IBM i

バージョン 7.2

ネットワーキング
リモート・アクセス・サービス

IBM i

バージョン 7.2

ネットワーキング
リモート・アクセス・サービス

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、 83 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。

本製品およびオプションに付属の電源コードは、他の電気機器で使用しないでください。

本書にはライセンス内部コードについての参照が含まれている場合があります。ライセンス内部コードは機械コードであり、IBM 機械コードのご使用条件に基づいて使用権を許諾するものです。

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

原典： IBM i
Version 7.2
Networking
Remote Access Services

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 2014.4

目次

リモート・アクセス・サービス

Point-to-Point Protocol (PPP) は、シリアル回線でデータを送信する際のインターネット標準です。

PPP は、インターネット・サービス・プロバイダー (ISP) の間で最も広く利用されている接続プロトコルです。 PPP を使用すると、個々のコンピューターからネットワークにアクセスできます。続いてそのネットワークがインターネットへのアクセスを提供します。 IBM® i 製品には、その広域ネットワーク (WAN) 接続の一部として TCP/IP PPP サポートが含まれています。

ロケーション間でデータの交換を行うには、PPP を使用して、IBM i プラットフォームとリモート・コンピューターを接続します。システムに接続されたリモート・システムは、PPP を介して、システムと同じネットワークに属するリソースや他のマシンにアクセスできます。システムを、PPP を使用してインターネットに接続するよう構成することもできます。 IBM Navigator for i のダイヤルアップ接続ウィザードは、システムをインターネットまたは社内ネットワークに接続するプロセスのガイドとなります。

IBM i 7.2 の新機能

リモート・アクセス・サービス: PPP 接続のトピックの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お読みください。

IBM Navigator for i を使用して、外付けのイーサネット装置サーバーの PPP 接続プロファイルを構成する方法を示すために、新しいシナリオである『イーサネット装置サーバーとのダイヤルアップ接続の確立』を追加しました。

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 (|) 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。

リモート・アクセス・サービスの 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 版を表示あるいはダウンロードするには、「リモート・アクセス・サービス」を選択します。

PDF ファイルの保存

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

1. ご使用のブラウザーで 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:

81 ページの『リモート・アクセス・サービスの関連情報』
IBM Redbooks® の資料および Web サイトには、リモート・アクセス・サービスのトピック・コレクション関連の情報が含まれています。以下の PDF ファイルは、どれも表示または印刷することができます。

PPP の概念

IBM i プラットフォームをリモート・ネットワーク、クライアント PC、別の IBM i プラットフォーム、またはインターネット・サービス・プロバイダー (ISP) に接続するには、PPP を使用できます。このプロトコルを十分に使用するには、このプロトコルの機能および IBM i の両方を理解しなければなりません。

関連資料:

81 ページの『リモート・アクセス・サービスの関連情報』
IBM Redbooks の資料および Web サイトには、リモート・アクセス・サービスのトピック・コレクション関連の情報が含まれています。以下の PDF ファイルは、どれも表示または印刷することができます。

PPP とは

Point-to-Point Protocol (PPP) は、 1 つのコンピューターから別のコンピューターに接続するのに使用される TCP/IP プロトコルです。コンピューターは、PPP を使用し、電話網またはインターネット上で通信します。

PPP 接続は、2 つのシステムが電話回線を通して物理的に接続したときに存在することになります。 1 つのシステムを他のシステムに接続するには、PPP を使用することができます。例えば、支社と本社の間に PPP 接続が確立されると、これらのオフィスはどちらも、ネットワークを介してもう一方のオフィスにデータを転送できるようになります。

PPP は、メーカーの異なるリモート・アクセス・ソフトウェア間の相互運用を可能にしています。 PPP ではまた、複数のネットワーク通信プロトコルが同じ物理通信回線を使用することもできます。

PPP プロトコルについては、以下の Request for Comment (RFC) 標準が記述しています。 RFC についての詳細は、RFC Editor の Web ページ にあります。

- RFC-1661 Point-to-Point Protocol
- RFC-1662 PPP on HDLC-like framing
- RFC-1994 PPP CHAP
- RFC-5072 IP Version 6 over PPP

接続プロファイル

Point-to-Point 接続プロファイルは、特定の Point-to-Point Protocol (PPP) 接続のパラメーターおよびリソースのセットを定義します。これらのパラメーターを使用するプロファイルを開始すると、ダイヤルアウト (発信) または PPP 接続の listen (受信) ができます。

PPP 接続または接続のセットについて、一連の特性を定義するために、以下の 2 つのタイプのプロファイルを使用できます。

- *発信元接続プロファイル*は、ローカル・システムから発信されて、リモート・システムによって受信される 2 地点間接続です。アウトバウンド接続は、このオブジェクトを使用して構成することができます。
- *受信側接続プロファイル*は、リモート・システムから発信されて、ローカル・システムによって受信される 2 地点間接続です。インバウンド接続は、このオブジェクトを使用して構成することができます。

接続プロファイルは、PPP 接続の動作方法を定義しています。接続プロファイル内の情報には、以下の質問の答えがあります。

- 接続で使用する接続プロトコルのタイプは何ですか? (PPP またはシリアル・ライン・インターネット・プロトコル (SLIP))
- システムは、ダイヤルアウトによってその他のコンピューターと接触しますか (発信元ですか)。それとも、他のシステムからの呼び出しを受信待機しますか (受信側ですか)。
- 接続ではどの通信回線を使用しますか。
- システムはどのように、使用する IP アドレスを決定しますか。
- システムはどのように他のシステムを認証しますか。システムはどこに認証情報を保管しますか。

接続プロファイルは、以下の詳細事項を論理的に表したものです。

- 回線およびプロファイル・タイプ
- 多重リンク設定
- リモート電話番号およびダイヤル・オプション
- 認証
- TCP/IP 設定: IP アドレスおよびルーティング、および IP フィルター
- 実行管理機能および接続カスタマイズ
- ドメイン・ネーム・サーバー

システムは、接続プロファイル内にこれらの構成情報を保管します。システムが他のシステムとの PPP 接続を確立するのに必要なコンテキストを示しています。接続プロファイルには、次の情報が含まれます。

- **プロトコル・タイプ**。 PPP か SLIP を選択することができます。 IBM は、可能な限り PPP を使用するよう推奨します。
- **モード選択**。モード選択は、この接続プロファイルの接続タイプと動作モードを指定します。

  接続タイプ。これは、接続で使用する回線のタイプと、それらがダイヤル (発信元) なのか、もしくは応答 (受信側) なのかを指定します。以下の接続タイプの中から選択することができます。
  - 交換回線
  - 専用 (占有) 回線
  - レイヤー 2 トンネリング・プロトコル (L2TP) (仮想回線)
  - Point-to-Point Protocol over Ethernet (PPPoE) (仮想回線)

PPPoE は、発信元接続プロファイルにのみサポートされています。

- **動作モード**。使用可能な動作モードは、接続のタイプにより異なります。

表 1. 発信元接続プロファイルに使用できる動作モード

接続タイプ	使用できる動作モード
交換回線	• ダイヤル • ダイヤル・オンデマンド (ダイヤルのみ) • ダイヤル・オンデマンド (応答可能な専用ピア) • ダイヤル・オンデマンド (リモート・ピア使用可能)
専用回線	起動側
L2TP	• 起動側 • マルチホップ起動側 • リモート・ダイヤル
PPP over Ethernet	起動側

表 2. 受信元接続プロファイルに使用できる動作モード

接続タイプ	使用できる動作モード
交換回線	応答
専用回線	終端側
L2TP	終端側 (ネットワーク・サーバー)

- **リンク構成**。これは、この接続で使用する回線サービスのタイプを指定します。

  この選択肢は、選択するモード選択のタイプによって異なります。交換回線と専用回線には、以下のいずれかを選択することができます。

  – 単一回線
  – 回線プール

  他のすべての接続タイプ (L2TP、PPPoE) については、回線サービス選択は、単一回線だけです。

関連資料:

45 ページの『ソフトウェアおよびハードウェア要件』
Point-to-Point Protocol (PPP) 環境には、PPP をサポートする 2 つ以上のコンピューターが必要です。それらコンピューターの 1 つである IBM i プラットフォームは、発信元と受信側のいずれにもなります。

グループ・ポリシー・サポート

グループ・ポリシーのサポートにより、ネットワーク管理者はリソースを管理するためのユーザー・ベースのグループ・ポリシーを定義できます。ユーザーが Point-to-Point Protocol (PPP) またはレイヤー 2 トンネリング・プロトコル (L2TP) セッションにログオンする際に、個々のユーザーにアクセス制御ポリシーを割り当てることができます。

ユーザーは、特定の 1 つのユーザー・クラスに所属するものとして認識することができます。各クラスにはそれぞれ固有のポリシーがあり、それによってリソース制限 (多重リンク・バンドルに含めることのできるリンク数など)、属性 (IP 転送など)、および適用する IP パケット・フィルター規則のセットの識別が定

義されます。例えば、グループ・ポリシーのサポートにより、ネットワーク管理者は、ネットワークへのフル・アクセスを許可する Work_at_Home グループや、一連のサービスだけに制限される Vendor_Workers グループを定義することができます。

関連資料:

19 ページの『シナリオ: システムを PPPoE アクセス・コンセントレーターに接続する』
多くのインターネット・サービス・プロバイダー (ISP) が、Point-to-Point Protocol over Ethernet (PPPoE) を使用してデジタル加入者回線 (DSL) 上での高速インターネット・アクセスを提供しています。システムをそれらの ISP に接続することにより、Point-to-Point Protocol (PPP) のメリットを保ったまま、高帯域幅の接続が提供されます。

34 ページの『シナリオ: グループ・ポリシーおよび IP フィルターを使用してリソースへのリモート・ユーザー・アクセスを管理する』
グループ・アクセス・ポリシーによって、接続のためのそれぞれのユーザー・グループを識別し、共通の接続属性およびセキュリティー設定をグループ全体に適用することができます。グループ・ポリシーと IP フィルター操作とを組み合わせて使用することにより、ネットワーク上の特定の IP アドレスへのアクセスを、許可したり制限したりすることができます。

シナリオ: PPP 接続を使用したリモート・アクセス

以下のシナリオは、Point-to-Point Protocol (PPP) の動作、またネットワーク内に PPP 環境を実装する方法を示すものです。また、シナリオは、PPP の基本的な概念を紹介するものでもあり、初心者であれ、熟達したユーザーであれ、タスクの計画と構成の前にここを参照するのは有益でしょう。

関連資料:

81 ページの『リモート・アクセス・サービスの関連情報』
IBM Redbooks の資料および Web サイトには、リモート・アクセス・サービスのトピック・コレクション関連の情報が含まれています。以下の PDF ファイルは、どれも表示または印刷することができます。

シナリオ: 単一の IBM i 上の PPP と DHCP

このシナリオでは、IBM i モデルを、LAN とリモート・ダイヤルイン・クライアント用の動的ホスト構成プロトコル (DHCP) サーバーとして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、しばしば、会社のネットワークにアクセスすることが必要になります。ダイヤルイン・クライアントは、Point-to-Point Protocol (PPP) を使用して IBM i モデルにアクセスできます。ネットワークにアクセスするためには、ダイヤルイン・クライアントには、直接接続のネットワーク・クライアントと全く同じように、IP 情報が必要です。 IBM i DHCP サーバーは、他の直接接続クライアントの場合と同様に PPP ダイヤルイン・クライアントに IP アドレス情報を配布することができます。次の図は、仕事をするために会社のネットワークにダイヤルして入る必要のあるリモートのクライアントを示しています。

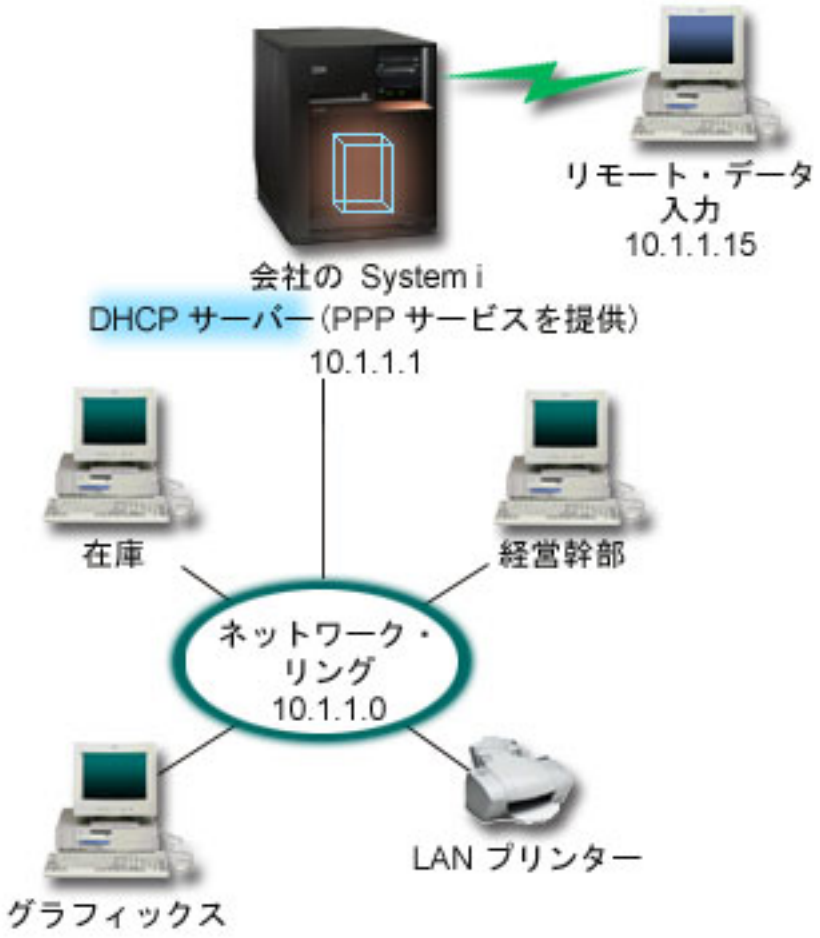


図 1. 単一の IBM i モデルにある PPP と DHCP

リモートの従業員が正常に会社のネットワークに加わるために、IBM i モデルは、リモート・アクセス・サービスと DHCP の組み合わせを使用する必要があります。リモート・アクセス・サービスの機能は、IBM i モデルのためにダイヤルイン機能を作成します。適切にセットアップされると、クライアントがダイヤルイン接続を確立した後、PPP サーバーは、DHCP サーバーに対して、そのリモート・クライアントに TCP/IP 情報を配布するように伝えます。

このシナリオでは、1 つの DHCP サブネット・ポリシーが、オンサイトのネットワーク・クライアントとダイヤルイン・クライアントの両方を対象としています。

IP 配布に関して PPP プロファイルで DHCP が使われるようにする場合、 PPP プロファイル内でそのようにしなければなりません。受信側接続プロファイルの TCP/IP 設定では、リモート IP アドレスの割り当て方式を「固定」から「DHCP」に設定します。ダイヤルイン・クライアントが、 LAN プリンターなどの他のネットワーク・クライアントと通信できるようにするため、プロファイルの TCP/IP 設定と TCP/IP 構成 (スタック) のプロパティーで、IP 転送を許可することも必要です。 PPP プロファイルの中だけで IP 転送を設定しても、IBM i モデルは IP パケットの受け渡しを行いません。プロファイルとスタックの両方に IP 転送を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 アドレスは、DHCP サーバーのサブネット定義内に入る IP アドレスでなければなりません。このシナリオでは、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 となっている必要があります。また、このアドレスは、DHCP クライアントに割り当てられることのないように、DHCP サーバーのアドレス・プールからは除外されている必要があります。

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 3. グローバル構成オプション (DHCP サーバーによる処理を受けるすべてのクライアントに適用)

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 更新を実行するか		いいえ
システムは、BOOTP クライアントをサポートするか		いいえ

表 4. オンサイト・クライアントとダイヤルイン・クライアントの両方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
リース期間		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
サーバーによって割り当てられたのではないサブネット・アドレス		10.1.1.1 (IBM Navigator for i の「受信先接続プロファイル」のプロパティーの「TCP/IP IPv4 設定」に指定されているローカル・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 に設定します。
  1. IBM Navigator for i のリモート・アクセス・サービス用の「**サービス**」タスクを使用して、DHCP サーバーまたはリレー接続による DHCP WAN クライアント接続を使用可能にします。
  2. IBM Navigator for i の「受信先接続プロファイル」の「TCP/IP IPv4 プロパティー (TCP/IP IPv4 Properties)」の下で、IP アドレス割り当て方式として「DHCP」を選択します。
- IBM Navigator for i の「受信先接続プロファイル」の「TCP/IP IPv4 プロパティー (TCP/IP IPv4 Properties)」の下で、リモート・システムによるその他のネットワークへのアクセス (IP 転送) を許可します。
- IBM Navigator for i の「TCP/IP 属性」の下で IP データグラムの転送を使用可能にします。

シナリオ: 異なる IBM i モデル上の DHCP プロファイルと PPP プロファイル

このシナリオでは、2 つの IBM i モデルを、2 つの LAN とリモート・ダイヤルイン・クライアント用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セットアップする方法について説明します。

単一の IBM i モデル上の PPP と DHCP についてのシナリオは、単一のシステム上で PPP と DHCP を使用することにより、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示し

ています。ネットワークの物理的なレイアウトのため、あるいはセキュリティー上の問題のために、PPP と DHCP のサーバーを別個に用意するか、または DHCP サービスのない専用 PPP サーバーを用意するほうが望ましい場合があるかもしれません。次の図は、ダイヤルイン・クライアントがあるが、PPP と DHCP のポリシーが複数の異なるサーバーにあるネットワークを表しています。

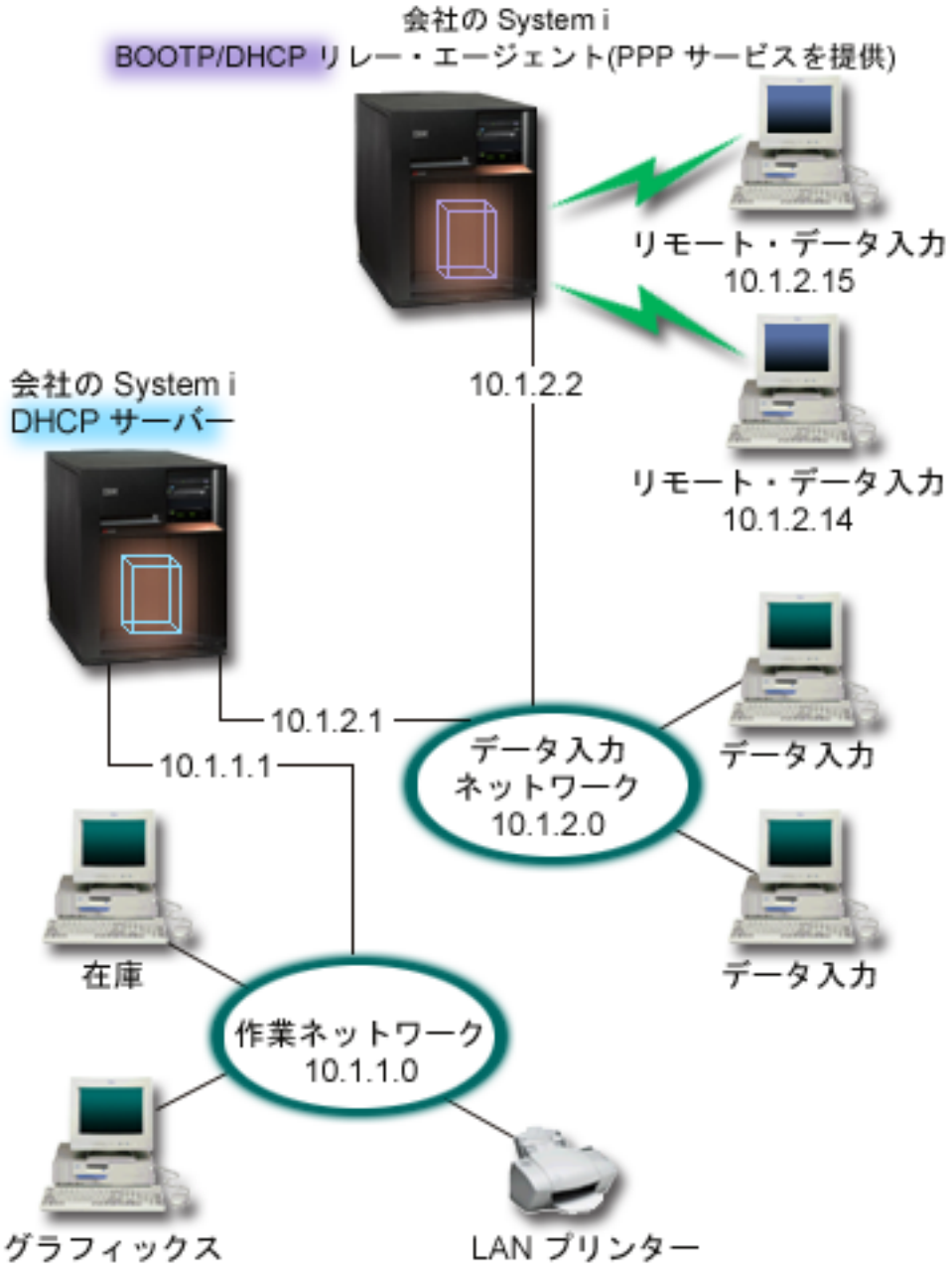


図 2. 異なる IBM i モデル上の DHCP および PPP プロファイル

リモート・データ入力クライアントは、IBM i PPP サーバーにダイヤルします。そのサーバー上の PPP プロファイルは、単一の IBM i モデル上の PPP と DHCP のシナリオで使用されているような DHCP のリモート IP アドレス方式でなければなりません。 PPP プロファイルと、PPP プロファイル上の TCP/IP 設定には IP 転送が必要です。さらに、このサーバーは DHCP リレー・エージェントとして働くので、BOOTP/DHCP リレー・エージェントもオンになっている必要があります。これによって、IBM i リモー

ト・アクセス・サーバーは、DHCPDISCOVER パケットを DHCP サーバーに受け渡すことができます。そして、DHCP サーバーが応答し、 PPP サーバーを介してダイヤルイン・クライアントに TCP/IP 情報を配布します。

DHCP サーバーは、10.1.1.0 と 10.1.2.0 の両方のネットワークへの IP アドレスの配布に責任を持ちます。データ入力ネットワークにおいて DHCP サーバーは、ダイヤルインまたは直接接続のネットワーク・クライアントに 10.1.2.10 から 10.1.2.40 までの範囲の IP アドレスを割り当てます。データ入力クライアントは、また、作業ネットワークと通信するために 10.1.2.1 のルーター・アドレス (オプション 3) を必要とし、IBM i DHCP サーバーでは IP 転送が使用可能になっている必要があります。

また、PPP プロファイル内のローカル・インターフェース IP アドレスは、DHCP サーバーのサブネット定義内に入る IP アドレスでなければなりません。このシナリオでは、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 となっている必要があります。また、このアドレスは、DHCP クライアントに割り当てられることのないように、DHCP サーバーのアドレス・プールからは除外されている必要があります。ローカル・インターフェース 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・エージェントによる DHCP 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 サーバーによる処理を受けるすべてのクライアントに適用)

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 更新を実行するか		いいえ
システムは、BOOTP クライアントをサポートするか		いいえ

表 6. 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
リース期間		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
サーバーによって割り当てられたのではないサブネット・アドレス		なし

表 7. 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
リース期間	24 時間 (デフォルト)

表 7. 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
サーバーによって割り当てられたの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 IBM i プラットフォーム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します。

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 アドレスへのリレー・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 に設定します。
  1. IBM Navigator for i のリモート・アクセス・サービス用の「サービス」タスクを使用して、DHCP サーバーまたはリレー接続による DHCP WAN クライアント接続を使用可能にします。
  2. IBM Navigator for i の「受信先接続プロファイル」の「TCP/IP IPv4 設定プロパティー (TCP/IP IPv4 Settings Properties)」の下で、IP アドレス割り当て方式として「DHCP の使用 (Use DHCP)」を選択します。
- IBM Navigator for i の「受信先接続プロファイル」の「TCP/IP IPv4 設定プロパティー (TCP/IP IPv4 Settings Properties)」の下で、リモート・システムによるその他のネットワークへのアクセス (IP 転送) を許可します (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ため)。
- IBM Navigator for i の「TCP/IP 属性」の下で IP データグラム転送を使用可能にします (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ため)。

シナリオ: L2TP 任意トンネルを IPSec で保護する

このシナリオでは、営業所のホストと、IPSec で保護されている L2TP を使用する本社オフィスとの間の接続をどのようにセットアップするかを学びます。営業所は動的に割り当てられた IP アドレスを持ち、一方、本社オフィスの IP アドレスは静的でグローバルにルーティング可能なものです。

状況

ここでは、別の州に小さな営業所が 1 つあるとします。営業所は、平日はいつでも、会社のイントラネット内の IBM i モデルについての機密情報にアクセスする必要があります。現在は、営業所に本社ネットワークへのアクセスを提供するため、高価な専用回線を使用しています。イントラネットへのアクセスの保護は従来どおり提供したいのですが、最終的には、専用回線に関係する出費を削減したいと考えています。これは、本社ネットワークを拡張する Layer 2 Tunnel Protocol (L2TP) の任意トンネルを作成することによって行えます。これによって、営業所は、本社のサブネットの一部であるかのようになります。 VPN は、L2TP トンネルを介したデータ・トラフィックを保護します。

リモートの営業所は、L2TP 任意トンネルによって、本社ネットワークの L2TP ネットワーク・サーバー (LNS) に直接トンネルを確立します。 L2TP アクセス・コンセントレーター (LAC) の機能は、クライアント側にあります。トンネルは、リモート・クライアントのインターネット・サービス・プロバイダー (ISP)

には透過であり、したがって、ISP は L2TP をサポートする必要がありません。 L2TP の概念についての詳細は、「Layer 2 Tunnel Protocol (L2TP)」を参照してください。

重要: このシナリオでは、インターネットに直接接続されているセキュリティー・ゲートウェイを示します。シナリオを簡単にするために、ファイアウォールは故意に落としてあります。これは、ファイアウォールが必要ではないことを示唆しているわけではありません。インターネットに接続するときは、常に、関連するセキュリティー上のリスクを考慮してください。

目標

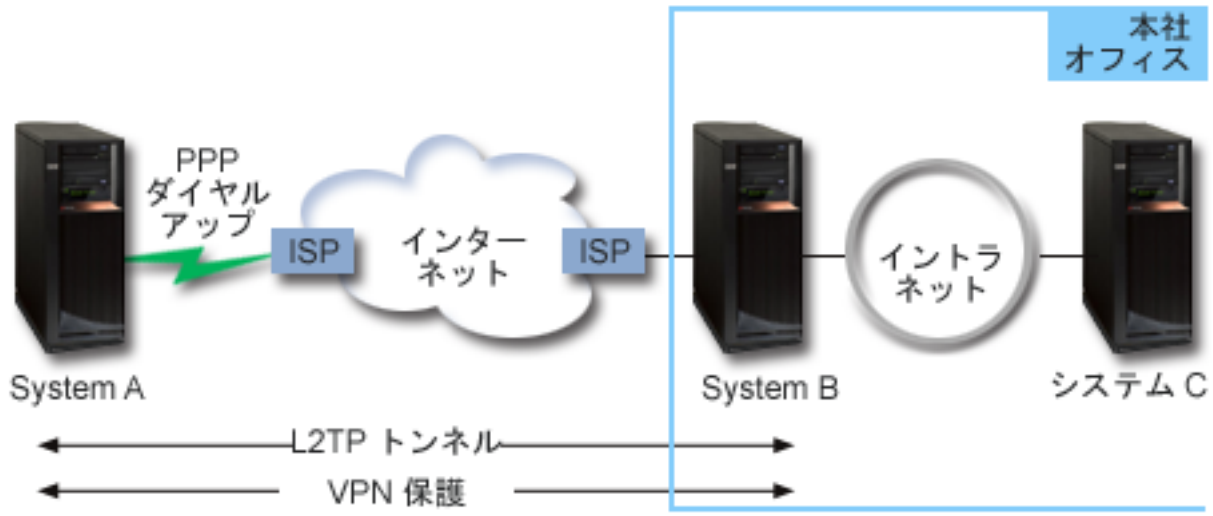
このシナリオでは、営業所のシステムは、VPN で保護された L2TP トンネルを持つゲートウェイ・システムを介して本社のネットワークに接続されます。

このシナリオの主な目標は、以下のとおりです。

- 営業所のシステムが、常に、本社オフィスへの接続を開始します。
- この営業所のシステムは、本社ネットワークへのアクセスを必要とするこの営業所ネットワーク内の唯一のシステムです。すなわち、この営業所のシステムは、営業所のネットワーク内でゲートウェイとしてではなく、ホストの役割を果たします。
- 本社システムは、本社オフィスのネットワークのホスト・コンピューターです。

詳細

以下の図は、このシナリオのネットワーク特性を示しています。



System A

- 本社ネットワーク内のすべてのシステムにある TCP/IP アプリケーションへのアクセス権が必要です。
- その ISP から動的に割り当てられる IP アドレスを受け取ります。
- L2TP サポートを提供するように構成されている必要があります。

System B

- System A 上の TCP/IP アプリケーションへのアクセス権が必要です。

- サブネットは、マスクが 255.255.0.0 の 10.6.0.0 です。このサブネットは、本社設置場所の VPN トンネルのデータ・エンドポイントを表します。
- IP アドレス 205.13.237.6 でインターネットに接続します。これは接続のエンドポイントです。すなわち、System B は、キー管理を実行し、着信と発信の IP データグラムに IPSec を適用します。 System B は、IP アドレス 10.6.11.1 でそのサブネットに接続します。

