

# Catalyst スイッチまたは企業ネットワークにおける DHCP の説明とトラブルシューティング

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[主なコンセプト](#)

[シナリオ例](#)

[背景説明](#)

[DHCP について](#)

[現在の DHCP RFC 参照](#)

[DHCP メッセージ表](#)

[リースの更新](#)

[DHCP パケット](#)

[DHCP サーバと同じサブネットにあるクライアントが DHCP アドレスを取得する場合のクライアントサーバ間のやり取り](#)

[DHCP/BootP リレー エージェントの役割](#)

[Cisco IOS ルータでの DHCP/BootP リレー エージェント機能の設定](#)

[手動バインディングの設定](#)

[セカンダリ IP セグメントで DHCP を稼働させる方法](#)

[DHCP リレー機能を使用した DHCP クライアントサーバ間のやり取り](#)

[Pre-Execution Environment \( PXE \) ブートアップ DHCP の注意事項](#)

[スニファトレースを使用した DHCP の理解とトラブルシューティング](#)

[同一の LAN セグメントにある DHCP クライアントとサーバのスニファトレースの解読](#)

[DHCP リレー エージェントとして設定されているルータによって分けられた DHCP クライアントとサーバのスニファトレースの解読](#)

[DHCP のトラブルシューティング：クライアントワークステーションが DHCP アドレスを取得できない場合](#)

[事例 1：DHCP サーバが DHCP クライアントと同じ LAN セグメントまたは VLAN 上にある場合](#)

[事例 2：DHCP/BootP リレー エージェント機能が設定されたルータによって、DHCP サーバと DHCP クライアントが分けられている場合](#)

[ルータ上の DHCP サーバがエラー POOL EXHAUSTED でアドレスの割り当てに失敗](#)

[DHCP のトラブルシューティング モジュール](#)

[DHCP 問題の発生源について](#)

[ip dhcp pool コマンドのオプション {option number} ASCII の後に入力されたキーワードが二重引用符で囲まれている](#)

[付録 A：IOS DHCP](#)

[関連情報](#)

## 概要

このドキュメントは、Cisco Catalyst スイッチ ネットワークで発生する可能性のある一般的な Dynamic Host Configuration Protocol ( DHCP ) 問題のトラブルシューティング方法について説明しています。また、Cisco IOS® DHCP/BootP リレー エージェント機能を使用した場合のトラブルシューティングについても記載されています。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

### 表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

### 主なコンセプト

DHCP の主なコンセプトを次に示します。

- DHCP クライアントには、最初は IP アドレスが設定されていないため、ブロードキャスト要求を送信して DHCP サーバから IP アドレスを取得する必要があります。
- デフォルトでは、ルータはブロードキャストを転送しません。DHCP サーバが別のブロードキャスト ドメイン ( レイヤ 3 ( L3 ) ネットワーク ) にある場合は、クライアントの DHCP ブロードキャスト要求に対応する必要があります。これには、DHCP リレー エージェントを使用します。
- Cisco ルータでの DHCP リレーの実装は、インターフェイスレベルの `ip helper` コマンドによって提供されます。

### シナリオ例

#### シナリオ 1 : Cisco DHCP

上記の図のように設定すると、インターフェイス Ethernet1 は、クライアントがブロードキャストした DHCPDISCOVER を、インターフェイス Ethernet1 経由で 192.168.2.2 に転送します。DHCP サーバは、ユニキャストによって要求に応答します。この例では、ルータにこれ以上の設定は必要ありません。

## シナリオ 2 : L3 Cisco Catalyst DHCP

上記の図のように設定すると、インターフェイス VLAN20 は、クライアントがブロードキャストした DHCPDISCOVER を、インターフェイス VLAN10 経由で 192.168.2.2 に転送します。DHCP サーバは、ユニキャストによって要求に応答します。この例では、ルータにこれ以上の設定は必要ありません。スイッチ ポートはホスト ポートとして設定し、Spanning-Tree Protocol ( STP; スパニング ツリー プロトコル ) PortFast を有効に、トランキングとチャネリングを無効にする必要があります。

### 背景説明

DHCP が提供するメカニズムにより、TCP/IP を使用するコンピュータは、ネットワークを通じて自動的にプロトコル設定パラメータを取得できます。DHCP は、[Internet Engineering Task Force](#) ( IETF; インターネット技術特別調査委員会 ) の [Dynamic Host Configuration-Working Group](#) ( DHC-WG ) によって策定されたオープン スタンドアードです。

DHCP はクライアント サーバ パラダイムをベースにしており、DHCP クライアント ( デスクトップコンピュータなど ) は設定パラメータを得るために DHCP サーバに要求を出します。DHCP サーバは、通常、中央に配置されており、ネットワーク管理者によって操作されます。ネットワーク管理者によってサーバが運用されているため、DHCP クライアントには、現在のネットワーク アーキテクチャに固有のパラメータが確実に動的に設定されます。

ほとんどの企業ネットワークは、Virtual LAN ( VLAN; 仮想 LAN ) と呼ばれるサブネットワークに分割された複数のサブネットから構成されており、ルータはサブネットワークの間をルーティングしています。デフォルトでは、ルータはブロードキャストを通過させないため、DHCP リレーエージェント機能を使用して DHCP ブロードキャストを転送するようにルータを設定しない限り、サブネットごとに DHCP サーバが必要となります。

## DHCP について

DHCP は当初 [Requests for Comments \(RFCs\) 1531](#) で定義され、その後 [RFC 2131](#) に置き換えられました。DHCP は、[RFC 951](#) で定義されている Bootstrap Protocol ( BootP; ブートストラップ プロトコル ) に基づいています。

DHCP は、IP アドレス、サブネット マスク、デフォルト ゲートウェイなどの初期設定情報を起動時に取得するために、ワークステーション ( ホスト ) によって使用されます。IP ネットワークで通信するためには、すべてのホストに IP アドレスが必要です。DHCP を使用すれば、各ホストに IP アドレスを手動で設定するという管理上の負担が軽減されます。また、ホストが別の IP サブネットに移動した場合は、それまで使用していたものと異なる IP アドレスを使用しなければなりません。DHCP は、この処理を自動的に実行します。DHCP の場合、ホストは適切な IP サブネット内の IP アドレスを選択できます。

### 現在の DHCP RFC 参照

- RFC 2131 : DHCP
- RFC 2132 - DHCP オプションと BootP ベンダー拡張
- RFC 1534 - DHCP と BootP 間の相互運用性
- RFC 1542 - BootP の明確化と機能拡張
- RFC 2241 - Novell デイレクトリ サービスの DHCP オプション
- RFC 2242 - Netware/IP ドメイン名と情報

• RFC 2489 : Procedure for Defining New DHCP Options

DHCP ではクライアント サーバ モデルが採用されており、1 台以上のサーバ ( DHCP サーバ ) が、クライアントの起動時に、IP アドレスやその他のオプション設定パラメータをクライアント ( ホスト ) に割り当てます。これらの設定パラメータは、サーバからクライアントに一定時間リースされます。ホストが起動する際、ホストの TCP/IP スタックは、各種設定パラメータの中から特に IP アドレスとサブネット マスクを取得するために、ブロードキャスト ( DHCPDISCOVER ) メッセージを送信します。これにより、DHCP サーバとホストの間で交換が開始されます。この交換処理中に、クライアントは、次に示す明確に規定された状態を遷移します。

1. Initializing
2. Selecting
3. Requesting
4. Bound
5. Renewing
6. Rebinding

上記の状態を遷移する際、クライアントとサーバは、次の DHCP メッセージ表に示されたタイプのメッセージを交換します。

## DHCP メッセージ表

参照	メッセージ	使用目的
0 x 0 0 1	DHC PDIS COVER	クライアントが使用可能な DHCP サーバを探しています。
0 x 0 2	DHC POFF FER	サーバがクライアントの DHCPDISCOVER に応答します。
0 x 0 3	DHC PRE QUEST	クライアントは、パケット内の定義に従ってサーバに対してのブロードキャストを行い、特定の 1 台のサーバから提供されたパラメータを要求します。
0 x 0 4	DHC PDECLIN E	クライアントがサーバに、与えられたネットワーク アドレスがすでに使用中であることを伝えます。
0 x 0 5	DHC PACK	サーバがクライアントに、割り当てられたネットワーク アドレスなどの設定パラメータを送信します。
0 x 0 6	DHC PNACK	サーバがクライアントに、設定パラメータの要求を拒否することを伝えます。
0	DHC	クライアントがサーバに、ネットワーク アドレス

X 0 7	PRE LEASE	スを解放し、残りのリースをキャンセルすることを伝えます。
0 X 0 8	DHC PINF ORM	クライアントにアドレスがすでに外部的に設定されている場合に、クライアントがサーバに対してローカル設定パラメータのみを要求します。

## DHCPDISCOVER

クライアントは初めて起動するときに ( Initializing 状態 )、ローカルの物理サブネット上の User Datagram Protocol ( UDP ) ポート 67 ( BootP サーバ ) 宛てに DHCPDISCOVER メッセージを送信します。クライアントは自身が所属するサブネットを知る手段を持たないため、DHCPDISCOVER は、送信元 IP アドレス 0.0.0.0 を使用してすべてのサブネットにブロードキャスト ( 宛先 IP アドレス 255.255.255.255 ) されます。送信元 IP アドレスが 0.0.0.0 であるのは、クライアントに IP アドレスが設定されていないためです。このローカルサブネット上に、適切に設定されて正常に稼働している DHCP サーバがある場合、その DHCP サーバはブロードキャストを受信し、DHCP OFFER メッセージで応答します。ローカルサブネット上に DHCP サーバがない場合は、DHCP サーバがあるサブネットに DHCPDISCOVER メッセージを転送する DHCP/BootP リレー エージェントが、このローカルサブネット上に存在する必要があります。

このリレー エージェントは、専用ホスト ( Microsoft Windows サーバなど ) またはルータ ( インターフェイス レベルで ip helper 文が設定された Cisco ルータなど ) のどちらでもかまいません。

