IBM Systems - iSeries

ネットワーキング
DHCP (Dynamic Host Configuration Protocol)

バージョン 5 リリース 4

IBM Systems - iSeries

ネットワーキング
DHCP (Dynamic Host Configuration Protocol)

バージョン 5 リリース 4

お願い

本書および本書で紹介する製品をご使用になる前に、 65 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM i5/OS (プロダクト番号 5722-SS1) バージョン 5 リリース 4 モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、それ以降のすべてのリリースおよびモディフィケーションに適用されます。このバージョンは、すべての RISC モデルで稼動するとは限りません。また CISC モデルでは稼動しません。

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

http://www.ibm.com/jp/manuals/main/mail.html

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.ibm.com/jp/manuals/ の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原　典： IBM Systems - iSeries
Networking
Dynamic Host Configuration Protocol
Version 5 Release 4

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2006.2

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、
平成角ゴシック体™W5、平成角ゴシック体™W7

目次

動的ホスト構成プロトコル

動的ホスト構成プロトコル (DHCP) は、中央サーバーを使用して IP アドレスやネットワーク全体のその他の構成明細を管理する TCP/IP 規格です。

DHCP サーバーは、クライアントからの要求に応答し、クライアントに動的にプロパティーを割り当てます。

印刷可能 PDF

この情報の PDF を表示および印刷する方法について説明します。

本書の PDF 版を表示またはダウンロードするには、DHCP (約 1399 KB) を選択してください。

PDF ファイルの保存

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を右クリックする (上記のリンクを右クリックする)。
2. PDF をローカルに保存するオプションをクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「**保存**」をクリックする。

Adobe Reader のダウンロード

PDF を表示したり印刷したりするには、ご使用のシステムに Adobe Reader をインストールする必要があります。 Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html) から無料でダウンロードできます。

DHCP の概念

DHCP はクライアントと対話し、ネットワーク内で機能します。

DHCP は、動的クライアント構成のための自動化方式を提供します。DHCP 対応になっているクライアントは、それぞれ固有の IP アドレスと構成パラメーターをサーバーから自動的に取得します。このプロセスは、一連のステップを経て発生します。

DHCP クライアント/サーバー間の対話

クライアントはサーバーから DHCP 情報を入手し、クライアントとサーバー間で特定のメッセージが送信されます。 DHCP はリースを取得して戻します。

DHCP は、動的クライアント構成のための自動化方式を提供します。DHCP 対応になっているクライアントは、それぞれ固有の IP アドレスと構成パラメーターをサーバーから自動的に取得します。このプロセスは、次の図に示す一連のステップにしたがって、発生します。

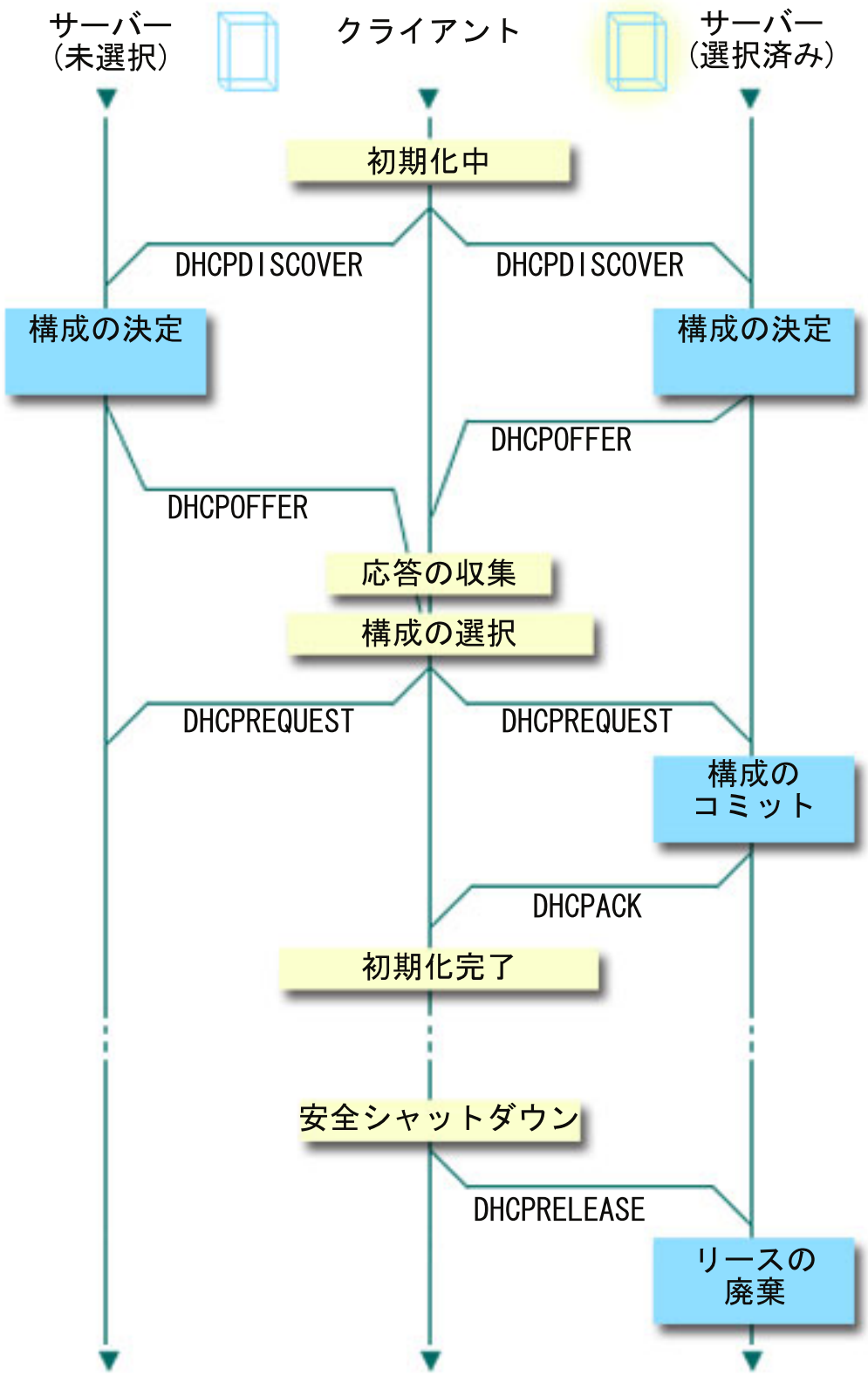


図 1. DHCP クライアント/サーバー間の対話

「クライアントが DHCP 情報を要求する : DHCPDISCOVER」
最初に、クライアントは、IP アドレスを要求する DISCOVER メッセージを送信します。

DISCOVER メッセージには、クライアントに固有の ID (通常、MAC アドレス) が入っています。このメッセージには、要求されたオプション (たとえば、サブネット・マスク、ドメイン・ネーム・サーバー、ドメイン・ネーム、または静的経路) など、他の要求も含めることができます。メッセージは、ブロードキャストとして発信されます。ネットワークにルーターが含まれている場合、接続されているネットワーク上の DHCP サーバーに DISCOVER パケットを転送するように、それらのルーターを構成できます。

「DHCP サーバーが、クライアントに対して情報を提供する : DHCPOFFER」

DISCOVER メッセージを受信した DHCP サーバーは、応答として OFFER メッセージを送信できます。OFFER メッセージを受信した DHCP サーバーがクライアントに OFFER メッセージを送り返せない場合がありますが、その理由はさまざまです。多くの場合、すべての使用可能アドレスが現在リースされている、サブネットが設定されていない、もしくはクライアントがサポートされていないことが理由です。DHCP サーバーが応答として OFFER メッセージを送信した場合、DHCPOFFER には使用可能な IP アドレスと、DHCP セットアップで定義された他の構成情報がすべて含まれます。

「クライアントが DHCP サーバーのオファーを受け入れる : DHCPREQUEST」

クライアントは、DISCOVER に応答した DHCP サーバーから OFFER メッセージを受信します。クライアントは、要求した設定値と提案された内容を比較して、使用するサーバーを選択します。提案を受け入れるクライアントは、REQUEST メッセージを送信して、選択したサーバーを示します。このメッセージは、ネットワーク全体にブロードキャストされ、どのサーバーが選択されたのかがすべての DHCP サーバーに分かるようにします。

「DHCP サーバーがクライアントを確認し、IP アドレスをリースする : DHCPACK」

サーバーは、REQUEST メッセージを受信すると、そのアドレスに「リース済み」というマークを付けます。選択されなかったサーバーは、提案されたアドレスをそれぞれの使用可能プールに戻します。 選択されたサーバーは、クライアントに肯定応答 (DHCPACK) を送信します。この応答には、追加の構成情報が含まれています。

これで、クライアントは、IP アドレスと構成パラメーターを使用できるようになります。クライアントは、リースの有効期限が切れるまで、あるいは DHCPRELEASE メッセージをサーバーに送信してリースを終了するまで、これらの設定値を使用します。

「クライアントが、リースの更新を試みる : DHCPREQUEST、DHCPACK」

クライアントは、リース期間の半分が経過した時点でリースの更新を始めます。クライアントは、REQUEST メッセージをサーバーに送信することによって、更新を要求します。サーバーは、この要求を受け入れた場合は、クライアントに DHCPACK メッセージを送信します。 サーバーが要求に応答しない場合、クライアントは、リースの有効期限が切れるまで、引き続きその IP アドレスと構成情報を使用できます。リースがまだ有効な間は、クライアントとサーバーは、DHCPDISCOVER および DHCPREQUEST プロセスを実行する必要はありません。リースの有効期限が切れたら、クライアントは、DHCPDISCOVER プロセスを最初からやり直す必要があります。

「クライアントがリースを終了する : DHCPRELEASE」

クライアントは、RELEASE メッセージを DHCP サーバーに送信することにより、リースを終了します。 すると、サーバーは、そのクライアントの IP アドレスを使用可能アドレス・プールに戻します。

関連概念

6 ページの『リレー・エージェントとルーター』

ネットワーク内で DHCP リレー・エージェントを使用する必要がある場合、またルーターで十分な場合があります。 DHCP リレー・エージェントとルーターの両方を使用して、効率良くしかも安全にネットワーク全体にデータを転送することができます。

『リース』
DHCP リースについて説明し、DHCP クライアントのリース時間を決める際に考慮すべき問題点を提示します。

58 ページの『問題: クライアントが IP アドレスまたはその構成情報を受信しない』
クライアントが IP アドレスまたはその構成情報を受信できない場合、問題が発生する可能性があります。 IP アドレスは、クライアントと DHCP サーバー間の 4 ステップからなるプロセスを経て、クライアントにリースされます。

リース

DHCP リースについて説明し、DHCP クライアントのリース時間を決める際に考慮すべき問題点を提示します。

DHCP が構成情報をクライアントに送信する場合、その情報は、リース期間付きで送信されます。リース期間とは、クライアントが、割り当てられた IP アドレスを使用できる時間の長さです。リース期間中、DHCP サーバーは、その IP アドレスを他のクライアントに割り当てることができません。リースの目的は、クライアントが IP アドレスを使用できる時間の長さを制限することです。アドレスの数よりクライアントの数が多い場合、リースの効力により、未使用クライアントは IP アドレスを利用できません。また、限られた時間で管理者がネットワーク上のすべてのクライアントに対して構成変更を行うことも可能になります。リースの有効期限が切れると、クライアントは新しいリースを DHCP に要求します。構成データが変更されている場合には、その時点で新しいデータがクライアントに送信されます。

リースの更新

クライアントは、リース期間の半分が経過した時点でリースの更新を始めます。たとえば、24 時間リースの場合、クライアントは、12 時間後にリースの更新を試みます。クライアントは、DHCPREQUEST メッセージをサーバーに送信することによって、更新を要求します。更新要求には、クライアントの現在の IP アドレスと構成情報が入れられます。

サーバーは、この要求を受け入れると、クライアントに DHCPACK メッセージを送信します。サーバーが要求に応答しない場合、クライアントは、リースの有効期限が切れるまで、引き続きその IP アドレスと構成情報を使用できます。リースがまだ有効であれば、クライアントとサーバーは、DHCPDISCOVER および DHCPREQUEST プロセスを実行する必要はありません。リースの有効期限が切れたら、クライアントは、DHCPDISCOVER プロセスを最初からやり直す必要があります。

サーバーに接続できない場合、クライアントは、リースの有効期限が切れるまで、割り当てられたアドレスを引き続き使用できます。前の例では、クライアントは、最初にリースの更新を試みてからリースの有効期限が切れるまでに、12 時間の猶予があります。 12 時間の停止中、新しいユーザーは新しいリースを入手することはできませんが、停止の始まった時点で電源がオンになったコンピューターについてリースが有効期限切れになることはありません。

リース時間の決定

DHCP サーバーのデフォルトのリース時間は 24 時間です。 DHCP サーバーに設定するリース時間の長さは、いくつかの要因により異なります。 DHCP サーバーの使用目的、サイトの使用パターン、サービスの配置を考慮する必要があります。適切なリース時間を決める上で、以下の質問が役に立ちます。

アドレスの数よりユーザーの数が多いですか?
ユーザーの数の方が多い場合、リース時間を短くしてください。そうすれば、クライアントは、未使用リースの有効期限が切れるまで待つ必要がなくなります。

サポートに必要な最小時間がありますか?

標準的ユーザーが最小 1 時間接続しているのであれば、最小で 1 時間のリースが必要ということになります。

ネットワークで処理できる DHCP メッセージ・トラフィックの量はどのくらいですか?

クライアントの数が多い場合、または DHCP パケットが送信される通信回線が低速の場合は、ネットワーク・トラフィックが問題の原因となる場合があります。リース期間を短くすると、ネットワーク上の更新要求によるサーバーやネットワークのトラフィックの負荷が大きくなります。

配置するサービス計画の種類と、ネットワークで停止を処理できる程度はどのくらいですか?

日常保守や、停止による潜在的な影響を考慮に入れてください。リース時間がサーバー停止の少なくとも 2 倍あれば、すでにリースに入っている稼動中のクライアントがリースを失うことはありません。考えられる最長のサーバー停止について名案があれば、そのような問題は避けられます。

DHCP サーバーのネットワーク環境のタイプは? 標準的なクライアントは何をしますか?

DHCP サーバーがサービスを行うネットワーク上でクライアントが何を行うかを考えてください。たとえば、クライアントが基本的に、さまざまな時刻にネットワークに接続するモバイルで、1 日に一度か二度電子メールを確認するような環境の場合は、相対的に短いリース時間が必要です。この場合、すべてのクライアントそれぞれについて IP アドレスを 1 つ取り除けておく必要はありません。リース時間を制限することにより、クライアントの数よりも少ない IP アドレスでモバイル・クライアントをサポートできます。

一方、ほとんどの従業員が固定位置にある 1 次ワークステーションをもっているオフィス環境の場合は、24 時間のリース時間の方が適しています。この環境では、営業時間中にネットワークに接続する各クライアントが使用できる IP アドレスを用意しておくことも必要です。この場合、短いリース時間を設定すると、DHCP サーバーがリース更新をクライアントとより頻繁にネゴシエーションするようになるため、ネットワーク・トラフィック過剰が発生します。

ネットワーク構成はどのくらい変わりますか?

ネットワーク・トポロジーがかなり頻繁に変わる場合は、長いリースは避ける必要があります。リース期間が長いと、構成パラメーターを変更しなければならない場合に不都合です。リースの長さにより、影響を受ける各クライアントに連絡しなければならない場合と、クライアントを再始動する、つまり、リースが更新されるまで一定の時間の間待つだけの場合との違いが生じることがあります。

ネットワーク・トポロジーがほとんど変わらず、アドレス・プールに IP アドレスが十分に備わっていれば、無限のリース、つまり有効期限のないリースを使用するよう DHCP を構成することはできますが、無限リースはお勧めしません。 無限リースを使用すると、IP アドレスはクライアントに無制限にリースされます。そのようなクライアントは、無限リースを受信した後はリース更新プロセスの必要はありません。無限リースがクライアントに割り当てられると、そのアドレスを別のクライアントに割り当てることはできません。したがって、無限リースの場合、後になって、そのクライアントに新しい IP アドレスを割り当てようとしたり、そのクライアントの IP アドレスを別のクライアントにリースしようとすると、問題が発生します。

ネットワーク内には、ファイル・サーバーなど、必ず同じ IP アドレスを受信するクライアントをもつことがあります。無限リースを使用する代わりに、クライアントに特定のアドレスを割り当て、それに長いリース期間を指定してください。クライアントは、それでも、指定された時間の間、アドレスをリースし、そのリースを更新しなければなりませんが、サーバーはそのクライアント専用に IP アドレスを予約します。そうすれば、たとえば、新しいファイル・サーバーを獲得した場合、クライアント ID (MAC アドレス) を変更するだけで、サーバーは、その新しいファイル・サーバーに同じアドレスを割り当てます。新しいファイル・サーバーに無限のリースを指定した場合には、DHCP サーバーは、リースが明示的に削除された場合を除き、もう一度そのアドレスを割り当てることはできません。

関連概念

47 ページの『ネットワーク・トポロジーに関する考慮事項』
大部分の DHCP セットアップは、ネットワーク・トポロジー、ネットワーク上の装置 (たとえば、ルーター)、DHCP でクライアントをどのようにサポートしたいかを考えることで計画できます。

関連資料

1 ページの『DHCP クライアント/サーバー間の対話』
クライアントはサーバーから DHCP 情報を入手し、クライアントとサーバー間で特定のメッセージが送信されます。 DHCP はリースを取得して戻します。

リレー・エージェントとルーター

ネットワーク内で DHCP リレー・エージェントを使用する必要がある場合、またルーターで十分な場合があります。 DHCP リレー・エージェントとルーターの両方を使用して、効率良くしかも安全にネットワーク全体にデータを転送することができます。

初めに、DHCP クライアントは、どのようなネットワークに接続されているかが分からないため、それぞれの DISCOVER パケットをブロードキャストします。一部のネットワークでは、DHCP サーバーが、クライアントと同じ LAN 上にない場合があります。したがって、ブロードキャストされたクライアントの DHCP パケットを、DHCP サーバーが入っている LAN に転送する必要があります。ルーターによっては、DHCP パッケージを転送する構成になっているものがあります。ご使用のルーターが DHCP パケット転送をサポートしている場合は、それだけで十分です。ただし、ほとんどのルーターは、ブロードキャスト・アドレスの宛先 IP アドレスをもつパケット (DHCP パケット) を転送しません。この場合、ルーターが DHCP パケットを転送できないのであれば、DHCP サーバーをもつ LAN に DHCP パケットを転送するための BOOTP/DHCP リレー・エージェントがこの LAN に備わっている必要があります。リレー・エージェントおよびルーターを使用するサンプル・ネットワークについては、例: DHCP と PPP プロファイルが異なる iSeries™ サーバー上にある場合を参照してください。

この場合、DHCP サーバーは異なるネットワーク上にあるため、クライアントは、ルーター・オプション (オプション 3) を定義しておく必要があります。このオプションは、DHCP サーバーをもつネットワークに自分のネットワークを接続するルーターの IP アドレスを指定します。

これらのシナリオでは、BOOTP/DHCP リレー・エージェントを使用しない場合、それらのクライアントにサービスする他の LAN に DHCP サーバーを追加する必要があります。ネットワーク内にもつべき DHCP サーバーの台数を決める際に役立つように、ネットワーク・トポロジーに関する考慮事項を参照してください。

関連概念

47 ページの『ネットワーク・トポロジーに関する考慮事項』
大部分の DHCP セットアップは、ネットワーク・トポロジー、ネットワーク上の装置 (たとえば、ルーター)、DHCP でクライアントをどのようにサポートしたいかを考えることで計画できます。

58 ページの『問題: クライアントが IP アドレスまたはその構成情報を受信しない』
クライアントが IP アドレスまたはその構成情報を受信できない場合、問題が発生する可能性があります。 IP アドレスは、クライアントと DHCP サーバー間の 4 ステップからなるプロセスを経て、クライアントにリースされます。

関連タスク

51 ページの『DHCP サーバーおよび BOOTP/DHCP リレー・エージェントの構成』
このトピックでは iSeries DHCP サーバーの構成に使用する必要のあるソフトウェアについて説明します。また、DHCP 構成での作業方法、DHCP サーバー管理プログラムの使用法、および DHCP/BOOTP リレー・エージェントのセットアップ手順について説明します。

関連資料

1 ページの『DHCP クライアント/サーバー間の対話』
クライアントはサーバーから DHCP 情報を入手し、クライアントとサーバー間で特定のメッセージが送信されます。 DHCP はリースを取得して戻します。

43 ページの『例: DHCP と PPP プロファイルが異なる iSeries サーバー上にある場合』
2 つの LAN とリモート・ダイヤルイン・クライアントのためのネットワーク DHCP サーバーおよび DHCP/BOOTP リレー・エージェントとして 2 台の iSeries サーバーをセットアップする方法について説明します。

DHCP クライアントのサポート

DHCP を使用して、大きなグループ (サブネット) としてすべてのクライアントを管理するのではなく、ネットワーク内の各クライアントを個別に管理することができます。

この DHCP セットアップ方式によって、DHCP サーバーによって識別されたクライアントのみが IP アドレスと構成情報を受信できるようになります。

通常、DHCP を使用してアドレス・プールからクライアントのサブネットまで IP アドレスを分配する方法を考えます。ネットワークに DHCP 情報を要求するクライアントはいずれも、DHCP 管理者によって明示的に除外された場合を除き、サブネットが使用されているときはアドレス・プールから IP アドレスを受信できます。ただし、DHCP サーバーは、逆のこと、つまり、特定のクライアントにのみ DHCP サービスを限定することもできます。

DHCP サーバーは、個々のクライアント・レベルと、クライアントのタイプ (BOOTP または DHCP) の両方でサービスを制限できます。個々のクライアント・レベルでサービスを制限するためには、各ネットワーク・クライアントを DHCP 構成内で個別に識別する必要があります。各クライアントは、それぞれのクライアント ID (通常、それぞれの MAC アドレス) で識別されます。 DHCP 構成で識別されたクライアントだけに、DHCP サーバーから IP アドレスと構成情報が割り当てられます。クライアントが DHCP 構成にリストされていない場合、そのクライアントは、DHCP サーバーからサービスを拒否されます。この方式により、認識されていないホストが DHCP サーバーから IP アドレスや構成情報を取得できないようにすることができます。

