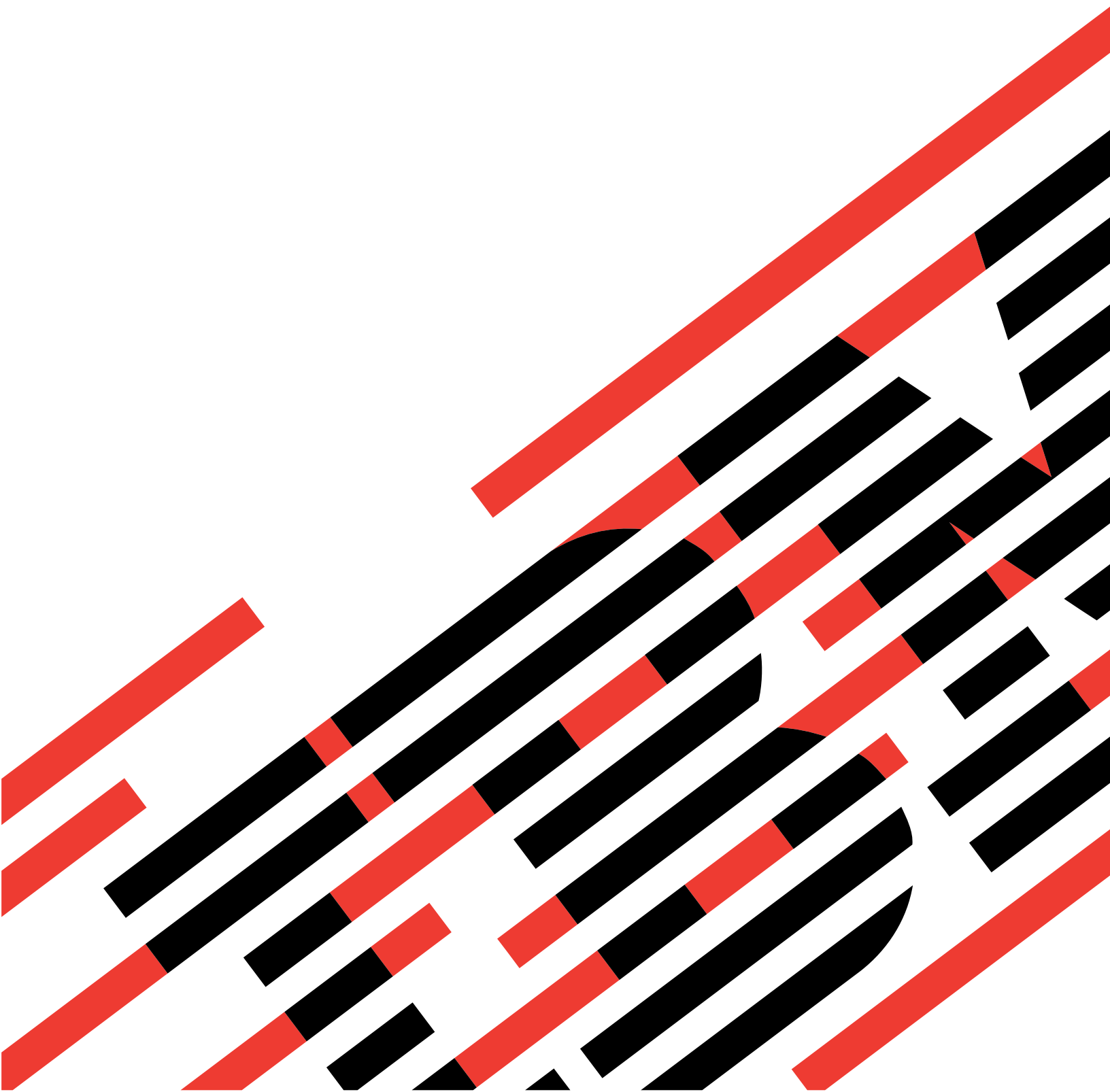


IBM

@server

iSeries

ネットワーキング
TCP/IP セットアップ





@server

iSeries

ネットワーキング
TCP/IP セットアップ

目次

第 1 部 TCP/IP セットアップ	1
第 1 章 V5R2 の新機能	3
第 2 章 トピックの印刷	5
第 3 章 Internet Protocol version 6 (IPv6)	7
IPv6 とは?	7
使用可能な IPv6 機能	8
シナリオ: IPv6	9
IPv6 ローカル・エリア・ネットワーク (LAN) の作成	10
IPv4 ローカル・エリア・ネットワーク (LAN) を介した IPv6 パケットの送信	12
IPv4 広域ネットワーク (WAN) を介した IPv6 パケットの送信	15
概念: IPv6	15
IPv6 アドレス・フォーマット	16
IPv6 アドレス・タイプ	17
IPv6 のトンネリング	18
近隣ディスカバリー	18
ステートレス・アドレスの自動構成	19
IPv4 と IPv6 との比較	21
IPv6 に関する関連情報	30
第 4 章 TCP/IP セットアップの計画	31
TCP/IP セットアップの要件	31
TCP/IP セキュリティーの考慮事項	32
第 5 章 TCP/IP のインストール	33
第 6 章 TCP/IP の構成	35
はじめての TCP/IP の構成	35
EZ セットアップ・ウィザードを使用した TCP/IP の構成	35
文字ベースのインターフェースを使用した TCP/IP の構成	36
回線記述の構成 (イーサネット)	36
インターフェースの構成	37
経路の構成	37
ローカル・ドメインおよびホスト名の定義	37
ホスト・テーブルの定義	37
TCP/IP の開始	38
IPv6 の構成	38
セットアップ要件	38
IPv6 構成ウィザードを使用した IPv6 の構成	39
第 7 章 iSeries ナビゲーターを使用した TCP/IP のカスタマイズ	41
第 8 章 IPv6 のトラブルシューティング	45
第 9 章 TCP/IP のセットアップに関する関連情報	47

第 1 部 TCP/IP セットアップ

iSeries™ が納入されたら、直ちに使用可能な状態にしたいことでしょう。このセクションでは、iSeries サーバー上で接続をセットアップし、TCP/IP を構成するための、ツールと手順を説明します。この初期作業を完了した後、独自のニーズに合うように、アプリケーションによって TCP/IP を拡張する用意ができたことになります。

V5R2 の新機能

新規および変更された TCP/IP 機能について知ることができます。

トピックの印刷

Portable Document Format (PDF) 版の「TCP/IP セットアップ」を印刷またはダウンロードする場合は、このトピックを参照してください。

Internet Protocol version 6 (IPv6)

新しい Internet Protocol, IPv6 は、インターネットの将来においてかぎとなる役割を果たします。iSeries サーバーでは、その IPv6 を使用することができます。このトピックには、IPv6 についての一般情報と、それを iSeries サーバーにインプリメントする方法に関する説明があります。

TCP/IP セットアップの計画

このトピックは、iSeries サーバー上での TCP/IP のインストールと構成の準備に役立てることができます。インストールと構成の基本的な要件が提示されるので、TCP/IP の構成を始めるときには、必要な情報すべてを手に入れているはずで、関連する用語や概念の参照情報も提供されます。

TCP/IP のインストール

このトピックでは、プロダクトのインストールを手順ごとに説明し、iSeries サーバーの操作に備えます。

TCP/IP の構成

このトピックでは、iSeries の稼働と TCP/IP の構成の方法を示しています。さらに、IPv6 の構成方法についても確認できます。

iSeries ナビゲーターによる TCP/IP のカスタマイズ

このトピックでは、iSeries ナビゲーターを使用したカスタマイズ・オプションを説明しています。

TCP/IP トラブルシューティング

TCP/IP 接続またはトラフィックに関して何らかの問題に直面した場合は、『TCP/IP トラブルシューティング』を参照してソリューションを見つけてください。このトラブルシューティング・ガイドは、IPv4 と IPv6 のどちらに関係した問題の解決にも役立ちます。

TCP/IP のセットアップについての関連情報

このトピックは、「さらに何ができるのか」という質問に答えています。サーバーのパフォーマンスを向上させるサービスやアプリケーションへの参照情報を見出せます。

第 1 章 V5R2 の新機能

バージョン 5 リリース 2 の「TCP/IP セットアップ」のトピックに新しく加わった項目は以下のとおりです。

- **文字ベースのインターフェースを使用した TCP/IP の構成**

文字ベースのインターフェースを使用してサーバーを構成する必要があるカスタマーのための TCP/IP のセットアップ方法を示しています。TCP/IP の推奨のセットアップ方法は、EZ セットアップ・ウィザードを使用する方法です。ただし、PC から iSeries ナビゲーターを使用する場合は、iSeries ナビゲーターを実行する前に基本 TCP/IP 構成が必要なので、この場合は文字ベースのインターフェースを使用して基本構成を実行しなければなりません。

- **Internet Protocol version 6 (IPv6)**


IPv6 に関する基本的な情報と、これが iSeries サーバーにどのようにインプリメントされるかについての説明があります。

- **IPv6 の構成**

IPv6 用サーバーの構成のためのセットアップ要件とその手順について説明します。

- **iSeries Navigator による TCP/IP のカスタマイズ**

このトピックには記述が追加されています。TCP/IP 構成の新しいカスタマイズ方法についての説明が含まれています。IPv6 の構成、または新しいインターフェースと経路の作成には、iSeries ナビゲーターの新しいウィザードを使用します。

このリリースの新機能または変更点に関する他の情報については、プログラム資料説明書  を参照してください。


第 2 章 トピックの印刷

PDF 版をダウンロードして表示するには、TCP/IP セットアップ (約 881 KB、56 ページ) を選択します。

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

1. ブラウザーで PDF を開く (上記のリンクをクリックする)。
2. ブラウザーのメニューから「ファイル」をクリックする。
3. 「名前を付けて保存」をクリックする。(IE の場合は、フロッピーディスクのアイコン (名前を付けて保存) をクリックする。)
4. PDF を保存したいディレクトリーに進む。
5. 「保存」をクリックする。

Adobe Acrobat Reader のダウンロード

これらの PDF ファイルを表示または印刷するために Adobe Acrobat Reader が必要な場合は、Adobe の Web サイト (www.adobe.com/prodindex/acrobat/readstep.html)  からダウンロードできます。

第 3 章 Internet Protocol version 6 (IPv6)

Internet Protocol version 6 (IPv6) は、Internet Protocol version 4 (IPv4) の更新版であり、インターネット標準として徐々に IPv4 に置き換わりつつあります。

読者は、会社の e-business を向上させるために IPv6 の使用を検討している方かもしれませんし、または IPv6 アプリケーションを作成して、この拡張された Internet Protocol によって会社に利をもたらそうと考えているプログラマーかもしれません。IPv6 に関する基本的な情報、および iSeries サーバー上で IPv6 を使用する方法については、以降のトピックをお読みください。

IPv6 とは？

なぜ IPv6 がインターネット標準として IPv4 から置き換わりつつあるのか、また、これをどのように使用すれば利点があるかについて説明します。

使用可能な IPv6 の機能

IPv6 が iSeries サーバーに現在どのようにインプリメントされるかを説明します。

IPv6 シナリオ

ビジネスで IPv6 が使用される状況を理解するための例を示します。

IPv6 の概念

基本的な IPv6 の概念について説明します。IPv4 と IPv6 の違いがよく分からない場合は、このトピックで、IPv4 アドレスと IPv6 アドレスの違いや、IPv4 パケット・ヘッダーと IPv6 パケット・ヘッダーの違いなどに関する詳細な比較を参照してください。

IPv6 の構成

サーバーに IPv6 を構成するためのハードウェアおよびソフトウェア要件と、その方法について説明します。

IPv6 のトラブルシューティング

IPv6 問題に対するソリューションを示します。

IPv6 についての関連情報

IPv6 の理解を助ける情報源へのリンクがあります。

IPv6 とは？

Internet Protocol version 6 (IPv6) は、インターネット・プロトコルにおける次なる進化です。ほとんどのインターネットは現在 IPv4 を使用しており、このプロトコルはここ 20 年の間、信頼性と弾力性のあるプロトコルでした。しかし、IPv4 には厳しい制限があり、この制限がインターネットが拡大するにつれてより多くの問題を引き起こすようになっていきます。

特に、インターネットに加えられるすべての新しい装置に必要とされる IPv4 アドレスは、ますます不足してきています。IPv6 拡張のかぎは、IP アドレス・スペースを 32 ビットから 128 ビットに拡張し、事実上無限の固有 IP アドレスを使用可能にすることです。新しい IPv6 アドレスのテキスト・フォーマットは以下のとおりです。

