endereço de rede comprometido. |
| 0x06 | DHCPNACK | A comunicação de servidor com cliente, recusando o pedido para o parâmetro de configuração. |
| 0x07 | DHCPRELEASE | A comunicação de cliente com servidor, abandonando o endereço de rede e cancelando aluguer restante. |

| | | |
|------|------------|--|
| 0x08 | DHCPINFORM | A comunicação de cliente com servidor, pedindo somente parâmetros da configuração local que o cliente já configurou 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 qual sub-rede pertence, a mensagem DHCPDISCOVER é um broadcast de todas as sub-redes (endereço IP de destino de 255.255.255.255), com um endereço IP de origem de 0.0.0.0. O endereço IP de origem é 0.0.0.0, porque o cliente não tem um endereço IP configurado. Se um servidor DHCP existir nessa sub-rede local e estiver configurado e em operação corretamente, o servidor DHCP ouvirá a transmissão 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.

Este agente de transmissão pode qualquer um ser um host dedicado (por exemplo, Microsoft Windows server), ou roteador (por exemplo, um roteador Cisco configurado com indicações do ajudante de IP do nível de 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. Este mensagem dhcpoffer contém a informação de configuração inicial para o cliente. Por exemplo, o servidor DHCP preencherá 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 enviará o DHCPOFFER ao endereço de broadcast, mas incluirá o endereço do hardware dos clientes no campo do chaddr da oferta, assim que o cliente sabe que é o destino pretendido. Se o servidor DHCP não estiver na sub-rede local, ele devolverá o DHCPOFFER como um pacote unicast, na porta 67 do UDP, para o Agente de Transmissão DHCP/BootP que originou o DHCPDISCOVER. O DHCP/BootP Relay Agent então transmitirá ou unicast o DHCPOFFER na sub-rede local na porta 68 UDP, segundo o flag de transmissão ajustado pelo cliente bootp.

DHCPREQUEST

Depois que o cliente recebe um DHCPOFFER, ele responde com uma mensagem do DHCPREQUEST, indicando sua intenção de aceitar os parâmetros no DHCPOFFER e entra no estado Requesting (Solicitando). O cliente pode receber várias mensagens de DHCPOFFER, uma de cada servidor DHCP que recebeu a mensagem original de DHCPDISCOVER. O cliente escolhe um DHCPOFFER e responde apenas para aquele servidor DHCP, implicitamente recusando as demais mensagens DHCPOFFER. O cliente identifica o servidor selecionado preenchendo o campo de opção Identificador do Servidor com o endereço IP dos servidores

DHCP. O DHCPREQUEST também é um broadcast, portanto, todos os servidores de DHCP que enviaram um DHCP OFFER verão o DHCPREQUEST, e cada um saberá se o seu DHCP OFFER foi aceito ou rejeitado. Qualquer opção adicional de configuração que o cliente exija deve ser incluída no campo de opções da mensagem DHCPREQUEST. Apesar de o cliente ter recebido uma oferta de endereço IP, ele enviará a mensagem DHCPREQUEST com um endereço IP de origem 0.0.0.0. Nesse momento, o cliente ainda não recebeu a verificação de que está pronto para usar o endereço IP.

DHCPACK

Depois que o servidor de DHCP recebe o DHCPREQUEST, ele reconhece a requisição com uma mensagem DHCPACK, e isso 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 arrendamento em seu banco de dados e o identifica de maneira exclusiva, utilizando o identificador cliente ou chaddr e o endereço IP associado. Ambos, cliente e servidor, utilizam essa combinação de identificadores para consultar o leasing. O identificador de cliente é o MAC address do dispositivo mais o tipo de mídia.

Antes que o cliente DHCP comece a utilizar o novo endereço, ele deve calcular os parâmetros de tempo associados ao endereço alugado, que são LT (Tempo de Leasing), T1 (Tempo de Renovação) e T2 (Tempo de Religação). 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 entrando no estado de requisição. O cliente retransmitirá o DHCPREQUEST pelo menos quatro vezes em 60 segundos antes de reiniciar o estado inicializando.

DHCPDECLINE

O cliente recebe DHCPACK e, opcionalmente, realizará uma verificação final nos parâmetros. O cliente executa este procedimento, enviando solicitações de protocolo ARP para o endereço IP fornecido no DHCPACK. Se o cliente detecta que o endereço é já dentro uso recebendo uma resposta à requisição ARP, o cliente enviará um mensagem DHCPDECLINE ao server e reiniciará o processo de configuração entrando no estado de pedido.

DHCPINFORM

Se um cliente tiver obtido um endereço de rede por outros meios ou tiver um endereço IP manualmente configurado, uma estação de trabalho cliente pode usar a mensagem de requisição DHCPINFORM para obter outros parâmetros de configuração local, como o nome de domínio e os servidores DNS. Os servidores DHCP que recebem uma mensagem DHCPINFORM constróem uma mensagem DHCPACK com qualquer parâmetro de configuração local adequado para o cliente sem alocar um novo endereço IP. Este DHCPACK será enviado a unicast ao

cliente.

DHCPRELEASE

Um DHCP Client pode escolher abandonar seu aluguer em um endereço de rede enviando um mensagem dhcprelease ao servidor DHCP. O cliente identifica o aluguel a ser liberado, usando o campo de identificador de cliente e o endereço de rede na mensagem DHCPRELEASE. Se você precisa de estender a escala atual do conjunto de DHCP, remova o conjunto de endereço atual e especifique a escala nova dos endereços IP de Um ou Mais Servidores Cisco ICM NT sob o conjunto de DHCP. A fim remover os endereços IP de Um ou Mais Servidores Cisco ICM NT específicos ou um intervalo de endereço que você quer estar no conjunto de DHCP, use o [comando ip dhcp excluded-address](#).

Note: Se os dispositivos usam o BOOTP, os alugueres infinitos do comprimento estão mostrados nos emperramentos DHCP do Roteadores.

[Renovando a concessão](#)

Como o endereço IP é concedido somente a partir do servidor, a concessão deve ser renovada periodicamente. Quando um meio do Lease Time expirarem ($T1=0.5 \times LT$), o cliente tentará renovar o aluguer. O cliente entra no estado de Renewing e envia uma mensagem DHCPREQUEST para o servidor, que mantém a licença atual. O servidor responderá à solicitação de renovação com uma mensagem DHCPACK se concordar em renovar a concessão. A mensagem DHCPACK conterá a nova concessão e todos os novos parâmetros de configuração, caso alguma alteração seja feita no servidor durante o tempo da concessão anterior. Se, por algum motivo, o cliente não puder chegar ao servidor que mantém o arrendamento, tentará renovar o endereço de qualquer servidor DHCP depois que o servidor DHCP original não responder às solicitações de renovação em um tempo $T2$. O valor padrão do $T2$ é $(7/8 \text{ de } x \text{ LT})$. Isso significa $T1 < T2 < LT$.

Se, anteriormente, o cliente teve um endereço IP de DHCP atribuído e ele for reiniciado, o cliente requisitará especificamente o endereço IP anteriormente alugado em um pacote DHCPREQUEST. Esta DHCPREQUEST ainda terá 0.0.0.0 como endereço IP de origem e o destino com o endereço IP de difusão 255.255.255.255.