L2TP の観点からは、*System A* は L2TP 起動側として、一方 *System B* は L2TP 終端側として動作します。

構成タスク

TCP/IP 構成がすでに存在し、機能していれば、以下のタスクを完了する必要があります。

シナリオ: L2TP 任意トンネルを IPSec で保護する

このシナリオでは、営業所のホストと、IPSec で保護されている L2TP を使用する本社オフィスとの間の接続をどのようにセットアップするかを学びます。営業所は動的に割り当てられた IP アドレスを持ち、一方、本社オフィスの IP アドレスは静的でグローバルにルーティング可能なものです。

状況

ここでは、別の州に小さな営業所が 1 つあるとします。営業所は、平日はいつでも、会社のイントラネット内の IBM i モデルについての機密情報にアクセスする必要があります。現在は、営業所に本社ネットワークへのアクセスを提供するため、高価な専用回線を使用しています。イントラネットへのアクセスの保護は従来どおり提供したいのですが、最終的には、専用回線に関係する出費を削減したいと考えています。これは、本社ネットワークを拡張する Layer 2 Tunnel Protocol (L2TP) の任意トンネルを作成することによって行えます。これによって、営業所は、本社のサブネットの一部であるかのようになります。 VPN は、L2TP トンネルを介したデータ・トラフィックを保護します。

リモートの営業所は、L2TP 任意トンネルによって、本社ネットワークの L2TP ネットワーク・サーバー (LNS) に直接トンネルを確立します。 L2TP アクセス・コンセントレーター (LAC) の機能は、クライアント側にあります。トンネルは、リモート・クライアントのインターネット・サービス・プロバイダー (ISP) には透過であり、したがって、ISP は L2TP をサポートする必要がありません。 L2TP の概念についての詳細は、「Layer 2 Tunnel Protocol (L2TP)」を参照してください。

重要: このシナリオでは、インターネットに直接接続されているセキュリティー・ゲートウェイを示します。シナリオを簡単にするために、ファイアウォールは故意に落としてあります。これは、ファイアウォールが必要ではないことを示唆しているわけではありません。インターネットに接続するときは、常に、関連するセキュリティー上のリスクを考慮してください。

目標

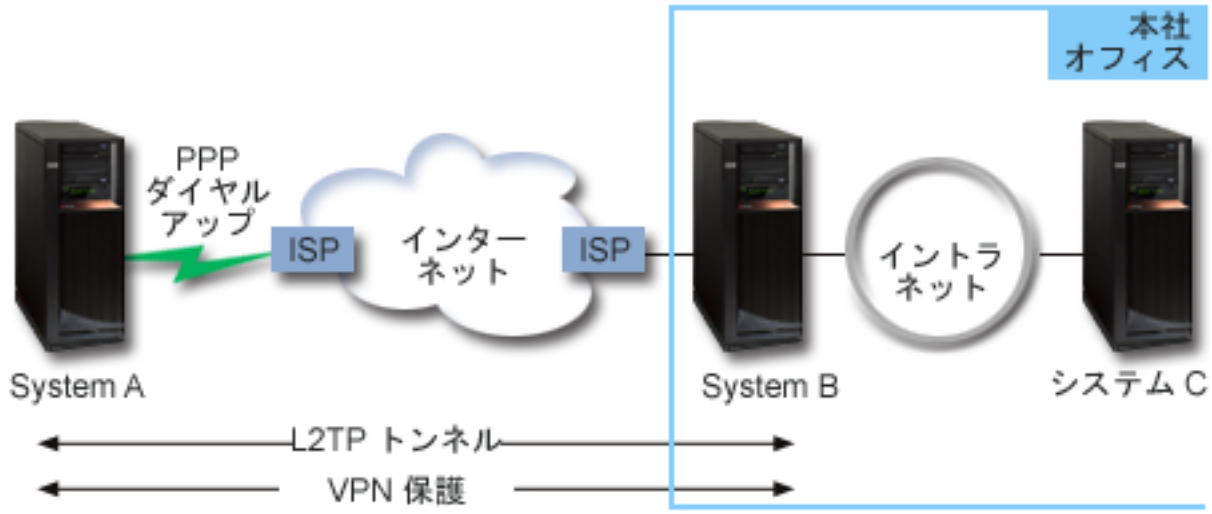
このシナリオでは、営業所のシステムは、VPN で保護された L2TP トンネルを持つゲートウェイ・システムを介して本社のネットワークに接続されます。

このシナリオの主な目標は、以下のとおりです。

- 営業所のシステムが、常に、本社オフィスへの接続を開始します。
- この営業所のシステムは、本社ネットワークへのアクセスを必要とするこの営業所ネットワーク内の唯一のシステムです。すなわち、この営業所のシステムは、営業所のネットワーク内でゲートウェイとしてではなく、ホストの役割を果たします。
- 本社システムは、本社オフィスのネットワークのホスト・コンピューターです。

詳細

以下の図は、このシナリオのネットワーク特性を示しています。



System A

- 本社ネットワーク内のすべてのシステムにある TCP/IP アプリケーションへのアクセス権が必要です。
- その ISP から動的に割り当てられる IP アドレスを受け取ります。
- L2TP サポートを提供するように構成されている必要があります。

System B

- System A 上の TCP/IP アプリケーションへのアクセス権が必要です。
- サブネットは、マスクが 255.255.0.0 の 10.6.0.0 です。このサブネットは、本社設置場所の VPN トンネルのデータ・エンドポイントを表します。
- IP アドレス 205.13.237.6 でインターネットに接続します。これは接続のエンドポイントです。すなわち、System B は、キー管理を実行し、着信と発信の IP データグラムに IPSec を適用します。 System B は、IP アドレス 10.6.11.1 でそのサブネットに接続します。

L2TP の観点からは、*System A* は L2TP 起動側として、一方 *System B* は L2TP 終端側として動作します。

構成タスク

TCP/IP 構成がすでに存在し、機能していれば、以下のタスクを完了する必要があります。

System A での VPN の構成

System A で VPN 接続を構成するには、以下のステップに従ってください。

計画ワークシートの内容を使用して、以下の手順で System A に VPN を構成してください。

1. **Internet Key Exchange ポリシーを構成する**
   a. IBM Navigator for i で、**「ネットワーク」** > **「IP ポリシー」** > **「仮想プライベート・ネットワーキング」**を展開します。

b. 「**IP セキュリティー・ポリシー**」をクリックして、「**IP セキュリティー・ポリシー**」パネルを開きます。

c. 「**Internet Key Exchange ポリシー**」を右クリックして、「**新規 Internet Key Exchange ポリシー**」を選択する。

d. 「**リモート・サーバー**」のページで、「**IP バージョン 4 アドレス**」を ID のタイプとして選択した後、「**IP アドレス**」フィールドに 205.13.237.6 を入力する。

e. 「**関連**」のページで、「**事前共用キー**」を選択して、この接続では事前共用キーを使用してこのポリシーを認証することを示します。

f. 「**キー**」フィールドに事前共用キーを入力する。事前共用キーは、パスワードのように扱ってください。

g. ローカル・キー・サーバーの ID のタイプに「**キー ID**」を選択した後、「**ID**」フィールドでキー ID を入力する。 例えば、thisisthekeyid のようになります。ローカル・キー・サーバーには、事前に知ることのできない、動的に割り当てられた IP アドレスが存在することを忘れないでください。System A が接続を開始すると、System B はこの ID を使用して System A を識別します。

h. 「**変換**」のページで、「**追加**」をクリックして、キー保護のために System A が System B に提案した変換を追加し、フェーズ 1 のネゴシエーションの開始時に IKE ポリシーが一致保護を使用するかどうかを指定する。

i. 「**IKE ポリシー変換**」ページで、認証メソッドには「**事前共用キー**」を、ハッシュ・アルゴリズムおよび PRF アルゴリズムには「**SHA**」を、暗号化アルゴリズムには「**3DES-CBC**」を選択します。それから、Diffie-Hellman グループと IKE キー満了期間にはデフォルト値を受け入れます。

j. 「**OK**」をクリックして、「**変換**」ページに戻る。

k. 「**IKE アグレッシブ・モード・ネゴシエーション (一致保護なし)**」を選択する。

注: 事前共用キーとアグレッシブ・モード・ネゴシエーションを一緒に構成で使用しなければならない場合は、ディクショナリーをスキャンするアタックで解かれそうにないわかりにくいパスワードを選択してください。パスワードを定期的に変更することもお勧めします。

l. 「**OK**」をクリックして、構成を保管する。

2. **データ・ポリシーを構成する**

a. IBM Navigator for i で、「**ネットワーク**」 > 「**IP ポリシー**」 > 「**仮想プライベート・ネットワーキング**」を展開します。

b. 「**IP セキュリティー・ポリシー**」をクリックして、「**IP セキュリティー・ポリシー**」パネルを開きます。

c. 「**データ・ポリシー**」を右クリックして、「**新規データ・ポリシー**」を選択します。

d. 「**一般**」のページで、データ・ポリシーの名前を指定する。例えば、l2tpremoteuser です。

e. 「**提案**」のページに移動する。提案は、起動側および応答側のキー・サーバーが、 2 つのエンドポイント間の動的接続を確立する際に使用する、プロトコルのコレクションです。ユーザーは、複数の接続オブジェクトで、単一のデータ・ポリシーを使用することができます。ただし、すべてのリモート VPN キー・サーバーが、同じデータ・ポリシー・プロパティーを持っているとは限りません。したがって、1 つのデータ・ポリシーに、いくつかの提案を追加することができます。リモート・キー・サーバーとの VPN 接続を確立する場合は、起動側と応答側のデータ・ポリシーの提案が、少なくとも 1 つは一致していなければなりません。

f. 「**追加**」をクリックして、データ・ポリシー提案を追加する。

g. カプセル化モードに「**トランスポート**」を選択する。

h. キーの有効期限を指定します。

i. 「**変換**」タブをクリックします。

j. 「**追加**」をクリックして変換を追加します。変換によって、このデータ・ポリシーが IKE フェーズ 2 折衝中に使用するプロトコル、認証アルゴリズム、および暗号化アルゴリズムが定義されます。接続の起動側は、1 つ以上のデータ・ポリシー候補を応答側に送信します。次に応答側は、このセキュア接続を完了するためにその関連セキュリティー・ポリシーの中から一致する候補を選択します。

k. 「**OK**」をクリックして変換を保存します。

l. 「**OK**」をクリックして、新規のデータ・ポリシーを保管する。

3. **動的キー・グループを構成する**

a. VPN インターフェースの下にある「**セキュア接続**」をクリックします。

b. 「**グループ別**」を右クリックして、「**新規動的キー・グループ**」を選択する。

c. 「**一般**」のページで、グループの名前を指定する。例えば、l2tptocorp です。

d. 「**ローカルで開始された L2TP トンネルを保護する**」を選択する。

e. システムの役割には、「**システムが両方ともホストです**」を選択する。

f. 「**ポリシー**」のページに移動する。「**データ・ポリシー**」ドロップダウン・リストから、**データ・ポリシーの構成**のステップで作成したデータ・ポリシー l2tpremoteuser を選択します。

g. 「**ローカル・システムが接続を開始します**」を選択して、System B との接続を開始できるのは System A のみであることを示す。

h. 「**接続**」のページに移動する。「**このグループに次のポリシー・フィルターを生成**」を選択します。「**編集**」をクリックして、ポリシー・フィルターのパラメーターを定義します。

i. 「**ポリシー・フィルター - ローカル・アドレス**」のページで、 ID のタイプに「**キー ID**」を選択する。

j. ID には、キー ID thisisthekeyid を選択する。この ID は IKE ポリシーで定義されています。

k. 「**ポリシー・フィルター - リモート・アドレス**」のページに移動する。「**ID のタイプ**」ドロップダウン・リストから、「**IP バージョン 4 アドレス**」を選択します。

l. 「**ID**」フィールドに 205.13.237.6 と入力する。

m. 「**ポリシー・フィルター - サービス**」のページに進む。「**ローカル・ポート**」フィールドおよび「**リモート・ポート**」フィールドで、1701 を入力します。ポート 1701 は、L2TP の事前割り当てポートです。

n. 「**プロトコル**」ドロップダウン・リストから、「**UDP**」を選択する。

o. 「**OK**」をクリックして、「**接続**」のページに戻る。

p. 「**インターフェース**」のページに移動する。このグループが適用される任意の回線または PPP プロファイルを選択します。このグループにはまだ PPP プロファイルを作成していません。このプロファイルの作成後、このグループのプロパティーを編集して、次のステップで作成する PPP プロファイルにグループが適用されるようにします。

q. 「**OK**」をクリックして、動的キー・グループ l2tptocorp を作成する。

4. **動的キー接続を構成する**

a. 「**接続**」パネルから、「**グループ別**」を右クリックして「**開く**」を選択します。これで、System A 上で構成したすべての動的キー・グループのリストが表示されます。

b. 「**l2tptocorp**」を右クリックして、「**新規動的キー接続**」を選択する。

c. 「**一般**」のページで、接続のオプション記述を指定する。

d. リモート・キー・サーバーでは、ID のタイプに「**IP バージョン 4 アドレス**」を選択する。

e. 「**IP アドレス**」ドロップダウン・リストから、205.13.237.6 を選択する。

f. 「**要求時に開始**」の選択を解除する。

g. 「**ローカル・アドレス**」のページに移動する。 ID のタイプに「**キー ID**」を選択した後、「**ID**」ドロップダウン・リストから thisisthekeyid を選択します。

h. 「**リモート・アドレス**」のページに移動する。 ID のタイプに「**IP バージョン 4 アドレス**」を選択します。

i. 「**ID**」フィールドに 205.13.237.6 と入力する。

j. 「**サービス**」のページに移動する。「**ローカル・ポート**」フィールドおよび「**リモート・ポート**」フィールドで、1701 を入力します。ポート 1701 は、L2TP の事前割り当てポートです。

k. 「**プロトコル**」ドロップダウン・リストから、「**UDP**」を選択する。

l. 「**OK**」をクリックして、動的キー接続を作成する。

System A 上で PPP 接続プロファイルおよび仮想回線を構成する

System A 上で VPN 接続を構成したので、今度は System A 用の PPP プロファイルを作成する必要があります。PPP プロファイルは、それに関連した物理的回線は持っていません。代わりに、仮想回線を使用します。これは、PPP トラフィックが L2TP トンネル経由で通過するためです。これに対し、VPN は L2TP トンネルを保護します。

System A 用 PPP 接続プロファイルを作成するには、以下のステップに従ってください。

1. IBM Navigator for i で、「**ネットワーク**」 > 「**リモート・アクセス・サービス**」の順に展開します。
2. 「**発信元接続プロファイル**」を右クリックし、「**処置**」 > 「**新規プロファイル**」をクリックします。
3. 「**セットアップ**」のページで、プロトコル・タイプに「**PPP**」を選択する。
4. モード選択では、「**L2TP (仮想回線)**」を選択する。
5. 「**作動モード**」ドロップダウン・リストから、「**オンデマンド・イニシエーター (自発的トンネル)**」を選択する。
6. 「**OK**」をクリックして、「PPP プロファイルのプロパティー」のページに移動する。
7. 「**一般**」ページで、接続のタイプと宛先を識別する名前を入力する。この場合は、toCORP と入力します。指定する名前は、10 文字以下でなければなりません。
8. オプション: プロファイルの記述を指定する。
9. 「**接続**」のページに移動する。
10. 「**仮想回線名**」フィールドで、ドロップダウン・リストから **tocorp** を選択する。この回線には、関連した物理インターフェースがないことを思い出してください。仮想回線は、この PPP プロファイルのさまざまな特性、例えば最大フレーム・サイズ、認証情報、ローカル・ホスト名などを、記述します。「**L2TP 回線のプロパティー**」ダイアログ・ボックスが開きます。
11. 「**一般**」ページで、仮想回線の記述を入力する。
12. 「**認証**」ページに移動する。
13. 「**ローカル・ホスト名**」フィールドで、ローカル・キー・サーバーのホスト名 SystemA を入力する。
14. 「**OK**」をクリックして、新しい仮想回線の記述を保管し、「**接続**」のページに戻る。
15. 「**リモート・トンネル・エンドポイント IP アドレス**」フィールドに、リモート・トンネル・エンドポイント・アドレス 205.13.237.6 を入力する。
16. 「**IP-SEC 保護が必要**」を選択し、「**接続グループ名**」ドロップダウン・リストから、前のステップ 13 ページの『System A での VPN の構成』 で作成した動的キー・グループ l2tptocorp を選択する。
17. 「**TCP/IP IPv4 設定**」ページに移動します。

18. 「**ローカル IP アドレス**」セクションで、「**リモート・システムによる割り当て**」を選択する。
19. 「**リモート IP アドレス**」セクションで、「**固定 IP アドレスを使用**」を選択する。 10.6.11.1 と入力します。これは、サブネット内のリモート・システムの IP アドレスです。
20. 経路指定セクションで、「**追加の静的経路を定義**」を選択し、「**経路**」をクリックする。PPP プロファイルに経路指定情報が提供されない場合は、System A は、リモート・トンネル・エンドポイントに到達できるのみであり、10.6.0.0 サブネット上の他のシステムには到達できません。
21. 「**追加**」をクリックして、静的経路項目を追加する。
22. サブネット 10.6.0.0、およびサブネット・マスク 255.255.0.0 を入力し、すべての 10.6.*.* トラフィックを、L2TP トンネル経由で経路指定する。
23. 「**OK**」をクリックして、静的経路を追加する。
24. 「**認証**」ページに移動し、この PPP プロファイルのユーザー名とパスワードを設定する。
25. 「ローカル・システムの識別」セクションで、「**リモート・システムがこの iSeries サーバーの識別を検査することを許可します**」を選択する。
26. 「**使用する認証プロトコル**」の下で、「**暗号化パスワードが必要 (CHAP-MD5)**」を選択する。「ローカル・システムの識別」セクションで、「**リモート・システムがこの iSeries サーバーの識別を検査することを許可します**」を選択する。
27. ユーザー名 SystemA とパスワードを入力する。
28. 「**OK**」をクリックして PPP プロファイルを保管します。
29. パスワードを再入力して、パスワードを確認します。

l2tptocorp 動的キー・グループを toCorp PPP プロファイルに適用する

PPP 接続プロファイルを構成した後、ユーザーが作成した動的キー・グループ l2tptocorp に戻り、PPP プロファイルと関連付ける必要があります。

動的キー・グループを PPP プロファイルと関連付けるには、以下の手順を実行します。

1. IBM Navigator for i で、「**ネットワーク**」 > 「**IP ポリシー**」 > 「**仮想プライベート・ネットワーキング**」を展開します。
2. 「**セキュア接続**」をクリックして「**接続**」パネルを開き、「**グループ別**」を右クリックしてから「**開く**」を選択します。
3. 動的キー・グループ l2tptocorp を右クリックし、「**プロパティー**」を選択する。
4. 「**インターフェース**」のページに移動し、 16 ページの『System A 上で PPP 接続プロファイルおよび仮想回線を構成する』 で作成した PPP プロファイル toCorp に「**このグループを適用**」を選択する。
5. 「**OK**」をクリックして、l2tptocorp を PPP プロファイル toCorp を適用する。

System B での VPN の構成

System B で VPN 接続を構成するには、System A で VPN 接続を構成する際に実行したものと同じステップに従い、必要に応じて、IP アドレスと ID を変更してください。

開始する前に、以下の他の事項を考慮事項に入れてください。

- System A でローカル・キー・サーバーに指定したキー ID で、リモート・キー・サーバーを識別する (thisisthekeyid など)。
- *正確に* 同じ事前共用キーを使用する。
- 変形を、System A で構成したものと確実に一致させる。これを行わないと、接続は失敗します。

- 動的キー・グループの「一般」のページで、「**ローカルで開始された L2TP トンネルを保護する**」を指定しないでください。
- リモート・システムが接続を開始する。
- 接続が要求時に開始しなければならないことを指定する。

System B 上で PPP 接続プロファイルおよび仮想回線を構成する

System B 上で VPN 接続を構成したので、今度は System B 用の PPP プロファイルを作成する必要があります。PPP プロファイルは、それに関連した物理的回線は持っていません。代わりに、仮想回線を使用します。これは、PPP トラフィックが L2TP トンネル経由で通過するためです。これに対し、VPN は L2TP トンネルを保護します。

System B 用 PPP 接続プロファイルを作成するには、以下のステップに従ってください。

1. IBM Navigator for i で、「**ネットワーク**」 > 「**リモート・アクセス・サービス**」の順に展開します。
2. 「**受信先接続プロファイル**」をクリックして「**受信先接続プロファイル**」パネルを開き、「**処置**」 > 「**新規プロファイル**」をクリックします。
3. 「**セットアップ**」のページで、プロトコル・タイプに「**PPP**」を選択する。
4. モード選択では、「**L2TP (仮想回線)**」を選択する。
5. 「**作動モード**」ドロップダウン・リストから、「**ターミネーター (ネットワーク・サーバー)**」を選択する。
6. 「**OK**」をクリックして「PPP プロファイルのプロパティー」ページに移動する。
7. 「**一般**」ページで、接続のタイプと宛先を識別する名前を入力する。この場合は、`tobranch` と入力します。指定する名前は、10 文字以下でなければなりません。
8. オプション: プロファイルの記述を指定する。
9. 「**接続**」のページに移動する。
10. ローカル・トンネル・エンドポイントの IP アドレス 205.13.237.6 を選択する。
11. 「**仮想回線名**」フィールドで、ドロップダウン・リストから **tobranch** を選択する。この回線には、関連した物理インターフェースがないことを思い出してください。仮想回線は、この PPP プロファイルのさまざまな特性、例えば最大フレーム・サイズ、認証情報、ローカル・ホスト名などを、記述します。「**仮想回線名**」フィールドの横にある「**開く**」をクリックして、「**L2TP 回線のプロパティー**」パネルを開きます。
12. 「**一般**」ページで、仮想回線の記述を入力する。
13. 「**認証**」ページに移動する。
14. 「**ローカル・ホスト名**」フィールドで、ローカル・キー・サーバーのホスト名 `SystemB` を入力する。
15. 「**OK**」をクリックして、新しい仮想回線の記述を保管し、「**接続**」のページに戻る。
16. 「**TCP/IP 設定**」ページに移動する。
17. 「**ローカル IP アドレス**」セクションで、ローカル・システムの固定 IP アドレス 10.6.11.1 を選択する。
18. 「**リモート IP アドレス**」セクションで、アドレス割り当て方式として「**アドレス・プール**」を選択する。開始アドレスを入力した後、リモート・システムに割り当てることができるアドレスの数を指定します。
19. 「**リモート・システムが他のネットワークにアクセスすること (IP 転送) を許可**」を選択する。
20. 「**認証**」ページに移動し、この PPP プロファイルのユーザー名とパスワードを設定する。

21. 「ローカル・システムの識別」セクションで、「**リモート・システムがこの iSeries サーバーの識別を検査することを許可します**」を選択する。 これで、「**ローカル・システム識別**」ダイアログ・ボックスが開きます。
22. 「**使用する認証プロトコル**」の下で、「**暗号化パスワードが必要 (CHAP-MD5)**」を選択する。
23. ユーザー名 SystemB とパスワードを入力する。
24. 「**OK**」をクリックして PPP プロファイルを保管します。

パケット・ルールを活動化する

VPN ウィザードにより、この接続が正しく作動するために必要なパケット・ルールが自動的に作成されます。ただし、VPN 接続を開始できるようにするには、その前に、両方のシステムでこれらのパケット・ルールを活動化しなければなりません。

System A でパケット・ルールを活動化するには、以下の手順を実行します。

1. IBM Navigator for i で、「**ネットワーク**」 > 「**IP ポリシー**」を展開します。
2. 「**パケット規則**」をクリックして「**パケット規則**」パネルを開き、「**処置**」 > 「**規則の活動化**」をクリックします。この処置により、「**パケット・ルールの活動化**」パネルが開きます。
3. VPN で生成されたルールのみを活動化するのか、選択したファイルのみを活動化するのか、あるいは VPN で生成されたルールと選択したファイルの両方を活動化するのかを選択する。例えば、VPN で生成されたルールに加えて、各種の PERMIT ルールや DENY ルールをインターフェースに適用したい場合には、VPN で生成されたルールと選択したファイルの両方の活動化を選択することができます。
4. 活動化するルールのあるインターフェースを選択します。この場合、「**これらの規則をすべてのインターフェースおよびすべての Point-to-Point フィルター ID で活動化します**」を選択します。
5. ダイアログ・ボックスで 「**OK**」 をクリックして、指定した 1 つまたは複数のインターフェースでルールの検査と活動化を実行することを確認する。「OK」をクリックすると、システムはそのルールに構文およびセマンティックのエラーがないかどうかを検査し、エディター下部のメッセージ・ウィンドウでその結果を報告します。
6. 上記のステップを繰り返して、System B でパケット・ルールを活動化する。

シナリオ: システムを PPPoE アクセス・コンセントレーターに接続する

多くのインターネット・サービス・プロバイダー (ISP) が、Point-to-Point Protocol over Ethernet (PPPoE) を使用してデジタル加入者回線 (DSL) 上での高速インターネット・アクセスを提供しています。システムをそれらの ISP に接続することにより、Point-to-Point Protocol (PPP) のメリットを保ったまま、高帯域幅の接続が提供されます。

状況

あなたは、ビジネスでもっと速いインターネット接続が必要とされるため、地元の ISP によるデジタル加入者回線 (DSL) サービスに関心があります。初期調査の後、ISP が PPPoE を使用してそのクライアントに接続していることがわかりました。この PPPoE 接続を使用して、システムを介したブロードバンド・インターネット接続を提供する必要があります。

図 3. PPPoE によるシステムから ISP への接続

ソリューション

システムを介して、 ISP への PPPoE 接続をサポートすることができます。システムは新しい PPPoE 仮想回線タイプを使用します。これは、タイプ
2743、2760、2838、2849、287F、5700、5701、5706、5707、573A、5767、または 576A イーサネット・アダプターを使用するように構成された、物理イーサネット回線に結び付いています。この仮想回線は、イーサネット・ローカル・エリア・ネットワーク (LAN) 上の PPP セッション・プロトコルをサポートします。そのイーサネット LAN は、リモート ISP へのゲートウェイを提供する DSL モデムに接続しています。このゲートウェイにより LAN 接続のユーザーは、PPPoE 接続を使用して、高速のインターネット・アクセスを実現できます。システムと ISP の間の接続が開始された後、LAN 上の個々のユーザーは、システムに割り振られた IP アドレスを使用して、PPPoE 上で ISP にアクセスできます。追加のセキュリティーを提供するには、PPPoE 仮想回線にフィルター規則を適用して、特定の着信インターネット・トラフィックを制限することができます。

構成の例

IBM Navigator for iからサンプル PPP 構成をセットアップするには、以下の手順を実行します。

1. ISP とともに使用する接続装置を構成します。
2. システムで、発信元接続プロファイルを構成します。

   必ず、次の情報を入力してください。
   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: PPP over Ethernet
   - **動作モード**: 起動側 (Initiator)
   - **リンク構成**: 単一回線 (Single line)

3. 「新規 2 地点間プロファイルのプロパティー」の「一般」ページで、発信元プロファイルの名前と記述を入力します。この名前は、接続プロファイルと仮想 PPPoE 回線の両方を指します。
4. 「**接続**」をクリックして、「接続」ページを開きます。この接続プロファイルの名前に対応する **PPPoE 仮想回線名**を選択します。回線を選択した後、IBM Navigator for i は **回線プロパティー**ダイアログを表示します。
   a. 「一般」ページで、PPPoE 仮想回線のわかりやすい説明を入力します。
   b. 「**リンク**」をクリックして、「リンク」のページを開きます。物理回線名の選択リストで、この接続で使用するイーサネット回線を選択し、「**実行**」をクリックします。あるいは、新しいイーサネット回線を定義する必要がある場合には、回線名を入力して「**開く**」をクリックします。 IBM Navigator for i に、「**新規イーサネット回線のプロパティー**」ダイアログが表示されます。

      注: PPPoE では、タイプ 2743、2760、2838、2849、287F、5700、5701、5706、5707、573A、5767、または 576A のイーサネット・アダプターが必要です。

      1) 「一般」ページで、イーサネット回線のわかりやすい説明を入力し、回線定義が、必要なハードウェア・リソースを使用していることを確認してください。
      2) 「**リンク**」をクリックして、「リンク」のページを開きます。物理イーサネット回線のプロパティーを入力します。詳しくは、イーサネット・アダプターの資料およびオンライン・ヘルプを参照してください。
      3) 「**OK**」をクリックして、PPPoE 仮想回線のプロパティー・ページに戻ります。
   c. 「**制限 (Limits)**」をクリックして LCP 認証のプロパティーを定義するか、または「**OK**」をクリックして「新規 2 地点間プロファイル」の「接続」ページに戻ります。
   d. 「接続」ページに戻ったら、 ISP によって提供されている情報に基づいて PPPoE サーバー・アドレスを指定します。
5. システムが自身の認証を実行することを ISP が求めている場合、またはシステムがリモート・システムの認証を実行するようにする場合は、「**認証**」をクリックして、「認証」ページを開き、要求された情報を入力します。
6. 「**TCP/IP IPv4 設定**」をクリックして、「TCP/IP IPv4 設定」ページを開き、この接続プロファイルの IP アドレス処理パラメーターを指定します。使用される設定は、ISP によって提供されます。 LAN 接続のユーザーが、システムに割り振られた IP アドレスを使用して ISP に接続できるようにするには、「**アドレスを隠す (Hide addresses; Full masquerading)**」を選択します。
7. 「**DNS**」をクリックして「DNS」ページを開き、ISP が提供する DNS サーバーの IP アドレスを入力します。
8. 「**OK**」をクリックしてプロファイルを完成させます。