## DHCP OFFER

DHCPDISCOVER メッセージを受信した DHCP サーバは、UDP ポート 68 ( BootP クライアント ) の DHCP OFFER メッセージで応答します。クライアントは DHCP OFFER を受信すると、Selecting 状態に移行します。この DHCP OFFER メッセージには、クライアント用の初期設定情報が含まれています。たとえば、DHCP サーバは、DHCP OFFER メッセージの yiaddr フィールドに、要求された IP アドレスを設定します。サブネット マスクとデフォルト ゲートウェイは、それぞれオプション フィールドの subnet mask と router options に指定されます。DHCP OFFER メッセージに含まれるその他の一般的なオプションには、IP アドレスのリース時間、更新時間、ドメイン ネーム サーバ、NetBIOS ネーム サーバ ( WINS ) などがあります。DHCP サーバは DHCP OFFER をブロードキャスト アドレスに送信しますが、オフアーの chaddr フィールドにクライアントのハードウェア アドレスを設定します。そのため、クライアントはその DHCP OFFER の宛先が自分自身であるかがわかります。DHCP サーバがローカルサブネット上にない場合、DHCP サーバは、DHCPDISCOVER の転送元である DHCP/BootP リレー エージェントに、ユニキャスト パケットとして UDP ポート 67 の DHCP OFFER を送信します。その後、DHCP/BootP リレー エージェントは、Bootp クライアントによって設定されるブロードキャスト フラグに応じて、UDP ポート 68 のローカルサブネットに DHCP OFFER をブロードキャストまたはユニキャストします。

## DHCPREQUEST

クライアントは DHCP OFFER を受信した後、DHCP OFFER のパラメータを受け入れる意向を示すために DHCPREQUEST メッセージで応答し、Requesting 状態に移行します。クライアントが最初に送信した DHCPDISCOVER メッセージを複数の DHCP サーバが受信し、各 DHCP サーバがそれぞれメッセージを返信してきた場合、クライアントは複数の DHCP OFFER メッセージを受信することになります。この場合、クライアントは 1 つの DHCP OFFER を選択してその

DHCP サーバのみに応答し、その他すべての DHCP OFFER メッセージを暗黙的に辞退します。クライアントは、選択したサーバを明確にするために、Server Identifier オプション フィールドに DHCP サーバの IP アドレスを設定します。DHCPREQUEST もブロードキャストされるため、DHCP OFFER を送信した DHCP サーバすべてが DHCPREQUEST を確認し、自身が返答した DHCP OFFER が受け入れられたかどうかを知ることができます。DHCPREQUEST メッセージのオプション フィールドには、クライアントが要求するその他の設定オプションも含まれています。クライアントは IP アドレスをオファーされた場合でも、送信元 IP アドレスに 0.0.0.0 を指定して DHCPREQUEST メッセージを送信します。これは、この時点ではまだクライアントがその IP アドレスを使用してよいという明確な確認を受信していないためです。

## DHCPACK

DHCP サーバは DHCPREQUEST を受信すると、その要求に対して DHCPACK メッセージで確認応答します。これによって初期化プロセスが完了します。DHCPACK メッセージには、送信元アドレスとして DHCP サーバの IP アドレス、宛先アドレスとして再びブロードキャストが指定され、DHCPREQUEST メッセージでクライアントから要求されたすべてのパラメータが含まれています。クライアントは DHCPACK を受信すると Bound 状態に移行し、割り当てられた IP アドレスを自由に使用してネットワーク上で通信できるようになります。一方、DHCP サーバはリース情報をデータベースに格納し、client identifier または chaddr と、対応する IP アドレスを使用してリースを一意に識別します。クライアントとサーバはどちらも、この識別情報の組み合わせを使用してリースを参照します。client identifier は、デバイスの Mac アドレスとメディア タイプです。

DHCP クライアントは、新しいアドレスの使用を開始する前に、リースされたアドレスに関連する時間パラメータ、つまり Lease Time ( LT; リース時間 )、Renewal Time ( T1; 更新時間 )、および Rebind Time ( T2; 再バインド時間 ) を計算します。標準的なデフォルト LT は 72 時間です。必要であれば、一定量のアドレスを維持するために、リース時間を短縮できます。

## DHCPNAK

選択された DHCP サーバは、DHCPREQUEST メッセージの要求に応えられない場合、DHCPNAK メッセージで応答します。クライアントは、DHCPNAK メッセージを受信するか、または DHCPREQUEST メッセージへの応答を受信されないと、Requesting 状態に移行して設定プロセスを再び開始します。クライアントは、60 秒以内に最低 4 回 DHCPREQUEST を再送信しても応答がない場合、Initializing 状態に戻ります。

## DHCPDECLINE

クライアントは DHCPACK を受信すると、オプションでパラメータの最終チェックを実行します。クライアントはこの手順を実行するために、DHCPACK で提供された IP アドレスの Address Resolution Protocol ( ARP ) 要求を送信します。クライアントが ARP 要求への応答を受信し、指定したアドレスが使用中であることが判明した場合、クライアントはサーバに DHCPDECLINE メッセージを送信し、Requesting 状態に移行して設定プロセスを再び開始します。

## DHCPINFORM

クライアントが他の手段によってすでにネットワーク アドレスを取得している場合、または IP アドレスが手動で設定されている場合には、クライアント ワークステーションは、DHCPINFORM 要求メッセージを使用して、ドメイン名や Domain Name Server ( DNS; ドメイン ネーム サーバ ) といったその他のローカル設定パラメータを取得できます。DHCPINFORM メッセージを受信した DHCP サーバは、そのクライアントに応じた適切なローカル設定パラメータ

タで DHCPACK メッセージを構成します。その際、新たに IP アドレスは割り当てません。DHCPACK はユニキャストでクライアントに送信されます。

## DHCPRELEASE

DHCP クライアントは、DHCPRELEASE メッセージを DHCP サーバに送信することで、ネットワークアドレスに関するリースを解放できます。クライアントは DHCPRELEASE メッセージの client identifier フィールドとネットワークアドレスを使用して、解放するリースを識別します。現在の DHCP プール範囲を拡張する必要がある場合は、現在のアドレスプールを削除して、DHCP プールの下で新しい IP アドレスの範囲を指定します。 [特定の IP アドレスまたは DHCP プールに含めるアドレスの範囲を削除するには、ip dhcp excluded-address コマンドを使用します。](#)

注: デバイスで BOOTP が使用されている場合は、ルータの DHCP バインディングで無期限のリースが表示されます。

## [リースの更新](#)

IP アドレスはサーバからリースされているだけなので、ときどきリースを更新する必要があります。リース時間の半分 ( $T1=0.5 \times LT$ ) が経過すると、クライアントはリースの更新を試みます。クライアントは Renewing 状態に移行し、現在のリースの継続を要求する DHCPREQUEST メッセージをサーバに送信します。サーバは、リースの更新を許可する場合、更新要求に対して DHCPACK メッセージで応答します。前のリース時間中にサーバに変更が加えられた場合、DHCPACK メッセージには新しいリースと新しい設定パラメータが含まれます。クライアントがリースを保持しているサーバになんらかの理由で到達できず、時間 T2 以内にその DHCP サーバから更新要求への応答が得られなかった場合は、任意の DHCP サーバからアドレスの更新を試みます。T2 のデフォルト値は ( $7/8 \times LT$ ) です。これは、 $T1 < T2 < LT$  を意味します。

DHCP によって IP アドレスを割り当てられていたクライアントが再起動した場合、そのクライアントは DHCPREQUEST パケットを使用し、以前にリースされていた IP アドレスを明確に要求します。この DHCPREQUEST には、送信元 IP アドレスとして 0.0.0.0、宛先 IP アドレスとしてブロードキャストアドレス 255.255.255.255 が含まれています。

リポート時に DHCPREQUEST を送信するクライアントは、server identifier フィールドに値を設定する必要はありませんが、その代わりに IP address オプション フィールドに要求する IP アドレスを設定する必要があります。RFC に厳密に準拠したクライアントでは、DHCP オプション フィールドではなく、ciaddr フィールドに要求するアドレスが設定されます。DHCP サーバはどちらの方法にも対応します。DHCP サーバの動作は、多数のファクタに基づいて決まります。たとえば Windows NT DHCP サーバでは、使用されているオペレーティングシステムバージョンなどのファクタがあり、その他にもスコープなどのファクタが関係します。DHCP サーバは、クライアントから要求された IP アドレスがまだ使用できると判断した場合、DHCPREQUEST に対して何も応答しないか、または DHCPACK を送信します。クライアントから要求された IP アドレスが使用できないと判断した場合は、クライアントに DHCPNACK を返信します。この場合、クライアントは Initializing 状態に移行し、DHCPDISCOVER メッセージを送信します。

注: DHCP サーバは、IP アドレスのプールの一番下にある IP アドレスを、DHCP クライアントに割り当てます。一番下のアドレスは、そのリースが期限切れになった場合、要求されると、別のクライアントに割り当てられます。DHCP アドレスが割り当てられる順序を変更することはできません。

## [DHCP パケット](#)

DHCP メッセージは可変長で、次の表に示すフィールドから構成されています。

注: このパケットは、オリジナルの BootP パケットの修正バージョンです。

フィールド	バイト	名前	説明
op	1	OpCode	パケットが要求と応答のいずれであることを識別します ( 1=BOOTREQUEST、 2=BOOTREPLY )。
htype	1	ハードウェアタイプ	ネットワーク ハードウェア アドレスのタイプを指定します。
hlen	1	ハードウェア長	ハードウェア アドレス長を指定します。
ホップ	1	ホップ	クライアントが 0 を設定し、要求がルータを経由して転送されるたびに値がインクリメントされます。
xid	4	トランザクション ID	クライアントによって選択されたランダムな数字。特定の DHCP トランザクションで交換される DHCP メッセージにはすべて同じ ID ( xid ) が設定されます。
secs	2	秒	DHCP プロセスが始まってから経過した秒数を指定します。
フラグ	2	フラグ	メッセージがブロードキャストとユニキャストのいずれであることを指定します。
ciaddr	4	クライアント IP アドレス	Bound、Renew、または Rebinding 状態の場合のように、クライアントが自身の IP アドレスを知っているときのみ使用されます。
yiaddr	4	相手先 IP アドレス	クライアント IP アドレスが 0.0.0.0 の場合、DHCP サーバはオファーされたクライアント IP アドレスをこのフィールドに設定します。
siaddr	4	サーバ IP アドレス	クライアントが DHCP サーバの IP アドレスを知っている場合は、このフィールドに DHCP サーバのアドレスが設定されます。それ以外では、DHCP サーバからの DHCPOFFER および DHCPACK で使用されます。
giaddr	4	ルータ IP アドレス ( GI	ゲートウェイ IP アドレス。 DHCP/BootP リレー エージェントによって設定されます。



		ADDR )	
chaddr	16	クライアント MAC アドレス	DHCP クライアントの MAC アドレス。
sname	64	サーバ名	オプションのサーバホスト名。
file	128	ブートファイル名	ブートファイル名。
options	variable	オプションパラメータ	DHCP サーバが提供できるオプションのパラメータ。RFC 2132 に、使用可能なすべてのオプションが記載されています。

