System i

ネットワーキング
TCP/IP 経路指定および作業負荷の平準化

バージョン 6 リリース 1

System i

ネットワーキング
TCP/IP 経路指定および作業負荷の平準化

バージョン 6 リリース 1

ご注意

本書および本書で紹介する製品をご使用になる前に、 39 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM i5/OS (プロダクト番号 5761-SS1) のバージョン 6、リリース 1、モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、それ以降のすべてのリリースおよびモディフィケーションに適用されます。このバージョンは、すべての RISC モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

IBM 発行のマニュアルに関する情報のページ

http://www.ibm.com/jp/manuals/

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(URL は、変更になる場合があります)

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

原　典： System i
Networking
TCP/IP routing and workload balancing
Version 6 Release 1

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2008.2

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

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

目次

TCP/IP 経路指定および作業負荷の平準化

統合された経路指定機能を使用することによって、ご使用のシステムの TCP/IP トラフィックの経路指定と平準化を行うことができ、外部ルーターの必要性がなくなります。

経路指定および作業負荷の平準化の各種方式およびそのバックグラウンド情報を知ることで、システムで使用可能なオプションをより深く理解することができます。 各方式については、どのように接続が作成されるかを理解できるように、図を使って説明します。これらの方式には、経路指定方法の構成に関する説明は含まれません。このトピック・コレクションでは、ご使用のシステムがより良く処理することができるようにするために理解する必要がある経路指定の原理および概念に焦点を当てています。

これらの方法がなぜ重要か

少ない外部ルーターとサーバーを使用することができるため、これらの方法の技法によりご使用の接続のコスト全体が低減される場合があります。これらの経路指定方法を使用して、さらに効果的に IP アドレスを管理できるので、IP アドレスを解放することができます。作業負荷平準化方法を使用して、システムの通信作業負荷を平準化することによりシステムのパフォーマンス全体を向上させることができます。

V6R1 の新機能

TCP/IP 経路指定および作業負荷の平準化のトピック・コレクションにおける新規情報または大幅な変更点については、以下をお読みください。

サポートされている新規のルーティング・プロトコル

i5/OS® オペレーティング・システムは、Open Shortest Path First (OSPF) ルーティング・プロトコルをサポートするために拡張されました。*Open Shortest Path First* (OSPF) はリンク状態ルーティング・プロトコルで、同じエリア内のルーターまたはシステムは、そのエリアのトポロジーが記述されている同一のリンク状態データベースを維持します。

仮想 IP 機能拡張

TCP/IP 経路指定および作業負荷の平準化のトピック・コレクションに影響を与える仮想 IP 機能拡張は、以下の通りです。

- 仮想 IP アドレスのサポートが拡張され、IPv6 アドレスが追加されました。
- Point-to-Point Protocol (PPP) インターフェースまたはレイヤー 2 トンネリング・プロトコル (L2TP)・インターフェースで、仮想 IP アドレスをローカル IP アドレスとして使用して、リモート接続にフォールト・トレランスを提供することができます。
- 仮想 IP インターフェースが活動中に、仮想 IP プロキシー ARP を構成することができます。

これらの IPv6 拡張機能については、18 ページの『仮想 IP による経路指定』 および 19 ページの『フォールト・トレランス』 トピックを参照してください。

文書化された新規の負荷平準化方式

仮想 IP およびプロキシー ARP を負荷平準化の方式として使用することは V6R1 では新しくありませんが、この負荷平準化方式は本書には記載されていませんでした。そのため、29 ページの『仮想 IP および

プロキシー ARP を使用した負荷平準化』 トピックが、この負荷平準化方式を紹介するために追加されました。

新着情報および変更点

技術的な変更が行われた場所を示すために、Information Center では以下のマークを使用しています。

- 新規または変更情報が開始する位置のマークを付けるための»
- 新規または変更情報が終了する位置のマークを付けるための«

PDF ファイルでは、新規および変更情報の左マージンにリビジョン・バー (|) が表示される場合があります。

このリリースの新着情報または変更点に関する他の情報を検索するには、「プログラム資料説明書 (Memo to users)」を参照してください。

TCP/IP 経路指定および作業負荷の平準化の PDF ファイル

この情報の PDF ファイルを表示および印刷することができます。

PDF バージョンのこの文書を表示またはダウンロードするには、「TCP/IP 経路指定および作業負荷の平準化」を選択します。

PDF ファイルの保管

表示用または印刷用の PDF 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 のリンクを右クリックする。
2. PDF をローカルに保管するオプションをクリックする。
3. PDF を保管するディレクトリーを指定する。
4. 「**保存**」をクリックする。

Adobe Reader のダウンロード

上記の文書を PDF 形式で表示または印刷するには、Adobe® Reader が必要です。 Adobe Reader は、Adobe の Web サイト (www.adobe.com/products/acrobat/readstep.html) から無償でダウンロードすることができます。

関連資料

37 ページの『TCP/IP 経路指定および作業負荷の平準化に関する関連情報』

他の Information Center のトピック・コレクションには、TCP/IP 経路指定および作業負荷の平準化のトピック・コレクションに関連する情報が含まれています。

リリースごとの TCP/IP 経路指定機能

経路指定機能を使用する前に、ご利用のシステムが、実行する機能をサポートしている正しいリリースかどうかを必ず確認してください。

V3R1: 静的経路ベースのパケット転送

V3R7/V3R2: Serial Line Internet Protocol (SLIP)、プロキシー・アドレス解決プロトコル (ARP) 経路指定、および IP アドレスが定義されていない接続ネットワーク・サポート。

V4R1: 動的経路指定情報プロトコル バージョン 1 (RIPv1)。

V4R2: 動的経路指定情報プロトコル バージョン 2 (RIPv2)、透過サブネット、および重複経路ベースの負荷平準化。

V4R3: 仮想 IP アドレス、IP アドレスのマスカレード、ネットワーク・アドレス変換 (NAT)、および無クラス・ドメイン間経路指定 (CIDR)。

V4R4: OptiConnect 経由の IP。

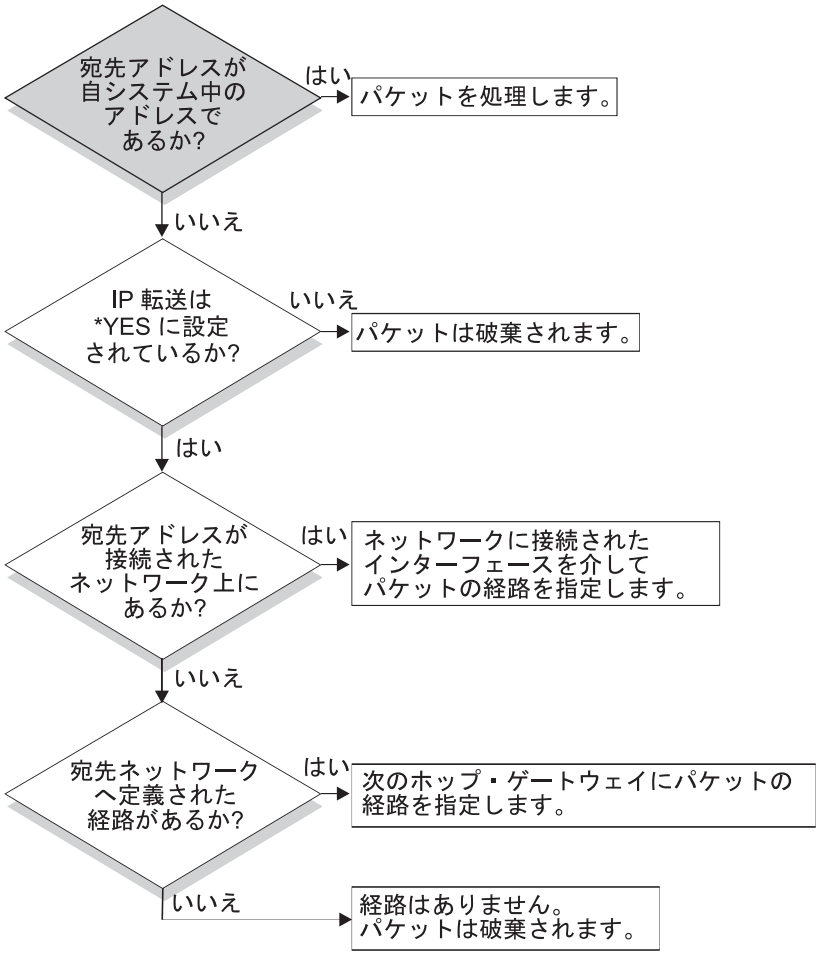
V5R4: 優先インターフェース・リスト。

V6R1: Open Shortest Path First (OSPF) ルーティング・プロトコルおよび IPv6 アドレス用の仮想 IP アドレス・サポート

パケット処理

パケット処理について十分理解していると、経路指機能のインプリメント方法を決定する際に役立ちます。

次の単純化されたフローチャートは、i5/OS オペレーティング・システムが IP パケット (データグラム) を受信したときに実行される論理プロセスを示しています。実際のフローは、このフローと異なる場合がありますが、結果は同じです。以下の論理では、デフォルトのパケット処理の場合のみについて説明しています。高度な経路指定技法を使用する場合は、パケット処理が多少異なる場合があります。



まず、IP ヘッダーにある宛先アドレスがシステムで定義されたすべてのアドレスと照合されます。使用しているシステムに対してパケットが定義されている場合、パケットは IP スタックを経由して TCP などの高レベル・ソフトウェアに渡された後、宛先ポートで listen しているアプリケーションに渡されます。

ローカルでパケットが受け入れられない場合は、IP 転送属性の確認が行われます。IP 転送属性が *YES に設定されている場合は、このシステムがルーターのようにパケットを転送するよう構成されます。転送属性が、TCP/IP 属性あるいは PPP プロファイルで *NO に設定されている場合は、パケットは破棄されます。