関連概念:

4 ページの『グループ・ポリシー・サポート』
グループ・ポリシーのサポートにより、ネットワーク管理者はリソースを管理するためのユーザー・ベースのグループ・ポリシーを定義できます。ユーザーが Point-to-Point Protocol (PPP) またはレイヤー 2 トンネリング・プロトコル (L2TP) セッションにログオンする際に、個々のユーザーにアクセス制御ポリシーを割り当てることができます。

関連タスク:

60 ページの『接続プロファイルの作成』
システム間に PPP 接続を構成するための最初のステップは、システム上に接続プロファイルを作成することです。

関連資料:

64 ページの『リンク構成』
リンク構成は、接続を確立するために Point-to-Point Protocol (PPP) 接続プロファイルが使用する回線サービスのタイプを定義します。

56 ページの『システムの認証』
IBM i プラットフォームでの PPP 接続では、リモート・クライアントからシステムへのダイヤルインと、システムがダイヤルしている ISP または別のシステムへの接続の両方を認証するためのオプションがいくつかサポートされます。

51 ページの『IP アドレス処理』
Point-to-Point Protocol (PPP) 接続では、接続プロファイルのタイプに応じて、IP アドレスを管理するため異なるいくつかのセットのオプションを使用できるようになっています。

51 ページの『IP パケット・フィルター』
IP パケット・フィルターは、個々のユーザーがネットワークにログオンしたときに利用できるサービスを制限します。

シナリオ: リモート・ダイヤルイン・クライアントをシステムに接続する

在宅勤務者やモバイル・クライアントなどのリモート・ユーザーは、会社のネットワークにアクセスしなければならなくなることがよくあります。こうしたダイヤルイン・クライアントは、Point-to-Point Protocol (PPP) を使用してシステムにアクセスできます。

状況

あなたは、企業のネットワークの管理担当者として、システムとネットワーク・クライアントの両方を保守しなければなりません。あなたは、仕事場に来て問題の障害追及と修正を行うよりも、自宅のようなリモート・ロケーションから作業できる機能を必要としています。あなたの会社には、インターネットと結合するためのネットワーク接続がないので、あなたは PPP 接続を使用してシステムにダイヤルインすることになるでしょう。また、あなたが現在所有しているモデムは、7852-400 エレクトロニック支援モデムだけであり、接続にはこのモデムを利用する必要があります。

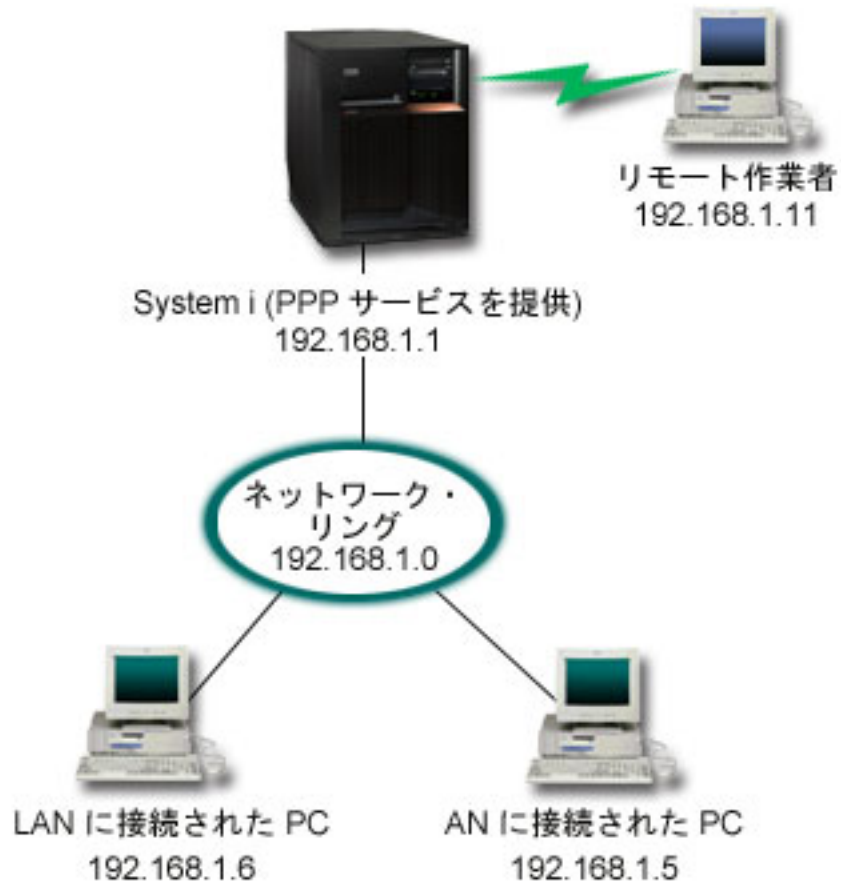


図 4. リモート・クライアントとシステムとの接続

ソリューション

PPP を使用し、手持ちのモデムを用いて自宅の PC をシステムに接続することができます。このタイプの PPP 接続にエレクトロニック支援モデムを使用するので、そのモデムが同期と非同期の両方のモードで構成されていることを確認する必要があります。この図は、2 つの PC のある LAN に接続された、PPP サービスを備えたシステムを示しています。リモート接続の作業者がシステムにダイヤルインします。システムにより認証が実施され、作業用ネットワークの一部となります (192.168.1.0)。この場合、ダイヤルイン・ クライアントに静的な IP アドレスを割り当てるのは、非常に簡単です。

リモート接続作業者は、チャレンジ・ハンドシェーク認証プロトコル (CHAP-MD5) を使用することによって、システムの認証を受けます。システムでは MS_CHAP を使用することはできないので、PPP クライアントは、必ず CHAP-MD5 を使用しなければなりません。

上に示したようにリモート作業者が会社のネットワークにアクセスできるようにしたい場合は、 TCP/IP スタックと PPP 受信側プロファイルで IP 転送をオンに設定する必要があります。また、IP ルーティングを正しく構成する必要もあります。ネットワーク内でリモート・クライアントが実行できるアクションを制限したり保護したりするには、 IP パケットを処理するためのフィルター規則を使用することができます。

リモート作業者が IPv6 を使用して会社のネットワークにアクセスできるようにするには、接続プロファイルで IPv6 を使用可能にする必要もあります。特定の IPv6 アドレスを割り当てる必要はありません。しかし、リモート作業者にデフォルト以外のリンク・ローカル IPv6 アドレス割り当てる場合は、IPv6 アドレ

ス接頭部を構成するか、会社のネットワークで DHCPv6 サーバーが使用可能なら該当するオプションを設定する必要があります。この例では、アドレス接頭部 2001:DBA:: とデフォルト経路を通知すること、およびネットワーク内の DHCPv6 サーバーが IP アドレスを提供できることを想定しています。DHCPv6 サーバーがリモート・ダイヤルイン・クライアントに情報を返せるようにするには、接続プロファイル内でグローバル IPv6 アドレスを構成しなければなりません。

エレクトロニック支援モデムが一度に処理できる接続は 1 つだけなので、上の図に含まれるリモート・ダイヤルイン・クライアントは 1 つだけです。

構成の例

IBM Navigator for iからサンプル PPP 構成をセットアップするには、以下の手順を実行します。

1. ダイヤルアップ・ネットワーキングを構成し、リモート PC 上にダイヤルアップ接続を作成します。
2. システムで受信接続プロファイルを構成します。

   必ず、次の情報を入力してください。
   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: 交換回線
   - **動作モード**: 応答
   - **リンク構成**: これは、環境によって、単一回線または回線プールのいずれかになります。
3. 「新規 2 地点間プロファイルのプロパティー」の「一般」ページで、受信側プロファイルの名前と記述を入力します。
4. 「**接続**」をクリックして、「接続」ページを開きます。適切な「**回線名**」を選択するか、新しい名前を入力し、「**開く**」をクリックして新規の回線を作成します。
   a. 「一般」ページで、7852–400 アダプターが接続されている既存のハードウェア・リソースをクリックし、「フレーム指示」に「**非同期**」を設定します。
   b. 「**モデム**」をクリックして、「モデム」のページを開きます。名前選択リストから、「**IBM 7852–400**」モデムを選択し、「**実行**」をクリックします。
   c. 「**OK**」をクリックして「新規 2 地点間プロファイルのプロパティー」ページに戻ります。
5. 「**認証**」をクリックして、「認証」ページを開きます。
   a. 「**このシステムでリモート・システムの ID 検査が必要**」を選択します。
   b. 「**暗号化されたパスワード (CHAP-MD5) を許可**」を選択します。
   c. 「**妥当性検査リストを使用してローカルから認証**」を選択し、新規のリモート・ユーザーを妥当性検査リストに追加する。
6. 「**TCP/IP IPv4 設定**」をクリックして、「TCP/IP IPv4 設定」ページを開きます。
   a. 「**IPv4 を使用可能に設定**」を選択します。
   b. ローカル IP アドレス 192.168.1.1 を選択します。
   c. リモート IP アドレスの場合は、開始 IP アドレスが 192.168.1.11 である「**固定 IP アドレス**」を選択します。
   d. 「**リモート・システムが他のネットワークにアクセスすること (IP 転送) を許可**」を選択する。
7. 「**TCP/IP IPv6 設定**」をクリックして、「TCP/IPv6 設定 (TCP/IPv6 Settings)」ページを開きます。
   a. 「**IPv6 を使用可能に設定**」を選択します。
   b. 「**固定ローカル IP アドレス**」でグローバル IPv6 アドレスを指定します。このアドレスは、IPv6 アドレスを配布するための DHCPv6 サーバー構成と互換性がなければなりません。

c. 「**インターフェース ID**」で「**生成**」を選択します。
d. 「**他のネットワークへのアクセスをリモート・システムに許可 (IP 転送)**」で「はい」を選択します。
e. 「**アドレス接頭部**」を「2001:DBA::」に設定します。
f. 「**IPv6 デフォルト経路の通知**」を選択します。
g. 「**DHCPv6 の通知 - 管理対象アドレス構成**」を選択します。

8. 「**OK**」をクリックしてプロファイルを完成させます。

関連概念:

45 ページの『PPP の計画』
Point-to-Point Protocol (PPP) には、PPP 接続の作成と管理が含まれます。

関連タスク:

60 ページの『接続プロファイルの作成』
システム間に PPP 接続を構成するための最初のステップは、システム上に接続プロファイルを作成することです。

関連資料:

57 ページの『MD5 によるチャレンジ・ハンドシェーク認証プロトコル』
Challenge Handshake Authentication Protocol (CHAP-MD5) は、認証システムおよび遠隔装置だけが認識する値を計算するためのアルゴリズム (MD-5) を使用します。

64 ページの『リンク構成』
リンク構成は、接続を確立するために Point-to-Point Protocol (PPP) 接続プロファイルが使用する回線サービスのタイプを定義します。

65 ページの『回線プール』
PPP 接続が回線プールの回線を使用するように設定するには、この回線サービスを選択します。PPP 接続が開始すると、システムは回線プールから未使用回線を選択します。ダイヤル・オンデマンド・プロファイルの場合、システムはリモート・システムの TCP/IP トラフィックを検出するまで回線を選択しません。

シナリオ: モデムを使用してオフィスの LAN をインターネットに接続する

普通、管理担当者は、従業員がインターネットにアクセスできるように、オフィス・ネットワークをセットアップします。管理者は、システムからインターネット・サービス・プロバイダー (ISP) に接続するために、モデムを使用できます。 LAN に接続された PC クライアントは、IBM i オペレーティング・システムをゲートウェイとして使用することにより、インターネット通信が可能です。

状況

あなたの企業が使用している企業のアプリケーションにおいて、ユーザーがインターネットにアクセスする必要が生じています。アプリケーションでは、大量のデータの交換は必要ないため、あなたはシステムと LAN 接続の PC クライアントの両方をインターネットへ接続させるために、モデムを使用できなければなりません。この状況を次の図で説明します。

図 5. モデムを使用してオフィスの LAN をインターネットに接続する

ソリューション

内蔵 (または互換性のあるその他の) モデムを使用してシステムを ISP に接続することができます。 ISP への PPP 接続を確立するには、システム上に Point-to-Point Protocol (PPP) 発信元プロファイルを作成する必要があります。

システムと ISP の間に接続を確立すると、LAN 接続 PC が、システムをゲートウェイとして使用して、インターネットと通信することができるようになります。発信元プロファイルでは、「アドレスを隠す」オプションがオンになっており、プライベート IP アドレスを保持している LAN クライアントがインターネットと通信できるようになっていることを確認することが必要です。

ISP が IPv6 アドレッシングをサポートする場合は、発信元プロファイル内で IPv6 を使用可能にすることもできます。

システムとネットワークがインターネットに接続するにあたっては、セキュリティーのリスクを理解していなければなりません。利用している ISP のセキュリティー・ポリシーを理解し、システムとネットワークを保護するためのさらなる処置を講じてください。

インターネットの使用状況によっては、帯域幅が問題になることがあります。

構成の例

IBM Navigator for iからサンプル構成をセットアップするには、以下の手順を実行します。

1. システムで、発信元接続プロファイルを構成します。

   必ず、次の情報を選択してください。

   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: 交換回線
   - **動作モード**: ダイヤル
   - **リンク構成**: これは、環境によって、単一回線または回線プールのいずれかになります。

2. 「新規 2 地点間プロファイルのプロパティー」の「一般」ページで、発信元プロファイルの名前と記述を入力します。
3. 「**接続**」をクリックして、「接続」ページを開きます。適切な回線名を選択するか、新しい名前を入力し、「**開く**」をクリックして新規の回線を作成します。
   a. 新規回線のプロパティーの「一般」ページで、既存のハードウェア・リソースを選択します。内部モデム・リソースを選択する場合、モデム・タイプとフレーム設定は自動的に選択されます。
   b. 「**OK**」をクリックして「新規 2 地点間プロファイルのプロパティー」ページに戻ります。
4. 「**追加**」をクリックして、ISP サーバーに接続するのにダイヤルする電話番号を入力します。必須の接頭部を必ず含めるようにしてください。
5. 「**認証**」をクリックして「認証」ページを開き、「**このシステムの ID 検査を行うことをリモート・システムに許可する**」を選択します。認証プロトコルを選択し、必要なユーザー名やパスワードの情報を入力します。
6. 「**TCP/IP IPv4 設定**」をクリックして、「TCP/IP IPv4」ページを開きます。
   a. 「**IPv4 を使用可能に設定**」を選択します。
   b. リモートとローカルの両方の IP アドレスに対して、「**リモート・システムによる割り当て**」を選択します。
   c. 「**リモート・システムをデフォルト経路として追加**」を選択します。
   d. 「**アドレスの非表示 (フル・マスカレード)**」にチェック・マークを付けて、内部 IP アドレスがインターネットに経路指定されないようにします。
7. IPv6 アドレッシングを使用可能にする場合は、「**TCP/IP IPv6 設定**」をクリックして、「TCP/IP IPv6」ページを開きます。
   a. 「**IPv6 を使用可能に設定**」を選択します。
   b. b. 「**固定ローカル IP アドレス**」で「*None」を選択します。
   c. 「**インターフェース ID**」で「**生成**」を選択します。
   d. 「**他のネットワークへのアクセスをリモート・システムに許可 (IP 転送)**」で「いいえ」を選択します。
   e. 「**デフォルト経路の受け入れ**」を選択します。

8. 「**DNS**」をクリックして「DNS」(ドメイン・ネーム・システム) ページを開き、ISP が提供する DNS サーバーの IP アドレスを入力します。
9. 「**OK**」をクリックしてプロファイルを完成させます。

接続プロファイルを使用してインターネットに接続する場合は、「IBM Navigator for i」から、接続プロファイルを右マウス・ボタン・クリックして、「**開始**」を選択します。状況が「**アクティブ**」に変われば接続は正常です。最新表示を行って表示を更新してください。

注: ネットワーク上のその他のシステムでも適切なルーティングが定義され、それらのシステムからインターネットに結合する TCP/IP トラフィックがシステムを介して送信されるようになっていることを確認する必要があります。

関連概念:

45 ページの『PPP の計画』
Point-to-Point Protocol (PPP) には、PPP 接続の作成と管理が含まれます。

関連タスク:

60 ページの『接続プロファイルの作成』
システム間に PPP 接続を構成するための最初のステップは、システム上に接続プロファイルを作成することです。

関連資料:

65 ページの『回線プール』
PPP 接続が回線プールの回線を使用するように設定するには、この回線サービスを選択します。PPP 接続が開始すると、システムは回線プールから未使用回線を選択します。ダイヤル・オンデマンド・プロファイルの場合、システムはリモート・システムの TCP/IP トラフィックを検出するまで回線を選択しません。

64 ページの『リンク構成』
リンク構成は、接続を確立するために Point-to-Point Protocol (PPP) 接続プロファイルが使用する回線サービスのタイプを定義します。

シナリオ: モデムを使用して会社のネットワークとリモート・ネットワークを接続する

モデムを使用することにより、2 つのリモート・ロケーション (本社と支社など) の間でデータの交換を実行できます。 Point-to-Point Protocol (PPP) を使用して本社のシステムと支社のシステムの間の接続を確立することによって、2 つの LAN を接続することができます。

状況

支社と本社のネットワークが、異なる 2 つのロケーションにあるとします。支社は、毎日、本社と接続して、データ入力アプリケーションのためのデータベース情報を交換する必要があります。データ交換量は物理ネットワーク接続を購入するほどのものではないので、必要に応じて、モデムを使用して 2 つのネットワークを接続することにします。

図 6. モデムを使用して会社のネットワークとリモート・ネットワークを接続する

ソリューション

図のように、システム間の接続を確立することによって、2 つの LAN を PPP で接続することができます。ここでは、リモート・オフィスが本社への接続を開始するものと想定しましょう。あなたは、リモート・システム上に発信元プロファイルを、本社のシステム上に受信側プロファイルを構成します。

リモート・オフィスの PC が、会社の LAN (192.168.1.0) にアクセスする必要がある場合は、本社の受信側プロファイルの IP 転送をオンにする必要があります。また、IP アドレス・ルーティングが PC で使用できるようにする必要もあります (この例では、192.168.2、192.168.3、192.168.1.6、および 192.168.1.5)。さらに、TCP/IP スタックの IP 転送も活動化しておく必要があります。このように構成することにより、LAN の間の基本的な TCP/IP 通信が可能になります。セキュリティーの要素や、LAN 相互間でホスト名を解決する DNS についても考慮する必要があります。

また、接続プロファイルの「TCP/IP IPv6 設定」セクションで IP 転送を有効にすることにより、リモート・オフィスの PC 用に IPv6 アクセスを構成することもできます。 TCP/IP スタックの IP 転送も活動化しておく必要があります。しかし、IP 転送が有効でも、アドレス接頭部をいずれかの LAN 上の PC に提供するために PPP リンク上のルーター・アドバタイズメント・メッセージを使用することはできません。その理由は、ルーター・アドバタイズメント・メッセージは PPP リンクに対してローカルだからです。したがって、PC の IPv6 アドレス割り当ては、PPP 接続プロファイルの構成による影響を受けません。

構成の例

IBM Navigator for iからサンプル構成をセットアップするには、以下の手順を実行します。

1. リモート・オフィスのシステムで、発信元接続プロファイルを構成します。

   必ず、次の情報を選択してください。
   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: 交換回線
   - **動作モード**: ダイヤル
   - **リンク構成**: これは、環境によって、単一回線または回線プールのいずれかになります。
2. 「新規 2 地点間プロファイルのプロパティー」の「一般」ページで、発信元プロファイルの名前と記述を入力します。
3. 「**接続**」をクリックして、「接続」ページを開きます。適切な回線名を選択するか、新しい名前を入力し、「**開く**」をクリックして新規の回線を作成します。
   a. 新規回線のプロパティーの「一般」ページで、既存のハードウェア・リソースを選択し、「フレーム指示」に「**非同期**」を設定します。
   b. 「**モデム**」をクリックして、「モデム」のページを開きます。名前選択リストから、使用するモデムを選択します。
   c. 「**OK**」をクリックして「新規 2 地点間プロファイルのプロパティー」ページに戻ります。
4. 「**追加**」をクリックして、本社のシステムに接続する電話番号を入力します。必須の接頭部がある場合、必ずそれを含めてください。
5. 「**認証**」をクリックして「認証」ページを開き、「**このシステムの ID 検査を行うことをリモート・システムに許可する**」を選択します。「**暗号化パスワードが必要 (CHAP-MD5)**」を選択し、必要なユーザー名とパスワードの情報を入力します。
6. 「**TCP/IP IPv4 設定**」をクリックして、「TCP/IP IPv4 設定」ページを開きます。
   a. 「**IPv4 を使用可能に設定**」を選択します。

b. 「**ローカル IP アドレス**」については、「**固定 IP アドレスの使用**」選択ボックスから、リモート・オフィスの LAN インターフェースの IP アドレス (192.168.2.1) を選択します。

c. リモート IP アドレスについては、「**リモート・システムによる割り当て**」を選択します。

d. ルーティング・セクションで、「**リモート・システムをデフォルト経路として追加**」を選択します。

7. 「**TCP/IP IPv6 設定**」をクリックして、「TCP/IP IPv6 設定」ページを開きます。

a. 「**IPv6 を使用可能に設定**」を選択します。

b. 「**インターフェース ID**」で「生成」を選択します。

c. 「**他のネットワークへのアクセスをリモート・システムに許可 (IP 転送)**」で「はい」を選択します。

d. 「**アドレス接頭部**」で *None を選択します。

e. 「**IPv6 デフォルト経路の通知**」または「**DHCPv6 の通知**」を選択しないでください。

f. 該当する IPv6 経路を追加します。

8. 「**DNS**」をクリックして、DNS 設定ページを開きます。

a. 以下のいずれかのオプションを入力します。

- 社内 LAN 上の DNS サーバーの IP アドレスまたはホスト名。
- 接続の確立時に DNS サーバーを追加しない場合は、「なし」を選択します。

9. 「**OK**」をクリックして発信元プロファイルを完成させます。

10. 本社のシステムで、受信接続プロファイルを構成します。

必ず、次の情報を選択してください。

- **プロトコル・タイプ**: PPP
- **接続タイプ**: 交換回線
- **動作モード**: 応答
- **リンク構成**: これは、環境によって、単一回線または回線プールのいずれかになります。

11. 「新規 2 地点間プロファイルのプロパティー」の「一般」ページで、受信側プロファイルの名前と記述を入力します。

12. 「**接続**」をクリックして、「接続」ページを開きます。適切な回線名を選択するか、新しい名前を入力し、「**開く**」をクリックして新規の回線を作成します。

a. 「一般」ページで、既存のハードウェア・リソースを選択し、「フレーム指示」に「**非同期**」を設定します。

b. 「**モデム**」をクリックして、「モデム」のページを開きます。名前選択リストから、使用するモデムを選択します。

c. 「**OK**」をクリックして「新規 2 地点間プロファイルのプロパティー」ページに戻ります。

13. 「**認証**」をクリックして、「認証」ページを開きます。

a. 「**このシステムでリモート・システムの ID 検査が必要**」にチェック・マークを付けます。

b. 妥当性検査リストに新しいリモート・ユーザーを追加します。

c. 「CHAP-MD5」認証をチェックします。

14. 「**TCP/IP IPv4 設定**」をクリックして、「TCP/IP IPv4 設定」ページを開きます。

a. 「**IPv4 を使用可能に設定**」を選択します。

b. ローカル IP アドレスについては、「**選択**」ボックスから、本社のインターフェースの IP アドレス (192.168.1.1) を選択します。

c. リモート IP アドレスについては、「**リモート・システムのユーザー ID をベースにする**」を選択します。「**ユーザー名によって定義される IP アドレス**」ダイアログが表示されます。「**追加**」をクリックします。「呼び出し側のユーザー名」、「IP アドレス」、および「サブネット・マスク」の各フィールドに入力します。このシナリオでは、次のように入力するのが適切です。

- 「呼び出し側のユーザー名」: `Remote_site`
- 「IP アドレス」: `192.168.2.1`
- 「サブネット・マスク」: `255.255.255.0`

「**OK**」をクリックし、再度「**OK**」をクリックして「TCP/IP 設定」ページに戻ります。

d. 「**IP 転送**」を選択して、ネットワーク内のその他のシステムがこのシステムをゲートウェイとして使用できるようにします。

15. 「**TCP/IP IPv6 設定**」をクリックして、「TCP/IP IPv6 設定」ページを開きます。
    a. 「**IPv6 を使用可能に設定**」を選択します。
    b. 「**インターフェース ID**」で「生成」を選択します。
    c. 「**他のネットワークへのアクセスをリモート・システムに許可 (IP 転送)**」で「はい」を選択します。
    d. 「**アドレス接頭部**」で「なし」を選択します。
    e. 「**IPv6 デフォルト経路の通知**」または「**DHCPv6 の通知**」を選択しないでください。
    f. 該当する IPv6 経路を追加します。
16. 「**OK**」をクリックして受信側プロファイルを完成させます。

関連タスク:

60 ページの『接続プロファイルの作成』
システム間に PPP 接続を構成するための最初のステップは、システム上に接続プロファイルを作成することです。

関連資料:

64 ページの『リンク構成』
リンク構成は、接続を確立するために Point-to-Point Protocol (PPP) 接続プロファイルが使用する回線サービスのタイプを定義します。

65 ページの『回線プール』
PPP 接続が回線プールの回線を使用するように設定するには、この回線サービスを選択します。PPP 接続が開始すると、システムは回線プールから未使用回線を選択します。ダイヤル・オンデマンド・プロファイルの場合、システムはリモート・システムの TCP/IP トラフィックを検出するまで回線を選択しません。

シナリオ: RADIUS NAS でダイヤルアップ接続を認証する

システム上で稼働する Network Access Server (NAS) は、ダイヤルイン・クライアントから別個の Remote Authentication Dial In User Service (RADIUS) サーバーへ認証要求をルーティングすることができます。認証されると、RADIUS はユーザーに割り当てられる IP アドレスを制御することもできます。

状況

企業のネットワークには、分散ダイヤルアップ・ネットワークから 2 台のシステムにダイヤルインするリモート・ユーザーがいます。認証、サービス、およびアカウンティングを集中管理する方法が必要です。これにより、1 つのシステムでユーザー ID とパスワードの検証要求を処理し、どの IP アドレスが彼らに割り当てられたものかを判別できるようになります。

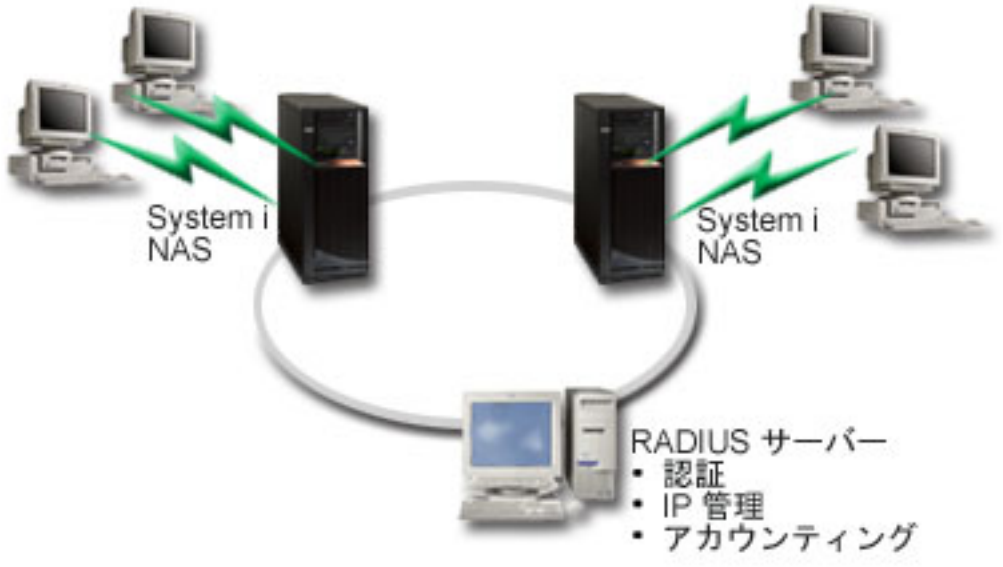


図 7. RADIUS サーバーによるダイヤルアップ接続の認証

ソリューション

ユーザーが接続を試行すると、システムで稼働している NAS は、ネットワーク上の RADIUS サーバーに認証情報を転送します。RADIUS サーバーは企業のネットワークのためのすべての認証情報を保守し、認証の要求と応答を処理します。ユーザーが妥当性検査される場合、相手側の IP アドレスを割り当てるように RADIUS サーバーを構成することもでき、 RADIUS サーバーはアカウンティングを活動化して、ユーザー・アクティビティーおよび使用状況を追跡することができます。 RADIUS をサポートするためには、システム上に RADIUS NAS サーバーを定義する必要があります。

