



IBM i

ネットワーキング

DHCP (Dynamic Host Configuration Protocol)

7.1





IBM i

ネットワーキング

DHCP (Dynamic Host Configuration Protocol)

7.1

ご注意!

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 i 7.1 (プロダクト番号 5770-SS1)、および新しい版で明記されていない限り、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 モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

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 i
Networking
Dynamic Host Configuration Protocol
7.1

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

第1刷 2010.4

© Copyright International Business Machines Corporation 1998, 2010.

目次

動的ホスト構成プロトコル	1		ISC の DHCP 4 の使用	52
IBM i 7.1 の新機能	1		ISC DHCP サーバーの使用に関する考慮事項	53
DHCP の PDF ファイル	1		DHCP フェイルオーバー	54
DHCP の概念	2		DHCP を使用するためのクライアントの構成	54
DHCP クライアント/サーバー間の対話	2		Windows Me クライアント用に DHCP を使用可能に設定	54
リース	5		Windows Me クライアントの DHCP リースの検査	54
リレー・エージェントとルーター	7		Windows 2000 クライアント用に DHCP を使用可能に設定	55
DHCP クライアントのサポート	8		MAC アドレスおよび DHCP リースの検査	55
BOOTP	9		DNS A レコードの更新	55
動的更新	9		Windows XP クライアント用に DHCP を使用可能に設定	56
DHCP オプションの検索	11		MAC アドレスおよび DHCP リースの検査	56
例: DHCP	27		DNS A レコードの更新	56
例: 単純な DHCP サブネット	28		動的更新を DNS に送信するための DHCP の構成	57
例: 複数の TCP/IP サブネット	30		DNS 動的更新を使用不可に設定	58
例: DHCP とマルチホーミング	32		リースされた IP アドレスの管理	58
例: DNS と DHCP が同じ System i 上にある場合	36		DHCP のトラブルシューティング	59
例: DNS と DHCP プロファイルが異なる System i モデル上にある場合	38		詳しい DHCP エラー情報の収集	59
例: PPP と DHCP が単一 System i 上にある場合	40		DHCP サーバーのトレース	59
例: DHCP と PPP プロファイルが異なる System i モデル上にある場合	42		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	60
DHCP の計画	45		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	61
セキュリティーに関する考慮事項	46		問題: DNS レコードが DHCP によって更新されない	61
ネットワーク・トポロジーに関する考慮事項	46		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	63
DHCP の構成	49		DHCP の関連情報	63
DHCP サーバーおよび BOOTP/DHCP リレー・エージェントの構成	50			
DHCP サーバーの構成または表示	50			
DHCP サーバーの始動または停止	50			
自動的に始動するための DHCP サーバーの構成	51			
DHCP サーバー・モニターのアクセス	51			
BOOTP/DHCP リレー・エージェントの構成	51			
BOOTP/DHCP リレー・エージェントの始動または停止	51			
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	51			
ISC の DHCP 4 を使用するための DHCP サーバーの構成	52			
			付録. 特記事項	65
			プログラミング・インターフェース情報	67
			商標	67
			使用条件	67

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、セントラル・サーバーを使用して IP アドレスやその他のネットワーク全体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を割り当てます。

IBM i 7.1 の新機能

動的ホスト構成プロトコルのトピック・コレクションに関する新情報や重要な変更情報について説明します。



ISC DHCP 4

DHCP バージョン 4 の実装として業界標準になっている Internet Systems Consortium (ISC), Inc. による実装環境を、IBM® i で使用できるようになりました。

- ISC の DHCP 4 では、IBM i の DHCP サーバー実装では現在使用できない機能が提供されています。
- ISC の DHCP 4 の使用方法についての情報を記載しています。
- マイグレーション時に必要な ISC DHCP サーバーの使用に関する考慮事項について説明します。
- ISC DHCP 4 サーバーは、2 つの DHCP サーバー・ピア間の DHCP フェイルオーバーをサポートするようになりました。

新規情報または変更情報の見分け方

技術上の変更が加えられた場所を見分けるのに役立つように、Information Center では以下のイメージを使用しています。

-  イメージにより、新規または変更された情報の開始点を示します。
-  イメージにより、新規または変更された情報の終了点を示します。

PDF ファイルでは、左マージンに新規および変更情報のリビジョン・バー (I) があります。

今回のリリースの新規情報または変更情報に関するその他の情報は、プログラム資料説明書を参照してください。

DHCP の PDF ファイル

この情報の PDF ファイルを表示または印刷できます。

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

PDF ファイルの保存

表示または印刷のために PDF をワークステーションに保存するには、以下のようになります。

1. ご使用のブラウザで PDF 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

これらの PDF を表示または印刷するには、Adobe Reader がご使用のシステムにインストールされている必要があります。このアプリケーションは、Adobe Web サイト

(www.adobe.com/products/acrobat/readstep.html)  から無償でダウンロードできます。

関連資料

63 ページの『DHCP の関連情報』

IBM Redbooks® および Web サイトには DHCP トピックのコレクションに関連する情報が収められています。PDF ファイルはいつでも表示および印刷できます。

DHCP の概念

動的ホスト構成プロトコル (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 をよく理解していただくために、いくつかの DHCP 関連概念について説明します。

DHCP クライアント/サーバー間の対話

動的ホスト構成プロトコル (DHCP) クライアントとサーバー間の対話により、クライアントはその IP アドレスと対応する構成情報を DHCP サーバーから取得することが可能になります。

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。

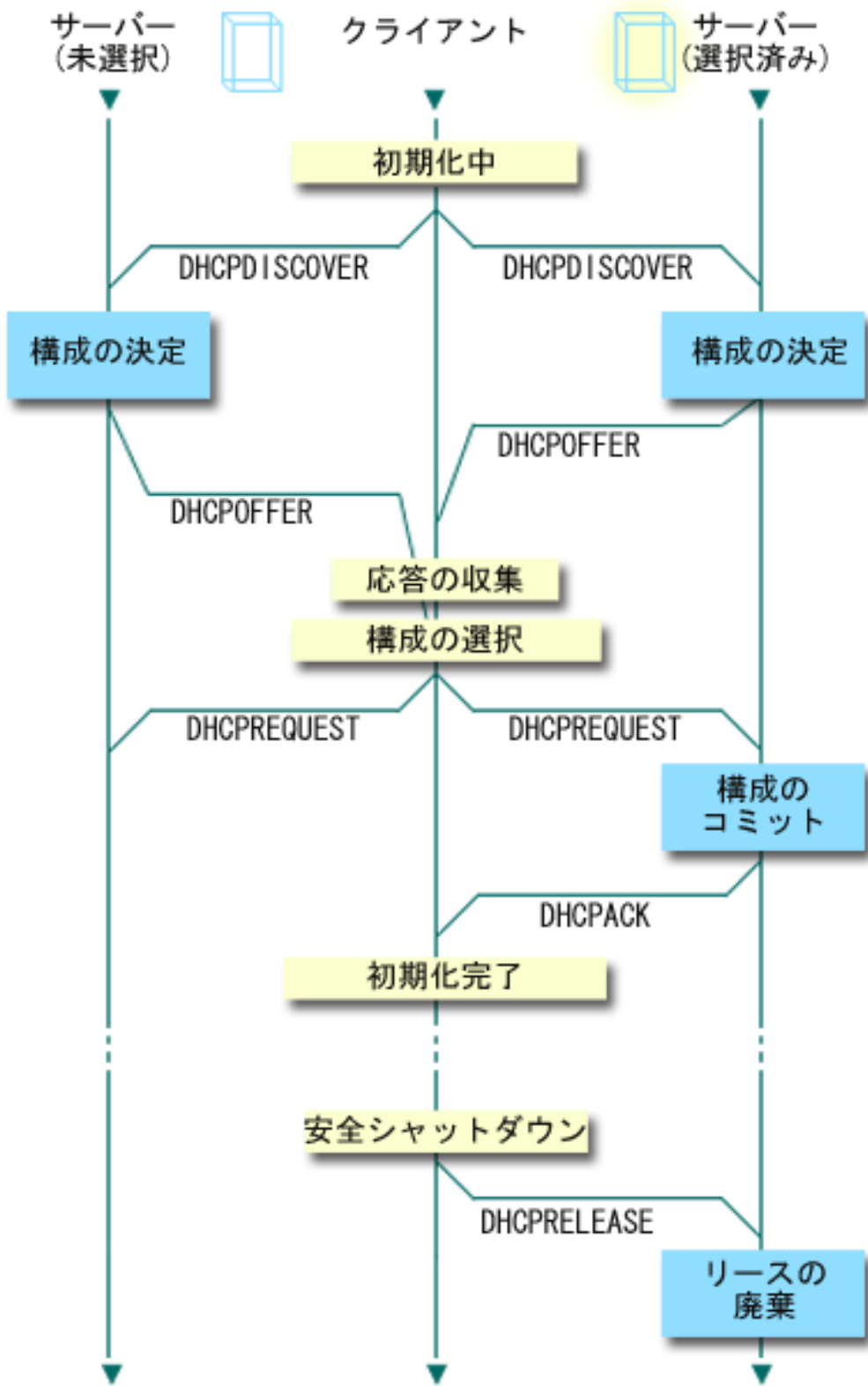


図1. DHCP クライアント/サーバー間の対話

「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 DHCPDISCOVER メッセージを送信します。

DHCPDISCOVER 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使用されている場合、接続されているネットワーク上の DHCP サーバーに DHCPDISCOVER 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 : DHCPPOFFER」

DHCPDISCOVER メッセージを受信した DHCP サーバーは、応答として DHCPPOFFER メッセージを送信できます。この DHCP サーバーがクライアントに DHCPPOFFER メッセージを送り返さ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、サブネットが構成されていない、もしくはクライアントがサポートされていない、などです。DHCP サーバーが応答として DHCPPOFFER メッセージを送信した場合、DHCPPOFFER 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、DHCPDISCOVER メッセージに回答した DHCP サーバーから DHCPPOFFER 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、DHCPREQUEST 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、DHCPREQUEST 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、リース時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、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。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。サーバーが要求に回答しない場合、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、DHCPRELEASE 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

7 ページの『リレー・エージェントとルーター』

動的ホスト構成プロトコル (DHCP) リレー・エージェントとルーターを使用して、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 が構成情報をクライアントに送信する場合、その情報は、リース時間付きで送信されます。リース時間とは、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。リース時間はそれぞれの要求に応じて変更できます。

リース

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、リース時間付きで送信されます。リース時間とは、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。リース時間はそれぞれの要求に応じて変更できます。

リースの期間中、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、リース時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 サーバーのリース時間を設定する場合、その目標、サイトの使用パターン、および DHCP サーバーのサービスの配置について考慮します。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、有効期限が切れて未使用リースにな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く場合、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。リース時間を短くすると、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時間に対して少なくとも 2 倍あれば、すでにリースに入っている稼働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にします。この場合、すべてのクライアントそれぞれに IP アドレス・セットを別に 1 つ持つ必要はありません。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、より頻繁に交渉するようになるため、ネットワーク・トラフィックが過剰に発生します。

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。リース時間が長いと、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間待たなければならない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。しかし、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ら、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きに、問題が発生する可能性があります。

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、それに長いリース時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、その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。DHCP サーバーはそのクライアント専用として IP アドレスを予約します。そうすれば、たとえば、新規ファイル・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、サーバーはその新規ファ

イル・サーバーに同じアドレスを割り当てることができます。新規ファイル・サーバーに無限リースを指定した場合、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ができません。

関連概念

46 ページの『ネットワーク・トポロジーに関する考慮事項』

動的ホスト構成プロトコル (DHCP) セットアップの計画は、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、などのいくつかの要因を検討する必要があります。

関連資料

2 ページの『DHCP クライアント/サーバー間の対話』

動的ホスト構成プロトコル (DHCP) クライアントとサーバー間の対話により、クライアントはその IP アドレスと対応する構成情報を DHCP サーバーから取得することが可能になります。

リレー・エージェントとルーター

動的ホスト構成プロトコル (DHCP) リレー・エージェントとルーターを使用して、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 DHCPDISCOVER 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 サーバーが配置されている 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、そのルーターは DHCP パケットを DHCP サーバーが配置されている LAN に転送します。ただし、多くのルーターは、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) の転送をサポートしません。この場合、DHCP サーバーが接続されている LAN に DHCP パケットを転送するために、LAN にはブートストラップ・プロトコル (BOOTP)/DHCP リレー・エージェントが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、42 ページの『例: DHCP と PPP プロファイルが異なる System i モデル上にある場合』を参照してください。