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
```

ここで x は 4 ビットを表す 16 進数字です。

拡張された IPv6 のアドレッシング機能は、アドレスごとの問題の解決策を提供します。これは、より多くの人々が携帯電話や携帯用コンピューターなどのモバイル・コンピューターを使用するようになっているので特に重要です。ワイヤレス・ユーザーの需要の増大は、IPv4 アドレスのごとくに拍車をかけます。拡張された IPv6 の IP アドレス機能は、増大するワイヤレス装置の数に見合う IP アドレスを供給することによってこの問題を解決します。

このアドレッシング機能に加えて、IPv6 はネットワーク上のアドレスの構成および管理タスクを単純化する新しい機能を提供しています。ネットワークの構成と保守は、非常に労力を要する作業です。IPv6 は、いくつかのネットワーク管理者のタスクを自動化することによって、作業負荷を軽減しています。

IPv6 を使用していれば、別のインターネット・サービス・プロバイダー (ISP) に変える際に、装置アドレスの番号を付け替える必要はありません。アドレスは全世界的に固有なので、同じアドレスを持ち続けることができます。

IPv6 の自動構成機能は、ユーザーに代わって自動的にインターフェースとルーターのアドレスを構成します。ステートレス自動構成では、IPv6 はマシンの MAC アドレスと、ローカル・ノードによって提供されるネットワーク接頭部を取り、それら 2 つのアドレスを結合して新しい固有な IPv6 アドレスを作成します。この機能によって DHCP サーバーは不要となり、結果として管理者の時間と会社の経費が節減されます。

IPv6 に関するより詳しい説明については、『IPv6 についての関連情報』を参照してください。

特に iSeries サーバーに関連した IPv6 情報については、『使用可能な IPv6 機能』を参照してください。

使用可能な IPv6 機能

IBM® では、いくつかのソフトウェア・リリースにおいて、iSeries サーバー用に IPv6 を実装する予定です。現在 IPv6 は、IPv6 アプリケーションの開発と検査の目的で、アプリケーション開発プラットフォームにインプリメントされています。IPv6 機能は、既存の TCP/IP アプリケーションに対して透過的で、IPv4 機能と共存します。

以下は、IPv6 の影響を受ける主な iSeries サーバー機能です。

• 構成

IPv6 の構成プロセスは IPv4 のプロセスとは異なるという点にご注意ください。IPv6 機能を使用する場合は、IPv6 用の回線を構成することによってサーバーの TCP/IP 構成を変更する必要があります。IPv6 はイーサネット回線上またはトンネル回線上に構成できます。

IPv6 トラフィック用のイーサネット回線を構成する場合は、IPv6 ネットワークを介して IPv6 パケットを送信することになります。『IPv6 ローカル・エリア・ネットワーク (LAN) の作成』の、IPv6 用のイーサネット回線を構成する状況について説明するシナリオを参照してください。

トンネル回線を構成する場合は、既存の IPv4 ネットワークを介して IPv6 パケットを送信することになります。『IPv4 ローカル・エリア・ネットワーク (LAN) を介した IPv6 パケットの送信』と『IPv4 広域ネットワーク (WAN) を介した IPv6 パケットの送信』にある、構成した IPv6 用トンネル回線を構成する 2 つの状況について説明するシナリオを参照してください。

IPv6 対応のネットワークの構成方法については、『IPv6 の構成』を参照してください。

• ソケット

ソケット・アプリケーションは、IPv6 の API とツールを使用して開発および検査してください。IPv6 はソケットを拡張し、アプリケーションが新しいアドレス・ファミリー AF_INET6 を使用して IPv6 を使用できるようにしています。この拡張は、既存の IPv4 アプリケーションには影響しません。IPv4 お

よび IPv6 並行のトラフィックか、IPv6 のみのトラフィックをサポートするアプリケーションを作成することができます。IPv6 のソケットの詳細については、『AF_INET6 アドレス・ファミリーの使用』を参照してください。

• DNS

ドメイン・ネーム・システム (DNS) は、AAAA アドレスと逆探索用の新しいドメイン IP6.ARPA をサポートしています。確かに DNS は IPv6 情報を検索しますが、サーバーは IPv4 を使用して DNS と通信しなければなりません。

• TCP/IP のトラブルシューティング

PING、netstat、トレース経路、および IPv6 ネットワークとトンネル用の通信トレースなどの標準のトラブルシューティング・ツールを使用してください。これらのツールは、現在 IPv6 アドレス・フォーマットをサポートしています。IPv4 と IPv6 のどちらのネットワークの問題を解決する場合にも、『TCP/IP トラブルシューティング』を参照してください。

IPv6 に関する情報については、『IPv6 についての関連情報』を参照してください。

シナリオ: IPv6

以下のシナリオを検討して、IPv6 をインプリメントする理由と、以下の各状況におけるネットワークのセットアップ方法について理解してください。

- IPv6 ローカル・エリア・ネットワーク (LAN) の作成
- IPv4 ローカル・エリア・ネットワーク (LAN) を介した IPv6 パケットの送信
- IPv4 広域ネットワーク (WAN) を介した IPv6 パケットの送信

注: このシナリオでは、IP アドレス 10.x.x.x は公開 IP アドレスを表します。これらのシナリオで使用されているアドレスはすべて、例示のみを目的としています。

IPv6 対応のサーバーの構成方法については、『IPv6 の構成』を参照してください。

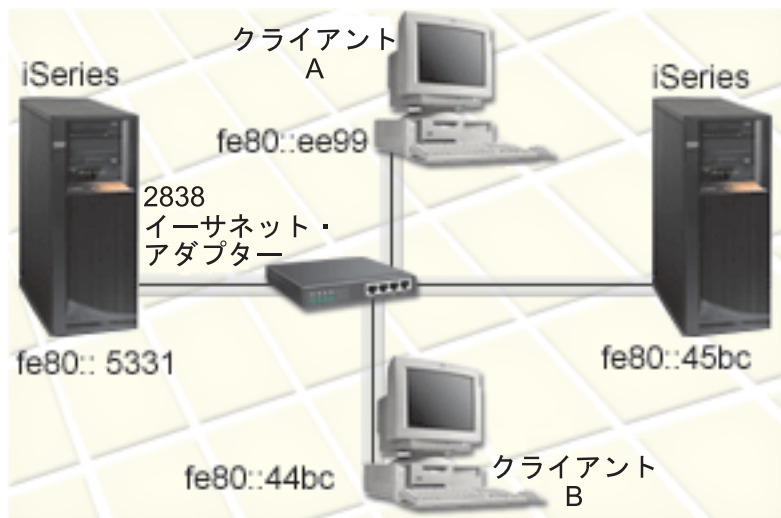
基本的な IPv6 の概念の定義については、『IPv6 の概念』を参照してください。

IPv6 ローカル・エリア・ネットワーク (LAN) の作成

状況

IPv6 は、インターネット標準として最終的には IPv4 と置き換わります。その結果、会社はその会計操作用に IPv6 をインプリメントし、接続に IPv6 を使用する新しい会計アプリケーションを購入することを決定します。アプリケーションは、サイトのイーサネット・ローカル・エリア・ネットワーク (LAN) に接続する異なるサーバー上にある、そのアプリケーションの他のインスタンスに接続する必要があります。ユーザーの仕事は、IPv6 用にサーバーを構成することによって、会社が会計アプリケーションの使用を開始できるようにすることです。以下の図は、このシナリオにおけるネットワーク・セットアップを示しています。

会計部門 IPv6 ネットワーク



ソリューション

IPv6 LAN を作成する場合は、IPv6 用のイーサネット回線記述を構成する必要があります。IPv6 パケットは、従業員が会計アプリケーションを使用するときにネットワーク上の iSeries サーバーとクライアントの間を移動します。

セットアップ要件は、以下のとおりです。

- OS/400[®] バージョン 5 リリース 2 以上
- 2838 または 2849 イーサネット・アダプター (IPv6 用に現行でサポートされているハードウェア・リリースはこのタイプだけです)
- iSeries Access for Windows[®] と iSeries ナビゲーター (iSeries ナビゲーターのネットワーク・コンポーネント)
- IPv6 用のイーサネット回線を構成する際は、サーバー上で TCP/IP が実行していなければならないので、事前にサーバーに別の IPv4 の物理インターフェースが構成されていなければなりません。サーバーを IPv4 対応に構成していない場合は、『はじめての TCP/IP の構成』を参照してください。

構成

IPv6 用のイーサネット回線記述を構成する場合は、iSeries ナビゲーターの「**IPv6 の構成 (IPv6 Configuration)**」ウィザードを使用する必要があります。IPv6 は iSeries ナビゲーターからのみ構成でき、文字ベースのインターフェースからは構成できません。

このウィザードでは、IPv6 を構成するサーバーのハードウェア通信リソースの名前 (たとえば、CMN01) が必要です。これは現行で IPv4 用に構成されていない、2838 または 2849 のいずれかのイーサネット・アダプターでなければなりません。

「**IPv6 の構成 (IPv6 Configuration)**」ウィザードを使用するには、以下のステップに従ってください。

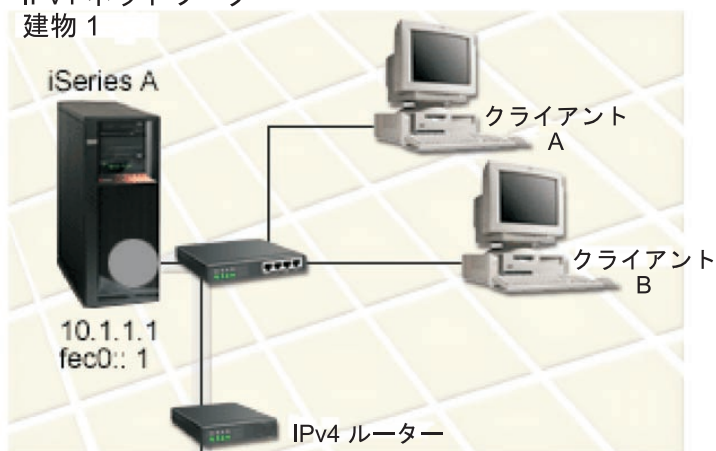
1. iSeries ナビゲーターで、ご使用の「サーバー」 → 「ネットワーク (Network)」 → 「TCP/IP の構成 (TCP/IP Configuration)」を選択します。
2. 「IPv6」を右マウス・ボタン・クリックし、「IPv6 の構成 (IPv6 Configuration)」をクリックして、ウィザードの指示に従ってイーサネット回線を IPv6 用に構成します。

IPv4 ローカル・エリア・ネットワーク (LAN) を介した IPv6 パケットの送信

状況

会社では新しい IPv6 会計アプリケーションを作成しました。これは、サーバー対クライアントのアプリケーションで、ローカルに使用します。このアプリケーションは、同じサイトにあるものの、他の建物および LAN の中にあるそのアプリケーション自体の他のインスタンスと通信します。会社はこのアプリケーションに IPv6 を使用したいと思っていますが、その IPv4 のインフラストラクチャー全体を IPv6 に変更する準備はできていません。ユーザーの仕事は、IPv6 パケットがローカル IPv4 ネットワーク上を通れるようにするための、IPv6 トンネル回線を構成することです。以下の図は、このシナリオにおけるネットワークのセットアップを示しています。

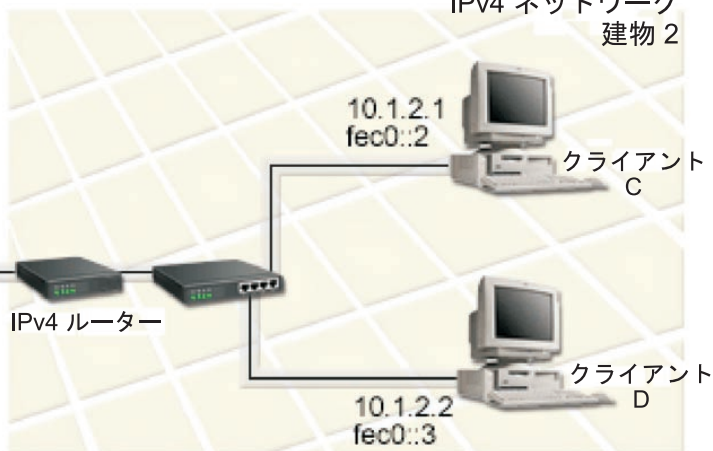
売掛管理
IPv4 ネットワーク
建物 1



赤の構成済みトンネル
ローカル・エンドポイント = 10.1.1.1
リモート・エンドポイント = 10.1.2.1
ローカル IPv6 アドレス = fec0::1

青の構成済みトンネル
ローカル・エンドポイント = 10.1.1.1
リモート・エンドポイント = 10.1.2.2
ローカル IPv6 アドレス = fec0::1

買掛管理
IPv4 ネットワーク
建物 2



ソリューション

これらの IPv4 ネットワーク上で IPv6 を使用するには、2 つの構成済みトンネルといくつかの関連経路を作成しなければなりません。例示のため、1 つのトンネルは赤で描かれ、もう 1 つのトンネルは青で描かれています。

まず、赤のトンネルについて考慮しましょう。

- 赤のトンネルは建物 1 の中にある iSeries A (ローカル・エンドポイント 10.1.1.1) から始まり、建物 2 の中にあるクライアント C (リモート・エンドポイント 10.1.2.1) で終わっています。

- iSeries A は IPv4 パケット内に IPv6 パケットをカプセル化し、その IPv4 パケットをトンネルを介してクライアント C に送信します。クライアント C はこの IPv6 パケットのカプセル化を解くことによって、IPv6 アプリケーションのもう 1 つのインスタンスに接続できます。

次に、青のトンネルのついでに考慮しましょう。

- 青のトンネルは赤のトンネルと同様に建物 1 の中にある iSeries A (ローカル・エンドポイント 10.1.1.1) から始まっていますが、この青のトンネルは建物 2 の中にあるクライアント D (リモート・エンドポイント 10.1.2.2) で終わっています。

- iSeries A は IPv4 パケット内に IPv6 パケットをカプセル化し、その IPv4 パケットをトンネルを介してクライアント D に送信します。クライアント D はこの IPv6 パケットのカプセル化を解くことによって、IPv6 アプリケーションのもう 1 つのインスタンスに接続できます。

各トンネルの接続は Point-to-Point なので、トンネルごとにリモート・エンドポイントを定義する必要があります。これは、2 つの経路を作成することによって実現します。各経路は同一のトンネル回線に関連付けられますが、別々のリモート・エンドポイントをネクスト・ホップとして定義します。つまり、ユーザーは 1 経路を作成するとき、各トンネルのリモート・エンドポイントを定義することになります。

トンネルのエンドポイントを定義して、建物 2 の中のクライアントにパケットが到達できるようにする初期経路の作成に加え、ユーザーはさらに 2 つの経路を作成して、パケットが建物 1 の中にあるサーバーに戻ってこられるようにする必要があります。

セットアップ要件は以下のとおりです。

- OS/400 バージョン 5 リリース 2 以上
- iSeries Access for Windows と iSeries ナビゲーター (iSeries ナビゲーターのネットワーク・コンポーネント)
- 構成したトンネル回線を作成する前に、TCP/IP (IPv4 を使用する) がサーバー上に構成されていなければなりません。サーバーを IPv4 対応に構成していない場合は、IPv6 用のトンネル回線を構成する前に『はじめての TCP/IP の構成』を参照してください。

構成

構成したトンネル回線を作成するには、iSeries ナビゲーターの「IPv6 の構成 (IPv6 Configuration)」ウィザードおよび「新しい IPv6 経路 (New IPv6 Route)」ウィザードを使用する必要があります。IPv6 は iSeries ナビゲーターからのみ構成でき、文字ベースのインターフェースからは構成できません。

「IPv6 の構成 (IPv6 Configuration)」ウィザードを使用して赤のトンネル回線を作成するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、ご使用の「サーバー」→「ネットワーク (Network)」→「TCP/IP の構成 (TCP/IP Configuration)」を選択します。
2. 「IPv6」を右マウス・ボタン・クリックし、「IPv6 の構成 (IPv6 Configuration)」をクリックして、ウィザードの指示に従ってトンネル回線を IPv6 用に構成します。「IPv6 の構成 (IPv6 Configuration)」ウィザードが完了すると、構成されたトンネル回線の新しい経路の作成を促すプロンプトが出され、「新しい IPv6 経路 (New IPv6 Route)」ウィザード・ダイアログが表示されます。新しい経路を作成して、IPv6 パケットが赤のトンネルを通ることができるようにする必要があります。
3. 「新しい IPv6 経路 (New IPv6 Route)」ウィザードで、赤のトンネル用の経路を作成します。リモート・エンドポイント 10.1.2.1 をネクスト・ホップとして指定し、fec0::2 を宛先アドレスとして指定します。