ネットワーク・クライアントおよびそれらが受信する構成情報に対してさらに大きな制御を必要とする場合は、DHCP クライアントが、アドレス・プールから IP アドレスを受信するのではなく、静的 IP アドレスを受信するようにセットアップすることができます。クライアントが定義済みの IP アドレスを受信するようセットアップする場合、オーバーラップを避けるために、そのクライアントは、その IP アドレスを受信できる唯一のクライアントでなければなりません。動的 IP アドレス割り振りを使用すると、DHCP サーバーが、クライアントの IP アドレス割り当てを管理します。

もっと広いレベルでは、DHCP サーバーは、クライアントのタイプ (つまり BOOTP または DHCP) に基づいてクライアントへのサービスを制限できます。 DHCP サーバーは、BOOTP クライアントへのサービスを拒否できます。

関連概念

8 ページの『BOOTP』
このトピックでは BOOTP とは何かを説明し、BOOTP と DHCP の歴史も紹介します。

47 ページの『ネットワーク・トポロジーに関する考慮事項』
大部分の DHCP セットアップは、ネットワーク・トポロジー、ネットワーク上の装置 (たとえば、ルーター)、DHCP でクライアントをどのようにサポートしたいかを考えることで計画できます。

BOOTP

このトピックでは BOOTP とは何かを説明し、BOOTP と DHCP の歴史も紹介します。

ブートストラップ・プロトコル (BOOTP) は、DHCP が開発される前に使用されていたホスト構成プロトコルです。BOOTP サポートは、DHCP を簡素化したものです。BOOTP では、クライアントは、それぞれの MAC アドレスで識別され、特定の IP アドレスが割り当てられます。基本的に、ネットワーク内の各クライアントは 1 つの IP アドレスにマップされます。動的アドレス割り当てはなく、各ネットワーク・クライアントは BOOTP 構成内で識別する必要があります。クライアントは BOOTP サーバーから一定量の構成情報しか受信できません。

DHCP は BOOTP を基にしているため、DHCP サーバーは BOOTP クライアントをサポートできます。現在 BOOTP をご使用の場合は、BOOTP クライアントに影響を与えずに、DHCP をセットアップしたり、使用することができます。BOOTP クライアントを正しくサポートするには、ブートストラップ・サーバーの IP アドレスとブート・ファイル名オプション (オプション 67) を指定して、サーバー全体または各種サブネットについて BOOTP サポートを有効にする必要があります。

BOOTP クライアントのサポートには、BOOTP サーバーよりも、DHCP を使用する方が優先されます。DHCP を使用して BOOTP クライアントをサポートする場合でも、各 BOOTP クライアントは、基本的に、単一の IP アドレスにマップされるため、そのアドレスを別のクライアントが再使用することはできません。ただし、DHCP をこのように使用すると、BOOTP クライアントを IP アドレスに 1 対 1 でマッピングするよう設定しなくて済むという利点があります。 DHCP サーバーは、それでも、アドレス・プールから BOOTP クライアントに IP アドレスを動的に割り当てます。 BOOTP クライアントに割り当てられると、IP アドレスは永続的にそのクライアントが使用するように予約され、そのアドレス予約が明示的に削除されるまでそのままです。最後には、ホスト構成管理がさらに容易になるように BOOTP クライアントを DHCP に変換することを考慮する必要があります。

関連概念

7 ページの『DHCP クライアントのサポート』
DHCP を使用して、大きなグループ (サブネット) としてすべてのクライアントを管理するのではなく、ネットワーク内の各クライアントを個別に管理することができます。

BOOTP

47 ページの『ネットワーク・トポロジーに関する考慮事項』
大部分の DHCP セットアップは、ネットワーク・トポロジー、ネットワーク上の装置 (たとえば、ルーター)、DHCP でクライアントをどのようにサポートしたいかを考えることで計画できます。

動的更新

DHCP がクライアントに IP アドレスを割り当てる際に、DNS サーバーと一緒に DHCP サーバーを使用して DNS 内のクライアント情報を動的に更新することができます。

ドメイン・ネーム・システム (DNS) は、ホスト名とその関連 IP アドレスを管理するための分散データベース・システムです。DNS により、ホストを見つけるために、IP アドレス (xxx.xxx.xxx.xxx) でなく「www.example.com」など単純な名前を使用できます。

以前は、すべての DNS データが静的データベースに格納されていました。すべての DNS リソース・レコードの作成と保守を管理者が行わなければなりませんでした。現在では、BIND 8 を実行する DNS サーバーを、他のソースから要求を受け入れてゾーン・データを動的に更新するよう構成することができます。

ご使用の DHCP サーバーがホストに新しいアドレスを割り当てるたびに、更新要求を DNS サーバーに送信するように構成できます。この自動化されたプロセスにより、急速に成長あるいは変化する TCP/IP ネッ

トワーク内での DNS サーバー管理が軽減されます。ホスト・ロケーションが頻繁に変更されるネットワークでも同様です。DHCP を使用するクライアントが IP アドレスを受信すると、そのデータは、即時に DNS サーバーに送信されます。この方法により、DNS は、ホストの IP アドレスが変更された場合でも、ホストについての照会を正しく解決し続けることができます。

アドレス・マッピング (A) レコード、逆検索ポインター (PTR) レコード、またはその両方をクライアントに代わって更新するように、DHCP を構成できます。 A レコードは、クライアントの DNS 名をその IP アドレスにマップします。 PTR レコードは、ホストの IP アドレスをそのホスト名にマップします。クライアントのアドレスが変わると、DHCP は、更新内容を DNS サーバーに自動的に送信できるので、ネットワーク内の他のホストは DNS 照会によりそのクライアントの IP アドレスを見つけることができます。動的に更新されるレコードごとに、関連テキスト (TXT) レコードが作成され、そのレコードが DHCP によって作成されたことが示されます。

注: PTR レコードだけを更新するように DHCP を設定する場合は、各クライアントからのその A レコードの更新ができるように DNS を構成する必要があります。

更新の送信が許されている許可ソースのリストを作成すると、動的ゾーンが保護されます。DNS は、リソース・レコードを更新する前に、着信する要求パケットが許可されたソースからのものであるか検査します。

動的更新は、単一の iSeries サーバー上の DNS/DHCP 間、異なる iSeries サーバー間、または動的更新が可能な他のサーバーに対して行えます。

関連概念

47 ページの『ネットワーク・トポロジーに関する考慮事項』
大部分の DHCP セットアップは、ネットワーク・トポロジー、ネットワーク上の装置 (たとえば、ルーター)、DHCP でクライアントをどのようにサポートしたいかを考えることで計画できます。

60 ページの『問題: DNS レコードが DHCP によって更新されない』
iSeries DHCP サーバーは、DNS リソース・レコードを動的に更新することができます。動的更新エラーの原因は、DNS レコードの更新の失敗にある可能性があります。

関連タスク

56 ページの『動的更新を DNS に送信するための DHCP の構成』
DHCP サーバーが IP アドレスをクライアントにリースするときに動的に DNS リソース・レコードを更新するように DHCP サーバーと DNS サーバーを構成することができます。

動的更新を受信するための DNS の構成

関連情報

ドメイン・ネーム・システム (DNS)

リソース・レコード

DHCP オプションの検索

DHCP には、DHCP サーバーに情報を要求した場合にクライアントに送信できる構成オプションが多数あります。すべての DHCP オプションについて説明する索引ツールを使用できます。

DHCP オプションは、IP アドレスのほかに、DHCP サーバーがクライアントに渡す追加の構成データを定義します。一般的なオプションには、サブネット・マスク、ドメイン・ネーム、ルーター IP アドレス、ドメイン・ネーム・サーバー IP アドレス、および静的ルートが含まれます。

標準的な DHCP オプションは、RFC 2132: DHCP オプションおよび BOOTP ベンダー拡張機能の定義に基づくもので、これについては以下の表で説明します。iSeries ナビゲーターの「DHCP **オプション**」ページを使用して、カスタマイズされたオプションも構成できます。

表 1.

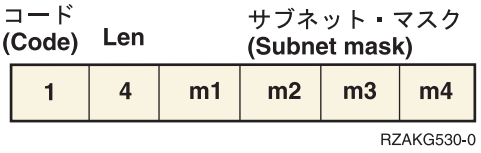
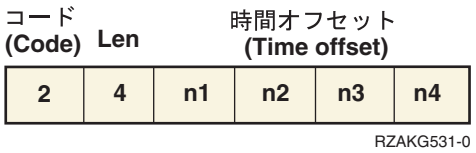
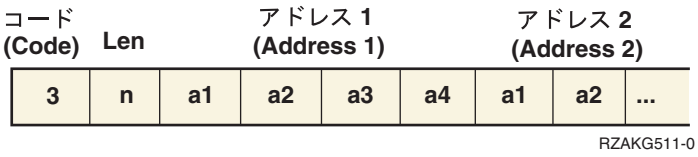
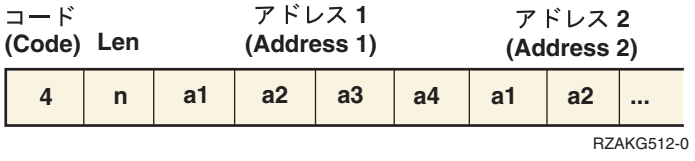
オプション番号	**オプション**	**説明**
1	サブネット・マスク (Subnet mask)	サブネット・マスク・オプションは、RFC 950 に従ってクライアントのサブネット・マスクを指定します。サブネット・マスク・オプションとルーター・オプションの両方を DHCP 応答に指定する場合は、サブネット・マスク・オプションを最初にする必要があります。 サブネット・マスク・オプションのコードは 1 であり、長さは 4 オクテットです。 
2	時間オフセット (Time offset)	時間オフセット・フィールドは、クライアントのサブネットと協定世界時 (UTC) とのオフセットを秒単位で指定します。オフセットは、2 の補数の 32 ビット整数で表されます。正のオフセット値は、0 度の子午線の東にある位置を示し、負のオフセット値は、0 度の子午線の西にある位置を示します。 時間オフセット・オプションのコードは 2 であり、長さは 4 オクテットです。 
3	ルーター (Router)	ルーター・オプションは、クライアントのサブネット上にあるルーターの IP アドレスのリストを指定します。ルーターは優先順位に従ってリストしなければなりません。 ルーター・オプションのコードは 3 です。ルーター・オプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 
4	タイム・サーバー (Time server)	タイム・サーバー・オプションは、クライアントが使用可能な RFC 868 タイム・サーバーのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 タイム・サーバー・オプションのコードは 4 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 

表 1. (続き)

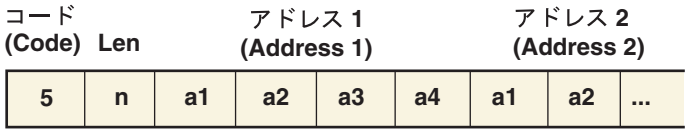
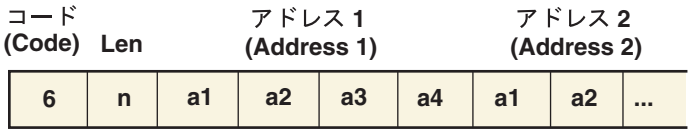
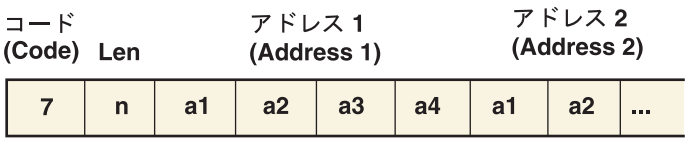
オプション番号	オプション	説明
5	ネーム・サーバー (Name server)	ネーム・サーバー・オプションは、クライアントが使用可能な IEN 116 ネーム・サーバーのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 ネーム・サーバー・オプションのコードは 5 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。  RZAKG513-0
6	ドメイン・ネーム・サーバー (Domain Name Server)	ドメイン・ネーム・サーバー・オプションは、クライアントが使用可能なドメイン・ネーム・システム (STD 13、RFC 1035) ネーム・サーバーのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 ドメイン・ネーム・サーバー・オプションのコードは 6 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。  RZAKG514-0
7	ログ・サーバー (Log server)	ログ・サーバー・オプションは、クライアントが使用可能な MIT-LCS UDP ログ・サーバーのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 ログ・サーバー・オプションのコードは 7 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。  RZAKG515-0
8	Cookie サーバー (Cookie server)	Cookie サーバー・オプションは、クライアントが使用可能な RFC 865 Cookie サーバーのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 Cookie サーバー・オプションのコードは 8 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。  RZAKG516-0

表 1. (続き)

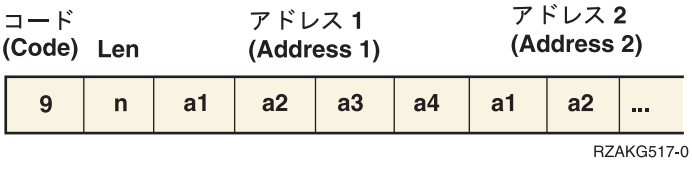
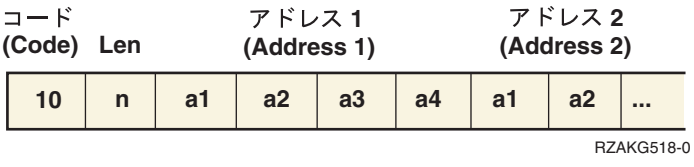
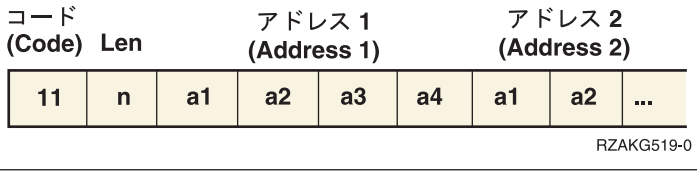
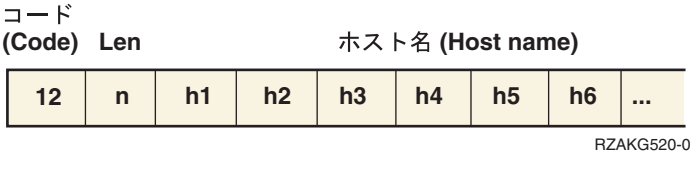
オプション番号	オプション	説明
9	LPR サーバー (LPR server)	LPR サーバー・オプションは、クライアントが使用可能な RFC 1179 ライン・プリンター・サーバーのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 LPR サーバー・オプションのコードは 9 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 
10	Impress サーバー (Impress server)	Impress サーバー・オプションは、クライアントが使用可能な Imagen Impress サーバーのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 Impress サーバー・オプションのコードは 10 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 
11	リソース・ロケーション・サーバー (Resource location server)	このオプションは、クライアントが使用可能な RFC 887 リソース・ロケーション・サーバーのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 このオプションのコードは 11 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 
12	ホスト名 (Host name)	このオプションは、クライアントの名前を指定します。この名前は、ローカル・ドメイン・ネームで修飾することも修飾しないこともできます (ドメイン・ネームの優先検索方法については、セクション 3.17 を参照)。文字セットの制約事項については、RFC 1035 を参照してください。 このオプションのコードは 12 であり、長さは 1 以上です。 

表 1. (続き)

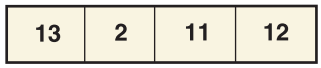
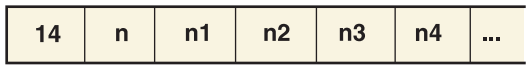
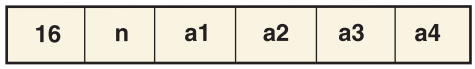
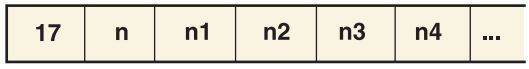
オプション番号	オプション	説明
13	ブート・ファイル・サイズ (Boot file size)	このオプションは、クライアントのデフォルト・ブート・イメージの長さを 512 オクテットのブロック数で指定します。ファイルの長さは、符号なし 16 ビット整数として指定します。 このオプションのコードは 13 であり、長さは 2 です。 コード (Code) Len ファイル・サイズ (File size)  RZAKG541-0
14	Merit ダンプ・ファイル (Merit dump file)	このオプションは、クライアントが破損した場合に、クライアントのコア・イメージがダンプされる先のファイルのパス名を指定します。このパスは、NVT ASCII 文字セットからの文字で構成される文字ストリングとしてフォーマットされます。 このオプションのコードは 14 です。長さは 1 以上です。 コード (Code) Len ダンプ・ファイル・パス名 (Dump file pathname)  RZAKG521-0
15	ドメイン・ネーム (Domain name)	このオプションは、ドメイン・ネーム・システムを介してホスト名を解決するときにクライアントが使用するドメイン・ネームを指定します。 このオプションのコードは 15 です。長さは 1 以上です。 コード (Code) Len ドメイン・ネーム (Domain name)  RZAKG522-0
16	スワップ・サーバー (Swap server)	これは、クライアントのスワップ・サーバーの IP アドレスを指定します。 このオプションのコードは 16 であり、長さは 4 です。 コード (Code) Len スワップ・サーバー・アドレス (Swap server address)  RZAKG523-0
17	ルート・パス (Root path)	このオプションは、クライアントのルート・ディスクが入っているパス名を指定します。このパスは、NVT ASCII 文字セットからの文字で構成される文字ストリングとしてフォーマットされます。 このオプションのコードは 17 です。長さは 1 以上です。 コード (Code) Len ルート・ディスク・パス名 (Root disk pathname)  RZAKG524-0

表 1. (続き)

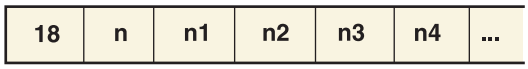
オプション番号	オプション	説明
18	拡張パス (Extensions path)	BOOTP 応答内の 64 オクテットのベンダー拡張フィールドと同じように解釈できる情報が入っているファイル (TFTP を使用して検索可能) を指定するストリング。ただし、次の例外があります。 • ファイルの長さに制約がない。 • ファイル内の Tag 18 に対するすべての参照 (つまり、BOOTP Extensions Path フィールドのインスタンス) は無視される。 このオプションのコードは 18 です。長さは 1 以上です。 コード (Code) Len 拡張パス名 (Extensions pathname)  RZAKG525-0
19	IP 転送 (IP forwarding)	このオプションは、クライアントがパケットの転送用に IP 層を構成するかどうかを指定します。値が 0 である場合は、IP 転送が使用不可であり、値が 1 である場合は、IP 転送が使用可能です。 このオプションのコードは 19 であり、長さは 1 です。 コード (Code) Len 値  RZAKG544-0
20	非ローカル・ソース・ルーティング (Non-Local source routing)	このオプションは、クライアントが、非ローカル・ソース・ルートでデータグラムの転送を許可するように IP 層を構成するかどうかを指定します。値が 0 である場合、このデータグラムの転送は許可されません。値が 1 である場合、転送は許可されます。 このオプションのコードは 20 であり、長さは 1 です。 コード (Code) Len 値  RZAKG545-0

表 1. (続き)

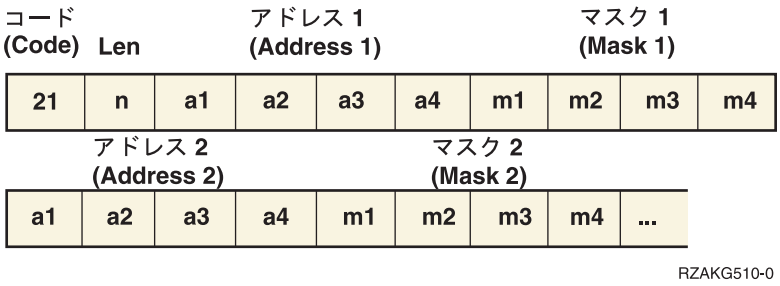
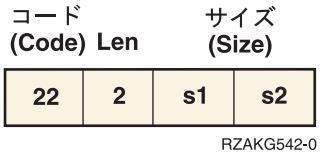
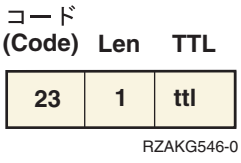
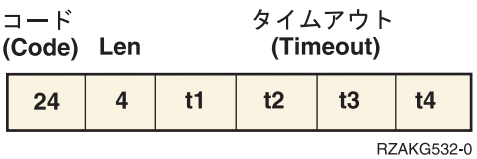
オプション番号	オプション	説明
21	ポリシー・フィルター (Policy filter)	このオプションは、非ローカル・ソース・ルーティング用のポリシー・フィルターを指定します。このフィルターは、着信ソース・ルートのフィルター操作に使用する宛先とマスクのペアを指定する、IP アドレスとマスクのリストから構成されます。 フィルターのいずれかと一致しないネクスト・ホップ・アドレスを持つ、任意のソース・ルート・データグラムは、クライアントによって破棄されます。 このオプションのコードは 21 です。このオプションの長さは 8 以上であり、8 の倍数でなければなりません。 
22	最大データグラム再アセンブル・サイズ (Maximum datagram reassembly size)	このオプションは、クライアントが再アセンブルする用意ができているデータグラムの最大サイズを指定します。このサイズは、符号なし 16 ビット整数として指定します。最小のリーガル値は 576 です。 このオプションのコードは 22 であり、長さは 2 です。 
23	デフォルト IP 存続時間 (Default IP time to live)	このオプションは、クライアントが発信データグラム上で使用するデフォルトの存続時間 (TTL) を指定します。この TTL は、1 から 255 の間の値を持つオクテットとして指定します。 このオプションのコードは 23 であり、長さは 1 です。 
24	Path MTU エージング・タイムアウト (Path MTU aging timeout)	このオプションは、RFC 1191 で定義されたメカニズムによって、エージング Path MTU 値が検出されるときに使用するタイムアウト (秒数) を指定します。このタイムアウトは、符号なし 32 ビット整数として指定します。 このオプションのコードは 24 であり、長さは 4 です。 

表 1. (続き)