いずれの場合でも、DHCP サーバーは別に分離されたネットワーク上にあるため、ご使用のクライアントは、そのクライアントのネットワークを DHCP サーバーのあるネットワークへ接続するための、ルーターの IP アドレスを持っている必要があります。この DHCP サーバーはルーター・オプション (オプション 3) に指定されます。

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。ネットワークに接続される DHCP サーバーの台数を決める際に参考になる 46 ページの『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

46 ページの『ネットワーク・トポロジーに関する考慮事項』

動的ホスト構成プロトコル (DHCP) セットアップの計画は、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、などのいくつかの要因を検討する必要があります。

関連タスク

50 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』

DHCP サーバーおよび BOOTP/DHCP リレー・エージェントで、DHCP サーバーまたは BOOTP/DHCP リレー・エージェントの構成、開始、または停止などの作業を行う場合は、以下の情報を使用してください。

関連資料

2 ページの『DHCP クライアント/サーバー間の対話』

動的ホスト構成プロトコル (DHCP) クライアントとサーバー間の対話により、クライアントはその IP アドレスと対応する構成情報を DHCP サーバーから取得することが可能になります。

DHCP クライアントのサポート

DHCP を使用して、ラージ・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、またはクライアントのタイプ (ブートストラップ・プロトコル (BOOTP) または DHCP) における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、アドレスの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 (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

『BOOTP』

ブートストラップ・プロトコル (BOOTP) は、動的ホスト構成プロトコル (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 は DHCP のサブセットです。

46 ページの『ネットワーク・トポロジーに関する考慮事項』

動的ホスト構成プロトコル (DHCP) セットアップの計画は、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、などのいくつかの要因を検討する必要があります。

BOOTP

ブートストラップ・プロトコル (BOOTP) は、動的ホスト構成プロトコル (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 は DHCP のサブセットです。

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。BOOTP には動的アドレス割り当てではなく、各ネットワーク・クライアントは BOOTP 構成で識別する必要があり、クライアントは BOOTP サーバーから一定限度の量の構成情報だけを受け取ることができます。

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 を使用している場合は、BOOTP クライアントに影響を与えずに、DHCP をセットアップして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、システム全体または各種サブネットに対して BOOTP サポートをオン (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 を使用の方が優先されます。DHCP を使用して BOOTP クライアントをサポートする場合でも、それぞれの 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

8 ページの『DHCP クライアントのサポート』

DHCP を使用して、ラージ・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

46 ページの『ネットワーク・トポロジーに関する考慮事項』

動的ホスト構成プロトコル (DHCP) セットアップの計画は、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、などのいくつかの要因を検討する必要があります。

動的更新

動的ホスト構成プロトコル (DHCP) がクライアントに IP アドレスを割り当てる際に、ドメイン・ネーム・システム (DNS) サーバーと一緒に DHCP サーバーを構成して 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 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、ユーザーは IP アドレス (xxx.xxx.xxx.xxx) を使用するのではなく、「www.example.com」などの単純名を使用してホストを配置することができます。

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。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 サーバーへ自動的に送信できるため、ネットワーク内の他のホストは、その新しい IP アドレスで DNS を照会することにより、そのクライアント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 System i® モデル、異なる System i モデル、または動的更新が可能な他のシステム上の DNS と DHCP との間で行うことができます。

関連概念

Domain Name System

46 ページの『ネットワーク・トポロジに関する考慮事項』

動的ホスト構成プロトコル (DHCP) セットアップの計画は、ネットワーク・トポロジ、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、などのいくつかの要因を検討する必要があります。

61 ページの『問題: DNS レコードが DHCP によって更新されない』

System i 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。 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。この情報は動的更新のエラーをトラブルシューティングするときに役立ちます。

関連タスク

57 ページの『動的更新を DNS に送信するための DHCP の構成』

動的ホスト構成プロトコル (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。

Configuring DNS to receive dynamic updates

関連資料

Domain Name System resource records

DHCP オプションの検索

動的ホスト構成プロトコル (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 オプションを参照するための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。 System i Navigator ナビゲーターの「DHCP オプション」画面を使用して、カスタマイズされたオプションも構成できます。

表 1. 標準 DHCP オプション

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)	<p>サブネット・マスク・オプションは、 Request For Comments (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指定する必要があります。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">サブネット・マスク (Subnet mask)</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>4</td> <td>m1</td> <td>m2</td> <td>m3</td> <td>m4</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG530-0</p>	コード (Code)	Len	サブネット・マスク (Subnet mask)				1	4	m1	m2	m3	m4						
コード (Code)	Len	サブネット・マスク (Subnet mask)																		
1	4	m1	m2	m3	m4															
2	時間オフセット (Time offset)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">時間オフセット (Time offset)</th> </tr> </thead> <tbody> <tr> <td>2</td> <td>4</td> <td>n1</td> <td>n2</td> <td>n3</td> <td>n4</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG531-0</p>	コード (Code)	Len	時間オフセット (Time offset)				2	4	n1	n2	n3	n4						
コード (Code)	Len	時間オフセット (Time offset)																		
2	4	n1	n2	n3	n4															
3	ルーター (Router)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG511-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			3	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
3	n	a1	a2	a3	a4	a1	a2	...												
4	タイム・サーバー (Time server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>4</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG512-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			4	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
4	n	a1	a2	a3	a4	a1	a2	...												

表 1. 標準 DHCP オプション (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)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>5</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG513-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			5	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
5	n	a1	a2	a3	a4	a1	a2	...												
6	ドメイン・ネーム・サーバー (Domain Name Server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>6</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG514-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			6	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
6	n	a1	a2	a3	a4	a1	a2	...												
7	ログ・サーバー (Log server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>7</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG515-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			7	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
7	n	a1	a2	a3	a4	a1	a2	...												
8	Cookie サーバー (Cookie server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>8</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG516-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			8	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
8	n	a1	a2	a3	a4	a1	a2	...												

表 1. 標準 DHCP オプション (続き)

オプション番号	オプション	説明																		
9	LPR サーバー (LPR server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>9</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG517-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			9	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
9	n	a1	a2	a3	a4	a1	a2	...												
10	Impress サーバー (Impress server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>10</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG518-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			10	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
10	n	a1	a2	a3	a4	a1	a2	...												
11	リソース・ロケーション・サーバー (Resource location server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>11</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG519-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			11	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
11	n	a1	a2	a3	a4	a1	a2	...												
12	ホスト名 (Host name)	<p>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。</p> <p>このオプションのコードは 12 であり、長さは 1 以上です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="6">ホスト名 (Host name)</th> </tr> </thead> <tbody> <tr> <td>12</td> <td>n</td> <td>h1</td> <td>h2</td> <td>h3</td> <td>h4</td> <td>h5</td> <td>h6</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG520-0</p>	コード (Code)	Len	ホスト名 (Host name)						12	n	h1	h2	h3	h4	h5	h6	...	
コード (Code)	Len	ホスト名 (Host name)																		
12	n	h1	h2	h3	h4	h5	h6	...												

表 1. 標準 DHCP オプション (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)	<p>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。</p> <p>このオプションのコードは 13 であり、長さは 2 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="2">ファイル・サイズ (File size)</th> </tr> </thead> <tbody> <tr> <td>13</td> <td>2</td> <td>11</td> <td>12</td> </tr> </tbody> </table> <p>RZAKG541-0</p>	コード (Code)	Len	ファイル・サイズ (File size)		13	2	11	12						
コード (Code)	Len	ファイル・サイズ (File size)														
13	2	11	12													
14	Merit ダンプ・ファイル (Merit dump file)	<p>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。</p> <p>このオプションのコードは 14 です。長さは 1 以上です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="5">ダンプ・ファイル・パス名 (Dump file pathname)</th> </tr> </thead> <tbody> <tr> <td>14</td> <td>n</td> <td>n1</td> <td>n2</td> <td>n3</td> <td>n4</td> <td>...</td> </tr> </tbody> </table> <p>RZAKG521-0</p>	コード (Code)	Len	ダンプ・ファイル・パス名 (Dump file pathname)					14	n	n1	n2	n3	n4	...
コード (Code)	Len	ダンプ・ファイル・パス名 (Dump file pathname)														
14	n	n1	n2	n3	n4	...										
15	ドメイン・ネーム (Domain name)	<p>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。</p> <p>このオプションのコードは 15 です。長さは 1 以上です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="5">ドメイン・ネーム (Domain name)</th> </tr> </thead> <tbody> <tr> <td>15</td> <td>n</td> <td>d1</td> <td>d2</td> <td>d3</td> <td>d4</td> <td>...</td> </tr> </tbody> </table> <p>RZAKG522-0</p>	コード (Code)	Len	ドメイン・ネーム (Domain name)					15	n	d1	d2	d3	d4	...
コード (Code)	Len	ドメイン・ネーム (Domain name)														
15	n	d1	d2	d3	d4	...										
16	スワップ・サーバー (Swap server)	<p>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。</p> <p>このオプションのコードは 16 であり、長さは 4 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">スワップ・サーバー・アドレス (Swap server address)</th> </tr> </thead> <tbody> <tr> <td>16</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> </tr> </tbody> </table> <p>RZAKG523-0</p>	コード (Code)	Len	スワップ・サーバー・アドレス (Swap server address)				16	n	a1	a2	a3	a4		
コード (Code)	Len	スワップ・サーバー・アドレス (Swap server address)														
16	n	a1	a2	a3	a4											
17	ルート・パス (Root path)	<p>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。</p> <p>このオプションのコードは 17 です。長さは 1 以上です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="5">ルート・ディスク・パス名 (Root disk pathname)</th> </tr> </thead> <tbody> <tr> <td>17</td> <td>n</td> <td>n1</td> <td>n2</td> <td>n3</td> <td>n4</td> <td>...</td> </tr> </tbody> </table> <p>RZAKG524-0</p>	コード (Code)	Len	ルート・ディスク・パス名 (Root disk pathname)					17	n	n1	n2	n3	n4	...
コード (Code)	Len	ルート・ディスク・パス名 (Root disk pathname)														
17	n	n1	n2	n3	n4	...										

表 1. 標準 DHCP オプション (続き)

オプション番号	オプション	説明							
18	拡張パス (Extensions path)	<p>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で、ただし、以下の例外があります。</p> <ul style="list-style-type: none"> 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。 <p>このオプションのコードは 18 です。長さは 1 以上です。</p> <p>コード (Code) Len 拡張パス名</p> <table border="1"> <tr> <td>18</td> <td>n</td> <td>n1</td> <td>n2</td> <td>n3</td> <td>n4</td> <td>...</td> </tr> </table> <p style="text-align: right;">RZAKG525-0</p>	18	n	n1	n2	n3	n4	...
18	n	n1	n2	n3	n4	...			
19	IP 転送 (IP forwarding)	<p>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。</p> <p>このオプションのコードは 19 であり、長さは 1 です。</p> <p>コード (Code) Len 値</p> <table border="1"> <tr> <td>19</td> <td>1</td> <td>0/1</td> </tr> </table> <p style="text-align: right;">RZAKG544-0</p>	19	1	0/1				
19	1	0/1							
20	非ローカル・ソース・ルーティング (Non-Local source routing)	<p>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。</p> <p>このオプションのコードは 20 であり、長さは 1 です。</p> <p>コード (Code) Len 値</p> <table border="1"> <tr> <td>20</td> <td>1</td> <td>0/1</td> </tr> </table> <p style="text-align: right;">RZAKG545-0</p>	20	1	0/1				
20	1	0/1							

表 1. 標準 DHCP オプション (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)	<p>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。</p> <p>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。</p> <p>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。</p> <p>コード (Code) Len アドレス 1 (Address 1) マスク 1</p> <table border="1"> <tr> <td>21</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>m1</td> <td>m2</td> <td>m3</td> <td>m4</td> </tr> </table> <p>アドレス 2 (Address 2) マスク 2</p> <table border="1"> <tr> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>m1</td> <td>m2</td> <td>m3</td> <td>m4</td> <td>...</td> </tr> </table> <p style="text-align: right;">RZAKG510-0</p>	21	n	a1	a2	a3	a4	m1	m2	m3	m4	a1	a2	a3	a4	m1	m2	m3	m4	...
21	n	a1	a2	a3	a4	m1	m2	m3	m4												
a1	a2	a3	a4	m1	m2	m3	m4	...													
22	最大データグラム再アセンブル・サイズ (Maximum datagram reassembly size)	<p>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ない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。</p> <p>このオプションのコードは 22 であり、長さは 2 です。</p> <p>コード (Code) Len サイズ (Size)</p> <table border="1"> <tr> <td>22</td> <td>2</td> <td>s1</td> <td>s2</td> </tr> </table> <p style="text-align: right;">RZAKG542-0</p>	22	2	s1	s2															
22	2	s1	s2																		
23	デフォルト IP 存続時間 (Default IP time to live)	<p>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。</p> <p>このオプションのコードは 23 であり、長さは 1 です。</p> <p>コード (Code) Len TTL</p> <table border="1"> <tr> <td>23</td> <td>1</td> <td>ttl</td> </tr> </table> <p style="text-align: right;">RZAKG546-0</p>	23	1	ttl																
23	1	ttl																			
24	Path MTU エージング・タイムアウト (Path MTU aging timeout)	<p>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。</p> <p>このオプションのコードは 24 であり、長さは 4 です。</p> <p>コード (Code) Len タイムアウト (Timeout)</p> <table border="1"> <tr> <td>24</td> <td>4</td> <td>t1</td> <td>t2</td> <td>t3</td> <td>t4</td> </tr> </table> <p style="text-align: right;">RZAKG532-0</p>	24	4	t1	t2	t3	t4													
24	4	t1	t2	t3	t4																