## DHCP サーバと同じサブネットにあるクライアントが DHCP アドレスを取得する場合のクライアントサーバ間のやり取り

パケット	送信元 MAC アドレス	宛先 MAC アドレス	送信元 IP アドレス	宛先 IP アドレス
DHCPDISCOVER	クライアント	ブロードキャスト	0.0.0.0	255.255.255.255
DHCPOFFER	DHCP サーバ	ブロードキャスト	DHCP サーバ	255.255.255.255
DHCPREQUEST	クライアント	ブロードキャスト	0.0.0.0	255.255.255.255
DHCPACK	DHCP サーバ	ブロードキャスト	DHCP サーバ	255.255.255.255

## DHCP/BootP リレー エージェントの役割

デフォルトでは、ルータはブロードキャスト パケットを転送しません。DHCP クライアントメッセージは宛先 IP アドレスとして 255.255.255.255 (全ネットワークへのブロードキャスト) を使用するため、ルータに DHCP/BootP リレー エージェントが設定されていない限り、DHCP クライアントの要求をサブネットが異なる DHCP サーバに送信できません。DHCP/BootP リレー エージェントは、DHCP クライアントの代わりに DHCP サーバに DHCP 要求を転送します。DHCP/BootP リレー エージェントは、DHCP サーバに転送する DHCP フレームの送信元 IP アドレスの最後に自身の IP アドレスを付加します。これにより、DHCP サーバは DHCP/BootP リレー エージェントにユニキャストで応答できます。また、DHCP/BootP リレー エージェントは、ゲートウェイ IP アドレス フィールドに、クライアントからの DHCP メッセージを受信したインターフェイスの IP アドレスを設定します。DHCP サーバでは、ゲートウェイ ip address フィールドを使用して、DHCPDISCOVER、DHCPREQUEST、または DHCPINFORM メッセージの送信元のサブネットを特定します。

# Cisco IOS ルータでの DHCP/BootP リレー エージェント機能の設定

BootP または DHCP 要求を転送するための Cisco ルータの設定は簡単で、IP ヘルパー アドレスを、DHCP/BootP サーバ、またはサーバが存在するネットワークのサブネット ブロードキャスト アドレスを指すように設定するだけです。たとえば、次のようなネットワーク ダイアグラムについて考えてみます。

[クライアントから DHCP サーバに BootP/DHCP 要求を転送するには、ip helper-address interface コマンドを使用します。](#) IP ヘルパー アドレスは、UDP ポート番号に基づいて任意の UDP ブロードキャストを転送するように設定できます。デフォルトでは、IP ヘルパー アドレスは次の UDP ブロードキャストを転送します。

- Trivial File Transfer Protocol ( TFTP ) ( ポート 69 )
- DNA ( ポート 53 )、時刻サービス ( ポート 37 )
- NetBIOS ネーム サーバ ( ポート 137 )
- NetBIOS データグラム サーバ ( ポート 138 )
- Boot Protocol ( DHCP/BootP ) クライアントおよびサーバのデータグラム ( ポート 67 と 68 )
- Terminal Access Control Access Control System ( TACACS ) サービス ( ポート 49 )
- IEN-116 ネーム サーバ ( ポート 42 )

IP ヘルパー アドレスは、UDP ブロードキャストをユニキャストまたはブロードキャスト IP アドレスに直接送信できます。ただし、IP ヘルパー アドレスを使用して、UDP ブロードキャストをあるサブネットから別のサブネットのブロードキャスト アドレスに転送することは推奨できません。これを行うと、大量のブロードキャスト フラッディングが発生するおそれがあるためです。次の例のように、1つのインターフェイスに対して IP ヘルパー アドレスのエントリを複数設定することもできます。

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname router  
!  
!  
!  
interface Ethernet0  
ip address 192.168.2.1 255.255.255.0  
no ip directed-broadcast  
!  
interface Ethernet1  
ip address 192.168.1.1 255.255.255.0  
ip helper-address 192.168.2.2  
ip helper-address 192.168.2.3  
!--- IP helper-address pointing to DHCP server no ip  
directed-broadcast !!! line con 0 exec-timeout 0 0  
transport input none line aux 0 line vty 0 4 login ! end
```

Cisco ルータは、DHCP リレー エージェントとして設定された DHCP サーバのロード バランシングをサポートしていません。Cisco ルータは、そのインターフェイスに関して言及されているすべてのヘルパー アドレスに、DHCPDISCOVER メッセージを転送します。サブネットをサポートするために複数の DHCP サーバを使用すると、DHCPDISCOVER、DHCP OFFER および

DHCPREQUEST/DHCPDECLINE メッセージが DHCP クライアントとサーバの各ペアの間で交換されるため、DHCP トラフィックが増加します。

## 手動バインディングの設定

手動バインディングを設定する方法は 2 つあり、一方は Windows ホスト用、他方は非 Windows ホスト用です。設定に使用するコマンドは 2 つあり、1 つは Microsoft DHCP クライアントのためであり、他は Microsoft 以外 DHCP のクライアントのためです: [DHCP client-identifier](#) (手動バインディング- Microsoft DHCP クライアント) および [DHCP ハードウェア アドレス](#) (手動バインディング- Microsoft 以外 DHCP のクライアント)。コマンドが 2 つある理由は、Windows が稼働する PC ではその MAC アドレスが変更され、MAC アドレスの先頭に 01 が付加されるからです。設定例を次に示します。

- 次の設定は、Microsoft DHCP クライアント用です。configuration terminal  
`ip dhcp pool new_pool host ip_address subnet_mask client-identifier 01XXXXXXXXXXXX !---  
xxxxxx represents 48 bit MAC address prepended with 01`
- 次の設定は、非 Microsoft DHCP クライアント用です。configuration terminal  
`ip dhcp pool new_pool host ip_address subnet_mask hardware-address XXXXXXXXXXXX !--- xxxxxx  
represents 48 bit MAC address`

## セカンダリ IP セグメントで DHCP を稼働させる方法

DHCP にはデフォルト時、プライマリ IP アドレスを使用して設定されたインターフェイスから要求を受信した場合のみ、応答パケットが送信されるという制限があります。DHCP トラフィックでは、ブロードキャスト アドレスが使用されます。ルータ インターフェイスは、DHCP 要求を受信すると、その DHCP 要求とともに、該当インターフェイス上で設定されているプライマリ IP の送信元アドレスを DHCP サーバに転送 (IP ヘルパー アドレスが設定されている場合) し、DHCP 応答パケット内で (クライアントのために) 使用すべき IP プールを DHCP サーバに教えます。

インターフェイス上で設定されているセカンダリ IP ネットワーク上のデバイスから DHCP ブロードキャスト要求が来るのか否かをルータが判断する方法はありません。回避策として、サブインターフェイスの設定 (ルータに接続されているデバイスが dot1q タギングをサポートしている場合) により 2 つのサブネットを分割し、両者が対応する IP アドレスを正しく取得できるようにします。

[セカンダリ アドレスの方が望ましい場合は、グローバル設定コマンド ip dhcp smart-relay を有効にするという回避策もあります。](#) ただし、その場合は、プライマリ アドレス プールに対する要求が 3 回連続してあった後、DHCP サーバから応答がないとき、DHCP 要求のリレーにセカンダリ IP しか使用されないという制限があります。

## DHCP リレー機能を使用した DHCP クライアント サーバ間のやり取り

次の表は、DHCP クライアントが DHCP サーバから IP アドレスを取得するプロセスを示しています。この表は、上記の[ネットワーク ダイアグラム](#)に基づいています。ダイアグラム上の数値は、下表で説明されているパケットを表します。この表は、DHCP クライアント サーバ間のやり取りにおけるパケット フローを理解するためのリファレンス ポイントです。また、DHCP の問題発生箇所を特定する上でも役立ちます。

パケット	ク ラ イ	サ ー バ	GI ア ド	パケ ット の送	パケ ット の送	パケット の宛先 MAC ア	パケ ット の宛
------	-------------	-------------	--------------	----------------	----------------	----------------------	----------------

	ア ン ト IP ア ド レ ス	IP ア ド レ ス	レ ス	信 元 MAC ア ド レ ス	信 元 IP ア ド レ ス	ド レ ス	先 IP ア ド レ ス
1. DHCPDISCOVER がクライアントから送信されます。	0.0 .0. 0	0. 0. 0. 0	0. 0. 0. 0	0005 .DC C9. C64 0	0.0.0 .0	ffff.ffff.ffff (broadcast)	255. 255. 255. 255
2. ルータの E1 インターフェイスで DHCPDISCOVER が受信されます。ルータはこのパケットが DHCP UDP ブロードキャストであると認識します。ここからルータは DHCP/BootP リレーエージェントとして動作します。ゲートウェイ IP アドレスフィールドに着信インターフェイスの IP アドレスを設定し、送信元 IP アドレスを着信インターフェイスの IP アドレスに変更して、要求を DHCP サーバに直接転送します。	0.0 .0. 0	0. 0. 0. 0	19 2. 16 8. 1. 1	イン ター フェ イス E2 の MAC ア ド レ ス	192. 168. 1.1	DHCP サーバの MAC ア ドレス	192. 168. 2.2
3. DHCP サーバは DHCPDISCOVER を受信し、DHCP リレーエージェントに対して	19 2.1 68. 1.2	19 2. 16 8. 2. 2	19 2. 16 8. 1. 1	DHC P サ ーバ の MAC ア ド レ ス	192. 168. 2.2	インター フェイス E2 の MAC ア ドレス	192. 168. 1.1

DHCPOFFER を送信します 。							
4. DHCP リレ ーエージェント は DHCPOFFER を受信し、 DHCPOFFER ブロードキャ ストをローカ ル LAN に転送 します。	19 2.1 68. 1.2	19 2. 16 8. 2. 2	19 2. 16 8. 1. 1	イン ター フェ イス E1 の MAC アド レス	192. 168. 1.1	ffff.ffff.ffff (ブロー ドキャス ト)	255. 255. 255. 255
5. DHCPREQUE ST がクライ アントから送 信されます。	0.0 .0. 0	0. 0. 0. 0	0. 0. 0. 0	0005 .DC C9. C64 0	0.0.0 .0	ffff.ffff.ffff (broadca st)	255. 255. 255. 255
6. ルータの E1 インターフ ェイスで DHCPREQUE ST が受信さ れます。ルー タはこのパケ ットが DHCP UDP ブロード キャストであ ると認識しま す。ここから ルータは DHCP リレ ーエージェント として動作し ます。ゲート ウェイ IP アド レスフィールド に着信イン ターフェイス の IP アドレス を設定し、送 信元 IP アドレ スを着信イン ターフェイス の IP アドレス に変更して、 要求を DHCP サーバに直接 転送します。	0.0 .0. 0	0. 0. 0. 0	19 2. 16 8. 1. 1	イン ター フェ イス E2 の MAC アド レス	192. 168. 1.1	DHCP サ ーバの MAC ア ドレス	192. 168. 2.2
7. DHCP サー バは DHCPREQUE	19 2.1 68.	19 2. 16	19 2. 16	DHC P サ ーバ	192. 168. 2.2	インター フェイス E2 の	192. 168. 1.1

ST を受信し、DHCP/BootP リレー エージェントに対して DHCPACK を送信します。	1.2	8.2.2	8.1.1	の MAC アドレス		MAC アドレス	
8. DHCP/BootP リレー エージェントは DHCPACK を受信し、DHCPACK ブロードキャストをローカル LAN に転送します。クライアントは ACK を受け入れて、クライアント IP アドレスを使用します。	192.168.1.2	192.168.8.2	192.168.8.1	インターフェイス E1 の MAC アドレス	192.168.1.1	ffff.ffff.ffff (ブロードキャスト)	255.255.255.255

## Pre-Execution Environment ( PXE ) ブートアップ DHCP の注意事項

Pre-Execution Environment ( PXE ) を使用すると、ローカル ハード ドライブでオペレーティング システムをブートする前に、ネットワーク上でサーバからワークステーションをブートすることができます。ネットワーク管理者は、特定のワークステーションがある実際の場所まで出向いて、手動でワークステーションをブートする必要がなくなります。オペレーティング システムや診断プログラムなどのソフトウェアを、ネットワーク経由でサーバからデバイスにロードできます。PXE 環境では DHCP を使用してその IP アドレスを設定します。

DHCP サーバがネットワークの別のルーティング セグメントに存在する場合は、ルータで DHCP/BootP リレー エージェントの設定を行う必要があります。[ローカル ルータ インターフェイスでは、ip helper address コマンドを設定する必要があります。](#) 設定の詳細は、このドキュメントの「[Cisco IOS ルータでの DHCP/BootP リレー エージェント機能の設定](#)」のセクションを参照してください。

## スニファトレースを使用した DHCP の理解とトラブルシューティング

### 同一の LAN セグメントにある DHCP クライアントとサーバのスニファトレースの解説

次のスニファトレースは 6 つのフレームから構成されています。これら 6 つのフレームは、

DHCP クライアントおよびサーバが同じ物理セグメントまたは論理セグメントに存在する場合の、DHCP の動作シナリオを示しています。DHCP のトラブルシューティングを行うときは、取得したスニフトレースを次のトレースと照合してください。次のトレースと一部異なる点があるかもしれませんが、一般的なパケット フローはほぼ同じです。パケットトレースは、DHCP の動作の仕組みに関する前述の説明に従います。