パケットの宛先アドレスは、システムが認識しているすべての *DIRECT 経路と照合されます。これは、定義済みインターフェースの *DIRECT 経路指定項目で指定されているサブネット・マスクにパケットの宛先アドレスを含めて、このシステムに直接接続されているネットワークを宛先とするパケットがあるかどうか判別することにより行われます。確認は、最も分割数の多い経路から最も分割数の少ない経路へと順に行われていきます。

次に、i5/OS がリモート・ホストに直接に接続されていない場合、経路指定テーブルが検索されます。確認は、最も分割数の多いホスト (サブネット・マスク 255.255.255.255) から最も分割数の少ない経路 (サブネット・マスク 0.0.0.0) へと順に行われていきます。経路が見つかると、パケットは次のホップ・ゲートウェイへ転送されます。

フローチャートの最後は、経路指定項目が見つからない場合にパケットが破棄されることを示しています。

一般的な経路指定の規則

これらの規則は、TCP/IP 一般、および i5/OS オペレーティング・システム上の TCP/IP に適用されます。

システム上のパケットを管理するには、システムに経路指定機能をインプリメントする際に、これらの規則を考慮する必要があります。これらの規則は、システム上のパケットに起こっている状態、およびそれらのパケットの行き先を判別する場合に役立ちます。 ほとんどの規則と同様に、この規則にも例外があります。

- システムには、IP アドレスはありません。IP アドレスがあるのはインターフェースだけです。

  注: 仮想 IP (コネクションレス) アドレスがシステムに割り当てられます。
- 通常、システムに宛先 IP アドレスが定義されている場合、パケットは、関連付けられているインターフェースに関係なく処理されます。

  この場合の例外は、アドレスが定義されていないインターフェースに関連付けられている場合、あるいは IP NAT またはフィルター操作が活動状態である場合、パケットは転送または破棄されます。
- IP アドレスおよびマスクによって、接続ネットワークのアドレスが定義されます。
- システムからの経路は、インターフェースに接続されるネットワーク・アドレスに基づいて選択されます。選択される経路は、以下の項目に基づきます。
  - 経路グループの検索順序: 直接経路、サブネットワーク経路、デフォルト経路の順です。
  - グループ内では、最も分割数の多いサブネット・マスクがある経路が選択されます。
  - 分割数が等しい経路の場合、リスト順序または負荷平準化技法に従って選択されます。
  - 経路はシステムによって手動でまたは動的に追加することができます。

経路指定接続の方式

経路指定では、ネットワーク・トラフィックがソースから宛先までどのパスを通り、そしてそのパスがどのように接続されるかを取り決めています。

2 地点間接続による経路指定

2 地点間接続を使用して、ローカル・システムからリモート・システムへ、またはローカル・ネットワークからリモート・ネットワークへ、データを送信することができます。

2 地点間接続は、通常、広域ネットワーク (WAN) を介して 2 つのシステムを結びます。ローカル・システムからリモート・システムへ、またはローカル・ネットワークからリモート・ネットワークへ、2 地点間接続を使ってデータを送信することができます。 2 地点間接続と Point-to-Point Protocol (PPP) とを混同しないよう注意してください。Point-to-Point Protocol (PPP) は、コンピューターとインターネットを接続するために一般的に使われている 2 地点間接続の 1 つのタイプです。 PPP 接続をセットアップし管理する方法の詳細については、PPP 接続を参照してください。

2 地点間接続は、ダイヤルアップ接続回線、非交換回線、およびフレーム・リレーなどのその他のネットワークを経由して行われます。2 地点間接続を行うための IP アドレスの構成には、IP アドレスが定義されている接続と IP アドレスが定義されていない接続の 2 つの方法があります。名前が示すように、IP アドレスが定義されている接続では各インターフェースに対して定義された固有の IP アドレスを使います。IP アドレスが定義されていない接続では、接続時に追加の IP アドレスは使いません。

IP アドレスが定義されているネットワーク接続

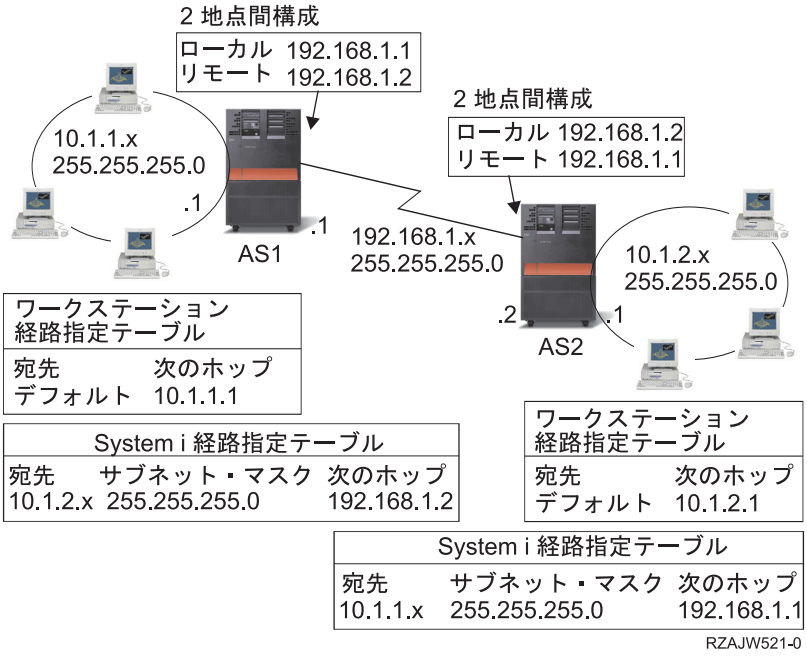
表面的には、IP アドレスが定義されている接続を使った 2 地点間接続を構成するのが最も簡単な方法に見えます。 IP アドレスが定義されている接続は、各接続端末に対して定義された固有の IP アドレスを使う 2 地点間接続です。

以下に IP アドレスが定義されている 2 地点間接続を行う場合の注意点を示します。

- 各接続端末は固有の IP アドレスを持つこと。
- リモート・システムへトラフィックが流れるように、システムに経路指定ステートメントを追加すること。
- 2 地点間リンクのアドレスは、ネットワーク管理者が管理すること。
- アドレスは、2 つのシステムだけを接続するために使用すること。

各 2 地点間接続がシステムに対して定義されている場合、接続の他方の終端にあるネットワークへの接続方法を記述する経路指定項目が、各終端に設けられている必要があります。 システムでの経路指定選択の処理は、各インターフェースに IP アドレスが与えられていることを前提として行われます。 これらのアドレスおよび経路は、ネットワーク管理者が管理する必要があります。小規模のネットワークでは、これらのアドレスの使用状況を簡単に把握することができ、また、追加アドレスが使用されることはあまりありません。しかし、大規模ネットワークでは、この方法を使用すると、各終端のインターフェースを定義するだけで、サブネットのアドレスがすべて使用されてしまうことがあります。

下の図は、2 つの System i™ プラットフォームの間での IP アドレスが定義されているネットワーク接続を示しています。 AS1 から AS2 へ接続するだけの場合、経路指定項目は必要ありません。リモート・ネットワーク (10.1.2.x) 内のシステムに接続したい場合は、図の経路指定項目を各システムに追加する必要があります。これは、リモート・ネットワーク 10.1.2.x が 192.168.1.x 接続の一部であるために必要になります。



IP アドレスが定義されていないネットワーク接続

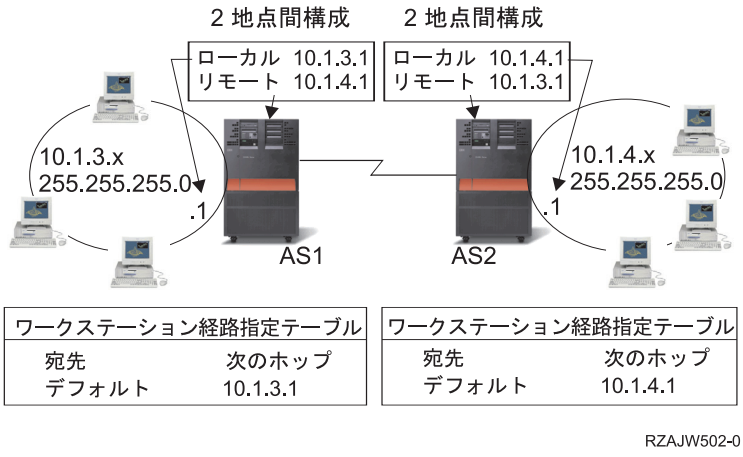
2 地点間接続を定義する場合、IP アドレスが定義されている接続よりも IP アドレスが定義されていない接続の方が複雑です。しかし、ネットワークを管理するには、IP アドレスが定義されていない接続の方がより単純で優れています。

i5/OS での経路指定選択の処理は、インターフェースに IP アドレスが与えられていることを前提として行われます。IP アドレスが定義されていない接続では、2 地点間で使用されるインターフェースが固有のアドレスを持ちません。IP アドレスが定義されていない接続で使用されるシステム・インターフェースの IP アドレスは、実際はリモート・システムの IP アドレスになります。

IP アドレスが定義されていない接続を行う場合の注意点

- 2 地点間インターフェースは、リモート・ネットワークで使用されるアドレスを持つこと。
- システムに経路指定ステートメントは必要ない。
- ネットワーク管理は、リンク用の IP アドレスを使用しないことで簡単になる。

以下の例では、AS1 が 10.1.4.x ネットワークのインターフェースを持ち、AS2 が 10.1.3.x ネットワークのインターフェースを持っています。AS1 はアドレス 10.1.3.1 で LAN ネットワーク 10.1.3.x に接続されています。そのため、AS1 は 10.1.3.x ネットワーク上のすべてのシステムに直接接続することができます。