表 1. 標準 DHCP オプション (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)	<p>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。</p> <p>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。</p> <p>コード (Code) Len サイズ 1 サイズ 2</p> <table border="1"> <tr> <td>25</td> <td>n</td> <td>s1</td> <td>s2</td> <td>s1</td> <td>s2</td> <td>...</td> </tr> </table> <p>RZAKG526-0</p>	25	n	s1	s2	s1	s2	...
25	n	s1	s2	s1	s2	...			
26	インターフェース MTU (Interface MTU)	<p>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。</p> <p>このオプションのコードは 26 であり、長さは 2 です。</p> <p>コード (Code) Len MTU</p> <table border="1"> <tr> <td>26</td> <td>2</td> <td>m1</td> <td>m2</td> </tr> </table> <p>RZAKG543-0</p>	26	2	m1	m2			
26	2	m1	m2						
27	すべてのサブネットがローカル (All subnets are local)	<p>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。</p> <p>このオプションのコードは 27 であり、長さは 1 です。</p> <p>コード (Code) Len 値</p> <table border="1"> <tr> <td>27</td> <td>1</td> <td>0/1</td> </tr> </table> <p>RZAKG547-0</p>	27	1	0/1				
27	1	0/1							
28	ブロードキャスト・アドレス (Broadcast address)	<p>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。</p> <p>このオプションのコードは 28 であり、長さは 4 です。</p> <p>コード (Code) Len ブロードキャスト・アドレス (Broadcast address)</p> <table border="1"> <tr> <td>28</td> <td>4</td> <td>b1</td> <td>b2</td> <td>b3</td> <td>b4</td> </tr> </table> <p>RZAKG533-0</p>	28	4	b1	b2	b3	b4	
28	4	b1	b2	b3	b4				

表 1. 標準 DHCP オプション (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)	<p>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。</p> <p>このオプションのコードは 29 であり、長さは 1 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th>値</th> </tr> </thead> <tbody> <tr> <td>29</td> <td>1</td> <td>0/1</td> </tr> </tbody> </table> <p>RZAKG548-0</p>	コード (Code)	Len	値	29	1	0/1												
コード (Code)	Len	値																		
29	1	0/1																		
30	マスク・サプライヤー (Mask supplier)	<p>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。</p> <p>このオプションのコードは 30 であり、長さは 1 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th>値</th> </tr> </thead> <tbody> <tr> <td>30</td> <td>1</td> <td>0/1</td> </tr> </tbody> </table> <p>RZAKG549-0</p>	コード (Code)	Len	値	30	1	0/1												
コード (Code)	Len	値																		
30	1	0/1																		
31	ルーター・ディスカバリーの実行 (Perform router discovery)	<p>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。</p> <p>このオプションのコードは 31 であり、長さは 1 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th>値</th> </tr> </thead> <tbody> <tr> <td>31</td> <td>1</td> <td>0/1</td> </tr> </tbody> </table> <p>RZAKG550-0</p>	コード (Code)	Len	値	31	1	0/1												
コード (Code)	Len	値																		
31	1	0/1																		
32	ルーター送信請求アドレス (Router solicitation address) オプション	<p>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。</p> <p>このオプションのコードは 32 であり、長さは 4 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス (Address)</th> </tr> <tr> <th></th> <th></th> <th>a1</th> <th>a2</th> <th>a3</th> <th>a4</th> </tr> </thead> <tbody> <tr> <td>32</td> <td>4</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> </tr> </tbody> </table> <p>RZAKG534-0</p>	コード (Code)	Len	アドレス (Address)						a1	a2	a3	a4	32	4	a1	a2	a3	a4
コード (Code)	Len	アドレス (Address)																		
		a1	a2	a3	a4															
32	4	a1	a2	a3	a4															

表 1. 標準 DHCP オプション (続き)

オプション番号	オプション	説明																																					
33	静的ルート (Static route)	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">宛先 1 (Destination 1)</th> <th colspan="4">ルーター 1 (Router 1)</th> </tr> </thead> <tbody> <tr> <td>33</td> <td>n</td> <td>d1</td> <td>d2</td> <td>d3</td> <td>d4</td> <td>r1</td> <td>R2</td> <td>r3</td> <td>r4</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="4">宛先 2 (Destination 2)</th> <th colspan="4">ルーター 2 (Router 2)</th> </tr> </thead> <tbody> <tr> <td>d1</td> <td>d2</td> <td>d3</td> <td>d4</td> <td>r1</td> <td>r2</td> <td>r3</td> <td>r4</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG509-0</p>	コード (Code)	Len	宛先 1 (Destination 1)				ルーター 1 (Router 1)				33	n	d1	d2	d3	d4	r1	R2	r3	r4	宛先 2 (Destination 2)				ルーター 2 (Router 2)				d1	d2	d3	d4	r1	r2	r3	r4	...
コード (Code)	Len	宛先 1 (Destination 1)				ルーター 1 (Router 1)																																	
33	n	d1	d2	d3	d4	r1	R2	r3	r4																														
宛先 2 (Destination 2)				ルーター 2 (Router 2)																																			
d1	d2	d3	d4	r1	r2	r3	r4	...																															
34	トレーラー・カプセル化 (Trailer encapsulation)	<p>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。</p> <p>このオプションのコードは 34 であり、長さは 1 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th>値</th> </tr> </thead> <tbody> <tr> <td>34</td> <td>1</td> <td>0/1</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG573-0</p>	コード (Code)	Len	値	34	1	0/1																															
コード (Code)	Len	値																																					
34	1	0/1																																					
35	ARP キャッシュ・タイムアウト (ARP cache timeout)	<p>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。</p> <p>このオプションのコードは 35 であり、長さは 4 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">時間 (Time)</th> </tr> </thead> <tbody> <tr> <td>35</td> <td>4</td> <td>t1</td> <td>t2</td> <td>t3</td> <td>t4</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG535-0</p>	コード (Code)	Len	時間 (Time)				35	4	t1	t2	t3	t4																									
コード (Code)	Len	時間 (Time)																																					
35	4	t1	t2	t3	t4																																		
36	イーサネット・カプセル化 (Ethernet encapsulation)	<p>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。</p> <p>このオプションのコードは 36 であり、長さは 1 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th>値</th> </tr> </thead> <tbody> <tr> <td>36</td> <td>1</td> <td>0/1</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG551-0</p>	コード (Code)	Len	値	36	1	0/1																															
コード (Code)	Len	値																																					
36	1	0/1																																					

表 1. 標準 DHCP オプション (続き)

オプション番号	オプション	説明														
37	TCP デフォルト TTL (TCP default TTL)	<p>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。</p> <p>このオプションのコードは 37 であり、長さは 1 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th>TTL</th> </tr> </thead> <tbody> <tr> <td>37</td> <td>1</td> <td>n</td> </tr> </tbody> </table> <p>RZAKG552-0</p>	コード (Code)	Len	TTL	37	1	n								
コード (Code)	Len	TTL														
37	1	n														
38	TCP キープアライブ・インターバル (TCP Keep-alive interval)	<p>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。</p> <p>このオプションのコードは 38 であり、長さは 4 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">時間 (Time)</th> </tr> </thead> <tbody> <tr> <td>38</td> <td>4</td> <td>t1</td> <td>t2</td> <td>t3</td> <td>t4</td> </tr> </tbody> </table> <p>RZAKG536-0</p>	コード (Code)	Len	時間 (Time)				38	4	t1	t2	t3	t4		
コード (Code)	Len	時間 (Time)														
38	4	t1	t2	t3	t4											
39	TCP キープアライブ・ガーベッジ (TCP Keep-alive garbage)	<p>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 1 ガーベッジ・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。</p> <p>このオプションのコードは 39 であり、長さは 1 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th>値</th> </tr> </thead> <tbody> <tr> <td>39</td> <td>1</td> <td>0/1</td> </tr> </tbody> </table> <p>RZAKG553-0</p>	コード (Code)	Len	値	39	1	0/1								
コード (Code)	Len	値														
39	1	0/1														
40	ネットワーク情報サービス・ドメイン (Network information service domain)	<p>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。</p> <p>このオプションのコードは 40 です。長さは 1 以上です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="5">NIS ドメイン・ネーム (NIS Domain name)</th> </tr> </thead> <tbody> <tr> <td>40</td> <td>n</td> <td>n1</td> <td>n2</td> <td>n3</td> <td>n4</td> <td>...</td> </tr> </tbody> </table> <p>RZAKG540-0</p>	コード (Code)	Len	NIS ドメイン・ネーム (NIS Domain name)					40	n	n1	n2	n3	n4	...
コード (Code)	Len	NIS ドメイン・ネーム (NIS Domain name)														
40	n	n1	n2	n3	n4	...										

表 1. 標準 DHCP オプション (続き)

オプション番号	オプション	説明																					
41	ネットワーク情報サーバー (Network information server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>41</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG556-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			41	n	a1	a2	a3	a4	a1	a2	...			
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)																	
41	n	a1	a2	a3	a4	a1	a2	...															
42	Network Time Protocol サーバー (Network time protocol servers) オプション	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>42</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG557-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			42	n	a1	a2	a3	a4	a1	a2	...			
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)																	
42	n	a1	a2	a3	a4	a1	a2	...															
44	NetBIOS over TCP/IP ネーム・サーバー (NetBIOS over TCP/IP name server)	<p>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。</p> <p>このオプションのコードは 44 です。このオプションの最小長さは 4 オクテットで、かつ、長さは常に 4 の倍数でなければなりません。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="4">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>44</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>b1</td> <td>b2</td> <td>b3</td> <td>b4</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG558-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)				44	n	a1	a2	a3	a4	b1	b2	b3	b4	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)																	
44	n	a1	a2	a3	a4	b1	b2	b3	b4	...													
45	NetBIOS over TCP/IP データグラム配布サーバー (NetBIOS over TCP/IP datagram distribution server)	<p>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。</p> <p>このオプションのコードは 45 です。このオプションの最小長さは 4 オクテットで、かつ、長さは常に 4 の倍数でなければなりません。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="4">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>45</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>b1</td> <td>b2</td> <td>b3</td> <td>b4</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG559-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)				45	n	a1	a2	a3	a4	b1	b2	b3	b4	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)																	
45	n	a1	a2	a3	a4	b1	b2	b3	b4	...													

表1. 標準 DHCP オプション (続き)

オプション番号	オプション	説明																		
46	NetBIOS over TCP/IP ノード・タイプ (NetBIOS over TCP/IP node type)	<p>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。</p> <table border="1"> <thead> <tr> <th>値</th> <th>ノード・タイプ (Node type)</th> </tr> </thead> <tbody> <tr> <td>0x1</td> <td>B ノード</td> </tr> <tr> <td>0x2</td> <td>P ノード</td> </tr> <tr> <td>0x4</td> <td>M ノード</td> </tr> <tr> <td>0x8</td> <td>H ノード</td> </tr> </tbody> </table> <p style="text-align: center;">RZAKG554-0</p> <p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th>ノード・タイプ (Node type)</th> </tr> </thead> <tbody> <tr> <td>46</td> <td>1</td> <td>上記参照</td> </tr> </tbody> </table> <p style="text-align: center;">RZAKG555-0</p>	値	ノード・タイプ (Node type)	0x1	B ノード	0x2	P ノード	0x4	M ノード	0x8	H ノード	コード (Code)	Len	ノード・タイプ (Node type)	46	1	上記参照		
値	ノード・タイプ (Node type)																			
0x1	B ノード																			
0x2	P ノード																			
0x4	M ノード																			
0x8	H ノード																			
コード (Code)	Len	ノード・タイプ (Node type)																		
46	1	上記参照																		
47	NetBIOS over TCP/IP 有効範囲 (NetBIOS over TCP/IP scope)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="5">NetBIOS スコープ</th> </tr> </thead> <tbody> <tr> <td>47</td> <td>n</td> <td>s1</td> <td>s2</td> <td>s3</td> <td>s4</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: center;">RZAKG528-0</p>	コード (Code)	Len	NetBIOS スコープ					47	n	s1	s2	s3	s4	...				
コード (Code)	Len	NetBIOS スコープ																		
47	n	s1	s2	s3	s4	...														
48	X Window システム・フォント・サーバー (X Window System Font server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>48</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: center;">RZAKG560-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			48	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
48	n	a1	a2	a3	a4	a1	a2	...												
49	X Window システム画面マネージャー (X Window System display manager)	<p>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。</p> <p>アドレスは優先順にリストしなければなりません。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>49</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: center;">RZAKG561-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			49	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
49	n	a1	a2	a3	a4	a1	a2	...												