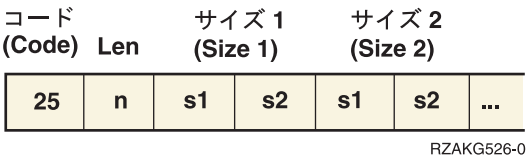
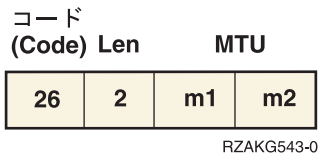
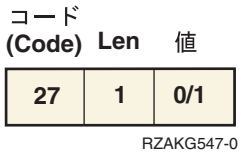
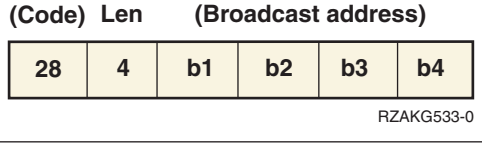
オプション番号	オプション	説明
25	Path MTU Plateau テーブル (Path MTU plateau table)	このオプションは、RFC 1191 で定義された Path MTU Discovery の実行時に使用する MTU サイズのテーブルを指定します。このテーブルは、符号なし 16 ビット整数のリストとしてフォーマットされ、最小のものから最大のものの順に並べられます。最小 MTU 値は、68 以上でなければなりません。 このオプションのコードは 25 です。長さは 2 以上であり、2 の倍数でなければなりません。 
26	インターフェース MTU (Interface MTU)	このオプションは、このインターフェース上で使用する MTU を指定します。この MTU は、符号なし 16 ビット整数として指定します。MTU の最小リーガル値は 68 です。 このオプションのコードは 26 であり、長さは 2 です。 
27	すべてのサブネットがローカル (All subnets are local)	このオプションは、クライアントが接続される先の IP ネットワークのすべてのサブネットが、クライアントが直接接続されるそのネットワークのサブネットと同じ MTU を使用するものと、クライアントが想定するかどうかを指定します。値 1 は、すべてのサブネットが同一 MTU を共用することを指定します。値が 0 である場合、直接接続されたネットワークの一部のサブネットにはそれより小さい MTU があるものと、クライアントが想定します。 このオプションのコードは 27 であり、長さは 1 です。 
28	ブロードキャスト・アドレス (Broadcast address)	このオプションは、クライアントのサブネット上で使用中のブロードキャスト・アドレスを指定します。ブロードキャスト・アドレスのリーガル値は、RFC 2132 のセクション 3.2.1.3 で指定されます。 このオプションのコードは 28 であり、長さは 4 です。 

表 1. (続き)

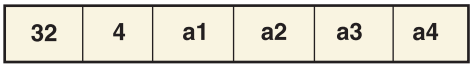
オプション番号	オプション	説明
29	マスク・ディスカバリーの実行 (Perform mask discovery)	このオプションは、クライアントが ICMP を使用してサブネット・マスク・ディスカバリーを実行するかどうかを指定します。値 0 は、クライアントがマスク・ディスカバリーを実行しないことを指定します。値 1 は、クライアントがマスク・ディスカバリーを実行することを指定します。 このオプションのコードは 29 であり、長さは 1 です。 コード (Code) Len 値  RZAKG548-0
30	マスク・サプライヤー (Mask supplier)	このオプションは、クライアントが ICMP を使用してサブネット・マスク要求に応答するかどうかを指定します。値 0 は、クライアントが応答しないことを指定します。値 1 は、クライアントが応答することを指定します。 このオプションのコードは 30 であり、長さは 1 です。 コード (Code) Len 値  RZAKG549-0
31	ルーター・ディスカバリーの実行 (Perform router discovery)	このオプションは、クライアントが、RFC 1256 で定義されたルーター・ディスカバリー・メカニズムを使用してルーターを請求するかどうかを指定します。値 0 は、クライアントがルーター・ディスカバリーを実行しないことを指定します。値 1 は、クライアントがルーター・ディスカバリーを実行することを指定します。 このオプションのコードは 31 であり、長さは 1 です。 コード (Code) Len 値  RZAKG550-0
32	ルーター送信請求アドレス (Router solicitation address) オプション	このオプションは、クライアントがルーター請求要求を送信する先のアドレスを指定します。 このオプションのコードは 32 であり、長さは 4 です。 コード (Code) Len アドレス (Address)  RZAKG534-0

表 1. (続き)

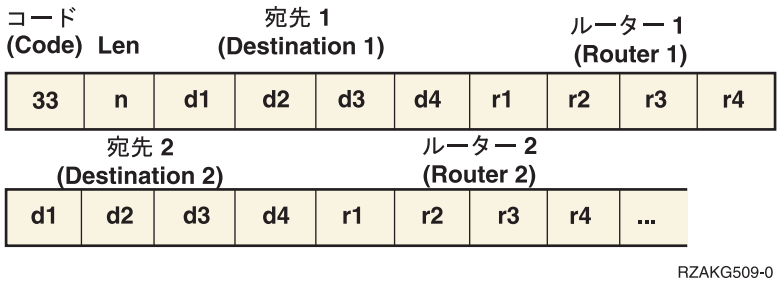
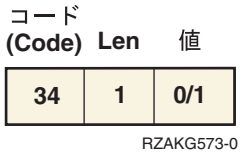
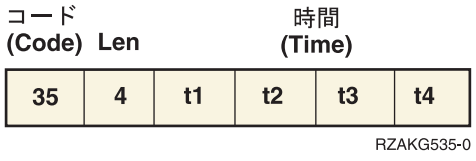
オプション番号	オプション	説明
33	静的ルート (Static route)	このオプションは、クライアントがそのルーティング・キャッシュ内にインストールする静的ルートのリストを指定します。同じ宛先への複数のルートが指定される場合、優先順位の高い順にリストされます。 これらのルートは、IP アドレスのペアのリストから構成されます。最初のアドレスは、宛先アドレスであり、2 番目のアドレスは、宛先のルーターです。 デフォルト・ルート (0.0.0.0) は、静的ルートのイリーガル宛先です。 このオプションのコードは 33 です。このオプションの長さは 8 以上であり、8 の倍数でなければなりません。 
34	トレーラー・カプセル化 (Trailer encapsulation)	このオプションは、クライアントが ARP プロトコルの使用時にトレーラーの使用 (RFC 893) をネゴシエーションするかどうかを指定します。値 0 は、クライアントがトレーラーの使用を試みないことを指定します。値 1 は、クライアントがトレーラーの使用を試みることを指定します。 このオプションのコードは 34 であり、長さは 1 です。 
35	ARP キャッシュ・タイムアウト (ARP cache timeout)	このオプションは、ARP キャッシュ入力のタイムアウト (秒数) を指定します。この時間は、符号なし 32 ビット整数として指定します。 このオプションのコードは 35 であり、長さは 4 です。 

表 1. (続き)

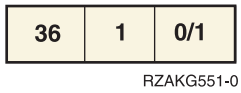
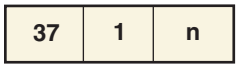
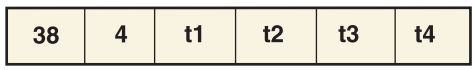
オプション番号	オプション	説明
36	イーサネット・カプセル化 (Ethernet encapsulation)	このオプションは、インターフェースがイーサネットである場合に、クライアントが Ethernet Version 2 (RFC 894) カプセル化を使用するか、IEEE 802.3 (RFC 1042) カプセル化を使用するかを指定します。値 0 は、クライアントが RFC 894 カプセル化を使用することを指定します。値 1 は、クライアントが RFC 1042 カプセル化を使用することを指定します。 このオプションのコードは 36 であり、長さは 1 です。 コード (Code) Len 値  RZAKG551-0
37	TCP デフォルト TTL (TCP default TTL)	このオプションは、TCP セグメントの送信時にクライアントが使用するデフォルト TTL を指定します。値は、符号なし 8 ビット整数として表されます。最小値は 1 です。 このオプションのコードは 37 であり、長さは 1 です。 コード (Code) Len TTL  RZAKG552-0
38	TCP キープアライブ・インターバル (TCP Keep-alive interval)	このオプションは、クライアント TCP が TCP 接続上でキープアライブ・メッセージを送信する前に待機しなければならないインターバル (秒数) を指定します。この時間は、符号なし 32 ビット整数として指定します。値 0 は、アプリケーションによって特に要求される場合を除いて、クライアントが接続上でキープアライブ・メッセージを生成しないことを指定します。 このオプションのコードは 38 であり、長さは 4 です。 コード (Code) Len 時間 (Time)  RZAKG536-0
39	TCP キープアライブ・ガーベッジ (TCP Keep-alive garbage)	このオプションは、以前のインプリメンテーションとの互換性を保つために、クライアントがガーベッジのオクテットと一緒に TCP キープアライブ・メッセージを送信するかどうかを指定します。値 0 は、ガーベッジ・オクテットが送信されないことを指定します。値 1 は、ガーベッジ・オクテットが送信されることを指定します。 このオプションのコードは 39 であり、長さは 1 です。 コード (Code) Len 値  RZAKG553-0

表 1. (続き)

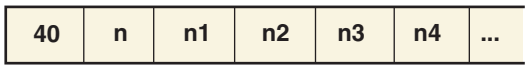
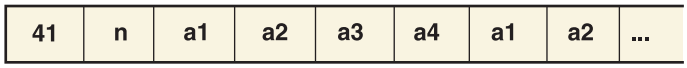
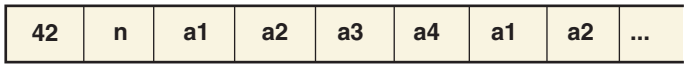
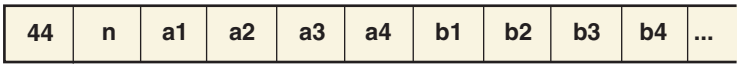
オプション番号	オプション	説明
40	ネットワーク情報サービス・ドメイン (Network information service domain)	このオプションは、クライアントの NIS ドメインの名前を指定します。このドメインは、NVT ASCII 文字セットからの文字で構成される文字ストリングとしてフォーマットされます。 このオプションのコードは 40 です。長さは 1 以上です。 コード (Code) Len NIS ドメイン・ネーム (NIS Domain name)  RZAKG540-0
41	ネットワーク情報サーバー (Network information server)	このオプションは、クライアントが使用可能な NIS サーバーを示す IP アドレスのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 このオプションのコードは 41 です。長さは 4 以上であり、4 の倍数でなければなりません。 コード (Code) Len アドレス 1 (Address 1) アドレス 2 (Address 2)  RZAKG556-0
42	Network Time Protocol サーバー (Network time protocol servers) オプション	このオプションは、クライアントが使用可能な NTP サーバーを示す IP アドレスのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 このオプションのコードは 42 です。長さは 4 以上であり、4 の倍数でなければなりません。 コード (Code) Len アドレス 1 (Address 1) アドレス 2 (Address 2)  RZAKG557-0
44	NetBIOS over TCP/IP ネーム・サーバー (NetBIOS over TCP/IP name server)	NetBIOS ネーム・サーバー (NBNS) オプションは、優先順にリストされた RFC 1001/1002 NBNS ネーム・サーバーのリストを指定します。 このオプションのコードは 44 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 コード (Code) Len アドレス 1 (Address 1) アドレス 2 (Address 2)  RZAKG558-0

表 1. (続き)

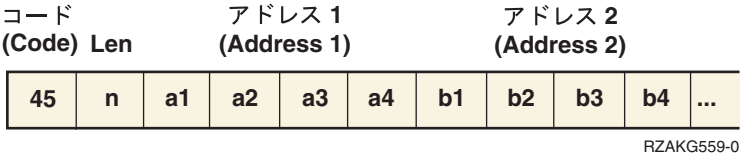
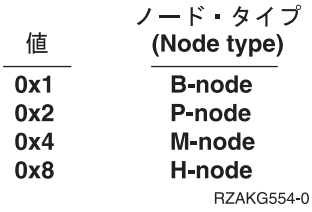
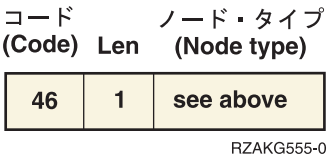
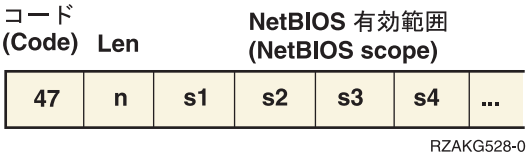
オプション番号	オプション	説明
45	NetBIOS over TCP/IP データグラム配布サーバー (NetBIOS over TCP/IP datagram distribution server)	NetBIOS データグラム配布サーバー (NBDD) オプションは、優先順にリストされた RFC 1001/1002 NBDD サーバーのリストを指定します。 このオプションのコードは 45 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 
46	NetBIOS over TCP/IP ノード・タイプ (NetBIOS over TCP/IP node type)	NetBIOS ノード・タイプ・オプションは、構成可能な NetBIOS over TCP/IP クライアントが、RFC 1001/1002 で記述されるとおりに構成できるようにします。この値は、次のようにクライアント・タイプを識別する単一オクテットとして指定します。  上記の図で、「0x」という表記は、基数 16 の数値 (16 進数) を示します。 このオプションのコードは 46 です。このオプションの長さは、常に 1 です。 
47	NetBIOS over TCP/IP 有効範囲 (NetBIOS over TCP/IP scope)	NetBIOS 有効範囲オプションは、RFC 1001/1002 で指定されているとおりに、クライアントの NetBIOS over TCP/IP 範囲パラメーターを指定します。 このオプションのコードは 47 です。このオプションの長さは 1 以上です。 

表 1. (続き)

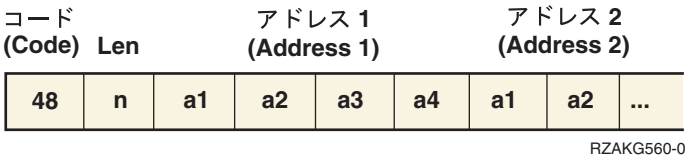
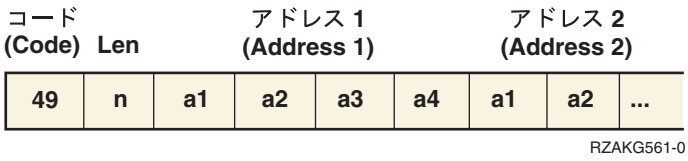
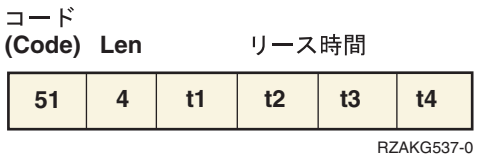
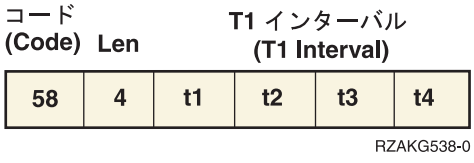
オプション番号	オプション	説明
48	X Window システム・フォント・サーバー (X Window System Font server)	このオプションは、クライアントが使用可能な X Window システム・フォント・サーバーのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 このオプションのコードは 48 です。このオプションの長さは 4 オクテット以上であり、4 の倍数でなければなりません。 
49	X Window システム画面マネージャー (X Window System display manager)	このオプションは、X Window システム画面マネージャーを実行するシステムで、クライアントが使用可能なシステムの IP アドレスのリストを指定します。 アドレスは優先順にリストしなければなりません。 このオプションのコードは 49 です。このオプションの長さは 4 以上であり、4 の倍数でなければなりません。 
51	IP アドレスのリース時間 (IP address lease time)	このオプションは、クライアント要求 (DHCPDISCOVER または DHCPREQUEST) で使用され、クライアントが IP アドレスのリース時間を要求できるようにします。サーバーの応答 (DHCPOFFER) で、DHCP サーバーはこのオプションを使用して、提供するリース時間を指定します。 この時間は、秒数単位で、符号なし 32 ビット整数として指定します。 このオプションのコードは 51 であり、長さは 4 です。 
58	更新 (T1) 時間値 (Renewal (T1) time value)	このオプションは、アドレス割り当てから、クライアントが RENEWING 状態に移行するまでの時間間隔を指定します。 この値は、秒数単位であり、符号なし 32 ビット整数として指定します。 このオプションのコードは 58 であり、長さは 4 です。 

表 1. (続き)

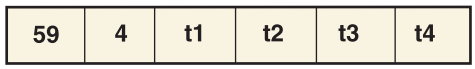
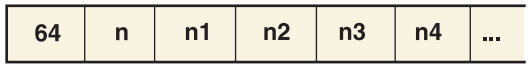
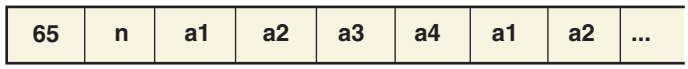
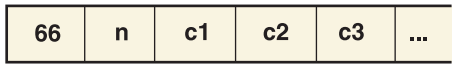
オプション番号	オプション	説明
59	再バインド (T2) 時間値オプション (Rebinding (T2) time value option)	このオプションは、アドレス割り当てから、クライアントが REBINDING 状態に移行するまでの時間間隔を指定します。 この値は、秒数単位であり、符号なし 32 ビット整数として指定します。 このオプションのコードは 59 であり、長さは 4 です。 コード (Code) Len T2 インターバル (T2 Interval)  RZAKG539-0
62	NetWare/IP ドメイン・ネーム (NetWare/IP domain name)	Netware/IP ドメイン・ネームを指定します。
63	NetWare/IP	必要な NetWare サブオプションを指定します。範囲は 1 から 255 です。NetWare/IP ドメイン・ネームを指定するには、オプション 62 を使用してください。
64	NIS ドメイン・ネーム (NIS domain name)	このオプションは、クライアントの NIS+ ドメインの名前を指定します。このドメインは、NVT ASCII 文字セットからの文字で構成される文字ストリングとしてフォーマットされます。 このオプションのコードは 64 です。長さは 1 以上です。 コード (Code) Len NIS クライアント・ドメイン・ネーム (NIS Client domain name)  RZAKG527-0
65	NIS サーバー (NIS server)	このオプションは、クライアントが使用可能な NIS+ サーバーを示す IP アドレスのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 このオプションのコードは 65 です。長さは 4 以上であり、4 の倍数でなければなりません。 コード (Code) Len アドレス 1 (Address 1) アドレス 2 (Address 2)  RZAKG562-0
66	サーバー名 (Server name)	このオプションは、DHCP ヘッダー内の sname フィールドが DHCP オプションに使用された場合に TFTP サーバーの識別に使用されます。 このオプションのコードは 66 であり、長さは 1 以上です。 コード (Code) Len TFTP サーバー (TFTP Server)  RZAKG571-0

表 1. (続き)

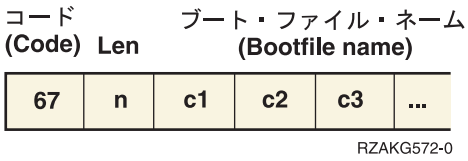
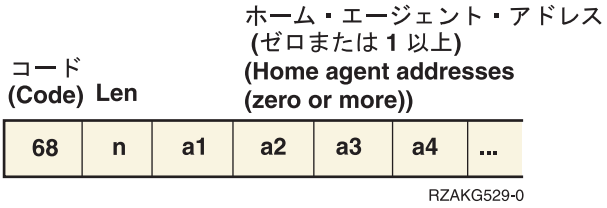
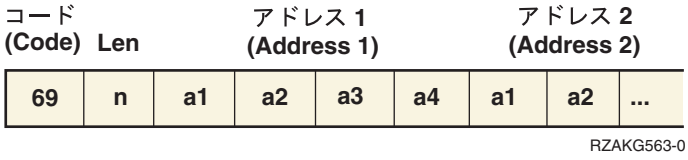
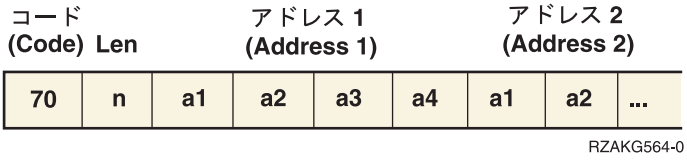
オプション番号	オプション	説明
67	ブート・ファイル名 (Boot file name)	このオプションは、DHCP ヘッダー内の file フィールドが DHCP オプションに使用された場合にブート・ファイルの識別に使用されます。 このオプションのコードは 67 であり、長さは 1 以上です。 
68	ホーム・アドレス (Home address)	このオプションは、クライアントが使用可能なモバイル IP ホーム・エージェントを示す IP アドレスのリストを指定します。エージェントは優先順位に従ってリストしなければなりません。 このオプションのコードは 68 です。このオプションの最小の長さは 0 (使用可能なホーム・エージェントがないことを示す) です。長さは 4 の倍数でなければなりません。通常の長さは、単一のホーム・エージェントのアドレスが入っている、4 オクテットであると予想されます。 
69	SMTP サーバー (SMTP server)	SMTP サーバー・オプションは、クライアントが使用可能な SMTP サーバーのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 SMTP サーバー・オプションのコードは 69 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 
70	POP3 サーバー (POP3 server)	POP3 サーバー・オプションは、クライアントが使用可能な POP3 のリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 POP3 サーバー・オプションのコードは 70 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 

表 1. (続き)

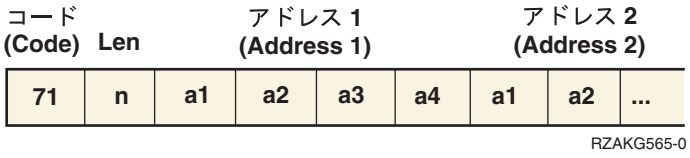
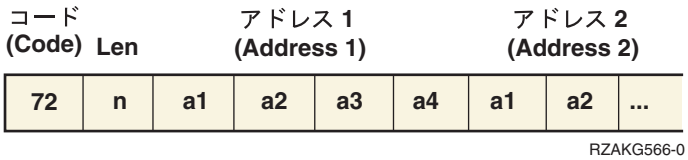
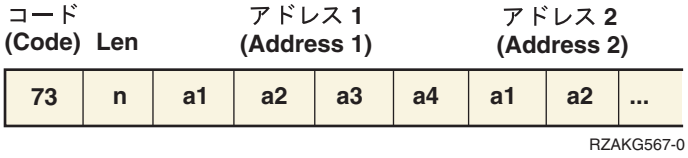
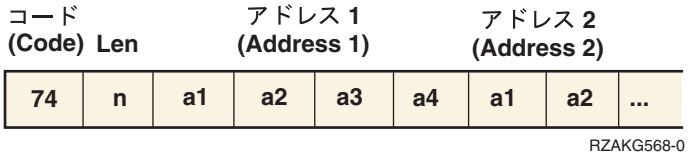
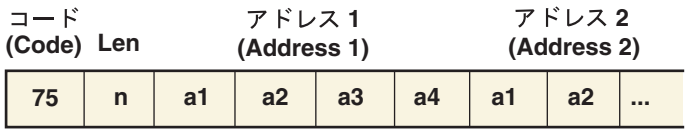
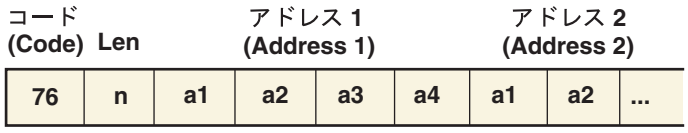
オプション番号	オプション	説明
71	NNTP サーバー (NNTP server)	NNTP サーバー・オプションは、クライアントが使用可能な NNTP のリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 NNTP サーバー・オプションのコードは 71 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 
72	WWW サーバー (WWW server)	WWW サーバー・オプションは、クライアントが使用可能な WWW のリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 WWW サーバー・オプションのコードは 72 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 
73	Finger サーバー (Finger server)	Finger サーバー・オプションは、クライアントが使用可能な Finger のリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 Finger サーバー・オプションのコードは 73 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 
74	IRC サーバー (IRC server)	IRC サーバー・オプションは、クライアントが使用可能な IRC のリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 IRC サーバー・オプションのコードは 74 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 