構成の例

IBM Navigator for iからサンプル構成をセットアップするには、以下の手順を実行します。

1. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**すべてのタスク**」 > 「**リモート・アクセス・サービス**」を展開して、「**サービス**」を選択します。
2. 「**RADIUS**」タブで、「**RADIUS ネットワーク・アクセス・サーバー接続を使用可能にする (Enable RADIUS Network Access Server connection)**」と、「**RADIUS を認証に使用可能にする (Enable RADIUS for authentication)**」を選択します。ご使用の RADIUS ソリューションによりますが、RADIUS ハンドル接続アカウンティングおよび TCP/IP アドレス構成を使用可能にすることもできます。
3. 「**RADIUS NAS 設定 (RADIUS NAS settings)**」ボタンをクリックします。
4. 「一般」ページで、このサーバーの説明を入力します。
5. 「認証サーバー」ページで (および、オプションで「アカウンティング・サーバー」ページでも)、「**追加**」をクリックして以下の情報を入力します。
   a. 「**ローカル IP アドレス**」ボックスには、RADIUS サーバーとの接続に使用するインターフェース用の IP アドレスを入力します。
   b. 「**サーバー IP アドレス**」ボックスでは、RADIUS サーバー用の IP アドレスを入力します。
   c. 「**パスワード**」ボックスでは、 RADIUS サーバーに対してシステムを識別させるために使用するパスワードを入力します。

d. 「**ポート**」ボックスでは、 RADIUS サーバーとの通信に使用するシステム上のポートを入力します。デフォルトでは、認証サーバーはポート 1812、アカウンティング・サーバーはポート 1813 です。

6. 「**OK**」をクリックします。
7. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**リモート・アクセス・サービス**」を展開して、「**受信先接続プロファイル**」を選択します。
8. 認証用に RADIUS サーバーを使用する予定の接続プロファイルを選択します。 RADIUS サービスは、受信側接続プロファイルにのみ適用できます。
9. 「認証」ページで、「**このシステムでリモート・システムの ID 検査が必要**」を選択します。
10. 「**RADIUS サーバーを使用してリモート側で認証 (Authenticate remotely using a RADIUS server)**」を選択します。
11. 認証プロトコルを選択します (PAP、または CHAP-MD5)。このプロトコルは RADIUS サーバーでも使用されていなければなりません。
12. 「**接続の編集とアカウンティングに RADIUS を使用する (Use RADIUS for connection editing and accounting)**」を選択します。
13. 「**OK**」をクリックして、接続プロファイルへの変更を保管します。

RADIUS サーバーのセットアップも行う必要があります。これには、認証プロトコル、ユーザー・データ、パスワード、およびアカウンティング情報のサポートが含まれています。詳しくは、ご使用の RADIUS ベンダー資料を参照してください。

この接続プロファイルを使用してユーザーがダイヤルインすると、指定された RADIUS サーバーにシステムは認証情報を転送します。ユーザーが妥当性検査されると、接続は許可され、RADIUS サーバーに関するユーザーの情報で指定されている接続制限が使用されます。

関連タスク:

76 ページの『接続プロファイルにおける RADIUS および DHCP サービスの使用可能化』
PPP 受信接続プロファイルで RADIUS または動的ホスト構成プロトコル (DHCP) のサービスを有効にするための手順を以下に示します。

関連資料:

56 ページの『システムの認証』
IBM i プラットフォームでの PPP 接続では、リモート・クライアントからシステムへのダイヤルインと、システムがダイヤルしている ISP または別のシステムへの接続の両方を認証するためのオプションがいくつかサポートされます。

58 ページの『Remote Authentication Dial In User Service の概要』
Remote Authentication Dial In User Service (RADIUS) は、分散ダイヤルアップ・ネットワーク内のリモート・アクセス・ユーザーのために、認証、アカウンティング、および IP を集中管理するサービスを提供するインターネット標準プロトコルです。

シナリオ: グループ・ポリシーおよび IP フィルターを使用してリソースへのリモート・ユーザー・アクセスを管理する

グループ・アクセス・ポリシーによって、接続のためのそれぞれのユーザー・グループを識別し、共通の接続属性およびセキュリティー設定をグループ全体に適用することができます。グループ・ポリシーと IP フィルター操作とを組み合わせて使用することにより、ネットワーク上の特定の IP アドレスへのアクセスを、許可したり制限したりすることができます。

状況

ネットワークには、いくつかのグループの分散ユーザーがあり、それぞれのユーザーについて、社内 LAN 上で異なるリソースにアクセスする必要があります。データ入力ユーザーのグループは、データベースおよびその他のいくつかのアプリケーションへのアクセスを必要とします。他の会社の人々のグループにとっては、HTTP、ファイル転送プロトコル (FTP)、および Telnet サービスへのダイヤルアップ・アクセスが必要ですが、セキュリティーの理由から、このグループが TCP/IP のその他のサービスまたはトラフィックにアクセスすることは許可されません。それぞれのユーザーについて詳細に渡る接続属性および許可を定義するのは労力の無駄です。一方、この接続プロファイルのすべてのユーザーに対してネットワーク制限を課すと、十分な制御ができなくなります。このシステムに定期的にダイヤルするユーザーで構成されるいくつかの特定のグループについて、接続設定および許可を定義できるような方法が必要でしょう。

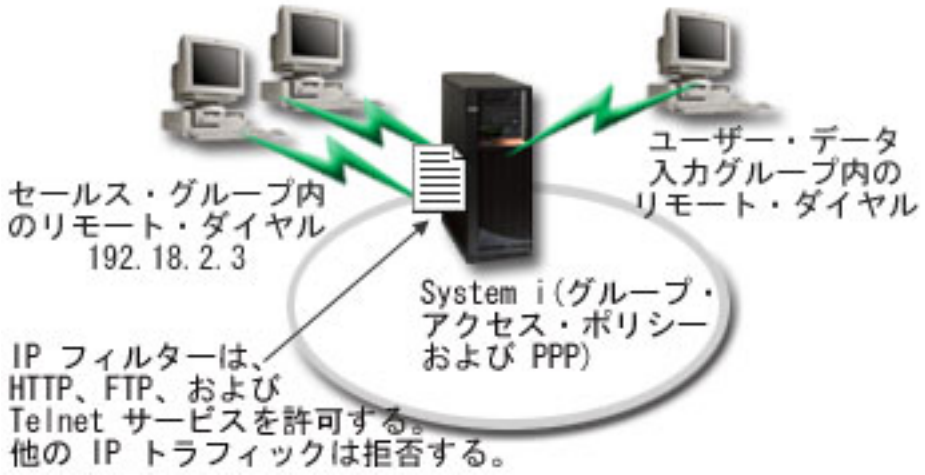


図 8. グループ・ポリシー設定に基づいて接続設定をダイヤルアップ接続に適用する

ソリューション

2 つの異なるユーザーのグループにそれぞれ固有の IP フィルター制限を適用する必要があります。これを達成するには、グループ・アクセス・ポリシーおよび IP フィルター規則を作成します。グループ・アクセス・ポリシーは IP フィルター規則を参照するので、最初にフィルター規則を作成する必要があります。この例では、PPP フィルターを作成して、IBM ビジネス・パートナー・グループ・アクセス・ポリシーについての IP フィルター・ルールを組み込む必要があります。これらのフィルター規則は HTTP、FTP、および Telnet サービスを許可するものの、システムを介したその他のすべての TCP/IP トラフィックおよびサービスへのアクセスは制限します。このシナリオでは、セールス・グループで必要なフィルター規則のみ示します。ただし、データ入力グループに類似したフィルターを設定することもできます。

最後に、グループ・アクセス・ポリシーを (グループごとに 1 つずつ) 作成して、グループを定義する必要があります。グループ・アクセス・ポリシーを使用すると、共通接続属性をユーザーのグループに定義することができます。システムでグループ・アクセス・ポリシーを妥当性検査リストに追加することにより、認証プロセスの際にこれらの接続設定を適用できます。このグループ・アクセス・ポリシーは、ユーザーのセッションにいくつかの設定を指定します。これには、IP アドレスを制限する IP フィルター規則を適用する機能、およびセッション中にユーザーが使用できる TCP/IP サービスが含まれます。

構成の例

IBM Navigator for iからサンプル構成をセットアップするには、以下の手順を実行します。

1. このグループ・アクセス・ポリシーの許可および制限を指定する Point-to-Point Protocol (PPP) フィルター ID および IP パケット・ルール・フィルターを作成します。
   a. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**すべてのタスク**」 > 「**リモート・アクセス・サービス**」 > 「**受信先接続プロファイル**」を展開して、「**グループ・アクセス・ポリシー**」を選択します。
   b. 画面右側に表示される事前定義のグループの 1 つを右クリックして、「**プロパティー**」を選択します。

      注: 新しくグループ・アクセス・ポリシーを作成する場合は、「**グループ・アクセス・ポリシー**」を右クリックして、「**新規グループ・アクセス・ポリシー**」を選択します。「**一般**」タブに入力します。「**TCP/IP 設定**」タブを選択して、以下のステップ e に進みます。
   c. 「**TCP/IP IPv4 設定**」タブを選択して、「**拡張**」をクリックします。
   d. 「**IP パケット規則をこの接続に使用**」を選択してから、「**規則ファイルの編集 (Edit Rules File)**」をクリックします。これにより、IP パケット規則エディターが始動し、 PPP フィルター・パケット規則ファイルがオープンします。
   e. 「**挿入 (Insert)**」メニューをオープンしてから、「**フィルター (Filters)**」を選択して、フィルター・セットを追加します。「**一般**」タブを使用してフィルター・セットを定義し、「**サービス**」タブを使用して、HTTP などの、許可するサービスを定義します。以下のフィルター・セット、"services_rules" では、HTTP、FTP、および Telnet サービスが使用可能です。フィルター規則には、暗黙的デフォルト否定ステートメントが組み込まれ、明示的に許可されていないすべての TCP/IP サービスまたは IP トラフィックを制限します。

      注: 以下の例の IP アドレスは、グローバル経路指定が可能であり、例としてのみ使用できます。

```
###The following 2 filters will permit HTTP (Web browser) traffic in & out of the system.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 80 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        80 FRAGMENTS = NONE JRN = OFF

###The following 4 filters will permit FTP traffic in & out of the system.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 21 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        21 FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 20 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        20 FRAGMENTS = NONE JRN = OFF
###The following 2 filters will permit telnet traffic in & out of the system.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
```

```
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 23 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT  %
        = 23 FRAGMENTS = NONE JRN = OFF
```

f. 「**挿入 (Insert)**」メニューをオープンしてから、「**フィルター・インターフェース (Filter Interface)**」を選択します。フィルター・インターフェースを使用して PPP フィルター ID を作成し、定義したフィルター・セットを組み込みます。

1) 「**一般**」タブで、PPP フィルター ID に permitted_services を入力します。

2) 「**フィルター・セット**」タブで、フィルター・セット**services_rules** を選択してから、「**追加**」をクリックします。

3) 「OK」をクリックします。規則ファイルに以下の行が追加されます。

```
###The following statement binds (associates) the 'services_rules' filter set with the
PPP filter ID "permitted_services." This PPP filter ID
can then be applied to the physical interface associated with a PPP connection profile
or Group Access Policy.

FILTER_INTERFACE PPP_FILTER_ID = permitted_services SET = services_rules
```

g. 変更を保管し、終了します。後でこの変更を元に戻す必要が生じた場合には、文字ベース・インターフェースを使用して次のコマンドを入力します。RMVTCPTBL *ALL。このコマンドを実行すると、システム上のすべてのフィルター規則および NAT が削除されます。

h. 「**拡張 TCP/IP 設定 (Advanced TCP/IP settings)**」ダイアログでは、「**PPP フィルター ID (PPP filter identifier)**」ボックスをブランクにし、「**OK**」をクリックして終了します。後で、この接続プロファイルにではなく、グループ・アクセス・ポリシーに、この作成したばかりのフィルター ID を適用する必要があります。

2. このユーザー・グループに新規のグループ・アクセス・ポリシーを定義します。

a. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**すべてのタスク**」 > 「**リモート・アクセス・サービス**」 > 「**受信先接続プロファイル**」 > 「**グループ・アクセス・ポリシー**」を展開して、「**グループ・アクセス・ポリシー**」を選択します。

b. 「一般」ページで、「グループ・アクセス・ポリシー」に名前および説明を入力します。

c. 「TCP/IP 設定」ページで以下のようにします。

- 「**この接続に IP パケット規則を使用する (Use IP packet rules for this connection)**」を選択し、 PPP フィルター ID **permitted_services** を選択します。

d. 「**OK**」を選択し、グループ・アクセス・ポリシーを保管します。

3. このグループに関連付けられるユーザーにグループ・アクセス・ポリシーを適用します。

a. これらのダイヤルアップ接続を制御する受信側接続プロファイルを選択します。

b. 受信側接続プロファイルの「認証」ページでは、ユーザーの認証情報を含む妥当性検査リストを選択してから、「**開く**」をクリックします。

c. セールス・グループで、グループ・アクセス・ポリシーを適用させたいユーザーを選択してから、「**開く**」をクリックします。

d. 「**グループ・ポリシーをユーザーに適用する**」をクリックしてから、ステップ 2 で定義されたグループ・アクセス・ポリシーを選択します。

e. それぞれのセールス・ユーザーごとに繰り返します。

関連概念:

73 ページの『グループ・アクセス・ポリシーの構成』
「受信側接続プロファイル」の下の「**グループ・アクセス・ポリシー**」 フォルダーには、リモート・ユーザーのグループに設定する 2 地点間接続パラメーターを構成するためのオプションがあります。これは、リモート・システムが発信し、ローカル・システムが受信する 2 地点間接続にのみ適用されます。

4 ページの『グループ・ポリシー・サポート』
グループ・ポリシーのサポートにより、ネットワーク管理者はリソースを管理するためのユーザー・ベースのグループ・ポリシーを定義できます。ユーザーが Point-to-Point Protocol (PPP) またはレイヤー 2 トンネリング・プロトコル (L2TP) セッションにログオンする際に、個々のユーザーにアクセス制御ポリシーを割り当てることができます。

関連タスク:

60 ページの『接続プロファイルの作成』
システム間に PPP 接続を構成するための最初のステップは、システム上に接続プロファイルを作成することです。

75 ページの『PPP 接続への IP パケット・フィルター規則の適用』
ご使用のネットワークで IP アドレスへのユーザーまたはグループのアクセスを制限するには、パケット規則ファイルを使用することができます。

関連資料:

59 ページの『妥当性検査リスト』
妥当性検査リストは、リモート・ユーザーに関連したユーザー ID とパスワードの情報を保管するために使用されます。

56 ページの『システムの認証』
IBM i プラットフォームでの PPP 接続では、リモート・クライアントからシステムへのダイヤルインと、システムがダイヤルしている ISP または別のシステムへの接続の両方を認証するためのオプションがいくつかサポートされます。

関連情報:

IP フィルター操作とネットワーク・アドレス変換

シナリオ: L2TP を使用して論理区画間でモデムを共用する

4 つの論理区画に渡る仮想イーサネットをセットアップしたとします。選択されている論理区画の間で、外部 LAN にアクセスするために 1 つのモデムを共用できるようにするとします。

状況

あなたは、中規模の会社のシステム管理者であると想定してください。社内のコンピューター機器を新しいものに交換する場合、システム管理者は、その機会にハードウェアを合理的に使用することを考えることでしょう。まず、古い 3 台のシステムで処理していた作業を、新しいシステム 1 台でまとめて処理することにします。そのシステムに 3 つの論理区画を作成します。新しいシステムには 2793 内部モデムが搭載されています。これは、所有しているものの中で Point-to-Point Protocol (PPP) をサポートする唯一の入出力プロセッサー (IOP) です。ほかに、古い 7852–400 エレクトロニック支援モデムもあります。

ソリューション

複数のシステムおよび区画で、ダイヤルアップ接続用に同じモデムを共用して、それぞれがモデムを持たなくても良いようにすることができます。これは L2TP トンネルを使用しており、発信呼び出しが可能な L2TP プロファイルを構成している場合に可能です。ネットワーク内では、トンネルは仮想イーサネット・ネットワークと物理的なネットワーク上で実行されます。物理回線は、ネットワーク内でモデムを共用する別のシステムに接続されています。

詳細

以下の図は、このシナリオのネットワーク特性を示しています。

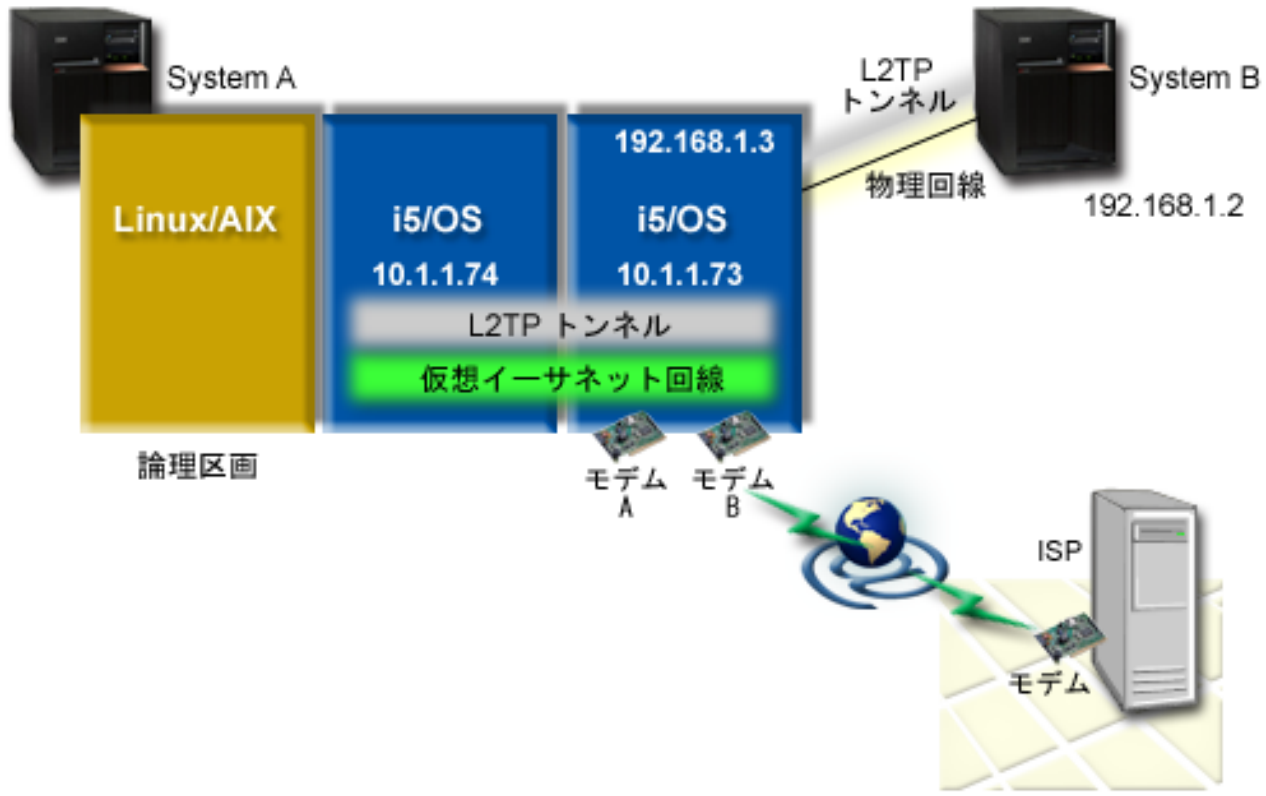


図 9. ダイヤルアップ接続用に同じモデムを共用する複数システム

前提条件

System A は以下のセットアップ要件を満たしていなければなりません。

- IBM i 5.3 以降が、ASYNC 対応モデムを所有する区画にインストールされていること。
- 区画設定が可能なハードウェア。
- IBM Navigator for i
- システム上に少なくとも 2 つの論理区画 (LPAR) を作成済みであること。モデムを所有する区画には、IBM i 5.3 以降がインストールされている必要があります。他の区画には、IBM i、Linux、または AIX® をインストールしておくことができます。このシナリオでは、区画は IBM i か Linux オペレーティング・システムを使用しています。
- 区画間での通信のために仮想イーサネットを作成しました。

関連情報:

論理区画

シナリオの詳細: L2TP を使用して論理区画間でモデムを共用する

前提条件が満たされていれば、レイヤー 2 トンネリング・プロトコル (L2TP) プロファイルの構成を開始できます。

ステップ 1: モデムの接続された区画のすべてのインターフェースに関して L2TP 終端側プロファイルを構成する:

どのインターフェースについても、終端側プロファイルを作成するには、以下の手順を実行します。

1. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**すべてのタスク**」 > 「**リモート・アクセス・サービス**」 > 「**受信先接続プロファイル**」を展開して、「**受信先接続プロファイルの作成**」をクリックします。
2. 「設定」ページで以下のオプションを選択して、「**OK**」をクリックします。
   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: L2TP (仮想回線)
   - **動作モード**: 終端側 (ネットワーク・サーバー)
   - **回線サービスのタイプ (Type of line service)**: 単一回線
3. 「**新規プロファイル - 一般**」タブで、以下のフィールドに入力します。
   - **名前**: toExternal
   - **説明**: ダイヤル呼び出しする受信側接続
   - 「**TCP でプロファイルを開始 (Start profile with TCP)**」を選択します。
4. 「**新規プロファイル - 接続**」タブで、以下のフィールドに入力してから、「**実行**」をクリックします。
   - **ローカル・トンネル・エンドポイント IP アドレス (Local tunnel endpoint IP address)**: ANY
   - **仮想回線名 (Virtual line name)**: toExternal。この回線には、物理インターフェースは関連付けられていません。仮想回線は、この PPP プロファイルのさまざまな特性を記述します。「L2TP 回線プロパティー (L2TP Line Properties)」ウィンドウが表示されたなら、「**認証**」タブをクリックして、システムのホスト名を入力します。「**OK**」をクリックして、「新規 PPP プロファイル・プロパティー (New PPP Profile Properties)」ウィンドウの「**接続 (Connection)**」タブに戻ります。
5. 「**発信呼び出しの確立を許可する (Allow out-going call establishment)**」をクリックします。「**発信呼び出しダイヤルのプロパティー (Outgoing call dial properties)**」ダイアログが表示されます。
6. 「発信呼び出しダイヤルのプロパティー (Outgoing Call Dial Properties)」ページで、回線サービスのタイプを選択します。
   - **回線サービスのタイプ (Type of line service)**: 回線プール
   - **名前 (Name)**: dialOut
   - 「**新規 (New)**」をクリックします。「**新規回線プールのプロパティー (New Line Pool Properties)**」ダイアログが表示されます。
7. 「新規回線プールのプロパティー (New Line Pool Properties)」ウィンドウで、発信呼び出しを許可する回線とモデムを選択して、「**追加**」をクリックします。これらの回線を定義する必要がある場合、「**新規回線 (New Line)**」を選択します。これらのモデムを所有する区画上のインターフェースは、この回線プールから開かれているどの回線に対しても使用を試みます。「新規回線のプロパティー (New Line Properties)」ウィンドウが表示されます。
8. 「**新規回線のプロパティー - 一般 (New Line Properties - General)**」タブで、以下のフィールドに入力します。
   - **名前 (Name)**: line1
   - **説明 (Description)**: 回線プールの最初の回線と最初のモデム (2793 内部モデム)
   - **ハードウェア・リソース (Hardware resource)**: cmn03 (通信ポート)

9. 他のすべてのタブについてはデフォルトを受け入れて、「**OK**」をクリックして、「新規回線プールのプロパティー (New Line Pool Properties)」ウィンドウに戻ります。
10. 「新規回線プールのプロパティー (New Line Pool Properties)」ウィンドウで、発信呼び出しを許可する回線とモデムを選択して、「**追加**」をクリックします。そのプールに対して 2793 モデムが選択されていることを検査します。
11. 再度「**新規回線**」を選択して、7852–400 エレクトロニック支援モデムを追加します。「新規回線のプロパティー (New Line Properties)」ウィンドウが表示されます。
12. 「**新規回線のプロパティー - 一般 (New Line Properties - General)**」タブで、以下のフィールドに入力します。
    - **名前 (Name)**: line2
    - **説明 (Description)**: 回線プールの 2 番目の回線と 2 番目のモデム (7852-400 外付けエレクトロニック支援モデム)
    - **ハードウェア・リソース (Hardware resource)**: cmn04 (V.24 ポート)
    - **フレーム (Framing)**: 非同期 (Asynchronous)
13. 「**新規回線のプロパティー - モデム**」タブで、外部モデム (7852–400) を選択して、「**OK**」をクリックして「新規回線プールのプロパティー」ウィンドウに戻ります。
14. 回線プールに追加する他の使用可能な回線を選択して、「**追加**」をクリックします。この例では、先に追加した 2 つの新しいモデムが「**プールに選択された回線 (Selected lines for pool)**」フィールドに表示されていることを確認して、「**OK**」をクリックして「発信呼び出しダイヤルのプロパティー (Outgoing Call Dial Properties)」ウィンドウに戻ります。
15. 「発信呼び出しダイヤルのプロパティー (Outgoing Call Dial Properties)」ウィンドウで、「**デフォルトの電話番号 (Default Dial Numbers)**」を入力し、「**OK**」をクリックして、「新規 PPP プロファイルのプロパティー (New PPP Profile Properties)」ウィンドウに戻ります。

    注: これらの番号は、モデムを使用する他のシステムによって頻繁に発信ダイヤルされるインターネット・サービス・プロバイダー (ISP) の番号になる可能性があります。他のシステムが電話番号に *PRIMARY または *BACKUP を指定する場合、実際にダイヤルされる番号はここで指定される番号になります。他のシステムが実際の電話番号を指定する場合、その電話番号が使用されます。
16. 「**TCP/IP 設定**」タブで、以下の値を選択します。
    - **ローカル IP アドレス**: なし
    - **リモート IP アドレス**: なし

    注: プロファイルを使用して L2TP セッションを終了させるには、システムを表すローカル IP アドレスを選択する必要があります。リモート IP アドレスについては、ご使用のシステムと同じサブネットにあるアドレス・プールを選択できます。すべての L2TP セッションは、このプールから IP アドレスを取得します。
17. 「**認証**」タブでは、すべてデフォルトを使用します。

これで、モデムを所有する区画での L2TP 終端側プロファイルの構成は終了です。次のステップは、10.1.1.74 に対する L2TP リモート・ダイヤル、発信元プロファイルの構成です。

関連資料:

67 ページの『複数接続プロファイル・サポート』
複数接続をサポートする 2 地点間接続プロファイルを使うと、1 つの接続プロファイルで、多数のデジタル、アナログ、または L2TP 呼び出しを処理することができます。

ステップ 2: 10.1.1.74 に対する L2TP 発信元プロファイルの構成:

以下の手順は、レイヤー 2 トンネリング・プロトコル (L2TP) 発信元プロファイルを作成するためのものです。

1. 10.1.1.74 上の IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**すべてのタスク**」 > 「**リモート・アクセス・サービス**」 > 「**発信元接続プロファイル**」を展開して、「**発信元接続プロファイルの作成**」をクリックします。
2. 「設定」ページで以下のオプションを選択して、「**OK**」をクリックします。
   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: L2TP (仮想回線)
   - **動作モード**: リモート・ダイヤル
   - **回線サービスのタイプ (Type of line service)**: 単一回線
3. 「**一般**」タブで、以下のフィールドに入力します。
   - **名前 (Name)**: toModem
   - **説明 (Description)**: モデムの接続された区画への発信元接続
4. 「**接続**」タブで、以下のフィールドに入力します。

   仮想回線名 (Virtual line name): toModem。この回線には、物理インターフェースは関連付けられていません。仮想回線は、この PPP プロファイルのさまざまな特性を記述します。「L2TP 回線プロパティー (L2TP Line Properties)」ウィンドウが表示されます。
5. 「**一般**」タブで、仮想回線の説明を入力します。
6. 「**認証**」タブでは、区画のローカル・ホスト名を入力し、「**OK**」をクリックして、「接続」ページに戻ります。
7. 「**リモート電話番号 (Remote telephone numbers)**」フィールドに、*PRIMARY と *BACKUP を追加します。これにより、プロファイルはモデムの接続された区画の終端側プロファイルと同じ電話番号を使用できるようになります。
8. 「**リモート・トンネル・エンドポイント・ホスト名または IP アドレス (Remote tunnel endpoint host name or IP address)**」フィールドに、リモート・トンネル・エンドポイント IP アドレス (10.1.1.73) を入力します。
9. 「**認証**」タブで、「**リモート・システムがこの iSeries サーバーの識別を検査することを許可**」を選択します。
10. 使用する認証プロトコルで、「**暗号化されたパスワード (CHAP-MD5) が必要 (Require encrypted password (CHAP-MD5))**」を選択します。デフォルトでは、「**拡張可能認証プロトコルを許可 (Allow extensible authentication protocol)**」も選択されます。

    注: このプロトコルは、ダイヤル先のシステムが使用するプロトコルと一致する必要があります。
11. ユーザー名とパスワードを入力します。

    注: ユーザー名とパスワードは、ダイヤル先のシステムで有効なユーザー名およびパスワードにする必要があります。
12. 「**TCP/IP IPv4 設定**」タブに移動して、以下の必須フィールドを確認します。
    - **ローカル IP アドレス**: リモート・システムに割り当てられた値
    - **リモート IP アドレス**: リモート・システムに割り当てられた値
    - **経路指定 (Routing)**: 追加の経路指定は必要がありません

13. 「**OK**」をクリックして PPP プロファイルを保管します。

ステップ 3: 192.168.1.2 に対する L2TP リモート・ダイヤル・プロファイルの構成:

リモート・トンネル・エンドポイントを 192.168.1.3 (System B の接続先物理インターフェース) に変更した上で ステップ 2 を繰り返すことにより、192.168.1.2 のレイヤー 2 トンネリング・プロトコル (L2TP) リモート・ダイヤル・プロファイルを構成することができます。