表 1. 標準 DHCP オプション (続き)

オプション番号	オプション	説明														
51	IP アドレスのリース時間 (IP address lease time)	<p>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。</p> <p>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。</p> <p>このオプションのコードは 51 であり、長さは 4 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">リース時間</th> </tr> </thead> <tbody> <tr> <td>51</td> <td>4</td> <td>t1</td> <td>t2</td> <td>t3</td> <td>t4</td> </tr> </tbody> </table> <p>RZAKG537-0</p>	コード (Code)	Len	リース時間				51	4	t1	t2	t3	t4		
コード (Code)	Len	リース時間														
51	4	t1	t2	t3	t4											
58	更新 (T1) 時間値 (Renewal (T1) time value)	<p>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。</p> <p>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。</p> <p>このオプションのコードは 58 であり、長さは 4 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">T1 インターバル (T1 Interval)</th> </tr> </thead> <tbody> <tr> <td>58</td> <td>4</td> <td>t1</td> <td>t2</td> <td>t3</td> <td>t4</td> </tr> </tbody> </table> <p>RZAKG538-0</p>	コード (Code)	Len	T1 インターバル (T1 Interval)				58	4	t1	t2	t3	t4		
コード (Code)	Len	T1 インターバル (T1 Interval)														
58	4	t1	t2	t3	t4											
59	再バインド (T2) 時間値 (Rebinding (T2) time value)	<p>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。</p> <p>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。</p> <p>このオプションのコードは 59 であり、長さは 4 です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">T2 インターバル (T2 Interval)</th> </tr> </thead> <tbody> <tr> <td>59</td> <td>4</td> <td>t1</td> <td>t2</td> <td>t3</td> <td>t4</td> </tr> </tbody> </table> <p>RZAKG539-0</p>	コード (Code)	Len	T2 インターバル (T2 Interval)				59	4	t1	t2	t3	t4		
コード (Code)	Len	T2 インターバル (T2 Interval)														
59	4	t1	t2	t3	t4											
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)	<p>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。</p> <p>このオプションのコードは 64 です。長さは 1 以上です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="5">NIS クライアント・ドメイン・ネーム (NIS Client domain name)</th> </tr> </thead> <tbody> <tr> <td>64</td> <td>n</td> <td>n1</td> <td>n2</td> <td>n3</td> <td>n4</td> <td>...</td> </tr> </tbody> </table> <p>RZAKG527-0</p>	コード (Code)	Len	NIS クライアント・ドメイン・ネーム (NIS Client domain name)					64	n	n1	n2	n3	n4	...
コード (Code)	Len	NIS クライアント・ドメイン・ネーム (NIS Client domain name)														
64	n	n1	n2	n3	n4	...										

表 1. 標準 DHCP オプション (続き)

オプション番号	オプション	説明																		
65	NIS サーバー (NIS server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>65</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG562-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			65	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
65	n	a1	a2	a3	a4	a1	a2	...												
66	サーバー名 (Server name)	<p>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。</p> <p>このオプションのコードは 66 であり、長さは 1 以上です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">TFTP サーバー (TFTP Server)</th> </tr> </thead> <tbody> <tr> <td>66</td> <td>n</td> <td>c1</td> <td>c2</td> <td>c3</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG571-0</p>	コード (Code)	Len	TFTP サーバー (TFTP Server)				66	n	c1	c2	c3	...						
コード (Code)	Len	TFTP サーバー (TFTP Server)																		
66	n	c1	c2	c3	...															
67	ブート・ファイル名 (Boot file name)	<p>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。</p> <p>このオプションのコードは 67 であり、長さは 1 以上です。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">ブート・ファイル名 (Bootfile name)</th> </tr> </thead> <tbody> <tr> <td>67</td> <td>n</td> <td>c1</td> <td>c2</td> <td>c3</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG572-0</p>	コード (Code)	Len	ブート・ファイル名 (Bootfile name)				67	n	c1	c2	c3	...						
コード (Code)	Len	ブート・ファイル名 (Bootfile name)																		
67	n	c1	c2	c3	...															
68	ホーム・アドレス (Home address)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="5">ホーム・エージェント・アドレス (ゼロ以上) (Home agent addresses (zero or more))</th> </tr> </thead> <tbody> <tr> <td>68</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG529-0</p>	コード (Code)	Len	ホーム・エージェント・アドレス (ゼロ以上) (Home agent addresses (zero or more))					68	n	a1	a2	a3	a4	...				
コード (Code)	Len	ホーム・エージェント・アドレス (ゼロ以上) (Home agent addresses (zero or more))																		
68	n	a1	a2	a3	a4	...														
69	SMTP サーバー (SMTP server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>69</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG563-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			69	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
69	n	a1	a2	a3	a4	a1	a2	...												

表 1. 標準 DHCP オプション (続き)

オプション番号	オプション	説明																		
70	POP3 サーバー (POP3 server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>70</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG564-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			70	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
70	n	a1	a2	a3	a4	a1	a2	...												
71	NNTP サーバー (NNTP server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>71</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG565-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			71	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
71	n	a1	a2	a3	a4	a1	a2	...												
72	WWW サーバー (WWW server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>72</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG566-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			72	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
72	n	a1	a2	a3	a4	a1	a2	...												
73	Finger サーバー (Finger server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>73</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG567-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			73	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
73	n	a1	a2	a3	a4	a1	a2	...												
74	IRC サーバー (IRC server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>74</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG568-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			74	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
74	n	a1	a2	a3	a4	a1	a2	...												

表 1. 標準 DHCP オプション (続き)

オプション番号	オプション	説明																		
75	StreetTalk サーバー (StreetTalk server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>75</td> <td>n</td> <td>A1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG569-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			75	n	A1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
75	n	A1	a2	a3	a4	a1	a2	...												
76	STDA サーバー (STDA server)	<p>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。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>コード (Code)</th> <th>Len</th> <th colspan="4">アドレス 1 (Address 1)</th> <th colspan="3">アドレス 2 (Address 2)</th> </tr> </thead> <tbody> <tr> <td>76</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG570-0</p>	コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)			76	n	a1	a2	a3	a4	a1	a2	...
コード (Code)	Len	アドレス 1 (Address 1)				アドレス 2 (Address 2)														
76	n	a1	a2	a3	a4	a1	a2	...												
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。																		

関連情報

 DHCP Options and BOOTP Vendor Extensions

例: DHCP

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。以下に示す例は、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、および一部の VSR4 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

46 ページの『ネットワーク・トポロジーに関する考慮事項』

動的ホスト構成プロトコル (DHCP) セットアップの計画は、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、などのいくつかの要因を検討する必要があります。

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 内の動的ホスト構成プロトコル (DHCP) サーバーとして、System i モデルをセットアップする方法について説明します。

この例では、System i モデルは、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. System i モデルのための単純な 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 アドレスに関連した情報を入力して、この情報の保守を容易に行うことができます。(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。) この状態で、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、管理者はシステム上で DHCP ポリシーを 1 つ作成するだけで済みます。このポリシーで各クライアントに IP 情報を配布します。

PC クライアントがそれぞれの DHCPDISCOVER 信号を発信すると、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 情報を DHCP サーバーから取得する LAN ベースのプリンターも設置されています。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。この解決策の 1 つは、プリンターに固定の 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	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
システム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)
システムは DNS 更新を実行していますか?		No
システムは 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

『例: 複数の TCP/IP サブネット』

この例では、DHCP 対応ルーターで接続された 2 つの LAN を備えた動的ホスト構成プロトコル (DHCP) サーバーとして、System i モデル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』

この例では、インターネット・ルーターでインターネットに接続された LAN 対応の動的ホスト構成プロトコル (DHCP) サーバーとして、System i モデル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

この例では、DHCP 対応ルーターで接続された 2 つの LAN を備えた動的ホスト構成プロトコル (DHCP) サーバーとして、System i モデル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を除いて、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階にあり、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、2 つの LAN によるネットワークがルーターを使用して接続されている System i 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。実際の企業の場合、一般に、それぞれのサブネットごとのクライアントはかなりの数になっています。



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、DHCPDISCOVER 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
システム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)	
システムは DNS 更新を実行していますか?	No	
システムは 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

28 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 内の動的ホスト構成プロトコル (DHCP) サーバーとして、System i モデルをセットアップする方法について説明します。

例: DHCP とマルチホーミング

この例では、インターネット・ルーターでインターネットに接続された LAN 対応の動的ホスト構成プロトコル (DHCP) サーバーとして、System i モデルをセットアップする方法について説明します。

この例は、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 System i モデル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 System i 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、次の図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、システムはマルチホーミングです。

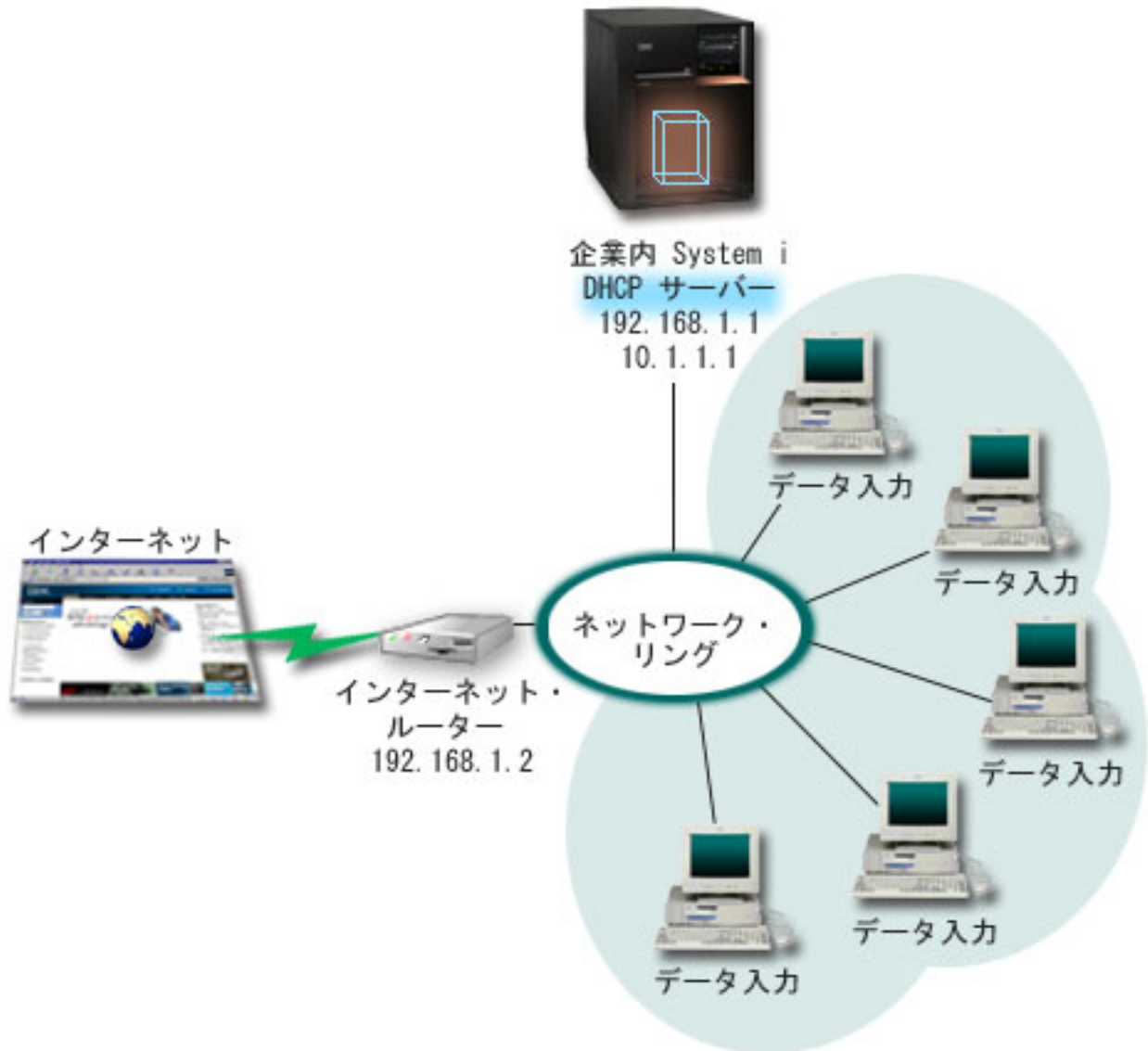


図4. 同じアダプターに複数の IP アドレスが割り当てられている DHCP の使用法

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、使用する DHCP サーバーを構成する際にはセキュリティーのかかわり合いを考慮してください。