```
----- 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: Source port = 68 (BootPc/DHCP) UDP: Destination port = 67
(BootPs/DHCP) UDP: Length = 584 UDP: No checksum UDP: [576 byte(s) of data] UDP: DHCP: -----
DHCP Header ----- DHCP: DHCP: Boot record type = 1 (Request) DHCP: Hardware address type = 1
(10Mb Ethernet) DHCP: Hardware address length = 6 bytes DHCP: DHCP: Hops = 0 DHCP: Transaction
id = 00000882 DHCP: Elapsed boot time = 0 seconds DHCP: Flags = 8000 DHCP: 1... .... = Broadcast
IP datagrams DHCP: Client self-assigned IP address = [0.0.0.0] DHCP: Client IP address
= [0.0.0.0] DHCP: Next Server to use in bootstrap = [0.0.0.0] DHCP: Relay Agent = [0.0.0.0]
DHCP: Client hardware address = 0005DCC9C640 DHCP: DHCP: Host name = "" DHCP: Boot file name =
"" DHCP: DHCP: Vendor Information tag = 63825363 DHCP: Message Type = 1 (DHCP Discover) DHCP:
Maximum message size = 1152 DHCP: Client identifier =
00636973636F2D303030352E646363392E633634302D564C31 DHCP: Parameter Request List: 7 entries DHCP:
1 = Client's subnet mask DHCP: 66 = TFTP Option DHCP: 6 = Domain name server DHCP: 3 = Routers
on the client's subnet DHCP: 67 = Boot File Option DHCP: 12 = Host name server DHCP: 150 =
Unknown Option DHCP: Class identifier = 646F63736973312E30 DHCP: Option overload =3 (File and
Sname fields hold options) DHCP: ----- Frame 2 - DHCP OFFER -----
----- Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2[192.168.1.1] [255.255.255.255] 331 0:01:26.825 0.015.172
05/07/2001 11:52:03 AM DHCP: Reply, Message type: DHCP Offer DLC: ----- DLC Header ----- DLC:
DLC: Frame 2 arrived at 11:52:03.8258; frame size is 331 (014B hex) bytes. DLC: Destination =
BROADCAST FFFFFFFF, Broadcast DLC: Source = Station 0005DCC42484 DLC: Ethertype = 0800 (IP)
DLC: IP: ----- IP Header ----- IP: IP: Version = 4, header length = 20 bytes IP: Type of service
= 00 IP: 000. .... = routine IP: ...0 .... = normal delay IP: .... 0... = normal throughput IP:
.... .0.. = normal reliability IP: .... ..0. = ECT bit - transport protocol will ignore the CE
bit IP: .... ..0 = CE bit - no congestion IP: Total length = 317 bytes IP: Identification = 5
IP: Flags = 0X IP: .0.. .... = may fragment IP: ..0. .... = last fragment IP: Fragment offset =
0 bytes IP: Time to live = 255 seconds/hops IP: Protocol = 17 (UDP) IP: Header checksum = F901
(correct) IP: Source address = [192.168.1.1] IP: Destination address = [255.255.255.255] IP: No
options IP: UDP: ----- UDP Header ----- UDP: Source port = 67 (BootPs/DHCP)
Destination port = 68 (BootPc/DHCP) UDP: Length = 297 UDP: No checksum UDP: [289 byte(s) of
data] UDP: DHCP: ----- DHCP Header ----- DHCP: DHCP: Boot record type = 2 (Reply) DHCP: Hardware
address type = 1 (10Mb Ethernet) DHCP: Hardware address length = 6 bytes DHCP: DHCP: Hops = 0
DHCP: Transaction id = 00000882 DHCP: Elapsed boot time = 0 seconds DHCP: Flags = 8000 DHCP:
1... .... = Broadcast IP datagrams DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2] DHCP: Next Server to use in bootstrap = [0.0.0.0] DHCP:
Relay Agent = [0.0.0.0] DHCP: Client hardware address = 0005DCC9C640 DHCP: DHCP: Host name = ""
DHCP: Boot file name = "" DHCP: DHCP: Vendor Information tag = 63825363 DHCP: Message Type = 2
(DHCP Offer) DHCP: Server IP address = [192.168.1.1] DHCP: Request IP address lease time = 85535
(seconds) DHCP: Address Renewel interval = 42767 (seconds) DHCP: Address Rebinding interval =
74843 (seconds) DHCP: Subnet mask = [255.255.255.0] DHCP: Domain Name Server address =
[192.168.1.3] DHCP: Domain Name Server address = [192.168.1.4] DHCP: Gateway address =
[192.168.1.1] DHCP: ----- Frame 3 - DHCPREQUEST -----
----- Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3[0.0.0.0] [255.255.255.255] 618 0:01:26.829 0.003.586 05/07/2001 11:52:03 AM DHCP:
```

Request, Message type: **DHCP Request** DLC: ----- DLC Header ----- DLC: DLC: Frame 56 arrived at 11:52:03.8294; frame size is 618 (026A hex) bytes. DLC: **Destination = BROADCAST 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 Renewel interval = 43200 (seconds) DHCP: Address Rebinding interval = 75600 (seconds) DHCP: Subnet mask = [255.255.255.0] DHCP: **Domain Name Server address = [192.168.1.3]** DHCP: **Domain Name Server address = [192.168.1.4]** DHCP: **Gateway address = [192.168.1.1]** DHCP: - - - - - **Frame 5 - ARP** - - - - - Frame  
Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary 5 0005DCC9C640 Broadcast 60 0:01:26.846 0.002.954 05/07/2001 11:52:03 AM ARP: R PA=[192.168.1.2] HA=0005DCC9C640 PRO=IP DLC: ----- DLC Header ----- DLC: DLC: Frame 58 arrived at 11:52:03.8470; frame size is 60 (003C hex) bytes. DLC: Destination = BROADCAST 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:

## [DHCP リレー エージェントとして設定されているルータによって分けられた DHCP クライアントとサーバのスニファトレースの解説](#)

### Sniffer B のトレース