再び「新しい IPv6 経路 (New IPv6 Route)」ウィザードを使用して、青のトンネル用の経路を作成します。青のトンネルは「IPv6 の構成 (IPv6 Configuration)」ウィザードを使用して作成する必要はありません。青のトンネルは、「新しい IPv6 経路 (New IPv6 Route)」ウィザードを使用してそのリモート・エンドポイントを定義すると作成されます。「新しい IPv6 経路 (New IPv6 Route)」ウィザードを使用するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、ご使用の「サーバー」→「ネットワーク (Network)」→「TCP/IP の構成 (TCP/IP Configuration)」→「IPv6」を選択します。
2. 「経路 (Routes)」を右マウス・ボタン・クリックし、「新しい経路 (New Route)」をクリックして、ウィザードの指示に従って青のトンネル用に IPv6 経路を構成します。リモート・エンドポイント 10.1.2.2 をネクスト・ホップとして指定し、fec0::3 を宛先アドレスとして指定します。

構成したトンネル回線とトンネルのエンドポイントを定義する経路を作成したら、パケットが建物 1 の中のサーバーに戻るために通るクライアント C 上の経路とクライアント D 上の経路を作成する必要があります。これらの各経路に対しては、10.1.1.1 をネクスト・ホップとして指定し、fec0::1 を宛先アドレスとして指定する必要があります。

IPv4 広域ネットワーク (WAN) を介した IPv6 パケットの送信

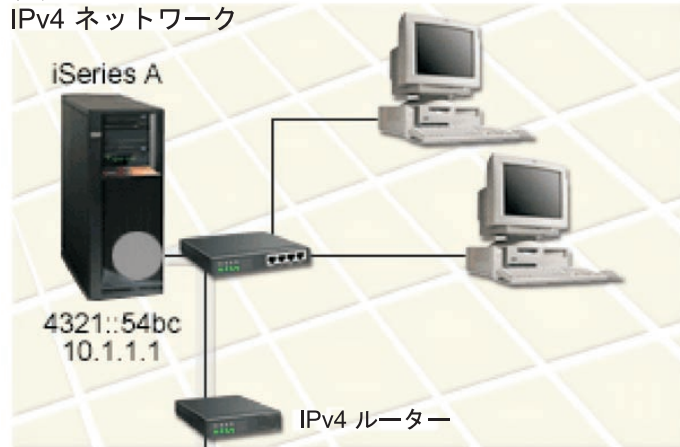
状態

会社のシカゴのオフィスにあるサーバー上で、売掛管理に関する会計アプリケーションを使用しているとして、このアプリケーションを、ダラスのオフィスのサーバーに接続する必要があるとします。どちらの都市のサーバー上でも、このアプリケーションは IPv6 アドレッシングを使用しています。この ISP では 2 つのサイト間に IPv6 ルーターを提供しないので、2 つのサーバー間にトンネルを構成する必要があります。アプリケーション・パケットは、2 つのサーバー間を IPv4 広域ネットワークを介し、トンネルを通じて送信されます。以下の図では、このシナリオにおけるネットワークのセットアップを示しています。

注: このシナリオでは、IP アドレス 10.x.x.x は、グローバルに経路指定できる公開 IP アドレスを表します。ここで使用されているアドレスはすべて、例示のみを目的としています。

売掛管理
シカゴ

IPv4 ネットワーク

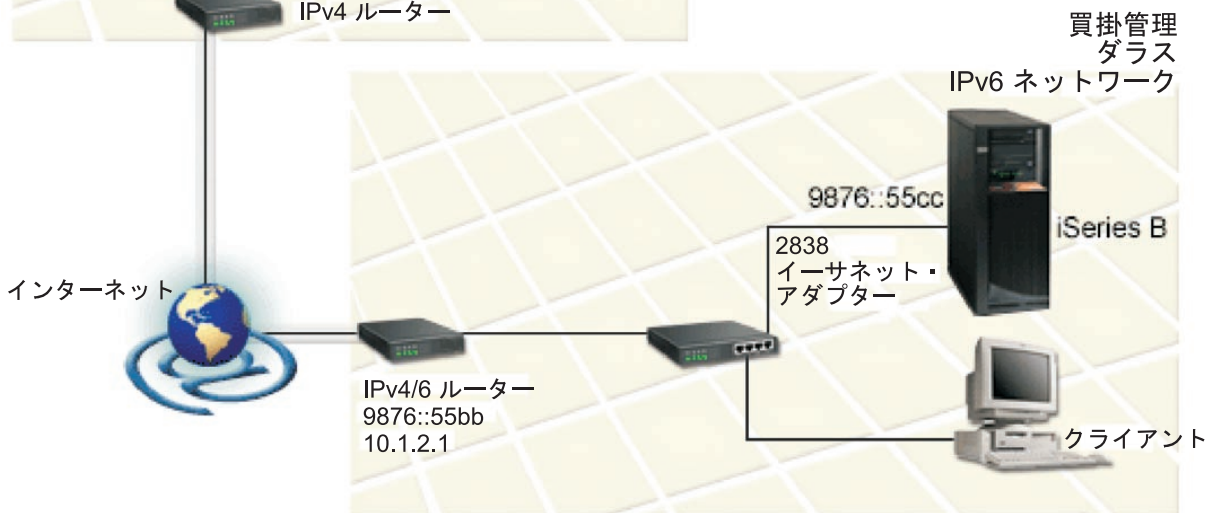


緑の構成済みトンネル

ローカル・エンドポイント = 10.1.1.1

リモート・エンドポイント = 10.1.2.1

ローカル IPv6 アドレス = 4321::54bc



買掛管理

ダラス

IPv6 ネットワーク

インターネット

ソリューション

IPv4 インフラストラクチャーで構成される広域ネットワークを介する IPv6 を使用するには、構成済みのトンネル回線と、いくつかの関連付けられた経路を作成しなければなりません。これは以下のような動作をします。

- トンネルは、シカゴの iSeries A (ローカル・エンドポイント 10.1.1.1) で始まり、ダラスの IPv4/6 ルーター (リモート・エンドポイント 10.1.2.1) で終わる。
- iSeries A 上のアプリケーションから、iSeries B 上のアプリケーションに接続する必要があります。iSeries A は、IPv4 パケット中の IPv6 パケットをカプセル化し、トンネルを介して IPv4/6 ルーターに送信します。このルーターは、IPv6 パケットをカプセル化解除し、IPv6 パケットを iSeries B に転送します。
- 逆のパスを経てパケットがシカゴに戻る。

トンネルは Point-to-Point なので、トンネルのリモート・エンドポイントを定義する必要があります。そのためには、このトンネル回線に関連付けられた経路を作成します。経路に、リモート・エンドポイントを

|(10.1.2.1) ネクスト・ホップとして定義します。つまり、経路を作成する際にリモート・エンドポイントを定義します。さらに、経路に宛先アドレスを 9876::55cc (iSeries B に関連付けられている IPv6 アドレス)と定義します。

| トンネル・エンドポイントを定義する初期経路を作成して、パケットをダラスの iSeries B に送信できるようにするだけでなく、さらに 2 つの経路を作成して、パケットがシカゴの iSeries A に戻れるようにする必要があります。

| セットアップ要件は以下のとおりです。

| • OS/400 バージョン 5 リリース 2 以上

| • iSeries Access for Windows と iSeries ナビゲーター (iSeries ナビゲーターのネットワーク・コンポーネント)

| • 構成済みのトンネル回線を作成する前に、サーバー上で TCP/IP (IPv4 を使用) を構成しなければならない。サーバーを IPv4 対応に構成していない場合は、IPv6 用のトンネル回線を構成する前に『はじめての TCP/IP の構成』を参照してください。

構成

| 構成したトンネル回線を作成するには、iSeries ナビゲーターの「IPv6 の構成 (IPv6 Configuration)」ウィザードおよび「新しい IPv6 経路 (New IPv6 Route)」ウィザードを使用する必要があります。構成済みのトンネルは iSeries ナビゲーターからのみ構成でき、文字ベースのインターフェースからは構成できません。

| 「IPv6 の構成 (IPv6 Configuration)」ウィザードを使用してトンネル回線を作成するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、ご使用の「サーバー」→「ネットワーク (Network)」→「TCP/IP の構成 (TCP/IP Configuration)」を選択します。
2. 「IPv6」を右マウス・ボタン・クリックし、「IPv6 の構成 (IPv6 Configuration)」を選択して、ウィザードの指示に従って IPv6 用にトンネル回線を構成します。「IPv6 の構成 (IPv6 Configuration)」ウィザードが完了すると、構成されたトンネル回線の新しい経路の作成を促すプロンプトが出され、「新しい IPv6 経路 (New IPv6 Route)」ウィザード・ダイアログが表示されます。新しい経路を作成して、IPv6 パケットがトンネルを通ることができるようにする必要があります。
3. 「新規 IPv6 経路 (New IPv6 Route)」ウィザードで、トンネルのホスト経路を作成します。エンドポイント 10.1.2.1 をネクスト・ホップとして指定し、9876::55cc を宛先アドレスとして指定します。

| 構成済みのトンネル回線と、トンネル・エンドポイントを定義した経路を作成し終わったら、iSeries B 上および IPv4/6 ルーター上に経路を作成して、パケットをシカゴに送り戻せるようにしなければなりません。iSeries B 上の経路の場合は、9876::55bb をネクスト・ホップとして指定し、4321::54bc を宛先アドレスとして指定する必要があります。IPv4/6 ルーター上の経路の場合は、10.1.1.1 をネクスト・ホップとして指定し、4321::54bc を宛先アドレスとして指定する必要があります。

| 注: ダラスの IPv4/6 ルーターは 9876::55cc に対する直接経路を持つ必要がありますが、この経路は自動的に作成されるので、手操作による構成は必要ありません。

概念: IPv6

| IPv6 の働きについて理解を深めるには、以下の IPv6 の概念に関する説明をお読みください。

IPv4 と IPv6 との比較

IPv4 の属性と IPv6 の属性とを比較しています。この表を使用すると、特定の機能を短時間で見つけて、それぞれのインターネット・プロトコルでの使用法を比較できます。

IPv6 アドレス・フォーマット

IPv6 アドレスのサイズとフォーマットについて説明しています。

IPv6 アドレス・タイプ

IPv6 の範囲内の新しいアドレス・タイプについて説明しています。

IPv6 のトンネリング

IPv6 のトンネリングにより、IPv4 ネットワークを介して IPv6 パケットを送信する方法について説明しています。

近隣ディスカバリー

近隣ディスカバリーを使用して、ホストやルーターが相互に通信できるようにする方法について説明しています。

ステートレス・アドレスの自動構成

ステートレス・アドレスの自動構成により、ネットワーク管理者のタスクの一部を自動化する方法について説明しています。

IPv6 アドレス・フォーマット

IPv6 アドレスのサイズは 128 ビットです。推奨されている IPv6 アドレス表記は、
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (ここでそれぞれの x は、4 ビットを表す 16 進数字) です。
IPv6 アドレスの範囲は、0000:0000:0000:0000:0000:0000:0000:0000 ~
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff です。

この推奨されているフォーマットに加えて、他の 2 種類の短縮されたフォーマットでも IPv6 アドレスを指定できます。

• 先行ゼロを省略する

先行ゼロを省略して IPv6 アドレスを指定します。たとえば、IPv6 アドレス
1050:0000:0000:0000:0005:0600:300c:326b は、1050:0:0:0:5:600:300c:326b と表記できます。

• 2 つのコロン

連続したゼロの代わりに 2 つのコロン (::) を使用して、IPv6 アドレスを指定します。たとえば、IPv6 アドレス
ff06:0:0:0:0:0:0:c3 は、ff06::c3 と表記できます。2 つのコロンは IP アドレス中で 1 回しか使用できません。

IPv6 アドレスの代替フォーマットは、コロンとドット表記を組み合わせたものなので、IPv4 アドレスを IPv6 アドレス中に組み込むことができます。左端の 96 ビットには 16 進値を指定し、組み込んだ IPv4 アドレスを指す右端の 32 ビットには 10 進値を指定します。混合ネットワーク環境で作業している場合、このフォーマットを使用すると、IPv6 ノードと IPv4 ノードの間で確実に互換性を保つことができます。

以下の 2 つのタイプの IPv6 アドレスで、この代替フォーマットが使用されます。

• IPv4 マップ式 IPv6 アドレス

このタイプのアドレスは、IPv4 ノードを IPv6 アドレスとして表すのに使用します。このアドレスを使用すると、IPv6 アプリケーションと IPv4 アプリケーションの間で直接通信できます。たとえば、
0:0:0:0:ffff:192.1.56.10 や ::ffff:192.1.56.10/96 (短縮フォーマット) などです。

IPv4 互換 IPv6 アドレス

このタイプのアドレスは、トンネリング用に使います。これによって、IPv6 ノードは IPv4 インフラストラクチャー全体で通信できます。たとえば、`0:0:0:0:0:0:192.1.56.10` や `::192.1.56.10/96` (短縮フォーマット) などです。

これらのフォーマットはすべて有効な IPv6 アドレス・フォーマットです。iSeries ナビゲーター中でこれらの IPv6 アドレス・フォーマットのいずれかを指定してください。

IPv6 アドレス・タイプ

IPv6 アドレスは、以下の 3 つの基本タイプに分類されます。

ユニキャスト・アドレス

ユニキャスト・アドレスは、1 つのインターフェースを指定します。ユニキャスト・アドレスの宛先に送信されるパケットは、1 つのホストから宛先ホストに送達されます。

以下の 3 種類のユニキャスト・アドレスがあります。

リンク・ローカル・アドレス

リンク・ローカル・アドレスは、1 つのローカル・リンク (ローカル・ネットワーク) 上で使用するように設計されています。リンク・ローカル・アドレスは、すべてのインターフェース上で自動的に構成されます。リンク・ローカル・アドレスの接頭部には、`fe80::/10` が使用されます。ルーターは、リンク・ローカル・アドレスを含む宛先アドレスやソース・アドレスが指定されたパケットは転送しません。

サイト・ローカル・アドレス

サイト・ローカル・アドレスは、特定のサイトで使用するように設計されています。サイト・ローカル・アドレスの接頭部には、`fec0::/10` が使用されます。ルーターは、特定のサイトの外側のサイト・ローカル・アドレスを含むソース・アドレスが指定されたパケットは転送しません。

グローバル・アドレス

グローバル・アドレスは、どのネットワーク上でも使用できるように設計されています。グローバル・アドレスで使用される接頭部の先頭は、2 進数 `001` です。

特殊なタイプのユニキャスト・アドレスには、以下の 2 種類があります。

未指定アドレス

未指定アドレスは、`0:0:0:0:0:0:0:0` とするか、または 2 つのコロン (`::`) を使用して省略することができます。未指定アドレスは、アドレスの不在を示し、ホストに割り当てられることはありません。このアドレスは、まだアドレスが割り当てられていない IPv6 ホストで使用できます。たとえば、ホストで別のノードのアドレスを発見するためにパケットが送信される際には、そのホストでは未指定アドレスがソース・アドレスとして使用されます。

ループバック・アドレス

ループバック・アドレスは、`0:0:0:0:0:0:0:1` とするか、または `::1` と省略することができます。ループバック・アドレスは、ノードからパケットがそのノード自体に送信される際に使用されます。

エニーキャスト・アドレス

エニーキャスト・アドレスは、1 つのアドレスを共用するインターフェースの集合 (別々の場所にあ

る場合もある) をすべて指定します。エニーキャスト・アドレスに送信されるパケットは、グループ中の最寄りのメンバーだけに送達されます。iSeries サーバーは、エニーキャスト・アドレッシングを現在のところサポートしていません。

マルチキャスト・アドレス

マルチキャスト・アドレスは、インターフェースの集合 (複数の場所にある場合もある) を指定します。マルチキャスト・アドレスの接頭部には、ff が使用されます。パケットがマルチキャスト・アドレスに送信される場合には、1 つのパケットのコピーがグループの個々のメンバーに送達されます。現在のところ、iSeries サーバーには、マルチキャスト・アドレッシングの基本サポートが備えられています。マルチキャスト・インターフェースの作成と適用に関するサポートは、現在のところサポートされていません。

IPv6 のトンネリング