DHCP セットアップを構成する場合は、System i モデルが 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 DHCPDISCOVER パケットを送信したときにどうなるかを理解しておくに役立ちます。

クライアントが DHCPDISCOVER パケットを送信すると、このパケットはネットワーク・リング上でブロードキャストされます。そのため、System i DHCP サーバーは、パケットがどの IP アドレスに向けられていたのか判別できません。このパケットに 10.1.1.1 インターフェイス 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 インターフェイ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・ネットワークのサブネット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。これを行うための最も簡単な方法は、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 (またはそれより多く) 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。DHCPDISCOVER パケットに 192.168.1.1 インターフェイスのマークが付けられている場合でも、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、インターネットにアクセスするために、データ入力サブネットがこのサブネットのクライアントに、これらのクライアントのルーター・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 System i インターフェイスです。さらに、2 つのインターフェイスが互いにパケットを経路指定するために、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、ネットワーク・アドレス変換 (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イスが同じネットワークに接続していればいつでも、同じ問題が発生する可能性があります。次の図は、System i モデル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。DHCPDISCOVER パケットは、192.168.1.1 インターフェイスによって応答される可能性があるためです。

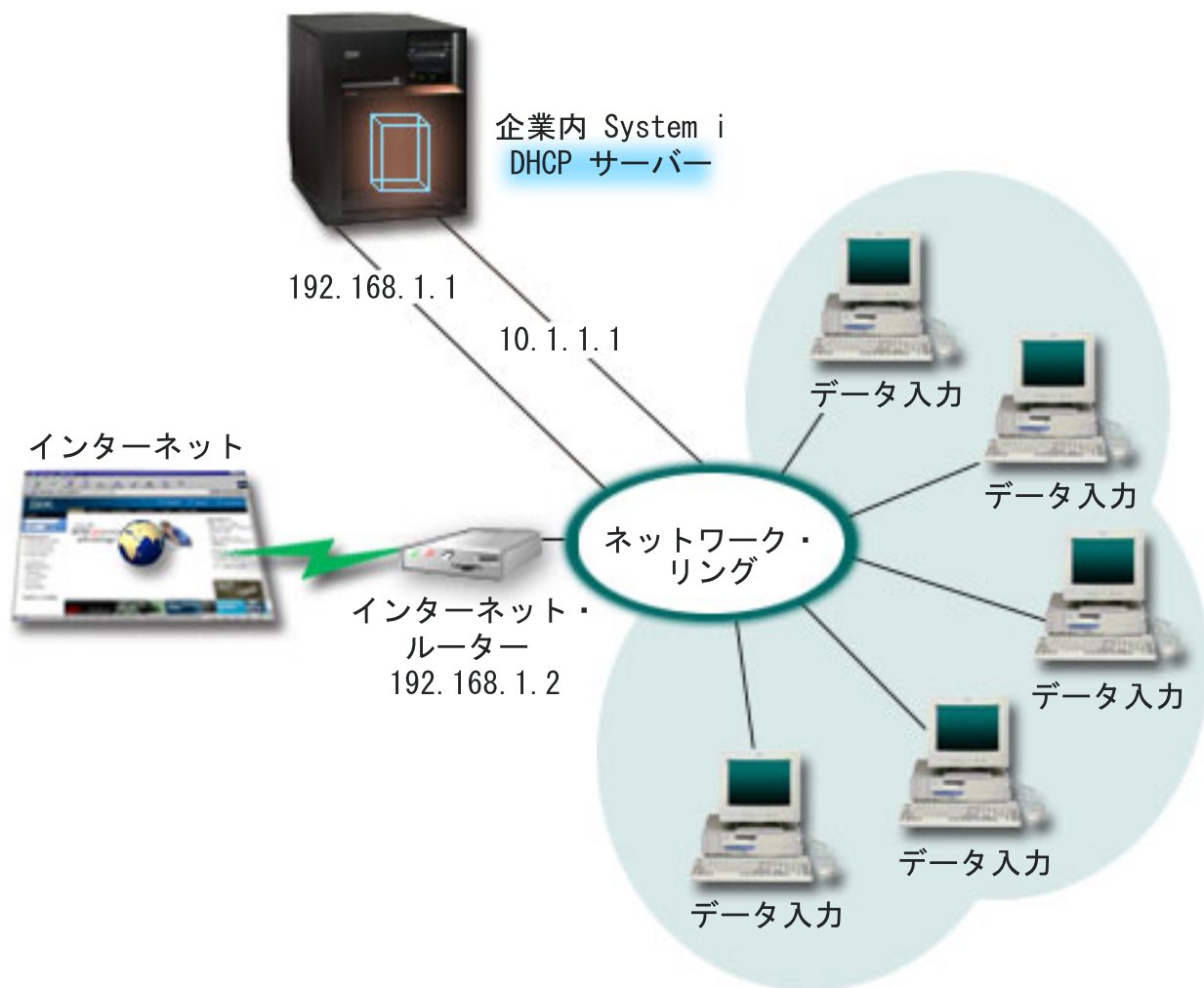


図5. 複数のインターフェースが同じネットワークに接続されている DHCP の使用法

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
システムは DNS 更新を実行していますか?	No
システムは 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 DHCPDISCOVER 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

関連資料

28 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 内の動的ホスト構成プロトコル (DHCP) サーバーとして、System i モデルをセットアップする方法について説明します。

例: DNS と DHCP が同じ System i 上にある場合

この例では、ドメイン・ネーム・システム (DNS) 更新と共存する動的ホスト構成プロトコル (DHCP) サーバーとして、System i モデルを簡易 LAN 上にセットアップする方法について説明します。

次の図を使って、System i モデルが DHCP および DNS サーバーとしてどのように機能するかについて、単純なサブネットで説明します。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。これらのクライアントは、ネットワーク・ドライブをそのホスト名にマッピングすることにより、グラフィックス・ファイル・サーバーに接続します。

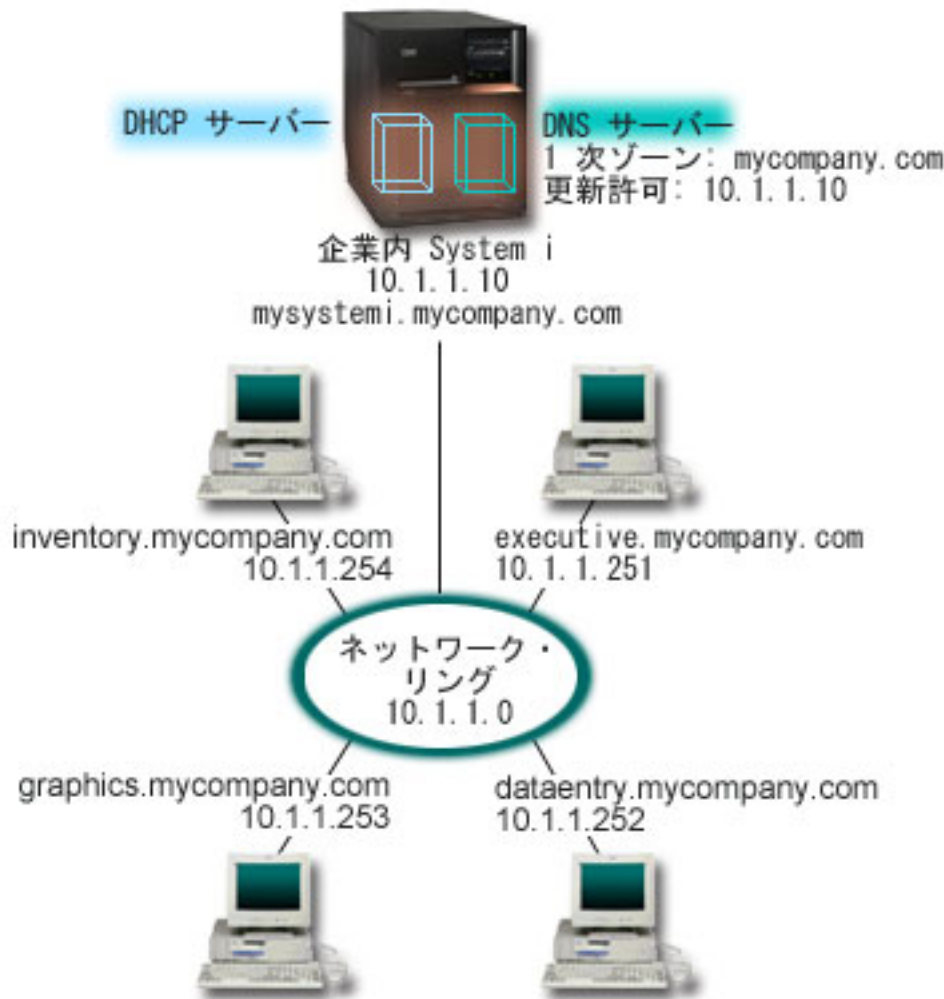


図6. 動的 DNS および DHCP

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。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。

現行 DNSサーバーを使用して、DHCP による断続的なアドレスの変更と同時に、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 トピックのコレクションに収められている「例: DNS と DHCP が同じ System i 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
システムは 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	
システムは 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。DNS トピックのコレクションに収められている「例: 同じ System i にある DNS と DHCP」を参照してください。

例: DNS と DHCP プロファイルが異なる System i モデル上にある場合

この例では、簡易 LAN を介して動的更新を実行するために、2 つの異なる System i モデル上に動的ホスト構成プロトコル (DHCP) とドメイン・ネーム・システム (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 が別個の System i モデル上で実行している小型のサブネット・ネットワークの説明です。DNS を実行するシステムは DNS と DHCP が同じ System i モデル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。