```
----- Frame 1 - DHCPDISCOVER -----  
- - - Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary 1  
[0.0.0.0] [255.255.255.255] 618 0:02:05.759 0.025.369 05/31/2001 06:53:04 AM DHCP: Request,  
Message type: DHCP Discover DLC: ----- DLC Header ----- DLC: DLC: Frame 124 arrived at  
06:53:04.2043; frame size is 618 (026A hex) bytes. DLC: Destination = BROADCAST FFFFFFFF,  
Broadcast DLC: Source = Station 0005DCF2C441 DLC: Ethertype = 0800 (IP) DLC: IP: ----- IP Header  
----- IP: IP: Version = 4, header length = 20 bytes IP: Type of service = 00 IP: 000. .... =  
routine IP: ...0 .... = normal delay IP: .... 0... = normal throughput IP: .... .0.. = normal  
reliability IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit IP: .... ..0 =  
CE bit - no congestion IP: Total length = 604 bytes IP: Identification = 183 IP: Flags = 0X IP:  
.0.. .... = may fragment IP: ..0. .... = last fragment IP: Fragment offset = 0 bytes IP: Time to  
live = 255 seconds/hops IP: Protocol = 17 (UDP) IP: Header checksum = B8DA (correct) IP: Source  
address = [0.0.0.0] IP: Destination address = [255.255.255.255] IP: No options IP: UDP: -----  
UDP Header ----- UDP: UDP: Source port = 68 (BootPc/DHCP) UDP: Destination port = 67  
(BootPs/DHCP) UDP: Length = 584 UDP: No checksum UDP: [576 byte(s) of data] UDP: DHCP: -----  
DHCP Header ----- DHCP: DHCP: Boot record type = 1 (Request) DHCP: Hardware address type = 1  
(10Mb Ethernet) DHCP: Hardware address length = 6 bytes DHCP: DHCP: Hops = 0 DHCP: Transaction  
id = 00001425 DHCP: Elapsed boot time = 0 seconds DHCP: Flags = 8000 DHCP: 1... .... = Broadcast IP datagrams  
DHCP: Client self-assigned IP address = [0.0.0.0] DHCP: Client IP address  
= [0.0.0.0] DHCP: Next Server to use in bootstrap = [0.0.0.0] DHCP: Relay Agent = [0.0.0.0]  
DHCP: Client hardware address = 0005DCF2C441 DHCP: DHCP: Host name = "" DHCP: Boot file name =  
"" DHCP: DHCP: Vendor Information tag = 63825363 DHCP: Message Type = 1 (DHCP Discover) DHCP:  
Maximum message size = 1152 DHCP: Client identifier =  
00636973636F2D303065302E316566322E633434312D4574302F30 DHCP: Parameter Request List: 7 entries  
DHCP: 1 = Client's subnet mask DHCP: 6 = Domain name server DHCP: 15 = Domain name DHCP: 44 =  
NetBIOS over TCP/IP name server DHCP: 3 = Routers on the client's subnet DHCP: 33 = Static route  
DHCP: 150 = Unknown Option DHCP: Class identifier = 646F63736973312E30 DHCP: Option overload =3  
(File and Sname fields hold options) DHCP: - - - - - Frame 2 -  
DHCPOFFER - - - - - Frame Status Source Address Dest. Address Size  
Rel. Time Delta Time Abs. Time Summaryr 125 [192.168.1.1] [255.255.255.255] 347 0:02:05.772  
0.012.764 05/31/2001 06:53:04 AM DHCP: Reply, Message type: DHCP Offer DLC: ----- DLC Header ---  
-- DLC: DLC: Frame 125 arrived at 06:53:04.2171; frame size is 347 (015B hex) bytes. DLC:  
Destination = BROADCAST 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 Renewel interval = 49735 (seconds) DHCP: Address Rebinding interval = 87037 (seconds) DHCP: Subnet mask = [255.255.255.0] DHCP: Domain Name Server address = [192.168.10.1] DHCP: Domain Name Server address = [192.168.10.2] DHCP: NetBIOS Server address = [192.168.10.1] DHCP: NetBIOS Server address = [192.168.10.3] DHCP: Domain name = "cisco.com" DHCP: - - - - -

- - - **Frame 3 - DHCPREQUEST** - - - - - Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary 3 [0.0.0.0] [255.255.255.255] 618 0:02:05.774 0.002.185 05/31/2001 06:53:04 AM DHCP: Request, Message type: **DHCP Request** DLC: ----  
- DLC Header ----- DLC: DLC: Frame 126 arrived at 06:53:04.2193; frame size is 618 (026A hex) bytes. DLC: **Destination = BROADCAST 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 Renewel interval = 86400 (seconds) DHCP: Address Rebinding interval = 151200 (seconds) DHCP: Subnet mask = [255.255.255.0] DHCP: Domain Name Server address = [192.168.10.1] DHCP: Domain Name Server address = [192.168.10.2] DHCP: NetBIOS Server address = [192.168.10.1] DHCP: NetBIOS Server address = [192.168.10.3] DHCP: Domain name = "cisco.com" DHCP: - - - - -

- - - **Frame 5 - ARP** - - - - - Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary 5 Cisc14F2C441

```

Broadcast 60 0:02:05.798 0.011.763 05/31/2001 06:53:04 AM ARP: R PA=[192.168.1.2]
HA=Cisc14F2C441 PRO=IP DLC: ----- DLC Header ----- DLC: DLC: Frame 128 arrived at 06:53:04.2439;
frame size is 60 (003C hex) bytes. DLC: Destination = BROADCAST 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:

```

## Sniffer A のトレース

```

- - - - - Frame 1 - DHCPDISCOVER - - - - -
- - - Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary 118
[192.168.1.1] [192.168.2.2] 618 0:00:51.212 0.489.912 05/31/2001 07:02:54 AM DHCP: Request,
Message type: DHCP Discover DLC: ----- DLC Header ----- DLC: DLC: Frame 118 arrived at
07:02:54.7463; frame size is 618 (026A hex) bytes. DLC: Destination = Station 0005DC0BF2F4 DLC:
Source = Station 003094248F72 DLC: Ethertype = 0800 (IP) DLC: IP: ----- IP Header ----- IP: IP:
Version = 4, header length = 20 bytes IP: Type of service = 00 IP: 000. .... = routine IP: ...0
.... = normal delay IP: .... 0... = normal throughput IP: .... .0.. = normal reliability IP:
.... ..0. = ECT bit - transport protocol will ignore the CE bit IP: .... ...0 = CE bit - no
congestion IP: Total length = 604 bytes IP: Identification = 52 IP: Flags = 0X IP: .0.. .... =
may fragment IP: ..0. .... = last fragment IP: Fragment offset = 0 bytes IP: Time to live = 255
seconds/hops IP: Protocol = 17 (UDP) IP: Header checksum = 3509 (correct) IP: Source address =
[192.168.1.1] IP: Destination address = [192.168.2.2] IP: No options IP: UDP: ----- UDP Header -
---- UDP: UDP: Source port = 67 (BootPs/DHCP) UDP: Destination port = 67 (BootPs/DHCP) UDP:
Length = 584 UDP: Checksum = 0A19 (correct) UDP: [576 byte(s) of data] UDP: DHCP: ----- DHCP
Header ----- DHCP: DHCP: Boot record type = 1 (Request) DHCP: Hardware address type = 1 (10Mb
Ethernet) DHCP: Hardware address length = 6 bytes DHCP: DHCP: Hops = 1 DHCP: Transaction id =
000005F4 DHCP: Elapsed boot time = 0 seconds DHCP: Flags = 8000 DHCP: 1... .... .... =
Broadcast IP datagrams DHCP: Client self-assigned IP address = [0.0.0.0] DHCP: Client IP address
= [0.0.0.0] DHCP: Next Server to use in bootstrap = [0.0.0.0] DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441 DHCP: DHCP: Host name = "" DHCP: Boot file name =
"" DHCP: DHCP: Vendor Information tag = 63825363 DHCP: Message Type = 1 (DHCP Discover) DHCP:
Maximum message size = 1152 DHCP: Client identifier =
00636973636F2D303065302E316566322E633434312D4574302F30 DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask DHCP: 6 = Domain name server DHCP: 15 = Domain name DHCP: 44 =
NetBIOS over TCP/IP name server DHCP: 3 = Routers on the client's subnet DHCP: 33 = Static route
DHCP: 150 = Unknown Option DHCP: Class identifier = 646F63736973312E30 DHCP: Option overload =3
(File and Sname fields hold options) DHCP: - - - - - Frame 2 -
DHCPOFFER - - - - -
- - - Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary 2 [192.168.2.2] [192.168.1.1] 347 0:00:51.214 0.002.133
05/31/2001 07:02:54 AM DHCP: Request, Message type: DHCP Offer DLC: ----- DLC Header ----- DLC:
DLC: Frame 119 arrived at 07:02:54.7485; frame size is 347 (015B hex) bytes. DLC: Destination =
Station 003094248F72 DLC: Source = Station 0005DC0BF2F4 DLC: Ethertype = 0800 (IP) DLC: IP: ----
- IP Header ----- IP: IP: Version = 4, header length = 20 bytes IP: Type of service = 00 IP:
000. .... = routine IP: ...0 .... = normal delay IP: .... 0... = normal throughput IP: .... .0..
= normal reliability IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit IP:
.... ...0 = CE bit - no congestion IP: Total length = 333 bytes IP: Identification = 41 IP:
Flags = 0X IP: .0.. .... = may fragment IP: ..0. .... = last fragment IP: Fragment offset = 0
bytes IP: Time to live = 255 seconds/hops IP: Protocol = 17 (UDP) IP: Header checksum = 3623
(correct) IP: Source address = [192.168.2.2] IP: Destination address = [192.168.1.1] IP: No
options IP: UDP: ----- UDP Header ----- UDP: UDP: Source port = 67 (BootPs/DHCP) UDP:
Destination port = 67 (BootPs/DHCP) UDP: Length = 313 UDP: Checksum = A1F8 (correct) UDP: [305