表 1. (続き)

オプション番号	オプション	説明
75	StreetTalk サーバー (StreetTalk server)	StreetTalk サーバー・オプションは、クライアントが使用可能な StreetTalk サーバーのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 StreetTalk サーバー・オプションのコードは 75 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 
76	STDA サーバー (STDA server)	StreetTalk Directory Assistance (STDA) サーバー・オプションは、クライアントが使用可能な STDA サーバーのリストを指定します。サーバーは優先順位に従ってリストしなければなりません。 StreetTalk Directory Assistance サーバー・オプションのコードは 76 です。このオプションの長さは 4 オクテット以上であり、常に 4 の倍数でなければなりません。 
77	ユーザー・クラス (User class)	ホストがメンバーであるクラス名を指定します。DHCP サーバーの構成時に、DHCP サーバーに対してこのクラスをあらかじめ定義しておく必要があります。
78	ディレクトリー・エージェント (Directory agent)	クライアントがメッセージの処理に Service Location Protocol を使用する場合、ディレクトリー・エージェントの IP アドレスを指定します。
79	サービス・スコープ (Service scope)	サービス要求メッセージに応答するのに Service Location Protocol を使用するディレクトリー・エージェントの有効範囲を指定します。
80	命名機関 (Naming authority)	クライアントがメッセージの処理に Service Location Protocol を使用する場合、ディレクトリー・エージェントの命名機関を指定します。この命名機関は、URL で使用される方式の構文を指定します。

関連概念

47 ページの『ネットワーク・トポロジーに関する考慮事項』
大部分の DHCP セットアップは、ネットワーク・トポロジー、ネットワーク上の装置 (たとえば、ルーター)、DHCP でクライアントをどのようにサポートしたいかを考えることで計画できます。

関連情報

http://www.rfc-editor.org/rfc/rfc2132.txt

DHCP の例

種々のネットワークのセットアップ方法について図と例を検討することにより、どの方法がお客様のインストールに最適かを判断できます。

あるテクノロジーについて理解するには、たいていの場合、他の人がそのテクノロジーをどのように使用しているかを見てみるのが一番の早道です。次に示す例は、DHCP の機能、各種ネットワーク・セットアップへの DHCP の組み込み方法、および V5R4 機能への結合方法を示しています。DHCP の初心者にも、経験を積んだ DHCP 管理者にも最適な開始点です。

関連概念

47 ページの『ネットワーク・トポロジーに関する考慮事項』
大部分の DHCP セットアップは、ネットワーク・トポロジー、ネットワーク上の装置 (たとえば、ルーター)、DHCP でクライアントをどのようにサポートしたいかを考えることで計画できます。

例: 単純な DHCP サブネット

4 つの PC クライアントと 1 台の LAN ベース・プリンターを備えた単純な LAN 内の DHCP サーバーとして iSeries サーバーをセットアップする場合について説明します。

次の図は、iSeries サーバー、4 台の PC クライアント、1 台の LAN ベース・プリンターをもつ単純な LAN を示しています。この例では、iSeries サーバーは、10.1.1.0 IP サブネットのための DHCP サーバーとして機能します。 このサーバーは、その 10.1.1.1 インターフェースを介して LAN に接続しています。

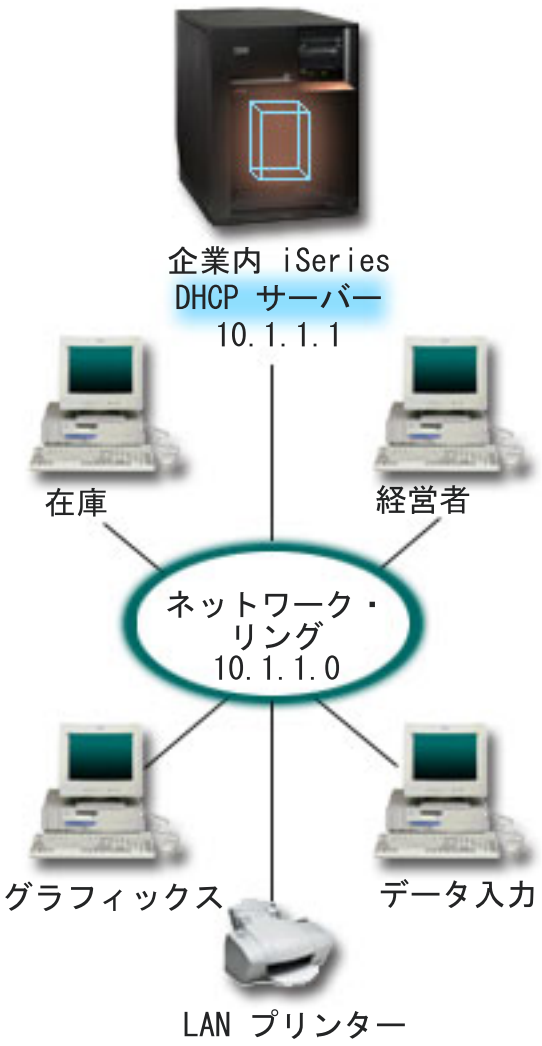


図 2. iSeries サーバーのための単純な LAN セットアップ

PC クライアントの数がこのくらい少ないと、管理者は、あまり動かずに各 PC の IP 情報を容易に入力できます。この場合、管理者に必要なことは、4 台の PC のところへ行くことだけです。 4 台の PC が 200 台の PC に増えたとします。こうなると、各 PC の IP 情報をセットアップするだけでも時間のかかる作業であり、正確さが欠ける場合も出てきます。 DHCP により、IP 情報をクライアントに割り当てるプロセスが単純化されます。 サブネット 10.1.1.0 に数百台のクライアントがある場合でも、管理者は、iSeries サーバー上で DHCP ポリシーを 1 つ作成するだけで済みます。このポリシーが、各クライアントに IP 情報を配布します。

PC クライアントがそれぞれの DHCP DISCOVER 信号を発信すると、iSeries サーバーは、適切な IP 情報を使って応答します。この例では、会社には、その IP 情報の取得にも DHCP を使う、LAN ベースのプリンターも装備されています。 PC クライアントはプリンターの IP アドレスが同じままであるかどうかで左右されるため、ネットワーク管理者は、DHCP ポリシーでその旨を明らかにする必要があります。このソリューションの 1 つは、プリンターに定数 IP アドレスを割り当てることです。 DHCP サーバーにより、クライアントの MAC アドレスを使って、LAN プリンターと同様に DHCP ポリシーにクライアントを定義できます。 DHCP クライアント定義で、IP アドレスやルーター・アドレスといった特定の値を目的のクライアントに割り当てることができます。

クライアントが TCP/IP ネットワークと通信するためには、少なくとも IP アドレスとサブネット・マスクが必要です。クライアントがそれぞれの IP アドレスを DHCP サーバーから取得すると、DHCP サーバーは、構成オプションを使用して、詳細な構成情報 (たとえば、それぞれのサブネット・マスクなど) を渡します。

単純な LAN のための DHCP セットアップの計画

表 2. グローバル構成オプション (DHCP サーバーがサービスするすべてのクライアントに適用されます)。

オブジェクト	**値**
構成オプション オプション 1: サブネット・マスク オプション 6: ドメイン・ネーム・サーバー オプション 15: ドメイン・ネーム	 255.255.255.0 10.1.1.1 mycompany.com
サーバーによる割り当てではないサブネット・アドレス	10.1.1.1 (ドメイン・ネーム・サーバー)
サーバーは、DNS 更新を実行していますか?	No
サーバーは、BOOTP クライアントをサポートしていますか?	No

表 3. PC のためのサブネット

オブジェクト	**値**
サブネット名	SimpleSubnet
管理するアドレス	10.1.1.2 - 10.1.1.150
リース時間	24 時間 (デフォルト)
構成オプション 継承されるオプション	グローバル構成からのオプション

表 4. プリンターのためのクライアント

オブジェクト	**値**
クライアント名	LANPrinter
クライアント・アドレス	10.1.1.5
構成オプション 継承されるオプション	グローバル構成からのオプション

関連資料

30 ページの『例: 複数の TCP/IP サブネット』
DHCP 対応のルーターによって接続される 2 つの LAN を備えた DHCP サーバーとして iSeries サーバーをセットアップする方法について説明します。

32 ページの『例: DHCP とマルチホーミング』
インターネット・ルーターによってインターネットに接続される LAN のための DHCP サーバーとして iSeries サーバーをセットアップする方法について説明します。

例: 複数の TCP/IP サブネット

DHCP 対応のルーターによって接続される 2 つの LAN を備えた DHCP サーバーとして iSeries サーバーをセットアップする方法について説明します。

この例は、追加の TCP/IP サブネットがあること以外、前の例、単純な DHCP サブネットと同じです。オフィスとデータ入力クライアントがオフィス建物の別のフロアにあり、ルーターで分離されているものとします。ネットワーク管理者が、すべてのクライアントに、DHCP を介してそれぞれの IP 情報を受信させたいと考えている場合、この状態では、単純な DHCP サブネットとの固有の違いがいくつか出ます。次の図は、ネットワーク間でルーターを使用する 2 つの LAN に接続されている iSeries DHCP サーバーのネットワーク・レイアウト例を示しています。図では、複雑にならないように、クライアントの数を意図的に制限しています。実際の使用状態では、各サブネットにかなりの数のクライアントが装備されています。

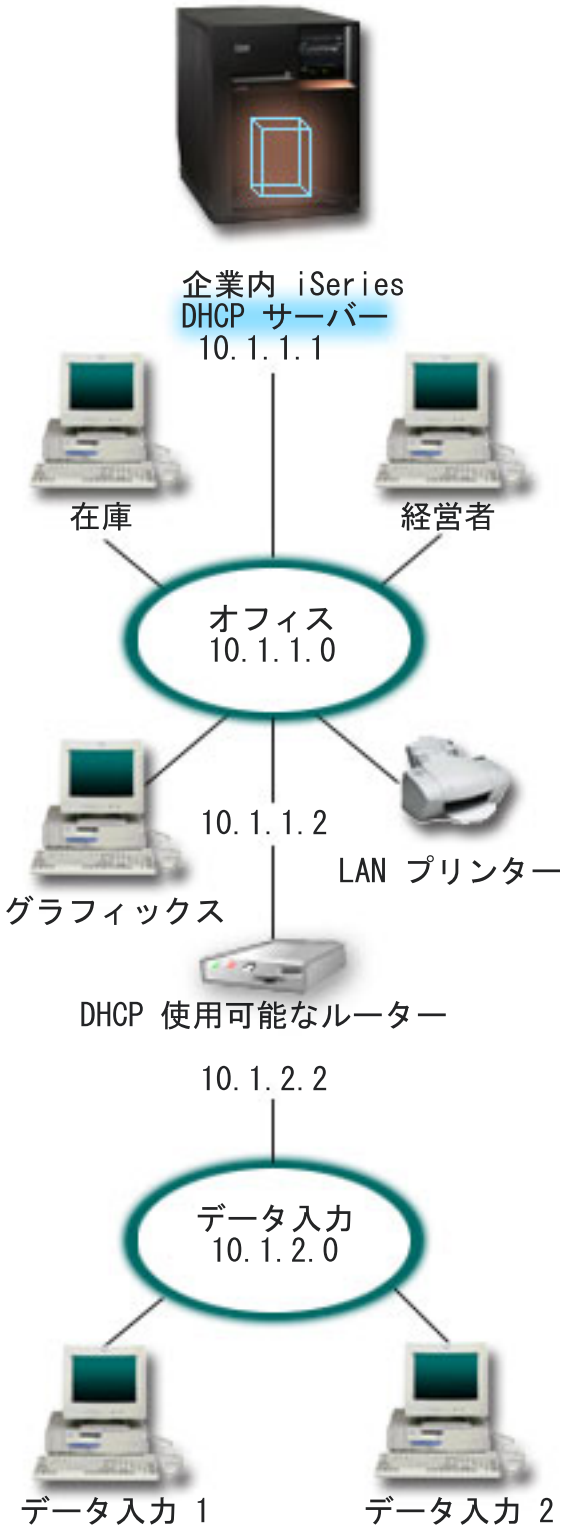


図 3. 複数の LAN をルーターを介して接続した場合

2 つのネットワークを接続するルーターは、DHCP DISCOVER パケットを渡すことができるものでなければなりません。そうでないと、データ入力クライアントは、IP 情報を受信したり、ネットワークにアクセスすることができません。また、DHCP ポリシーでは、データ入力およびオフィス・サブネット用に 1 つ

ずつ、合計 2 つのサブネット定義が必要になります。最小限、サブネット間の違いは、IP サブネットとルーター・アドレスです。データ入力サブネットは、オフィス・サブネットと通信するために、10.1.2.2 というルーター・アドレスを受信する必要があります。

複数の LAN のための DHCP セットアップの計画

表 5. グローバル構成オプション (DHCP サーバーがサービスするすべてのクライアントに適用されます)。

オブジェクト		**値**
構成オプション	オプション 1: サブネット・マスク	255.255.255.0
	オプション 6: ドメイン・ネーム・サーバー	10.1.1.1
	オプション 15: ドメイン・ネーム	mycompany.com
サーバーによる割り当てではないサブネット・アドレス		10.1.1.1 (ドメイン・ネーム・サーバー)
サーバーは、DNS 更新を実行していますか?		No
サーバーは、BOOTP クライアントをサポートしていますか?		No

表 6. オフィス・クライアントのためのサブネット

オブジェクト		**値**
サブネット名		Office
管理するアドレス		10.1.1.3 - 10.1.1.150
リース時間		24 時間 (デフォルト)
構成オプション	オプション 3: ルーター	10.1.1.2
	継承されるオプション	グローバル構成からのオプション
サーバーによる割り当てではないサブネット・アドレス		10.1.1.2 (ルーター)

表 7. データ入力クライアントのためのサブネット

オブジェクト		**値**
サブネット名		DataEntry
管理するアドレス		10.1.2.3 - 10.1.2.150
リース時間		24 時間 (デフォルト)
構成オプション	オプション 3: ルーター	10.1.2.2
	継承されるオプション	グローバル構成からのオプション
サーバーによる割り当てではないサブネット・アドレス		10.1.2.2 (ルーター)

関連資料

27 ページの『例: 単純な DHCP サブネット』
4 つの PC クライアントと 1 台の LAN ベース・プリンターを備えた単純な LAN 内の DHCP サーバーとして iSeries サーバーをセットアップする場合について説明します。

例: DHCP とマルチホーミング

インターネット・ルーターによってインターネットに接続される LAN のための DHCP サーバーとして iSeries サーバーをセットアップする方法について説明します。

この例は、最初の例、単純な DHCP サブネットと非常によく似ています。この例では、データ入力クライアントは、クライアント相互および iSeries サーバーとの間で通信しているだけです。クライアントは、IP 情報を iSeries の DHCP サーバーから動的に取得します。

ただし、クライアントの新しいバージョンのデータ入力アプリケーションではネットワークがインターネットと通信することが必須であるため、会社は、図 4-1 に示されているとおり、インターネット・ルーターを介してインターネットにアクセスできるようにしました。管理者は、ルーターのほかに、インターネットと通信するために IP アドレスをもつインターフェースをもう 1 つ追加しました。同じアダプターに複数の IP アドレスが割り当てられると、iSeries サーバーはマルチホーミングです。

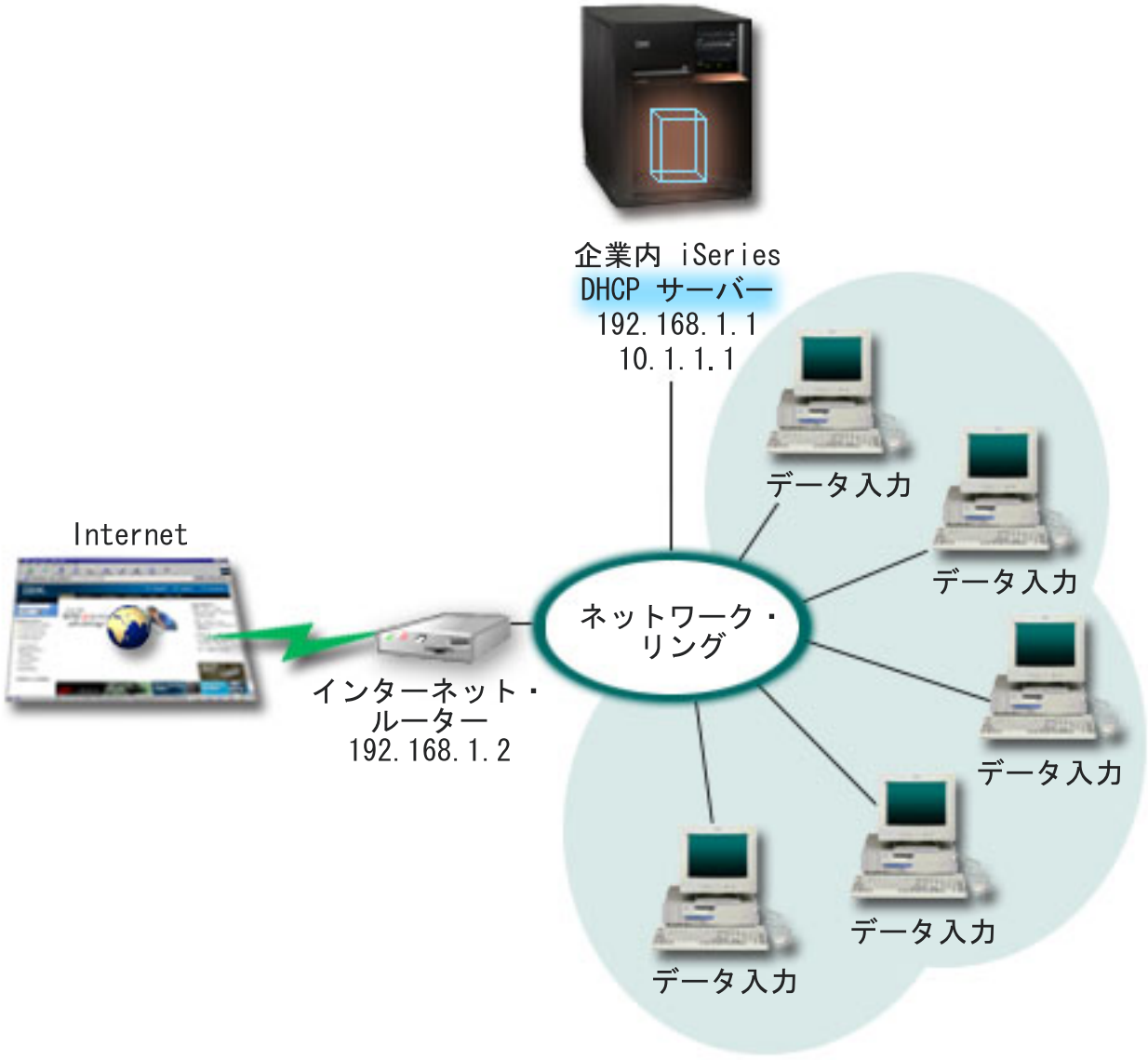


図 4. 同じアダプターに複数の IP アドレスが割り当てられている DHCP の使用法

注: これは、ネットワークをインターネットに接続する実現可能な仕組みですが、安全度の高いものではありません。この仕組みは、この DHCP 例の目的には適していますが、ご自分の DHCP サーバーを構成する際にはセキュリティーの意味を考慮してください。

DHCP セットアップは、iSeries サーバーが 2 つの異なる IP アドレスで認識されていることを考慮する必要があります。このシナリオに合わせて DHCP を正しくセットアップする方法を理解するには、クライアントが DHCP DISCOVER パケットを送信したときにどうなるかを理解しておくと役に立ちます。

クライアントが DHCP DISCOVER パケットを送信すると、リングでブロードキャストされます。そのため、iSeries サーバーは、パケットがどの IP を目指していたのか判別できません。このパケットに 10.1.1.1 インターフェース IP (DHCP に使用されたもの) が示されていれば、クライアントは、予想どおりに IP 情報を受信します。しかし、実際には、パケットに 192.168.1.1 アドレス (インターネットに接続されたもの) が示される可能性があります。このパケットが 192.168.1.1 インターフェースで受信された場合、データ入力クライアントは IP 情報を受信しません。

この状態で DHCP をセットアップするには、データ入力 DHCP サブネットを作成するだけでなく、インターネット・ネットワークのためのものも作成する必要があります。インターネット・ポリシーは、使用可能なアドレスをもたないサブネットで構成されています。インターネット・ネットワークのためのものを作成する最も簡単な方法は、IP アドレスを少なくとも 1 つ (192.168.1.1 など) 使ってサブネットを定義し、その同じ IP アドレスを除外することです。サブネットが 2 つ定義されたら、その 2 つ (またはそれ以上) のサブネットを結合して、1 つのサブネット・グループにします。DISCOVER パケットに 192.168.1.1 インターフェースが示されている場合、データ入力サブネットは、引き続き有効な IP 情報を送出します。