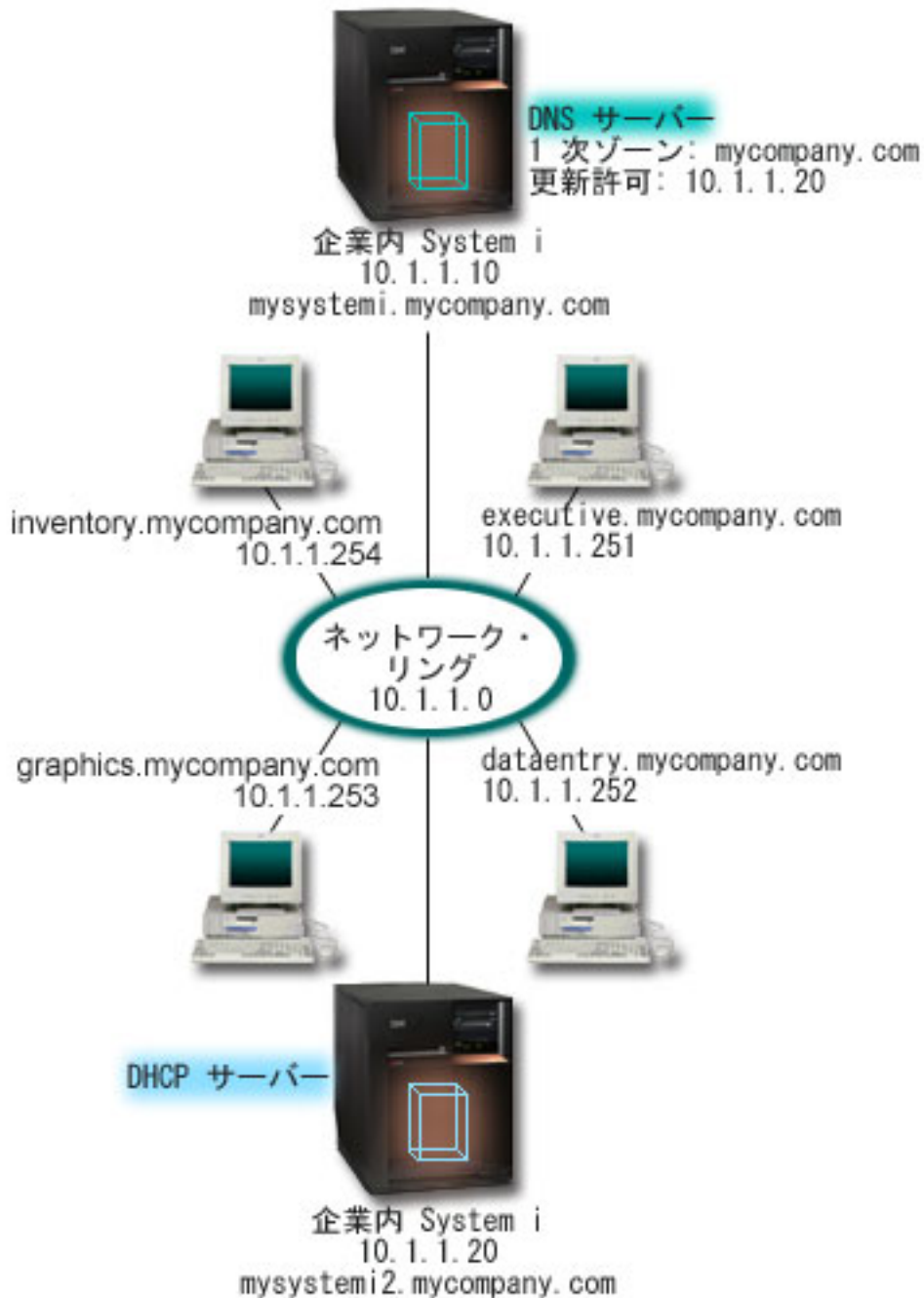


図7. DNS と DHCP プロファイルが異なる System i モデル上にある場合

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 System i 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® ドメイン・ネーム・システム (オプション 31) のインストール

DHCP を実行する System i モデル (この場合は、mysystemi2) 上に i5/OS ドメイン・ネーム・システム (オプション 31) をインストールします。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 System i モデル上に作成するには、以下の手順に従ってください。

1. System i Navigator で、「**対象のシステム**」→「**ネットワーク**」→「**サーバー**」→「**DNS**」の順に展開します。
2. 左側の画面区画で、「**DNS**」を右マウス・ボタンでクリックして、「**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、以下のフィールドに記入します。
 - **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 System i モデルおよび DHCP を実行する System i モデル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ます。

関連概念

Domain Name System requirements

関連情報

Update DNS API

例: PPP と DHCP が単一 System i 上にある場合

この例では、LAN およびリモート・ダイヤルイン・クライアント対応の動的ホスト構成プロトコル (DHCP) サーバーとして、System i モデル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、System i モデルには Point-to-Point Protocol (PPP) を使用してアクセス権限を取得できます。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に IP 情報が必要です。System i DHCP サーバーは、他のいずれの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場合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 (クライアント) を示しています。

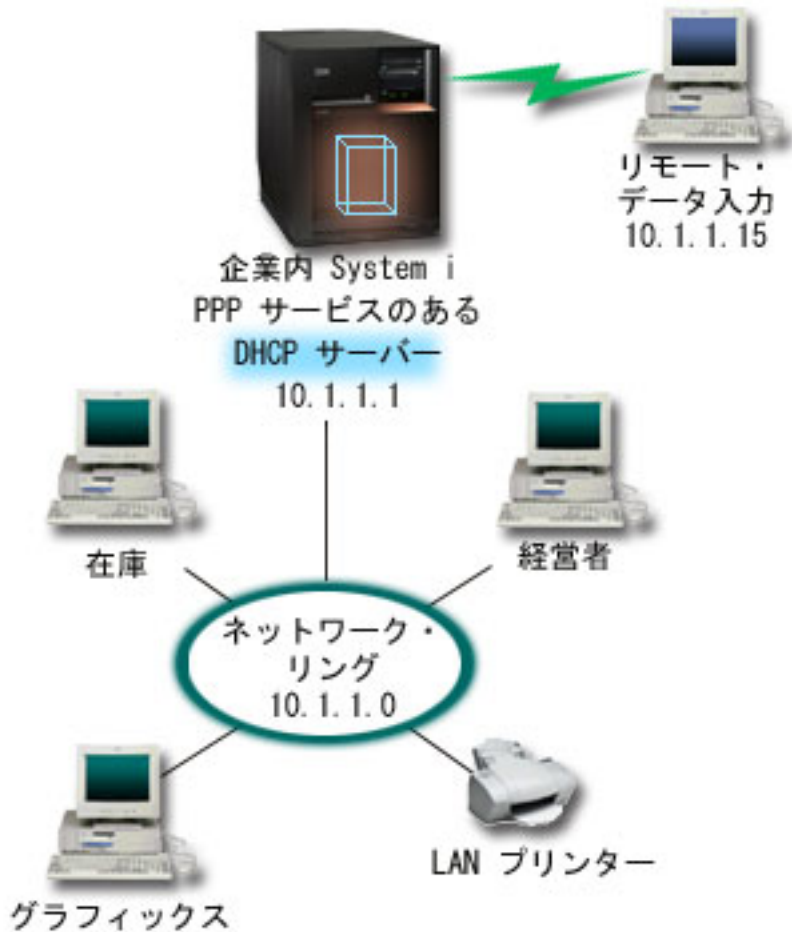


図8. PPP と DHCP が単一 System i モデルにある場合

遠隔地にいる従業員（クライアント）が正常に会社のネットワークの一部になるためには、System i モデルがリモート・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。リモート・アクセス・サービス機能は System i モデルのダイヤルイン機能を作成します。正しくセットアップされていれば、クライアントがダイヤルイン接続を確立すると、PPP サーバーが TCP/IP 情報をそのリモート・クライアントに配布するよう 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 プロファイルだけで「on (オン)」に設定した場合、System i モデルは 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含まれる 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 IP 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
システムは DNS 更新を実行していますか?	No	
システムは 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 (System i Navigator 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. System i Navigator 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. System i Navigator の受信側接続プロファイルの TCP/IP 設定特性の下の、「DHCP を IP アドレス割り当て方式に使用する (Use DHCP for the IP address assignment method)」を選択します。
- System i Navigator 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。
- System i Navigator 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。

関連資料

『例: DHCP と PPP プロファイルが異なる System i モデル上にある場合』

この例では、LAN およびリモート・ダイヤルイン・クライアント対応のネットワーク動的ホスト構成プロトコル (DHCP) サーバーおよび BOOTP/DHCP リレー・エージェントとして、2 つの System i モデル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 System i モデル上にある場合

この例では、LAN およびリモート・ダイヤルイン・クライアント対応のネットワーク動的ホスト構成プロトコル (DHCP) サーバーおよび BOOTP/DHCP リレー・エージェントとして、2 つの System i モデルをセットアップする方法について説明します。

PPP と DHCP が単一の System i モデル上にある場合には、PPP と DHCP を単一システム上で使用して、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、あるいはセキュリティーについては、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・クライアントは持っているが、PPP ポリシーと 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。

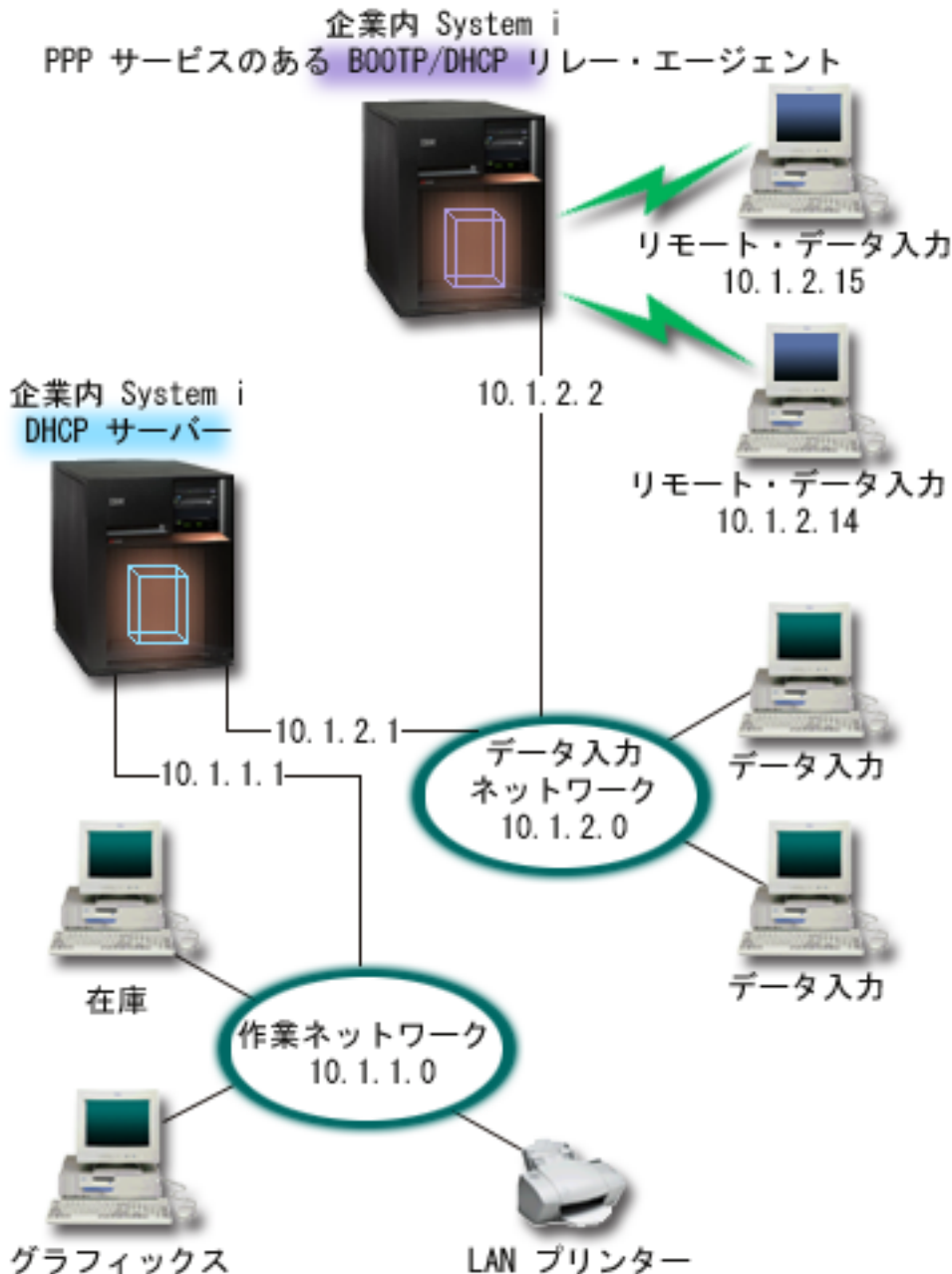


図9. DHCP と PPP プロファイルが異なる System i モデル上にある場合

リモート・データ入力クライアントは、System i PPP サーバーにダイヤルインします。そのサーバー上の PPP プロファイルは、「PPP と DHCP が単一 System i モデル上にある場合」の例で使用された PPP プロファイルのように、DHCP のリモート IP アドレス方式を持っている必要があります。PPP サーバー上の PPP プロファイルおよび TCP/IP スタック特性は IP 転送を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・エージェントがオンになっている必要があります。これで、System i リモート・アクセス・サーバーは、DHCPDISCOVER パケットを DHCP サーバーに渡すことができます。次に、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、DHCP サーバーは 10.1.2.10 から 10.1.2.40 までの範囲の 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には、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、System i 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含まれる 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
システムは DNS 更新を実行していますか?		No
システムは 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)

表 18. データ入力ネットワーク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 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 System i プラットフォーム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. System i Navigator 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. System i Navigator の受信側接続プロファイルの TCP/IP 設定特性の下の、「DHCP を IP アドレス割り当て方式に使用する (Use DHCP for the IP address assignment method)」を選択します。
- System i Navigator 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)。
- System i Navigator 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)。

関連資料

40 ページの『例: PPP と DHCP が単一 System i 上にある場合』

この例では、LAN およびリモート・ダイヤルイン・クライアント対応の動的ホスト構成プロトコル (DHCP) サーバーとして、System i モデルをセットアップする方法について説明します。