Um cliente enviando um DHCPREQUEST durante uma reinicialização não deve preencher o campo de identificador do servidor e, por sua vez, deve preencher o campo de opção de endereço IP solicitado. Os clientes estritamente em conformidade com o RFC irão preencher o campo ciaddr com o endereço solicitado em vez do campo de opção DHCP. O servidor DHCP aceitará o método. O comportamento do servidor de DHCP depende de inúmeros fatores como por exemplo, no caso de servidores de DHCP em Windows NT, da versão do sistema operacional que está sendo utilizada, além de outros fatores, como superescopo. Se o servidor de DHCP determinar que o cliente ainda pode utilizar o endereço de IP solicitado, ele permanecerá silencioso ou enviará um pacote 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. O cliente irá para o estado de inicialização e enviará uma mensagem de DHCPDISCOVER.

Note: O servidor DHCP atribui o endereço IP de Um ou Mais Servidores Cisco ICM NT inferior de um pool dos endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes DHCP. Quando o aluguer do endereço inferior expira, está atribuído a um outro cliente se se pede. Você não pode fazer nenhuma mudanças nos endereços de DHCP da ordem é atribuído.

Pacote DHCP

A mensagem do DHCP é variável em comprimento e consiste em campos listados na tabela a seguir.

Note: Este pacote é uma versão modificada do pacote original BOOTP.

| Ca mpo | Byt es | Nom e | Descrição |
|------------------|-----------|---------------------------------------|--|
| op | 1 | Opco de | Identifica o pacote como um pedido ou uma resposta: 1=BOOTREQUEST, 2=BOOTREPLY |
| htyp e | 1 | Tipo de hard ware | Especifica o tipo de endereço do hardware de rede. |
| hlen | 1 | Tama nho do hard ware | Especifica a extensão do endereço de hardware. |
| salt os | 1 | Salto s | 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 trans ação | Um número aleatório selecionado pelo cliente. Todas as mensagens DHCP trocadas em uma determinada transação DHCP usam o ID (xid). |
| seg und os | 2 | Segu ndos | Especifica o número de segundos desde o início do processo de DHCP. |
| flag s | 2 | Flags | Indica se a mensagem será transmitida por difusão ou unicast. |
| ciad dr | 4 | Ende reço IP client e | Utilizado apenas o cliente sabe seu endereço IP, como no caso dos estados Bound, Renew ou Rebinding. |
| yiad dr | 4 | Seu ender eço IP | Se o endereço IP do cliente for 0.0.0.0, o servidor DHCP colocará o endereço IP oferecido ao cliente nesse campo. |
| siad dr | 4 | Ende reço IP do servi dor | Se o cliente conhece o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP, este campo estará povoado com o endereço do servidor DHCP. Caso contrário, ele será usado em DHCPOFFER e DHCPACK a partir do servidor DHCP. |

| | | | |
|---------|----------|----------------------------------|---|
| giaddr | 4 | Endereço IP do roteador (GIADDR) | O endereço IP de porta de comunicação, preenchido pelo agente do relé 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. |

[Conversão entre cliente-servidor para cliente obtendo o endereço DHCP em que o cliente e o servidor DHCP residem na mesma sub-rede](#)

| Descrição do Pacote | Endereço MAC de Origem | Endereço MAC de destino | ADDR IP da fonte | End IP de destino |
|---------------------|------------------------|-------------------------|------------------|-------------------|
| DHCPDISCOVER | Cliente | Broadcast | 0.0.0.0 | 255.255.255.255 |
| DHCPOFFER | DHCPSever | Broadcast | DHCPSever | 255.255.255.255 |
| DHCPREQUEST | Cliente | Broadcast | 0.0.0.0 | 255.255.255.255 |
| DHCPACK | DHCPSever | Broadcast | DHCPSever | 255.255.255.255 |

[Função do agente de transmissão de DHCP/BootP](#)

O Roteadores, à revelia, não enviará pacotes de transmissão. Como as mensagens de cliente DHCP usam o endereço de destino IP de 255.255.255.255 (todas as transmissões de rede), os clientes DHCP não poderão enviar solicitações a um servidor DHCP em uma sub-rede diferente, a menos que o Agente de retransmissão DHCP/BootP esteja configurado no roteador. O Agente de Relay de DHCP/BootP irá encaminhar as solicitações de DHCP em nome de um cliente de DHCP para o servidor de DHCP. O agente de transmissão de DHCP/BootP anexará seu próprio endereço IP ao endereço IP da origem dos quadros DHCP que estão indo para o servidor DHCP. Isto permite que o servidor DHCP responda através do unicast ao DHCP/BootP Relay Agent. O DHCP/BootP Relay Agent igualmente povoará o campo de endereço IP de Gateway com o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação em que o mensagem DHCP é recebido do cliente. O servidor DHCP usa o campo de endereço IP de Gateway para determinar a sub-rede de que o DHCPDISCOVER, o DHCPREQUEST, ou o mensagem DHCPINFORM originam.

[Configurando o DHCP/BootP Relay Agent Feature no Cisco IOS Router](#)

A configuração de um roteador Cisco para encaminhar solicitações de BootP ou DHCP é simples - configure um endereço IP auxiliar apontando para o servidor DHCP/BootP ou para o endereço de transmissão de sub-rede da rede que contém o servidor. Por exemplo, considere o seguinte diagrama de rede:

[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. À revelia, o endereço auxiliar IP enviará os seguintes broadcasts de 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 de IP podem direcionar as difusões de UDP para um endereço IP de unicast ou de difusão. No entanto, não é recomendável usar o IP helper-address para encaminhar broadcasts de UDP de uma sub-rede para o endereço de broadcast de outra sub-rede, devido ao grande número de inundações de broadcast possíveis. As entradas múltiplas do endereço auxiliar IP em uma interface única são apoiadas também, como mostrado abaixo:

```
!  
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 apoiam o Balanceamento de carga dos servidores DHCP que são configurados como agentes de transmissão de DHCP. Os roteadores Cisco encaminham o mensagem DHCPDISCOVER a todos os helper addresss (endereço do ajudante) mencionados para essa relação. Tendo dois ou mais servidores DHCP servir uma sub-rede aumenta somente o tráfego DHCP enquanto os DHCPDISCOVER, os DHCPOFFER, e os DHCPREQUEST/mensagens DHCPDECLINE são trocados entre cada par de DHCP Client e server.

[Ajustando emperramentos manuais](#)

Há duas maneiras de estabelecer emperramentos manuais; um é para o host de Windows, e o outro é para anfitriões não-Windows. Há dois comandos diferentes usados para configurar; um é para clientes DHCP de Microsoft, e o outro é para clientes DHCP de NON-Microsoft: [Cliente-identificador DHCP](#) (emperramento do manual - Clientes DHCP de Microsoft) e [hardware-endereço DHCP](#) (emperramento do manual - clientes DHCP de NON-Microsoft). A razão para dois comandos diferentes é que um PC que seja executado com Windows altera seus MAC, e uns **01** é adicionado no início do endereço. Estas são as configurações de exemplo:

- O seguinte é a configuração para clientes DHCP de Microsoft

```

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

```

- O seguinte é a configuração para clientes DHCP de NON-Microsoft