RZAJW502-0

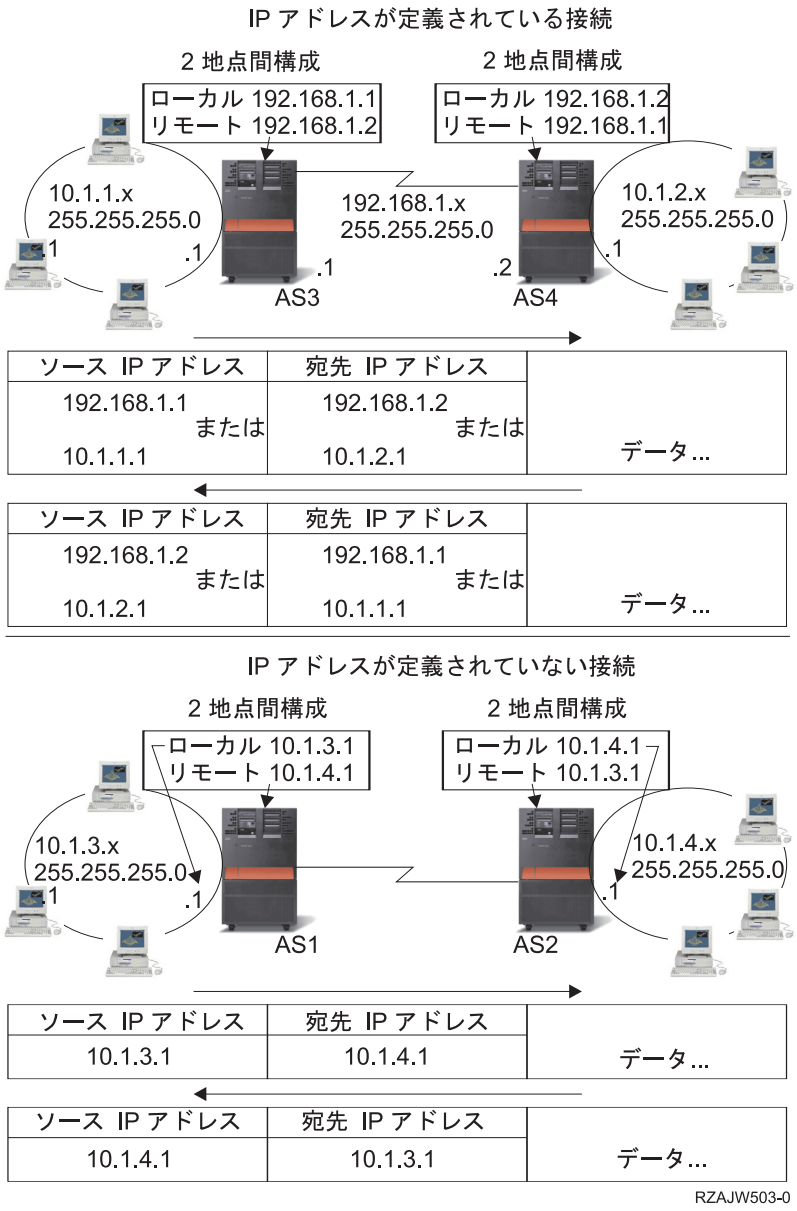
また、この例では AS2 も示されています。 AS2 はアドレス 10.1.4.1 で LAN ネットワーク 10.1.4.x に接続されています。そのため、AS2 は 10.1.4.x ネットワーク上のすべてのシステムに直接接続することができます。各システム (AS1 および AS2) は、ローカル・インターフェースとしてそれぞれの経路指定テーブルにリモート・アドレスを追加します。このアドレスは特別なものとして取り扱われるので、このアドレスへのパケットがローカルで処理されることはありません。リモート・アドレスを宛先とするパケットは、インターフェースからもう一つの接続の終端へ転送されます。もう一方の接続の終端でパケットが受信されると、通常のパケット処理が行われます。

AS1 を 10.1.4.x ネットワークに、そして AS2 を 10.1.3.x ネットワークに接続する必要があるとします。これらの 2 つのシステムが同じ部屋にあれば、各システムに LAN アダプターを追加して、適切な LAN に新しいインターフェースを接続することができます。その場合、AS1 および AS2 に経路指定項目を追加する必要はありません。しかし、この例ではシステムがそれぞれ異なる場所にあるため、2 地点間接続を使用しなければなりません。2 地点間接続を使用する場合でも、経路指定項目を追加したくない場合があります。Point-to-Point Protocol (PPP) 接続を IP アドレスが定義されていない接続として定義すれば、システ

ムに経路指定項目を追加せずに LAN アダプターを使用した場合と同じ結果を得ることができます。 そのためには、各システムが経路の解決を行うために使用するリモート・システムの IP アドレスを借りることになります。

IP アドレスが定義されていない接続のデータ・フローと IP アドレスが定義されている接続のデータ・フロー

次の図は、IP アドレスが定義されている 2 地点間接続および IP アドレスが定義されていない 2 地点間接続で使用されるアドレスを示しています。図の上半分は IP アドレスが定義されている接続の例で、リモート・システムに接続するためにリモート・システム・アドレス 192.168.1.2 あるいは 10.1.2.1 が使用されています。これは、次のホップとして 10.1.2.1 から 192.168.1.2 へパケットを送る経路指定項目が AS3 にあるためです。リターン・パケットで使用されるアドレスは、受信するパケットによって決まります。図の下半分は、IP アドレスが定義されていない接続で使用されるアドレスを示しています。アウトバウンド・パケットのソースは 10.1.3.1、宛先は 10.1.4.1 になります。システムには、2 地点間接続を行うリモート・システムのアドレスを使ってリモート・ネットワークに直接接続するインターフェースがあるため、どちらのシステムにも経路指定項目は必要ありません。



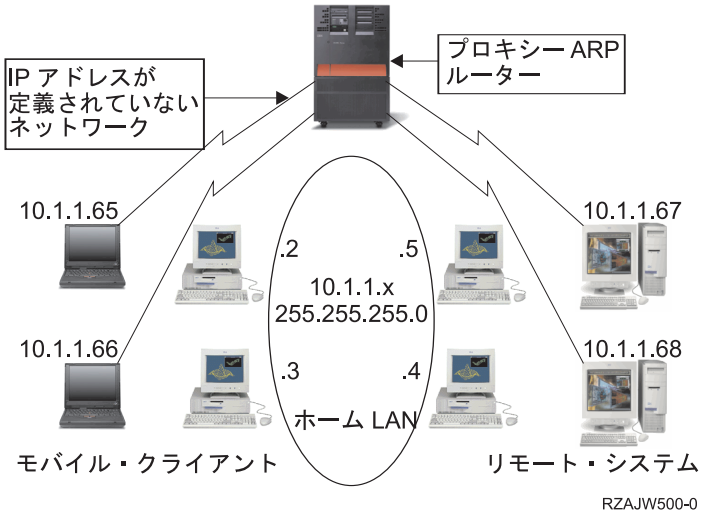
関連概念

PPP 接続

プロキシー・アドレス解決プロトコル経路指定

プロキシー・アドレス解決プロトコル (ARP) は、新しい論理ネットワークを構築したり、経路指定テーブルを変更せずに、物理的に独立しているネットワーク間の接続性を提供します。このトピックではまた、プロキシー ARP の経路指定の拡張技法である透過サブネット記述を含んでいます。

ARP 経路指定を使用すると、物理的に異なる別個のネットワークを、単一の論理ネットワークのように見せることができます。ローカル・エリア・ネットワーク (LAN) に直接接続されていないシステムを、LAN 上の他のシステムに対し LAN に接続されているかのように見せかけることができます。これは、ダイヤルイン・インターフェースからネットワーク全体へ接続を行うダイヤルアップ・モデルに便利です。次の図に、考えられるモデルを示しています。10.1.1.x はホームの LAN を表し、10.1.1.65 から 10.1.1.68 はリモート・システムを表しています。

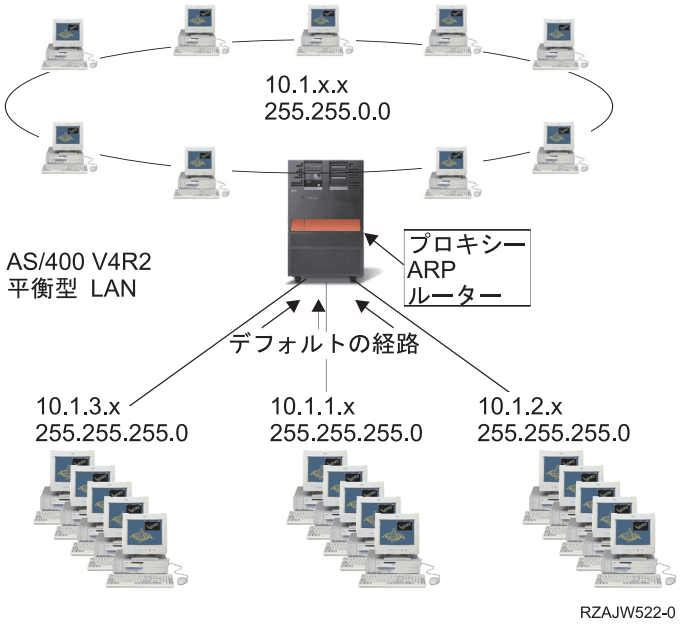


ホームの LAN (10.1.1.x) 上のシステムからリモート・システムにデータを送信する場合、最初に ARP 要求を行います。これは、ターゲット・システムのアドレスを取得するために、 LAN セグメントに接続しているすべてのシステムへ送信されるブロードキャストです。リモート側で接続されているシステムからこのブロードキャストは見えません。しかし、プロキシー ARP によって、ご使用のシステムはリモート接続されているシステムを認識しています。ご使用のシステムは、リモート接続されているいずれかのシステムに対する ARP 要求を受信すると、その ARP 要求に対する応答として該当システムのアドレスを返します。システムは次にデータを受信して、そのデータを該当のリモート・システムへ転送します。 この転送を行うためには、IP 転送を *YES に設定する必要があります。 リモート・システムが接続されていない場合、システムは ARP 要求に応答せず、要求側のシステムからデータが送信されることもありません。