DHCP の計画

動的ホスト構成プロトコル (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について計画することに時間を費やしていなければ、時間のかかる、エラーの発生しやすいプロセスです。

DHCP サーバーをより効率良く構成するために、ネットワーク・セットアップおよびセキュリティー関連について、事前によく検討しておいてください。

関連資料

49 ページの『DHCP の構成』

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、ドメイン・ネーム・システム (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ます。

セキュリティに関する考慮事項

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。

ネットワークでの DHCP の対話の性質を考慮すれば、ご使用の System i モデルを外部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 System i モデル上にある場合、IP フィルター処理とネットワーク・アドレス変換を使用して、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可能になります。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 System i モデル上にある場合は、「System i およびインターネット・セキュリティ」トピックを参照してください。

関連概念

IP filtering and network address translation

セキュリティ

ネットワーク・トポロジーに関する考慮事項

動的ホスト構成プロトコル (DHCP) セットアップの計画は、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、などのいくつかの要因を検討する必要があります。

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にも理解できます。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 に接続する装置、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 (たとえば、プリンター) 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。あるサーバーに障害が起きた場合でも、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行うことができます。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、これらのアドレスについては DHCP サーバーが動的に割り当てるようにするのかどうか、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るかどうかについても検討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、BOOTP サーバー構成を DHCP サーバーへ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。さらに、ある場合にはクライアントが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同じルーターが指定されている場合、ルーターが変わったら、すべてのクライアントの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 構成要件が必要になるものがあります。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事前に分かっていると、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覧にそろえて見るには、11 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あります。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あります。DNS の利点と要件については、Information Center の DNS トピックをお読みください。

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 アドレスをそれらのリモート・クライアントへ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、40 ページの『例: PPP と DHCP が単一 System i 上にある場合』または 42 ページの『例: DHCP と PPP プロファイルが異なる System i モデル上にある場合』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

27 ページの『例: DHCP』

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『リレー・エージェントとルーター』

動的ホスト構成プロトコル (DHCP) リレー・エージェントとルーターを使用して、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。

8 ページの『DHCP クライアントのサポート』

DHCP を使用して、ラージ・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。

5 ページの『リース』

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、リース時間付きで送信されます。リース時間とは、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。リース時間はそれぞれの要求に応じて変更できます。

9 ページの『BOOTP』

ブートストラップ・プロトコル (BOOTP) は、動的ホスト構成プロトコル (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 は DHCP のサブセットです。

9 ページの『動的更新』

動的ホスト構成プロトコル (DHCP) がクライアントに IP アドレスを割り当てる際に、ドメイン・ネーム・システム (DNS) サーバーと一緒に DHCP サーバーを構成して 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。

Domain Name System

DHCP の構成

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、ドメイン・ネーム・システム (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ます。

関連資料

45 ページの『DHCP の計画』

動的ホスト構成プロトコル (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について計画することに時間を費やしていなければ、時間のかかる、エラーの発生しやすいプロセスです。

DHCP サーバーをより効率良く構成するために、ネットワーク・セットアップおよびセキュリティー関連について、事前によく検討しておいてください。

DHCP サーバーおよび BOOTP/DHCP リレー・エージェントの構成

DHCP サーバーおよび BOOTP/DHCP リレー・エージェントで、DHCP サーバーまたは BOOTP/DHCP リレー・エージェントの構成、開始、または停止などの作業を行う場合は、以下の情報を使用してください。

関連概念

7 ページの『リレー・エージェントとルーター』

動的ホスト構成プロトコル (DHCP) リレー・エージェントとルーターを使用して、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 構成の作成、または既存の DHCP 構成の表示を行うことができます。

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. System i Navigator で、「**対象のシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**DHCP**」の順に展開します。
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することができます。

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」ウィンドウへのショートカットの作成

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. System i Navigator で、「**対象のシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**DHCP**」の順に展開します。
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 サーバーの構成は、以下の手順に従って、DHCP サーバーを始動したり、停止したりできます。

1. System i Navigator で、「**対象のシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**DHCP**」の順に展開します。
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

DHCP サーバーが自動的に始動するように構成するには、以下の手順に従ってください。

1. System i Navigator で、「対象のシステム」 → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」 → 「DHCP」 の順に展開します。
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 が開始されるときに始動」チェック・ボックスを選択します。
5. 「OK」をクリックします。

DHCP サーバー・モニターのアクセス

動的ホスト構成プロトコル (DHCP) サーバー・モニターは、IBM System i DHCP サーバーのアクティブ・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・インターフェースを使用して、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、以下の手順に従ってください。

1. System i Navigator で、「対象のシステム」 → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」 → 「DHCP」 の順に展開します。
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

i5/OS 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。

DHCP/BOOTP リレー・エージェントをセットアップするには、以下の手順に従ってください。

1. System i Navigator で、「対象のシステム」 → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」 → 「BOOTP/DHCP リレー・エージェント」 の順に展開します。
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て、「OK」をクリックします。

BOOTP/DHCP リレー・エージェントの始動または停止

DHCP/BOOTP リレー・エージェントの構成後は、以下の手順に従って、この DHCP/BOOTP リレー・エージェントを始動したり、停止したりできます。

1. System i Navigator で、「対象のシステム」 → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」 → 「BOOTP/DHCP リレー・エージェント」 の順に展開します。
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

TCP/IP が開始されるときに、BOOTP/DHCP リレー・エージェントを自動的に始動するように構成するには、以下の手順に従ってください。

1. System i Navigator で、「対象のシステム」 → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」 → 「BOOTP/DHCP リレー・エージェント」 の順に展開します。

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 が開始されるときに始動**」チェック・ボックスを選択して、「**OK**」をクリックします。

ISC の DHCP 4 を使用するための DHCP サーバーの構成

DHCP バージョン 4 の実装として業界標準になっている Internet Systems Consortium (ISC), Inc. による実装では、現時点の IBM i の DHCP サーバー実装では使用できない機能が提供されます。具体的に言えば、ISC の DHCP 4 は、インターネット・プロトコル・バージョン 6 (IPv6) に対するサポートと、2 つの DHCP ピア・サーバー間のフェイルオーバーを提供します。IBM i システム管理者は、IBM i の DHCP 実装と ISC の DHCP 4 のどちらを実行するのを選択することができます。

ISC の DHCP 4 の使用

ISC の DHCP 4 を実装した DHCP サーバーを構成、開始、および停止するには、以下のようにします。

IBM i で ISC の DHCP 4 サーバーを使用するには、以下の手順を実行します。

1. 必ず、IBM i オプション 31 (ドメイン・ネーム・システム (DNS)) およびオプション 33 (ポータブル・アプリケーション・ソリューション環境 (PASE)) をシステムにインストールしておいてください。
2. 次のコマンドにより、ISC の DHCP 4 サーバーを使用するようにオペレーティング・システムに指示するための環境変数を定義します。

```
ADDENVVAR ENVVAR('QIBM_ISC_DHCP') VALUE('Y') LEVEL(*SYS)
```

注: QIBM_ISC_DHCP 環境変数を指定していない場合は、IBM i DHCP サーバーが使用されます。

3. DHCP 属性変更 (CHGDHCPA) コマンドを実行します。このコマンドで、既存の DHCP 構成が ISC DHCP サーバーで使用される構成ファイルにマイグレーションされます。IBM i DHCP サーバーが提供するすべての構成オプションが ISC DHCP サーバーでサポートされているわけではありません。しかし、可能な限り多くの構成がマイグレーションされます。マイグレーション後は、IBM i DHCP サーバー構成に加えた変更は ISC DHCP サーバー構成ファイルには反映されません。
4. 新しく作成された構成ファイルを手動で編集します。ISC DHCP サーバーを管理したり ISC DHCP サーバーが管理するリースをモニターしたりするためのグラフィカル・インターフェースは、提供されていません。関連付けられているすべての構成ファイルを手動で編集する必要があります。
5. IPv4 DHCP サーバーを実行するか、IPv6 DHCP サーバーを実行するか、またはその両方を同一のシステムで実行するかを決定します。
 - a. IPv4 と IPv6 の両方の DHCP サーバーを同一システム上で実行する場合は、次のコマンドを実行します。

```
CHGDHCPA IPVERSION(*ALL)
```
 - b. IPv6 DHCP サーバーのみを実行する場合は、次のコマンドを実行します。

```
CHGDHCPA IPVERSION(*IPV6)
```
 - c. IPv4 DHCP サーバーのみを実行する場合は、次のコマンドを実行します。

```
CHGDHCPA IPVERSION(*IPV4)
```
6. 次のコマンドを使用して、サーバーを開始します。

```
STRTCPSVR SERVER(*DHCP)
```
7. 次のコマンドを使用して、サーバーを終了します。

```
ENDTCPSVR SERVER(*DHCP)
```

関連情報

Internet Systems Consortium

ISC DHCP Web サイト

ISC DHCP サーバーの使用に関する考慮事項

既存の IBM i DHCP サーバーから ISC DHCP サーバーへマイグレーションする場合、検討が必要な構成上の考慮事項がいくつかあります。

ISC DHCP サーバーで使用されるファイルは、次の統合ファイル・システム (IFS) ディレクトリーに保管されます。

/QIBM/USERDATA/OS400/DHCP/ETC

既存の DHCP サーバーから ISC DHCP サーバーへ構成ファイルをマイグレーションする場合、以下のオプションはサポートされません。

1. グローバル定義の予約済みアドレスはマイグレーションされません。予約済みアドレスは、サブネット単位で定義する必要があります。
2. 「順序正しく」「バランスのよい」サブネットになるようにサブネット・グループ属性を指定してあっても、それらの属性はマイグレーションされません。また、マイグレーション後に、サブネットを手動で「共有ネットワーク」サブネット・グループにグループ化することが必要になる場合があります。「共有ネットワーク」サブネット・グループは、そのグループ内のサブネットが同一のネットワーク・セグメントに接続されるかどうかを DHCP サーバーに通知します。
3. ロギング・ディレクティブはマイグレーションされません。ただし、手動でロギングをオンにすることはできます。手動でサーバーを開始して `-D` オプション (*SERVER モードの場合) または `-K` オプション (*RELAY モードの場合) を渡すと、ロギングがオンになります。STRTCPSVR コマンドでオプションを指定するには次のようにします。
`STRTCPSVR SERVER(*DHCP) INSTANCE(*DFT '-D')`
4. dhcpsd.cfg ファイル内の次のキーワードとその関連データは、マイグレーションされません。
`appendDomainName`、`balanced`、`inOrder`、`leaseExpireInterval`、
`logFileName`、`logFileSize`、`logItem`、`numLogFiles`、`releaseDNSA`、`releaseDNSP`、
`reservedTime`、`statisticSnapshot`、および `usedIPAddressExpireInterval`。
5. ネイティブ IBM i DHCP サーバーは IPv6 をサポートしていないため、ISC DHCP サーバー用に空の構成ファイルが作成されます。
6. マイグレーションの一部として、ISC DHCP の開始時に、すべてのアクティブな DHCP リースのマイグレーションが試行されます。また、有効期限の切れたリースについても DNS レコードが更新される可能性があります。マイグレーションが試行されるのは、ISC サーバーが最初に使用される時のみです。
7. ISC DHCP コード配布では、DHCP クライアントが提供されています。ただし、これは IBM i では使用できません。代わりに、IBM i では、IPv4 および IPv6 の両方に対する独自の DHCP クライアント・サポートを提供しています。TCP/IP インターフェース追加 (ADDTCPIFC) コマンドによって、回線を DHCP クライアントとして構成することができます。

ネイティブ IBM i DHCP サーバーと ISC DHCP サーバーは、どちらも DHCP サーバーまたはリレー・エージェントとして実行することができます。どちらの DHCP 実装でも、CHGDHCPA コマンドのモード (MODE) パラメーターによって、DHCP サーバーとして実行するか、リレー・エージェントとして実行するかを指定します。アドレス・バインディング通知、アドレス解放通知、および要求パケット妥当性検査のための DHCP 出口プログラムは、ISC DHCP サーバーおよび IPv6 に対応しています。

関連情報

- Internet Systems Consortium
- ISC DHCP Web サイト
- DHCP サーバー出口プログラム

DHCP フェイルオーバー

- ISC DHCP 4 サーバーは、2 つの DHCP サーバー・ピア間のフェイルオーバーをサポートしています。
- ネイティブ IBM i DHCP サーバーを実行している DHCP へのフェイルオーバーはサポートされません。
- ほとんどの場合、ピアから別のピアへのフェイルオーバーは、自動的に実行されます。ただし、場合によってはサーバーの異常終了が発生し、手操作による介入が必要になることがあります。DHCP サーバー変更 (CHGDHCP SVR) コマンドを使用して、作動可能な方の DHCP フェイルオーバー・ピアにフェイルオーバー・パートナーがダウンしていることを通知できます。