```

byte(s) of data] UDP: DHCP: ----- DHCP Header ----- DHCP: DHCP: Boot record type = 2 (Request)  
DHCP: Hardware address type = 1 (10Mb Ethernet) DHCP: Hardware address length = 6 bytes DHCP:  
DHCP: Hops = 0 DHCP: Transaction id = 000005F4 DHCP: Elapsed boot time = 0 seconds DHCP: Flags =  
8000 DHCP: 1... .. = Broadcast IP datagrams DHCP: Client self-assigned IP address =  
[0.0.0.0] DHCP: Client IP address = [192.168.1.2] DHCP: Next Server to use in bootstrap =  
[0.0.0.0] **DHCP: Relay Agent = [192.168.1.1] DHCP: Client hardware address = 0005DCF2C441** DHCP:  
DHCP: Host name = "" DHCP: Boot file name = "" DHCP: DHCP: Vendor Information tag = 63825363  
DHCP: Message Type = 2 (DHCP Offer) DHCP: Server IP address = [192.168.2.2] DHCP: Request IP  
address lease time = 172571 (seconds) DHCP: Address Renewel interval = 86285 (seconds) DHCP:  
Address Rebinding interval = 150999 (seconds) DHCP: Subnet mask = [255.255.255.0] DHCP: **Domain  
Name Server address = [192.168.10.1] DHCP: Domain Name Server address = [192.168.10.2] DHCP:  
NetBIOS Server address = [192.168.10.1] DHCP: NetBIOS Server address = [192.168.10.3] DHCP:  
Domain name = "cisco.com"** DHCP: - - - - - **Frame 3 - DHCPREQUEST** -  
- - - - - Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary 3 [192.168.1.1] [192.168.2.2] 618 0:00:51.240 0.025.974 05/31/2001  
07:02:54 AM DHCP: Request, Message type: DHCP Request DLC: ----- DLC Header ----- DLC: DLC:  
Frame 120 arrived at 07:02:54.7745; frame size is 618 (026A hex) bytes. DLC: **Destination =  
Station 0005DC0BF2F4** DLC: **Source = Station 003094248F72** DLC: Ethertype = 0800 (IP) DLC: IP: ----  
- IP Header ----- IP: IP: Version = 4, header length = 20 bytes IP: Type of service = 00 IP:  
000. .... = routine IP: ...0 .... = normal delay IP: .... 0... = normal throughput IP: .... .0..  
= normal reliability IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit IP:  
.... ..0 = CE bit - no congestion IP: Total length = 604 bytes IP: Identification = 54 IP:  
Flags = 0X IP: .0.. .... = may fragment IP: ..0. .... = last fragment IP: Fragment offset = 0  
bytes IP: Time to live = 255 seconds/hops IP: Protocol = 17 (UDP) IP: Header checksum = 3507  
(correct) IP: **Source address = [192.168.1.1] IP: Destination address = [192.168.2.2]** IP: No  
options IP: UDP: ----- UDP Header ----- UDP: UDP: **Source port = 67 (BootPs/DHCP) UDP:  
Destination port = 67 (BootPs/DHCP)** UDP: Length = 584 UDP: Checksum = 4699 (correct) UDP: [576  
byte(s) of data] UDP: DHCP: ----- DHCP Header ----- DHCP: DHCP: Boot record type = 1 (Request)  
DHCP: Hardware address type = 1 (10Mb Ethernet) DHCP: Hardware address length = 6 bytes DHCP:  
DHCP: Hops = 1 DHCP: Transaction id = 000005F4 DHCP: Elapsed boot time = 0 seconds DHCP: Flags =  
8000 DHCP: 1... .. = Broadcast IP datagrams DHCP: Client self-assigned IP address =  
[0.0.0.0] DHCP: Client IP address = [0.0.0.0] DHCP: Next Server to use in bootstrap = [0.0.0.0]  
DHCP: **Relay Agent = [192.168.1.1] DHCP: Client hardware address = 0005DCF2C441** DHCP: DHCP: Host  
name = "" DHCP: Boot file name = "" DHCP: DHCP: Vendor Information tag = 63825363 DHCP: Message  
Type = 3 (DHCP Request) DHCP: Maximum message size = 1152 DHCP: **Client identifier =  
00636973636F2D303065302E316566322E633434312D4574302F30** DHCP: Server IP address = [192.168.2.2]  
DHCP: Request specific IP address = [192.168.1.2] DHCP: Request IP address lease time = 172571  
(seconds) DHCP: Parameter Request List: 7 entries DHCP: 1 = Client's subnet mask DHCP: 6 =  
Domain name server DHCP: 15 = Domain name DHCP: 44 = NetBIOS over TCP/IP name server DHCP: 3 =  
Routers on the client's subnet DHCP: 33 = Static route DHCP: 150 = Unknown Option DHCP: Class  
identifier = 646F63736973312E30 DHCP: Option overload =3 (File and Sname fields hold options)  
DHCP: - - - - - **Frame 4 - DHCPACK** - - - - -  
- - - - - Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary 4  
[192.168.2.2] [192.168.1.1] 347 0:00:51.240 0.000.153 05/31/2001 07:02:54 AM DHCP: Request,  
Message type: **DHCP Ack** DLC: ----- DLC Header ----- DLC: DLC: Frame 121 arrived at 07:02:54.7746;  
frame size is 347 (015B hex) bytes. DLC: **Destination = Station 003094248F72** DLC: **Source =  
Station 0005DC0BF2F4** DLC: Ethertype = 0800 (IP) DLC: IP: ----- IP Header ----- IP: IP: Version =  
4, header length = 20 bytes IP: Type of service = 00 IP: 000. .... = routine IP: ...0 .... =  
normal delay IP: .... 0... = normal throughput IP: .... .0.. = normal reliability IP: .... ..0.  
= ECT bit - transport protocol will ignore the CE bit IP: .... ..0 = CE bit - no congestion IP:  
Total length = 333 bytes IP: Identification = 42 IP: Flags = 0X IP: .0.. .... = may fragment IP:  
..0. .... = last fragment IP: Fragment offset = 0 bytes IP: Time to live = 255 seconds/hops IP:  
Protocol = 17 (UDP) IP: Header checksum = 3622 (correct) IP: **Source address = [192.168.2.2] IP:  
Destination address = [192.168.1.1]** IP: No options IP: UDP: ----- UDP Header ----- UDP: UDP:  
**Source port = 67 (BootPs/DHCP) UDP: Destination port = 67 (BootPs/DHCP)** UDP: Length = 313 UDP:  
Checksum = 7DF6 (correct) UDP: [305 byte(s) of data] UDP: DHCP: ----- DHCP Header ----- DHCP:  
DHCP: Boot record type = 2 (Request) DHCP: Hardware address type = 1 (10Mb Ethernet) DHCP:  
Hardware address length = 6 bytes DHCP: DHCP: Hops = 0 DHCP: Transaction id = 000005F4 DHCP:  
Elapsed boot time = 0 seconds DHCP: Flags = 8000 DHCP: 1... .. = Broadcast IP  
datagrams DHCP: Client self-assigned IP address = [0.0.0.0] DHCP: Client IP address =  
[192.168.1.2] DHCP: Next Server to use in bootstrap = [0.0.0.0] DHCP: **Relay Agent =  
[192.168.1.1] DHCP: Client hardware address = 0005DCF2C441** DHCP: DHCP: Host name = "" DHCP: Boot  
file name = "" DHCP: DHCP: Vendor Information tag = 63825363 DHCP: Message Type = 5 (DHCP Ack)  
DHCP: Server IP address = [192.168.2.2] DHCP: Request IP address lease time = 172800 (seconds)

```
DHCP: Address 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:
```

## DHCP のトラブルシューティング：クライアントワークステーションが DHCP アドレスを取得できない場合

### 事例 1：DHCP サーバが DHCP クライアントと同じ LAN セグメントまたは VLAN 上にある場合

DHCP サーバとクライアントが同じ LAN セグメントまたは VLAN にある環境で、クライアントが DHCP サーバから IP アドレスを取得できない場合、その原因がローカル ルータにあることはほとんどありません。この問題は、ほとんどの場合、DHCP サーバと DHCP クライアントを接続するデバイスに関連しています。ただし、DHCP サーバまたはクライアント自体に問題がある場合もあります。次のトラブルシューティング モジュールに従って、問題を引き起こしているデバイスを特定してください。

注: VLAN ごとに DHCP サーバを設定するには、DHCP アドレスをクライアントに提供する VLAN ごとに異なる DHCP プールを定義します。

### 事例 2：DHCP/BootP リレー エージェント機能が設定されたルータによって、DHCP サーバと DHCP クライアントが分けられている場合

DHCP サーバとクライアントが異なる LAN セグメントまたは VLAN にある環境では、DHCP/BootP リレー エージェントとして機能するルータが、DHCPREQUEST を DHCP サーバに転送する役割を果たします。DHCP サーバとクライアントだけでなく、DHCP/BootP リレー エージェントのトラブルシューティングもあわせて行うには、追加のトラブルシューティング ステップが必要です。次のトラブルシューティング モジュールに従って、問題を引き起こしているデバイスを特定してください。

### ルータ上の DHCP サーバがエラー POOL EXHAUSTED でアドレスの割り当てに失敗

一部のアドレスが、プールから解放された後もクライアントによって保持されている場合があります。これは、`show ip dhcp conflict` の出力によって確認できます。2 つのホストが同一の IP アドレスを使用すると、アドレス競合が発生します。アドレスの割り当て時、DHCP は ping および gratuitous ARP を使用して、競合をチェックします。

競合が検出されると、該当するアドレスがプールから削除されます。該当するアドレスは、管理者が競合を解決するまで割り当てられません。この問題を解決するには、`no ip dhcp conflict logging` を設定します。

## DHCP のトラブルシューティング モジュール

### DHCP 問題の発生源について

DHCP 問題はさまざまな原因で起こります。最も可能性の高い原因は、設定の問題です。しかし、オペレーティング システム、Network Interface Card (NIC; ネットワーク インターフェイスカード) のドライバ、ルータで動作している DHCP/BootP リレー エージェントなどのソフトウ

エアの不良によっても、各種の DHCP 問題が引き起こされる可能性があります。このように原因となりうる領域が複数あるため、トラブルシューティングには体系的なアプローチが必要となります。

## DHCP 問題の原因となりうるもの

- Catalyst スイッチのデフォルト コンフィギュレーション
- DHCP/BootP リレー エージェントの設定
- NIC の互換性の問題、または DHCP 機能の問題
- NIC の障害または不適切な NIC ドライバのインストール
- 頻繁なスパニング ツリー計算による断続的なネットワークの停止
- オペレーティング システムの動作またはソフトウェアの不良
- DHCP サーバのスコープ設定またはソフトウェアの不良
- Cisco Catalyst スイッチまたは IOS DHCP/BootP リレー エージェントのソフトウェアの不良
- 予想と異なるインターフェイスで DHCP オファーを受信したため、Unicast Reverse Path Forwarding ( uRPF ) チェックが失敗する Reverse Path Forwarding ( RPF ) 機能がインターフェイス上で有効になっていると、Cisco ルータは送信元アドレスが 0.0.0.0、宛先アドレスが 255.255.255.255 の Dynamic Host Configuration Protocol ( DHCP; ダイナミック ホスト コンフィギュレーション プロトコル ) パケットおよび BOOTstrap Protocol ( BOOTP; ブートストラップ プロトコル ) パケットを廃棄する場合があります。また、ルータは、該当インターフェイスをマルチキャスト IP の宛先とする IP パケットをすべて廃棄する場合があります。この問題は [CSCdw31925](#) ( [登録ユーザのみ](#) ) でドキュメント化されています。
- DHCP データベース エージェントを使用していないが、DHCP 競合のロギングが無効にされていない

このドキュメントでは、上記のリストにあるような根本原因を特定するために、次のトラブルシューティング モジュールを使用しています。

### A. [物理的な接続の確認](#)

この手順はすべての事例に適用されます。

最初に、DHCP クライアントとサーバの物理的な接続を確認します。Catalyst スイッチに接続されている場合は、DHCP クライアントとサーバがどちらも物理的に接続されているかを確認します。

2948G、4000、5000、6000 シリーズ スイッチなどの Catalyst CatOS スイッチでは、`show port <mod#>/<port_range>` コマンドを使用して、ポートのステータスを確認します。ポートのステータスが `connected` 以外である場合、そのポートでは、DHCP クライアント要求も含め、すべてのトラフィックが通過しません。このコマンドからの出力例を次に示します。

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

Catalyst 2900XL/3500XL/2950/3550 などの IOS ベースのスイッチでは、`show port status` に相当するコマンドとして `show interface <interface>` を使用します。インターフェイスの状態が `<interface> is up, line protocol is up` 以外である場合、そのポートでは DHCP クライアント要求も含め、すべてのトラフィックが通過しません。このコマンドからの出力例を次に示します。

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

物理的な接続を確認した結果、実際に Catalyst スイッチと DHCP クライアント間のリンクがない

場合は、『[Cisco Catalyst スイッチと NIC との互換性に関する問題のトラブルシューティング](#)』を参照して、物理層の接続上の問題に関する追加のトラブルシューティングを行います。