透過サブネット

透過サブネットを、プロキシー ARP の概念を拡張する方法として使うことができます。透過サブネットをサブネット全体、またはホスト全域のプロキシーとして使うことができます。透過サブネットを使うことにより、プライマリー・ネットワークのアドレス・スペースからスタブ・ネットワークにアドレスを割り当てることができます。

透過サブネットは単一のホストに対して機能するため、サブネット全体やホスト全域に接続できます。次の図でスタブ・ネットワーク (10.1.1.x から 10.1.3.x まで) は、アドレスがプライマリー・ネットワークのアドレス・スペース (10.1.x.x) から割り当てられています。



透過サブネット機能をさらに拡張して、リモート側の実 LAN を操作することができます。 WAN 上で透過サブネットを使用すると、リモート・ネットワークがホーム・ネットワークに接続されているように見せかけることができます。上の図では、3 つのネットワークがホームの 10.1.x.x ネットワークに System i プラットフォームを経由して接続されています。これらのネットワークはすべてサブネット・マスクを使って定義されているため、ホーム・ネットワークに対して透過的になっています。プロキシー ARP は、ホーム・ネットワーク上で、10.1.1.x、10.1.2.x、および 10.1.3.x サブネット内のシステムに対するあらゆる ARP 要求に応答します。 このアクションのため、ホーム・ネットワークに対するトラフィックは、自動的にホーム・ネットワークのシステムに経路指定されることになります。そして、このシステムによって、適切なリモート・システムへデータが送信されます。リモートのシステムは、データを処理するか、あるいはリモート LAN 内の正しいシステムにデータを転送します。 リモート LAN のワークステーションは、最初のホップ・ゲートウェイとして、そのネットワーク内のリモート・システムに向けられたデフォルトの経路を持たなければなりません。新たな論理ネットワークは作られないため、ホーム LAN 内のワークステーションに経路指定項目を追加する必要はありません。

動的経路指定

動的経路指定とは、ネットワークが変更された場合に自動的に経路指定テーブルを再構成する低保守方式のことです。

| 動的経路指定は、Interior Gateway Protocol (IGP) によって提供されます。 Routing Information Protocol
| (RIP) と Open Shortest Path First (OSPF) プロトコルは、i5/OS オペレーティング・システムがサポートする 2 つの IGP です。

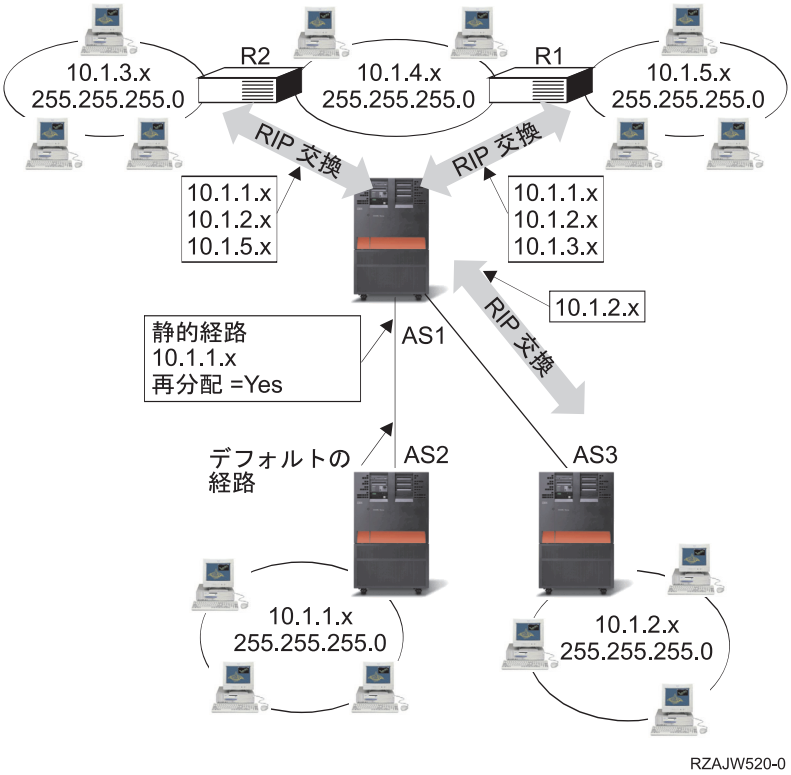
経路指定情報プロトコル

経路指定情報プロトコル (RIP) は距離ベクトル型ルーティング・プロトコルです。距離ベクトル型プロトコルが稼働しているルーターは、ルーティング更新メッセージで経路指定テーブルのすべてまたは一部を近隣に送信します。

RIP を使用して、RIP ネットワークの一部としてホストを構成できます。このタイプの経路指定には保守の必要がほとんどなく、また、ネットワークが変更またはネットワーク通信が停止した場合、経路指定テー

ブルが自動的に再構成されます。RIPv2 が System i 製品に追加されたため、ユーザーは RIP パケットを送受信してネットワーク全体の経路を更新できます。

下の図では、静的経路は AS2 を通じたネットワーク 10.1.1.x への接続を記述するセントラル・システム (AS1) に追加されます。これは、経路の再分配を「はい」に設定して、ネットワーク管理者によって追加される静的経路です。このように設定すると、この経路が他のルーターおよびシステムと共用されるため、10.1.1.x にトラフィックがある場合、中央の System i プラットフォーム (AS1) にそのトラフィックが経路指定されます。 AS2 が経路指定されたシステムを起動すると、RIP 情報が送受信されます。 この例では、AS2 が 10.1.2.x への直接接続を所有しているというメッセージが AS1 によって送信されます。



以下のプロセスは、上の図のトラフィックの経路指定を説明したものです。

- AS1 では、AS2 からのこの RIP パケットが受信および処理されます。AS1 に 10.1.2.x への経路がない場合、この経路が保存されます。同じ数またはそれ以下のホップである 10.1.2.x へのパスがある場合、この新しい経路情報は破棄されます。この例では、AS1 に経路データが保存されます。
- AS1 では、10.1.5.x への経路情報がある R1 から情報が受信されます。AS1 にこの経路情報が保存されます。
- AS1 では、10.1.3.x への経路情報がある R2 から情報が受信されます。AS1 にこの経路情報が保存されます。
- 次に AS1 から RIP メッセージが送信される場合、AS1 では認識されているが、R1 では認識されていない接続をすべて記述する情報が R1 に送信されます。AS1 から 10.1.1.x、10.1.2.x、および 10.1.3.x に関する経路情報が送信されますが、R1 が 10.1.4.x に接続しており、経路が必要ないことがわかっているため、R1 には 10.1.4.x に関する情報が送信されません。同様の情報が R2 および AS3 に送信されます。

Open Shortest Path First

Open Shortest Path First (OSPF) は IP ネットワークのために開発され、Shortest Path First (SPF) アルゴリズムに基づいたリンク状態ルーティング・プロトコルです。OSPF は Interior Gateway Protocol (IGP) です。

OSPF ネットワークでは、同じエリア内のルーターまたはシステムは、そのエリアのトポロジーが記載されている同一のリンク状態データベースを維持します。同じエリア内の各ルーターまたはシステムは、同じエリア内の他のすべてのルーターまたはシステムから受け取ったリンク状態広告 (LSA)、およびそれ自身が生成した LSA から、リンク状態データベースを生成します。LSA は近隣およびパス経費についての情報が含まれているパケットです。リンク状態データベースに基づいて、各ルーターまたはシステムは SPF アルゴリズムを使用して、それ自身をルートとして最短パスのスパンニング・ツリーを計算します。

OSPF の主な利点は以下のとおりです。

- 経路指定情報プロトコル (RIP) のような距離ベクトル型ルーティング・プロトコルと比べて、OSPF は大規模な異機種のインターネットワークのサービスを提供するにはより適しています。 OSPF は、ネットワーク・トポロジーが変更されたとき、短時間で経路指定を再計算できます。
- OSPF では、自律システム (AS) をエリアに分割し、エリアのトポロジーの分離を保持して、OSPF のルーティング・トラフィックおよび各エリアのリンク状態データベースのサイズを減らすことができます。
- OSPF は同コストのマルチパス・ルーティングを提供します。異なるネクスト・ホップを使用して TCP スタックに重複経路を追加できます。

OSPF Hello プロトコルおよびリンク状態データベース交換

OSPF ネットワークのルーターまたはシステムがそれらのインターフェースが機能していることを確認した後、最初に近隣探索のために OSPF インターフェースを介した Hello プロトコルを使用して、Hello パケットを送信します。近隣は共通ネットワークにインターフェースを持つルーターまたはシステムです。その後、隣接するルーターまたはシステムはリンク状態データベースを交換して、隣接関係を確立します。

以下の図は、サブネット 9.7.85.0 での 2 つのシステムの近隣探索と隣接関係の確立のプロセスを示しています。各システムは、共通のサブネット 9.7.85.0 に OSPF インターフェースを持っています (システム A にはインターフェース 9.7.85.1 およびシステム B にはインターフェース 9.7.85.2)。サブネット 9.7.85.0 はエリア 1.1.1.1 に属しています。