IPv6 トンネリングを使用すると、iSeries サーバーから IPv6 ノード (ホストおよびルーター) に IPv4 ドメインを介して接続できます。トンネリングにより、下層の IPv4 インフラストラクチャーに変更を加えずに、孤立している IPv6 ノードやネットワークと通信できます。トンネリングによって IPv4 プロトコルと IPv6 プロトコルとは連携できるので、IPv4 の接続を維持しながら IPv6 のインプリメントに移ることができます。

トンネルは、IPv4 ネットワーク上の 2 つの二重スタック (IPv4 および IPv6) ノードで構成されます。これらの二重スタック・ノードは、IPv4 通信と IPv6 通信の両方を処理できます。IPv6 インフラストラクチャーの端にある 1 つの二重スタック・ノードによって、着信したそれぞれの IPv6 パケットの先頭に IPv4 ヘッダーが挿入され (カプセル化)、既存のリンクを介して通常の IPv4 トラフィックのように送信されます。IPv4 ルーターにより転送が続行されます。トンネルの反対の端では、もう 1 つの二重スタック・ノードによって、追加された IP ヘッダーが IPv6 パケットから除去され (カプセル化解除)、標準的な IPv6 を使用して最終的な宛先に経路指定されます。

iSeries サーバーの IPv6 トンネリングは、構成済みのトンネル回線を介して実行されます。この回線は仮想回線です。構成済みのトンネル回線には、IPv6 トンネルをサポートしている経路指定可能な IPv4 アドレスが指定されたノードに対する IPv6 通信が備えられています。これらのノードの場所はどこでもかまいません。つまり、ローカル IPv4 ドメイン内でもリモート・ドメイン内でもかまいません。

構成済みのトンネルは、Point-to-Point です。このタイプのトンネル回線を構成するには、124.10.10.150 などのローカル・トンネル・エンドポイント (IPv4 アドレス) と、1080:0:0:0:8:800:200c:417a などのローカル IPv6 アドレスを指定しなければなりません。さらに、IPv6 経路も作成して、トンネルを介してトラフィックを送信できるようにしなければなりません。この経路を作成する際に、トンネルのリモート・エンドポイント (IPv4 アドレス) の 1 つを経路のネクスト・ホップとして定義します。構成できるトンネルの数やトンネルのエンドポイントの数には限度はありません。

IPv6 のトンネリングについて説明したシナリオと図については、『IPv4 ローカル・エリア・ネットワーク (LAN) を介した IPv6 パケットの送信』および『IPv4 広域ネットワーク (WAN) を介した IPv6 パケットの送信』を参照してください。

近隣ディスカバリー

近隣ディスカバリー機能は、IPv6 ノード (ホストまたはルーター) で、他の IPv6 ノードを発見したり、ノードのリンク層アドレスを判別したり、IPv6 パケットを転送できるルーターを検索したり、近隣のアクティブな IPv6 のキャッシュを保守したりするのに使用します。IPv6 ノードは、以下の 5 つの Internet Control Message Protocol バージョン 6 (ICMPv6) メッセージを使用して、他のノードと通信します。

ルーター送信請求

これらのメッセージは、ホストからルーターにルーター通知を生成するように要求する場合に送信されます。ネットワーク上でホストがはじめて使用可能になった時点で、そのホストによって初期ルーター送信請求が送信されます。

ルーター通知

これらのメッセージは、ルーターで周期的に送信されるか、またはルーター送信請求の応答として送信されます。ルーター通知によって提供される情報は、ホストでサイト・ローカル・インターフェース、グローバル・インターフェース、および関連した経路を自動的に作成するために使用されます。またルーター通知には、最大伝送単位やホップ限度などの、ホストで使用される他の構成情報も含まれます。

近隣送信請求

これらのメッセージは、近隣のリンク層アドレスを判別したり、依然として近隣にアクセス可能かどうかを検証したりする場合に、ノードによって送信されます。

近隣通知

これらのメッセージは、ノードで近隣送信請求の応答として送信されるか、またはアドレス変更を通知する非送信請求メッセージとして送信されます。

リダイレクト

ルーターは、これらのメッセージを使用して、さらに適した宛先の先頭ホップをホストに通知します。

近隣ディスカバリーとルーター・ディスカバリーの詳細については、RFC 2461 を参照してください。

RFC 2461 を表示するには、RFC Editor (<http://www.rfc-editor.org/rfcsearch.html>)  を参照してください。

ステートレス・アドレスの自動構成

ステートレス・アドレスの自動構成とは、IPv6 ノード (ホストまたはルーター) で IPv6 アドレスをインターフェース用に自動的に構成するのに使用するプロセスのことです。アドレス接頭部と、ノードの MAC アドレスかユーザー指定のインターフェース ID を結合して、さまざまな IPv6 アドレスがノードで作成されます。接頭部には、リンク・ローカル接頭部 (fe80::/10) と、ローカル IPv6 ルーターによって通知される長さ 64 の接頭部 (存在する場合) が含まれます。また、リンク・タイプがマルチキャスト可能な場合は、ステートレス・アドレスの自動構成により該当するマルチキャスト・インターフェースも作成されます。

ノードでは、重複アドレス検出が実行され、アドレスの固有性が検証されてから、インターフェースに割り当てられます。ノードから新しいアドレスに近隣送信請求 QUERY が送信され、応答が待機されます。ノードで応答が受信されないと、アドレスは固有であると想定されます。ノードで近隣通知形式の応答が受信された場合は、アドレスはすでに使用中です。ノードで暫定 IPv6 アドレスが固有でないと判別されると、自動構成は停止し、手操作でインターフェースを構成することが必要になります。

IPv4 と IPv6 との比較

IBM では、いくつかのソフトウェア・リリースにおいて、iSeries サーバー用に IPv6 をインプリメントする予定です。現在 IPv6 は、IPv6 アプリケーションの開発と検査の目的で、アプリケーション開発プラットフォームにインプリメントされています。

IPv6 と IPv4 の詳細な違いについて知りたいと思われるでしょう。以下の表で、IPv4 に関連した従来の属性と、IPv6 の類似の属性と簡単に比較することができます。以下のリストから属性を選択して、表で比較してください。

- 21 ページの『アドレス』
- 21 ページの『アドレス割り振り』

- | • 22 ページの『アドレス存続時間』
- | • 22 ページの『アドレス・マスク』
- | • 22 ページの『アドレス接頭部』
- | • 22 ページの『アドレス解決プロトコル (ARP)』
- | • 22 ページの『アドレス・スコープ』
- | • 22 ページの『アドレス・タイプ』
- | • 23 ページの『通信トレース』
- | • 23 ページの『構成』
- | • 23 ページの『ドメイン・ネーム・システム (DNS)』
- | • 23 ページの『動的ホスト構成プロトコル (DHCP)』
- | • 23 ページの『ファイル転送プロトコル (FTP)』
- | • 23 ページの『フラグメント』
- | • 24 ページの『ホスト・テーブル』
- | • 24 ページの『インターフェース』
- | • 24 ページの『Internet Control Message Protocol (ICMP)』
- | • 24 ページの『Internet Group Management Protocol (IGMP)』
- | • 24 ページの『IP ヘッダー』
- | • 25 ページの『IP ヘッダー・オプション』
- | • 25 ページの『IP ヘッダー・プロトコル・バイト』
- | • 25 ページの『IP ヘッダー Type of Service (TOS) バイト』
- | • 25 ページの『iSeries ナビゲーター・サポート』
- | • 25 ページの『LAN 接続』
- | • 25 ページの『Layer 2 Tunnel Protocol (L2TP)』
- | • 25 ページの『ループバック・アドレス』
- | • 25 ページの『Maximum Transmission Unit (MTU)』
- | • 26 ページの『netstat』
- | • 26 ページの『Network Address Translation (NAT)』
- | • 26 ページの『ネットワーク・テーブル』
- | • 26 ページの『ノード情報照会』
- | • 26 ページの『パケット・フィルター操作』
- | • 26 ページの『パケット転送』
- | • 26 ページの『パケット・トンネル処理』
- | • 27 ページの『PING』
- | • 27 ページの『Point-to-Point Protocol (PPP)』
- | • 27 ページの『ポート制限』
- | • 27 ページの『ポート』
- | • 27 ページの『私用アドレスと共通アドレス』
- | • 27 ページの『プロトコル・テーブル』
- | • 28 ページの『Quality of Service (QOS)』
- | • 28 ページの『再番号付け』
- | • 28 ページの『経路』
- | • 28 ページの『Routing Information Protocol (RIP)』
- | • 28 ページの『サービス・テーブル』
- | • 28 ページの『Simple Network Management Protocol (SNMP)』
- | • 29 ページの『ソケット API』
- | • 29 ページの『ソース・アドレス選択』
- | • 29 ページの『開始および停止』
- | • 29 ページの『Telnet』

- 30 ページの『トレース経路』
- 30 ページの『トランスポート層』
- 30 ページの『未指定アドレス』
- 30 ページの『仮想プライベート・ネットワーキング (VPN)』

	IPv4	IPv6
アドレス	<p>32 ビット (4 バイト) の長さ。アドレスは、アドレス・クラスに応じてネットワーク部分とホスト部分で構成されます。最初の数ビットに基づいて、A、B、C、D、または E アドレス・クラスが定義されます。IPv4 アドレスの合計数は 4 294 967 296 です。</p> <p>IPv4 アドレスのテキスト書式は、<code>nnn.nnn.nnn.nnn</code> です ($0 \leq nnn \leq 255$ で、個々の <code>n</code> は 10 進数字)。先行ゼロは省略できます。印刷文字の最大数は 15 で、これにはマスクは数えられていません。</p>	<p>128 ビット (16 バイト) の長さ。基本アーキテクチャーは、ネットワーク番号が 64 ビット、およびホスト番号が 64 ビットです。IPv6 アドレスのホスト部分 (またはその一部) が MAC アドレスか他のインターフェース ID になることがよくあります。</p> <p>サブネット接頭部によっては、IPv6 のアーキテクチャーの方が IPv4 より複雑になります。</p> <p>IPv6 アドレスの数は、IPv4 アドレスの数の 10^{28} (79 228 162 514 264 337 593 543 950 336) 倍の長さです。</p> <p>IPv6 アドレスのテキスト形式は、<code>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx</code> (個々の <code>x</code> は 4 ビットを表す 16 進数字) です。先行ゼロは省略できます。アドレスのテキスト形式中に 2 つのコロン (<code>::</code>) を 1 回使用して、任意の数の 0 ビットを指定できます。たとえば、<code>::ffff:10.120.78.40</code> は IPv6 IPv4 マップ式アドレスです。(詳細については、RFC 2373 を参照してください。この RFC を表示するには、RFC Editor (http://www.rfc-editor.org/rfcsearch.html) を参照してください。)</p>
アドレス割り振り	<p>元々は、アドレスはネットワーク・クラス別に割り振られています。アドレス・スペースが少なくなるにつれて、無クラス・ドメイン間経路指定 (CIDR) を使用して行われる割り振りは縮小されます。割り振りは、各種公共機関や国家間で調整されていません。</p>	<p>割り振りは最初期の段階で行われます。Internet Engineering Task Force (IETF) および Internet Architecture Board (IAB) は、事実上すべての組織、家庭、またはエンティティー用に長さ /48 のサブネット接頭部を割り振ることを推奨しています。この場合、組織がサブネットを行う余地が 16 ビット分残ります。アドレス・スペースは、世界中のすべての人が自分用に長さ /48 のサブネット接頭部を持てるだけの大きさになっています。</p>

	IPv4	IPv6
アドレス存続時間	通常、DHCP を使用して割り当てられたアドレスを除いて、この概念は適用できません。	IPv6 アドレスには、優先および有効という 2 つの存続時間があります。常に優先存続時間 <= 有効存続時間になります。 優先存続時間の有効期限が切れると、そのアドレスはソース IP アドレスとして使用されなくなります。有効存続時間の有効期限が切れると、そのアドレスは着信パケットの有効宛先 IP アドレスとして使用 (認識) されなくなります。 リンク・ローカル・アドレスなどの一部の IPv6 アドレスは、無期限の優先および有効存続時間になるように定義されています (『アドレス・スコープ』を参照)。
アドレス・マスク	ホスト部分からネットワークを指定するのに使用されます。	使用されません (『アドレス接頭部』を参照)。
アドレス接頭部	ホスト部分からネットワークを指定するのに使用されることがあります。アドレスの表示形式上に /nn 接尾部として書き込まれていることがあります。	アドレスのサブネット接頭部を指定するのに使用されます。印刷形式の後に /nnn (最大 3 桁の 10 進数字、0 <= nnn <= 128) 接尾部として書き込まれます。たとえば、fe80::982:2a5c/10 の場合、最初の 10 ビットによりサブネット接頭部が構成されます。
アドレス解決プロトコル (ARP)	アドレス解決プロトコルは、IPv4 アドレスに関連した物理アドレス (MAC またはリンク・アドレス) を検索するために、IPv4 で使用されます。	IPv6 では、これらの機能は、Internet Control Message Protocol version 6 (ICMPv6) を使用して、ステートレス自動設定および近隣探索のアルゴリズムの一部として IP 自体に組み込まれています。したがって、ARP6 などは存在しません。