データ リンク エラーが頻繁に発生すると、一部の Catalyst スイッチのポートが errdisabled 状態になる場合があります。errdisable 状態の詳細と、この状態から復旧する方法については、『[CatOS プラットフォームでの errDisable ポート状態からの復旧](#)』および『[Cisco IOS プラットフォームでの errDisable ポート状態からの復旧](#)』を参照してください。

## **B. クライアント ワークステーションにスタティック IP アドレスを設定してネットワーク接続性をテスト**

この手順はすべての事例に適用されます。

DHCP 問題のトラブルシューティングでは、クライアント ワークステーションにスタティック IP アドレスを設定してネットワーク接続性を確認することが重要です。ワークステーションにスタティック IP アドレスを設定してもネットワーク リソースに到達できない場合、問題の根本原因は DHCP ではありません。この場合は、ネットワーク接続性のトラブルシューティングが必要です。

## **C. 起動時における問題の確認**

この手順はすべての事例に適用されます。

DHCP クライアントが起動時に DHCP サーバから IP アドレスを取得できない場合は、クライアントから DHCP サーバに手動で DHCP 要求を送信して IP アドレスを取得できるかを試してみます。DHCP サーバから IP アドレスを手動で取得するには、クライアントのオペレーティング システムに応じて次のステップに従います。

**Microsoft Windows 95/98/ME :** Start ボタンをクリックして、WINIPCFG.exe プログラムを実行します。RenewAll ボタンに先行している ReleaseAll ボタンをクリックして下さい。これで、DHCP クライアントは IP アドレスを取得できますか。

**Microsoft Windows NT/2000 :** [スタート]>[ファイル名を指定して実行] フィールドに cmd と入力して、コマンド プロンプト ウィンドウを開きます。コマンド プロンプト ウィンドウで、次のように ipconfig/renew コマンドを発行します。これで、DHCP クライアントは IP アドレスを取得できますか。

PC の起動プロセスが完了した後、DHCP クライアントから IP アドレスを手動で更新することで IP アドレスを取得できる場合、おそらく DHCP の起動の問題です。DHCP クライアントが Cisco Catalyst スイッチに接続している場合、最も可能性が高いのは、STP PortFast またはチャネリングとトランキングの処理に関する設定の問題です。その他には、NIC カードの問題やスイッチ ポートの起動の問題などが考えられます。スイッチ ポートの設定と NIC カードの問題が DHCP 問題の根本原因である可能性を除外するには、トラブルシューティング [ステップ D](#) と [E](#) を参照してください。

## **D. スイッチ ポートの設定の確認 ( STP PortFast とその他のコマンド )**

スイッチが Catalyst 2900/4000/5000/6000 の場合は、ポートの STP PortFast が有効で、トランキング/チャネリングが無効になっていることを確認します。デフォルト設定は、STP PortFast が無効で、トランキング/チャネリングが自動です ( 該当する場合 )。2900XL/3500XL/2950/3550 スイッチでは、STP PortFast のみが必須の設定です。Catalyst スイ

ツチの初期設置時に最もよく見られる DHCP クライアントの問題は、これらの設定変更によって解決します。

Catalyst スイッチに接続する DHCP が正常に動作するために必要なスイッチ ポート設定の要件については、次の文書を参照してください。

### [『PortFast と他のコマンドを使用したワークステーションの接続始動遅延の修復』](#)

上記の文書の設定ガイドラインを参照した後、この文書に戻ってトラブルシューティングを続けてください。

## **E. NIC カードまたは Catalyst スイッチに関する既知の問題のチェック**

Catalyst スイッチの設定が適切な場合は、Catalyst スイッチまたは DHCP クライアントの NIC に、DHCP 問題の原因となるソフトウェアの互換性の問題がある可能性があります。このトラブルシューティング ステップでは、次のドキュメントを参照して、Catalyst スイッチまたは NIC のソフトウェアの問題が DHCP 問題の原因である可能性を除外します。

### [「Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues \( Cisco Catalyst スイッチと NIC との互換性に関する問題のトラブルシューティング \)」](#)

互換性の問題を適切に除外するには、DHCP クライアントのオペレーティング システムに関する知識と、メーカー、モデル、ドライバのバージョンといった NIC 固有の情報が必要となります。

## **F. DHCP サーバと同じサブネットまたは VLAN にあるクライアントが IP アドレスを取得しているかどうかを確認**

クライアントが DHCP サーバと同じサブネットまたは VLAN にある場合に、DHCP が正常に機能しているかどうかを判別することは重要です。DHCP サーバと同じサブネットまたは VLAN で DHCP が正常に機能している場合は、DHCP/BootP リレー エージェントに問題がある可能性があります。DHCP サーバと同じサブネットまたは VLAN の DHCP テストでも問題が見られる場合は、実際に DHCP サーバに問題がある可能性があります。

## **G. ルータの DHCP/BootP リレー設定の確認**

次のステップに従って設定を確認します。

1. ルータで DHCP リレーを設定している場合は、`ip helper-address` コマンドが適切なインターフェイス上に配置されていることを確認します。ip helper-address コマンドは、DHCP クライアント ワークステーションの着信インターフェイス上にあり、正しい DHCP サーバを指している必要があります。
2. グローバル設定コマンド `no service dhcp` がないことを確認します。この設定パラメータは、ルータの DHCP サーバ機能とリレー機能をすべて無効にします。デフォルト コンフィギュレーションの `service dhcp` はデフォルト設定コマンドで、コンフィギュレーションには表示されません。[service dhcp が有効でない場合、クライアントは DHCP サーバから IP アドレスを取得しません。](#)注: [以前の Cisco IOS リリースが稼働しているルータの場合は、service dhcp コマンドの代わりに、ip bootp server コマンドによって DHCP リレー エージェント機能が処理されます。](#)このため、ip helper-address コマンドが DHCP UDP ブロードキャストを転送して、DHCP クライアントの代わりに DHCP リレー エージェントとして動作するように設定されている場合は、これらのルータで ip bootp server コマンドを有効にす



る必要があります。

3. **ip helper-address** コマンドを使用して、UDP ブロードキャストをサブネット ブロードキャスト アドレスに転送する場合は、UDP ブロードキャスト パケットが経由するすべての発信インターフェイスで `no ip directed-broadcast` が設定されていないことを確認します。 `no ip directed-broadcast` は、ダイレクト ブロードキャストから物理ブロードキャストへの変換をブロックします。このインターフェイス設定は、ソフトウェア バージョン 12.0 以上のデフォルト コンフィギュレーションです。
4. DHCP ブロードキャストを DHCP サーバのサブネット ブロードキャスト アドレスに転送すると、ソフトウェアの問題を引き起こすことがあります。DHCP のトラブルシューティングを行うときは、次のように、必ず DHCP UDP ブロードキャストを DHCP サーバの IP アドレスに転送するようにしてください。

## H. [加入者識別 \( 82 \) オプションがオン](#)

DHCP リレー エージェント情報 ( オプション 82 ) 機能を使用すると、DHCP クライアントから DHCP サーバに DHCP 要求を転送する際に、DHCP リレー エージェント ( Catalyst スイッチ ) が自身に関する情報と接続されているクライアントに関する情報を含めることが可能になります。

DHCP サーバはこの情報を使用して、サービスプロバイダー ネットワークの加入者ごとに、IP アドレスを割り当てたり、アクセス制御を実行したり、Quality of Service ( QoS ) とセキュリティ ポリシー ( またはその他のパラメータ割り当てポリシー ) を設定したりすることができます。

スイッチで DHCP スヌーピングを有効にすると、自動的にオプション 82 が有効になります。

DHCP サーバがオプション 82 を使用してパケットを処理するように設定されていない場合、その要求にはアドレスが割り当てられません。

この問題を解決するには、グローバル設定コマンド `no ip dhcp relay information option` を使用して、スイッチ ( リレー エージェント ) の加入者識別オプション ( 82 ) を無効にします。

## I. [DHCP データベース エージェントと DHCP 競合のロギング](#)

DHCP データベース エージェントとは、DHCP バインディング データベースが格納されているホストのことです ( FTP、TFTP、RCP サーバなど )。DHCP データベース エージェントは複数設定でき、各エージェントでデータベース更新と転送の間のインターバルを設定できます。 [データベース エージェントとデータベース エージェント パラメータを設定するには、ip dhcp database コマンドを使用します。](#)

DHCP データベース エージェントを設定しない場合は、DHCP サーバで DHCP アドレス競合の記録を無効にしてください。 [DHCP アドレス競合のロギングを無効にするには、no ip dhcp conflict logging コマンドを実行します。](#) `clear ip dhcp conflict` を使用して、以前にロギングされた競合をクリアします。

競合のロギングの無効化に失敗すると、次のエラー メッセージが表示されます。

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

## J. [IP Phone 接続の CDP を調べる](#)

Cisco IP Phone に接続されているスイッチポートで Cisco Discovery Protocol ( CDP; Cisco 検出

プロトコル)が無効に設定されている場合、DHCP サーバは適切な IP アドレスを電話機に割り当てることができません。DHCP サーバは、スイッチポートのデータ VLAN またはサブネットに属している IP アドレスを割り当てる傾向があります。CDP が有効になっている場合、スイッチは、Cisco IP Phone が DHCP を要求していて、正しいサブネット情報を提供できることを検出できます。その場合、DHCP サーバは、音声 VLAN またはサブネット プールから IP アドレスを割り当てることができます。DHCP サービスを音声 VLAN にバインドする際、特別なステップは必要ありません。

## K. ダウンした SVI の削除による DHCP スヌーピング処理の中断

Cisco Catalyst 6500 シリーズ スイッチでは、特定の VLAN に対してスヌーピングするよう DHCP を設定した後、SVI (シャットダウン状態) が自動的に作成されます。この SVI の存在は、DHCP スヌーピングの正確なオペレーションに直接関係しています。

Native IOS が稼働する Cisco Catalyst 6500 シリーズ スイッチ上の DHCP スヌーピングはほとんど、スイッチ プロセッサ (SP またはスーパーバイザ) ではなく、ルート プロセッサ (RP または MSFC) に実装されます。Cisco Catalyst 6500 シリーズは、RP が加入している Local Target Logic (LTL) にパケットを供給する VACL 付きのハードウェア内でパケットを代行受信します。フレームは、RP に入ると、スヌーピング部に渡される前に、まず L3 インターフェイス (SVI) IDB と関連付けられる必要があります。SVI がないと、この IDB が存在しないため、パケットは RP 内で廃棄されます。