注: これらは、例を示すための架空の IP アドレスです。

ステップ 4: 接続のテスト:

両方のシステムの構成が終了したら、接続性をテストして、システムがモデムを共用して外部ネットワークと通信できるかどうかを確認する必要があります。

1. レイヤー 2 トンネリング・プロトコル (L2TP) 終端側プロファイルがアクティブであることを確認します。
   a. 10.1.1.73 上の IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**リモート・アクセス・サービス**」を展開して、「**受信先接続プロファイル**」をクリックします。
   b. 右側の画面領域で、必要なプロファイル (toExternal) を探して、その「**状況 (Status)**」フィールドが「アクティブ (Active)」であることを確認します。「アクティブ (Active)」でない場合、プロファイルを右クリックして、「**開始 (Start)**」を選択します。
2. 10.1.1.74 のリモート・ダイヤル・プロファイルを開始します。
   a. 10.1.1.74 上の IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**リモート・アクセス・サービス**」を展開して、「**発信元接続プロファイル**」をクリックします。
   b. 右側の画面領域で、必要なプロファイル (toModem) を探して、その「**状況 (Status)**」フィールドが「アクティブ (Active)」であることを確認します。「アクティブ (Active)」でない場合、プロファイルを右クリックして、「**開始 (Start)**」を選択します。
3. System B でリモート・ダイヤル・プロファイルを開始します。
   a. 192.168.1.2 上の IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**リモート・アクセス・サービス**」を展開して、「**発信元接続プロファイル**」をクリックします。
   b. 右側の区画で、作成したプロファイルを探して、その「**状況 (Status)**」フィールドが「アクティブ (Active)」であることを確認します。「アクティブ (Active)」でない場合、プロファイルを右クリックして、「**開始 (Start)**」を選択します。
4. 可能であれば、これまでダイヤルしていたインターネット・サービス・プロバイダー (ISP) または他の宛先に対して ping して、両方のプロファイルがアクティブであることを確認します。 10.1.1.74 と 192.168.1.2 の両方からの ping を試行します。
5. 別の方法として、接続状況を調べることもできます。
   a. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**リモート・アクセス・サービス**」を展開して、「**発信元接続プロファイル**」をクリックします。
   b. 右側の区画で、作成したプロファイルを右クリックして、「**接続**」を選択します。「接続状況 (Connection Status)」ウィンドウで、いずれのプロファイルがアクティブ、非アクティブ、接続中、およびそれ以外であるかを確認できます。

シナリオ: イーサネット装置サーバーとのダイヤルアップ接続の確立

ほとんどの IBM i 区画が、イーサネット接続を介してネットワークに接続されています。ただし、一部のリモート・アプリケーションまたはサービスは、ダイヤルアップ接続を介してのみ使用可能です。イーサネ

| ット装置サーバー (イーサネット・シリアル・サーバーまたはイーサネット端末サーバーとしても知られています) には、モデムを接続できるイーサネット・ポートおよびシリアル・ポートの両方があります。これらのポートを使用して、イーサネット接続のみを持つシステムは、イーサネット装置サーバー上のモデムにアクセスして、ダイヤルアップ接続を確立することができます。

状況

会社の企業アプリケーションの 1 つが、PPP ダイヤルアップ接続を使用してのみアクセス可能なリモート・システムにホストされています。IBM i には、ローカル・ネットワークへのイーサネット接続がありますが、ダイヤルアップ接続用の WAN カードがありません。

ソリューション

ローカル・ネットワーク上のイーサネット装置サーバーを使用して、ダイヤルアップ接続を確立することができます。イーサネット装置サーバーにアクセスして、リモート・システムへの PPP 接続を確立するには、IBM i で Point-to-Point Protocol (PPP) 発信元プロファイルを作成する必要があります。

構成の例

IBM Navigator for iからサンプル構成をセットアップするには、以下の手順を実行します。

1. システムで、発信元接続プロファイルを構成します。

   必ず、次の情報を選択してください。
   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: 交換回線
   - **動作モード**: ダイヤル
   - **リンク構成**: 単一回線 (Single line)
2. 「新規 2 地点間プロファイルのプロパティー」の「一般」ページで、発信元プロファイルの名前と記述を入力します。
3. 「**接続**」をクリックして、「接続」ページを開きます。適切な PPP 回線名を選択するか、新しい名前を入力し、「**開く**」をクリックして新規の PPP 回線を作成します。

   注: イーサネット装置サーバーにアクセスできる PPP 回線は、**CRTLINPPP** CL コマンドを使用して RSRCNAME(*ETHDEVSVR) を指定することで作成することもできます。

   a. 新規回線のプロパティーの「一般」ページで、イーサネット装置サーバーを使用するためのオプションを選択します。イーサネット装置サーバーにアクセスするために使用する IP アドレスおよびポートを構成します。

   b. 「**OK**」をクリックして「新規 2 地点間プロファイルのプロパティー」ページに戻ります。

   c. 「**追加**」をクリックして、アプリケーションをホストしているリモート・システムに接続するためにダイヤルする電話番号を入力します。

   d. 「**認証**」をクリックして「認証」ページを開き、「**このシステムの ID 検査を行うことをリモート・システムに許可する**」を選択します。認証プロトコルを選択し、必要なユーザー名やパスワードの情報を入力します。
4. 「**TCP/IP IPv4 設定**」をクリックして、「TCP/IP IPv4」ページを開きます。通常、デフォルト設定が許容可能です。必要な変更を行います。
5. 「**TCP/IP IPv6 設定**」をクリックして、「TCP/IP IPv6」ページを開きます。通常、デフォルト設定が許容可能です。必要な変更を行います。

6. 「**DNS**」をクリックして「DNS」(ドメイン・ネーム・システム) ページを開き、ISP が提供する DNS サーバーの IP アドレスを入力します。
7. 「**OK**」をクリックしてプロファイルを完成させます。

接続プロファイルを使用してリモート・システムに接続する場合は、IBM Navigator for i から接続プロファイルを右クリックして、「**開始**」を選択します。状況が「アクティブ」に変われば接続は正常です。最新表示を行って表示される状況を更新してください。

関連概念:

『PPP の計画』
Point-to-Point Protocol (PPP) には、PPP 接続の作成と管理が含まれます。

関連タスク:

60 ページの『接続プロファイルの作成』
システム間に PPP 接続を構成するための最初のステップは、システム上に接続プロファイルを作成することです。

PPP の計画

Point-to-Point Protocol (PPP) には、PPP 接続の作成と管理が含まれます。

関連資料:

22 ページの『シナリオ: リモート・ダイヤルイン・クライアントをシステムに接続する』
在宅勤務者やモバイル・クライアントなどのリモート・ユーザーは、会社のネットワークにアクセスしなければならなくなることがよくあります。こうしたダイヤルイン・クライアントは、Point-to-Point Protocol (PPP) を使用してシステムにアクセスできます。

25 ページの『シナリオ: モデムを使用してオフィスの LAN をインターネットに接続する』
普通、管理担当者は、従業員がインターネットにアクセスできるように、オフィス・ネットワークをセットアップします。管理者は、システムからインターネット・サービス・プロバイダー (ISP) に接続するために、モデムを使用できます。 LAN に接続された PC クライアントは、IBM i オペレーティング・システムをゲートウェイとして使用することにより、インターネット通信が可能です。

81 ページの『リモート・アクセス・サービスの関連情報』
IBM Redbooks の資料および Web サイトには、リモート・アクセス・サービスのトピック・コレクション関連の情報が含まれています。以下の PDF ファイルは、どれも表示または印刷することができます。

43 ページの『シナリオ: イーサネット装置サーバーとのダイヤルアップ接続の確立』
ほとんどの IBM i 区画が、イーサネット接続を介してネットワークに接続されています。ただし、一部のリモート・アプリケーションまたはサービスは、ダイヤルアップ接続を介してのみ使用可能です。イーサネット装置サーバー (イーサネット・シリアル・サーバーまたはイーサネット端末サーバーとしても知られています) には、モデムを接続できるイーサネット・ポートおよびシリアル・ポートの両方があります。これらのポートを使用して、イーサネット接続のみを持つシステムは、イーサネット装置サーバー上のモデムにアクセスして、ダイヤルアップ接続を確立することができます。

ソフトウェアおよびハードウェア要件

Point-to-Point Protocol (PPP) 環境には、PPP をサポートする 2 つ以上のコンピューターが必要です。それらコンピューターの 1 つである IBM i プラットフォームは、発信元と受信側のいずれにもなります。

リモート・システムがアクセスできるようにするため、システムは以下の要件を満たしている必要があります。

- IBM Navigator for i

- 次の 2 つの接続プロファイルのうちのいずれか
  - アウトバウンド PPP 接続を処理するための発信元接続プロファイル
  - インバウンド PPP 接続を処理するための受信側接続プロファイル
- インストール済みのアダプター

  次のアダプターの中から 1 つを選択することができます。
  - 2742*: 2 回線 IOA。
  - 2743/2760/2838/2849/287F/5700/5701/5706/5707/573A/5767/576A: PPPoE 接続用またはイーサネット装置サーバーを使用するためのイーサネット・アダプター。
  - 2793/576C: 2 ポート WAN IOA (ポート 1 には V.92 組み込みモデムが、ポート 2 には標準通信インターフェースがある)。ポート 2 を使用するには、適切なケーブルを備えた外付けモデムが必要です。
  - 2805: 4 ポート WAN IOA (V.92 アナログ・モデム内蔵)。
  - 57D4*: 2 回線 IOA

  * これらのアダプターでは、外付けモデムおよび互換性のあるケーブルが必要です。
- RFC 2217 をサポートする外付けのイーサネット装置サーバー。これらのサーバーは、イーサネット・シリアル・サーバーまたはイーサネット端末サーバーと呼ばれる場合があります。これらのサーバーには、モデムを接続できるイーサネット・ポートおよび 1 つ以上のシリアル・ポートがあります。
- インターネットに接続しようと考えている場合、インターネット・サービス・プロバイダー (ISP) のダイヤルアップ・アカウントを用意する必要があります。必要な電話番号とインターネット接続のための情報を ISP から入手する必要があります。

関連概念:

51 ページの『イーサネット装置サーバー』
イーサネット装置サーバー (イーサネット・シリアル・サーバーまたはイーサネット端末サーバーとしても知られています) には、モデムを接続できるイーサネット・ポートおよびシリアル・ポートの両方があります。

関連資料:

3 ページの『接続プロファイル』
Point-to-Point 接続プロファイルは、特定の Point-to-Point Protocol (PPP) 接続のパラメーターおよびリソースのセットを定義します。これらのパラメーターを使用するプロファイルを開始すると、ダイヤルアウト (発信) または PPP 接続の listen (受信) ができます。

50 ページの『モデム』
Point-to-Point Protocol (PPP) 接続では、外付けモデムと内蔵モデムの両方を使用できます。

接続の選択肢

Point-to-Point Protocol (PPP) は、シリアル 2 地点間リンクを介してデータグラムを送信することができます。

PPP は、2 地点間通信を標準化することによって、複数の取引先の装置と複数のプロトコルの相互接続を可能にしています。 PPP データ・リンク層は、同期と非同期の両方の 2 地点間通信リンクのデータグラムをカプセル化するのに、ハイレベル・データ・リンク制御 (HDLC) のようなフレームを使用します。

PPP は広い範囲のリンク・タイプをサポートするのに対し、シリアル・ライン・インターネット・プロトコル (SLIP) がサポートするのは非同期のリンク・タイプだけです。 SLIP は一般に、アナログ・リンクに

採用されます。ローカル電話会社の提供する、従来の遠隔通信サービスの機能やコストの規模は、広がっています。これらのサービスでは、顧客と中央局の間で、現存する電話会社の音声ネットワーク機構が使用されます。

PPP リンクは、ローカル・ホストとリモート・ホストの間の物理接続を確立します。接続されるリンクには、専用帯域幅があります。また、多様なデータ速度やプロトコルもあります。 PPP リンクでは、以下のような接続の選択肢の中から選択することができます。

アナログ電話回線

モデムを使用して専用回線や交換回線にデータを送信するアナログ接続は、2 地点間スケールの最下部に位置します。

専用回線は、指定された 2 つのロケーション間の全時間接続ですが、交換回線は、標準の音声電話回線です。現在の最も高速なモデムは、圧縮なしの速度 56 kbps で作動します。しかし、無条件音声帯域電話回線の信号対ノイズ比率を考慮に入れると、この速度には至らないこともよくあります。

モデムの製造業者が主張する、高いビット/秒 (bps) 率は、通常、それらのモデムが使用するデータ圧縮 (CCITT V.42bis) アルゴリズムによるものです。 V.42bis には、データ・ボリュームを 4 分の 1 に縮小する潜在能力がありますが、圧縮はデータに依存しているため、50 % に達することさえめったにありません。データが既に圧縮されたり暗号化されたりしている場合、 V.42bis を適用するとデータが大きくなることさえあります。 X2 や 56Flex は、アナログ電話回線の bps 率を 56 kbps に伸ばします。これは、ハイブリッド・テクノロジーであり、 PPP リンクの一端をデジタルに、もう一方の端をアナログにする必要があります。さらに、56 kbps が適用されるのは、データをリンクのデジタル終端からアナログ終端へ移動するときだけです。このテクノロジーは、リンクのデジタル終端とハードウェアを自分のロケーションに備えている ISP に接続する場合に最適です。通常、V.24 アナログ・モデムへは、RS-232 シリアル・インターフェースを介し、非同期プロトコルを用いて、最高で 115.2 kbps の速度で接続することができます。

V.90 標準により、K56flex/x2 の互換性の問題は排除されました。 V.90 標準は、モデム業界の x2 と K56flex の関係者による交渉の結果です。 V.90 テクノロジーは、公衆交換電話ネットワークをデジタル・ネットワークと見なすことによって、インターネットからコンピューターまでのデータの速さを 56 kbps にまで高めています。V.90 テクノロジーは、アナログ・モデムが行うようにデータを変調するのではなく、それをデジタル式にエンコードするという点で、その他の標準とは異なっています。データ転送は非対称的な方式であるため、アップストリーム送信 (ほとんどの場合、必要な帯域幅がより小さい、コンピューターから中央側へのキー・ストロークやマウスによるコマンド) は、引き続き、最大 33.6 kbps の従来の速度で流れます。モデムから送信されるデータは、V.34 標準を鏡映するアナログ送信として送信されます。V.90 の最高速度は、ダウンストリーム・データ送信でのみ利用されます。

V.92 標準は、アップストリーム速度を 48 kbps にまで上げることにより、V.90 を改善したものとなっています。加えて、ハンドシェーク・プロセスが改善されたために、接続時間を短くすることができ、保留機能をサポートするモデムは、電話回線が、着信呼び出しを受け入れる、あるいは、呼び出し待機を使用する間にも、接続したままでいることができます。

PPP 接続の L2TP (トンネリング) サポート

レイヤー 2 トンネリング・プロトコル (L2TP) は、Point-to-Point Protocol (PPP) を拡張するトンネリング・プロトコルであり、要求元の L2TP クライアント (L2TP アクセス・コンセントレーター (LAC)) とターゲットの L2TP サーバー・エンドポイント (L2TP Network Server (LNS)) とをつなぐリンク層トンネルをサポートします。

レイヤー 2 トンネリング・プロトコル

レイヤー 2 トンネリング・プロトコル (L2TP) トンネルを使用すると、ダイヤルアップ・プロトコルの終端のロケーションと、ネットワークへのアクセスが提供されるロケーションを分離できます。このため、L2TP は*仮想 PPP* とも呼ばれます。

以下の図は、3 種類の L2TP のトンネリングのインプリメンテーション例を示しています。

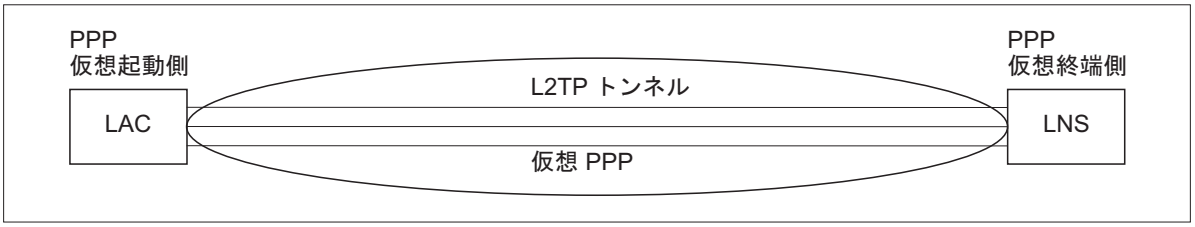


図 10. PPP 仮想起動側または PPP 仮想終端側

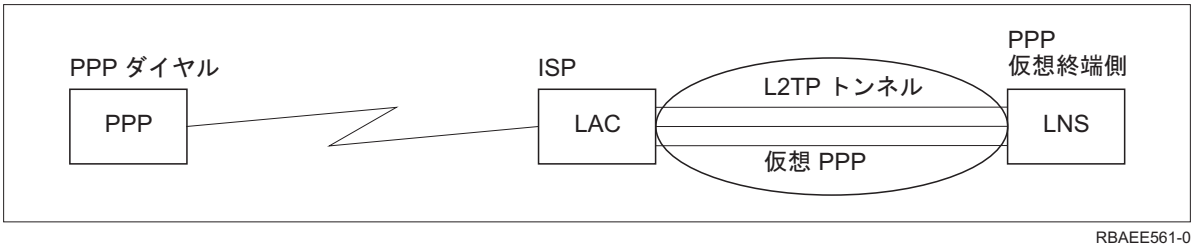


図 11. PPP ダイヤル起動側または PPP 仮想終端側

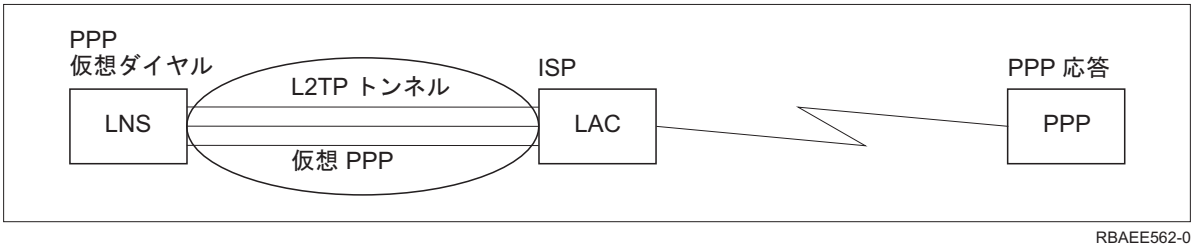


図 12. PPP 仮想ダイヤルまたは PPP 仮想応答

L2TP プロトコルは、Request for Comment (RFC) 標準 RFC-2661 として文書化されています。 L2TP トンネルは、PPP セッション全体にわたることができますが、 2 セグメント・セッションの 1 セグメントにおいてのみ使用することもできます。これは、以下のような 4 つの異なるトンネル伝送モデルに代表されます。

関連情報:

シナリオ: L2TP 任意トンネルを IPSec で保護する

RFC Editor

任意トンネル:

任意トンネル・モデルでは、トンネルは、ユーザーが、通常はレイヤー 2 トンネリング・プロトコル (L2TP) 対応のクライアントを使用して作成します。

その結果として、ユーザーは L2TP パケットをインターネット・サービス・プロバイダー (ISP) に送信し、それらの L2TP パケットは、そこから L2TP ネットワーク・サーバー (LNS) に転送されます。任意トンネリングでは、ISP による L2TP のサポートは不要であり、L2TP トンネルの起動側は、リモート・クライアントと同じシステム上にあります。このモデルの場合、トンネルは、L2TP クライアントから LNS までの Point-to-Point Protocol (PPP) セッション全体にわたります。

必須トンネル・モデル - 着信呼び出し:

必須トンネル・モデル - 着信呼び出しでは、ユーザーがアクションを起こさなくてもトンネルが作成され、ユーザーは何ら選択できるものはありません。

その結果として、ユーザーは Point-to-Point Protocol パケットをインターネット・サービス・プロバイダー (ISP) に送信します (レイヤー 2 トンネリング・プロトコル (L2TP) アクセス・コンセントレーター (LAC))。 ISP は L2TP のパケットをカプセル化し、トンネルを通じてそれらを L2TP ネットワーク・サーバー (LNS) に送信します。必須トンネル伝送の場合は、ISP が L2TP 対応でなければなりません。このモデルの場合、トンネルの範囲は、ISP と LNS の間の PPP セッションのセグメントだけです。

必須トンネル・モデル - リモート・ダイヤル:

必須トンネル・モデル - リモート・ダイヤルでは、ホーム・ゲートウェイ (L2TP ネットワーク・サーバー (LNS)) がインターネット・サービス・プロバイダー (ISP) (LAC) へのトンネルを開始し、ISP に、Point-to-Point Protocol (PPP) 応答クライアントへのローカル呼び出しを実行するよう指示します。

このモデルは、リモート PPP 応答クライアントが ISP との間に永続的な確立済みの電話番号を所有している場合に使用することを意図しています。インターネットにおける所在が確立されている会社が、ダイヤルアップ・リンクを必要とするリモート・オフィスへの接続を確立しようとする場合は、このモデルの使用が期待されます。このモデルでは、トンネルは、LNS と ISP の間の PPP セッションのセグメントにしか及びません。

L2TP マルチホップ接続:

レイヤー 2 トンネリング・プロトコル (L2TP) マルチホップ接続は、クライアント L2TP アクセス・コンセントレーター (LAC) や L2TP ネットワーク・サーバー (LNS) の代わりに L2TP トラフィックの宛先変更を実行するための 1 つの手段となります。

マルチホップ接続は、L2TP のマルチホップ・ゲートウェイ (L2TP の終端側プロファイルと起動側プロファイルをリンクするシステム) を使用して確立します。マルチホップ接続を確立するため、L2TP マルチホップ・ゲートウェイは、 LAC のセットへ向かう LNS として、また、提供されている LNS へ向かう LAC としての両方の役割を担います。クライアント LAC から L2TP マルチホップ・ゲートウェイへのトンネルが確立され、 L2TP マルチホップ・ゲートウェイとターゲット LNS との間にもう 1 つのトンネルが確立されます。クライアント LAC からの L2TP トラフィックは、 L2TP マルチホップ・ゲートウェイによってターゲット LNS に宛先変更され、ターゲット LNS からのトラフィックは、クライアント LAC に宛先変更されます。

PPP 接続のための PPPoE (DSL) サポート

デジタル加入者回線 (DSL) は、カスタマーの所在地とインターネット・サービス・プロバイダー (ISP) を結ぶ既存のメタル (銅線) 電話ケーブルを使用して、より広い帯域幅を取得するのに使用されるテクノロジーのクラスのことです。

DSL は、単一の銅線電話線で、音声および高速データ・サービスを同時に行うことができます。モデム速度は、各種の圧縮その他の技法を使用することで、次第に速くなっているものの、現在の最高速度 (56 kbps) で、このテクノロジーの理論上の限界が近づいています。 DSL テクノロジーを使用すると、対より線を介して、中央オフィスから住宅、学校、または業務地への非常に高速の通信を提供できます。地域によっては、2 Mbps もの速度が可能です。PPP は、通常、ダイヤルアップ・モデム接続のようなシリアル通信で使用されます。多くの DSL インターネット・サービス・プロバイダーは、現在、PPP over Ethernet (PPPoE) を使用しています。これは、ログインおよびセキュリティー機能が優れているためです。

DSL モデム は、銅線電話回線のいずれかの終端に配置されて、コンピューター (または LAN) が DSL 接続でインターネットに接続できるようにする装置です。ダイヤルアップ接続とは異なり、通常は、専用電話回線を必要としません (POTS スプリッター・ボックスで、回線を同時に共用するようにします)。 DSL モデムは、従来のアナログ・モデムに類似しているものの、スループットはかなり高くなります。

接続機器

システムは、さまざまな装置を使用して、Point-to-Point Protocol (PPP) 接続を処理します。

以下の装置が、PPP 環境で使用できる通信機器の種類です。

- モデム
- イーサネット装置サーバー
- イーサネット・アダプター (PPPoE 接続用)

モデム

Point-to-Point Protocol (PPP) 接続では、外付けモデムと内蔵モデムの両方を使用できます。

モデムで使用されるコマンド・セットは、たいていモデムの資料で説明されています。これらのコマンドは、モデムのリセットや初期設定を行ったり、リモート・システムの電話番号をダイヤルするようモデムに指示したりするのに用いられます。モデム・モデルは、それぞれ別個の初期化コマンド・ストリングを持つので、これらは、PPP 接続プロファイルで使用する前に定義する必要があります。内部モデムの場合、このモデム・ストリングは既に定義済みで、使用可能です。

システムには、事前定義された多くのモデム・モデルがありますが、IBM Navigator for i を通して新しいモデルを定義することも可能です。既存の定義は、新しいタイプを定義する際の基本とすることができます。モデムが使用しているコマンドが分からない場合や、モデムの資料が手に入らない場合は、 Generic Hayes モデム定義を開始してください。事前定義されている定義を変更することはできませんが、既存の初期化コマンドやダイヤル・ストリングに、追加のコマンドを加えることは可能です。

PPP 接続を確立するには、システムに付属しているエレクトロニック支援モデムを使用することができます。旧システムにおいて、エレクトロニック支援モデムは IBM 7852-400 外付けモデムでした。このモデムは、MultiTech MT5600BA-V92 V.92 Data/Fax World Modem で置き換えられました。新しいシステムでは、576C、2793、またはサポートされるその他の内蔵モデムをエレクトロニック支援モデムとして使用できます。

関連資料:

45 ページの『ソフトウェアおよびハードウェア要件』
Point-to-Point Protocol (PPP) 環境には、PPP をサポートする 2 つ以上のコンピューターが必要です。それらコンピューターの 1 つである IBM i プラットフォームは、発信元と受信側のいずれにもなります。

イーサネット装置サーバー

イーサネット装置サーバー (イーサネット・シリアル・サーバーまたはイーサネット端末サーバーとしても知られています) には、モデムを接続できるイーサネット・ポートおよびシリアル・ポートの両方があります。

イーサネット接続のみを持つ IBM i システムは、イーサネット装置サーバーとそのモデムにアクセスして、ダイヤルアップ接続を確立することができます。IBM i は、RFC 2217 をサポートするイーサネット装置サーバーのみにアクセスできます。

関連資料:

45 ページの『ソフトウェアおよびハードウェア要件』
Point-to-Point Protocol (PPP) 環境には、PPP をサポートする 2 つ以上のコンピューターが必要です。それらコンピューターの 1 つである IBM i プラットフォームは、発信元と受信側のいずれにもなります。

IP アドレス処理

Point-to-Point Protocol (PPP) 接続では、接続プロファイルのタイプに応じて、IP アドレスを管理するため異なるいくつかのセットのオプションを使用できるようになっています。

- DHCP は、ご使用のネットワークの IP アドレス割り当てを集中管理できます。ここで、ネットワークに DHCP サービスをセットアップおよび管理する方法を調べてください。 動的ホスト構成プロトコルを参照してください。
- DNS を使用すると、ホスト名および関連する IP アドレスを管理できます。ここで、ネットワークに DNS サービスをセットアップおよび管理する方法を調べてください。 DNS を参照してください。
- BOOTP は、クライアント・ワークステーションをご使用のシステムに関連付け、これらに IP アドレスを割り当てるのに使用されます。ここで、ネットワークに BOOTP サービスをセットアップおよび管理する方法を調べてください。 ブートストラップ・プロトコルを参照してください。

関連資料:

19 ページの『シナリオ: システムを PPPoE アクセス・コンセントレーターに接続する』
多くのインターネット・サービス・プロバイダー (ISP) が、Point-to-Point Protocol over Ethernet (PPPoE) を使用してデジタル加入者回線 (DSL) 上での高速インターネット・アクセスを提供しています。システムをそれらの ISP に接続することにより、Point-to-Point Protocol (PPP) のメリットを保ったまま、高帯域幅の接続が提供されます。

IP パケット・フィルター

IP パケット・フィルターは、個々のユーザーがネットワークにログオンしたときに利用できるサービスを制限します。

パケット・フィルター操作では、宛先の IP アドレスかポート、あるいはその両方に基づいて、アクセスを許可したり、拒否したりできます。それぞれが独自の固有な PPP フィルター ID を持つパケット・フィルター規則のセットを複数定義することにより、それぞれ異なるポリシーが課されます。パケット・フィルター規則は、特定の受信側接続プロファイルに対して割り当てることもできますし、フィルター規則を適用するグループ・ポリシーを使用することによって、そのカテゴリーのユーザーに対して割り当てることもできます。パケット・フィルター規則自体は、PPP ではなく、System i® ナビゲーター IP パケット規則の下で定義されています。

L2TP 接続の場合、 IPSec フィルターを持つ VPN を使用してネットワーク・トラフィックを保護しなければなりません。

関連資料:

19 ページの『シナリオ: システムを PPPoE アクセス・コンセントレーターに接続する』
多くのインターネット・サービス・プロバイダー (ISP) が、Point-to-Point Protocol over Ethernet (PPPoE) を使用してデジタル加入者回線 (DSL) 上での高速インターネット・アクセスを提供しています。システムをそれらの ISP に接続することにより、Point-to-Point Protocol (PPP) のメリットを保ったまま、高帯域幅の接続が提供されます。

関連情報:

IP フィルター操作とネットワーク・アドレス変換

仮想プライベート・ネットワーキング (VPN)