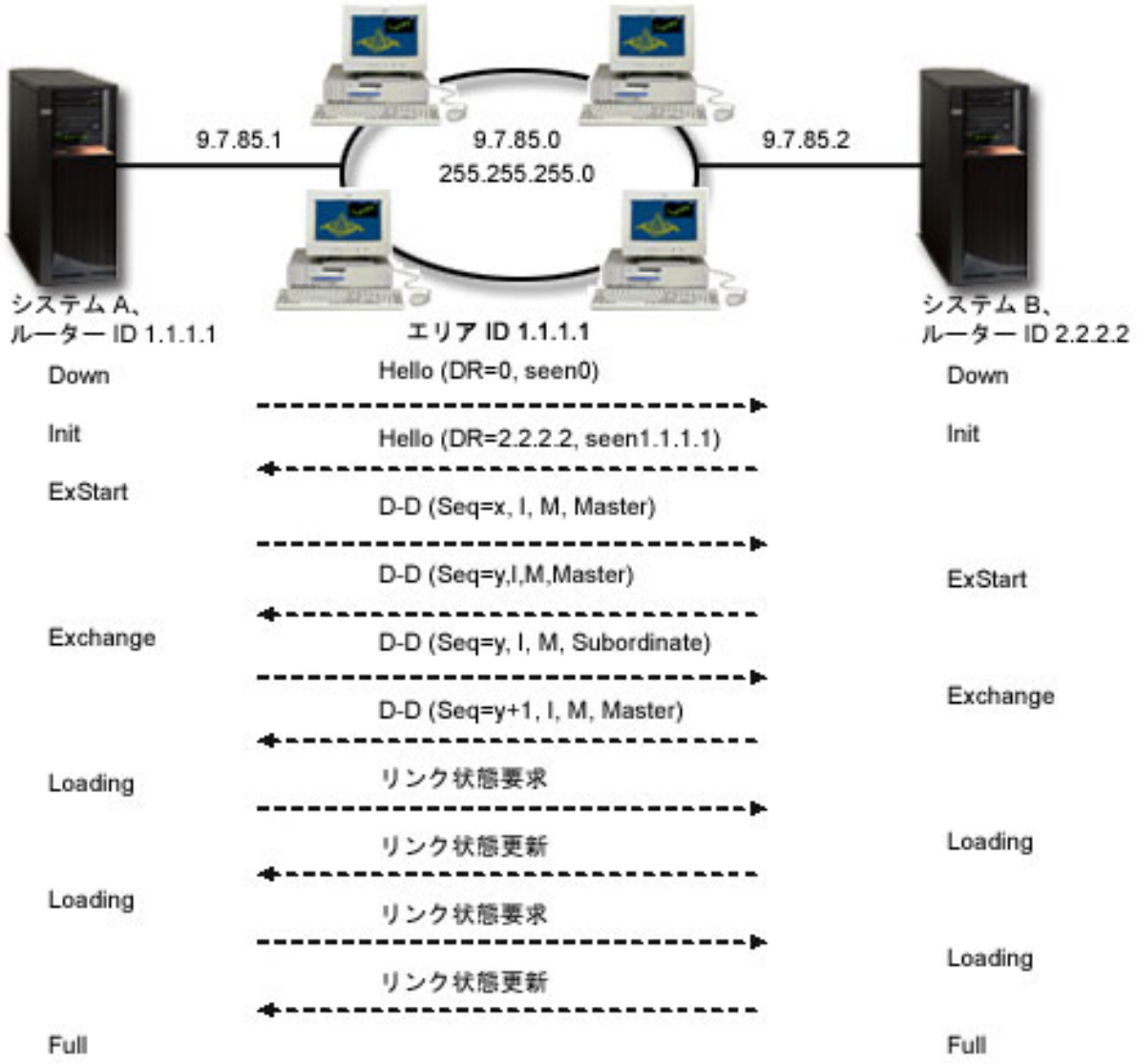


図 1. OSPF Hello プロトコルおよびデータベースの交換

EXSTART フェーズ
これはリンク状態データベースの交換の最初のステップです。2 つのシステム間でどちらが主でどちらが従属するかをネゴシエーションします。

EXCHANGE フェーズ
2 つのシステムはデータベース記述パケットを交換して、各システムのリンク状態データベースに含まれない LSA を見つけ出します。各システムは、そのリンク状態データベースに含まれない LSA を再伝送リストに格納します。

LOADING フェーズ
各システムはリンク状態要求パケットを送信し、近隣 (この例では他のシステム) に対して EXCHANGE フェーズで再伝送リストに格納されたすべての LSA を送信するように要求します。近隣は LSA を含むリンク状態更新パケットを送信して、その要求に応答します。

FULL フェーズ
2 つのシステムの LSA の交換が終了し、リンク状態データベースの同期がとれたとき、システム間の隣接関係が確立されます。

隣接関係がエリア内のすべてのルーターまたはシステム間で確立された後、エリア内の各ルーターまたはシステムは定期的に LSA を送信してその隣接関係を共用するか、あるいはその状態変更を報告します。確立された隣接関係を LSA と比較することで、エリア内のルーターまたはシステムはエリアのトポロジーの変更を発見し、それに応じてリンク状態データベースを更新することができます。

指定ルーターとバックアップ指定ルーター

少なくとも 2 つの接続ルーターを持つマルチアクセス OSPF ネットワークでは、ルーターは Hello プロトコルを使用して指定ルーターとバックアップ指定ルーターを選びます。 (マルチアクセス・ネットワークは、複数の装置が同時に接続して通信が行えるネットワークです。)

指定ルーターはすべてのマルチアクセス・ネットワーク用に LSA を生成し、ネットワーク内の他のルーターに LSA をフラッディングし、どのルーター同士が隣接になるべきかを決定します。ネットワーク内の他のすべてのルーターは、指定ルーターと隣接になります。 指定ルーターによって、ネットワーク・トラフィックとこのネットワークのリンク状態データベースのサイズが減少します。

バックアップ指定ルーターは、ネットワーク内のすべてのルーター (指定ルーターを含む) と隣接関係を確立する必要があることを除けば、他のルーターと何の違いもありません。バックアップ指定ルーターは、現在の指定ルーターに障害が発生したときに指定ルーターに昇格します。

図 1 では、サブネット 9.7.85.0 はブロードキャスト・ネットワークです。したがって、サブネット 9.7.85.0 のルーターは、Hello プロトコルを使用して指定ルーターとバックアップ指定ルーターを選びます。この例では、システム A が指定ルーターとして選ばれ、システム B がバックアップ指定ルーターとして選ばれています。

OSPF AS をエリアに分割する

RIP とは異なり、OSPF は階層内で作動できます。階層内の最大のエンティティーは AS です。AS は共通のルーティング・ストラテジーを共用する共通の管理下にあるネットワークのグループです。AS をエリアに分割することができ、互いにルーターによって接続されます。エリアは連続したネットワークのグループと接続ホストで構成されています。エリアのトポロジーはエリアの外側のエンティティーからは認識できません。同じエリア内のルーターは、同一のリンク状態データベースを持ちます。分離したエリアのトポロジーにより、ルーティング・トラフィックの減少と各エリアのリンク状態データベースの小型化が可能になります。

OSPF エリアの境界に位置し、これらのエリアをバックボーン・ネットワークに接続しているルーターは、エリア境界ルーターと呼ばれます。エリア境界ルーターは複数のエリアに複数のインターフェースを持ち、各エリアの個別のリンク状態データベースを維持しています。

以下の図では、2 つのエリア (エリア 1.1.1.1 とエリア 2.2.2.2) が構成されています。システム B はエリア境界ルーターで、エリア 1.1.1.1 にはインターフェース 9.7.85.2 が、エリア 2.2.2.2 にはインターフェース 9.5.104.241 が接続されています。システム B は 2 つのリンク状態データベース (各エリアに 1 つ) を持ちます。システム B はインターフェース 9.7.85.2 を通してエリア 1.1.1.1 のシステム A および ルーター C と隣接関係を確立し、インターフェース 9.5.104.241 を通してエリア 2.2.2.2 のシステム D と隣接関係を確立します。