アドレス・スコープ	ユニキャスト・アドレスの場合は、この概念は適用されません。指定された私用アドレス範囲およびループバックがあります。この外側では、アドレスはグローバルなものに見なされます。	IPv6 では、アドレス・スコープはアーキテクチャーの一部です。ユニキャスト・アドレスには 3 つの定義済みスコープ (リンク・ローカル、サイト・ローカル、グローバル) があり、マルチキャスト・アドレスには 14 のスコープがあります。ソースと宛先のデフォルト・アドレス選択では、スコープが考慮されます。 スコープ・ゾーンは、特定のネットワーク内のスコープのインスタンスです。その結果、IPv6 のアドレスは、ゾーン ID と一緒に入力するか、ゾーン ID と関連付ける必要があります。構文は %zid で、この zid は番号 (通常は小さい番号) または名前です。ゾーン ID は、アドレスの後ろで、接頭部の前に書きます。たとえば、2ba::1:2:14e:9a9b:c%3/48 のようになります。
アドレス・タイプ	ユニキャスト、マルチキャスト、およびブロードキャスト。	ユニキャスト、マルチキャスト、およびエニーキャスト。説明については、IPv6 アドレス・タイプを参照してください。

	IPv4	IPv6
通信トレース	iSeries サーバーに入って出て行く TCP/IP (およびその他の) パケットの詳細なトレースを収集するツール。	IPv6 の場合も同様で、IPv4 でトンネル処理される ICMPv6 パケットおよび IPv6 パケットも含め、IPv6 がサポートされます。
構成	通信する前に、新しくインストールされたシステムで構成を行う必要があります。つまり、IP アドレスと経路を割り当てる必要があります。	構成は任意に選択することができ、必要な機能に応じて異なります。iSeries ナビゲーターを使用して、適切なイーサネットまたはトンネル・インターフェースを IPv6 インターフェースとして指定する必要があります。この指定を完了させれば、IPv6 インターフェースは自己構成するようになります。したがって、システムは、ネットワークのタイプと IPv6 ルーターが存在するかどうかに応じて、他のローカルおよびリモートの IPv6 システムと通信できるようになります。
ドメイン・ネーム・システム (DNS)	<p>アプリケーションは、ホスト名を受け入れ、次いでソケット API <code>gethostbyname()</code> を使って DNS を利用し、IP アドレスを取得します。</p> <p>アプリケーションは、IP アドレスを受け入れ、次いで <code>gethostbyaddr()</code> を使って DNS を利用し、ホスト名を取得することもできます。</p> <p>IPv4 の場合、リバース・ルックアップ用のドメインは <code>in-addr.arpa</code> です。</p>	<p>IPv6 の場合も同様です。IPv6 は、AAAA (A の 4 倍長) のレコード・タイプとリバース・ルックアップ (IP から名前) を使用してサポートされます。アプリケーションは、DNS から IPv6 アドレスを受け入れ (または受け入れず)、次いで IPv6 を使用して (または使用しないで) 通信を行うことを選択できます。</p> <p>ソケット API <code>gethostbyname()</code> は IPv6 で変更されていません。 <code>getaddrinfo()</code> API を使用して (アプリケーションの選択に基づいて) IPv6 アドレスのみ、または IPv4 と IPv6 の両方のアドレスを取得することができます。</p> <p>IPv6 の場合、リバース・ニブル・ルックアップに使用されるドメインは <code>ip6.arpa</code> です。見つからない場合は <code>ip6.int</code> が使用されます (API <code>getnameinfo()</code> を参照)。</p>
動的ホスト構成プロトコル (DHCP)	IP アドレスや他の構成情報を動的に取得するために使用されます。	現在、DHCP は IPv6 をサポートしていません。
ファイル転送プロトコル (FTP)	ファイル転送プロトコルを使用すれば、複数のネットワーク間でファイルを送受信できます。	現在、FTP は IPv6 をサポートしていません。
フラグメント	パケットが通る次のリンクに対してパケットが大きすぎる場合、送信側 (ホストまたはルーター) によってパケットをフラグメント化することができます。	IPv6 の場合、フラグメント化はソース・ノードでのみ行われ、再組み立ては宛先ノードでのみ行われます。現在、フラグメント化拡張ヘッダーはサポートされていません。

	IPv4	IPv6
ホスト・テーブル	iSeries ナビゲーターでは、IP アドレスをホスト名に関連付ける構成可能テーブル。たとえば、127.0.0.1 と loopback を関連付けます。このテーブルは、DNS ルックアップの前または DNS ルックアップが失敗した後 (どちらになるかは、ホスト名検索の優先順位によって決まる) で、ソケット・ネーム・リゾルバーによって使用されます。	現在、このテーブルは IPv6 をサポートしていません。IPv6 ドメイン解決のために、AAAA レコードを DNS 内で構成する必要があります。DNS は、リゾルバーと同じシステムでローカルに実行することも、別のシステムで実行することもできます。
インターフェース	<p>パケットを送受信するために TCP/IP によって使用される概念上のまたは論理的なエンティティーで、IPv4 アドレスを使用して名前が付けられていないとしても、常に IPv4 アドレスと密接な関係があります。論理インターフェースとして呼ばれることもあります。</p> <p>STRTCPIFC および ENDTCPIFC コマンドを使用したり、iSeries ナビゲーターを使用して、互いに独立して、または TCP/IP とは無関係に開始および停止できます。</p>	<p>IPv4 と同じ概念。</p> <p>iSeries ナビゲーターだけを使用して、互いに独立して、また TCP/IP と無関係に開始および停止できます。</p>
Internet Control Message Protocol (ICMP)	ICMP は、ネットワーク情報を伝達するために IPv4 によって使用されます。	<p>IPv6 でも同じように使用されますが、Internet Control Message Protocol version 6 (ICMPv6) には、いくつかの新しい属性が備えられています。</p> <p>宛先到達不能、エコー要求およびエコー応答などの基本エラー・タイプは残されています。近隣探索および関連機能をサポートするために、新しいタイプおよびコードが追加されています。</p>
Internet Group Management Protocol (IGMP)	IGMP は、IPv4 ルーターによって、特定のマルチキャスト・グループ用のトラフィックを必要とするホストを検索するために使用され、IPv4 ホストによって、(ホスト上の) 既存のマルチキャスト・グループ・リスナーの情報を IPv4 ルーターに伝えるために使用されます。	IPv6 では、MLD (multicast listener discovery) プロトコルに置き換えられています。IPv4 での IGMP の機能の仕方と基本的には同じですが、いくつかの MLD 固有の ICMPv6 タイプ値を追加することによって ICMPv6 を使用します。
IP ヘッダー	20 ~ 60 バイトの可変長。指定された IP オプションに応じて長さが変わります。	40 バイトの固定長。IP ヘッダー・オプションはありません。一般に、IPv6 ヘッダーは IPv4 ヘッダーよりも単純です。

	IPv4	IPv6
IP ヘッダー・オプション	IP ヘッダーに添付できる (トランスポート・ヘッダーより前にある) さまざまなオプション。	IPv6 ヘッダーにはオプションがありません。その代わりに、IPv6 では追加の (オプションの) 拡張ヘッダーが追加されています。拡張ヘッダーは AH および ESP (IPv4 から未変更)、hop-by-hop、経路指定、フラグメント、および宛先です。現在、IPv6 は拡張ヘッダーをサポートしていません。
IP ヘッダー・プロトコル・バイト	トランスポート層またはパケット・ペイロードのプロトコル・コード。たとえば、ICMP。	IPv6 ヘッダーの直後にあるヘッダーのタイプ。IPv4 プロトコル・フィールドと同じ値を使用します。しかし、構造的な影響として、次のヘッダーの現在定義されている範囲を使用することができます。また、この範囲は簡単に拡張できます。トランスポート・ヘッダー、拡張ヘッダー、または ICMPv6 が、次のヘッダーとなります。
IP ヘッダー Type of Service (TOS) バイト	トラフィック・クラスを指定するために、QoS および DiffServ によって使用されます。	IPv4 と同じように、IPv6 トラフィック・クラスを指定します。別のコードを使用しません。現在、IPv6 は TOS をサポートしていません。
iSeries ナビゲーター・サポート	iSeries ナビゲーターは、TCP/IP 用の完全な構成機能を提供しています。	iSeries ナビゲーターによって、IPv6 用のオプションの構成が完全に提供されています。これには、「IPv6 構成 (IPv6 Configuration)」ウィザードも含まれます。
LAN 接続	物理ネットワークに到達するために IP インターフェースによって使用されます。多くのタイプがあります。たとえば、トークンリング、イーサネット、および PPP などです。物理インターフェース、リンク、または回線と呼ばれることもあります。	IPv6 にも同じ概念があります。現在、2838 および 2849 イーサネット・カードとトンネル回線だけがサポートされています。
Layer 2 Tunnel Protocol (L2TP)	L2TP は仮想 PPP と考えることができ、サポートされるどの回線タイプでも機能します。	現在、L2TP は IPv6 をサポートしていません。
ループバック・アドレス	127.*.*.* (通常は 127.0.0.1) というアドレスを持つインターフェース。ノードが自身に向けてパケットを送信するためだけに使用できます。物理インターフェース (回線記述) には *LOOPBACK という名前が付けられます。	概念は IPv4 と同じで、単一のループバック・アドレスは 0000:0000:0000:0000:0000:0000:0000:0001 または ::1 (短縮形) です。仮想物理インターフェースには *LOOPBACK6 という名前が付けられます。
Maximum Transmission Unit (MTU)	リンクの最大転送単位は、イーサネットまたはモデムなどの特定のリンク・タイプがサポートする最大バイト数です。IPv4 の場合、576 が一般的な最小値です。	IPv6 には、MTU に 1280 バイトという設計済みの下限があります。つまり、IPv6 はこの限度より小さくパケットをフラグメント化することはありません。IPv6 を 1280 より小さい MTU のリンクを介して送信する場合は、リンク層は透過的に IPv6 パケットのフラグメント化とデフラグメント化を行います。

	IPv4	IPv6
netstat	TCP/IP 接続、インターフェース、または経路の状況を調べるためのツール。iSeries ナビゲーターおよび 5250 を利用して使うことができます。	IPv6 の場合も同様で、IPv6 は、5250 および iSeries ナビゲーターの両方でサポートされています。
Network Address Translation (NAT)	TCP/IP に組み込まれている基本ファイアウォール機能で、iSeries ナビゲーターを使用して構成されます。	現在、NAT は IPv6 をサポートしていません。より一般的に言えば、IPv6 では NAT は必要ありません。IPv6 の拡張されたアドレス・スペースにより、アドレスこぼれ問題が解消され、再番号付けが行いやすくなります。
ネットワーク・テーブル	iSeries ナビゲーターでは、ネットワーク名をマスクなしの IP アドレスに関連付ける構成可能なテーブル。たとえば、ホスト Network14 と IP アドレス 1.2.3.4 を関連付けます。	現在、IPv6 ではこのテーブルは変更されていません。
ノード情報照会	存在しません。	内容を別にして、PING のように機能する単純で便利なネットワーク・ツール。IPv6 ノードは、別の IPv6 ノードからターゲットの DNS 名、IPv6 ユニキャスト・アドレス、または IPv4 アドレスを照会します。現在、サポートされていません。
パケット・フィルタ操作	TCP/IP に組み込まれている基本ファイアウォール機能で、iSeries ナビゲーターを使用して構成されます。	現在、パケット・フィルタ操作は IPv6 をサポートしていません。ただし、IPv4 フィルタ操作は、トンネル処理された IPv6 トラフィックに適用できます。
パケット転送	非ローカル IP アドレス用に受信する IP パケットを転送するように iSeries サーバーを構成できます。通常、インバウンド・インターフェースとアウトバウンド・インターフェースは別々の LAN に接続されます。	現在、IPv6 パケットは転送されません。
パケット・トンネル処理	IPv4 では、トンネル処理は、トンネル・モード VPN 接続用の VPN (IPv4 での IPv4 トンネル処理) と L2TP で行われます。	IPv6 の場合、IPv4 パケットでのトンネル処理が、その発展の主要部分であると预期されています。現在、最低 5 つの異なるタイプの 6-in-4 トンネル処理が IETF によって定義されており、属性と利点はそれぞれ異なります。 IPv6 ノードが既存の IPv4 インターネット上で通信できるようにするために、基本的で柔軟なタイプの IPv6-in-IPv4 トンネル処理がサポートされています。構成済みトンネル処理と呼ばれるものは、2 つの IPv6 ノード間に仮想 Point-to-Point リンクを提供し、*TNLCFG64 と呼ばれる新しいタイプのトンネル回線を使用します。

	IPv4	IPv6
PING	到達性をテストするための TCP/IP の基本ツール。 iSeries ナビゲーター および 5250 を利用して使うことができます。	IPv6 の場合も同様で、IPv6 は、5250 および iSeries ナビゲーターの両方でサポートされています。
Point-to-Point Protocol (PPP)	PPP は、さまざまなモデムや回線タイプを介したダイヤルアップ・インターフェースをサポートしています。	現在、PPP は IPv6 をサポートしていません。
ポート制限	これらの iSeries パネルを使用すれば、 TCP または UDP 用の選択したポート番号またはポート番号の範囲を構成して、それらが特定のプロファイルでしか使用できないようにすることができます。	IPv6 ではサポートされていません。構成済みの制限は、IPv4 にのみ適用されます。
ポート	TCP および UDP は別々のポート・スペースを持ち、それぞれ 1 ～ 65535 の範囲のポート番号で識別されます。	IPv6 の場合、ポートの機能は IPv4 と同じです。これらのポートは新しいアドレス・ファミリーに入っているため、4 つの別個のポート・スペースがあります。たとえば、アプリケーションをバインドできる TCP ポート 80 スペースは 2 つ (AF_INET と AF_INET6 に 1 つずつ) あります。