関連情報

- Internet Systems Consortium
- ISC DHCP Web サイト

DHCP を使用するためのクライアントの構成

動的ホスト構成プロトコル (DHCP) サーバーの構成後に、クライアントの構成情報を DHCP サーバーから要求するためにも、さらにクライアントを構成する必要があります。

以下の情報は、Windows® クライアントの構成情報を DHCP サーバーから要求するために、このクライアントを構成するための手順の説明です。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 Me クライアント用に DHCP を使用可能に設定

Windows Me クライアント用の動的ホスト構成プロトコル (DHCP) 機能は、Windows Me オペレーティング・システムが提供するグラフィカル・インターフェースから使用可能または使用不可に設定できます。

DHCP を使用可能にするには、以下の手順に従ってください。

- 「スタート」で、「設定」→「コントロール パネル」の順にクリックします。
- 「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。
- 「TCP/IP プロトコル」を選択して、「プロパティ」をクリックします。
- 「IP アドレス」タブで、「DHCP サーバーから IP アドレスを取得する」をクリックして、「OK」をクリックします。

Windows Me クライアントの DHCP リースの検査:

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が備わっています。このユーティリティにより、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。

- 「MS-DOS コマンド プロンプト」を開きます。
- 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 2000 クライアント用に DHCP を使用可能に設定

Windows 2000 クライアント用の動的ホスト構成プロトコル (DHCP) 機能は、Windows 2000 オペレーティング・システムが提供するグラフィカル・インターフェースから使用可能または使用不可に設定できません。

DHCP を使用可能にするには、以下の手順に従ってください。

1. 「スタート」メニューで、「設定」→「ネットワークとダイヤルアップ接続」の順に選択します。
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」を選択します。
3. 「TCP/IP プロトコル」を選択して、「プロパティ」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」をクリックします。

MAC アドレスおよび DHCP リースの検査:

Windows 2000 クライアントおよび Windows XP 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を使用して、DHCP リースの解除や更新も行えます。

Windows 2000 または Windows XP クライアントの DHCP リースを検査するには、以下の手順に従ってください。

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。

クライアントのために DNS A レコードを更新するために DHCP サーバーが必要な場合は、Microsoft® Windows 2000 および Windows XP の DHCP クライアントを構成します。この構成により DNS 管理が単純化されます。DNS 更新について、それぞれのクライアントにレコードをそれぞれ個別に更新させるのではなく、すべてのクライアント用の DHCP サーバーで更新できるためです。

DNS A レコードの更新:

クライアントのために DHCP サーバーを使用して DNS A レコードを更新する場合は、以下の手順に従って Windows 2000 または Windows XP を使用可能にします。

1. 「スタート」メニューで、ご使用の Windows 環境に合わせて、以下のいずれかの手順を実行します。
 - Windows XP: 「コントロール パネル」→「ネットワーク接続」の順に選択します。
 - Windows 2000: 「設定」→「ネットワークとダイヤルアップ接続」の順に選択します。
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」を選択します。
3. 「TCP/IP プロトコル」を選択して、「プロパティ」を選択します。
4. 「詳細設定」をクリックします。「DNS」タブで、「この接続のアドレスを DNS に登録する」がチェック解除されていることを確認します。

5. 「TCP/IP 詳細設定」パネルで、「OK」をクリックします。
6. 「インターネット プロトコル TCP/IP のプロパティ」パネルで、「OK」をクリックします。
7. 「OK」をクリックします。

Windows XP クライアント用に DHCP を使用可能に設定

Windows XP クライアント用の動的ホスト構成プロトコル (DHCP) 機能は、Windows XP オペレーティング・システムが提供するグラフィカル・インターフェースから使用可能または使用不可に設定できます。

DHCP を使用可能にするには、以下の手順に従ってください。

1. 「スタート」メニューで、「コントロール パネル」 → 「ネットワーク接続」の順に選択します。
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」を選択します。
3. 「TCP/IP プロトコル」を選択して、「プロパティ」を選択します。
4. 「全般」タブで、「IP アドレスを自動的に取得する」を選択します。
5. 「OK」をクリックします。

MAC アドレスおよび DHCP リースの検査:

Windows 2000 クライアントおよび Windows XP 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が備わっています。このユーティリティを使用して、DHCP リースの解除や更新も行えます。

Windows 2000 または Windows XP クライアントの DHCP リースを検査するには、以下の手順に従ってください。

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、ユーティリティを再度実行する必要があります。同じユーティリティを異なるパラメータで使用して、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。

クライアントのために DNS A レコードを更新するために DHCP サーバーが必要な場合は、Microsoft Windows 2000 および Windows XP の DHCP クライアントを構成します。この構成により DNS 管理が単純化されます。DNS 更新について、それぞれのクライアントにレコードをそれぞれ個別に更新させるのではなく、すべてのクライアント用の DHCP サーバーで更新できるためです。

DNS A レコードの更新:

クライアントのために DHCP サーバーを使用して DNS A レコードを更新する場合は、以下の手順に従って Windows 2000 または Windows XP を使用可能にします。

1. 「スタート」メニューで、ご使用の Windows 環境に合わせて、以下のいずれかの手順を実行します。
 - Windows XP: 「コントロール パネル」 → 「ネットワーク接続」の順に選択します。
 - Windows 2000: 「設定」 → 「ネットワークとダイヤルアップ接続」の順に選択します。
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」を選択します。
3. 「TCP/IP プロトコル」を選択して、「プロパティ」を選択します。

4. 「詳細設定」をクリックします。「DNS」タブで、「この接続のアドレスを DNS に登録する」がチェック解除されていることを確認します。
5. 「TCP/IP 詳細設定」パネルで、「OK」をクリックします。
6. 「インターネット プロトコル TCP/IP のプロパティ」パネルで、「OK」をクリックします。
7. 「OK」をクリックします。

動的更新を DNS に送信するための DHCP の構成

動的ホスト構成プロトコル (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、このサーバーにドメイン・ネーム・システム (i5/OS のオプション 31) を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。動的更新を実行できる、別の System i モデル上で DNS サーバーを稼働できます。オプション 31 のインストールの検査については、「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」 の順に展開します。
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で、「グローバル」を右マウス・ボタンでクリックして、「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」ページをクローズします。

関連概念

9 ページの『動的更新』

動的ホスト構成プロトコル (DHCP) がクライアントに IP アドレスを割り当てる際に、ドメイン・ネーム・システム (DNS) サーバーと一緒に DHCP サーバーを構成して 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 動的更新を使用不可に設定

ドメイン・ネーム・システム (DNS) 動的更新を使用不可に設定することによって、DNS サーバーを管理する責任は管理者に戻されます。ホストがロケーションをほとんど変更しないネットワーク、ほとんど拡張しなくて変更されないネットワーク、および厳格な DNS サーバー管理が必要なネットワークには、DNS 動的更新を使用不可に設定することが適しているといえます。

クライアントから DNS 動的更新を使用不可に設定するには、以下の手順を実行します。

1. 「スタート」メニューで、「設定」→「ネットワークとダイヤルアップ接続」の順に選択します。
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」を選択します。
3. 「TCP/IP プロトコル」を選択して、「プロパティ」を選択します。
4. 「詳細設定」を選択します。
5. 「DNS」タブで、「この接続のアドレスを DNS に登録する」オプションと「この接続 DNS サフィックスを DNS 登録に使う」オプションを選択解除します。
6. 「OK」をクリックします。

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。

リースされた IP アドレスの管理

動的ホスト構成プロトコル (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する場合は、DHCP 構成ツールを使用します。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・モニターを使用できます。

DHCP サーバー・モニターは、System i DHCP サーバーのアクティブ・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・インターフェースを使用して、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、もはや使用されていない 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ます。リース情報を使用して、IP アドレスをその他のクライアントに使用可能にするために、どのリースを削除できるかどうかについて判別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、もはやそのアドレスを使用しようとしませんが、確実に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

61 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。動的ホスト構成プロトコル (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

DHCP 問題のご使用のトラブルシューティングを行う場合は、以下のガイドラインに従ってください。

ここに示されていない問題が発生した場合は、45 ページの『DHCP の計画』トピックを検討して、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。

関連資料

Using communications trace to solve communication problems

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. System i Navigator で、「**対象のシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**DHCP**」の順に展開します。
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、System i 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。この通信トレースは、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 ログ・ファイルは DHCP サーバーのロギング情報を記録する場合に使用されます。問題を起こした場所や理由を見つけるには、DHCP ログ・ファイルの表示が役立ちます。

DHCP サーバーをトレースする手順は、次のとおりです。

1. System i Navigator で、「**対象のシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」 → 「**DHCP**」の順に展開します。
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**」をクリックします。

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・ボタンでクリックして、「特性」 → 「ロギング」の順に選択します。
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」をクリックします。
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 に収められている DHCP ログ・ファイルを表示します。以下の手順のいずれかを実行します。
 - System i Navigator で、「対象のシステム」 → 「ファイル・システム」 → 「統合ファイル・システム」 → 「ルート」 → 「このファイルのディレクトリー」の順に展開します。
 - 文字ベース・インターフェースから「オブジェクト・リンクによる処理 (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、クライアントと動的ホスト構成プロトコル (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、2 ページの『DHCP クライアント/サーバー間の対話』トピック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、46 ページの『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 DHCPDISCOVER 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 DHCPDISCOVER 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/BOOTP 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、7 ページの『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 System i モデル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・システムのための DHCP 構成について詳しくは、32 ページの『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・メッセージをシステム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ています。

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・モニターの使用方法については、58 ページの『リースされた IP アドレス

スの管理』に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。

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。動的ホスト構成プロトコル (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。DHCP 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・モニターを使用します。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 を持つこととなります。

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提供できますが、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

58 ページの『リースされた IP アドレスの管理』

動的ホスト構成プロトコル (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する場合は、DHCP 構成ツールを使用します。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・モニターを使用できます。

問題: DNS レコードが DHCP によって更新されない

System i 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。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。この情報は動的更新のエラーをトラブルシューティングするときに役立ちます。

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。

i5/OS ドメイン・ネーム・システム、オプション 31 が DHCP を実行している System i モデルに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 ドメイン・ネーム・システム・フィーチャー、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 は DHCP サーバーと同じシステムに常駐し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。

TCP/IP ドメイン (CHGTCPDMN) コマンドを使用して、DHCP が常駐している System i モデル上の 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 System i モデルからネーム・サーバー探索 (NSLOOKUP) ツールを実行して、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。システムが 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

9 ページの『動的更新』

動的ホスト構成プロトコル (DHCP) がクライアントに IP アドレスを割り当てる際に、ドメイン・ネーム・システム (DNS) サーバーと一緒に DHCP サーバーを構成して 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、動的ホスト構成プロトコル (DHCP) サーバーがドメイン・ネーム・システム (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 System i 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 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ため、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 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見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機能しない場合は、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。しかし、一部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で提供される動的更新ユーティリティを使用すると、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

IBM Redbooks および Web サイトには DHCP トピックのコレクションに関連する情報が収められています。PDF ファイルはいずれも表示および印刷できます。


IBM Redbooks








AS/400® TCP/IP Autoconfiguration: DNS and DHCP Support  (5181 KB)

この IBM Redbooks 資料は、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 Redbooks 資料に記載されている情報は、例を使って説明していますので、DNS および DHCP サポートのインストール

ール、調整、構成、およびトラブルシューティングに役立ちます。

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 の廃止) 
- 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) 
- RFC 3315: IPv6 の動的ホスト構成プロトコル (DHCPv6) 

関連資料

1 ページの『DHCP の PDF ファイル』
この情報の PDF ファイルを表示または印刷できます。

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。

〒242-8502
神奈川県大和市下鶴間1623番14号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

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を提供し、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。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認できません。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をお願いします。

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ます、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

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。本書のサンプル・プログラムは特定物として現存するままの状態を提供されるものであり、いかなる保証も提供されません。IBM は、当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

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_.

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 i 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

IBM、IBM ロゴ、および ibm.com は、世界の多くの国で登録された International Business Machines Corp. の商標または登録商標です。他の製品名およびサービス名は、IBM または各社の商標です。現時点での IBM の商標リストについては、www.ibm.com/legal/copytrade.shtml の「Copyright and trademark information」をご覧ください。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

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等はそれぞれ各社の商標です。

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を提供され、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なしで提供されます。



Printed in Japan