このシナリオを機能させるには、データ入力サブネットのポリシーが、インターネットにアクセスするためにそのクライアントにルーター・アドレスを渡す必要があります。この場合、ルーター・アドレスは 10.1.1.1 という iSeries インターフェースです。さらに、2 つのインターフェースが互いにパケットの経路を指定するために、IP データグラム転送を「on (オン)」に設定することも必要です。この例では、予約済み IP アドレスを使用して、内部 IP アドレスと外部 IP アドレスの両方を表します。ご使用のネットワークがこのシナリオと同じである場合は、データ入力クライアントがインターネットと通信するために NAT を使用することも必要です。

このマーキング問題を回避するためにサブネット・グループを使用することは、マルチホーミングの例だけに限ったことではありません。複数のインターフェースが同じネットワークに接続していればいつでも、同じ問題にぶつかる可能性があります。次の図は、iSeries サーバーがデータ入力ネットワークへの物理接続を 2 つもつ方法を示しています。このネットワーク構成では、マルチホーミング・セットアップと同じ DHCP グループ・ポリシーが必要です。DHCP DISCOVER パケットは、192.168.1.1 インターフェースによって応答される可能性があるためです。

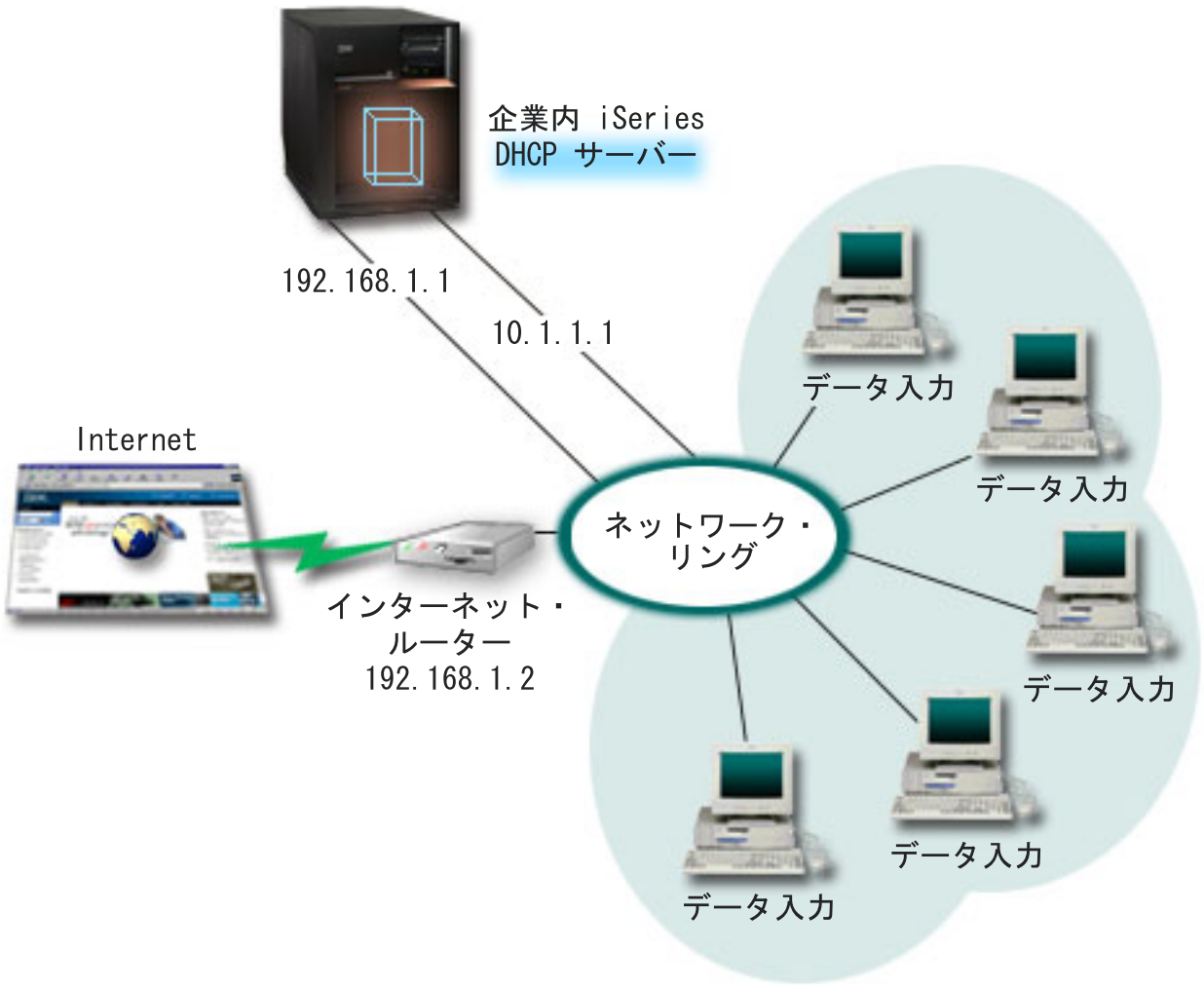


図 5. 複数のインターフェースが同じネットワークに接続されている DHCP の使用法

マルチホーミングのための DHCP セットアップの計画

表 8. グローバル構成オプション (DHCP サーバーがサービスするすべてのクライアントに適用されます)。

オブジェクト	値
サーバーは、DNS 更新を実行していますか?	No
サーバーは、BOOTP クライアントをサポートしていますか?	No

表 9. データ入力クライアントのためのサブネット

オブジェクト	値
サブネット名	データ入力
管理するアドレス	10.1.1.2 - 10.1.1.150
リース時間	24 時間 (デフォルト)

表 9. データ入力クライアントのためのサブネット (続き)

オブジェクト		値
構成オプション	オプション 1: サブネット・マスク	255.255.255.0
	オプション 3: ルーター	10.1.1.1
	オプション 6: ドメイン・ネーム・サーバー	10.1.1.1
	オプション 15: ドメイン・ネーム	mycompany.com
サーバーによる割り当てではないサブネット・アドレス		10.1.1.1 (ルーター、DNS サーバー)

表 10. インターネット・クライアントのためのサブネット (空のサブネット)

オブジェクト	値
サブネット名	Internet
管理するアドレス	192.168.1.1 - 192.168.1.1
サーバーによる割り当てではないサブネット・アドレス	192.168.1.1 (すべての IP アドレスが使用可能)

表 11. すべての着信 DISCOVER パケットのためのサブネット・グループ

オブジェクト	値
サブネット・グループ名	Multihomed
グループに組み込まれるサブネット	サブネット Internet サブネット DataEntry

その他のセットアップ

- 2 つのインターフェースのために IP データグラム転送を「on (オン)」に設定する
- データ入力クライアント用に NAT をセットアップする

関連概念

58 ページの『問題: クライアントが IP アドレスまたはその構成情報を受信しない』
クライアントが IP アドレスまたはその構成情報を受信できない場合、問題が発生する可能性があります。 IP アドレスは、クライアントと DHCP サーバー間の 4 ステップからなるプロセスを経て、クライアントにリースされます。

関連資料

27 ページの『例: 単純な DHCP サブネット』
4 つの PC クライアントと 1 台の LAN ベース・プリンターを備えた単純な LAN 内の DHCP サーバーとして iSeries サーバーをセットアップする場合について説明します。

例: DNS と DHCP が同じ iSeries サーバー上にある場合

単純な LAN のための動的 DNS 更新を備えた DHCP サーバーとして iSeries サーバーをセットアップする方法について説明します。

図 6 は、単純なサブネットの場合に iSeries サーバーが DHCP および DNS サーバーとして機能する方法を示しています。この作業環境では、在庫、データ入力、および経営者の各クライアントはグラフィックス・ファイル・サーバーからのグラフィックスを使って文書を作成するものとします。それらのクライアントは、ホスト名のネットワーク・ドライブにより、グラフィックス・ファイル・サーバーに接続します。

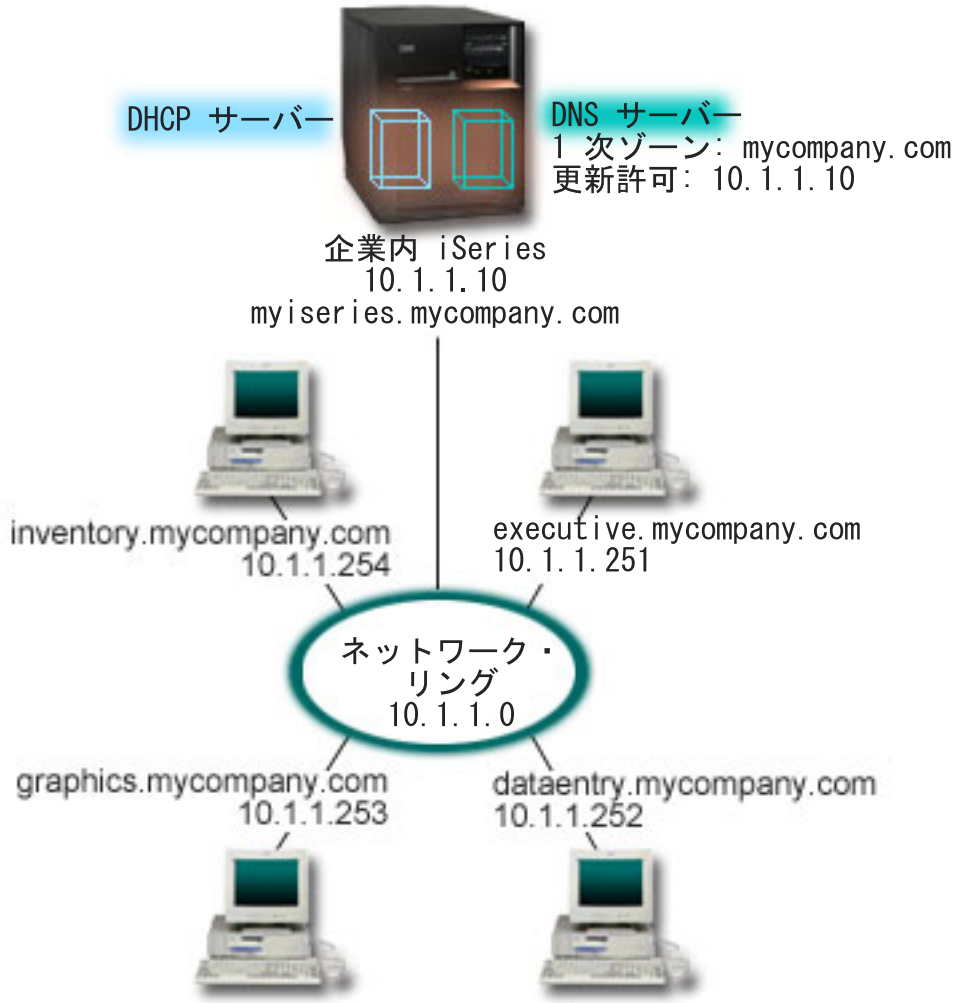


図 6. 動的 DNS および DHCP

以前のバージョンの DHCP および DNS は、互いに独立していました。 DHCP が新しい IP アドレスをクライアントに割り当てると、管理者が手動で DNS レコードの更新を行わなければなりませんでした。この例で、グラフィックス・ファイル・サーバーの IP アドレスが、DHCP による割り当てのために変更された場合、その従属クライアントはネットワーク・ドライブをホスト名にマップできません。 DNS レコードには、ファイル・サーバーの以前の IP アドレスが入っているためです。

V5R1 の新しい DNS サーバーでは、DHCP による断続的なアドレスの変更に連動して、DNS レコードを動的に更新することができます。たとえば、グラフィックス・ファイル・サーバーがそのリースを更新し、DHCP により 10.1.1.250 という IP アドレスを割り当てられると、関連する DNS レコードは動的に更新されます。これにより、その他のクライアントは、中断なしで、ホスト名でグラフィックス・ファイル・サーバーについて DNS サーバーを照会することができます。

アドレス・マッピング (A) レコード上および逆検索ポインター (PTR) レコード上のリソース・レコードをクライアントに代わって更新するように、DHCP を構成できます。 A レコードは、クライアントのホスト名をその IP アドレスにマップします。 PTR レコードは、クライアントの IP アドレスをそのホスト名にマップします。 動的に更新されるレコードごとに、関連テキスト (TXT) レコードが作成され、そのレコードが DHCP によって作成されたことが示されます。 DHCP に A レコードと PTR レコードの両方の更新を許すのか、または PTR レコードのみの更新を許すのかを選択できます。動的更新を受け入れるよう DNS を構成する方法についての詳細は、DNS トピックの「例: DNS と DHCP が同じ iSeries サーバー上にある場合」を参照してください。

注: PTR レコードだけを更新するように DHCP を設定する場合は、各クライアントからのその A レコードの更新ができるように DNS を構成する必要があります。すべての DHCP クライアントで、その固有の更新要求レコードの作成がサポートされるわけではありません。この方式を選ぶ前に、ご使用のクライアント・プラットフォームの資料を参照してください。

DNS 更新を使用可能にするには、ご使用の DHCP サーバーのための DNS キーを作成する必要があります。 DNS キーは、配布した IP アドレスに基づいて DHCP サーバーが DNS レコードを更新することを許可します。その場合、DHCP 構成では、DNS 更新を発生させたい有効範囲レベルを選んでください。たとえば、すべてのサブネットに DNS 更新を実行させたい場合は、更新をグローバル・レベルに設定してください。 1 つのサブネットだけに更新を実行させたい場合は、そのサブネットだけを更新に設定してください。

動的 DNS を使用した場合の DHCP セットアップの計画

表 12. グローバル構成オプション (DHCP サーバーがサービスするすべてのクライアントに適用されます)。

オブジェクト		**値**
構成オプション	オプション 1: サブネット・マスク	255.255.255.0
	オプション 6: ドメイン・ネーム・サーバー	10.1.1.10
	オプション 15: ドメイン・ネーム	mycompany.com
サーバーは、DNS 更新を実行していますか?		Yes -- A レコードと PTR レコードの両方
サーバーは、BOOTP クライアントをサポートしていますか?		No

表 13. ネットワーク・リングのためのサブネット

オブジェクト		**値**
サブネット名		NetworkSubnet
管理するアドレス		10.1.1.250 - 10.1.1.254
リース時間		24 時間 (デフォルト)
構成オプション	継承されるオプション	グローバル構成からのオプション

その他のセットアップ:

DHCP が更新を DNS に送信することを許可する。例: DNS と DHCP が同じ iSeries サーバー上にある場合を参照してください。

関連資料

39 ページの『例: DNS と DHCP が異なる iSeries サーバー上にある場合』
単純な LAN を介して動的更新を実行するために、2 つの異なる iSeries サーバー上に DHCP と DNS をセットアップする方法について説明します。

例: DNS と DHCP が異なる iSeries サーバー上にある場合

単純な LAN を介して動的更新を実行するために、2 つの異なる iSeries サーバー上に DHCP と DNS をセットアップする方法について説明します。

次の図は、DNS および DHCP サーバーが別個の iSeries サーバー上で稼動している小型のサブネット・ネットワークについて説明します。 DNS を実行する iSeries サーバーは、DNS と DHCP が同じ iSeries 上にある場合と同様に構成されます。ただし、動的更新を送信するよう DHCP サーバーを構成するステップがいくつか追加されています。

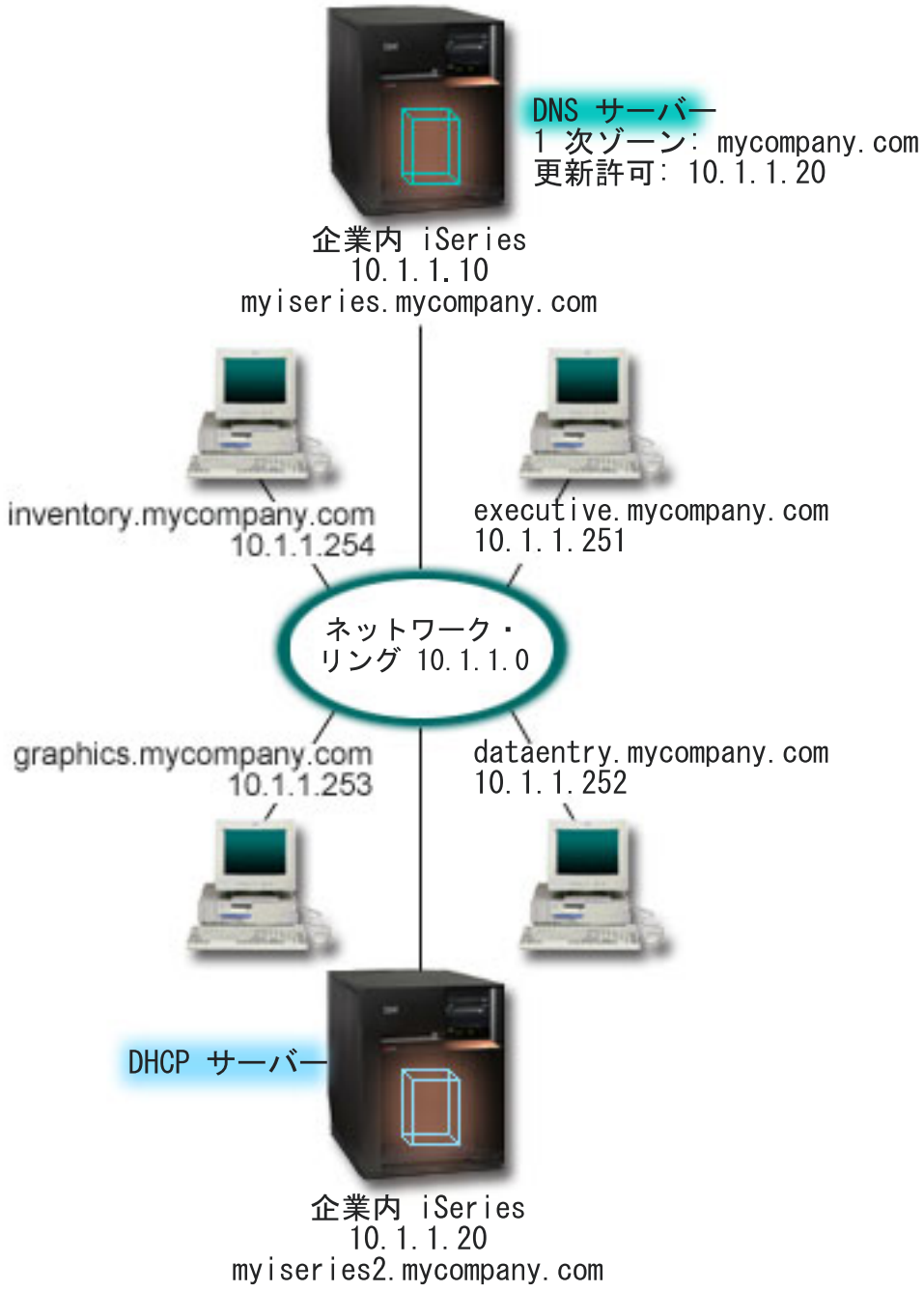


図 7. DNS と DHCP が異なる iSeries サーバー上にある場合

動的 DNS を使用した場合の DHCP セットアップの計画

グローバル構成オプションおよびサブネットの設定の例については、 36 ページの『例: DNS と DHCP が同じ iSeries サーバー上にある場合』 を参照してください。

その他のセットアップ:

i5/OS™ (オプション 31) のインストール。(ドメイン・ネーム・システム)
DHCP を実行する iSeries サーバー (この場合は、myiseries2) 上に i5/OS (オプション 31) をインストールしてください。このオプションには、リソース・レコード更新プロセスを管理する動的更新 API が組み込まれています。インストール手順については、DNS システム要件を参照してください。

DHCP が更新を DNS に送信することを許可する。
DHCP サーバーが DNS サーバーに更新を送信することを許可する必要があります。動的更新キーの定義プロセスを繰り返すか、目的のファイルを送信して、それを適切なディレクトリー・パスに入れます。

動的更新キーを両方の iSeries サーバー上に作成するには、次のステップに従ってください。

1. **iSeries ナビゲーター**で、「**使用する iSeries サーバー**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**DNS**」と展開します。
2. 左側の画面区画で、「**DNS**」を右マウス・ボタン・クリックして、「**動的更新キーの管理**」を選択します。
3. 「**動的更新キーの管理**」ページで、「**追加**」を選択します。
4. 「**動的更新キーの追加**」ページで、次のフィールドを記入します。
   - **キー名**: キーの名前 (たとえば、mycompany.key) を指定します。キー名は、ドットで終わる必要があります。
   - **動的更新ゾーン**: このキーが有効であるゾーン名を指定します。ゾーンは、複数個指定できます。
   - **生成キー**: 秘密鍵を生成するのに使用する方式を選択してください。
5. DNS を実行する iSeries と DHCP を実行する iSeries の両方に同じキーが定義されるように、上のステップを繰り返してください。

関連タスク

DNS システム要件

関連資料

36 ページの『例: DNS と DHCP が同じ iSeries サーバー上にある場合』
単純な LAN のための動的 DNS 更新を備えた DHCP サーバーとして iSeries サーバーをセットアップする方法について説明します。

API の動的更新

例: PPP と DHCP が単一の iSeries サーバー上にある場合

1 つの LAN とリモート・ダイヤルイン・クライアントのための DHCP サーバーとして iSeries サーバーをセットアップする方法について説明します。

ダイヤルイン・クライアントなどのリモート・クライアントは、会社のネットワークに頻繁にアクセスする必要があります。ダイヤルイン・クライアントは、iSeries サーバーには PPP を使ってアクセスできます。ネットワークにアクセスするには、ダイヤルイン・クライアントは、他の直接接続ネットワーク・クライアントと同様、IP 情報が必要です。 iSeries DHCP サーバーは、他のあらゆる直接接続クライアントと同様

に、PPP ダイヤルイン・クライアントに IP アドレス情報を配布できます。次の図は、作業を行うのに会社のネットワークにダイヤルインしなければならない、遠隔地にいる従業員を示しています。