IP アドレス管理の戦略

PPP 接続プロファイルを構成する前に、ご使用の IP アドレス管理の戦略に精通していなければなりません。この戦略は、認証戦略、セキュリティーの考慮事項、および TCP/IP 設定を含め、構成プロセスで数多くの決定に影響を与えます。

IBM i 7.1 以降、PPP は IPv4 アドレスと IPv6 アドレスの両方をサポートできるようになりました。PPP 接続プロファイルは、IPv4 のみ使用可能にするか、IPv6 のみ使用可能にするか、または IPv4 と IPv6 を両方とも使用可能にすることができます。デフォルトでは、PPP 接続プロファイルで IPv4 と IPv6 が両方とも使用可能になります。

注: 物理 PPP 接続の確立 (ダイヤルまたは応答など) と LCP 折衝および認証は、IPv4 と IPv6 の両方で同じです。

IPv4 アドレス管理

PPP リンクの両端で IPv4 を構成して使用可能にするには、IP 制御プロトコル (IPCP) を使用します。IPCP および IPv4 アドレス割り当てに関連したオプションは、接続プロファイルの「TCP/IP IPv4 設定」セクションにあります。

発信元接続プロファイル

通常、発信元プロファイルに定義されるローカルとリモートの IPv4 アドレスは、*「リモート・システムによる割り当て」*と定義されます。これによって、接続で使用される IP アドレスをリモート・システムの管理者が制御できるようになります。多くの ISP が追加料金で固定 IP アドレスを提供していますが、インターネット・サービス・プロバイダー (ISP) へのほとんどすべての接続はこの方法で定義されます。

ローカルまたはリモートの IP アドレスの固定 IP アドレスを定義する場合は、リモート・システムが、定義する IP アドレスを受け入れるように定義されていなければなりません。ローカル IP アドレスを固定 IP アドレスとして定義し、リモート・アドレスがリモート・システムによって割り当てられるよう定義するのが、1 つの典型的な設定です。接続するシステムを同様の方法で定義して、接続の際、その 2 つのシステムが、リモート・システムの IP アドレスを知る手段として、互いの IP アドレスを交換するようにすることができます。これは、1 つのオフィスが一時的な接続のために他のオフィスを呼び出す場合には便利かもしれません。

もう 1 つの考慮事項は、IP アドレスのマスカレードを使用可能にするかどうかです。例えば、システムが ISP を介してインターネットに接続している場合は、システムの背後で接続されているネットワークもインターネットにアクセスすることができます。基本的にシステムは、ISP が割り当てるローカル IP アドレス

の背後のネットワーク上にあるシステムの IP アドレスを隠して、すべての IP トラフィックがシステムからのものであるように見せかけます。また、LAN 上のシステムと使用中のシステムの両方に対する、ルーティングに関連した付加的な考慮事項もあります。 LAN 上のシステムのインターネット・トラフィックは使用中のシステムに送信されるようにする必要があり、使用中のシステムでは、「**リモート・システムをデフォルト経路として追加**」ボックスを有効にする必要があります。

受信側接続プロファイル

受信側接続プロファイルには、IPv4 アドレスの考慮事項やオプションが発信元接続プロファイルよりも多く存在します。IP アドレスの構成方法は、ご使用のネットワークでの IP アドレス管理プラン、この接続に固有のパフォーマンスおよび機能の要件、およびセキュリティー・プランにより異なります。

ローカル IP アドレス

単一の受信側プロファイルでは、固有 IP アドレスを定義するか、システム上の既存のローカル IP アドレスを使用することによって、PPP 接続の終端を識別できます。同時に複数の接続をサポートするよう定義されている受信側プロファイルには、既存のローカル IP アドレスを使用しなければなりません。存在している有効なローカル IP アドレスがない場合は、この目的で仮想 IP アドレスを作成することができます。

リモート IP アドレス

リモート IP アドレスを PPP クライアントに割り当てるのに使用できるオプションは数多くあります。以下のオプションは、受信側接続プロファイルの「TCP/IP」ページで指定できます。

注: リモート・システムが、LAN の一部と見なされるようにしたい場合には、 IP アドレス・ルーティングを構成する際に、LAN 接続システム用の IP アドレス範囲内で IP アドレスを指定し、 IP 転送がこの接続プロファイルとシステムの両方で使用可能にされていることを確認してください。

表 8. 受信側接続プロファイルの IPv4 アドレス割り当てオプション

オプション	説明
固定 IP アドレス	リモート・ユーザーがダイヤルインするときに与えられる単一の IP アドレスを定義します。これは、ホスト専用の IP アドレス (サブネット・マスクは 255.255.255.255) で、単一接続の受信側プロファイルにのみ有効です。
アドレス・プール	開始 IP アドレスと、追加で定義できる IP アドレスの数量範囲を指定します。接続するユーザーは、この定義の範囲内で、固有 IP アドレスを与えられます。これは、ホスト専用の IP アドレス (サブネット・マスクは 255.255.255.255) で、多重接続の受信側プロファイルにのみ有効です。
RADIUS	リモート IP アドレスとそのサブネット・マスクは、Radius サーバーが決定します。これは、以下のものが定義されている場合にのみ有効です。 • リモート・アクセス・サーバーのサービス構成で、認証と IP アドレッシングのための Radius サポートが使用可能になっている。 • 認証が、受信側接続プロファイルで使用可能となり、 Radius によってリモートで認証されるように定義されている。
DHCP	リモート IP アドレスは、DHCP サーバーにより直接、あるいは DHCP リレーにより間接的に決定できます。これは、リモート・アクセス・サーバーのサービス構成で、 DHCP サポートが使用可能になっている場合にのみ有効です。これは、ホスト専用の IP アドレス (サブネット・マスクは 255.255.255.255) です。

表 8. 受信側接続プロファイルの IPv4 アドレス割り当てオプション (続き)

オプション	説明
リモート・システムのユーザー ID を基にする	リモート IP アドレスは、リモート・システムが認証されたときにこれに定義されたユーザー ID によって決まります。これによって管理者は、ダイヤルインするユーザーに別々のリモート IP アドレス (とそのサブネット・マスク) を割り当てることができます。これはまた、これらそれぞれのユーザー ID に対して付加的な経路を定義し、既知のリモート・ユーザーに合わせて環境を調整することを可能にしています。この機能が適切に働くようにするには、認証を使用可能にする必要があります。
リモート・システムのユーザー ID に基づいて追加の IP アドレスを定義	リモート・システムのユーザー ID を基にして IP アドレスを定義する場合は、このオプションを使用することができます。IP アドレスの割り当て方式として「**ユーザー ID を基にする**」が定義されている場合は、このオプションが自動的に選択され (使用され) ます。このオプションは、固定 IP アドレスとアドレス・プールの IP アドレス割り当て方式でも使用できます。リモート・ユーザーがシステムに接続すると、そのユーザーに対して固有に定義されたリモート IP アドレスがあるかどうかを判別するための検索が実行されます。定義されている場合、接続には、その IP アドレスとマスクと可能な経路の設定が使用されます。ユーザーが定義されていない場合、IP アドレスはデフォルトとなり、定義されている固定 IP アドレスか、その次に有効なアドレス・プール IP アドレスとなります。
リモート・システムが独自の IP アドレスを割り当てることを許可	このオプションでは、リモート・ユーザーが折衝した場合に、独自の IP アドレスを定義することができます。リモート・ユーザーが独自の IP アドレスを使用するための折衝を行わないなら、リモート IP アドレスは、定義されているリモート IP アドレス割り当て方式により決定されます。このオプションは初期状態では使用不可になっており、これを使用可能にするにあたっては、注意深い考慮が必要です。
IP アドレス経路指定	ダイヤルアップ・クライアントが、システムが属する LAN 上で任意の IP アドレスにアクセスする必要がある場合、このクライアントおよびシステムには、IP アドレス・ルーティングが適切に構成されていなければなりません。

IPv6 アドレス管理

PPP リンクの両端で IPv6 を構成して使用可能にするには、IPv6 制御プロトコル (IPV6CP) を使用します。IPV6CP および IPv6 アドレス割り当てに関連したオプションは、接続プロファイルの「TCP/IPv6 Settings (TCP/IPv6 設定)」セクションにあります。

PPP リンク確立中には 64 ビットのインターフェース ID のみが折衝されるので、PPP リンクの IPv6 アドレス割り当ては IPv4 とは異なります。その後、ステートレス・アドレス自動構成を使用して PPP リンク用の IPv6 アドレスが自動的に構成されます。IPv6 アドレスは、アドレス接頭部を PPP リンクのインターフェース ID と結合して作成されます。PPP リンク用のリンク・ローカル IPv6 アドレスは常に、リンク・ローカル・アドレス接頭部 (fe80::/10) を PPP リンクのインターフェース ID と結合して作成されます。追加の IPv6 アドレスは、ルーター・アドバタイズメント・メッセージで受け取る 64 ビットのネットワーク接頭部を PPP リンクのインターフェース ID と結合して生成できます。動的ホスト構成プロトコル (DHCPv6) を使用して、追加の IPv6 アドレスを PPP リンクに割り当てることもできます。

ステートレス・アドレスの自動構成をサポートするために、IBM i TCP/IP スタックは PPP リンクを介する隣接者探索を実装しています。PPP リンクの隣接者探索には 2 種類のシナリオがあります。

1 つ目のシナリオは、PPP 接続プロファイルで IPv6 データグラム転送が有効と設定されており、プロファイルはリンクのサーバー・サイドにある、というものです。64 ビットのアドレス接頭部、ルーターがデフォルト・ルーターかどうか、および DHCPv6 サービスが使用可能かどうかなどの情報を含むルーター・

アドバタイズメント・メッセージが、PPP リンクを介して送信されます。リンクのクライアント・サイドは、この情報を使用して IPv6 アドレスを構成できます。

2 つ目のシナリオは、PPP 接続プロファイルで IPv6 データグラム転送が有効と設定されておらず、プロファイルはリンクのクライアント・サイドにある、というものです。ルーター送信請求メッセージが PPP リンクを介して送信され、応答で受け取るルーター・アドバタイズメント・メッセージからの情報を使用して IPv6 アドレスを構成します。

IBM i は、同時にリンクのクライアント・サイドとサーバー・サイドの両方になることはできません。

表 9. IPv6 アドレス割り当てオプション

オプション	説明
インターフェース ID	IPV6CP によって折衝されるオプションは、PPP リンクの両側の固有の 64 ビット・インターフェース ID だけです。デフォルト・オプションの「**生成**」を選択して、システムにより自動でランダム・インターフェース ID を作成することをお勧めします。リンクのインターフェース ID を指定することもできますが、別のインターフェース ID が IPV6CP によって折衝される可能性があります。 • PPP リンクの接続の確立時に、IPV6CP によって折衝されるインターフェース ID を使用してリンク・ローカル IPv6 アドレスが自動的に作成されます。 • インターフェース ID を、ルーター・アドバタイズメント・メッセージで受け取るアドレス接頭部と結合して、PPP リンク用の追加の IPv6 アドレスを自動的に作成することもできます。 • 接続プロファイルのインターフェース ID を表示すると、PPP リンクのために直前に折衝されたインターフェース ID が示されます。
他のネットワークへのアクセスをリモート・システムに許可 (IP 転送)	このリンク上で受け取った IPv6 データグラムを他のネットワークに転送するかどうかを指定します。IPv6 データグラム転送を使用可能にすると、システムはこのリンクでルーター機能 (ルーター・アドバタイズメント・メッセージの送信やルーター送信請求メッセージに対する応答など) を実行することもできるようになります。システム全域での IP データグラム転送は、TCP/IP 属性変更 (CHGTCPA) コマンドの IPDTGFWD パラメーターによって制御されます。 IP 転送を使用可能にすると、リモート・アクセス・クライアントは、このシステムの接続先の他のネットワークにアクセスできるようになります。IP 転送を使用不可にすると、リモート・アクセス・クライアントは、このサーバーにしかアクセスできなくなります。 **注:** IP 転送を許可すると、ルーター・アドバタイズメント・メッセージのみがこのリンク上で送信されます。
アドレス接頭部	PPP リンクで送信されるルーター・アドバタイズメント・メッセージに含まれるアドレス接頭部を指定します。リモート・システムは、ルーター・アドバタイズメント内のアドレス接頭部と、折衝済みのインターフェース ID を結合して、PPP リンク用の IPv6 アドレスを作成します。
IPv6 デフォルト経路の通知	システムが、このリンクで送信されるルーター・アドバタイズメント・メッセージによってデフォルト経路を通知するかどうかを指定します。
DHCPv6 の通知	情報が動的ホスト構成プロトコル (DHCPv6) を介して入手可能であることを通知する場合に、指定します。このオプションを選択する際には、「管理対象アドレス構成」オプションか「その他の構成」オプションを選択しなければなりません。このオプションの選択時には、システム上で DHCPv6 サーバーかリレー・エージェントを構成する必要もあります。

表 9. IPv6 アドレス割り当てオプション (続き)

オプション	説明
管理対象アドレス構成	このリンクで送信されるルーター・アドバタイズメント・メッセージ内で「管理対象アドレス構成」フラグ (M フラグ) を設定することを指定します。M フラグを設定すると、動的ホスト構成プロトコル (DHCPv6) を介してアドレスを入手できることが示されます。 **注:** 「**管理対象アドレス構成**」を選択すると、DHCPv6 は入手可能な構成情報をすべて返すため、「**その他の構成**」オプションを選択できません。この種の情報の例としては、DNS 関連の情報や、ネットワーク内の他のサーバーに関する情報があります。
その他の構成	このリンク上で送信されるルーター・アドバタイズメント・メッセージ内で「その他の構成」フラグ (O フラグ) を設定することを指定します。O フラグを設定すると、動的ホスト構成プロトコル (DHCPv6) を介してその他の構成情報を入手できることが示されます。この種の情報の例としては、DNS 関連の情報や、ネットワーク内の他のサーバーに関する情報があります。
デフォルト経路の受け入れ	システムが、このリンクで受け取るルーター・アドバタイズメント・メッセージ内のデフォルト経路を受け入れるかどうかを指定します。このオプションは、IP 転送が許可されない場合にのみ使用可能になります。
追加の静的経路の定義	ダイヤルアップ・クライアントが、システムが属する LAN 上で任意の IPv6 アドレスにアクセスする必要がある場合、このクライアントおよびシステムには、IPv6 アドレス・ルーティングが適切に構成されていなければなりません。

関連情報:

IPv6 の概念

システムの認証

IBM i プラットフォームでの PPP 接続では、リモート・クライアントからシステムへのダイヤルインと、システムがダイヤルしている ISP または別のシステムへの接続の両方を認証するためのオプションがいくつかサポートされます。

システムでは、認証情報を維持するためのいくつかの方法がサポートされています。それらの方法には、Remote Authentication Dial In User Service (RADIUS) サーバーのサポートのための許可ユーザーとそのパスワードのリストを内容とする、システム上の単純な検証リストが含まれます。 RADIUS サーバーは、ネットワーク・ユーザーの詳細情報を管理しています。またシステムでは、ユーザー ID とパスワードの情報を暗号化するためのオプションがいくつかサポートされています。その中には、単純なパスワード交換から、チャレンジ・ハンドシェーク認証プロトコル (CHAP-MD5) のサポートに至るまで、さまざまなものが含まれます。ダイヤルアウト時にシステムを妥当性検査するユーザー ID およびパスワードを含む、システム認証のためのプリファレンスは、IBM Navigator for i の接続プロファイルの「**認証**」タブで指定できます。

関連資料:

19 ページの『シナリオ: システムを PPPoE アクセス・コンセントレーターに接続する』
多くのインターネット・サービス・プロバイダー (ISP) が、Point-to-Point Protocol over Ethernet (PPPoE) を使用してデジタル加入者回線 (DSL) 上での高速インターネット・アクセスを提供しています。システムをそれらの ISP に接続することにより、Point-to-Point Protocol (PPP) のメリットを保ったまま、高帯域幅の接続が提供されます。

32 ページの『シナリオ: RADIUS NAS でダイヤルアップ接続を認証する』
システム上で稼働する Network Access Server (NAS) は、ダイヤルイン・クライアントから別個の Remote Authentication Dial In User Service (RADIUS) サーバーへ認証要求をルーティングすることができます。認

証されると、RADIUS はユーザーに割り当てられる IP アドレスを制御することもできます。

34 ページの『シナリオ: グループ・ポリシーおよび IP フィルターを使用してリソースへのリモート・ユーザー・アクセスを管理する』
グループ・アクセス・ポリシーによって、接続のためのそれぞれのユーザー・グループを識別し、共通の接続属性およびセキュリティー設定をグループ全体に適用することができます。グループ・ポリシーと IP フィルター操作とを組み合わせて使用することにより、ネットワーク上の特定の IP アドレスへのアクセスを、許可したり制限したりすることができます。

MD5 によるチャレンジ・ハンドシェーク認証プロトコル

Challenge Handshake Authentication Protocol (CHAP-MD5) は、認証システムおよび遠隔装置だけが認識する値を計算するためのアルゴリズム (MD-5) を使用します。

CHAP を使うと、ユーザー ID とパスワードが常に暗号化されるので、パスワード認証プロトコル (PAP) よりも安全なプロトコルと言えます。このプロトコルは、プレイバックおよび試行とエラーを繰り返すアクセス試行に効果的です。 CHAP 認証は、接続中に複数回発生することがあります。

認証システムは、ネットワークに接続しようとする遠隔装置に誰何 (すいか) を送信します。遠隔装置は、両方の装置が使用する共通アルゴリズム (MD-5) によって計算された値で応答します。認証システムは、その値を独自の計算結果と照合します。認証は、値が一致した場合に与えられます。一致しない場合、接続は終了します。

関連資料:

22 ページの『シナリオ: リモート・ダイヤルイン・クライアントをシステムに接続する』
在宅勤務者やモバイル・クライアントなどのリモート・ユーザーは、会社のネットワークにアクセスしなければならなくなることがよくあります。こうしたダイヤルイン・クライアントは、Point-to-Point Protocol (PPP) を使用してシステムにアクセスできます。

58 ページの『パスワード認証プロトコル』
Password Authentication Protocol (PAP) は両方向ハンドシェークを使用して、対等システムに ID を確立する簡単な方法を提供します。

拡張可能認証プロトコル

Extensible Authentication Protocol (EAP) は、第三者認証モジュールが PPP 実装と対話することを可能にしています。

EAP は、トークン (スマート) カード、Kerberos、公開鍵、 S/Key といった認証方式のための標準サポート・メカニズムを提供することによって PPP を拡張しています。 EAP は、第三者セキュリティー装置による認証の拡大に対する高まる需要に答えるものです。EAP は、ディクショナリー・アタックやパスワード解読を行うハッカーから、セキュアな仮想プライベート・ネットワーク (VPN) を保護します。 EAP は、Password Authentication Protocol (PAP) と Challenge Handshake Authentication Protocol (CHAP) を改善します。

EAP では、認証情報は、情報の中に組み込まれているのではなく、むしろ情報に付随していると言えます。そのため、リモート・システムは、情報の受け渡しを行う前に、必要な認証について折衝することができます。

システムは、直接には EAP をサポートしません。しかし、リモート認証は、上で説明した付加的な認証方式のいくつかをサポートしている Remote Authentication Dial In User Service (RADIUS) サーバーで使用することができます。

パスワード認証プロトコル

Password Authentication Protocol (PAP) は両方向ハンドシェークを使用して、対等システムに ID を確立する簡単な方法を提供します。

ハンドシェークは、リンクの確立時に行われます。リンクが確立されたら、遠隔装置はユーザー ID とパスワードの組み合わせを認証システムに送信します。この組み合わせが正しいかどうかに応じて、認証システムは接続を継続したり終了したりします。

PAP 認証では、ユーザー名とパスワードを、クリア・テキスト形式でリモート・システムに送信する必要があります。 PAP の場合、ユーザー ID とパスワードは暗号化されないので、トレースが可能となり、ハッカー・アタックを受けやすくなります。この理由から、可能な場合はいつでも Challenge Handshake Authentication Protocol (CHAP) を使用してください。

関連資料:

57 ページの『MD5 によるチャレンジ・ハンドシェーク認証プロトコル』

Challenge Handshake Authentication Protocol (CHAP-MD5) は、認証システムおよび遠隔装置だけが認識する値を計算するためのアルゴリズム (MD-5) を使用します。

Remote Authentication Dial In User Service の概要

Remote Authentication Dial In User Service (RADIUS) は、分散ダイヤルアップ・ネットワーク内のリモート・アクセス・ユーザーのために、認証、アカウンティング、および IP を集中管理するサービスを提供するインターネット標準プロトコルです。

RADIUS クライアント/サーバー・モデルには、 RADIUS サーバーのクライアントとしての Network Access Server (NAS) 操作があります。 NAS としての役割を担うシステムは、 RFC 2865 で定義されている RADIUS 標準プロトコルを使用し、指定された RADIUS サーバーに、ユーザーと接続の情報を送信します。

RADIUS サーバーは、受信したユーザーの接続要求に対して作動して、ユーザーを認証し、必要なすべての構成情報を NAS に返して、 NAS (システム) が認可済みのダイヤルイン・ユーザーに認可済みサービスを送達できるようにします。

RADIUS サーバーに届かない場合は、システムが代わりのサーバーに認証要求を発送します。これにより、グローバル企業は、どんなアクセス・ポイントが使用されていようと、コーポレート・ワイド・アクセスのための、固有なログイン・ユーザー ID を用いるダイヤルイン・サービスをユーザーに提供することができます。

RADIUS サーバーが認証要求を受信すると、その要求が妥当性検査され、 RADIUS サーバーが、ユーザー名とパスワード情報にアクセスするためのデータ・パケットを暗号化を解除します。この情報は、サポートされている適切なセキュリティー・システムに渡されます。これには、UNIX パスワード・ファイル、Kerberos、市販のセキュリティー・システム、あるいは、カスタム開発のセキュリティー・システムなどがあります。RADIUS サーバーは、IP アドレスなど、認証されたユーザーが利用を許可されているサービスを、システムに送り返します。RADIUS アカウンティング要求は、同様の方法で処理されます。リモート・ユーザーのアカウンティング情報は、指定された RADIUS アカウンティング・サーバーに送信することができます。 RADIUS アカウンティング標準プロトコルは、RFC 2866 で定義されています。 RADIUS アカウンティング・サーバーは、受信したアカウンティング要求に対して作動し、 RADIUS アカウンティング要求の情報を記録します。

関連資料:

32 ページの『シナリオ: RADIUS NAS でダイヤルアップ接続を認証する』
システム上で稼働する Network Access Server (NAS) は、ダイヤルイン・クライアントから別個の Remote Authentication Dial In User Service (RADIUS) サーバーへ認証要求をルーティングすることができます。認証されると、RADIUS はユーザーに割り当てられる IP アドレスを制御することもできます。

妥当性検査リスト

妥当性検査リストは、リモート・ユーザーに関連したユーザー ID とパスワードの情報を保管するために使用されます。

既存の妥当性検査リストを使用するか、受信側接続プロファイルの「認証」ページで独自に作成することができます。妥当性検査リスト項目には、ユーザー ID やパスワードに関連した認証プロトコル・タイプを示す必要があります。これは、**「暗号化されたパスワードが必要 (EAP または CHAP-MD5)」**か**「暗号化されていないパスワードが必要 (PAP)」**になります。

詳細については、オンライン・ヘルプを参照してください。

関連資料:

34 ページの『シナリオ: グループ・ポリシーおよび IP フィルターを使用してリソースへのリモート・ユーザー・アクセスを管理する』
グループ・アクセス・ポリシーによって、接続のためのそれぞれのユーザー・グループを識別し、共通の接続属性およびセキュリティー設定をグループ全体に適用することができます。グループ・ポリシーと IP フィルター操作とを組み合わせて使用することにより、ネットワーク上の特定の IP アドレスへのアクセスを、許可したり制限したりすることができます。

帯域幅に関する考慮事項 - 多重リンク

あるタスクを実行する際には、付加的な帯域幅が必要になることがありますが、常に必要とは限りません。

特殊なハードウェアや高価な通信回線を購入することは、適当ではないかもしれません。PPP 多重リンク・プロトコル (MP) は、複数の PPP リンクをグループ化し 1 つの仮想リンク、つまりバンドルを形成できます。このように複数のリンクをまとめると、標準のモデムと電話回線を使用する場合の、2 つのシステム間の有効帯域幅の合計は増加します。MP バンドルには最大 6 つのリンクを組み込むことができます。多重リンク接続を確立するには、 PPP リンクの両方の終端で多重リンク・プロトコルがサポートされている必要があります。多重リンク・プロトコルは、Request for Comment (RFC) 標準 RFC-1990 として文書化されています。

オンデマンド帯域幅

物理リンクを動的に追加したり除去したりする機能を使用することによって、帯域幅が必要なときにだけ供給されるように、システムを構成することができます。このアプローチは、一般にオンデマンド帯域幅と呼ばれ、実際にこれを使用しているときは、追加の帯域幅の料金を支払うだけで済みます。オンデマンド帯域幅の利益を得るには、 MP バンドル内の現在使用可能な合計帯域幅の稼働率をモニターする能力の備わった対等回線が少なくとも 1 つ必要です。帯域幅の使用率が、構成で定義された値を超えると、リンクがバンドルに加えられたり、バンドルからリンクが除去されたりすることがあります。対等回線は、Bandwidth Allocation Protocol を使用することにより、 MP バンドル内のリンクの追加と除去について折衝することができます。 PPP Bandwidth Allocation Protocol (BAP) と Bandwidth Allocation Control Protocol (BACP) は両方とも RFC-2125 に記述されています。

関連情報:

RFC Editor

PPP の構成

PPP を使用して 2 地点間接続をセットアップするにあたっては、PPP 環境の構成を行う必要があります。

関連資料:

81 ページの『リモート・アクセス・サービスの関連情報』
IBM Redbooks の資料および Web サイトには、リモート・アクセス・サービスのトピック・コレクション関連の情報が含まれています。以下の PDF ファイルは、どれも表示または印刷することができます。

接続プロファイルの作成

システム間に PPP 接続を構成するための最初のステップは、システム上に接続プロファイルを作成することです。

接続プロファイルは、以下の詳細事項を論理的に表したものです。

- 回線およびプロファイル・タイプ
- 多重リンク設定
- リモート電話番号およびダイヤル・オプション
- 認証
- TCP/IP 設定: IP アドレスおよびルーティング
- 実行管理機能および接続カスタマイズ
- ドメイン・ネーム・サーバー

「ネットワーク」ディレクトリーの下の「**リモート・アクセス・サービス**」には、以下のオブジェクトが含まれています。

- 発信元接続プロファイル
- 受信側接続プロファイル
- 「**モデム**」

接続プロファイルは、以下のステップに従って作成してください。

1. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**すべてのタスク**」 > 「**リモート・アクセス・サービス**」を展開します。
2. 以下のいずれかのオプションを選択します。
   - 「**発信元接続プロファイル**」を展開して、「**発信元接続プロファイルの作成**」をクリックします。
   - 「**受信先接続プロファイル**」を展開して、「**受信先接続プロファイルの作成**」をクリックして、システムがリモート・システムとユーザーからの着信接続を許可するように設定します。
3. 「新規 2 地点間接続プロファイルのセットアップ」ページで、プロトコル・タイプを選択します。
4. モード選択を指定します。
5. リンク構成を指定します。
6. 「**OK**」をクリックします。

   「新規 2 地点間プロファイルのプロパティー」ページが現れます。ご使用のネットワークに固有なその他の値を設定することもできます。より具体的な情報については、オンライン・ヘルプを参照してください。

関連タスク:

71 ページの『モデムと回線記述を関連付ける』
このトピックでは、モデムと回線記述を関連付ける手順を示します。

関連資料:

19 ページの『シナリオ: システムを PPPoE アクセス・コンセントレーターに接続する』
多くのインターネット・サービス・プロバイダー (ISP) が、Point-to-Point Protocol over Ethernet (PPPoE) を使用してデジタル加入者回線 (DSL) 上での高速インターネット・アクセスを提供しています。システムをそれらの ISP に接続することにより、Point-to-Point Protocol (PPP) のメリットを保ったまま、高帯域幅の接続が提供されます。

22 ページの『シナリオ: リモート・ダイヤルイン・クライアントをシステムに接続する』
在宅勤務者やモバイル・クライアントなどのリモート・ユーザーは、会社のネットワークにアクセスしなければならなくなることがよくあります。こうしたダイヤルイン・クライアントは、Point-to-Point Protocol (PPP) を使用してシステムにアクセスできます。

25 ページの『シナリオ: モデムを使用してオフィスの LAN をインターネットに接続する』
普通、管理担当者は、従業員がインターネットにアクセスできるように、オフィス・ネットワークをセットアップします。管理者は、システムからインターネット・サービス・プロバイダー (ISP) に接続するために、モデムを使用できます。 LAN に接続された PC クライアントは、IBM i オペレーティング・システムをゲートウェイとして使用することにより、インターネット通信が可能です。

28 ページの『シナリオ: モデムを使用して会社のネットワークとリモート・ネットワークを接続する』
モデムを使用することにより、2 つのリモート・ロケーション (本社と支社など) の間でデータの交換を実行できます。 Point-to-Point Protocol (PPP) を使用して本社のシステムと支社のシステムの間の接続を確立することによって、2 つの LAN を接続することができます。

34 ページの『シナリオ: グループ・ポリシーおよび IP フィルターを使用してリソースへのリモート・ユーザー・アクセスを管理する』
グループ・アクセス・ポリシーによって、接続のためのそれぞれのユーザー・グループを識別し、共通の接続属性およびセキュリティー設定をグループ全体に適用することができます。グループ・ポリシーと IP フィルター操作とを組み合わせて使用することにより、ネットワーク上の特定の IP アドレスへのアクセスを、許可したり制限したりすることができます。