```

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

```

[Como fazer o trabalho DHCP em segmentos IP secundários](#)

À revelia, o DHCP tem uma limitação que os pacotes de resposta estão enviados somente se o pedido é recebido da relação configurada com o endereço IP primário. O tráfego DHCP usa o endereço de broadcast. Quando a requisição DHCP for recebida pela interface do roteador, ele para a frente que ao servidor DHCP (quando o endereço auxiliar IP for configurado) com um endereço de origem do IP principal configurou na relação para deixar o servidor DHCP saber que IP pool deve usar (para o cliente) no pacote da resposta DHCP.

Não há nenhuma maneira para que o roteador saiba se o pedido da transmissão de DHCP vem de um dispositivo que esteja na rede IP secundária configurada na relação. Como uma ação alternativa, a configuração da secundário-relação (contanto que o dispositivo conectado ao dot1q dos suportes de roteador que etiqueta) para separar as duas sub-redes pode ser configurada, assim que ambos eles obtêm seus endereços IP de Um ou Mais Servidores Cisco ICM NT correspondentes corretamente.

Se o endereço secundário é a maneira preferida, há uma outra ação alternativa, que seja permitir o Smart-[relé DHCP do global configuration command ip](#). Isto tem uma limitação que usa somente o IP secundário para retransmitir a requisição DHCP se não há nenhuma resposta do servidor DHCP depois que três pedidos consecutivos para o pool do endereço primário.

Conversação cliente-servidor de DHCP com função de transmissão de DHCP

A tabela abaixo ilustra o processo para que um DHCP Client obtenha um endereço IP de Um ou Mais Servidores Cisco ICM NT de um servidor DHCP. [Esta tabela é modelada de acordo com o diagrama de rede acima](#). Cada valor numérico do diagrama representa um pacote descrito abaixo. Esta tabela é um ponto de referência para a compreensão do fluxo de pacote de conversação cliente-servidor DHCP. Esta tabela é igualmente útil para determinar onde os problemas de DHCP podem ocorrer.

| 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 IP de destino de pacote |
|---|------------------------|-------------------------|-------------|----------------------------------|---------------------------------|-----------------------------------|----------------------------------|
| 1. DHCP DISCOVER é enviado do cliente. | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0005.DC9.C640 | 0.0.0.0 | ffff.ffff.ffff (transmissão) | 255.255.255.255 |
| 2. O roteador recebe o DHCP DISCOVER na relação E1. O roteador reconhece que esse pacote é um broadcast DHCP UDP. O | 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 | 192.168.2.2 |

| | | | | | | | | |
|---|------|------|------|--------|------|------|--------|--|
| roteado r agora agirá como um agente de transmi ssão de DHCP/ BootP e preenc herá o campo de endere ço IP do gatewa y com o endere ço IP de interfac e de entrada , alterará o endere ço IP de origem para um endere ço IP de interfac e de entrada e encami nhará a solicita ção diretam ente ao servido r de DHCP. | | | | | | | | |
| 3. O | 192. | 192. | 192. | Endere | 192. | Ende | 192.16 | |

| | | | | | | | |
|--|-------------|-------------|-------------|---|-------------|---|-------------|
| servidor DHCP recebe o DHCP DISCOVER e está enviando um DHCP OFFER ao agente de transmissão de DHCP. | 168.1.2 | 168.2.2 | 168.1.1 | çõ MAC do servidor de DHCP | 168.2.2 | reço E2 MAC da interf ace | 8.1.1 |
| 4. O agente de transmissão de DHCP recebe um DHCP OFFER e desvia a difusão dele na LAN local. | 192.168.1.2 | 192.168.2.2 | 192.168.1.1 | Endere ço MAC da interfac e E1 | 192.168.1.1 | ffff.ffff .ffff (broa dcast) | 255.255.255 |
| 5. DHCP REQUEST enviado do cliente. | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0005.D CC9.C 640 | 0.0.0.0 | ffff.ffff .ffff (trans miss ão) | 255.255.255 |
| 6. O roteador recebe o DHCP REQUEST na relação E1. O | 0.0.0.0 | 0.0.0.0 | 192.168.1.1 | Endere ço E2 MAC da interfac e | 192.168.1.1 | Ende reço MAC do servi dor de DHC P | 192.168.2.2 |

| | | | | | | | |
|---|--|--|--|--|--|--|--|
| <p>roteador reconhece que este pacote é a difusão UDP do DHCP. O roteador agora atuará como um agente de transmissão de DHCP e encherá dentro o campo de endereço IP de Gateway com o endereço IP de interface de entrada, mudando o endereço IP de origem a um endereço IP de interface de entrada</p> | | | | | | | |
|---|--|--|--|--|--|--|--|

| | | | | | | | |
|--|-------------|-------------|-------------|----------------------------------|-------------|------------------------------|-------------|
| , e envia o pedido diretamente ao servidor DHCP. | | | | | | | |
| 7. O servidor DHCP recebe o DHCP REQUEST e está enviando o DHCPACK ao Agente de Transmissão de 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 | 192.168.1.1 |
| 8. O DHCP/BootP Relay Agent recebe o DHCPACK e encaminhará broadcast do DHCPACK no LAN local. O cliente aceitará o ACK e usará o endereço IP | 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 |

| | | | | | | | |
|---|--|--|--|--|--|--|--|
| de Um ou Mais Servido res Cisco ICM NT do cliente. | | | | | | | |
|---|--|--|--|--|--|--|--|

Considerações de DHCP de inicialização do ambiente da PRE- execução (PXE)

O ambiente da PRE-execução (PXE) permite que uma estação de trabalho carreg de um server em uma rede antes de carreg o sistema operacional no disco rígido local. Um administrador de rede não tem que fisicamente visitar a estação de trabalho específica e manualmente carreg a. Os sistemas operacionais e o outro software, tal como programas de diagnóstico, podem ser carregados no dispositivo de um server sobre a rede. Os usos DHCP do ambiente PXE configurar-la são endereço IP de Um ou Mais Servidores Cisco ICM NT.

A configuração do DHCP/BootP Relay Agent deve ser feita no roteador se o servidor DHCP é ficado situado em um outro segmento roteado da rede. [O comando ip helper-address na relação do roteador local deve ser configurado.](#) Refira a [característica configurando do DHCP/BootP Relay Agent na seção de roteador do Cisco IOS](#) deste documento para a informação de configuração.

Compreendendo e Troubleshooting de DHCP usando Sniffer Traces

Decodificando o farejador de rastreamento no servidor e no cliente DHCP no mesmo segmento de LAN

O farejador de rastreamento abaixo é compreendido de seis quadros. Esses seis quadros ilustram um cenário de trabalho para DHCP, onde o cliente e o servidor de DHCP residem no mesmo segmento físico ou lógico. Ao Troubleshoot DHCP, é importante combinar o farejador de rastreamento com os rastreamentos abaixo. Pode haver algumas diferenças se comparado aos rastreamentos abaixo, mas o fluxo de pacote geral 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 = 00636973636F2D30303030352E646363392E633634302D564C31**
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server
DHCP: 150 = Unknown Option

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

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

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2[192.168.1.1] [255.255.255.255] 331 0:01:26.825 0.015.172 05/07/2001 11:52:03 AM DHCP: Reply,
Message type: **DHCP Offer**

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

DLC:

DLC: Frame 2 arrived at 11:52:03.8258; frame size is 331 (014B hex) bytes.

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

DLC: **Source = Station 0005DCC42484**

DLC: Ethertype = 0800 (IP)

DLC:

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

IP:

IP: Version = 4, header length = 20 bytes

IP: Type of service = 00

IP: 000. = routine

IP: ...0 = normal delay

IP: 0... = normal throughput

IP:0.. = normal reliability

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

IP:0 = CE bit - no congestion

IP: Total length = 317 bytes

IP: Identification = 5

IP: Flags = 0X

IP: .0.. = may fragment

IP: ..0. = last fragment

IP: Fragment offset = 0 bytes

IP: Time to live = 255 seconds/hops

IP: Protocol = 17 (UDP)

IP: Header checksum = F901 (correct)

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

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

IP: No options

IP:

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

UDP:

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

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

UDP: Length = 297

UDP: No checksum

UDP: [289 byte(s) of data]

UDP:

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

DHCP:

DHCP: Boot record type = 2 (Reply)

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

DHCP: Hardware address length = 6 bytes

DHCP:

DHCP: Hops = 0

DHCP: **Transaction id = 00000882**

DHCP: Elapsed boot time = 0 seconds

DHCP: Flags = 8000

DHCP: 1... = Broadcast IP datagrams

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

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

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

DHCP: Relay Agent = [0.0.0.0]

DHCP: **Client hardware address = 0005DCC9C640**

DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Address Renewal interval = 42767 (seconds)
DHCP: Address Rebinding interval = 74843 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.1.3]**
DHCP: **Domain Name Server address = [192.168.1.4]**
DHCP: **Gateway address = [192.168.1.1]**
DHCP:

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

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3[0.0.0.0] [255.255.255.255] 618 0:01:26.829 0.003.586 05/07/2001 11:52:03 AM DHCP: Request,
Message type: **DHCP Request**

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

DLC:

DLC: Frame 56 arrived at 11:52:03.8294; frame size is 618 (026A hex) bytes.

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

DLC: **Source = Station 0005DCC9C640**

DLC: Ethertype = 0800 (IP)

DLC:

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

IP:

IP: Version = 4, header length = 20 bytes

IP: Type of service = 00

IP: 000. = routine

IP: ...0 = normal delay

IP: 0... = normal throughput

IP:0.. = normal reliability

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

IP:0 = CE bit - no congestion

IP: Total length = 604 bytes

IP: Identification = 10

IP: Flags = 0X

IP: .0.. = may fragment

IP: ..0. = last fragment

IP: Fragment offset = 0 bytes

IP: Time to live = 255 seconds/hops

IP: Protocol = 17 (UDP)

IP: Header checksum = B987 (correct)

IP: **Source address = [0.0.0.0]**

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

IP: No options

IP:

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

UDP:

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

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

UDP: Length = 584

UDP: No checksum

UDP: [576 byte(s) of data]

UDP:

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

DHCP:

DHCP: Boot record type = 1 (Request)

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

DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303030352E646363392E633634302D564C31**
DHCP: **Server IP address = [192.168.1.1]**
DHCP: **Request specific IP address = [192.168.1.2]**
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload = 3 (File and Sname fields hold options)
DHCP:

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

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4[192.168.1.1] [255.255.255.255] 331 0:01:26.844 0.014.658 05/07/2001 11:52:03 AM DHCP: Reply,
Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 57 arrived at 11:52:03.8440; frame size is 331 (014B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC42484**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 317 bytes
IP: Identification = 6
IP: Flags = 0X
IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes

```

IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F900 (correct)
IP: Source address = [192.168.1.1]
IP: Destination address = [255.255.255.255]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 68 (BootPc/DHCP)
UDP: Length = 297
UDP: No checksum
UDP: [289 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 00000882
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: Client hardware address = 0005DCC9C640
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 86400 (seconds)
DHCP: Address Renewal interval = 43200 (seconds)
DHCP: Address Rebinding interval = 75600 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.1.3]
DHCP: Domain Name Server address = [192.168.1.4]
DHCP: Gateway address = [192.168.1.1]
DHCP:

```

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

```

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

```

```
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

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

```
Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
6 0005DCC9C640 Broadcast 60 0:01:27.355 0.508.778 05/07/2001 11:52:04 AM ARP: R PA=[192.168.1.2]
  HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 59 arrived at 11:52:04.3557; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

[Decodificando o farejador de rastreamento do DHCP Client e Server separado por um roteador configurado como DHCP Relay Agent](#)

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 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:

Traço do 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 3 - DHCPREQUEST - - - - -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3 [192.168.1.1] [192.168.2.2] 618 0:00:51.240 0.025.974 05/31/2001 07:02:54 AM DHCP: Request,
Message type: DHCP Request

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

DLC:

DLC: Frame 120 arrived at 07:02:54.7745; frame size is 618 (026A hex) bytes.

DLC: **Destination = Station 0005DC0BF2F4**

DLC: **Source = Station 003094248F72**

DLC: Ethertype = 0800 (IP)

DLC:

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

IP:

IP: Version = 4, header length = 20 bytes

IP: Type of service = 00

IP: 000. = routine

IP: ...0 = normal delay

IP: 0... = normal throughput

IP:0.. = normal reliability

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

IP:0 = CE bit - no congestion

IP: Total length = 604 bytes

IP: Identification = 54

IP: Flags = 0X

IP: .0.. = may fragment

IP: ..0. = last fragment

IP: Fragment offset = 0 bytes

IP: Time to live = 255 seconds/hops

IP: Protocol = 17 (UDP)

IP: Header checksum = 3507 (correct)

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

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

IP: No options

IP:

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

UDP:

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

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

UDP: Length = 584

UDP: Checksum = 4699 (correct)

UDP: [576 byte(s) of data]

UDP:

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

DHCP:

DHCP: Boot record type = 1 (Request)

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

DHCP: Hardware address length = 6 bytes

DHCP:

DHCP: Hops = 1

DHCP: Transaction id = 000005F4

DHCP: Elapsed boot time = 0 seconds

DHCP: Flags = 8000

DHCP: 1... = Broadcast IP datagrams

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

DHCP: Client IP address = [0.0.0.0]

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

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

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

DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30**
DHCP: Server IP address = [192.168.2.2]
DHCP: Request specific IP address = [192.168.1.2]
DHCP: Request IP address lease time = 172571 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload = 3 (File and Sname fields hold options)
DHCP:

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

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4 [192.168.2.2] [192.168.1.1] 347 0:00:51.240 0.000.153 05/31/2001 07:02:54 AM DHCP: Request,
Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 121 arrived at 07:02:54.7746; frame size is 347 (015B hex) bytes.
DLC: **Destination = Station 003094248F72**
DLC: **Source = Station 0005DC0BF2F4**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 42
IP: Flags = 0X
IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3622 (correct)
IP: **Source address = [192.168.2.2]**
IP: **Destination address = [192.168.1.1]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 313