## L. 制限付きブロードキャスト アドレス

DHCP クライアントが DHCP パケット内のブロードキャスト ビットを設定すると、DHCP サーバおよびリレー エージェントはすべて 1 つのブロードキャスト アドレス (255.255.255.255) を使用して、DHCP メッセージをクライアントに送信します。ネットワークブロードキャストを送信するよう ip broadcast-address コマンドが設定されていると、DHCP によって送信されるすべて 1 のブロードキャストが上書きされます。この状況に対処するには、ip dhcp limited-broadcast-address コマンドを使用して、設定されているネットワークブロードキャストによって DHCP のデフォルトの動作が上書きされないようにします。

一部の DHCP クライアントは、すべて 1 つのブロードキャストのみを受け入れることができ、クライアントに接続されているルータ インターフェイス上で該当コマンドが設定されない限り、DHCP アドレスを取得することができません。

## M. ルータの debug コマンドによる DHCP のデバッグ

debug コマンドを使用して、ルータが DHCP 要求を受信しているかを確認

DHCP パケットのソフトウェア処理をサポートしているルータ上で、クライアントからの DHCP 要求が受信されているかどうかを確認できます。ルータがクライアントからの要求を受信していない場合、DHCP プロセスは失敗します。このトラブルシューティング ステップでは、デバッグ出力を得るために、access-list を設定する必要があります。この access-list はデバッグのためのものであり、これによってルータの動作が影響を受けることはありません。

グローバル設定モードで、次の access-list を入力します。

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

EXEC モードで、次の debug コマンドを入力します。

## debug ip packet detail 100

出力例 :

```
Router#debug ip packet detail 100 IP packet debugging is on (detailed) for access list 100
Router# 00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2 00:16:46: UDP
src=68, dst=67 00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
```

上記の出力から、ルータがクライアントからの DHCP 要求を受信していることがわかります。この出力が示しているのはパケットの要約情報のみであり、パケットそのものではありません。したがって、パケットが正常であるかどうかは判断できません。しかし、DHCP 用の適切な送信元 IP と宛先 IP、および UDP ポートを含むブロードキャスト パケットがルータで受信されていたのは確かです。

**debug コマンドを使用して、ルータが DHCP 要求を受信し、DHCP サーバに要求を転送しているかを確認**

ルータが DHCP サーバと正常に通信しているかどうかを確認するために、access-list のエントリを追加します。今度のデバッグもパケット自体を調べるものではありませんが、DHCP リレーエージェントが DHCP サーバに要求を転送しているかどうかは確認できます。

グローバル設定モードで、次の access-list を作成します。

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

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

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

次に、例を示します。

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

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

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

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

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

EXEC モードで、次の debug コマンドを入力します。

```
Router#
00:23:44: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:23:44: UDP src=68, dst=67
!--- Router receiving DHCPDISCOVER from DHCP client. 00:23:44: IP: s=192.168.1.1 (local),
d=192.168.2.2 (Ethernet4/1), len 604, sendg 00:23:44: UDP src=67, dst=67 !--- Router forwarding
DHCPDISCOVER unicast to DHCP server using DHCP/BootP Relay Agent source IP address. 00:23:44 IP:
s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4 00:23:44 UDP src=67, dst=67 !--- DHCP
server sending DHCP OFFER to DHCP/BootP Relay Agent. 00:23:44: IP: s=0.0.0.0 (Ethernet4/0),
d=255.255.255.255, len 604, rcvd 2 00:23:44: UDP src=68, dst=67 !--- Router receiving
DHCPREQUEST from DHCP client. 00:23:44: IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet4/1),
len 604, sendg 00:23:44: UDP src=67, dst=67 !--- Router forwarding DHCPDISCOVER unicast to DHCP
server using DHCP/BootP Relay Agent source IP address. 00:23:44 IP: s=192.168.2.2 (Ethernet1),
d=192.168.1.1, len 328, rcvd 4 00:23:44 UDP src=67, dst=67 !--- DHCP server sending DHCPACK back
```

to DHCP/BootP Relay Agent.

上記の出力から、ルータがクライアントからの DHCP 要求を受信し、DHCP/BootP リレー エージェントの設定に従って DHCP サーバに要求を転送していることがわかります。DHCP サーバも DHCP/BootP リレー エージェントに直接応答しています。この出力が示しているのはパケットの要約情報のみであり、パケットそのものではありません。したがって、パケットが正常であるか、あるいはサーバが DHCPNAK で応答しているかどうかは判断できません。しかし、DHCP 用の適切な送信元 IP と宛先 IP、および UDP ポートを含むブロードキャスト パケットがルータで受信されており、ルータと DHCP サーバの間で双方向の通信が行われていたのは確かです。

**debug ip udp コマンドを使用して、ルータが DHCP 要求を受信し、転送しているかを確認**

**debug ip udp コマンドを使用すれば、ルータを経由した DHCP 要求のパスをトレースできます。**

ただし、このデバッグ コマンドを実行すると、プロセス交換された UDP パケットがすべてコンソールに表示されるため、実稼働環境の運用に支障をきたします。このデバッグは、実稼働環境では行わないでください。

**警告：** >debug ip udp コマンドはルータの動作に影響を与えるため、CPU の使用率が上昇する可能性があります。

EXEC モードで、次の debug コマンドを入力します。

**debug ip udp**

出力例：

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

**debug ip dhcp server packet コマンドを使用して、ルータが DHCP 要求を受信し、転送しているかを確認**

ルータの IOS が 12.0.x.T または 12.1 で、IOS の DHCP サーバ機能をサポートしている場合は、debug ip dhcp server packet コマンドを使用して、別のデバッグ方法を実行できます。このデバッグは、IOS DHCP サーバ機能で使用するためのものでしたが、DHCP/BootP リレー エージェント機能のトラブルシューティングにも使用できます。上記のデバッグと同様に、このデバッグでも実際のパケットは表示されないため、問題を正確に判断することはできません。しかし、DHCP 処理について推論することは可能です。

EXEC モードで、次の debug コマンドを入力します。

## 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.
```

## 複数のデバッグの同時実行

複数のデバッグを同時に実行すると、DHCP/BootP リレー エージェントとサーバの動作についてかなりの量の情報を取得できます。これらの情報を使用すれば、上記のトラブルシューティングの概要に基づいて、DHCP/BootP リレー エージェント機能のどの部分が正常に動作していないかを推論できます。

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

## スニファトレースの取得と DHCP 問題の根本原因の特定

ルータ デバッグ手法を使用しても、必ずしも DHCP 問題の根本原因を正確に特定できるとは限りません。DHCP 問題を解決するための最終的なステップは、スニファトレースを取得して、プロセスのどの部分が正常に機能していないかを突き止めることです。DHCP パケットのトレー

スを解読するには、このドキュメントの「[同一の LAN セグメントにある DHCP クライアントとサーバのスニファトレースの解読](#)」および「[DHCP リレー エージェントとして設定されているルータによって分けられた DHCP クライアントとサーバのスニファトレースの解読](#)」の項を参照してください。

Catalyst スイッチで Switched Port Analyzer ( SPAN; 交換ポート アナライザ ) 機能を使用してスニファトレースを取得する方法については、次のドキュメントを参照してください。

- [Catalyst スイッチド ポート アナライザ \( SPAN \) 機能の設定](#)  
ルータでのデバッグを使用してパケットを解読するその他の方法

使用によって

Cisco ルータの [debug ip packet detail ダンプする](#) <acl> コマンド、システムログが Command Line Interface ( CLI ) で表示する hex の全体のパケットを取得することは可能性のあるです。 [上記の「debug コマンドを使用して、ルータが DHCP 要求を受信しているかを確認」および「debug コマンドを使用して、ルータが DHCP 要求を受信し、DHCP サーバに要求を転送しているかを確認」](#)の項の手順で、access-list に dump キーワードを追加すると、[同じデバッグ情報を 16 進数のパケット詳細とともに取得できます](#)。パケットの内容を解読するには、パケットを翻訳する必要があります。「付録 A」に例があります。

## [ip dhcp pool コマンドのオプション {option\\_number} ASCII の後に入力されたキーワードが二重引用符で囲まれている](#)

オプション番号が設定済みの DHCP オプションを持つ Cisco ルータは、URL を解析しようとする際、ip dhcp pool コマンドのオプション option number ASCII の後で入力されたキーワードが、ルータのリロード後に二重引用符に入っていることが原因で、障害が発生することがあります。この動作は IOS 12.4 ( 17a ) が稼働するデバイスで見られ、判明している不具合として [CSCsk96976](#) ( [登録ユーザ専用](#) ) に記載されています。

この問題は、IOS バージョン 12.4 ( 17b )、12.4 ( 18a ) 以降、および 12.4 ( 19 ) T1 で解決されています。

## [付録 A : IOS DHCP の設定例](#)

DHCP サーバ データベースはツリー構造で編成されています。ツリーのルートはナチュラル ネットワークのアドレスプール、ブランチはサブネットワークのアドレスプール、リーフはクライアントへの手動バインディングです。サブネットワークはネットワーク パラメータを継承し、クライアントはサブネットワーク パラメータを継承します。したがって、共通のパラメータ ( ドメイン名など ) は、ツリーの最上位 ( ネットワークまたはサブネットワーク ) レベルで設定する必要があります。

DHCP の設定方法と、それに関連するコマンドの詳細については、次のリンクを参照してください。

- [DHCP Configuration Task List](#)

```
version 12.1
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

```
hostname Router
!
enable password cisco
ip subnet-zero
no ip domain-lookup
ip dhcp excluded-address 10.10.1.1 10.10.1.199
!--- Address range excluded from DHCP pools. ! ip dhcp
pool test_dhcp !--- DHCP pool (scope) name is test_dhcp.
network 10.10.1.0 255.255.255.0 !--- DHCP pool (address
will be assigned in this range) for associated Gateway
IP address. default-router 10.10.1.1 !--- DHCP option
for default gateway. dns-server 10.30.1.1 !--- DHCP
option for DNS server(s). netbios-name-server 10.40.1.1
!--- DHCP option for NetBIOS name server(s) (WINS).
lease 0 0 1 !--- Lease time. ! interface Ethernet0
description DHCP Client Network ip address 10.10.1.1
255.255.255.0 no ip directed-broadcast ! interface
Ethernet1 description Server Network ip address
10.10.2.1 255.255.255.0 no ip directed-broadcast ! line
con 0 transport input none line aux 0 transport input
all line vty 0 4 login ! end
```

## 関連情報

- [VPN 3000 コンセントレータでの DHCP リレー機能の設定](#)
- [PIX/ASA 7.x における DHCP Relay の設定例](#)
- [ツールとリソース](#)
- [テクニカルサポート - Cisco Systems](#)