43 ページの『シナリオ: イーサネット装置サーバーとのダイヤルアップ接続の確立』
ほとんどの IBM i 区画が、イーサネット接続を介してネットワークに接続されています。ただし、一部のリモート・アプリケーションまたはサービスは、ダイヤルアップ接続を介してのみ使用可能です。イーサネット装置サーバー (イーサネット・シリアル・サーバーまたはイーサネット端末サーバーとしても知られています) には、モデムを接続できるイーサネット・ポートおよびシリアル・ポートの両方があります。これらのポートを使用して、イーサネット接続のみを持つシステムは、イーサネット装置サーバー上のモデムにアクセスして、ダイヤルアップ接続を確立することができます。

プロトコル・タイプ: PPP またはシリアル・ライン・インターネット・プロトコル (SLIP)

PPP は、2 地点間接続のプロトコルとして、シリアル・ライン・インターネット・プロトコル (SLIP) の代わりに選択することができます。

PPP は、メーカーの異なるリモート・アクセス・ソフトウェア間の相互運用を可能にしています。 PPP ではまた、複数のネットワーク通信プロトコルが同じ物理通信回線を使用することもできます。

以下のような理由で、SLIP の Request for Comment (RFC) は、インターネット標準にはなりません。

- SLIP には、2 つのホストの間の IP アドレスを定義するための標準的な方針がありません。そのため、無番号ネットを使用することができません。

- SLIP には、エラー検出やエラー圧縮のサポートがありません。 PPP には、エラー検出やエラー圧縮が実装されています。
- PPP には両方向認証があるのに対し、SLIP にはシステム認証のサポートがありません。

SLIP は現在でも使用されており、IBM i オペレーティング・システム上でサポートされています。しかし、IBM は、2 地点間接続のセットアップの際は PPP を使用することをお勧めします。 SLIP には多重リンク接続のサポートはありません。 PPP には、SLIP より優れた認証があります。 PPP には、圧縮機能があるので、パフォーマンスもこちらのほうが優れています。

注: このリリースでは、 ASYNC の回線タイプが定義される SLIP 接続プロファイルのサポートがなくなっています。これらの接続プロファイルがある場合は、 PPP 回線タイプを使用する SLIP プロファイルか PPP プロファイルのいずれかにマイグレーションする必要があります。

モード選択

Point-to-Point Protocol (PPP) 接続プロファイルにおけるモードの選択には、接続タイプと動作モードの選択が含まれます。選択するモードにより、新規 PPP 接続をシステムでどのように使用するかが指定されます。

以下のステップに従って、選択するモードを指定してください。

1. 以下のいずれかの接続タイプを選択します。
   - 交換回線
   - 専用回線
   - レイヤー 2 トンネリング・プロトコル (L2TP) (仮想回線)
   - Point-to-Point Protocol over Ethernet (PPPoE) 回線
2. 新しい PPP 接続に適した動作モードを選択します。
3. 選択した接続タイプと動作モードを記録します。この情報は、PPP 接続の構成を始めるときに必要となります。

交換回線:

モデム (内蔵または外付け) を使用する場合は、交換回線接続を選択してください。

交換回線接続タイプには、以下のような動作モードがあります。

応答

リモート・システムからシステムにダイヤルできるようにするには、この動作モードを選びます。

ダイヤル

システムからリモート・システムにダイヤルできるようにするには、この動作モードを選びます。

ダイヤル・オンデマンド (ダイヤルのみ)

システムでリモート・システムの TCP/IP トラフィックが検出された場合に、システムからリモート・システムに自動的にダイヤルアウトできるようにするには、この動作モードを選びます。データ伝送が完了し、ある特定の期間の間 TCP/IP トラフィックは発生しないと、接続は終了します。

ダイヤル・オンデマンド (応答可能な専用対等回線)

この動作モードは、システムから専用リモート・システムの呼び出しに応答できるようにする場合に選択します。この動作モードを使うと、リモート・システムの TCP/IP トラフィックが検出されたときに、システムからリモート・システムを呼び出すこともできるようになります。両方のシス

テムが IBM i オペレーティング・システムを使用し、この動作モードを使用している場合、両システム間の TCP/IP トラフィックはオンデマンドで流れるので、永続的な物理接続を行う必要はありません。この動作モードには専用リソースが必要です。動作モードが適正に機能するには、リモート対等回線がダイヤルインしなければなりません。

ダイヤル・オンデマンド (応答可能なリモート対等回線)

この動作モードは、リモート・システムにダイヤルまたは応答できるようにする場合に選択します。着信呼び出しを処理するには、この動作モードを指定する Point-to-Point Protocol (PPP) 接続プロファイルから既存の応答プロファイルを参照しなければなりません。このタイプを選択すると、1 つの応答プロファイルを使って、1 つまたは複数のリモート対等回線からのすべての着信呼び出しを処理し、発信呼び出しごとに別々のダイヤル・オンデマンド・プロファイルを処理することができます。この動作モードでは、リモート対等回線からの着信呼び出しを処理するための専用リソースは必要ありません。

専用回線:

ローカル・システムとリモート・システムを接続する専用回線がある場合、専用回線接続を選択します。専用回線を使用する場合、2 つのシステムを接続するためのモデムは必要ありません。

2 つのシステム間の専用回線の接続は、相手固定回線または専用回線と見なされます。これは常時接続されています。専用回線接続の一方の端は起動側として構成され、もう一方の端は終端側として構成されます。

専用回線接続タイプには、以下のような動作モードがあります。

終端側

この動作モードは、リモート・システムから専用回線を介してシステムにアクセスできるようにする場合に選びます。この動作モードは専用回線の応答プロファイルを参照します。

起動側

システムが専用回線を介してリモート・サーバーにアクセスできるようにするには、この動作モードを使用します。この動作モードは専用回線のダイヤル・プロファイルを参照します。

L2TP (仮想回線):

レイヤー 2 トンネリング・プロトコル (L2TP) を使用するシステムの間に接続を確立する場合は、L2TP 接続を選択します。

L2TP トンネルが確立された後、使用中のシステムとリモート・システムの間に仮想 Point-to-Point Protocol (PPP) 接続が作成されます。 L2TP トンネル伝送と IP セキュリティー (IP-SEC) を一緒に使用すると、インターネットを介してデータを安全に送信、経路指定、および受信することができます。

L2TP (仮想回線) 接続タイプには、以下のような動作モードがあります。

終端側

この動作モードは、リモート・システムから L2TP トンネルを介してシステムに接続できるようにする場合に選びます。

起動側

システムから L2TP トンネルを介してリモート・システムに接続できるようにするには、この動作モードを選びます。

リモート・ダイヤル

システムが L2TP トンネルを介して別のシステムまたはインターネット・サービス・プロバイダー (ISP) に接続し、ISP がリモート PPP クライアントにダイヤルするよう誘導できるようにするには、この動作モードを選択します。

マルチホップ起動側

システムでマルチホップ接続を確立できるようにするには、この動作モードを選択します。

注: このマルチホップ起動側に関連した L2TP 終端側プロファイルでは、「**マルチホップ接続を許可する (Allow multi-hop connection)**」チェック・ボックスがチェックされ、 PPP 妥当性検査リストに、PPP ユーザー名とマルチホップ起動側プロファイルをリンクする項目が含まれている必要があります。

PPPoE 回線:

Point-to-Point Protocol over Ethernet (PPPoE) 接続は、仮想回線を使用し、(イーサネット・アダプターを介して) PPP データをデジタル加入者回線 (DSL) モデムに送信します。 DSL モデムは、インターネット・サービス・プロバイダー (ISP) により提供されます。このモデムは、イーサネットに基づいた LAN にも接続されています。

これにより、IBM i オペレーティング・システム上で PPP セッションを通じて LAN ユーザーの高速インターネット・アクセスが可能になります。システムと ISP との間の接続が開始されたら、 LAN 上の個々のユーザーは、PPPoE 上で ISP との固有セッションを開始できます。

PPPoE 接続は、発信元接続プロファイルでのみ使用されます。接続は起動側動作モードを指定し、単一回線のみ使用します。

リンク構成

リンク構成は、接続を確立するために Point-to-Point Protocol (PPP) 接続プロファイルが使用する回線サービスのタイプを定義します。

回線サービスのタイプは、指定する接続タイプによって異なります。

関連資料:

19 ページの『シナリオ: システムを PPPoE アクセス・コンセントレーターに接続する』
多くのインターネット・サービス・プロバイダー (ISP) が、Point-to-Point Protocol over Ethernet (PPPoE) を使用してデジタル加入者回線 (DSL) 上での高速インターネット・アクセスを提供しています。システムをそれらの ISP に接続することにより、Point-to-Point Protocol (PPP) のメリットを保ったまま、高帯域幅の接続が提供されます。

22 ページの『シナリオ: リモート・ダイヤルイン・クライアントをシステムに接続する』
在宅勤務者やモバイル・クライアントなどのリモート・ユーザーは、会社のネットワークにアクセスしなければならなくなることがよくあります。こうしたダイヤルイン・クライアントは、Point-to-Point Protocol (PPP) を使用してシステムにアクセスできます。

25 ページの『シナリオ: モデムを使用してオフィスの LAN をインターネットに接続する』
普通、管理担当者は、従業員がインターネットにアクセスできるように、オフィス・ネットワークをセットアップします。管理者は、システムからインターネット・サービス・プロバイダー (ISP) に接続するために、モデムを使用できます。 LAN に接続された PC クライアントは、IBM i オペレーティング・システムをゲートウェイとして使用することにより、インターネット通信が可能です。

28 ページの『シナリオ: モデムを使用して会社のネットワークとリモート・ネットワークを接続する』
モデムを使用することにより、2 つのリモート・ロケーション (本社と支社など) の間でデータの交換を実行できます。 Point-to-Point Protocol (PPP) を使用して本社のシステムと支社のシステムの間の接続を確立

することによって、2 つの LAN を接続することができます。

単一回線:

アナログ・モデムに関連する Point-to-Point Protocol (PPP) 回線を定義するには、この回線サービスを選択します。また、このオプションは、モデムを必要としない専用回線でも使います。 PPP 接続プロファイルでは、常に同じ IBM i 通信ポート・リソースが使用されます。

必要なら、アナログ単一回線を、応答プロファイルとダイヤル・プロファイルとの間で共用に構成することができます。動的リソース共用は、リソースの使用可能度を拡張するために設計された新機能です。 V5R2 以前は、モデム・リソースは、これを使用するプロファイルが開始されるとすぐにコミットされていました。これは、リソースが受動待ち状態の場合でも、セッションごとに 1 つのリソースにユーザーを制限することになっていました。現在では、特定のリソースがアクセスされる際に新しい共用規則が適用されるようになりました。これには、2 つのケースがあります。 1 番目は、ダイヤル・プロファイルが応答プロファイルよりも前に開始された場合です。2 番目は、応答プロファイルがダイヤル・プロファイルよりも前に開始された場合です。前提として、リソース共用が使用可能にされていなければなりません。最初のケースでは、開始されたダイヤル・プロファイルは正常に接続します。後で開始された応答プロファイルは、回線が使用可能になるまで待機します。ダイヤル接続が終了したら、応答プロファイルは回線を要求し、開始します。2 番目のケースでは、開始された応答プロファイルは、着信接続を待機します。着信接続が実行されない限り、後で開始されたダイヤル・プロファイルは、回線を「貸す」応答プロファイルから回線を「借り」ます。それから、発信接続が確立されます。接続が終了したら、ダイヤル・プロファイルは回線を応答プロファイルに戻します。この応答プロファイルは、再び着信接続を受け入れる準備をします。共用機能を使用可能にするには、交換回線の記述について「**モデム**」タブをクリックしてから、「**動的リソース共用を使用可能にする (Enable Dynamic Resource Sharing)**」を選択します。

単一回線サービスは、L2TP (仮想回線) および PPPoE (仮想回線) 接続タイプでも用いられます。 L2TP (仮想回線) 接続タイプでは、単一回線にハードウェア通信ポート・リソースは使用されません。言い換えるなら、L2TP 接続で使用される単一回線は、*仮想* 的であり、トンネルを確立するのに必要な物理ハードウェアはありません。 PPPoE 接続で使用される単一回線も、物理イーサネット回線を、リモート接続をサポートする PPP 回線であるかのように扱う機能を提供するという点で、仮想的です。 PPPoE 仮想回線は、物理イーサネット回線にバインドされて、イーサネット LAN 接続を介して DSL モデムへの PPP プロトコル・データ転送をサポートするのに使用されます。

回線プール:

PPP 接続が回線プールの回線を使用するように設定するには、この回線サービスを選択します。PPP 接続が開始すると、システムは回線プールから未使用回線を選択します。ダイヤル・オンデマンド・プロファイルの場合、システムはリモート・システムの TCP/IP トラフィックを検出するまで回線を選択しません。

接続プロファイルの特定の回線記述を定義する代わりに、回線プールを使用することができます。回線プールには 1 つまたは複数の回線記述を指定できます。

回線プールを使用すれば、単一の接続プロファイルで複数の着信アナログ呼び出しと単一の発信アナログ呼び出しのいずれをも処理することができます。 PPP 接続が終了すると、回線は回線プールに戻されます。

回線プールを使用して同時に複数の着信アナログ呼び出しを処理する場合は、着信接続の最大数を指定する必要があります。これは、プロファイルの構成時に、「**新規 2 地点間プロファイルのプロパティー**」ダイアログの「**接続**」タブで設定できます。大きくなった帯域幅を使用する単一接続の回線プールを使用するには、多重リンク設定を使用してください。

回線プールを使用する利点:

- PPP 接続が開始するまで、これに回線リソースをコミットしません。

  特定の回線を使用する PPP 接続の場合、動的リソース共用が使用可能になっていない限り、回線が利用不能であれば、接続は終了します。回線プールを使用する接続の場合、プロファイルの開始時に回線プール内で少なくとも 1 回線は使用可能になっていなければなりません。

  さらに、リソースが共用として構成されている (動的リソース共用を使用可能にする) 場合、特に発信接続について、リソースの可用性が向上します。
- 回線プールとともにダイヤル・オンデマンド・プロファイルを使用すれば、リソースをさらに効果的に使用できます。

  システムは、ダイヤル・オンデマンド接続の使用時にのみ回線プールから回線を選択します。この同じ回線は、また別の機会に、他の接続で使用することができます。
- より少ないリソースのサポートで、より多くの PPP 接続を確立することができます。

  例えば、4 つの固有の接続タイプを必要とする環境がある場合でも、一定の時間に必要とする回線が 2 つだけであれば、回線プールを用いてこの環境を作動させることができます。 4 つのダイヤル・オンデマンド接続プロファイルを作成し、 2 つの回線記述を含んだ回線プールを個々のプロファイルに参照させます。個々の回線は 4 つの接続プロファイルすべてが使用できるので、2 つの接続をいつでも活動状態にすることができます。回線プールを使用すれば、4 つの別々の回線を持つ必要はありません。

  また、ご使用の環境が PPP クライアントと PPP サーバーとの間の組み合わせである場合、「単一回線」として使用される場合でも、「回線プール」に配置される場合でも、回線を共用する (動的リソース共用を使用可能にする) ことができます。最初に開始されたプロファイルは、接続がアクティブでない限り、リソースをコミットしません。例えば、PPP サーバーが開始されており、着信接続を listen している場合、これは、使用している回線を、PPP サーバーから共用回線を開始して「借り」た PPP クライアントに「貸し」ます。

回線プールの構成

回線プールは接続プロファイル内で定義されます。基本的な回線プールの構成については、以下のステップに従ってください。

1. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーキング**」 > 「**すべてのタスク**」 > 「**リモート・アクセス・サービス**」を展開します。
2. ダイヤル呼び出しまたは着信のための接続プロファイルを作成します。以下のいずれかのオプションを選択します。
   - 「**発信元接続プロファイル**」を展開して、「**発信元接続プロファイルの作成**」をクリックして、システムがリモート・システムへの接続を開始するように設定します。
   - 「**受信先接続プロファイル**」を展開して、「**受信先接続プロファイルの作成**」をクリックして、システムがリモート・システムとユーザーからの着信接続を許可するように設定します。
3. 発信元プロファイル (ダイヤルアウト) について、「PPP」、「交換回線 (Switched line)」、および「動作モード (Operating mode)」(通常はダイヤル) を選択します。リンク構成について、「**回線プール (Line pool)**」を選択します。「**OK**」をクリックすると、IBM Navigator for i はこの接続プロファイルのためにプロパティー・ウィンドウを開きます。

   注: 受信側接続プロファイルを作成するときに、回線プールを選択することもできます。フィールド値 (プロトコル・タイプ、接続タイプ、および動作モード) に応じて、回線プール・オプションは表示されたり、表示されなかったりします。

4. 「一般」ページで、プロファイルの名前と説明を入力します。
5. 「接続」ページで、回線プールの名前を入力して、「**新規**」をクリックします。すると、「**新規回線プールのプロパティー (New Line Pool Properties)**」ダイアログが開き、このシステムに使用できるすべての回線とモデムが表示されます。
6. 使用する回線 (複数可) を選択して、それらをプールに追加します。「**新規回線**」をクリックして、新しい回線を定義することもできます。
7. 「**OK**」をクリックしてこのプールを保管し、「新規 2 地点間プロファイルのプロパティー」ページに戻ります。
8. その他のページ (例えば、「TCP/IP IPv4 設定」、「TCP/IP IPv6 設定」、および「認証」)についての必要な情報を入力します。
9. 接続プロファイルは、回線のリストで使用可能なリソースまでたどり (プール内で)、接続にその回線を使用します。詳細については、IBM Navigator for i のヘルプを使用してください。

関連資料:

22 ページの『シナリオ: リモート・ダイヤルイン・クライアントをシステムに接続する』
在宅勤務者やモバイル・クライアントなどのリモート・ユーザーは、会社のネットワークにアクセスしなければならなくなることがよくあります。こうしたダイヤルイン・クライアントは、Point-to-Point Protocol (PPP) を使用してシステムにアクセスできます。

25 ページの『シナリオ: モデムを使用してオフィスの LAN をインターネットに接続する』
普通、管理担当者は、従業員がインターネットにアクセスできるように、オフィス・ネットワークをセットアップします。管理者は、システムからインターネット・サービス・プロバイダー (ISP) に接続するために、モデムを使用できます。 LAN に接続された PC クライアントは、IBM i オペレーティング・システムをゲートウェイとして使用することにより、インターネット通信が可能です。

28 ページの『シナリオ: モデムを使用して会社のネットワークとリモート・ネットワークを接続する』
モデムを使用することにより、2 つのリモート・ロケーション (本社と支社など) の間でデータの交換を実行できます。 Point-to-Point Protocol (PPP) を使用して本社のシステムと支社のシステムの間の接続を確立することによって、2 つの LAN を接続することができます。

複数接続プロファイル・サポート:

複数接続をサポートする 2 地点間接続プロファイルを使うと、1 つの接続プロファイルで、多数のデジタル、アナログ、または L2TP 呼び出しを処理することができます。

これが便利なのは、複数のユーザーからのシステムへの接続を可能にしたいが、各 PPP 回線を処理するために別個の 2 地点間接続プロファイルを指定したくない場合です。この機能が特に便利なのは、1 つのアダプターから 4 本の回線を使用できる 2805 型 4 ポート統合モデムの場合です。

複数接続プロファイルをサポートするアナログ回線の場合、指定された回線プール内の回線すべては最大接続数に達するまで使用されます。基本的に、回線プールに定義されている回線ごとに別個の接続プロファイル・スレッドが 1 つずつ開始されます。すべての接続プロファイル・スレッドは、それぞれの回線での着信呼び出し待ちになります。

複数接続プロファイルのローカル IP アドレス

複数接続プロファイルではローカル IP アドレスを使用できますが、そのアドレスはシステム上で定義された既存の IP アドレスでなければなりません。既存の IP アドレスを選択するには、ローカル IP アドレスのプルダウン・リストを使用できます。PPP プロファイルのローカル IP アドレスとしてローカル IP アドレスを選択すると、リモート・ユーザーはローカル・ネットワーク上のリソースにアクセスすることができ

ます。また、リモート IP アドレス・プール内の IP アドレスが、ローカル IP アドレスと同じネットワーク内にあるように定義しなければなりません。

ローカル IP アドレスを持っていない場合、あるいはリモート・ユーザーによる LAN へのアクセスを望まない場合は、システムの仮想 IP アドレスを定義しなければなりません。仮想 IP アドレスは、無回路インターフェースともいいます。 2 地点間プロファイルは、この IP アドレスをローカル IP アドレスとして使用できます。この IP アドレスは物理ネットワークに結合されていないため、システムに接続された他のネットワークにトラフィックを自動的に転送するわけではありません。

仮想 IP アドレスを作成するには、以下のステップに従ってください。

1. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**TCP/IP 構成**」 > 「**IPV4**」を展開して、「**IPv4 インターフェース**」をクリックします。
2. 「インターフェース」パネルで、「**処置**」メニューをクリックして、「**新しいインターフェース**」 > 「**仮想 IP**」を選択します。
3. インターフェース・ウィザードの指示に従って、仮想 IP インターフェースを作成します。仮想 IP アドレスが作成されると、2 地点間接続プロファイルはそのアドレスを使用できます。ご使用のプロファイルで IP アドレスを使用するには、「TCP/IP 設定」ページにある「**ローカル IP アドレス**」フィールドのプルダウン・リストを使用できます。

   注: 仮想 IP アドレスは、複数接続プロファイルを開始する前に活動状態にしておかなければなりません。そうしないと、プロファイルは開始しません。インターフェースの作成後に IP アドレスを活動化するには、インターフェース・ウィザードの使用時に IP アドレスを開始するためのオプションを選択します。

複数接続プロファイルのリモート IP アドレス・プール

複数接続プロファイルでは、リモート IP アドレス・プールも使用できます。典型的な 1 つの接続 2 地点間プロファイルでは、1 つのリモート IP アドレスを指定できるだけです。このアドレスは、接続の確立時に呼び出し側システムに与えられます。複数の呼び出し元からの同時接続が可能になったので、リモート IP アドレス・プールを使って、開始のリモート IP アドレスを定義することに加え、呼び出し側システムに与えられる他の IP アドレスの範囲も定義します。

回線プールの制約事項

複数接続用の回線プールを使用する際には、以下の制約事項が適用されます。

- 個々の回線は、一度に 1 つの回線プール内にしか置くことはできません。回線プールから回線を除去すると、その回線を別の回線プールで使用することができます。
- 回線プールを使用する複数接続プロファイルを開始する場合、回線プール内のすべての回線は、プロファイルに指定された最大接続数に達するまで使用されます。使用可能な回線がない場合、新しい接続はすべて失敗します。また、回線プール内に使用可能な回線がない状態で別のプロファイルが開始すると、そのプロファイルは終了します。
- 回線プールを持つ単一接続プロファイルを開始する場合、システムはその回線プールから 1 つの回線だけを使用します。同じ回線プールを使用する複数接続プロファイルを開始すると、回線プール内の残りの回線が使用可能になります。

関連タスク:

40 ページの『ステップ 1: モデムの接続された区画のすべてのインターフェースに関して L2TP 終端側プロファイルを構成する』
どのインターフェースについても、終端側プロファイルを作成するには、以下の手順を実行します。

リモート IP アドレス・プール:

システムは、複数の着信接続に使われるすべての応答または停止の 2 地点間接続プロファイルに、リモート IP アドレス・プールを使用することができます。

それには、レイヤー 2 トンネリング・プロトコル (L2TP) および最大接続数が 2 以上の回線プールが含まれます。この機能により、システムは個々の着信接続に固有のリモート IP アドレスを割り当てることができます。

最初に接続するシステムは、「開始 IP アドレス」フィールドに定義されている IP アドレスを受信します。その IP アドレスがすでに使用されている場合、その範囲内で次に使用可能な IP アドレスが付与されます。例えば、開始 IP アドレスが 10.1.1.1 で、「IP アドレスの数」が 5 に定義されていると仮定します。リモート IP アドレス・プール内で使用可能な IP アドレスは、10.1.1.1、10.1.1.2、10.1.1.3、10.1.1.4、および 10.1.1.5 になります。リモート IP アドレス・プールのアドレスに定義されるサブネット・マスクは、常に 255.255.255.255 になります。

リモート IP アドレス・プールを使用するときは、次の制約事項が適用されます。

- 複数の接続プロファイルが同じアドレス・プールを指定できます。ただし、そのプール内のすべての IP アドレスが使われると、他の接続が終了して IP アドレスが使用可能になるまで、その後のすべての要求は拒否されます。
- 他の着信システムがプール内の IP アドレスを使えるようにすると同時に、一部のリモート・システムに特定の IP アドレスを割り振るには、以下のステップに従ってください。
  1. 「**認証**」タブからリモート・システムの認証を使用可能にして、そのリモート・システムのユーザー名が認識できるようにします。
  2. 特定の IP アドレスを必要としないすべての着信接続要求に対して、リモート IP アドレス・プールを定義します。
  3. 「**リモート・システムのユーザー ID に基づいて追加の IP アドレスを定義**」をチェックし、「**ユーザー名によって定義されている IP アドレス**」をクリックして、特定のユーザー用のリモート IP アドレスを指定します。

  リモート・ユーザーがシステムに接続するとき、システムはそのユーザー用に特定の IP アドレスが定義されているかどうかを判別します。定義されている場合、その IP アドレスがリモート・システムに与えられます。定義されていない場合、リモート IP アドレス・プールの IP アドレスが返されます。

PPP 用のモデムの構成

モデムには、アナログ接続機能 (専用および交換回線) が備わっています。アナログ Point-to-Point Protocol (PPP) 接続の場合、外付けモデムまたは内蔵モデムを使用することができます。

関連資料:

79 ページの『PPP のトラブルシューティング』

Point-to-Point Protocol (PPP) 接続の問題に直面した場合、チェックリストを使用してエラー情報を収集することができます。このチェックリストは、エラーの徴候を確認して、PPP 接続の問題を解決するのに役立ちます。

新規モデムの構成

既存のモデム記述を使用して新しいモデムを構成するか、または以前のモデム記述に基づいてモデム記述を作成することができます。

新しいモデムを構成するには、次のステップを実行します。

1. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**すべてのタスク**」 > 「**リモート・アクセス・サービス**」 > 「**モデム**」を展開して、「**モデム情報の追加**」をクリックします。
2. 「**一般**」タブで、すべてのフィールド・ボックスに正しい値を入力します。
3. オプション: 「**追加パラメーター**」タブをクリックして、ご使用のモデムに必要な初期化コマンドを追加します。
4. 「**OK**」をクリックして項目を保管し、「新規モデムのプロパティー」ページをクローズします。

既存のモデム記述の使用

既存のモデム記述を使用できるかどうかを判別するには、以下のステップに従ってください。

1. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**リモート・アクセス・サービス**」を展開して、「**モデム**」をクリックします。
2. 「モデム」リストを調べて、製造社名、モデル、およびモデムの構造を検討します。

   注: ご使用のモデムがデフォルト・リストに含まれていれば、残りのステップを実行する必要はありません。
3. ご使用のモデムによく似たモデム記述を右ボタンでクリックして、「**プロパティー**」を選択し、コマンド・ストリングを調べます。
4. モデムの資料を調べて、モデムに合った特定のコマンド・ストリングを判別します。

   コマンド・ストリングがご使用のモデムの要件と一致していれば、デフォルトのモデム・プロパティーを使用します。一致しなければ、ご使用のモデムに合ったモデム記述を作成し、その記述を「モデム」リストに追加します。

既存のモデム記述に基づくモデム記述の作成

既存のモデム記述に基づいてモデム記述を作成するには、以下のステップに従ってください。

1. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**リモート・アクセス・サービス**」を展開して、「**モデム**」をクリックします。
2. 「モデム」リストから、「**Generic hayes**」を右マウス・ボタンでクリックし、「**これを基にした新規モデム**」を選択します。
3. 「**新規モデム**」ダイアログで、ご使用のモデムが必要とする情報に合うようにコマンド・ストリングを変更します。

関連資料:

79 ページの『PPP のトラブルシューティング』
Point-to-Point Protocol (PPP) 接続の問題に直面した場合、チェックリストを使用してエラー情報を収集することができます。このチェックリストは、エラーの徴候を確認して、PPP 接続の問題を解決するのに役立ちます。

モデムのコマンド・ストリングの設定

ご使用のモデムのユーザーズ・マニュアルには、これらと同等のコマンド・ストリングがあります。モデム記述では、製造元が推奨する設定値を使用してください。

表 10. システムに定義されているモデムおよびコマンド・ストリング

モデムのプロパティー	大半のモデムに該当するコマンド・ストリング
工場設定値にリセットされたモデム	AT&F または AT&Z

表 10. システムに定義されているモデムおよびコマンド・ストリング (続き)

モデムのプロパティー	大半のモデムに該当するコマンド・ストリング
モデムの初期設定:	
Verb の結果コードの表示	Q0 および V1
通常の CD または DTR モード	&C1 および &D2
エコー・モードのオフ	E0
搬送波検出用のデータ・セット作動可能 (DSR)	&S1
ハードウェア・フロー制御の使用可能化: (RTS/CTS)	
エラー訂正とオプションの圧縮の使用可能化 (V.42/V.42 bis)	
DTE-DCE 回線速度の、固定の 115.2 kbps (またはモデムの最大値) での稼働の可能化	
(オプション) モデムがこの機能をサポートする場合の非活動時間の使用可能化	
モデム応答モード:	
n リング後の応答	S0=*n* (ただし、*n* = 1 または 2)
m 秒後に搬送波 (接続) がない場合の切断	S7=*m*
モデムのダイヤル・タイプ	ATDT (トーン・ダイヤルの場合) または ATDP (パルス・ダイヤルの場合)