```
UDP: Checksum = 7DF6 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172800 (seconds)
DHCP: Address Renewal interval = 86400 (seconds)
DHCP: Address Rebinding interval = 151200 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:
```

[Troubleshooting de DHCP Quando Estações de Trabalho Cliente Não Conseguem Obter DHCP Addresses](#)

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

Quando o servidor e o cliente DHCP reside no mesmo segmento de LAN ou VLAN e o cliente não pode obter um endereço IP de um servidor DHCP, é improvável que o roteador local esteja causando um problema de DHCP. É provável que o problema esteja relacionado aos dispositivos que conectam o servidor DHCP e o cliente DHCP. Contudo, o problema pode ser com o servidor DHCP ou o cliente próprio. Siga os módulos de Troubleshooting abaixo para determinar qual dispositivo está causando o problema.

Note: Para configurar o servidor DHCP na pela base vlan, defina conjuntos de DHCP diferentes para endereços de DHCP de cada serviço VLAN a seus clientes.

[Casos Práticos 2: Servidor DHCP e Cliente DHCP são separados por um roteador configurado para a funcionalidade Agente de transmissão de DHCP/BootP](#)

Quando o servidor DHCP e o cliente residem nos segmentos de LAN ou nos VLAN diferentes, o

roteador que funciona como um DHCP/BootP Relay Agent é responsável para enviar o DHCPREQUEST ao servidor DHCP. São necessárias outras etapas de Troubleshooting para resolver o problema do DHCP/BootP Relay Agent, bem como do servidor e cliente DHCP. Depois dos módulos de Troubleshooting abaixo deve determinar que dispositivo está causando a edição.

O servidor DHCP no roteador não atribui Adresses com um erro ESGOTADO POOL

É possível que alguns endereços estão mantidos ainda por clientes, mesmo se são liberados do pool. Isto pode ser verificado pela saída do **conflito DHCP da mostra IP**. Um conflito de endereço ocorre quando dois anfitriões usam o mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT. Na atribuição de endereço, o DHCP verifica para ver se há conflitos com o sibilho e o ARP gratuito.

Se um conflito é detectado, o endereço está removido do pool. O endereço é atribuído até que o administrador resolva o conflito. Não configurar **nenhum conflito DHCP IP que registra** para resolver esta edição.

Módulos de Troubleshooting de DHCP

Compreendendo de onde podem ocorrer problemas de DHCP

Os problemas de DHCP podem elevar devido a uma multidão de razões. As razões mais comuns são problemas de configuração. Entretanto, muitos problemas de DHCP podem ser causados por defeitos de software nos sistemas operacionais, nos drivers NIC (Placa de Interface de Rede) ou nos Agentes DHCP/BootP Relay dos roteadores. Devido ao número potencialmente de áreas problemática, uma aproximação sistemática à pesquisa de defeitos é exigida.

Lista breve com causas possíveis para os problemas de DHCP:

- Configuração padrão do Catalyst Switch
- Configuração do DHCP/BootP Relay Agent
- Questão de compatibilidade de NIC ou questão de característica DHCP.
- NIC defeituoso ou a instalação imprópria do driver NIC
- Paradas de rede intermitentes devendo frequentar a medida - computações da árvore
- Comportamento do sistema operacional ou software com defeito
- Defeito do software ou da configuração do escopo do servidor DHCP
- Interruptor do Cisco catalyst ou defeito do software em DHCP/BootP Relay Agent IO
- Failing da verificação do Unicast Reverse Path Forwarding (uRPF) porque a oferta de DHCP é recebida em uma relação diferente do que esperada. Quando a característica do encaminhamento de caminho reverso (RPF) é permitida em uma relação, um roteador Cisco pode deixar cair os pacotes do protocolo de configuração dinâmica host (DHCP) e do protocolo de bootstrap (BOOTP) que têm endereços de origem de 0.0.0.0 e endereços de destino de 255.255.255.255. O roteador pode igualmente deixar cair todos os pacotes IP que têm um destino do IP de transmissão múltipla na relação. Esta edição é documentada em [CSCdw31925 \(clientes registrados somente\)](#).
- O Database Agent DHCP não é usado, mas o registro do conflito DHCP não é desabilitado

Este documento usará os módulos de Troubleshooting abaixo para determinar a causa-raiz, como

indicado na lista acima.

A. [Verifique 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 conectado a um Catalyst Switch, verifique que o DHCP Client e o server têm a conectividade física.

Para Catalyst Cactos switch tais como o 2948G, 4000, 5000, e os 6000 Series Switch, usam o **comando show port <mod->/<port_range>** notar o status de porta. Se o status da porta for diferente de conectado, a porta não passará nenhum tráfego, inclusive solicitações de cliente DHCP. A saída dos comandos é esta:

```
Switch (enable) show port 5/1
Port Name Status Vlan Duplex Speed Type
-----
5/1 connected 1 a-full a-100 10/100BaseTX
```

Para os IO baseados comuta como o Catalyst 2900XL/3500XL/2950/3550, o comando equivalente ao **estado de show port** é **<interface> da relação da mostra**. Se o estado da relação é qualquer coisa a não ser o **<interface>** está acima, protocolo de linha está acima, a porta não passará o tráfego, incluindo requisições de cliente de DHCP. A saída dos comandos é esta:

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

[Se a conexão física tiver sido verificada e de fato não houver um enlace entre o Catalyst Switch e o cliente DHCP, consulte o documento Troubleshooting dos Cisco Catalyst Switches Quanto à Compatibilidade de NIC para obter mais informações sobre como Troubleshoot o problema de conectividade da camada física.](#)

Os erros excessivos do link de dados fazem com que as portas em alguns Catalyst Switches entrem em um estado errdisabled. Refira a [recuperação do estado de porta errdisable nas plataformas cactos](#) e a [recuperação do estado de porta errdisable nas plataformas do IOS da Cisco](#), que descrevem o estado errdisable, explica como recuperar dela, e fornece exemplos de recuperação deste estado.

B. [Conectividade de rede de teste configurando a estação de trabalho cliente com endereço IP estático](#)

Esse procedimento se aplica a todos os estudos de caso.

Ao Troubleshoot qualquer problema relacionado ao DHCP, é importante verificar a conectividade da rede configurando um IP Address estático em uma estação de trabalho cliente. Caso a estação de trabalho não possa alcançar recursos da rede, mesmo tendo um endereço IP configurado estaticamente, a causa principal do problema não é o DHCP. Nesse ponto, o Troubleshooting de conectividade de rede é necessária.

C. [Verifique a edição como um problema de inicialização](#)

Esse procedimento se aplica a todos os estudos de caso.

Se o cliente de DHCP não for capaz de obter um endereço IP no servidor de DHCP ao inicializar, tente obter um endereço IP do servidor de DHCP, forçando o cliente a enviar uma solicitação de DHCP manualmente. Emita as seguintes etapas para obter manualmente um endereço IP de Um ou Mais Servidores Cisco ICM NT de um servidor DHCP para os sistemas operacionais alistados abaixo.

Microsoft Windows 95/98/ME: Clique o **botão Start Button**, e execute o programa WINIPCFG.exe. Clique o **botão de ReleaseAll**, seguido pelo **botão de RenewAll**. Pode o DHCP Client agora obter um endereço IP de Um ou Mais Servidores Cisco ICM NT?

Microsoft Windows nt/2000: Abra uma janela de prompt de comando pelo **Cmd de** datilografia no **começo/campo executado**. Emita o comando ipconfig/renew na janela de prompt do comando, como mostrado abaixo. O cliente DHCP agora é capaz de obter um endereço IP?

Caso o cliente de DHCP seja capaz de obter um endereço IP renovando-o manualmente depois que o PC conclui o processo de inicialização, é possível que exista um problema de inicialização de DHCP. Se o DHCP Client é anexado a um interruptor do Cisco catalyst, o problema é muito provavelmente devido a um problema de configuração que trata o STP portfast e/ou a canalização e o entroncamento. Outras possibilidades incluem edições do cartão NIC e questões de inicialização da porta de switch. [Os passos de Troubleshooting D e E](#) devem ser revistos para ordenar para fora edições da configuração de porta de switch e do cartão NIC como a causa de raiz do problema de DHCP.

D. Verifique a configuração de porta de switch (STP portfast e outros comandos)

Se o interruptor é um Catalyst 2900/4000/5000/6000, verifique que a porta tem o STP portfast permitido e o entroncamento/a canalização desabilitada. 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 requerida. Estas alterações de configuração resolvem as edições as mais comuns DHCP Client que ocorrem com uma instalação inicial de um Catalyst Switch.

Para mais documentação em relação às exigências de configuração de porta de switch necessárias para que o DHCP opere-se corretamente quando conectado aos Catalyst Switches, reveja por favor o seguinte documento:

[Utilização de Portfast e outros comandos para reparar retardos de conectividade da inicialização de estação de trabalho](#)

Após ter revisto as diretrizes de configuração no documento acima, retorne a este documento para o Troubleshooting adicional.

E. Verifique para ver se há o cartão ou questões de Catalyst switch de NIC conhecido

Se a configuração de Catalyst switch está correta, é possível que uma questão de compatibilidade de software pode existir no NIC do Catalyst Switch ou do cliente DHCP que poderia causar questões de DHCP. A próxima etapa no Troubleshooting é rever para fora o seguinte documento e a regra todas as questões de software com o Catalyst Switch ou o NIC que podem contribuir ao problema:

[Troubleshooting de Compatibilidade entre Catalyst Switches e NIC](#)

Conhecimento do sistema operacional do cliente DHCP, assim como informações específicas de NIC (como fabricante, modelo e versão de driver) serão necessários para descartar qualquer questão de compatibilidade.

[F. Distinção se os clientes DHCP obtêm o endereço IP de Um ou Mais Servidores Cisco ICM NT na mesma sub-rede ou o VLAN como o servidor DHCP](#)

É importante distinguir se o DHCP está ou não funcionando corretamente quando o cliente estiver na mesma sub-rede ou VLAN como o servidor de DHCP. Se o DHCP estiver funcionando corretamente na mesma sub-rede ou VLAN que o servidor de DHCP, é possível que o problema do DHCP seja com o DHCP/BootP Relay Agent. Se o problema persistir mesmo com o teste de DHCP na mesma sub-rede ou VLAN que o servidor DHCP, o problema pode realmente ser do servidor DHCP.

[G. Verifique a configuração do retardo DHCP/bootp do roteador](#)

Siga os passos abaixo para verificar a configuração:

1. Ao configurar a transmissão 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 de estações de trabalho clientes de DHCP e deve ser direcionado para o servidor DHCP correto.
2. Verifique se o comando de configuração global, no `service dhcp`, não está presente. Este parâmetro de configuração desabilita todos os servidores de DHCP e a funcionalidade de relay no roteador. A configuração padrão, `DHCP do serviço`, não parecerá na configuração, e é o comando `default configuration`. Se o [DHCP do serviço](#) não é permitido, os clientes não recebem os endereços IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP. **Note:** No Roteadores que executa um Cisco IOS mais velho libera-se, o [comando ip bootp server](#) segura a função do agente de transmissão de DHCP em vez do **comando `service dhcp`**. Devido a isto, o **comando `ip bootp server`** precisa de ser permitido neste Roteadores se o **comando `ip helper-address`** é configurado para enviar transmissões UDP de DHCP e atuar corretamente como um agente de transmissão de DHCP em nome do DHCP Client.
3. Ao aplicar os comandos `ip helper-address` para encaminhar transmissões UDP para um endereço de transmissão de sub-rede, verifique se no `ip directed-broadcast` não está configurado em nenhuma interface externa que os pacotes de transmissão UDP tenham que atravessar. O broadcast não-direcionado a IP vai bloquear qualquer tradução de um broadcast direcionado a broadcasts físicos. Esta configuração da interface é configuração padrão no 12.0 e mais recente das versões de software.
4. O encaminhamento de transmissões de DHCP para o endereço de transmissão da sub-rede do servidor DHCP é um problema ocasional do software. Ao pesquisar defeitos o DHCP, tente sempre enviar transmissões UDP de DHCP ao endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP, como mostrado abaixo:

[H. Opção da identificação de subscritor \(82\) girada sobre](#)

A característica da informação do agente de transmissão de DHCP (opção 82) permitir os agentes de transmissão de DHCP (Catalyst Switches) de incluir a informação sobre se e o cliente anexado quando ele para a frente requisições DHCP de um DHCP Client a um servidor DHCP.

O servidor DHCP pode usar esta informação para atribuir endereços IP de Um ou Mais Servidores Cisco ICM NT, executar o controle de acesso, e para ajustar o Qualidade de Serviço (QoS) e as políticas de segurança (ou as outras políticas da parâmetro-atribuição) para cada subscritor de uma rede de provedor de serviços.

Quando a espiação DHCP é permitida em um interruptor, permite automaticamente a opção 82.

Se o servidor DHCP não é configurado para segurar os pacotes com opção 82, cessa de atribuir o endereço a esse pedido.

A fim resolver esta edição, desabilite a opção da identificação de subscritor (82) no Switches (agentes de transmissão) com o comando global configuration, **nenhuma opção de informação do relé DHCP IP**.

I. Database Agent DHCP e de conflito DHCP registro

Um Database Agent DHCP é todo o host — por exemplo, um FTP, um TFTP, ou um servidor de RCP — esse armazena o base de dados dos emperramentos DHCP. Você pode configurar agentes múltiplos do base de dados DHCP, e você pode configurar o intervalo entre atualizações da base de dados e transferências para cada agente. Use o [comando ip dhcp database](#) configurar um Database Agent e parâmetros do Database Agent.

Se você escolhe não configurar um Database Agent DHCP, desabilite a gravação de conflitos do endereço de DHCP no servidor DHCP. Não execute **nenhum** [comando ip dhcp conflict logging](#) desabilitar o registro do conflito do endereço de DHCP. Cancele os conflitos previamente registrados com [conflito claro DHCP IP](#).

Se isto não desabilita o conflito que registra, este Mensagem de Erro aparece:

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

J. Verifique o CDP para ver se há conexões de telefone IP

Quando o switchport que está conectado ao Cisco IP Phone tem o Cisco Discovery Protocol (CDP) desabilitado, o servidor DHCP não pode atribuir um endereço IP de Um ou Mais Servidores Cisco ICM NT apropriado ao telefone. O servidor DHCP tende a atribuir o endereço IP de Um ou Mais Servidores Cisco ICM NT que pertence ao VLAN de dados/sub-rede do switchport. Se o CDP é permitido, o interruptor pode detectar que o Cisco IP Phone pede o DHCP e pode fornecer a informação de sub-rede correta. O servidor DHCP pode então distribuir um endereço IP de Um ou Mais Servidores Cisco ICM NT da Voz VLAN/pool da sub-rede. Não há nenhuma etapa explícita exigida para ligar o serviço DHCP à Voz vlan.

K. Remover abaixo do SVI interrompe a operação da espiação DHCP

Nos Cisco Catalyst 6500 Series Switch, um SVI (no estado de fechamento) está criado automaticamente depois que configura o DHCP à espiação para um VLAN particular. A presença

deste SVI tem implicações diretas na operação correta da espiação DHCP.

A espiação DHCP nos Cisco Catalyst 6500 Series Switch que executam o Native IOS é executada na maior parte no processador de rotas (RP ou MSFC), não no processador de switch (SP ou supervisor). O Cisco Catalyst 6500 Series intercepta pacotes no hardware com VACL que fornecem os pacotes a uma lógica de alvo local (LTL) subscrita pelo RP. Uma vez que os quadros incorporam o RP, precisam primeiramente de ser associados com uma relação L3 (SVI) IDB antes que possam ser passados fora à divisória da espiação. Sem um SVI, este IDB não existe, e os pacotes obtêm deixados cair no RP.

L. [Endereço de broadcast limitado](#)

Quando um DHCP Client ajusta a transmissão mordida em um pacote DHCP, o servidor DHCP e o agente de transmissão enviam mensagens DHCP aos clientes com o endereço de broadcast todas em uma (255.255.255.255). Se o [comando ip broadcast-address](#) foi configurado enviar um broadcast de rede, a transmissão todas em uma enviada pelo DHCP está cancelada. A fim remediar esta situação, use o comando do limitado-transmissão-[endereço DHCP IP](#) assegurar-se de que uma transmissão da rede configurada não cancele o comportamento do padrão DHCP.

Alguns clientes DHCP podem somente aceitar uma transmissão todas em uma e não podem adquirir um endereço de DHCP a menos que este comando for configurado na interface do roteador conectada ao cliente.

M. [Debugando o DHCP usando comandos debug do roteador](#)

Verifique que o roteador está recebendo a requisição DHCP usando comandos debug

No Roteadores que o processamento do software de suporte dos pacotes DHCP, você pode verificar se um roteador está recebendo a requisição DHCP do cliente. O processo DHCP falhará se o roteador não está recebendo pedidos do cliente. Este passo de Troubleshooting envolve a configuração de uma lista de acesso para depurar a saída. A finalidade da lista de acesso é apenas para depuração e não é intrusiva para o roteador.

No modo de configuração global, insira a seguinte lista de acesso:

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

No modo exec, insira o seguinte 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
```