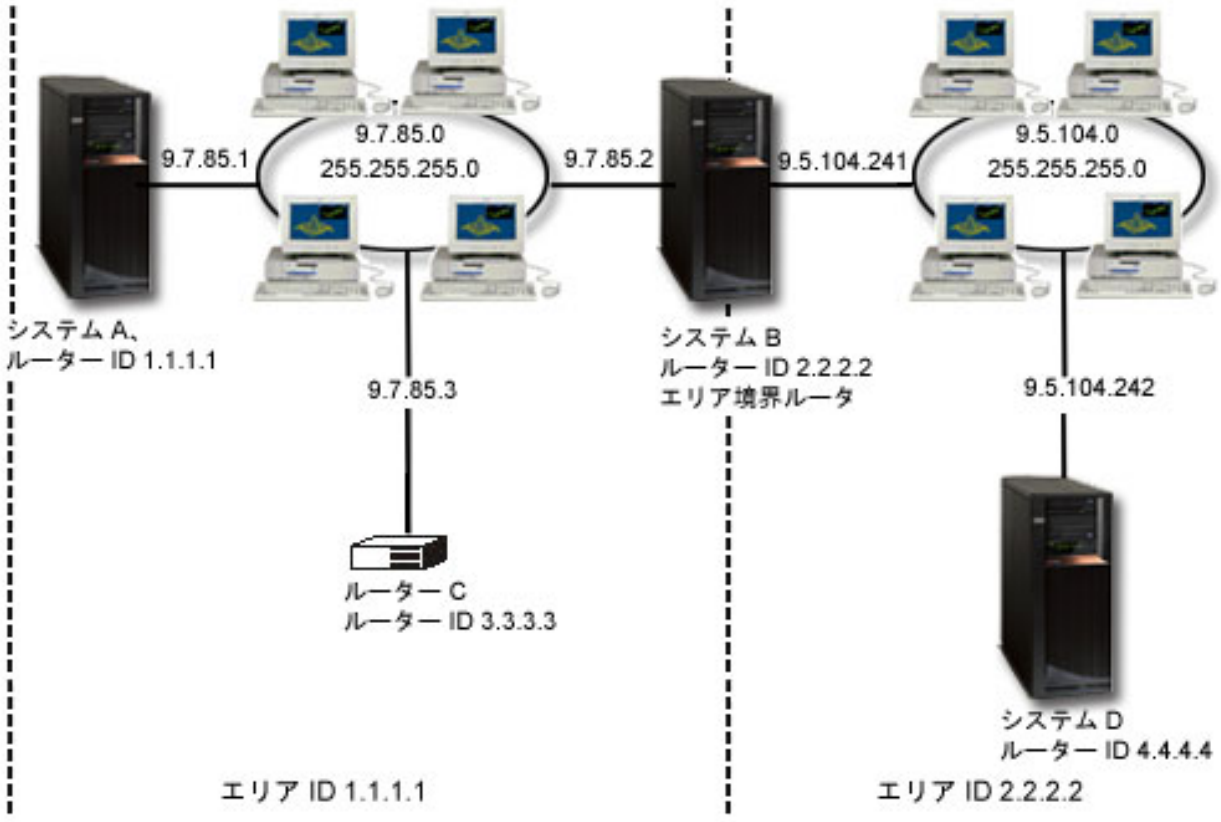


図 2. OSPF AS をエリアに分割する

関連概念

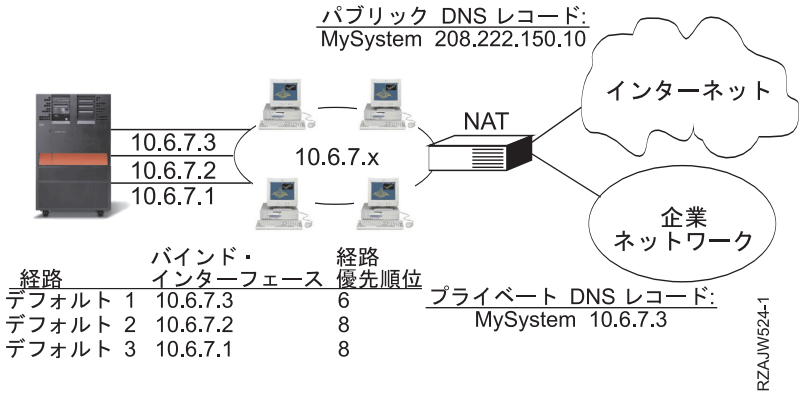
Open Shortest Path First (OSPF)

経路のバインド

経路のバインドは、情報の応答パケットを送信するインターフェースに対する制御を行います。

優先経路のバインドを行うまでは、情報の応答パケットを送信するインターフェースに対する制御が完了していません。経路の追加機能によって追加される優先経路バインド・インターフェースを使って、明示的に経路とインターフェースを結び付けることにより、パケットを送信するインターフェースをより制御することができます。

次の図では、3 つのインターフェースが同一のネットワークに接続されています。どのインターフェースでもインバウンド要求を受信できるように、応答は同じインターフェースに返され、ユーザーは重複経路を各インターフェースに追加しなければなりません。この例では、3 つのデフォルト経路が追加され、それぞれの経路は明示的に異なるインターフェースに結合されています。 このバインドは、インターフェースの起動や終了の順番にかかわらず、変更されることはありません。



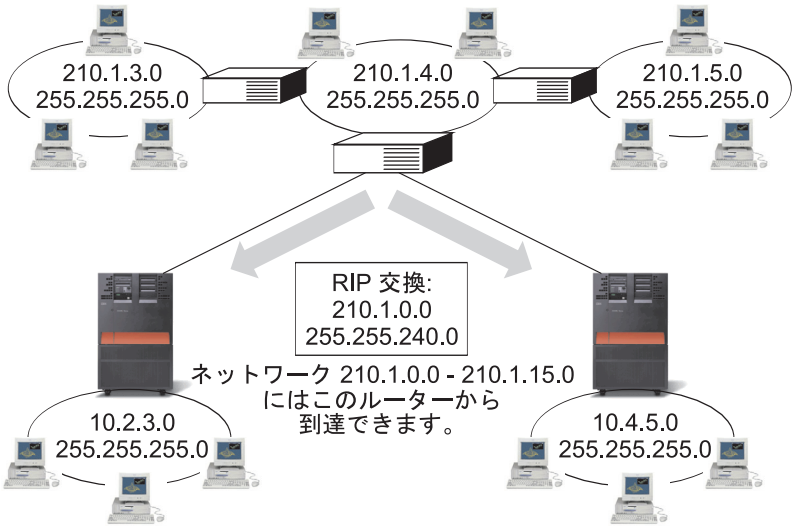
無クラス・ドメイン間経路指定

無クラス・ドメイン間経路指定を使うと、経路指定テーブルのサイズを削減し、業務で利用できる IP アドレスを増やすことができます。

無クラス・ドメイン間経路指定 (CIDR またはスーパーネッティング) は、複数のクラス -C アドレスの範囲を単一のネットワークまたは経路に結合する方法です。この経路指定方式によって、クラス -C インターネット・プロトコル (IP) アドレスが追加されます。これらのアドレスは、インターネット・サービス・プロバイダー (ISP) によって配布され、顧客によって使用されます。CIDR アドレスによって経路指定テーブルのサイズが縮小され、企業内でより多くの IP アドレスが使用可能になります。

以前は、ネットワーク・クラスに必要なマスクに等しいかそれより大きいサブネット・マスクの入力が必要でした。つまり、クラス -C アドレスの場合、255.255.255.0 のサブネットが指定可能な最大のサブネット (253 のホスト) です。IP アドレスを保存するには、ネットワーク内に 253 より多くのホストが必要な場合、インターネットによって複数のクラス -C アドレスが発行されます。これにより経路などの構成が困難になります。

現在、CIDR を使用すると、サブネット・マスクを使うことによって、これらの連続するクラス -C アドレスを単一のネットワーク・アドレスの範囲に結合できます。たとえば、4 つのクラス -C ネットワーク・アドレス (255.255.255.0 のサブネット・マスクをもつ 208.222.148.0、208.222.149.0、208.222.150.0、および 208.222.151.0) を配布する場合、サブネット・マスク 255.255.252.0 を使用することにより、これらのネットワーク・アドレスをスーパーネットにすることを ISP に依頼することができます。このマスクによって、経路指定のために 4 つのネットワークが 1 つに結合されます。 CIDR は割り当てられているものの、不必要な IP アドレスは削減するため有効です。

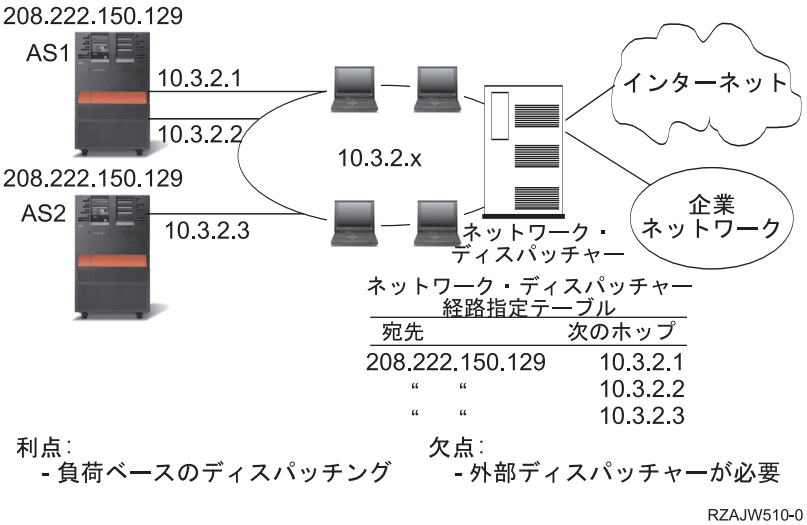


この例では、ネットワーク・アドレス 210.1.0.0 およびサブネット・マスク 255.255.240.0 を含む 1 つの RIP メッセージを送信するようにルーターが設定されています。このルーターは、このルーターを使って 210.1.0.0 から 210.1.15.0 までのネットワークで RIP メッセージが受信されることをシステムに通知します。CIDR が使用可能でない場合、このルーターによって、同じ情報を伝達するために必要な 16 個のメッセージの代わりに 1 つのメッセージが送信されます。

仮想 IP による経路指定

仮想 IP は、無線インターフェースまたはループバック・インターフェースとも呼ばれ、物理インターフェースにアドレスをバインドせずに、システムに 1 つ以上のアドレスを割り当てる方法を提供する強力な機能です。

これは、異なるアドレスにバインドしているシステムや、あるいはデフォルト・ポートにバインドする必要のある他のサービスを複数回繰り返して稼働させたい場合に使用することができます。 仮想 IP を使用するのは、ほとんどがローカルのゲートウェイと System i プラットフォームの間に複数のパスを作る場合であり、たとえば負荷平準化やフォールト・トレランスを目的にしています。 このとき、以下の図に示すように、それぞれのパスは追加のインターフェース、すなわちシステムの追加の非仮想 IP アドレスを意味します。



これらの複数のインターフェースの存在は、ローカル・ネットワークでのみ認識できるようしてください。リモート・クライアントがシステムの複数の IP アドレスを認識しないようにしてください。システムが、リモート・クライアントから単一の IP アドレスで認識されるのが理想的です。インバウンド・パケットがゲートウェイからローカル・ネットワークを通ってシステムに届くまでの経路は、リモート・クライアントからは認識できないようにしてください。 仮想 IP を使用すると、このようなことが可能になります。ローカル・クライアントはいずれかの物理 IP アドレスを使用してシステムと通信しますが、リモート・クライアントでは仮想 IP インターフェースだけが認識されます。