モデムと回線記述を関連付ける

このトピックでは、モデムと回線記述を関連付ける手順を示します。

1. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**リモート・アクセス・サービス**」を展開して、「**発信元接続プロファイル**」または「**受信先接続プロファイル**」をクリックします。
2. 以下のいずれかのオプションを選択します。
   - 既存の接続プロファイルを処理する場合は、接続プロファイルを右マウス・ボタン・クリックして、「**プロパティー**」を選択します。
   - 新規接続プロファイルを処理する場合は、新しい接続プロファイルを作成します。
3. 「新規 2 地点間プロファイルのプロパティー」ページから、「**接続**」タブを選択し、「**新規**」をクリックします。
   - リンク構成の名前を入力します。
   - 「**新規**」をクリックして「新規回線のプロパティー」ウィンドウを開きます。
4. 「新規回線のプロパティー」ウィンドウから、「**モデム**」タブをクリックし、モデムをリストから選択します。選択されたモデムは、この回線記述に関連付けられます。内部モデムには、適切なモデム定義が既に選択されているはずです。詳しくは、オンライン・ヘルプを参照してください。

発信元接続プロファイルを構成して、着信呼び出しを待機する受信側接続プロファイルに割り当てられる PPP 回線およびモデムを借りることができます。発信元の接続は、接続終了時に PPP 回線およびモデムを受信側接続プロファイルに戻します。この新機能を使用可能にするには、PPP 回線構成ウィンドウの「**モデム**」タブから「**動的リソース共用を使用可能にする (Enable dynamic resource sharing)**」オプションを選択します。PPP 回線は、受信側および発信元の接続プロファイルの「**接続**」タブから構成できます。

関連タスク:

60 ページの『接続プロファイルの作成』
システム間に PPP 接続を構成するための最初のステップは、システム上に接続プロファイルを作成するこ

とです。

リモート PC の構成

Windows 32 ビット・オペレーティング・システムを実行しているパーソナル・コンピューター (PC) から IBM i プラットフォームに接続するには、モデムがインストールされていて適切に構成されていることを確認し、PC 上に TCP/IP および「ダイヤルアップ・ネットワーク」がインストールされていることを確認してください。

PC 上での「ダイヤルアップ・ネットワーク」の構成については、 Microsoft Windows の資料を参照してください。必ず、次の情報を指定または入力してください。

- ダイヤルアップ接続のタイプは、必ず **PPP** にします。
- 暗号化パスワードを使用している場合は、必ず CHAP-MD5 を使用してください (IBM i オペレーティング・システムでは MS-CHAP はサポートされていません)。Windows のあるバージョンは、 MD-5 CHAP を直接にはサポートしていなくても、 Microsoft の付加的な支援を受けることによって、そのように構成することができます。
- 暗号化されていない (保護されていない) パスワードを使用する場合は、自動的にパスワード認証プロトコル (PAP) が使用されます。保護されていないその他のプロトコル・タイプはシステムではサポートされません。
- 通常、IP アドレスは、リモート・システムが定義するか、IBM i オペレーティング・システムが定義します。代替 IP アドレス方式 (独自の IP アドレスを定義するものなど) の使用を計画している場合は、システムがそのアドレス方式を受け入れるよう構成されているかどうかを確認してください。
- ご使用の環境にとって適切であれば、DNS IP アドレスを追加してください。

AT&T Global Network を介するインターネット・アクセスの構成

AT&T Global Network との通信には、特別なプロファイルを構成する必要があります。

このサービスを利用するには、「AT&T Global Network ダイヤル接続」ウィザードを使用して、交換ダイヤル PPP 接続プロファイルを構成し、AT&T Global Network にダイヤルすることができます。このウィザードは 8 つのパネルを順番に表示し、10 分ほどで完了します。ウィザードはいつでも取り消すことができ、既存のデータは保管されません。

AT&T Global Network 接続を使用できるアプリケーションには、次のタイプがあります。

- **電子メール・サービス**: 単一の AT&T Global Network アカウントからメールを定期的に検索して、システムに送信し、Lotus® Mail のユーザーまたは Simple Mail Transfer Protocol (SMTP) のユーザーに配布できるようにします。
- **ダイヤルアップ・ネットワーク**: AT&T Global Network とともに、他のダイヤルアップ・ネットワーク・アプリケーション (標準インターネット・アクセスなど) を使用します。

AT&T Global Network の接続プロファイルは、他の PPP 接続プロファイルと同じように保守します。

「AT&T Global Network ダイヤル接続」ウィザードを使用するには、以下のいずれかのアダプターが必要です。

- 2742 - 2 回線通信アダプター
- 2793/576C: 2 ポート WAN IOA (ポート 1 には V.92 組み込みモデムが、ポート 2 には標準通信インターフェースがある)。
- 2805: 4 ポート WAN IOA (V.92 モデム内蔵)。

| • 57D4 - 2 回線通信アダプター

「AT&T Global Network ダイヤル接続」ウィザードを開始する前に、ご使用の環境について、以下のような情報を収集する必要があります。

- 電子メール・サービス・アプリケーションまたはダイヤルアップ・ネットワーキング・アプリケーションの場合は、 AT&T Global Network アカウント情報 (アカウント番号、ユーザー ID、およびパスワード)。
- 電子メール・サービス・アプリケーションの場合は、メール・サーバーおよびドメイン・ネーム・サーバーの IP アドレス。
- 単一回線接続の場合は、使用するモデムの名前。

「AT&T Global Network ダイヤル接続」ウィザードを開始するには、以下のステップに従ってください。

1. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**すべてのタスク**」 > 「**リモート・アクセス・サービス**」 > 「**発信元接続プロファイル**」を展開して、「**新規 AT&T Global Network ダイヤル接続**」をクリックします。
2. 「AT&T Global Network ダイヤル接続」ウィザードが開始したら、「**ヘルプ**」をクリックして、パネルを完成させるための情報を調べます。

接続ウィザード

接続プロファイルの構成を行う間、手引きとして接続ウィザードを使用できます。

「新規ダイヤル接続 (New Dial Connection)」ウィザード

このウィザードでは、ダイヤルアップ接続プロファイルを構成して ISP またはイントラネットにアクセスするための手順が示されます。このウィザードを完了するには、ネットワーク管理者や ISP からいくらかの情報を入手する必要があります。このウィザードについての詳細は、オンライン・ヘルプを参照してください。

IBM ユニバーサル・コネクション・ウィザード

このウィザードでは、エレクトロニック支援ソフトウェアが IBM と接続するために使用するプロファイルを構成する手順が示されます。エレクトロニック支援は、固有の IBM i 環境のモニターを行い、そのシステムと状況に対して個別設定された修正を使用するよう勧めます。

関連情報:

ユニバーサル・コネクション

グループ・アクセス・ポリシーの構成

「受信側接続プロファイル」の下の「**グループ・アクセス・ポリシー**」 フォルダーには、リモート・ユーザーのグループに設定する 2 地点間接続パラメーターを構成するためのオプションがあります。これは、リモート・システムが発信し、ローカル・システムが受信する 2 地点間接続にのみ適用されます。

新規グループ・アクセス・ポリシーの構成は、次のように行います。

1. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**すべてのタスク**」 > 「**リモート・アクセス・サービス**」 > 「**受信先接続プロファイル**」 > 「**グループ・アクセス・ポリシー**」を展開して、「**新規グループ・アクセス・ポリシー**」を選択します。
2. 「**一般**」タブで、新規のグループ・アクセス・ポリシーの名前と記述を入力します。
3. 「**多重リンク**」タブをクリックして、多重リンク構成をセットアップします。

この多重リンク構成は、複数の物理回線を結合して 1 つのバンドルにすることを指定するものです。バンドルあたりの回線の最大数は、1 から 6 にすることができます。接続が行われるまでは、回線のタイプの設定が分からないため、デフォルト値は常に 1 です。特定のユーザーに対する多重リンク・プロトコルの機能を拡張したり、制限したりするには、グループ・アクセス・ポリシーを使用することができます。

「**バンドル当たりの最大リンク数**」では、1 つの論理回線にしたいリンク (または回線) の最大数を指定します。回線の最大数は、このグループ・ポリシーを PPP プロファイル用のセッションに設定するときに有効な空き回線の数より大きくすることはできません。

リモート・システムが Bandwidth Allocation Protocol (BACP) をサポートしている場合にのみ接続が確立されるよう指定するには、「**帯域幅割り振りプロトコルが必要**」をチェックします。BACP について折衝できない場合、単一リンクのみ許可されます。

4. 「**TCP/IP IPv4 設定**」タブをクリックして、以下の設定を有効にします。

リモート・システムが他のネットワークにアクセスすること (IP 転送) を許可。 このオプションは、IP 転送を行うか否かを指定するものです。このオプションを選択する場合は、必ずシステムをその接続のルーターとして使用できるようにしなければなりません。これを使用すれば、このシステムに宛先指定されていない IP のデータグラムを、このシステムを介して接続されているネットワークに渡すことができます。このオプションをブランクにすると、 IP は、リモート・システムからのデータグラムのうち、宛先のアドレスがこのシステムにとってローカルではないものを廃棄します。

セキュリティーの理由で、IP 転送を行いたくない場合もあるかもしれません。一方、ISP は一般に IP 転送を提供します。これが有効になるのは、システム全域で IP データグラム転送が行える場合だけであることに注意してください。そうでない場合は、たとえマークされていても無視されます。システム全域にわたる IP データグラム転送は、「TCP/IP 属性」ページの「**一般**」タブから表示することができます。

TCP/IP によるヘッダーの圧縮を要求する (Request TCP/IP header compression) (VJ)。 このオプションは、接続が確立された後に、 IP によってヘッダー情報が圧縮されるようにするか否かを指定するものです。通常、圧縮を行うと、対話式トラフィックや低速のシリアル回線では特に、パフォーマンスが向上します。ヘッダーの圧縮は、RFC 1332 で定義されている Van Jacobson (VJ) 方式に従って行われます。 PPP では、接続が確立される際に、圧縮の折衝が行われます。接続のもう 1 つの終端で、VJ 圧縮がサポートされていない場合、システムは、圧縮を用いない接続を確立します。

この接続に IP パケット規則を使用する (Use IP packet rules for this connection)。 このオプションは、このグループ・ポリシーにフィルター規則を適用するか否かを指定するものです。ネットワークの IP トラフィックは、フィルター規則によって制御されます。この IP パケット・フィルター操作コンポーネントを使用すると、指定する規則に従ってパケットのフィルター操作を実行することによってシステムを保護することができます。規則は、パケットのヘッダー情報に基づきます。

リモート・アクセス・ユーザーへのグループ・ポリシーの適用

新しい受信側接続プロファイルの 2 地点間プロパティーの設定を完了したならば、リモート・アクセス・ユーザーにグループ・アクセス・ポリシーを適用することができます。

リモート・アクセス・ユーザーにグループ・ポリシーを適用するには、次のステップを完了します。

1. 「**認証**」をクリックして、「認証」ページを開きます。
2. 「**このシステムでリモート・システムの ID 検査が必要**」をクリックします。
3. 「**妥当性検査リストを使用してローカルから認証**」を選択します。

4. 既存の妥当性検査リストがある場合は、リストからそれを選択し、「**実行**」をクリックします。初めてこれを作成する場合は、新しい妥当性検査リストに付ける名前を入力し、「**開く**」をクリックします。
5. 「妥当性検査リスト」ページで「**追加**」をクリックして、新規ユーザーをその妥当性検査リストに追加します。
6. 「ユーザーの追加」ページで、以下の情報を指定します。
   a. ユーザー名を定義する認証プロトコルを選択します。
   b. ユーザー名とパスワードを入力します。

      注: セキュリティーのため、Challenge Handshake Authentication Protocol 22314 (CHAP)、Extensible Authentication Protocol (EAP)、および Password Authentication Protocol (PAP) に定義されるユーザーには、同じパスワードを使用しないように推奨します。

   c. 「**グループ・ポリシーをユーザーに適用する**」をチェックし、リストからグループ・ポリシーを選択して「**開く**」をクリックします。

   グループ・ポリシーのプロパティーを変更したり、既存のセットアップを処理したりすることもできます。
7. 「**OK**」をクリックして構成を完了し、「2 地点間プロファイルのプロパティー」ページに戻ります。

関連資料:

34 ページの『シナリオ: グループ・ポリシーおよび IP フィルターを使用してリソースへのリモート・ユーザー・アクセスを管理する』
グループ・アクセス・ポリシーによって、接続のためのそれぞれのユーザー・グループを識別し、共通の接続属性およびセキュリティー設定をグループ全体に適用することができます。グループ・ポリシーと IP フィルター操作とを組み合わせて使用することにより、ネットワーク上の特定の IP アドレスへのアクセスを、許可したり制限したりすることができます。

関連情報:

IP フィルター操作とネットワーク・アドレス変換

PPP 接続への IP パケット・フィルター規則の適用

ご使用のネットワークで IP アドレスへのユーザーまたはグループのアクセスを制限するには、パケット規則ファイルを使用することができます。

Information Center のIP フィルター操作とネットワーク・アドレス変換のトピックには、PPP 接続プロファイルで参照できる IP パケット規則の作成方法についての解説があります。

既存の IP パケット・フィルター規則を使用する方法には、次の 2 つがあります。

- 接続プロファイル・レベルで
  1. 「**受信先接続プロファイル**」の「**2 地点間プロファイルのプロパティー**」に入力したら、「TCP/IP IPv4 設定」ページまたは「TCP/IP IPv6 設定」ページを選択して、「**拡張**」をクリックします。
  2. 「**IP パケット規則をこの接続に使用**」をチェックして、リストから PPP フィルター ID を選択します。
  3. 「**OK**」をクリックして PPP フィルターを接続プロファイルに適用します。
- ユーザー・レベルで
  1. 既存のグループ・アクセス・ポリシーを開くか、新規のグループ・アクセス・ポリシーを作成します。
  2. 「TCP/IP 設定」ページをクリックします。

3. 「**IP パケット規則をこの接続に使用**」をチェックして、リストから PPP フィルター ID を選択します。
4. 「**OK**」をクリックして PPP フィルターを適用します。

関連資料:

34 ページの『シナリオ: グループ・ポリシーおよび IP フィルターを使用してリソースへのリモート・ユーザー・アクセスを管理する』
グループ・アクセス・ポリシーによって、接続のためのそれぞれのユーザー・グループを識別し、共通の接続属性およびセキュリティー設定をグループ全体に適用することができます。グループ・ポリシーと IP フィルター操作とを組み合わせて使用することにより、ネットワーク上の特定の IP アドレスへのアクセスを、許可したり制限したりすることができます。

接続プロファイルにおける RADIUS および DHCP サービスの使用可能化

PPP 受信接続プロファイルで RADIUS または動的ホスト構成プロトコル (DHCP) のサービスを有効にするための手順を以下に示します。

1. IBM Navigator for i で、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**すべてのタスク**」 > 「**リモート・アクセス・サービス**」を展開して、「**サービス**」をクリックします。
2. 「**DHCP-WAN**」タブをクリックします。これにより、DHCP は自動的に使用可能になり、システムでどの DHCP サーバーおよびリレー・エージェント (ある場合) が稼働しているかを検出します。
3. RADIUS サービスを使用可能にするために、「**RADIUS**」タブをクリックします。
   a. 「**RADIUS ネットワーク・アクセス・サーバー接続を使用可能にする**」を選択します。
   b. 「**認証に RADIUS を使用可能にする (Enable RADIUS for authentication)**」を選択します。
   c. ご使用の RADIUS ソリューションに適用できる場合には、RADIUS アカウンティングおよび TCP/IP アドレス構成を使用可能にすることもできます。
4. 「**RADIUS NAS 設定 (RADIUS NAS settings)**」ボタンをクリックして、 RADIUS サーバーへの接続を構成します。
5. 「**OK**」をクリックして、戻って構成を保存します。

関連資料:

32 ページの『シナリオ: RADIUS NAS でダイヤルアップ接続を認証する』
システム上で稼働する Network Access Server (NAS) は、ダイヤルイン・クライアントから別個の Remote Authentication Dial In User Service (RADIUS) サーバーへ認証要求をルーティングすることができます。認証されると、RADIUS はユーザーに割り当てられる IP アドレスを制御することもできます。

PPP の管理

このトピックには、システム上で実行できる PPP 管理タスクについての情報が含まれています。

関連資料:

81 ページの『リモート・アクセス・サービスの関連情報』
IBM Redbooks の資料および Web サイトには、リモート・アクセス・サービスのトピック・コレクション関連の情報が含まれています。以下の PDF ファイルは、どれも表示または印刷することができます。

PPP 接続プロファイルのプロパティーの設定

接続プロファイルを作成する際は、普通、「2 地点間接続プロファイルのセットアップ」ウィンドウで、新規接続プロファイルのプロトコル、接続タイプ、動作モードを選択します。

このウィンドウで選択したものを入力すると、「接続プロファイルのプロパティー」シートが現れます。「2 地点間接続プロファイルのセットアップ」ウィンドウに指定する選択が、「接続プロファイルのプロパティー」シートのページの内容とタブの配列を決定します。発信元接続プロファイルのプロパティー・シートと受信側接続プロファイルのプロパティー・シートは異なります。

「新規 2 地点間プロファイルのプロパティー」ウィンドウの各ページを完了する際は、以下の指針に従うことができます。各ページで選択する設定値は、実際の環境、および構成する接続タイプによって異なります。 IBM Navigator for i のオンライン・ヘルプには、ウィンドウに表示されている各オプションの説明があります。詳細については、PPP の例と手順を参照してください。

PPP 活動のモニター

IBM Navigator for i を使用すると、接続プロファイルとセッション・ログを表示できます。

PPP 接続ジョブについて:

- 個々の PPP 接続スレッドの管理には、次のような 2 つの PPP 制御ジョブが使用されます。これらのジョブは、QSYSWRK サブシステムで実行します。
  - QTPPPCTL - 主要な PPP 制御ジョブ。各 PPP 接続スレッドは、このジョブで管理します。
  - QTPPPL2TP - L2TP サーバー。このジョブは、L2TP プロファイルが現在実行されている場合にのみ実行され、作成される L2TP トンネルを管理します。
- QTPPPCTL 内の PPP 接続スレッドは、QTCP ユーザー名の下で動きます。
- SLIP 接続ジョブは、QTCP というユーザー名の下にある QSYSWRK サブシステムで実行されます。SLIP ジョブ名には、次の 2 つのタイプがあります。
  - QTPPDIAL*nn* はダイヤルアウト・ジョブです。ただし、*nn* は 1 から 99 までの任意の数字です。
  - QTPPANS*nnn* はダイヤルイン・ジョブです。ただし、*nnn* は 1 から 999 までの任意の数字です。

接続プロファイルの処理:

1. IBM Navigator for i で、**「IBM i の管理」** > **「ネットワーク」** > **「リモート・アクセス・サービス」**を展開して、**「発信元接続プロファイル」**または**「受信先接続プロファイル」**をクリックします。
2. 「プロファイル」列で、任意の接続プロファイル名を右ボタンでクリックし、次のいずれかのオプションを選択します。
   - **「接続」**を選択すると、このプロファイルに関連したすべての接続の情報を表示するウィンドウが開きます。この情報には、現行接続かその前の接続のいずれか、またはその両方の接続データが含まれます。各接続に関して、ジョブ出力、接続詳細、コール・ログ、またはメッセージ・ログを表示するためのオプションが使用できます。
   - **「プロパティー」**を選ぶと、接続の現行プロパティーを表示する「プロパティー」ページが開きます。

接続情報の表示:

1. IBM Navigator for i で、**「IBM i の管理」** > **「ネットワーク」** > **「リモート・アクセス・サービス」**を展開して、**「発信元接続プロファイル」**または**「受信先接続プロファイル」**をクリックします。
2. 「プロファイル」列で、非活動状態を示さない任意の接続プロファイル名を右ボタンでクリックし、**「接続」**を選択して接続情報を表示します。

このプロファイルの (現行および以前の) 接続がそれぞれ表示されます。この状況フィールドは、接続の現行状況を示します。各 PPP ジョブの状況に応じて、接続されているユーザーのユーザー ID、スレッド ID、ローカルおよびリモート IP アドレス、PPP ジョブの名前などといったその他の情報が表示されます。

3. ジョブ出力、接続詳細、コール・ログ、またはメッセージ・ログを表示するには、「接続」を右マウス・ボタン・クリックして、ボタンを使用可能にします。
4. QTPPPCTL を表示するには、「**ジョブ**」をクリックします。「接続」ウィンドウから、ジョブ名を右マウス・ボタン・クリックし、「**プリンター出力**」または「**ジョブ・ログ**」を選択して、QTPPPCTL に関係するすべての接続スレッドについての情報を表示させます。
5. 接続の詳細を表示する場合は、「**詳細**」をクリックします。詳細は、現行で活動中の接続の詳細だけが表示されます。「詳細」ウィンドウでは、特定の接続の追加接続情報を表示することができます。
6. コール・ログを表示するには、「**コール・ログ (Call Log)**」をクリックします。
7. メッセージ・ログを表示するには、「**メッセージ・ログ (Message Log)**」をクリックします。

システムからの PPP 出力の処理:

PPP 出力の処理を実行するには、システム・コマンド行から WRKTCPPTP を入力します。

- (QTPPPCTL と QTPPPL2TP ジョブを含め) 活動中のすべての PPP ジョブを処理するには、 F14 (活動中のジョブの処理) を押します。
- 特定の接続プロファイルのすべての出力を処理するには、そのプロファイルに **option 8** (出力の処理) を選択します。
- PPP プロファイル構成を印刷するには、そのプロファイルに **option 6** (印刷) を選択します。印刷出力にアクセスするには **WRKSPLF** コマンドを使用します。

接続状況:

接続プロファイル状況は、接続プロファイルのリスト内にある各プロファイルの「**状況**」フィールドに表示されます。この接続プロファイルは、発信元接続プロファイルまたは受信先接続プロファイルのいずれかを選択した後に、「**IBM i の管理**」 > 「**ネットワーク**」 > 「**リモート・アクセス・サービス**」を選択して開きます。個々の接続の状況は、「接続」ウィンドウを用いて表示されます。

表 11. 1 次状況の記述

1 次状況の記述	**説明**
接続要求を待機中	受信側プロファイルが接続を待機している。
着信を待機中	システムが接続を待機している。
接続中	リモート・システムに接続中である。
アクティブ/接続アクティブ	接続が行われ、ジョブが正常に実行されている。
非アクティブ	現在、この接続プロファイルについて実行されているジョブがない。
終了	情報が有効である。
マルチホップ・ターミネーターがマルチホップ起動側を開始中	マルチホップが進行中。
マルチホップ接続がアクティブ	マルチホップは正常に接続された。

表 12. 2 次状況の記述

2 次状況の記述	説明
モデムの初期化中	ダイヤルアップ接続の開始時にモデムを初期化している。
モデム接続の待機中	PPP サーバーは listen 状況にある。
xxx-xxxx をダイヤル中	ダイヤルアップ・クライアントによりダイヤルされる番号。
着信呼び出し検出	PPP サーバーが着信モデム呼び出しを検出した。
モデム接続済み	PPP ハンドシェークが正常に完了した。
操作可能	PPP 接続がアクティブである。
リンク終了	相手側により接続が終了した。
停止	プロファイルまたはジョブが終了した。
認証失敗	PPP 接続は、認証が失敗したために確立できなかった。
接続の無活動タイムアウト	PPP 接続は、無活動タイムアウトが原因で確立できなかった。
IP アドレスの折衝中	PPP 接続は、IP の折衝の問題が原因で終了した。
リモート・モデム無応答	PPP 接続は、相手からの応答がないために確立できなかった。
プロトコル拒否	PPP 接続は、NCP の折衝が失敗したために確立できなかった。
再試行失敗	PPP 接続は、再試行カウントを超えたために確立できなかった。
相手側より PPPoE セッション確認を受信	PPPoE 折衝は正常に完了した。
L2TP 呼び出し確立	L2TP トンネル・アップ・メッセージ

PPP のトラブルシューティング

Point-to-Point Protocol (PPP) 接続の問題に直面した場合、チェックリストを使用してエラー情報を収集することができます。このチェックリストは、エラーの徴候を確認して、PPP 接続の問題を解決するのに役立ちます。

プログラム一時修正 (PTF) とトラブルシューティングに関係のある最新の情報については、IBMi 上の TCP/IP の Web サイト (英語) を参照してください。この Web サイトをたどると、このトピックに含まれる情報の補足や変更に関する最新情報を参照できます。

1. 必要なサポート資料:
   - リモート・ホスト・タイプ、オペレーティング・システム、およびレベル
   - IBM i オペレーティング・システムのレベル
   - プロファイルと同じ名前で出力キューに保管されているすべての出力ファイル
   - QTPPPCTL および QTPPPL2TP (L2TP プロファイルの場合) のジョブ・ログ
   - 実際の環境で使用している接続スクリプト
   - 接続障害の前後における接続プロファイルの状況
2. 推奨されるサポート資料:
   - 回線記述
   - 接続プロファイル

プロファイル設定は、WRKTCPPTP のオプション 6 で印刷できます。

- モデムのタイプおよびモデル
- モデムのコマンド・ストリング
- 通信のトレース

DMPCMNTRC コマンドを使用することにより、通信トレースをダンプして、*PCAP フォーマットで IFS ファイルに保存することをお勧めします。 *PCAP とはパケット・キャプチャー (PCAP) フォーマットのことであり、ネットワーク・プロトコル・アナライザーで使用されます。以下にその例を示します。

```
DMPCMNTRC CFGOBJ(QPPPCMN06) CFGTYPE(*LIN) TOSTMF('/home/cmntrc.pcap') FORMAT(*PCAP)
```

ITSO Redbook V4 TCP/IP for AS/400®: More Cool Things Than Ever では、以下の PPP 問題が扱われています。これには、詳細な問題解決情報もあります。

問題を特定し、解決策を見付けるには、以下の表のチェックリストを参照してください。

表 13. ITSO Redbook からの PPP 問題

問題	ソリューション
モデムのハードウェア構成 ディップ・スイッチとその他のハードウェア設定の構成に誤りがある。	正しいフレーム指示タイプでモデムが構成されているかどうかを確認します。これは、*非同期* か *同期* のいずれかです。詳細については、モデムのマニュアルを参照してください。
モデムの AT コマンド 使用するモデムが IBM Navigator for i のモデムの事前定義リストに含まれていない。	新しいモデムを作成します。
PPP のユーザーとパスワード PPP への接続試行中に、ユーザー名とパスワードのエラーが発生する。	• 大/小文字を正確に区別しつつ、ユーザー ID とパスワードを入力するようにします。 • 対等回線で使用されている認証プロトコルが同一であることを確認します。 • 一方の対等回線では PAP を使用しているのに、もう一方の対等回線は CHAP として構成されているということがないようにします。
接続プロファイルを開始する PPP 回線 指定された複数の PPP 回線が同じハードウェア・リソースによって使用されている。	同じハードウェア・リソースを使用している他の回線をオフに変更します。
PPP プロトコル PPP プロトコルの構成ミスのために、接続エラーが発生することがある。	構成エラーのために、対等回線どうしが相互に通信できないような状況では、より低レベルの PPP プロトコルを調査することが必要な場合があります。 PPP ログまたは PPP ジョブのジョブ・ログに問題が示されない場合は、通信トレース機能を使用することにより、問題を調査することができます。

関連概念:

69 ページの『PPP 用のモデムの構成』
モデムには、アナログ接続機能 (専用および交換回線) が備わっています。アナログ Point-to-Point Protocol (PPP) 接続の場合、外付けモデムまたは内蔵モデムを使用することができます。

69 ページの『新規モデムの構成』
既存のモデム記述を使用して新しいモデムを構成するか、または以前のモデム記述に基づいてモデム記述を作成することができます。

関連資料:

『リモート・アクセス・サービスの関連情報』
IBM Redbooks の資料および Web サイトには、リモート・アクセス・サービスのトピック・コレクション関連の情報が含まれています。以下の PDF ファイルは、どれも表示または印刷することができます。

リモート・アクセス・サービスの関連情報

IBM Redbooks の資料および Web サイトには、リモート・アクセス・サービスのトピック・コレクション関連の情報が含まれています。以下の PDF ファイルは、どれも表示または印刷することができます。

IBM Redbooks

- IBM i5/OS™ IP Networks: Dynamic!
- V4 TCP/IP for AS/400: More Cool Things Than Ever

Web サイト

最新のプログラム一時修正 (PTF) と、PPP および L2TP に関する最新構成情報については、IBM i 上の TCP/IP (英語) の Web サイト の PPP リンクを参照してください。この Web サイトをたどると、このトピック・コレクションに含まれる情報の補足や変更に関する最新情報を参照できます。

関連資料:

1 ページの『リモート・アクセス・サービスの 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。

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。

〒103-8510
東京都中央区日本橋箱崎町19番21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で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

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

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

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

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

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

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

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

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

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

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

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。これらのサンプル・プログラムは特定物として現存するままの状態で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、お客様の当該サンプル・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「リモート・アクセス・サービス」には、IBM i のサービスを利用するためのプログラムを、ユーザーが作成できるように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 Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、『www.ibm.com/legal/copytrade.shtml』 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。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

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。

UNIX は The Open Group の米国およびその他の国における登録商標です。

他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。

使用条件

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

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

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

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

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

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

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、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。

プログラム番号: 5770-SS1

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21