Com base na saída acima, está claro que o roteador está recebendo as solicitações de DHCP do

cliente. Essa saída mostra apenas um resumo do pacote, e não todo o pacote. Conseqüentemente, 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.

Verifique que o roteador está recebendo a requisição DHCP e as requisições de encaminhamento ao servidor DHCP usando comandos debug

Entradas adicionais na lista de acesso podem ser acrescentadas para ver se o roteador está conseguindo se comunicar com o servidor de DHCP. Novamente, essas depurações não examinam o pacote, mas você pode confirmar se o agente de retransmissão DHCP está encaminhando requisições ao servidor DHCP.

No modo de configuração global, crie a seguinte lista de acesso:

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

```
eq 67 do <dhcp_server> do host do <dhcp_relay_agent> do host UDP da licença da lista de acesso 100
```

```
eq 67 do <dhcp_relay_agent> do host do <dhcp_server> do host UDP da licença da lista de acesso 100
```

Por exemplo:

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

```
eq 67 de 192.168.2.2 do host de 192.168.1.1 do host UDP da licença da lista de acesso 100
```

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

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

```
eq 68 de 192.168.1.1 do host de 192.168.2.2 do host UDP da licença da lista de acesso 100
```

No modo exec, insira o seguinte comando debug:

```
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
```

Da saída acima, é claro que o roteador está recebendo as requisições DHCP do cliente e está enviando o pedido, pela configuração do DHCP/BootP Relay Agent, ao servidor DHCP. O servidor DHCP igualmente respondeu diretamente ao DHCP/BootP Relay Agent. Essa saída mostra apenas um resumo do pacote, e não todo o pacote. Por isso, não é possível determinar se o pacote está correto ou se o servidor está respondendo com um DHCPNAK. Todavia, o roteador recebeu um pacote de broadcast com as portas UDP e IP de origem e de destino corretas para o DHCP e não há comunicação em dois sentidos com o servidor de DHCP.

Verifique se o Roteador está Recebendo e Encaminhando a Requisição de DHCP Usando o

Comando debug ip udp

[O comando debug ip udp pode ser utilizado para traçar o caminho de uma solicitação de DHCP através de um roteador.](#) Todavia, essa depuração é intrusiva em um ambiente de produção, pois todos os pacotes UDP comutados e processados serão exibidos no console. Essa depuração não deve ser usada em produção.

aviso: O comando `debug ip udp` é intrusivo, e pode causar a utilização de unidade de processamento central alto (CPU).

No modo exec, insira o seguinte comando debug:

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 DHCPOFFER from DHCP server directed to
DHCP/BootP Relay Agent IP address. 00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68),
length=333 !--- Router forwarding DHCPOFFER from DHCP server to DHCP client via DHCP/BootP Relay
Agent. 00:18:48: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584 !--- Router
receiving DHCPREQUEST from DHCP client. 00:18:48: UDP: sent src=192.168.1.1(67),
dst=192.168.2.2(67), length=604 !--- Router forwarding DHCPDISCOVER unicast to DHCP server using
DHCP/BootP Relay Agent source IP address. 00:18:48: UDP: rcvd src=192.168.2.2(67),
dst=192.168.1.1(67), length=313 !--- Router receiving DHCPACK (or DHCPNAK) from DHCP directed to
DHCP/BootP Relay Agent IP address. 00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68),
length=333 !--- Router forwarding DHCPACK (or DHCPNAK) to DHCP client via DHCP/BootP Relay
Agent. 00:18:48: UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32 !--- DHCP
client verifying IP address not in use by sending ARP request for its own IP address. 00:18:50:
UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32 !--- DHCP client verifying
IP address not in use by sending ARP request for its own IP address.
```

Verifique se o roteador está recebendo e encaminhando a requisição de DHCP usando o comando `debug ip dhcp server packet`

Se o roteador IO é 12.0.x.T ou 12.1 e apoia a funcionalidade de servidor de DHCP IO, a eliminação de erros adicional pode ser feita usando o comando `debug ip dhcp server packet`. Isto debuga foi pretendido para o uso com os recursos de servidor de DHCP IOS, mas pode ser usado pesquisando defeitos a característica do DHCP/BootP Relay Agent também. Como com os passos de Troubleshooting precedentes, o roteador debuga não fornece uma determinação exata do problema desde que o pacote real não pode ser visto. Entretanto, as depurações permitem que se faça inferências no que diz respeito ao processamento de DHCP.

No modo exec, insira o seguinte comando debug:

debug ip dhcp server packet