私用アドレスと共通アドレス	IPv4 アドレスはすべて共通アドレスです。ただし、IETF RFC 1918 によって私用アドレスとして指定されている 3 つのアドレス範囲、つまり 10.*.*.* (10/8)、172.16.0.0 ～ 172.31.255.255 (172.16/12)、および 192.168.*.* (192.168/16) は例外です。私用アドレス・ドメインは、一般に組織内で使用されます。私用アドレスは、インターネット上で経路指定することはできません。	IPv6 にも類似の概念はありますが、重要な違いがあります。 アドレスは共通または一時アドレス (以前は匿名と表現されていた) です。RFC 3041 を参照してください。IPv4 私用アドレスとは異なり、一時アドレスはグローバルに経路指定できます。その動機も異なっており、IPv6 一時アドレスは、クライアントが通信を開始するときにクライアントの身元を隠すためのものです (プライバシー上の懸念)。一時アドレスには、限定された存続時間があり、リンク (MAC) アドレスであるインターフェース ID が含まれていません。一般に、一時アドレスと共通アドレスは見分けが付きません。 IPv6 には、設計済みスコープ指定を使用する、限定されたアドレス・スコープの概念があります (22 ページの『アドレス・スコープ』を参照)。
プロトコル・テーブル	iSeries ナビゲーターでは、プロトコル名をそれに割り当てられたプロトコル番号と関連付ける構成可能なテーブル。たとえば、UDP と 17 を関連付けます。システムは、少数のエントリ (IP、TCP、UDP、ICMP) が入った状態で出荷されています。	このテーブルは、変更なしで IPv6 をサポートします。

	IPv4	IPv6
Quality of Service (QoS)	Quality of Service (QoS) を使用すれば、TCP/IP アプリケーション用のパケット優先順位と帯域幅を要求できます。	現在、QoS は IPv6 をサポートしていません。ただし、IPv6 が IPv4 でトンネル処理されると、既存の iSeries QoS 機能を IPv4 トラフィックに適用することができ、IPv6 ペイロードが透過的に処理されるようになります。
再番号付け	手動で再構成することによって行います。DHCP の例外がある場合があります。一般に、サイトや組織にとって困難で面倒な処理となるので、可能な限り避けるべきです。	IPv6 の重要な構造上のエレメントで、特に /48 接頭部ではおおむね自動的に行われることになっています。
経路	論理的には、IP アドレスのセット (アドレスが 1 つだけの場合もある) を、物理インターフェースと単一のネクスト・ホップ IP アドレスにマップすること。宛先アドレスがこのセットの一部として定義されている IP パケットは、回線を使用してネクスト・ホップに転送されます。IPv4 の経路は、IPv4 インターフェースに関連付けられているので、IPv4 アドレスです。 デフォルトの経路は *DFTRROUTE です。	概念上は IPv4 と同じ。1 つの重要な違いがあります。つまり、IPv6 の経路は、インターフェースではなく、物理インターフェース (*TNLCFG64 や ETH03 などのリンク) に関連付けられています。これには、さまざまな理由があります。1 つの理由は、ソース・アドレス選択の機能の仕方が IPv6 と IPv4 で異なっていることです。29 ページの『ソース・アドレス選択』を参照してください。 信頼性を高めるために重複経路を使用することができますが、これは経路ルックアップ中は無視されます。
Routing Information Protocol (RIP)	RIP は、経路指定されたデーモンによってサポートされる経路指定プロトコルです。	現在、RIP は IPv6 をサポートしていません。IPv6 の経路指定では、静的経路が使用されます。
サービス・テーブル	iSeries サーバーでは、サービス名をポートおよびプロトコルに関連付ける構成可能なテーブル。たとえば、サービス名 FTP-control、ポート 21、TCP および UDP を関連付けます。 サービス・テーブルには、多くの既知のサービスがリストされています。多くのアプリケーションは、使用するポートをこのテーブルを使って判別します。	IPv6 ではこのテーブルは変更されていません。
Simple Network Management Protocol (SNMP)	SNMP はシステム管理用のプロトコルです。	現在、SNMP は IPv6 をサポートしていません。IPv6 の経路指定では、静的経路が使用されます。

	IPv4	IPv6
ソケット API	これらの API は、アプリケーションが TCP/IP を使用する手段となります。IPv6 を必要としないアプリケーションは、ソケットが IPv6 をサポートするよう変更されても影響を受けません。	IPv6 ではソケットが機能強化され、アプリケーションは AF_INET6 という新しいアドレス・ファミリーを使って、IPv6 を使用できるようになりました。 この機能強化は、既存の IPv4 アプリケーションが、IPv6 および API の変更による影響をまったく受けないように設計されています。現在の IPv4 および IPv6 トラフィック、または IPv6 専用トラフィックをサポートすることを求めるアプリケーションは、IPv4 にマップされた IPv6 アドレスを使用して簡単に適応させることができます。このアドレスの形式は <code>::ffff:a.b.c.d</code> で、 <code>a.b.c.d</code> はクライアントの IPv4 アドレスです。 新しい API でも、テキストからバイナリー、またバイナリーからテキストへの IPv6 アドレスの変換がサポートされています。 IPv6 用のソケット機能強化の詳細については、『AF_INET6 アドレス・ファミリーの使用』を参照してください。
ソース・アドレス選択	アプリケーションはソース IP を指定することができます (通常、ソケット <code>bind()</code> を使用して)。アプリケーションが <code>INADDR_ANY</code> にバインドする場合は、ソース IP はその経路に基づいて選択されます。	IPv4 の場合と同様に、アプリケーションは <code>bind()</code> を使用してソース IPv6 アドレスを指定することができます。IPv4 と同様に、 <code>in6addr_any</code> を使用することによって、システムに IPv6 ソース・アドレスを選択させることができます。IPv6 回線には多くの IPv6 アドレスがあるので、ソース IP を内部方式で選択することは困難です。
開始および停止	STRTCP および ENDTCP を使用して、TCP/IP を開始または終了します。	IPv4 と同じ。IPv4 と IPv6 は、互いに独立して、また TCP/IP と無関係に開始および停止することはできません。つまり、IPv4 か IPv6 だけではなく、TCP/IP 全体を開始および停止します。 AUTOSTART パラメーター = *YES (デフォルト) の場合、IPv6 インターフェースは自動的に開始します。IPv4 を使用しないで IPv6 を使用したり構成することはできません。また、IPv6 では IPv6 ループバックを構成しておく必要があります (<code>::1</code>)。
Telnet	Telnet を使用すれば、直接接続しているかのように、リモート・コンピュータにログオンしてそれを使用できます。	現在、Telnet は IPv6 をサポートしていません。

	IPv4	IPv6
トレース経路	パスを判別するための TCP/IP の基本ツール。iSeries ナビゲーターおよび 5250 を利用して使うことができます。	IPv6 の場合も同様で、IPv6 は、5250 および iSeries ナビゲーターの両方でサポートされています。
トランスポート層	TCP、UDP、RAW。新しいトランスポート・プロトコルである Stream Control Transmission Protocol (SCTP) の目的は、TCP と UDP の最も優れた機能、つまり保証された接続レス通信を提供することです。SCTP は初期使用段階にあるので、iSeries ではサポートされていません。	IPv6 では、同じ 3 つのトランスポート・プロトコルが存在し、機能も同じです。
未指定アドレス	明確に定義されていないもの。ソケット・プログラミングでは、0.0.0.0 を INADDR_ANY として使用します。	::/128 (128 0 ビット) と定義される。一部の近隣探索パケットや、ソケットなどの他のさまざまなコンテキストで、ソース IP として使用されます。ソケット・プログラミングでは、::/128 を in6addr_any として使用します。
仮想プライベート・ネットワーク (VPN)	仮想プライベート・ネットワーク (IPsec を使用) を使用すれば、既存の共通ネットワーク上にセキュアな私用ネットワークを拡張できます。	現在、VPN は IPv6 をサポートしていません。ただし、IPv6 が IPv4 でトンネル処理されると、既存の iSeries VPN 機能を IPv4 トラフィックに適用することができ、IPv6 ペイロードが透過的に処理されるようになります。

IPv6 に関する関連情報

IPv6 の詳細については、以下の参考資料を参照してください。

The Internet Engineering Task Force (IETF) (<http://www.ietf.cnri.reston.va.us/>) 

IPv6 を含め、インターネット・プロトコルを開発している個々のグループについて説明しています。

IP Version 6 (IPv6) (<http://playground.sun.com/pub/ipng/html/ipng-main.html>) 

現在の IPv6 仕様の説明と IPv6 のいくつかのソースへの参照があります。

IPv6 Forum (<http://www.ipv6forum.com/>) 

最新の IPv6 開発を伝えるニュース記事やイベントがあります。

第 4 章 TCP/IP セットアップの計画

iSeries サーバーのインストールと構成を始める前に、少しの時間を取って操作の計画を立ててください。計画のガイドラインとして、以下のトピックを参照してください。これらの計画のガイドラインは、IPv4 を使用する基本 TCP/IP のセットアップ向けです。IPv6 を構成する場合、セットアップ要件および構成の指示については、『IPv6 の構成』を参照してください。

TCP/IP セットアップの要件

TCP/IP セットアップに必要な基本的な構成情報を収集して記録します。

TCP/IP セキュリティーの考慮事項

ネットワークの新しいメンバーとしてのセキュリティー上のニーズを考慮します。

TCP/IP セットアップの要件

このページを印刷し、サーバーおよび接続する TCP/IP ネットワークの構成情報について記録してください。この情報は、後で TCP/IP を構成する際に必要になります。表の後の指示に従って、最初の 2 行の値を決定します。これらの用語のいずれかに精通しておられない方は、IBM レッドブック TCP/IP for

AS/400®: More Cool Things Than Ever  の第 2 章 『TCP/IP: Basic Installation and Configuration』を参照してください。

必要な情報	ご使用のシステム	例
システムにインストールされた通信アダプターのタイプ (下記参照)		イーサネット
リソース名		CMN01
iSeries サーバーの IP アドレス		199.5.83.158
iSeries サーバーのサブネット・マスク		255.255.255.0
ゲートウェイ・アドレス		199.5.83.129
ご使用のシステムのホスト名およびドメイン・ネーム		sys400.xyz.company.com
ドメイン・ネーム・サーバーの IP アドレス		199.4.191.76

通信アダプターの情報を見付けるには、以下の手順に従ってください。

1. サーバーのコマンド行に go hardware と入力してから、**Enter** を押します。
2. 「通信資源の処理 (オプション 1)」を選択するには、1 と入力してから、**Enter** を押します。


通信リソースは、リソース名でリストされます。ご使用のリソースを処理したり、詳細を調べるには、表示の指示に従ってください。

次にすること:

TCP/IP をインストールする

TCP/IP セキュリティーの考慮事項

TCP/IP 構成を計画する際には、セキュリティーの必要性を考慮しなければなりません。これらの戦略は、TCP/IP の機密漏れを防ぐのに役立ちます。

- **必要な TCP/IP アプリケーションのみ開始する。**
TCP/IP アプリケーションの機密漏れの仕方は、それぞれ異なります。特定のアプリケーションの要求を拒否するのにルーターだけに依存することはできません。二次的な防御策として、必須ではないアプリケーションの自動開始値を NO に設定します。
- **TCP/IP アプリケーションを実行する時間を制限する。**
サーバーを実行する時間を短くすることで、機密漏れを防ぎます。可能なら、オフ・タイムには FTP や Telnet などの TCP/IP サーバーを停止してください。
- **TCP/IP アプリケーションを開始および変更できる人を制御する。**
デフォルトでは、TCP/IP 構成の設定を変更するには、*IOSYSCFG 権限が必要です。*IOSYSCFG 権限のないユーザーは、TCP/IP 開始コマンドに対する *ALLOBJ 権限または明示的な権限が必要です。ユーザーに特殊権限を与えると、機密漏れの危険性が高くなることを意味します。それぞれのユーザーに与える権限について必要性を注意深く検討し、特殊権限を最小限にとどめるようにしてください。どのユーザーに特殊権限があるかについて記録を保持し、定期的にその権限の必要性について検討します。こうすることによっても、オフ・タイムのサーバー・アクセスの可能性を制限できます。
- **ご使用の TCP/IP 経路を制御する。**
 - IP 転送を禁止して、ハッカーが Web サーバーを使用して他のトラステッド・システムに侵入できないようにする。
 - 公開 Web サーバーでは、1 つの経路のみ定義し、インターネット・サービス・プロバイダーへのデフォルトの経路とする。
 - ご使用の Web サーバーの TCP/IP ホスト・テーブルの内部保護システムのホスト名および IP アドレスは構成しない。このテーブルで到達する必要がある他の公共サーバーの名前を入れるだけにします。
- **リモートの対話式サインオン用に設計された TCP/IP サーバーを制御する。**
FTP および Telnet などのアプリケーションの方が外部からの攻撃に弱いと言えます。機密漏れを制御する方法については、iSeries セキュリティーの手引き  の、対話式サインオンの制御に関するヒントの章をお読みください。

セキュリティーおよび使用できるオプションについての詳細は、『IBM Secureway: iSeries とインターネット』を参照してください。