仮想 IP 環境は、リモート接続されたクライアントのサーバーとして機能するシステムのためのものです。さらに重要なのは、仮想 IP アドレスが物理インターフェースと異なるサブネット上にあるということです。加えて、仮想 IP アドレスを使用することで、システムが単一のホストと見なされるようになりますが、より大きなネットワークやサブネットワークに接続されたホストと見なされるとは限りません。そのため、仮想 IP インターフェースのサブネット・マスクは、通常は 255.255.255.255 に設定します。

| 仮想 IP アドレスは単一の物理インターフェースにバインドされていないため、仮想 IP アドレスのための
| プロキシー ARP を使用可能にしない限り、システムは仮想 IP アドレスに対するアドレス解決プロトコル
| (ARP) には応答しません。 つまり、プロキシー ARP を有効にすることにより、ローカル・インターフェ
| ースは仮想 IP アドレスではなく ARP 要求に応答することができます。それ以外の場合は、リモート・シ
| ステムはアドレスを受信するために経路を定義する必要があります。現在は仮想 IP インターフェースが活
| 動中に、そのための仮想 IP プロキシー ARP を構成することができるようになっています。

上の例では、ワークステーションはすべて、システムの 10.3.2 インターフェースの 1 つを次のホップ・ゲートウェイとしています。 パケットがシステムに届くと、そのパケットのパケット処理が行われます。 宛先アドレスがシステム上で定義したアドレスのいずれかと一致すると (仮想 IP アドレスを含む)、システムはパケットを処理します。

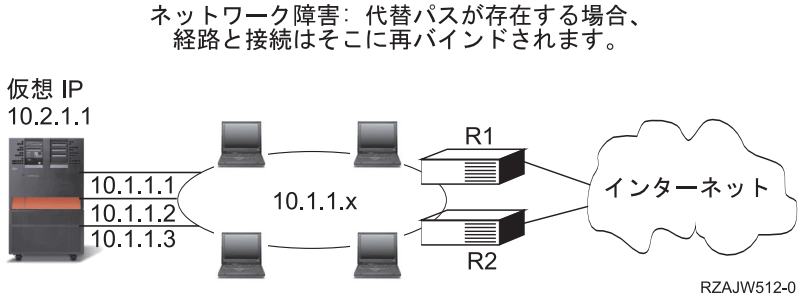
ドメイン・ネーム・システム (DNS) サーバーは、要求したシステムのアドレスを使用します。この場合、すべてのアドレスは同じシステムを表します。複数のシステムを 1 つの大きなシステムに統合するときに、仮想 IP 機能を使用することができます。

| 仮想 IP アドレスのサポートには現在、IPv6 アドレスが含まれます。

フォールト・トレランス

仮想 IP アドレスの別の使用法は、ルーター障害から保護することです。フォールト・トレランスでは、障害時に経路を復活させるいくつかの異なる方法を紹介しています。

この例では、障害後に経路を回復するいくつかの方法を示します。最も信頼性が高い接続は、仮想 IP アドレスがシステムで定義されている場合です。仮想 IP のサポートによって、インターフェースに障害が発生しても、セッションは別のインターフェースを使って通信できます。



ルーター R1 に障害が発生した場合

- R1 を経由する接続は、R2 を経由するように転送されます。
- 障害が発生したゲートウェイが R1 の回復を検出しても、活動状態の接続はそのまま R2 を経由して行われます。

インターフェース 10.1.1.1 に障害が発生した場合

- 10.1.1.1 への活動状態の接続は失われますが、10.1.1.2、10.1.1.3、および 10.2.1.1 へのその他の接続は存続します。
- 経路の再バインド
  - V4R2 より前のバージョン: 間接経路は、10.1.1.2 または 10.1.1.3 に再バインドされます。
  - V4R2: 優先バインド・インターフェースがなしに設定されている場合のみ、経路が再バインドされます。
  - V4R3 以降のバージョン: 仮想 IP アドレスおよび 1 次システム・アドレスとして 10.2.1.1 を定義する必要があります。
    - システムの 1 次 IP アドレスは、活動状態のままです。
    - 最低 1 つの物理インターフェースが活動状態である限り、システムはアクセス可能です。

| リモート接続にフォールト・トレランスを提供するために、Point-to-Point Protocol (PPP) インターフェース
| またはレイヤー 2 トンネリング・プロトコル (L2TP) インターフェースは、仮想 IP アドレスをローカル
| IP アドレスとして使用できるようになりました。

ネットワーク・アドレス変換 (NAT) による経路指定

ネットワーク・アドレス変換 (NAT) を使った経路指定では、私設ネットワークで使われている IP アドレスをマスクして私設ネットワークを保護する一方で、インターネットなどのリモート・ネットワークにアクセスすることができます。

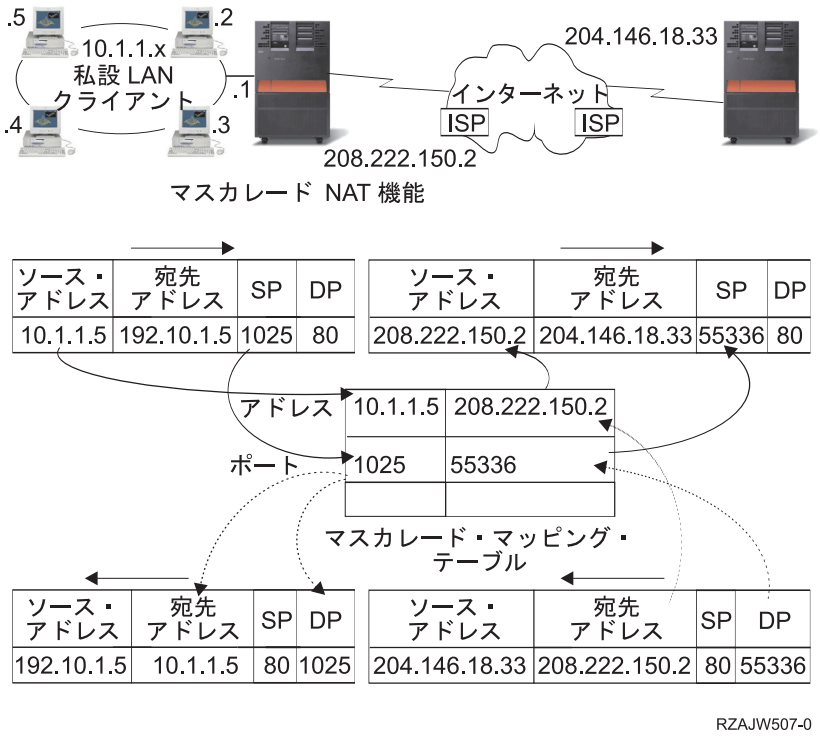
NAT によって、リモート・ネットワーク、通常、インターネットへのアクセスが提供されると同時に、ファイアウォール内で使用される IP アドレスのマスキングによって私設ネットワークが保護されます。

マスカレード NAT

マスカレード NAT を使用すると、私設ネットワークを、パブリック・インターフェースにバインドされたアドレスの背後に隠したり、そのアドレスで表すことができるようになります。

多くの場合、パブリック・インターフェースにバインドされたアドレスは、インターネット・サービス・プロバイダー (ISP) によって割り当てられるアドレスで、Point-to-Point Protocol (PPP) 接続の場合、アドレスは動的にすることができます。このタイプの変換は、外部公衆ネットワークに接続する私設ネットワーク内で行われる接続のみに使用可能です。各アウトバウンド接続は、異なるソース IP ポート番号を使って管理されます。

マスカレード NAT を使用すると、プライベート IP アドレスが割り当てられているワークステーションが、i5/OS オペレーティング・システムを介してインターネット上のホストと通信できるようになります。i5/OS には、ローカル ISP がインターネット・ゲートウェイとして割り当てた IP アドレスがあります。*ローカル接続システム* という用語は、接続の方式 (ローカル・エリア・ネットワークまたは広域ネットワーク) や接続の距離に関係なく、内部ネットワーク上のすべてのシステムを指します。*外部システム* という用語は、インターネット上にあるシステムを指します。次の図では、マスカレード NAT の動作を示します。



インターネット側からは、すべてのワークステーションがシステム内にあるように見えます。つまり、ただ 1 つの IP アドレスがシステムとワークステーションの両方に関連付けられています。 ルーターは、内部ワークステーションに向けたパケットを受信すると、内部 LAN 上のそのパケットを受信するアドレスを判別し、そこに送信します。

各ワークステーションでは、i5/OS がそのゲートウェイおよびデフォルトの宛先になるように設定する必要があります。 ワークステーションの 1 つが、インターネットに送信するためのパケットを i5/OS に送信すると、特定の通信接続 (ポート) とワークステーションの間で対応付けが行われます。 マスカレード NAT 機能はポート番号を保管するため、接続上でワークステーションのパケットに対する応答を受信した際に、正しいワークステーションへ応答を送信することができます。

活動状態のポート接続、および接続のどちらかの終端による最終アクセス時間の記録が、マスカレード NAT によって作成および保持されます。事前に決定された期間アイドル状態であるすべての接続は、それ以上使用されないという仮定に基づいて定期的にこれらの記録から除去されます。

ワークステーションとインターネットとの間のすべての通信は、ローカル接続システムで開始される必要があります。 これは、効果的なセキュリティー・ファイアウォールです。インターネット側は、ワークステーションの存在について何も認識していないため、そのアドレスをインターネットにブロードキャストできません。

マスカレード NAT をインプリメントするために重要なのは、さまざまな通信ストリームを区別するためにマスカレード NAT によって発行される論理ポートを使用することです。 TCP には、ソース・ポート番号および宛先ポート番号が含まれます。 NAT によって、これらの指定に論理ポート番号が追加されます。

インバウンドのマスカレード NAT 処理 (応答その他):