```
Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
```

```
!--- Router received DHCPDISCOVER/REQUEST/INFORM and setting Gateway IP address to 192.168.1.1
for forwarding. 00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..
!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM. !---
0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier. 00:20:54: DHCPD:
forwarding BOOTREPLY to client 00e0.1ef2.c441. !--- BOOTREPLY includes DHCPPOFFER and DHCPNAK. !-
-- Client's MAC address is 00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY to client
00e0.1ef2.c441. !--- Router is forwarding DHCPPOFFER or DHCPNAK broadcast on local LAN interface.
00:20:54: DHCPD: setting giaddr to 192.168.1.1. !--- Router received DHCPDISCOVER/REQUEST/INFORM
and set Gateway IP address to 192.168.1.1 for forwarding. 00:20:54: DHCPD: BOOTREQUEST from
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !--- BOOTREQUEST includes DHCPDISCOVER,
DHCPREQUEST, and DHCPINFORM. !--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client
identifier. 00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441. !--- BOOTREPLY
includes DHCPPOFFER and DHCPNAK. !--- Client's MAC address is 00e0.1ef2.c441. 00:20:54: DHCPD:
broadcasting BOOTREPLY to client 00e0.1ef2.c441. !--- Router is forwarding DHCPPOFFER or DHCPNAK
broadcast on local LAN interface.
```

Execução Simultânea de Múltiplas Depurações

Ao executar múltiplas depurações simultaneamente, uma quantidade considerável de informações pode ser descoberta com relação à operação do Agente de transmissão de DHCP/BootP e o servidor. Usando as descrições para o Troubleshooting, você pode tirar conclusões sobre onde a funcionalidade do DHCP/BootP Relay Agent pode não estar funcionando corretamente.

```
Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
!--- Router received DHCPDISCOVER/REQUEST/INFORM and setting Gateway IP address to 192.168.1.1
for forwarding. 00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..
!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM. !---
0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier. 00:20:54: DHCPD:
forwarding BOOTREPLY to client 00e0.1ef2.c441. !--- BOOTREPLY includes DHCPPOFFER and DHCPNAK. !-
-- Client's MAC address is 00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY to client
00e0.1ef2.c441. !--- Router is forwarding DHCPPOFFER or DHCPNAK broadcast on local LAN interface.
00:20:54: DHCPD: setting giaddr to 192.168.1.1. !--- Router received DHCPDISCOVER/REQUEST/INFORM
and set Gateway IP address to 192.168.1.1 for forwarding. 00:20:54: DHCPD: BOOTREQUEST from
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !--- BOOTREQUEST includes DHCPDISCOVER,
DHCPREQUEST, and DHCPINFORM. !--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client
identifier. 00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441. !--- BOOTREPLY
includes DHCPPOFFER and DHCPNAK. !--- Client's MAC address is 00e0.1ef2.c441. 00:20:54: DHCPD:
broadcasting BOOTREPLY to client 00e0.1ef2.c441. !--- Router is forwarding DHCPPOFFER or DHCPNAK
broadcast on local LAN interface.
```

Obtenha o farejador de rastreamento e determine a causa de raiz de problema de DHCP

A utilização de técnicas de depuração do roteador nem sempre determinará a causa principal exata de um problema de DHCP. A última etapa na solução de um problema de DHCP é obter um controle de rastreador e anotar onde o processo não está funcionando corretamente. [Os rastreamentos de pacotes DHCP podem ser decifrados consultando as seções Decoding Sniffer Trace of DHCP Client and Server on Same LAN Segment \(Decodificando o farejador de rastreamento do cliente e do servidor DHCP no mesmo segmento de LAN\) e Decoding Sniffer Trace of DHCP Client and Server Separated by Router Configured as a DHCP Relay Agent \(Decodificando o farejador de rastreamento do cliente e do servidor DHCP separado por um roteador configurado como agente de transmissão de DHCP\) presentes neste documento.](#)

Para obter informações sobre de obter farejadores de rastreamento usando a característica do Switched Port Analyzer (SPAN) em Catalyst Switches, refira o seguinte documento:

- [Configurando o Catalyst Switched Port Analyzer \(PERÍODO\).](#)

Método Alternativo de Decodificação de Pacote Utilizando depuração no Roteador

Usando

[comando debug ip packet detail dump <acl> em um roteador Cisco](#), é possível obter um pacote inteiro encanta dentro indicado na interface de linha do comando system log or (CLI). [As seções Using the Verify Router is Receiving DHCP Request Using debug Commands e Verify Router is Receiving DHCP Request and Forwarding Request to DHCP Server Using debug Commands acima, junto com a palavra-chave dump acrescentada à lista de acesso, fornecerão as mesmas informações sobre depuração, mas com os detalhes do pacote em hexadecimais.](#) Para determinar os índices do pacote, o pacote precisará traduzido. Um exemplo é fornecido no Apêndice A.

[As palavras-chaves incorporadas após a opção do comando ip dhcp pool {option_number} ASCII estão nas aspas duplas](#)

Um roteador Cisco com uma opção de DHCP com o número de opção configurado pode encontrar uma falha se tenta analisar gramaticalmente a URL porque alguma palavra-chave incorporada depois que o *número de opção* ASCII da **opção do comando ip dhcp pool** está nas aspas duplas depois que o roteador está recarregado. Este comportamento é considerado nos dispositivos que executam os IO 12.4(17a), que é um Bug conhecido e é documentado em [CSCsk96976 \(clientes registrados somente\)](#).

Esta edição é resolvida nas Versões do IOS 12.4(17b), 12.4(18a) e mais atrasado, e 12.4(19)T1.

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

O base de dados de servidor DHCP é organizado como uma árvore. A raiz da árvore é o conjunto de endereços para redes naturais, os ramos são conjuntos de endereços da sub-rede, e as folhas são emperramentos manuais aos clientes. As subredes herdaram os parâmetros da rede e os clientes herdaram os parâmetros da subrede. Consequentemente, os parâmetros comuns, por exemplo o Domain Name, devem ser configurados a (rede ou sub-rede) nível o mais alto da árvore.

Para obter mais informações sobre como configurar o DHCP e os comandos a ele associados, consulte o link a seguir:

- [Lista de Tarefas de Configuração DHCP](#)

```
Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
!--- Router received DHCPDISCOVER/REQUEST/INFORM and
setting Gateway IP address to 192.168.1.1 for
forwarding. 00:20:54: DHCPD: BOOTREQUEST from
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !---
BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and
DHCPINFORM. !---
0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates
client identifier. 00:20:54: DHCPD: forwarding BOOTREPLY
to client 00e0.1ef2.c441. !--- BOOTREPLY includes
DHCPPOFFER and DHCPNAK. !--- Client's MAC address is
00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY
to client 00e0.1ef2.c441. !--- Router is forwarding
DHCPPOFFER or DHCPNAK broadcast on local LAN interface.
00:20:54: DHCPD: setting giaddr to 192.168.1.1. !---
Router received DHCPDISCOVER/REQUEST/INFORM and set
```

```
Gateway IP address to 192.168.1.1 for forwarding.  
00:20:54: DHCPD: BOOTREQUEST from  
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !---  
BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and  
DHCPINFORM. !---  
0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates  
client identifier. 00:20:54: DHCPD: forwarding BOOTREPLY  
to client 00e0.1ef2.c441. !--- BOOTREPLY includes  
DHCPPOFFER and DHCPNAK. !--- Client's MAC address is  
00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY  
to client 00e0.1ef2.c441. !--- Router is forwarding  
DHCPPOFFER or DHCPNAK broadcast on local LAN interface.
```

Informações Relacionadas

- [Recursos de Frame Relay DHCP no exemplo de configuração do VPN 3000 concentrator](#)
- [PIX/ASA 7.x como um exemplo de configuração da transmissão de DHCP](#)
- [Ferramentas e recursos](#)
- [Suporte Técnico - Cisco Systems](#)