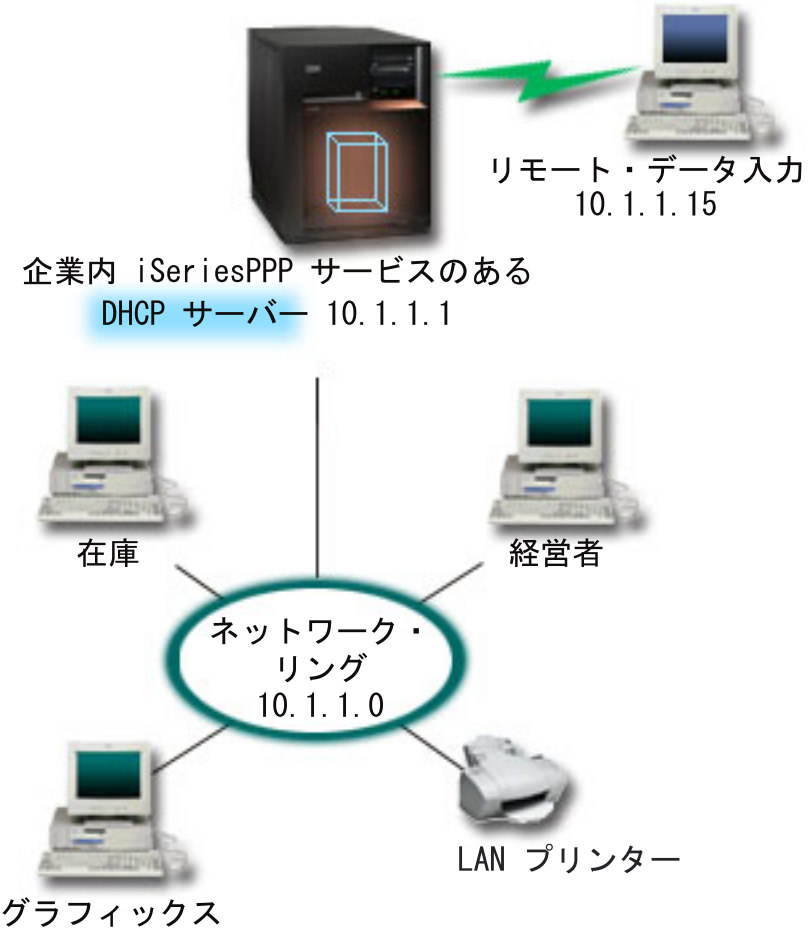


図 8. PPP と DHCP が単一の iSeries サーバー上にある場合

遠隔地にいる従業員が正常に会社のネットワークの一部になるためには、iSeries サーバーがリモート・アクセス・サービスと DHCP を組み合わせて使用する必要があります。 iSeries サーバーのためのダイヤルイン能力は、リモート・アクセス・サービス機能によって作成されます。正しくセットアップされていれば、作業者がダイヤルイン接続を確立すると、PPP サーバーが、TCP/IP 情報をその作業者に配布するよう DHCP サーバーに通知します。

この例では、1 つの DHCP サブネット・ポリシーが、オンサイト・ネットワーク・クライアントとダイヤルイン・クライアントの両方を扱います。

IP 配布について、PPP プロファイルに DHCP の指図に従わせたい場合は、その旨を PPP プロファイルで指示する必要があります。受信側接続プロファイルの TCP/IP 設定で、リモート IP アドレス割り当て方式を「Fixed (固定)」から「DHCP」に設定する必要があります。ダイヤルイン・クライアントが他のネットワーク・クライアント (たとえば LAN プリンター) と通信できるようにするには、プロファイルの TCP/IP 設定と TCP/IP 構成 (スタック) 特性で IP 転送を許可することも必要です。 IP 転送を PPP プロファイルでのみ「on (オン)」に設定した場合、iSeries サーバーは IP パケットを渡しません。プロファイルとスタックの両方で IP 転送を「on (オン)」に設定する必要があります。

また、PPP プロファイル内のローカル・インターフェース IP アドレスも、DHCP サーバー内のサブネット定義にある IP アドレスでなければなりません。この例では、PPP プロファイルのローカル・インターフェース・アドレスは 10.1.1.1 になります。このアドレスを、DHCP サーバーのアドレス・プールから除外しておくことも必要です。そうすれば、DHCP クライアントに割り当てられることはありません。

オンサイトおよび PPP クライアントのための DHCP セットアップの計画

表 14. グローバル構成オプション (DHCP サーバーがサービスするすべてのクライアントに適用されます)。

オブジェクト		**値**
構成オプション	オプション 1: サブネット・マスク	255.255.255.0
	オプション 6: ドメイン・ネーム・サーバー	10.1.1.1
	オプション 15: ドメイン・ネーム	mycompany.com
サーバーは、DNS 更新を実行していますか?		No
サーバーは、BOOTP クライアントをサポートしていますか?		No

表 15. オンサイトおよびダイヤルイン・クライアントのためのサブネット

オブジェクト		**値**
サブネット名		MainNetwork
管理するアドレス		10.1.1.3 - 10.1.1.150
リース時間		24 時間 (デフォルト)
構成オプション	継承されるオプション	グローバル構成からのオプション
サーバーによる割り当てではないサブネット・アドレス		10.1.1.1 (iSeries ナビゲーター内の受信側接続プロファイル特性の TCP/IP 設定に指定されたローカル・インターフェース・アドレス)

その他のセットアップ

- PPP 受信側接続プロファイルでリモート IP アドレス方式を DHCP に設定する。
  1. iSeries ナビゲーターのリモート・アクセス・サービスの「サービス」メニュー項目を使用して、DHCP サーバーとの DHCP WAN クライアント接続または中継接続を使用可能にします。
  2. iSeries ナビゲーターの受信側接続プロファイルの TCP/IP 設定特性の下で、DHCP を IP アドレス割り当て方式に使用するよう選択します。
- iSeries ナビゲーターの受信側接続プロファイルの TCP/IP 設定特性の下で、リモート・システムが他のネットワークにアクセス (IP 転送) できるようにする。
- iSeries ナビゲーターの TCP/IP 構成の設定特性の下で、IP データグラム転送を使用可能にする。

関連概念

47 ページの『ネットワーク・トポロジーに関する考慮事項』
大部分の DHCP セットアップは、ネットワーク・トポロジー、ネットワーク上の装置 (たとえば、ルーター)、DHCP でクライアントをどのようにサポートしたいかを考えることで計画できます。

関連資料

43 ページの『例: DHCP と PPP プロファイルが異なる iSeries サーバー上にある場合』
2 つの LAN とリモート・ダイヤルイン・クライアントのためのネットワーク DHCP サーバーおよび DHCP/BOOTP リレー・エージェントとして 2 台の iSeries サーバーをセットアップする方法について説明します。

例: DHCP と PPP プロファイルが異なる iSeries サーバー上にある場合

2 つの LAN とリモート・ダイヤルイン・クライアントのためのネットワーク DHCP サーバーおよび DHCP/BOOTP リレー・エージェントとして 2 台の iSeries サーバーをセットアップする方法について説明します。

前の例 PPP と DHCP が単一の iSeries サーバー上にある場合では、PPP と DHCP を 1 つの iSeries サーバー上で使用して、ダイヤルイン・クライアントがネットワークにアクセスできるようにする方法を説明しています。ネットワークの物理的レイアウトであれ、セキュリティー関連のことであれ、PPP サーバーと DHCP サーバーを分離させるか、または DHCP サービスを受けない専用の PPP サーバーを別個にもつ方が望ましいといえます。次の図は、ダイヤルイン・クライアントはもっているが、PPP と DHCP ポリシーは別々のサーバー上にあるネットワークを示しています。

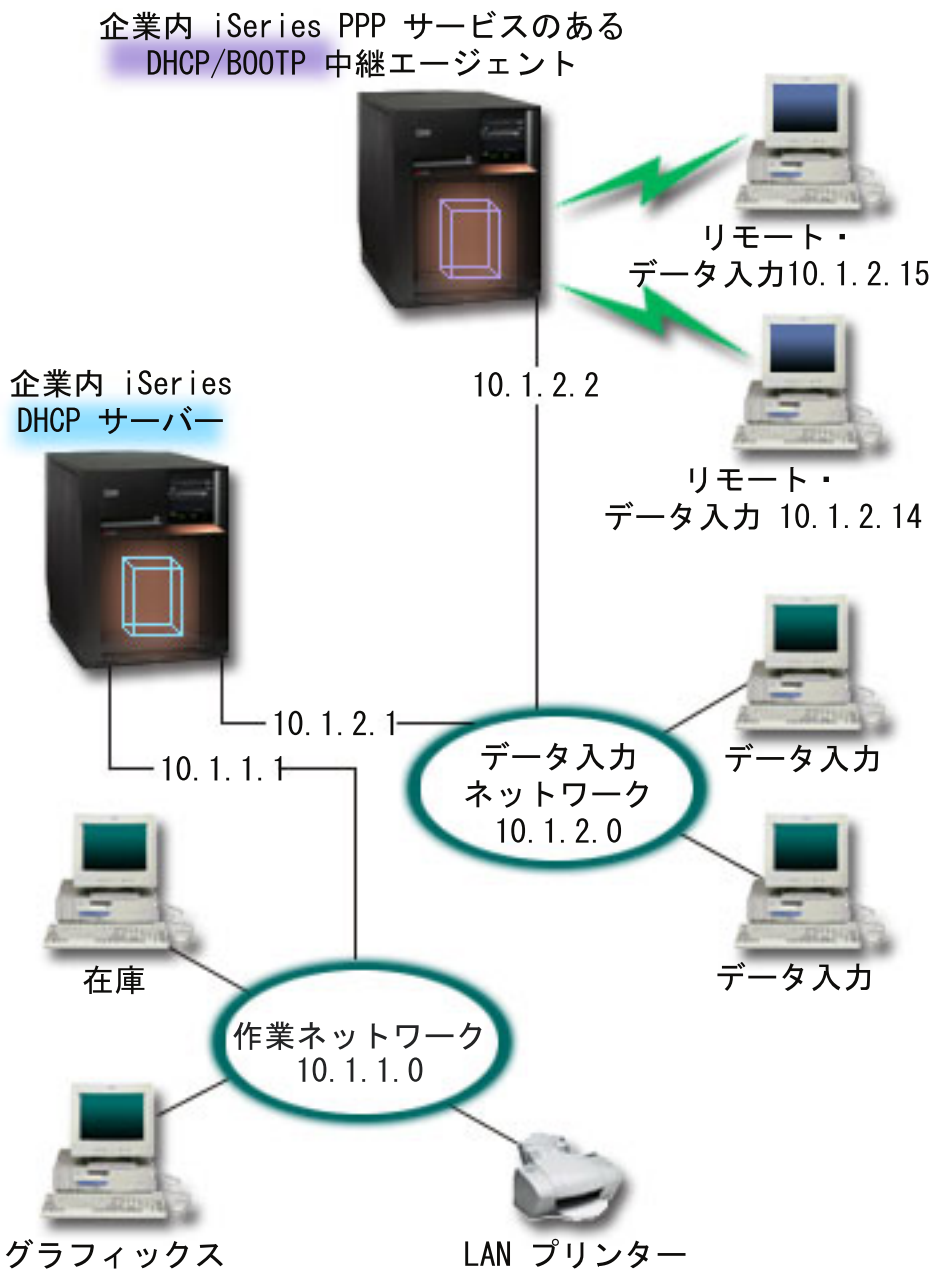


図 9. DHCP と PPP プロファイルが異なる iSeries サーバー上にある場合

リモート・データ入力クライアントは、ダイヤルインで iSeries PPP サーバーに入ります。そのサーバー上の PPP プロファイルは、PPP プロファイルと TCP/IP スタック特性に IP 転送が入っているだけでなく、前の例の場合と同様、DHCP のリモート IP アドレス方式も持っている必要があります。さらに、このサーバーは DHCP リレー・エージェントとして機能しているため、BOOTP/DHCP リレー・エージェント TCP/IP サーバーがオンになっている必要があります。このことにより、iSeries リモート・アクセス・サーバーは、DHCP DISCOVER パケットを DHCP サーバーに引き渡すことができます。引き渡しがあると、DHCP サーバーは、PPP サーバーを通じてダイヤルイン・クライアントに応答して TCP/IP 情報を配布します。

DHCP サーバーは、10.1.1.0 ネットワークと 10.1.2.0 ネットワークの両方に IP アドレスを配布する責任があります。データ入力ネットワークでは、10.1.2.10 から 10.1.2.40 までの IP アドレスをダイヤルイン・

クライアントまたは直接接続ネットワーク・クライアントに割り当てます。データ入力クライアントでは、作業ネットワークと通信するために 10.1.2.1 というルーター・アドレス (オプション 3) も必要であり、iSeries DHCP サーバーは、IP 転送も使用可能にしておく必要があります。

また、PPP プロファイル内のローカル・インターフェース IP アドレスも、DHCP サーバー内のサブネット定義にある IP アドレスでなければなりません。この例では、PPP プロファイルのローカル・インターフェース・アドレスは 10.1.2.2 になります。このアドレスを、DHCP サーバーのアドレス・プールから除外しておくことも必要です。そうすれば、DHCP クライアントに割り当てられることはありません。ローカル・インターネット IP アドレスは、DHCP サーバーが応答パケットを送信できるアドレスでなければなりません。

DHCP リレー・エージェントをもつ DHCP のための DHCP セットアップの計画

表 16. グローバル構成オプション (DHCP サーバーがサービスするすべてのクライアントに適用されます)。

オブジェクト		**値**
構成オプション	オプション 1: サブネット・マスク	255.255.255.0
	オプション 6: ドメイン・ネーム・サーバー	10.1.1.1
	オプション 15: ドメイン・ネーム	mycompany.com
サーバーは、DNS 更新を実行していますか?		No
サーバーは、BOOTP クライアントをサポートしていますか?		No

表 17. 作業ネットワークのためのサブネット

オブジェクト		**値**
サブネット名		WorkNetwork
管理するアドレス		10.1.1.3 - 10.1.1.150
リース時間		24 時間 (デフォルト)
構成オプション	継承されるオプション	グローバル構成からのオプション
サーバーによる割り当てではないサブネット・アドレス		なし

表 18. データ入力ネットワークのためのサブネット

オブジェクト		**値**
サブネット名		DataEntry
管理するアドレス		10.1.2.10 - 10.1.2.40
リース時間		24 時間 (デフォルト)
構成オプション	オプション 3: ルーター	10.1.2.1
	継承されるオプション	グローバル構成からのオプション
サーバーによる割り当てではないサブネット・アドレス		10.1.2.1 (ルーター) 10.1.2.15 (リモート・データ入力クライアントのローカル・インターフェース IP アドレス) 10.1.2.14 (リモート・データ入力クライアントのローカル・インターフェース IP アドレス)

PPP を実行する iSeries サーバー上での、その他のセットアップ

- BOOTP/DHCP リレー・エージェント TCP/IP サーバーをセットアップする

オブジェクト	値
インターフェース・アドレス	10.1.2.2
サーバー IP アドレスへの中継パケット	10.1.2.1

- PPP 受信側接続プロファイルでリモート IP アドレス方式を DHCP に設定する。
  1. iSeries ナビゲーターのリモート・アクセス・サービスの「サービス」メニュー項目を使用して、DHCP サーバーとの DHCP WAN クライアント接続または中継接続を使用可能にします。
  2. iSeries ナビゲーターの受信側接続プロファイルの TCP/IP 設定特性の下で、DHCP を IP アドレス割り当て方式に使用するよう選択します。
- iSeries ナビゲーターの受信側接続プロファイルの TCP/IP 設定特性の下で、リモート・システムが他のネットワークにアクセス (IP 転送) できるようにする (リモート・クライアントがデータ入力ネットワークと通信できるようにする)。
- iSeries ナビゲーターの TCP/IP 構成の設定特性の下で、IP データグラム転送を使用可能にする (リモート・クライアントがデータ入力ネットワークと通信できるようにする)。

関連概念

6 ページの『リレー・エージェントとルーター』
ネットワーク内で DHCP リレー・エージェントを使用する必要がある場合、またルーターで十分な場合があります。 DHCP リレー・エージェントとルーターの両方を使用して、効率良くしかも安全にネットワーク全体にデータを転送することができます。

47 ページの『ネットワーク・トポロジーに関する考慮事項』
大部分の DHCP セットアップは、ネットワーク・トポロジー、ネットワーク上の装置 (たとえば、ルーター)、DHCP でクライアントをどのようにサポートしたいかを考えることで計画できます。

関連資料

40 ページの『例: PPP と DHCP が単一の iSeries サーバー上にある場合』
1 つの LAN とリモート・ダイヤルイン・クライアントのための DHCP サーバーとして iSeries サーバーをセットアップする方法について説明します。

DHCP のための計画

ご使用のネットワークに合わせた DHCP のセットアップ方法の計画に必要な手順を説明します。

DHCP のセットアップは、DHCP サーバーをどのように構成すべきかを計画するのに時間をかけていなければ、時間のかかる、エラーの発生しやすいプロセスです。ネットワークのセットアップとセキュリティー関連の問題についてあらかじめ考慮する時間をとることにより、さらに効率良く、DHCP サーバーを構成することができます。以下に示すトピックでは、ネットワーク内で DHCP を構成する前に考慮すべき重要な問題点をいくつか提示します。

ネットワーク・トポロジーに関する考慮事項

大部分の DHCP セットアップは、ネットワーク・トポロジー、ネットワーク上の装置 (たとえば、ルーター)、DHCP でクライアントをどのようにサポートしたいかを考えるだけで計画できます。

セキュリティーに関する考慮事項

DHCP プロトコルは、IP アドレスを要求するクライアントがその要求を許可されているかを確認できません。ネットワークに対する DHCP の対話の性質により、ご使用の iSeries サーバーを外のクライアントから保護することは重要です。ご使用の DHCP サーバーが、トラステッド内部ネットワークの一部である iSeries サーバー上にある場合、パケット規則 (フィルター操作と NAT) を

使用すると、許可されていないパーティーからさらに保護することができます。ご使用の DHCP サーバーが、非トラステッド・ネットワーク (たとえば、インターネット) に接続されている iSeries サーバー上にある場合は、 iSeries およびインターネット・セキュリティー を参照してください。セキュリティーについてさらに詳しくは、Information Center のセキュリティーのトピックを参照してください。

関連概念

パケット・ルール (フィルター操作および NAT)

iSeries およびインターネット・セキュリティー

セキュリティー

関連タスク

57 ページの『DHCP のトラブルシューティング』
ジョブ・ログおよびトレース・データを表示できるだけでなく、一般的な問題のトラブルシューティング・リストを使用することもできます。

関連資料

51 ページの『DHCP の構成』
このトピックでは、DHCP サーバーおよびクライアントをセットアップする手順と、DNS に動的更新を送信するように DHCP を構成する手順を示しています。

ネットワーク・トポロジーに関する考慮事項

大部分の DHCP セットアップは、ネットワーク・トポロジー、ネットワーク上の装置 (たとえば、ルーター)、DHCP でクライアントをどのようにサポートしたいかを考えることで計画できます。

ネットワーク・トポロジーとは

DHCP のインプリメンテーションを計画する上で最も重要な局面の 1 つは、ご使用のネットワークのレイアウトつまりトポロジーを理解することです。ネットワーク・トポロジーが理解できると、DHCP の IP アドレス範囲、各クライアントに必要な構成情報、DHCP メッセージを転送するように構成する必要のある装置を短時間で識別でき、また、DHCP がご使用の DNS サーバーや PPP サーバーで動作するかどうかも理解できます。ご使用のネットワークの複雑さによっては、ネットワーク・トポロジーを紙面にスケッチすることが必要になる場合があります。すべての LAN、LAN を接続する装置、定義済みの IP アドレスを必要とする装置、およびクライアントの IP アドレスを含める必要があります。DHCP の例のいくつかを参考にすると、ネットワーク・トポロジーをスケッチする上で役立ちます。

DHCP サーバーの数の決定

複雑なネットワークの場合でも、すべてのネットワーク・クライアントを 1 台の DHCP サーバーだけで管理することができます。ネットワーク・トポロジーによっては、いくつかの DHCP/BOOTP リレー・エージェントをセットアップしたり、リレー・エージェントが動作するように、ルーターが DHCP パケットを転送できるようにする必要があります。

ネットワーク全体に対して DHCP サーバーを 1 台だけ使用すると、すべてのクライアントについてホスト構成管理が集中できます。ただし、ネットワーク内で複数の DHCP サーバーを使用することを考慮しなければならない場合があります。

SPOF (単一障害点) を回避するために、同一のサブネットを複数の DHCP サーバーが処理するように構成することができます。こうすると、あるサーバーに障害が起きても、別のサーバーがサブネットの処理を継続できます。それぞれの DHCP サーバーには、サブネットに直接接続するか、または DHCP/BOOTP リレー・エージェントを使用することによって、アクセス可能でなければなりません。

2 つの DHCP サーバーが同じアドレスを処理することはできないため、サブネットに定義されたアドレス・プールは、複数の DHCP サーバー間でも固有でなければなりません。したがって、特定のサブネットにサービスするために複数の DHCP サーバーを使用している場合、そのサブネットで使用されているアドレスの完全なリストが、複数のサーバー間で分割して所持されている必要があります。たとえば、あるサーバーを、サブネットに使用可能なアドレスの 70 % からなるアドレス・プールで構成し、もう 1 つのサーバーを、使用可能なアドレスの残りの 30 % からなるアドレス・プールで構成することができます。

複数の DHCP サーバーを使用すると、DHCP 関連のネットワーク・アクセス障害の発生する可能性は減少しますが、まったく障害が発生しないことは保証できません。特定のサブネットの DHCP サーバーに障害が起こった場合、もう一方の DHCP サーバーは、使用可能なアドレスの限られたプールを使い尽くす可能性があるなどの理由で、新しいクライアントからのすべての要求をサポートできないことがあります。

複数の DHCP サーバーを考えている場合、複数の DHCP サーバーは同じアドレスを共用できないことに注意してください。ネットワークで複数の DHCP サーバーを使用する場合、各サーバーを、それぞれ固有の IP アドレス範囲で構成する必要があります。

DHCP サーバーが管理しなければならない IP アドレスの識別

ネットワーク・トポロジーを使用して、DHCP サーバーに管理させたいネットワーク・アドレス範囲の文書化を始めてください。DHCP のアドレス・プールから除外しなければならない、手動で構成された IP アドレス (たとえば、ルーターの IP アドレス) をもつ装置を識別する必要があります。