第 5 章 TCP/IP のインストール

基本 TCP/IP サポートは OS/400 に付属しており、これによって iSeries サーバーからネットワークに接続することができます。ただし、Telnet、FTP、および SMTP のような任意の TCP/IP アプリケーションを使用するには、TCP/IP 接続ユーティリティもインストールする必要があります。これは、ご使用のオペレーティング・システムに含まれている、別個にインストール可能なライセンス製品です。

ご使用の iSeries サーバーで TCP/IP 接続ユーティリティをインストールするには、以下の手順に従います。

1. TCP/IP インストール・メディアをサーバーに挿入します。インストール・メディアが CD-ROM の場合は、光ディスク装置に挿入してください。インストール・メディアがテープの場合は、磁気テープ・ドライブに挿入してください。
2. コマンド行に GO LICPGM と入力してから、**Enter** を押して、「ライセンス・プログラムの処理」画面にアクセスします。
3. 「ライセンス・プログラムの処理」画面で、オプション **11** (ライセンス・プログラムの導入) を選択します。ライセンス・プログラムとそのオプション部の一覧が表示されます。
4. 57xxTC1 (iSeries TCP/IP 接続ユーティリティ) の横の「オプション」欄に **1** (導入) と入力します。**Enter** を押します。「ライセンス・プログラムの導入確認」画面に、インストールするよう選択したライセンス・プログラムが表示されます。確認してから **Enter** を押してください。
5. 「導入オプション」画面で、下記の選択項目を入力します。

インストール・デバイス	CD-ROM 装置からインストールする場合は、QOPT と入力します。 磁気テープ・ドライブからインストールする場合は、TAP01 と入力します。
インストールするオブジェクト	このオプションによって、プログラムと言語オブジェクトの両方、あるいはプログラムか言語オブジェクトの一方だけを選択してインストールできます。
自動再始動	このオプションは、インストール処理が正常に完了した後にシステムを自動的に始動させるかどうかを指定します。

TCP/IP 接続ユーティリティが正常にインストールされると、「ライセンス・プログラムの処理」メニューかサインオン画面のいずれかが表示されます。

6. オプション **50** (メッセージのログ表示) を選択して、ライセンス・プログラムを正常にインストールできたかどうかを調べてください。

エラーが発生した場合は、「ライセンス・プログラムの処理」画面の下の部分に「ライセンス・プログラムの処理 - 機能未完了」というメッセージが表示されます。問題が発生した場合は、TCP/IP 接続ユーティリティを再インストールしてください。それでも問題が解決されない場合には、サポートを依頼する必要があります。

注:

インストールできるその他のライセンス・プログラムには、次のようなものがあります。

- iSeries Access for Windows 95/NT (5769-XD1 V3R1M3 またはそれ以降)。これは、いくつかの TCP/IP コンポーネントの構成に使用する iSeries ナビゲーター・サポートを提供します。
- IBM HTTP Server iSeries (57xx-DG1)。これは Web サーバー・サポートを提供します。

- TCP/IP アプリケーションには、追加のライセンス・プログラムをインストールする必要があるものもあります。必要なプログラムを見つけるには、使用したいアプリケーションのセットアップ指示書を調べてください。

第 6 章 TCP/IP の構成

はじめて TCP/IP を構成する場合や、または IPv6 機能を使用するために既存の構成を変更したい場合もあるでしょう。このトピックでは、これらの各状況において TCP/IP を構成するための手順を記載しています。ご使用のサーバーで TCP/IP を構成する手順については、以下の任意に選択できる情報を参照してください。

はじめての TCP/IP の構成

新規サーバーをセットアップする場合には、これらの手順に従います。接続を確立して、最初に TCP/IP を構成します。

IPv6 の構成

IPv6 機能用のサーバーを構成するには、これらの手順に従います。インターネット・プロトコルの拡張アドレッシング機能および堅固な機能から益が得られます。IPv6 に精通しておられない方は、概要を知るために、Internet Protocol version 6 (IPv6) を参照してください。IPv6 を構成する前に、サーバー上に TCP/IP が構成されていなければなりません。

はじめての TCP/IP の構成

新規サーバー上に TCP/IP をセットアップするには、以下のメソッドのうちの 1 つを選択してください。

EZ セットアップ・ウィザードを使用して TCP/IP を構成する

PC で EZ セットアップ・ウィザードが備えられており使用できる場合には、この方法を使うことをお勧めします。EZ セットアップ・ウィザードは、iSeries サーバーに同梱されています。

文字ベースのインターフェースを使用して TCP/IP を構成する

EZ セットアップ・ウィザードを使用できない場合は、このメソッドを使用します。たとえば、iSeries ナビゲーターが実行する前に基本 TCP/IP 構成を必要とする PC から iSeries ナビゲーターを使用する場合には、このメソッドを使用する必要があります。

EZ セットアップ・ウィザードを使用した TCP/IP の構成

iSeries ナビゲーターは、TCP/IP の構成用の簡易なダイアログ・ボックスおよびウィザードを提供する、グラフィカル・ユーザー・インターフェースです。初期セットアップの場合には、iSeries ナビゲーターの EZ セットアップ・ウィザードを使用して、接続を確立し、最初に TCP/IP を構成してください。このインターフェースは使用が簡単であるため、サーバーでの作業にはこの方法を使うことをお勧めします。EZ セットアップ・ウィザードを収録した CD-ROM は、iSeries サーバーに同梱されています。


ご使用のサーバーを構成するには、以下の手順に従ってください。

1. EZ セットアップ・ウィザードを使用します。ご使用のサーバーに同梱されている CD-ROM からこのウィザードにアクセスします。ウィザードの指示に従って TCP/IP を構成してください。
2. TCP/IP を開始します。
 - a. iSeries ナビゲーターで、「サーバー」->「ネットワーク」の順に展開します。
 - b. 「TCP/IP 構成」を右クリックしてから、「始動」を選択します。TCP/IP が開始されるときに自動的に始動するように設定されたインターフェースおよびサーバーはすべて、この時点で始動されます。

これで、サーバー上での TCP/IP の構成が完了しました。iSeries ナビゲーターを使用して、ネットワークで変更が必要な場合は構成を変更してください。経路およびインターフェースを追加するには、『iSeries ナビゲーターを使用した TCP/IP のカスタマイズ』を、ネットワークで Internet Protocol version 6 を使用するには、『IPv6 の構成』を参照してください。

文字ベースのインターフェースを使用した TCP/IP の構成

iSeries ナビゲーターの EZ セットアップ・ウィザードを使用できない場合は、代わりに文字ベースのインターフェースを使用してください。たとえば、iSeries ナビゲーターが実行する前に基本 TCP/IP 構成を必要とする PC から iSeries ナビゲーターを使用する場合には、文字ベースのインターフェースを使用して基本構成を実行する必要があります。

このセクションで説明されている構成手順を実行するには、ユーザー・プロファイルで *IOSYSCFG 特殊権限が必要です。このタイプの権限の詳細については、iSeries 機密保護解説書  のユーザー・プロファイルに関する章を参照してください。

文字ベースのインターフェースを使用して TCP/IP を構成するには、以下の手順に従ってください。

1. コマンド行に GO TCPADM と入力して「TCP/IP 管理 (TCP/IP Administration)」メニューを表示し、Enter を押します。
2. オプション 1 (TCP/IP の構成) を指定して、「TCP/IP の構成」メニュー (CFGTCP) を表示し、Enter を押します。このメニューを使用して、構成タスクを選択します。サーバーの構成を開始する前にメニューを検討するために、いくらかの時間を取ってください。

サーバー上で TCP/IP を構成するには、以下の手順を実行してください。

1. 回線記述の構成
2. インターフェースの構成
3. 経路の構成
4. ローカル・ドメインおよびホスト名の定義
5. ホスト・テーブルの定義
6. TCP/IP の開始

回線記述の構成 (イーサネット)

これらの指示は、イーサネット通信アダプターを介した TCP/IP の構成向けです。ただし、トークンリングなど、異なるタイプのアダプターを使用する場合には、アダプターに固有のコマンドについて、TCP/IP 構成および解説書の付録 A を参照してください。

回線記述を構成するには、以下の手順に従ってください。

1. コマンド行に CRTLINETH と入力して「回線記述の作成 (イーサネット) (Create Line Desc (Ethernet)) (CRTLINETH)」メニューにアクセスし、Enter を押します。
2. 回線名を指定し、Enter を押します。(任意の名前を使用します。)
3. リソース名を指定し、Enter を押します。

次にすること:

1. インターフェースの構成

インターフェースの構成

インターフェースを構成するには、以下の手順に従ってください。

1. コマンド行に CFGTCP と入力して、「TCP/IP の構成」メニューにアクセスし、Enter を押します。
2. 「TCP/IP の構成」メニューでオプション 1 (TCP/IP インターフェースの処理) を選択し、Enter を押します。
3. オプション 1 (追加) を指定して「TCP/IP インターフェースの追加 (Add TCP/IP Interface)」画面を表示し、Enter を押します。
4. 事前定義された iSeries サーバー、サブネット・マスク・アドレス、および回線記述名を表すアドレス値を指定し、Enter を押します。

インターフェースを開始するには、構成したインターフェースにオプション 9 (開始) を指定し、Enter を押します。

次にすること:

経路の構成

経路の構成

リモート・ネットワークに接続するには、少なくとも 1 つの経路指定項目が必要です。経路指定項目が手動で追加されない場合、サーバーは、サーバーが接続されているのと同じネットワーク上にないシステムには接続できません。また、リモート・ネットワークからご使用のサーバーへの接続を試みる TCP/IP クライアントが、正しく機能できるようにするための経路指定項目も追加する必要があります。

少なくとも必ず 1 つのデフォルトの経路指定項目 (*DFTRROUTE) があるように、経路指定テーブルの定義を計画する必要があります。経路指定テーブル内のその他の項目に一致項目がない場合には、使用可能な最初のデフォルトの経路指定項目で指定された IP ルーターにデータが送信されます。

デフォルトの経路を構成するには、以下の手順に従ってください。

1. 「TCP/IP の構成」メニューでオプション 2 (TCP/IP 経路の処理) を選択し、Enter を押します。
2. オプション 1 (追加) を指定して「TCP/IP 経路の追加 (Add TCP/IP Route) (ADDTCPRTE)」に進み、Enter を押します。
3. 経路宛先に *DFTRROUTE、サブネット・マスクに *NONE、ネクスト・ホップに IP アドレスを指定し、Enter を押します。

次にすること:

ローカル・ドメインおよびホスト名の定義

ローカル・ドメインおよびホスト名の定義

ローカル・ドメインおよびホスト名を定義するには、以下の手順に従ってください。

1. 「TCP/IP の構成」メニューでオプション 12 (TCP/IP ドメインの変更) を選択し、Enter を押します。
2. 選択した名前がローカル・ホスト名およびローカル・ドメイン・ネームになるように指定し、残りのパラメーターはデフォルト値のままにしておき、Enter を押します。

次にすること:

ホスト・テーブルの定義

ホスト・テーブルの定義

ホスト・テーブルを定義するには、以下の手順に従ってください。

1. 「TCP/IP の構成」メニューでオプション 10 (TCP/IP ホスト・テーブル項目の処理) を選択し、Enter を押します。
2. オプション 1 (追加) を指定して「TCP/IP ホスト・テーブル項目の追加 (Add TCP/IP Host Table Entry)」画面を表示し、Enter を押します。
3. IP アドレス、関連したローカル・ホスト名、および完全修飾ホスト名を指定し、Enter を押します。
4. 正符号 (+) を指定し、必要であれば、複数のホスト名にスペースを使用できるようにします。
5. 名前によって通信したいネットワーク上の残りのそれぞれのホストに対して上記のステップを繰り返す、それぞれに項目を追加します。

次にすること:

TCP/IP の開始

TCP/IP の開始

TCP/IP を開始しない限り、TCP/IP のサービスを利用することはできません。

TCP/IP を開始するには、コマンド行に STRTCP を入力します。

TCP/IP 始動 (STRTCP) コマンドは、TCP/IP 処理を初期化および活動化し、TCP/IP インターフェースを開始し、サーバー・ジョブを開始します。AUTOSTART *YES を持つ TCP/IP インターフェースおよびサーバーのみが、STRTCP コマンドで開始されます。

これで、サーバー上での TCP/IP の構成が完了しました。iSeries ナビゲーターを使用して、ネットワークで変更が必要な場合は構成を変更してください。経路およびインターフェースを追加するには、『iSeries ナビゲーターを使用した TCP/IP のカスタマイズ』を、ネットワークで Internet Protocol version 6 を使用するには、『IPv6 の構成』を参照してください。

IPv6 の構成

ネットワーク上で IPv6 を使用することによって、次世代インターネットの活用に備えることができます。IPv6 機能を使用するには、IPv6 専用の回線を構成することによって TCP/IP 構成を変更する必要があります。2838 または 2849 イーサネット・アダプター上の回線、あるいは構成されたチャネル回線 (仮想回線) 上の回線のいずれかを構成する必要があります。IPv6 の構成の手順については、以下のトピックをお読みください。

セットアップ要件

このトピックでは、IPv6 用のサーバーを構成する場合のハードウェアおよびソフトウェア要件をリストしています。

IPv6 構成ウィザードを使用して IPv6 を構成する

IPv6 構成ウィザードを使用した、サーバー上での IPv6 の構成に関する手順を参照してください。