さらに、これらのアドレスが DHCP サーバーによって動的に割り当てられるかどうか、また、特定の IP アドレスを特定のクライアントに割り当てたいかどうかも考慮する必要があります。ファイル・サーバーなど、特定のサブネット上の特定のクライアント用に、特定のアドレスと構成パラメーターを予約しなければならない場合があります。あるいは、すべてのクライアントを特定の IP アドレスにマップしなければならない場合もあります。 IP アドレスの動的割り当てと静的割り当てについて詳しくは、DHCP クライアントのサポートを参照してください。

IP アドレスのリース時間の決定

DHCP サーバーのデフォルトのリース時間は 24 時間です。 DHCP サーバーに設定するリース時間の長さは、いくつかの要因により異なります。 DHCP サーバーの使用目的、サイトの使用パターン、サービスの配置を考慮する必要があります。DHCP クライアントのリース時間を決定する上で役立つ情報について詳しくは、リースを参照してください。

BOOTP クライアントのサポート

BOOTP サーバーを現在使用している場合は、DHCP サーバーが、BOOTP クライアントにほとんど、またはまったく影響を与えないでネットワーク上の BOOTP サーバーに取って替われることを考慮してください。ネットワーク上に現在 BOOTP クライアントがある場合、オプションが 3 つあります。

最も簡単なオプションは、BOOTP クライアントをサポートするように DHCP サーバーを構成することです。 BOOTP クライアントをサポートするのに DHCP を使用する場合、各 BOOTP クライアントは、基本的に、単一の IP アドレスにマップされるため、そのアドレスを別のクライアントが再使用することはできません。ただし、DHCP をこのように使用すると、BOOTP クライアントを IP アドレスに 1 対 1 でマッピングするよう設定しなくて済むという利点があります。 DHCP サーバーは、それでも、アドレス・プールから BOOTP クライアントに IP アドレスを動的に割り当てます。 BOOTP クライアントに割り当てられると、IP アドレスは永続的にそのクライアントが使用するように予約され、そのアドレス予約が明示的に削除されるまでそのままです。ネットワーク内に非常に多くの BOOTP クライアントがある場合は、このオプションが適しています。

別のオプションとして、iSeries BOOTP サーバー構成を DHCP サーバーに移行することが可能です。BOOTP サーバー構成にリストされている BOOTP クライアントごとに DHCP クライアントが作成されます。このオプションでは、クライアントを DHCP クライアントに再構成することをお勧めします。ただし、BOOTP 構成を DHCP に移行した場合、DHCP アドレス割り当ては、BOOTP クライアントにも DHCP クライアントにも作用します。このオプションは、BOOTP クライアントを DHCP に変換するのに適しています。 BOOTP クライアントは、DHCP に再構成するプロセスの間も、サポートされます。

最後に、3 つ目のオプションです。これは、各 BOOTP クライアントを DHCP に変更し、それらに動的にアドレスを割り当てるよう DHCP を構成するものです。このオプションを選択すると、基本的に、ネットワークから BOOTP が完全に除去されます。

ネットワーク・クライアントの構成情報の識別

ネットワーク・トポロジー・レイアウトを使用すると、DHCP 構成で識別する必要のある装置 (たとえば、ルーター) を明確に判別できます。クライアントがそれに関して知っておかなければならないネットワーク内の他のサーバー (たとえば、ドメイン・ネーム・システム (DNS) サーバー) も識別する必要があります。この情報は、ネットワーク全体、特定のサブネット、またはサブネットに関係なく特定のクライアントのいずれかに対して指定できます。

多くのクライアントに適用される装置がある場合、可能な限り高いレベルでそれらの装置を指定する必要があります。たとえば、ネットワーク全体の場合はグローバル・レベル、特定のサブネットの場合はサブネット・レベルです。こうすることにより、装置が変わったときに DHCP 構成に対して最小限の変更を行うだけで済みます。たとえば、ネットワーク内のあらゆるクライアントについて同じルーターを指定してある場合、ルーターが変わったら、すべてのクライアントについて構成を変更しなければなりません。しかし、ルーターをグローバル・レベルで指定してあれば (すべてのクライアントがこの構成情報を継承します)、情報を一度変更するだけで、すべてのクライアントについて変更されます。

クライアントのなかには、情報をクライアント・レベルで構成しなければならない、固有の TCP/IP 構成要件をもつものがあります。 DHCP は、そういったクライアントを認識し、それらのクライアントには固有の構成データを提供することができます。このことは、構成オプションだけでなく、リース時間および IP アドレスにもあてはまります。たとえば、あるクライアントに、他のいずれのクライアントよりも長いリース時間が必要な場合があります。あるいは、ファイル・サーバーなど、1 つのクライアントだけが専用の IP アドレスを必要とする場合もあります。それらのクライアントを一括して識別し、それらがどのような固有情報を必要としているかが分かっていると、DHCP サーバーの構成を始めるときに役立ちます。

すべての構成オプションを一堂にそろえて見るには、 9 ページの『DHCP オプションの検索』を参照してください。

DHCP サーバーでの動的 DNS の使用

現在、DNS サーバーを使用してすべてのクライアントのホスト名と IP アドレスを管理している場合、DHCP から動的更新を受け入れるように DNS サーバーを再構成する必要が必ず出てきます。動的 DNS を使用すると、DHCP に切り替えたときに、DNS サービスの中断や変更がクライアントに通知されません。 DNS サーバーとの DHCP の使用について詳しくは、動的更新を参照してください。

現在、DNS サーバーを使用していなくても、DHCP サーバーを追加したときに、DNS サーバーの追加を考慮する必要が出てきます。DNS の利点と要件について詳しくは、Information Center の DNS トピックを参照してください。

リモート・クライアントのための DHCP の使用法

PPP を使用してネットワークに接続するリモート・クライアントがある場合、それらのクライアントがネットワークに接続したときに IP アドレスを動的に割り当てるよう DHCP をセットアップすることができます。このようなセットアップが有用なネットワークの例については、例: PPP と DHCP が単一の iSeries サーバー上にある場合または例: DHCP と PPP プロファイルが異なる iSeries サーバー上にある場合を参照してください。 これらの例では、リモート・クライアント用に PPP と DHCP を併用するネットワークのセットアップ方法についても説明しています。

関連概念

6 ページの『リレー・エージェントとルーター』
ネットワーク内で DHCP リレー・エージェントを使用する必要がある場合、またルーターで十分な場合があります。 DHCP リレー・エージェントとルーターの両方を使用して、効率良くしかも安全にネットワーク全体にデータを転送することができます。

26 ページの『DHCP の例』
種々のネットワークのセットアップ方法について図と例を検討することにより、どの方法がお客様のインストールに最適かを判断できます。

7 ページの『DHCP クライアントのサポート』
DHCP を使用して、大きなグループ (サブネット) としてすべてのクライアントを管理するのではなく、ネットワーク内の各クライアントを個別に管理することができます。

4 ページの『リース』
DHCP リースについて説明し、DHCP クライアントのリース時間を決める際に考慮すべき問題点を提示します。

8 ページの『BOOTP』
このトピックでは BOOTP とは何かを説明し、BOOTP と DHCP の歴史も紹介します。

8 ページの『動的更新』
DHCP がクライアントに IP アドレスを割り当てる際に、DNS サーバーと一緒に DHCP サーバーを使用して DNS 内のクライアント情報を動的に更新することができます。

DNS

58 ページの『問題: クライアントが IP アドレスまたはその構成情報を受信しない』
クライアントが IP アドレスまたはその構成情報を受信できない場合、問題が発生する可能性があります。 IP アドレスは、クライアントと DHCP サーバー間の 4 ステップからなるプロセスを経て、クライアントにリースされます。

関連資料

9 ページの『DHCP オプションの検索』
DHCP には、DHCP サーバーに情報を要求した場合にクライアントに送信できる構成オプションが多数あります。 すべての DHCP オプションについて説明する索引ツールを使用できます。

40 ページの『例: PPP と DHCP が単一の iSeries サーバー上にある場合』
1 つの LAN とリモート・ダイヤルイン・クライアントのための DHCP サーバーとして iSeries サーバーをセットアップする方法について説明します。

43 ページの『例: DHCP と PPP プロファイルが異なる iSeries サーバー上にある場合』
2 つの LAN とリモート・ダイヤルイン・クライアントのためのネットワーク DHCP サーバーおよび DHCP/BOOTP リレー・エージェントとして 2 台の iSeries サーバーをセットアップする方法について説明します。

DHCP の構成

このトピックでは、DHCP サーバーおよびクライアントをセットアップする手順と、DNS に動的更新を送信するように DHCP を構成する手順を示しています。

関連資料

46 ページの『DHCP のための計画』
ご使用のネットワークに合わせた DHCP のセットアップ方法の計画に必要な手順を説明します。

DHCP サーバーおよび BOOTP/DHCP リレー・エージェントの構成

このトピックでは iSeries DHCP サーバーの構成に使用する必要のあるソフトウェアについて説明します。また、DHCP 構成での作業方法、DHCP サーバー管理プログラムの使用法、および DHCP/BOOTP リレー・エージェントのセットアップ手順について説明します。

関連概念

6 ページの『リレー・エージェントとルーター』
ネットワーク内で DHCP リレー・エージェントを使用する必要がある場合、またルーターで十分な場合があります。 DHCP リレー・エージェントとルーターの両方を使用して、効率良くしかも安全にネットワーク全体にデータを転送することができます。

DHCP サーバーの構成または表示

DHCP サーバー構成機能を使用して、新しい DHCP 構成を作成したり、既存の DHCP 構成を表示する必要があります。DHCP サーバー構成にアクセスするには次のようにします。

1. **iSeries ナビゲーター**で、「**使用する iSeries サーバー**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**DHCP**」と展開します。
2. 「**DHCP**」を右マウス・ボタンでクリックして、「**構成**」を選択します。

新しい DHCP 構成を作成する場合、DHCP サーバーのセットアップを手助けしてくれるウィザードを使用します。このウィザードは、基本的な構成に関する質問をいくつか出して、サブネットの作成プロセスをステップバイステップで進みます。ウィザードの完了後、構成を変更して、ネットワークの必要に合わせることができます。

DHCP サーバーの構成が済んでいる場合、DHCP サーバー構成機能により、DHCP サーバーから管理可能なすべてのサブネットとクライアント、およびクライアントに送信される構成情報を含め、現在の構成が表示されます。

「DHCP 構成」ウィンドウにショートカットを作成します。

DHCP 構成を頻繁に表示するため、デスクトップ上に「DHCP 構成」ウィンドウへのショートカットを作成する必要がある場合は、以下のステップを実行してください。

1. **iSeries ナビゲーター**で、「**使用する iSeries サーバー**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**DHCP**」と展開します。
2. 「**DHCP**」を右マウス・ボタンでクリックして、「**ショートカットの作成**」を選択します。

DHCP サーバーの始動または停止

DHCP サーバーが構成されると、そのサーバーを始動したり、停止したりできます。

1. **iSeries ナビゲーター**で、「**使用する iSeries サーバー**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**DHCP**」と展開します。

2. 「**DHCP**」を右マウス・ボタン・クリックして、「**始動**」または「**停止**」を選択します。

自動的に始動するための DHCP サーバーの構成

以下のステップによって、自動的に始動されるように DHCP サーバーを構成することができます。

1. **iSeries ナビゲーター**で、「**使用する iSeries サーバー**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**DHCP**」と展開します。
2. 「**DHCP**」を右マウス・ボタンでクリックして、「**構成**」を選択します。
3. 「**DHCP サーバー**」を右マウス・ボタンでクリックして、「**特性**」を選択します。
4. 「**TCP/IP が開始されたときに始動**」チェック・ボックスにチェックを付けます。
5. 「**OK**」をクリックする。

DHCP サーバー・モニターへのアクセス

DHCP サーバー・モニターは、IBM® iSeries DHCP サーバーのアクティブなリース情報をモニターするために提供されます。このグラフィカル・インターフェースにより、どの IP アドレスがリースされているか、それらがリースされている時間、それらのリースが満了して再度リース可能になるときを表示することができます。DHCP サーバー・モニターにアクセスするには、以下のステップに従ってください。

1. **iSeries ナビゲーター**で、「**使用する iSeries サーバー**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**DHCP**」と展開します。
2. 「**DHCP**」を右マウス・ボタンでクリックして、「**モニター**」を選択します。

BOOTP/DHCP リレー・エージェントの構成

iSeries サーバーは、DHCP/BOOTP リレー・エージェントを提供します。このエージェントを使用して、別のネットワーク上の DHCP サーバーに DHCP パケットを転送することができます。

iSeries DHCP/BOOTP リレー・エージェントをセットアップする手順は、次のとおりです。

1. **iSeries ナビゲーター**で、「**使用する iSeries サーバー**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**BOOTP/DHCP リレー・エージェント**」と展開します。
2. 「**BOOTP/DHCP リレー・エージェント**」を右マウス・ボタンでクリックして、「**構成**」を選択します。
3. リレー・エージェントが DHCP パケットを受信するインターフェースと、パケットの転送先を指定します。
4. 「**OK**」をクリックする。

BOOTP/DHCP リレー・エージェントの始動または停止

DHCP/BOOTP リレー・エージェントが構成されると、そのエージェントを始動したり、停止したりできます。

1. **iSeries ナビゲーター**で、「**使用する iSeries サーバー**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**BOOTP/DHCP リレー・エージェント**」と展開します。
2. 「**BOOTP/DHCP リレー・エージェント**」を右マウス・ボタン・クリックして、「**始動**」または「**停止**」を選択します。

自動的に始動するための BOOTP/DHCP リレー・エージェントの構成

また、TCP/IP が開始されたときに iSeries サーバーによって自動的に始動されるように BOOTP/DHCP リレー・エージェントを構成することもできます。

1. **iSeries ナビゲーター**で、「**使用する iSeries サーバー**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**BOOTP/DHCP リレー・エージェント**」と展開します。
2. 「**BOOTP/DHCP リレー・エージェント**」を右マウス・ボタンでクリックして、「**特性**」を選択します。
3. 「**TCP/IP が開始されたときに始動**」チェック・ボックスにチェックを付けます。
4. 「**OK**」をクリックする。

DHCP を使用するためのクライアントの構成

ここでは、Microsoft® Windows® クライアントおよび OS/2® クライアントがそれぞれの構成情報を DHCP サーバーに要求するように構成する手順を説明します。

DHCP サーバーが構成されると、各クライアントが DHCP を使用するように構成する必要があります。以下で、Windows クライアントおよび OS/2 クライアントがそれぞれの構成情報を DHCP サーバーに要求するように構成する手順を説明します。さらに、クライアントが固有の DHCP リース情報をどのように表示できるのかについても説明します。

Windows 95、Windows 98、または Windows Me クライアント用に DHCP を使用可能に設定

DHCP を使用可能にするには次のようにします。

1. 「**スタート** メニュー」で、「**設定**」 → 「**コントロール パネル**」と選択します。
2. 「**ネットワーク**」をダブルクリックして、「**プロトコル**」タブを選択します。
3. 「**TCP/IP プロトコル**」を選択して、「**特性**」ボタンを選択します。
4. 「**IP アドレス**」タブで、「**DHCP サーバーから IP アドレスを取得**」ラジオ・ボタンを選択します。
5. 「**OK**」をクリックする。

クライアントの DHCP リースの検査:

Windows 95、Windows 98、または Windows Me クライアントには、クライアントの MAC アドレスおよび DHCP リース情報を表示するユーティリティーが備わっています。このユーティリティーにより、DHCP リースの解除や更新も行えます。次のステップを実行して、クライアントの DHCP リースを検査します。

1. 「*MS-DOS* コマンド プロンプト」を開きます。
2. **WINIPCFG** を実行します。

注: このユーティリティーは、表示されている情報を動的に更新しないため、更新された状況を表示するためには、ユーティリティーを再度実行する必要があります。

Windows NT クライアント用に DHCP を使用可能に設定

DHCP を使用可能にするには次のようにします。

1. 「**スタート** メニュー」で、「**設定**」 → 「**コントロール パネル**」と選択します。
2. 「**ネットワーク**」をダブルクリックして、「**プロトコル**」タブを選択します。

3. 「**TCP/IP プロトコル**」を選択して、「**特性**」を選択します。
4. 「**IP アドレス**」タブで、「**DHCP サーバーから IP アドレスを取得**」を選択します。
5. 「**OK**」をクリックする。

MAC アドレスおよび DHCP リースの検査:

Windows NT® および Windows 2000 クライアントにも、クライアントの MAC アドレスおよび DHCP リース情報を表示するユーティリティーが備わっています。Windows NT および Windows 2000 クライアントの DHCP リースを検査するには、次のステップに従ってください。

1. 「コマンド・プロンプト」ウィンドウを開きます。
2. **IPCONFIG /ALL** を実行します。

注: このユーティリティーは、表示されている情報を動的に更新しないため、更新された状況を表示するためには、ユーティリティーを再度実行する必要があります。同じユーティリティーを異なるパラメーターで使用して、リースの解除 (IPCONFIG /RELEASE) や更新 (IPCONFIG /RENEW) が行えます。コマンドの可能なパラメーターをすべて見るためには、MS-DOS コマンド・プロンプトから IPCONFIG /? を実行します。

クライアントに代わって DHCP サーバーに DNS A レコードを更新させたい場合は、Microsoft Windows 2000 DHCP クライアントを構成する必要があります。ネットワークに標準的な既存の Windows クライアント (たとえば、Windows 95 および NT など) がある場合、更新を DHCP サーバーに任せることが必要な場合があります。これらのクライアントは、現在、DNS A レコードを更新しないためです。 DHCP サーバーに任せると、DNS 管理が単純化されます。DNS 更新は、いくつかのクライアントにそれぞれ固有のレコードを更新させるのではなく、すべてのクライアントについて DHCP サーバーから発生するためです。

Windows 2000 クライアント用に DHCP を使用可能に設定

DHCP を使用可能にするには次のようにします。

1. 「**スタート** メニュー」で、「**設定**」 → 「**ネットワークおよびダイヤルアップ接続**」と選択します。
2. 該当する接続名を右マウス・ボタンでクリックして、「**プロパティー**」を選択します。
3. 「**TCP/IP プロトコル**」を選択して、「**特性**」を選択します。
4. 「**全般**」タブで、「**DHCP サーバーから IP アドレスを取得**」を選択します。
5. 「**OK**」をクリックする。

MAC アドレスおよび DHCP リースの検査:

Windows NT および Windows 2000 クライアントにも、クライアントの MAC アドレスおよび DHCP リース情報を表示するユーティリティーが備わっています。Windows NT および Windows 2000 クライアントの DHCP リースを検査するには、次のステップに従ってください。

1. 「コマンド・プロンプト」ウィンドウを開きます。
2. **IPCONFIG /ALL** を実行します。

注: このユーティリティーは、表示されている情報を動的に更新しないため、更新された状況を表示するためには、ユーティリティーを再度実行する必要があります。同じユーティリティーを異なるパラメーターで使用して、リースの解除 (IPCONFIG /RELEASE) や更新 (IPCONFIG /RENEW) が行えます。コマンドの可能なパラメーターをすべて見るためには、MS-DOS コマンド・プロンプトから IPCONFIG /? を実行します。

クライアントに代わって DHCP サーバーに DNS A レコードを更新させたい場合は、Microsoft Windows 2000 DHCP クライアントを構成する必要があります。ネットワークに標準的な既存の Windows クライアント (たとえば、Windows 95 および NT など) がある場合、更新を DHCP サーバーに任せることが必要な場合があります。これらのクライアントは、現在、DNS A レコードを更新しないためです。 DHCP サーバーに任せると、DNS 管理が単純化されます。DNS 更新は、いくつかのクライアントにそれぞれ固有のレコードを更新させるのではなく、すべてのクライアントについて DHCP サーバーから発生するためです。

OS/2 Warp 4 クライアント用に DHCP を使用可能に設定

DHCP を使用可能にするには次のようにします。

1. 「**TCP/IP 構成**」を選択します。
2. 「**IP アドレスを自動的に取得する**」ラジオ・ボタンを選択します。
3. 「**OK**」をクリックする。

DHCPCD と入力すると、OS/2 ウィンドウから手動でクライアントを始動できます。また、クライアントが DHCP オプションを要求するようにクライアント構成ファイル (mptn\etc\dhcpcd.cfg) を更新することもできます。

Warp にも、リースをトラッキングするためのユーティリティーが備わっています。OS/2 ウィンドウから、DHCPMON と入力するか、TCP/IP フォルダーの DHCP モニター・アイコンを選択してください。DHCPMON -t と入力すると、クライアントを終了できます。

注: これにより DHCP の解除が発行されることはありません。DHCP クライアントがシャットダウンされるだけで、リースは更新されません。

クライアントの DHCP ログ・ファイルを表示して、クライアント/サーバー間の対話を表示したり、サーバーに戻されたオプションを見ることもできます。ファイル名は、クライアント構成ファイルで構成できます。システムのなかには、ルート・ディレクトリーに、dhcpcd.log というファイル名でログをもっているものがあります。また、以前に取得されたリースおよびオプションの情報は、クライアントによって、ファイル mptn\etc\dhcpc.db に保管されています。クライアントを「まったくの最初から」再始動しなければならない場合は、ファイル mptn\etc\dhcpc.db を消去してください。

DNS 動的更新を使用不可に設定

クライアントからの DNS 動的更新を使用不可にするには、次のようにします。

1. 「**スタート** メニュー」で、「**設定**」 → 「**ネットワークおよびダイヤルアップ接続**」と選択します。
2. 該当する接続名を右マウス・ボタンでクリックして、「**プロパティー**」を選択します。
3. 「**TCP/IP プロトコル**」を選択して、「**特性**」を選択します。
4. 「**拡張**」を選択します。
5. 「**DNS**」タブで、「この接続のアドレスを DNS に登録」オプションと「DNS 登録でこの接続 DNS サフィックスを使用」オプションを選択解除します。
6. 「**OK**」をクリックする。

これらのステップは、DNS レコード更新を DHCP サーバーに任せたいすべての接続について行ってください。

動的更新を DNS に送信するための DHCP の構成

DHCP サーバーが IP アドレスをクライアントにリースするときに動的に DNS リソース・レコードを更新するように DHCP サーバーと DNS サーバーを構成することができます。

ご使用の DHCP サーバーがホストに新しいアドレスを割り当てるたびに、更新要求を DNS サーバーに送信するように構成できます。この自動化されたプロセスにより、急速に成長あるいは変化する TCP/IP ネットワーク内での DNS サーバー管理が軽減されます。ホスト・ロケーションが頻繁に変更されるネットワークでも同様です。DHCP を使用するクライアントが IP アドレスを受信すると、そのデータは、即時に DNS サーバーに送信されます。この方法により、DNS は、ホストの IP アドレスが変更された場合でも、ホストについての照会を正しく解決し続けることができます。