セットアップ要件

これらの 2 つのタイプの IPv6 構成のうちのどちらがユーザーの状況に適しているかを判断してください。どちらのタイプを選択したらよいか分からない場合には、例として『IPv6 シナリオ』を参照してください。

ご使用のサーバー上で IPv6 を機能させるには、以下の要件を満たすようにしてください。

IPv6 用のイーサネット回線を構成する場合:

- | • OS/400 バージョン 5 リリース 2 以上
- | • iSeries Access for Windows および iSeries ナビゲーター
 - | – iSeries ナビゲーターのネットワーク・コンポーネント
- | • IPv6 専用の 2838 または 2849 イーサネット・アダプター
- | • IPv6 使用可能ルーターは、即時 LAN を超えて IPV6 トラフィックを送信する場合にのみ必要です。
- | • TCP/IP はサーバー上で実行している必要があるため、TCP/IP (IPv4 を使用) は、別の物理アダプター上で構成する必要があります。サーバーを IPv4 対応に構成していない場合は、IPv4 用の回線を構成する前に『はじめての TCP/IP の構成』を参照してください。

| 構成済みのトンネル回線 (TNLCFG64) を作成する場合:

- | • OS/400 バージョン 5 リリース 2 以上
- | • iSeries Access for Windows および iSeries ナビゲーター
 - | – iSeries ナビゲーターのネットワーク・コンポーネント
- | • TCP/IP (IPv4 を使用) は、IPv6 用のトンネル回線を構成する前にサーバー上で構成されていなければなりません。サーバーを IPv4 対応に構成していない場合は、『はじめての TCP/IP の構成』を参照してください。

| ウィザードへのアクセスの手順については、『IPv6 構成ウィザードを使用した IPv6 の構成』を参照してください。

| IPv6 構成ウィザードを使用した IPv6 の構成

| サーバー上で IPv6 を構成するには、iSeries ナビゲーター内の **IPv6 構成** ウィザードを使用して、サーバーの構成を変更しなければなりません。IPv6 は iSeries ナビゲーターからのみ構成でき、文字ベースのインターフェースからは構成できません。

| **注:** 文字ベースのインターフェースで、「回線記述の作成 (イーサネット)」CRTLINETH コマンドを使用することによって、IPv6 イーサネット回線記述を構成することができます。ただし、16 進数のマルチキャスト・グループ・アドレス 333300000001 を指定しなければなりません。次に、**IPv6 構成** ウィザードを使用して、IPv6 の構成を終了する必要があります。

| このウィザードでは、以下のものを入力する必要があります。

| **IPv6 用のイーサネット回線を構成する場合:**

| この構成によって、IPv6 ローカル・エリア・ネットワーク (LAN) を介して IPv6 パケットを送信することができます。このウィザードでは、IPv6 を構成するサーバーのハードウェア通信リソースの名前 (たとえば、CMN01) が必要です。これは現行で IPv4 用に構成されていない、2838 または 2849 のいずれかのイーサネット・アダプターでなければなりません。『IPv6 ローカル・エリア・ネットワーク (LAN) の作成』の、IPv6 用のイーサネット回線を構成する状況について示すシナリオを参照してください。

| **構成済みのトンネル回線 (TNLCFG64) を作成する場合:**

| このタイプの構成によって、IPv4 ネットワークを介して IPv6 パケットを送信することができます。このウィザードでは、ローカル・エンドポイント用の IPv4 アドレスと、トンネルと関連したローカル・インターフェース用の IPv6 アドレスが必要です。IPv6 用に構成されたトンネル回線を作成する 2 つの状況を示すシナリオについては、『IPv4 ローカル・エリア・ネットワーク (LAN) を介した IPv6 パケットの送信』および『IPv4 広域ネットワーク (WAN) を介した IPv6 パケットの送信』を参照してください。

| 「**IPv6 の構成 (IPv6 Configuration)**」ウィザードを使用するには、以下のステップに従ってください。

- | 1. iSeries ナビゲーターで、「サーバー」→「ネットワーク」→「TCP/IP 構成」の順に展開します。
- | 2. 「IPv6」を右クリックし、「IPv6 構成」を選択します。
- | 3. サーバー上で IPv6 を構成するには、ウィザードの指示に従ってください。

第 7 章 iSeries ナビゲーターを使用した TCP/IP のカスタマイズ

TCP/IP の構成後、構成のカスタマイズを行う場合があります。ネットワークが成長していくにつれて、プロパティーを変更したり、インターフェースを追加したり、ご使用のサーバーへの経路を追加したりする必要が生じることがあります。IPv6 アプリケーションを使用するために IPv6 (Internet Protocol version 6) のサーバーを構成することが必要になる場合があります。iSeries ナビゲーターのウィザードを使用すると、これらのタスクの多くを短時間で実行できます。

iSeries ナビゲーターを使用して構成をカスタマイズするための、以下のいずれかのトピックを選択してください。以下のトピックでは、iSeries ナビゲーターを使用して TCP/IP 構成を管理するための開始点を提供します。

- TCP/IP 設定の変更

- IPv6 の構成

- IPv4 インターフェースの追加

- IPv6 インターフェースの追加

- IPv4 経路の追加

- IPv6 経路の追加

TCP/IP 設定の変更

iSeries ナビゲーターを使用して、TCP/IP の設定を表示および変更することができます。たとえば、ドメイン・ネームまたはドメイン・ネーム、ネーム・サーバー、ホスト・テーブル項目、システム属性、ポートの制約事項、サーバー、あるいはクライアント接続について、プロパティーを変更することができます。一般プロパティーを変更することも、トランスポートなどの IPv4 または IPv6 のいずれかに固有のプロパティーを変更することもできます。

一般 TCP/IP プロパティーのページにアクセスするには、以下の手順に従ってください。

1. iSeries ナビゲーターで、「サーバー」→「ネットワーク」の順に選択します。
2. 「TCP/IP 構成」を右クリックし、「プロパティー」を選択して、「TCP/IP プロパティー」ダイアログをオープンします。
3. ダイアログの上部にあるタブを選択して、TCP/IP 情報を表示および編集できます。

ホスト・テーブル項目を追加および変更するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、「サーバー」→「ネットワーク」の順に選択します。
2. 「TCP/IP 構成」を右マウス・ボタン・クリックしてから、「ホスト・テーブル」を選択して、「ホスト・テーブル」ダイアログをオープンします。
3. 「ホスト・テーブル」ダイアログを使用して、ホスト・テーブル項目を追加、編集、または削除します。

IPv4 に固有のプロパティー・ページにアクセスするには、以下の手順に従ってください。

1. iSeries ナビゲーターで、「サーバー」→「ネットワーク」の順に選択します。
2. 「IPv4」を右マウス・ボタン・クリックし、「プロパティー」を選択して、「IPv4 プロパティー (IPv4 Properties)」ダイアログをオープンします。
3. ダイアログの上部にあるタブを選択して、IPv4 プロパティーの設定を表示および編集できます。

- | IPv6 に固有のプロパティ・ページにアクセスするには、以下のステップに従ってください。
- | 1. iSeries ナビゲーターで、「サーバー」→「ネットワーク」の順に選択します。
- | 2. 「IPv6」を右マウス・ボタン・クリックし、「プロパティ」を選択して、「IPv6 プロパティ (IPv6 Properties)」ダイアログをオープンします。
- | 3. ダイアログの上部にあるタブを選択して、IPv6 プロパティの設定を表示および編集できます。

| IPv6 の構成

| IPv6 に精通しておられない方は、概要を知るために、Internet Protocol version 6 (IPv6) を参照してください。

| IPv6 を構成するには、IPv6 構成ウィザードを使用して、サーバーの構成を変更しなければなりません。このウィザードを使用する前に、手順および特殊要件について、『IPv6 の構成』を参照してください。

| IPv4 インターフェースの追加

| 新規 IPv4 インターフェースを作成するには、以下の手順に従ってください。

- | 1. 「iSeries」ナビゲーターで、「サーバー」→「ネットワーク」→「TCP/IP 構成」→「IPv4」の順に選択します。
- | 2. 「インターフェース」を右マウス・ボタン・クリックし、「新規インターフェース」、「ローカル・エリア・ネットワーク」、「広域ネットワーク」、または「仮想 IP」を選択して、適切なタイプの IPv4 インターフェースを作成します。
- | 3. ウィザードの指示に従って、新規 IPv4 インターフェースを作成します。

| IPv6 インターフェースの追加

| 新規 IPv6 インターフェースを作成するには、以下の手順に従ってください。

- | 1. 「iSeries」ナビゲーターで、「サーバー」→「ネットワーク」→「TCP/IP 構成」→「IPv6」の順に選択します。
- | 2. 「インターフェース」を右クリックし、「新しいインターフェース (New Interface)」を選択します。
- | 3. ウィザードの指示に従って、新規 IPv6 インターフェースを作成します。

| IPv4 経路の追加

| 経路指定情報を変更すると、すべてただちに有効になります。

| 新規の IPv4 経路を構成するには、以下のステップに従ってください。

- | 1. 「iSeries」ナビゲーターで、「サーバー」→「ネットワーク」→「TCP/IP 構成」→「IPv4」の順に選択します。
- | 2. 「経路」を右マウス・ボタン・クリックし、「新規経路」を選択します。
- | 3. ウィザードの指示に従って、新規 IPv4 経路を構成します。

| IPv6 経路の追加

| 経路指定情報を変更すると、すべてただちに有効になります。

| 新規の IPv6 経路を構成するには、以下の手順に従ってください。

- | 1. 「iSeries」ナビゲーターで、「サーバー」→「ネットワーク」→「TCP/IP 構成」→「IPv6」の順に選択します。

- 1 2. 「経路」を右マウス・ボタン・クリックし、「新規経路」を選択します。
- 1 3. ウィザードの指示に従って、新規 IPv6 経路を構成します。



第 8 章 IPv6 のトラブルシューティング

- | サーバー上に IPv6 が構成されている場合、IPv4 の場合と同じく、いくつかのトラブルシューティング・
 - | ツールを使用することができます。たとえば、トレース経路などのツールおよび PING は、IPv4 および
 - | IPv6 アドレス・フォーマットの両方を受け入れるので、両方のタイプのネットワークの接続および経路を
 - | テストするためにそれらを使用することができます。さらに、通信トレース機能を使用して、IPv4 と
 - | IPv6 の両方の通信回線上的のデータをトレースすることができます。
- | IPv4 および IPv6 に関連した問題を解決するための技法を提供する一般的なトラブルシューティングの手
- | 引きについては、TCP/IP トラブルシューティングを参照してください。



第 9 章 TCP/IP のセットアップに関する関連情報

ここまででご使用のサーバーの稼働ができたので、次は、「サーバーで何ができるだろうか」と考えることでしょう。下記のリストは、TCP/IP のセットアップのトピックに関連のあるマニュアル、IBM Redbooks™ (PDF 形式)、および Information Center のトピックです。PDF を表示または印刷することができます。以下の参照情報を参考にして、iSeries サーバー 上の TCP/IP を最大限に利用してください。




マニュアル

- **TCP/IP 構成および解説**  (約 100 ページ)
この資料には、伝送制御プロトコル / インターネット・プロトコル (TCP/IP) の構成、ネットワークの操作および管理に関する情報が記載されています。
- **iSeries セキュリティーの手引き**  (約 254 ページ)
この資料には、iSeries のセキュリティー機能を使用して、サーバーおよびそれと関連した操作を保護するための基本的な推奨事項が記載されています。

Redbooks

- **TCP/IP Tutorial and Technical Overview** 
この Redbook には、TCP/IP の基本に関する情報が記載されています。
- **TCP/IP for AS/400: More Cool Things Than Ever** 
この Redbook には、よく使われる TCP/IP アプリケーションおよびサービスについての広範なリストが記載されています。

IPv6

- **The Internet Engineering Task Force (IETF)** (<http://www.ietf.cnri.reston.va.us/>) 
IPv6 を含め、インターネット・プロトコルを開発している個々のグループについて説明しています。
- **IP Version 6 (IPv6)** (<http://playground.sun.com/pub/ipng/html/ipng-main.html>) 
現在の IPv6 仕様の説明と IPv6 のいくつかのソースへの参照があります。
- **IPv6 Forum**(<http://www.ipv6forum.com/>) 
最新の IPv6 開発を伝えるニュース記事やイベントがあります。

その他の情報

- **TCP/IP**
このトピックには、構成という範囲を超えた TCP/IP アプリケーションおよびサービスについての情報があります。

表示用または印刷用の PDF ファイルを Netscape Navigator からワークステーションに保存するには、次のようになります。

1. ブラウザーで PDF を開く (上記のリンクをクリックする)。
2. ブラウザーのメニューから「ファイル」をクリックする。
3. 「名前を付けて保存」をクリックする。(IE の場合は、フロッピーディスクのアイコン (名前を付けて保存) をクリックする。)

4. PDF を保存したいディレクトリーに進む。
5. 「保存」をクリックする。

上記の PDF を表示または印刷するために Adobe Acrobat Reader が必要であれば、Adobe Web サイト (www.adobe.com/prodindex/acrobat/readstep.html)  からコピーをダウンロードすることができます。



Printed in Japan