レコード更新が発生するためには、オプション 31 をこの iSeries サーバーにインストールする必要があります。 DHCP サーバーは、オプション 31 によって提供されるプログラミング・インターフェースを使用して、動的更新を実行します。 DNS サーバーは、動的更新を実行できる、別の iSeries サーバー上で稼動できます。オプション 31 のインストールの確認については、DNS システム要件を参照してください。

DHCP サーバーが動的 DNS 更新を実行できるように DHCP 特性を構成する手順は、次のとおりです。

1. 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 右側の画面区画で、「**DHCP**」を右マウス・ボタン・クリックして、「**構成**」を選択します。
3. 「**DHCP サーバー構成**」ウィンドウの左側の画面区画で、「**グローバル**」を右マウス・ボタン・クリックして、「**特性**」を選択します。
4. 「**オプション**」タブを選択します。
5. 「**選択オプション**」リストから「**オプション 15: ドメイン・ネーム**」を選択します。「**選択オプション**」 リストにオプション 15 が出ていない場合は、「**選択可能オプション**」リストから「15: ドメイン・ネーム」を選択して、「**追加**」をクリックしてください。
6. 「**ドメイン・ネーム**」フィールドで、DNS を使用してホスト名を解決する際にクライアントが使用するドメイン・ネームを指定します。
7. 「**動的 DNS**」タブを選択します。
8. 「**DHCP サーバーは A レコードと PTR レコードの両方を更新する**」または「**DHCP サーバーは PTR レコードだけを更新する**」を選択します。
9. 「**ドメイン・ネームをホスト名に付加する**」を「**はい**」に設定します。
10. 「**OK**」をクリックして、「**グローバル特性**」をクローズします。

関連概念

8 ページの『動的更新』
DHCP がクライアントに IP アドレスを割り当てる際に、DNS サーバーと一緒に DHCP サーバーを使用して DNS 内のクライアント情報を動的に更新することができます。

関連資料

DNS システム要件

リースされた IP アドレスの管理

DHCP サーバー・モニターはリースのモニターと管理に役立ちます。

DHCP 構成ツールは、DHCP サーバー、DHCP サーバーがサービスするクライアント、およびクライアントに送信される情報をセットアップする上で役立ちます。DHCP 構成ツールに、DHCP が管理する IP アドレス・プールと、それらのアドレス・プールのリース時間を指定します。現在リースされている IP アドレスを知るには、DHCP サーバー・モニターを使用する必要があります。

DHCP サーバー・モニターは、IBM iSeries DHCP サーバーのアクティブなリース情報をモニターするために提供されます。このグラフィカル・インターフェースにより、どの IP アドレスがリースされているか、それらがリースされている時間、それらのリースが満了して再度リース可能になるときを表示することができます。

また、DHCP サーバー・モニターを使用して、すでに使用されていない IP アドレスを再利用できます。DHCP アドレス・プールを使い果たしてしまったら、アクティブなリース情報に目を通して、削除したいリースがないか判断し、該当する IP アドレスを他のクライアントで使用できるようにすることができます。たとえば、もうネットワーク上にはないが、アクティブな IP アドレス・リースをまだもっているクライアントがあります。このクライアントのアクティブな IP アドレス・リースは削除できます。この操作は、クライアントがもうそのアドレスを使用しようとしないことが確実である場合にのみ実行してください。DHCP サーバーは、クライアントのアクティブ IP アドレス・リースが削除されても、クライアントに通知しません。クライアントからの IP アドレスを解放せずに、まだネットワーク上にあるクライアントのアクティブなリースを削除すると、ネットワーク上で重複した IP アドレス割り当てが発生して終了することがあります。

関連概念

58 ページの『問題: クライアントが IP アドレスまたはその構成情報を受信しない』
クライアントが IP アドレスまたはその構成情報を受信できない場合、問題が発生する可能性があります。 IP アドレスは、クライアントと DHCP サーバー間の 4 ステップからなるプロセスを経て、クライアントにリースされます。

60 ページの『問題: IP アドレスの割り当てが同じネットワーク上で重複している』
IP アドレスは、ネットワーク全体で固有のものでなければなりません。DHCP サーバーは、1 つの IP アドレスを複数のクライアントに割り当てることはありません。

DHCP のトラブルシューティング

ジョブ・ログおよびトレース・データを表示できるだけでなく、一般的な問題のトラブルシューティング・リストを使用することもできます。

以下の情報は、ご使用の DHCP サーバーに発生している問題のトラブルシューティングの際に役立てていただくためのものです。ここに示されていない問題が発生した場合は、DHCP のための計画を参照して、DHCP 構成に必要な事項をすべて考慮してあるかどうかを確認してください。

次のリストから問題記述を選択するか、「詳しい DHCP エラー情報トピックの収集」を読んでサーバー・ログ・データおよびトレース情報にアクセスする方法を確認してください。

関連概念

iSeries 通信トレース

関連資料

46 ページの『DHCP のための計画』
ご使用のネットワークに合わせた DHCP のセットアップ方法の計画に必要な手順を説明します。

詳しい DHCP エラー情報の収集

直面している問題の背後にあるエラーの詳細を見つけ出す方法はいくつかあります。

1 つは、次のようなステップで DHCP サーバー・ジョブ・ログを見る方法です。

1. **iSeries ナビゲーター**で、「**使用する iSeries サーバー**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**DHCP**」と展開します。
2. 「**DHCP**」を右マウス・ボタンでクリックして、「**サーバー・ジョブ**」を選択します。

DHCP サーバー・ジョブ・ログにメッセージが入っていない場合は、iSeries 通信トレースまたは DHCP サーバーの内部プログラム・トレースから情報を収集する必要があります。 iSeries 通信トレースは、クライアント要求が DHCP サーバーに届いているかどうかや、DHCP サーバーがクライアントに応答しているかどうかを判断するのに役立ちます。クライアント要求が DHCP サーバーに届いていても応答していない場合は、DHCP サーバー内部プログラム・トレース機能を使用してください。

DHCP サーバーのトレース

DHCP サーバーをトレースする手順は、次のとおりです。

1. **iSeries ナビゲーター**で、「**使用する iSeries サーバー**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**DHCP**」と展開します。
2. 「**DHCP**」を右マウス・ボタンでクリックして、「**構成**」を選択します。
3. 「**DHCP サーバー**」を右マウス・ボタンでクリックして、「**特性**」を選択します。
4. 「**ロギング**」特性タブを選択します。
5. 「**ロギング可能化**」チェック・ボックスにチェックを付けます。
6. **ログ・ファイル名**は **dhcpsd.log** です。
7. 「トレース」および「統計」(トレースと統計のログを使用できるのはサポート回線だけです) 以外のすべての「**ログ**」カテゴリーにチェックを付けます。
8. 「**OK**」をクリックする。
9. サーバーがすでに始動されている場合は、「**DHCP サーバー**」を右マウス・ボタン・クリックし、「**更新サーバー**」を選択して、DHCP サーバーを再始動します。
10. 問題を再作成します。
11. 「**DHCP サーバー**」を右マウス・ボタン・クリックして、「**特性**」 → 「**ロギング**」を選択します。
12. 「**ロギング可能化**」を選択解除して、ロギングをオフにします。
13. 「**OK**」をクリックする。
14. 「**DHCP サーバー**」を右マウス・ボタン・クリックし、「**更新サーバー**」を選択して DHCP サーバーを再始動します。
15. 「QIBM/UserData/OS400/DHCP/dhcpsd.log」に入っている DHCP ログ・ファイルを表示します。**iSeries ナビゲーター**で、「**使用する iSeries サーバー**」 → 「**ファイル・システム**」 → 「**統合ファイル・システム**」 → 「**ルート**」 → 「**ファイルのディレクトリー**」と展開します。または、文字ベースのインターフェースから、**wrklnk** コマンドを使用して、オプション **5= 表示**を選択します。

問題: クライアントが IP アドレスまたはその構成情報を受信しない

クライアントが IP アドレスまたはその構成情報を受信できない場合、問題が発生する可能性があります。IP アドレスは、クライアントと DHCP サーバー間の 4 ステップからなるプロセスを経て、クライアントにリースされます。

クライアントが IP アドレスを受信する前に、4 つのステップすべてが発生する必要があります。 4 つのステップからなるプロセスについて詳しくは、DHCP クライアント/サーバー間の対話を参照してください。

この問題には次のような一般的な理由があります。

クライアントが、DHCP サーバーに設定されていないサブネットに接続されている。
DHCP 構成を調べて、DHCP サーバーが管理するすべてのサブネットが構成にリストされているか確認します。 DHCP サーバーがどのサブネットを管理しなければならないかが不明な場合は、ネットワーク・トポロジーに関する考慮事項を参照してください。

クライアントからの DHCP DISCOVER メッセージが DHCP サーバーに届かない。
DHCP サーバーがクライアントのサブネット上に IP アドレスをもっていない場合は、クライアントの DHCP/BOOTP メッセージを DHCP サーバーに転送できるルーターまたは DHCP DISCOVER リレー・エージェントが存在する必要があります。詳細については、リレー・エージェントとルーターを参照してください。サーバーは、ブロードキャスト・メッセージを受信するだけでなく、応答パケットをクライアントのサブネットに送り返すこともできなければなりません。

ご使用の iSeries サーバーがマルチホームである場合、DHCP 構成にサブネット・グループを追加する必要があります。マルチホーム・サーバー用の DHCP の構成方法について詳しくは、例: DHCP とマルチホーミングを参照してください。 この例では、クライアントのブロードキャスト・メッセージをサーバーが受信できるようにするために DHCP 構成に対して何を行う必要があるかを説明します。

DHCP サーバーは、クライアントに使用できるアドレスをアドレス・プールにもっていない。
現在 DHCP サーバーが使用しているアドレスを知るには、DHCP サーバー・モニターを使用できます。DHCP サーバー・モニターの使用法については、リースされた IP アドレスの管理で詳しく説明されています。 DHCP サーバーで使用可能なアドレスを使い果たしてしまった場合は、アドレス・プールに IP アドレスを追加するか、リース時間を短縮する、あるいはもう不要になった永続リースを削除することが必要です。

関連概念

47 ページの『ネットワーク・トポロジーに関する考慮事項』
大部分の DHCP セットアップは、ネットワーク・トポロジー、ネットワーク上の装置 (たとえば、ルーター)、DHCP でクライアントをどのようにサポートしたいかを考えることで計画できます。

6 ページの『リレー・エージェントとルーター』
ネットワーク内で DHCP リレー・エージェントを使用する必要がある場合、またルーターで十分な場合があります。 DHCP リレー・エージェントとルーターの両方を使用して、効率良くしかも安全にネットワーク全体にデータを転送することができます。

56 ページの『リースされた IP アドレスの管理』
DHCP サーバー・モニターはリースのモニターと管理に役立ちます。

関連資料

1 ページの『DHCP クライアント/サーバー間の対話』
クライアントはサーバーから DHCP 情報を入手し、クライアントとサーバー間で特定のメッセージが送信されます。 DHCP はリースを取得して戻します。

32 ページの『例: DHCP とマルチホーミング』
インターネット・ルーターによってインターネットに接続される LAN のための DHCP サーバーとして iSeries サーバーをセットアップする方法について説明します。

問題: IP アドレスの割り当てが同じネットワーク上で重複している

IP アドレスは、ネットワーク全体で固有のものでなければなりません。DHCP サーバーは、1 つの IP アドレスを複数のクライアントに割り当てることはありません。

一定の条件の下では、DHCP サーバーは、アドレスをクライアントに割り当てる前にそのアドレスが現在使用中でないことを確認しようとします。DHCP サーバーは、使用中であるはずのないアドレスが使用中であることを検出すると、一時的にそのアドレスに「使用中」のマークを付け、そのアドレスをどのクライアントにも割り当てません。サーバーが検出した IP アドレスのうち、使用中であってもサーバーが割り当てたものでない IP アドレスを表示するには、DHCP サーバー・モニターを使用してください。これらのアドレスは、USED (使用中) 状況になり、UNKNOWN_TO_IBMDHCP クライアント ID を持つことになります。

この問題には次のような一般的な理由があります。

同じ IP アドレスを割り当てるように構成されている DHCP サーバーが複数個ある。
同じ IP アドレスを割り当てるように構成されている DHCP サーバーが 2 つあると、2 つの異なるクライアントが同じ IP アドレスを受信することがあり得ます。どちらかのクライアントが一方の DHCP サーバーから IP アドレスを受信し、もう 1 つのクライアントが他方の DHCP サーバーから同じ IP アドレスを受信します。複数の DHCP サーバーが同じサブネットまたはネットワークにサービスできますが、同じアドレス・プールや重複するアドレス・プールを使って DHCP サーバーを構成しないでください。

DHCP が管理する IP アドレスを使ってクライアントが手動で構成されている。
DHCP サーバーは、通常、IP アドレスをクライアントに割り当てる前に、そのアドレスが現在使用中であるかどうか調べます。ただし、DHCP サーバーが目的の IP アドレスを調べているときに、手動で構成されたクライアントが現在ネットワークに接続されているとか、応答に使用できるかを保証することはできません。そのため、DHCP サーバーは、目的の IP アドレスを DHCP クライアントに割り当てることができます。手動で構成されたクライアントがネットワークに接続されていると、ネットワーク上で IP アドレスが重複します。DHCP によって管理される IP アドレスを使用して、クライアント用のネットワーク・セットアップを手動で構成しないでください。 IP アドレスを使ってクライアントを手動で構成する必要がある場合、その IP アドレスを、DHCP サーバーのアドレス・プールから除外する必要があります。

関連概念

56 ページの『リースされた IP アドレスの管理』
DHCP サーバー・モニターはリースのモニターと管理に役立ちます。

問題: DNS レコードが DHCP によって更新されない

iSeries DHCP サーバーは、DNS リソース・レコードを動的に更新することができます。動的更新エラーの原因は、DNS レコードの更新の失敗にある可能性があります。

この機能については、 8 ページの『動的更新』を参照してください。 DHCP サーバーは、ネーム・レゾリューション機能とプログラミング・インターフェースを使用して、更新する適切な動的 DNS サーバーを判別します。動的更新エラーの元を判別する際に、このことを利用できます。

DNS レコードが動的に更新されない場合は、以下の事項を検査してください。

更新されるサブネットとリソース・レコードのタイプ (A レコードおよび/または PTR レコード) を確認する。 DHCP 構成を調べ、クライアントのサブネットがリソース・レコードを動的に更新するようセットアップされていること、および更新されるレコードのタイプを確認します。

DHCP を実行する iSeries サーバー上に i5/OS オプション 31 (ドメイン・ネーム・システム) がインストールされていることを確認する。

DHCP サーバーは、i5/OS オプション 31 によって提供されるプログラミング・インターフェースを使用します。動的に更新される DNS が、DHCP サーバーと同じ iSeries サーバー上に収容されている必要はありません。

DHCP サーバーが、DNS サーバーに更新を送信する許可を得ているか確認する。

DNS 構成を調べて、DNS ゾーンが動的更新を許可する構成になっていること、および DHCP サーバーがアクセス制御リストに含まれていることを確認します。

DNS サーバーがクライアントのドメインを解決できるか確認する。

CHGTCPDMN コマンドを使用して、DHCP が収容されている iSeries サーバー上の DNS サーバーのリストを表示します。これらの DNS サーバーが、更新されるドメインを解決できることを確認します。そのためには、DHCP が実行している iSeries サーバーから NSLOOKUP を実行して、更新に失敗したドメイン内の名前 (または IP アドレス) を解決します。 DHCP サーバーは、クライアントの完全修飾ドメイン・ネーム (FQDN) を導き出して、その DNS レコードを更新する必要があります。 DHCP サーバーは、FQDN (クライアントのホスト名とドメイン・ネーム) を使わずに動的 DNS を更新しようとはしません。 DHCP サーバーは、次の手順を使用してクライアントの FQDN を導き出します。

1. クライアントからの DHCPREQUEST メッセージでオプション 81 (クライアント FQDN)。
2. クライアントからの DHCPREQUEST メッセージでオプション 12 (ホスト名) および/またはオプション 15 (ドメイン・ネーム)。
3. クライアントからの DHCPREQUEST メッセージでオプション 12 (ホスト名) および/または DHCP サーバーに構成されたオプション 15 (ドメイン・ネーム)。この場合、FQDN を導き出すには、ドメイン・ネームをホスト名に付加するように DHCP サーバーを構成する必要があります (グローバル・レベル、サブネット、クラス、またはクライアントの「**特性**」 → 「**動的 DNS**」タブに指定)。

TXT レコードが、対応する DNS レコードと一致しない。

既存の DNS リソース・レコードを調べて、関連付けられている DHCP クライアントを判別するよう DHCP サーバーを構成することができます。DHCP サーバーは、DNS で更新する A レコードと PTR レコードを使って対応する TXT レコードを作成することにより、判別します。サーバーが、DNS 更新を実行する前にクライアント ID を検査するよう構成されている場合、TXT レコード・データは、DHCP サーバーからアドレスを受信したクライアントのクライアント ID と一致しなければなりません。一致しない場合、DHCP サーバーは DNS A リソース・レコードを更新しません。これは、既存のレコードを上書きしないようにするためです。ただし、DHCP サーバーは、既存のレコードを無視し、TXT レコード内のデータに関係なく DNS 更新を実行するよう構成することができます (グローバル・レベル、サブネット、クラス、またはクライアントの「**特性**」 → 「**動的 DNS**」タブに指定)。

関連概念

8 ページの『動的更新』

DHCP がクライアントに IP アドレスを割り当てる際に、DNS サーバーと一緒に DHCP サーバーを使用して DNS 内のクライアント情報を動的に更新することができます。

問題: DHCP ジョブ・ログにメッセージ DNS030B があり、3447 というエラー・コードが付いている

エラー・コード 3447 は、DHCP サーバーが DNS サーバーからの応答を待っている間にタイムアウトになったことを意味します。これは、iSeries DHCP サーバーと DNS サーバー間のネットワークまたは接続問題が原因と考えられます。

このメッセージには、TCP5763 メッセージが付属しています。これには、DNS リソース・レコードのタイプと、DHCP サーバーが更新しようとしたリソース・レコードの詳細データが入っています。

リースが更新されるたびに DHCP iSeries サーバーが DNS リソース・レコードを更新しようとするため、リソース・レコードはすでに、初期 IP アドレス・リースまたは以前のリース更新からのゾーン構成ファイルに入っている可能性があります。 NSLOOKUP などのツールを使用して、DNS ゾーン構成データを調べてください。リソース・レコードはすでに存在しており、正しいデータが入っているので、処置は不要であることが分かります。

DNS にリソース・レコードが入っていない場合、リソース・レコードを更新する方法はいくつかあります。 DHCP iSeries サーバーは、次にリース更新要求があった時点でリソース・レコードを更新しようとします。したがって、その要求が発生するまで待つことになります。そうでないと、クライアントの電源をオンにしたときに、多くのクライアントが IP アドレスの更新または再獲得を試みます。クライアントを再始動してみる必要がありますが、それによって、DHCP サーバーが DNS リソース・レコードを再度更新しようとする可能性があります。

これらのオプションのどちらも効かない場合は、DNS リソース・レコードを手動で更新できます。手動による更新を行うときに動的ゾーンが実行中であってはならないため、この方法は、お勧めしません。そのため、DHCP サーバーからの他の動的更新は、このダウン時間中に失われます。ただし、いくつかのクライアントおよび BIND DNS サーバーのインプリメンテーションによって提供される動的更新ユーティリティーがあります。動的更新ユーティリティーを使用すると、リソース・レコードを更新できます。手動でゾーンを更新する (管理者は、更新するリソース・レコード・データを入力する必要があります) プロセスの場合と類似していますが、動的更新ユーティリティーを使用するとゾーンがアクティブである間の更新が可能です。

DHCP の関連情報

ここにリストされているのは、DHCP RFC および IBM Redbooks™ (PDF 形式) です。すべての PDF は表示および印刷できます。

DHCP RFCs

コメント要求 (RFC) では、インターネットに使用されるプロトコル規格および提案規格の書面による定義を記述しています。次の RFC は、DHCP および関連機能について理解する上で役立ちます。

- RFC 2131: 動的ホスト構成プロトコル (RFC 1541 は廃止)
- RFC 2132: DHCP オプションおよび BOOTP ベンダー拡張機能
- RFC 951: ブートストラップ・プロトコル (BOOTP)
- RFC 1534: DHCP と BOOTP 間の相互運用

- RFC 1542: ブートストラップ・プロトコルのための説明と拡張機能
- RFC 2136: ドメイン・ネーム・システム内の動的更新 (DNS UPDATE)

IBM Redbooks

AS/400® TCP/IP 自動構成: DNS および DHCP サポート

この Redbook は、i5/OS に組み込まれている、ドメイン・ネーム・システム (DNS) サーバーおよび動的ホスト構成プロトコル (DHCP) サーバーのサポートについて説明しています。この Redbook に記載されている情報は、例を使って DNS および DHCP サポートをインストール、調整、設定、およびトラブルシューティングするのに役立ちます。

注: この Redbook は、V5R1 で使用できるようになった新しい BIND 8 機能 (動的更新を含む) を含める更新はなされていません。しかし、一般的な DNS および DHCP 概念を知るには十分です。

PDF ファイルの保存

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を右クリックする (上記のリンクを右クリックする)。
2. PDF をローカルに保存するオプションをクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「**保存**」をクリックする。

Adobe Reader のダウンロード

PDF を表示したり印刷したりするには、ご使用のシステムに Adobe Reader をインストールする必要があります。 Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html) から無料でダウンロードできます。

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、IBM 機械コードのご使用条件、またはそれと同等の条項に基づいて、 IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

プログラミング・インターフェース情報

本書には、プログラムを作成するユーザーが IBM i5/OS のサービスを使用するためのプログラミング・インターフェースが記述されています。

商標

以下は、IBM Corporation の商標です。

AS/400
e(ロゴ)server
eServer
i5/OS
IBM
IBM (ロゴ)
iSeries
OS/2
Redbooks

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名などはそれぞれ各社の商標または登録商標です。

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。 ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、第三者の権利の不侵害の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12