このプロセスは、アウトバウンドのマスカレード NAT 処理のパートナーであり、対応するアウトバウンド・メッセージを展開し、正しいワークステーション情報を入手します。

前の図のインバウンド・メッセージは、インターネットからプライベート LAN へのパケットです。インバウンド・データグラムの場合は、宛先ポート番号は論理ポート番号です。(インバウンド・メッセージの場合、ソース・ポート番号は外部ポート番号です。アウトバウンド・メッセージの場合は、宛先ポート番号は外部ポート番号です。)

ローカル接続システムにバインドされているインターネットから返送される応答メッセージには、トランスポート層ヘッダーの宛先ポート番号としてマスカレード割り当ての論理ポート番号があります。 マスカレード NAT のインバウンド処理のステップは以下のとおりです。

1. マスカレード NAT によって、この論理ポート番号 (ソース・ポート) に対してそのデータベースが検索されます。検出されなかった場合、パケットは非送信パケットであると仮定され、送信元に未変更のまま返送されます。その後、通常の不明な宛先として処理されます。
2. 一致する論理ポート番号が検出された場合、ソース IP アドレスが既存の論理ポート番号テーブル項目の宛先 IP アドレスと一致することを確認するためにさらにチェックが行われます。一致した場合、元のローカル・システムのポート番号で、IP ヘッダーのソース・ポートが置換されます。 チェックに失敗した場合、パケットは未変更のままで返送されます。
3. ローカルの一致する IP アドレスが、パケットの IP 宛先に配置されます。
4. IP または TCP によって通常どおりにパケットが処理され、正しいローカル接続システムに送信されます。 マスカレード NAT には、正しいソース・ポート・アドレスおよび宛先ポート・アドレスを確認するために論理ポート番号が必要なため、マスカレード NAT はインターネットからの非送信データグラムを処理できません。

アウトバウンドのマスカレード NAT 処理:

メッセージがプライベート LAN からインターネットへ送信されるときに、このプロセスによりアウトバウンド・メッセージのソース・ポートは固有の論理ポート番号と置換されます。

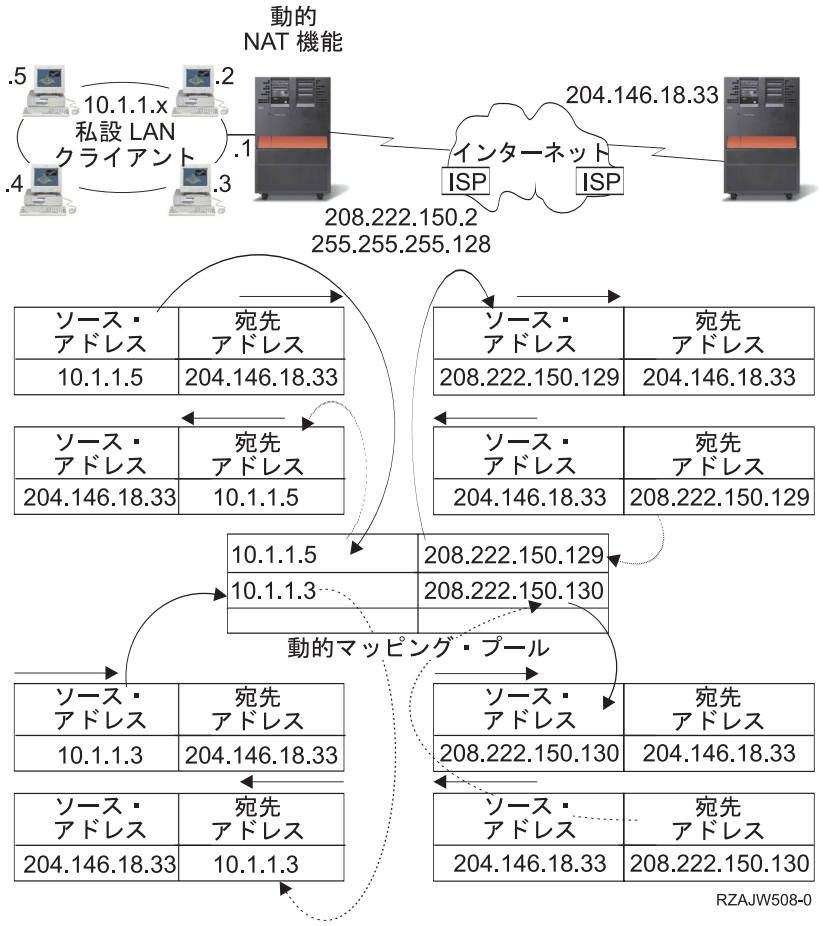
前の図のアウトバウンド・メッセージは、プライベート LAN からインターネットへのパケットです。アウトバウンド・メッセージ (ローカルから外部へ) には、発信元のワークステーションで使用されるソース・ポートが含まれます。 NAT によってこの番号が保存され、トランスポート・ヘッダー内のこの番号が固有の論理ポート番号に置換されます。アウトバウンド・データグラムの場合は、ソース・ポート番号は論理ポート番号です。マスカレード NAT アウトバウンド処理ステップは、次のとおりです。

1. アウトバウンドのマスカレード NAT 処理では、受信されるすべての IP パケットが外部 IP アドレスにバインドされると仮定されるため、パケットをローカルで経路指定する必要があるかどうかを決定するチェックが行われません。
2. 論理ポート番号のセットによって、ソース IP アドレスおよびソース・ポートだけでなく、トランスポート層における一致が検索されます。一致が検出された場合、対応する論理ポート番号がソース・ポートの代わりに使用されます。一致するポート番号が検出されなかった場合、新しいポート番号が作成され、新しい論理ポート番号が選択されて、ソース・ポートの代わりに使用されます。
3. ソース IP アドレスが変換されます。
4. IP によって通常どおりにパケットが処理され、正しい外部システムに送信されます。

動的 NAT

動的 NAT は、私設ネットワーク内から公衆ネットワークへの接続を確立するためだけに使用できます。

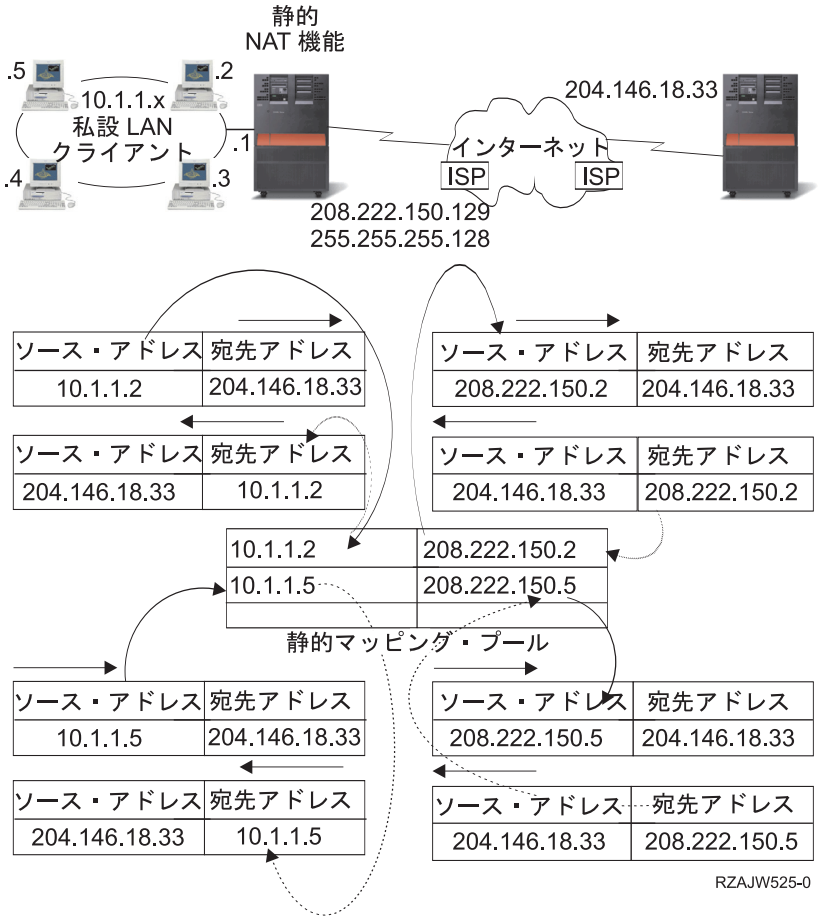
アウトバウンド接続が確立されるときに、ネットワーク・アドレスのプールが保守され、使用されます。各接続には、固有のパブリック・アドレスが割り当てられます。同時接続の最大数は、プール内のパブリック・アドレスの数と同等です。これは、アドレス間の 1 対 1 対応と同様です。動的 NAT を使用すると、動的 NAT アドレスによってインターネットと通信できます。下の図は動的 NAT を示します。



静的 NAT

静的 NAT では、公衆ネットワークから私設ネットワークへのインバウンド接続を使用することができます。

静的 NAT は、私用アドレスと共用アドレスとを単純に 1 対 1 でマッピングします。これには、公衆ネットワークから私設ネットワークへのインバウンド接続のサポートが必要になります。定義されたそれぞれのローカル・アドレスに対して、グローバルで固有な関連付けされたアドレスが必要です。



関連概念

27 ページの『DNS ベースの負荷平準化』
インバウンドの作業負荷には、DNS ベースの負荷平準化を使用します。ローカル・クライアントのために負荷平準化が必要な場合、DNS 負荷平準化を使用します。

OptiConnect および論理区画による経路指定

OptiConnect では高速の光ファイバー・バスを使用することによって、複数の System i プラットフォームを接続することができます。 OptiConnect および論理区画により、プロキシー ARP、2 地点間、および仮想 IP インターフェースなどの経路指定の基本原理を使用できる他の環境が提供されます。

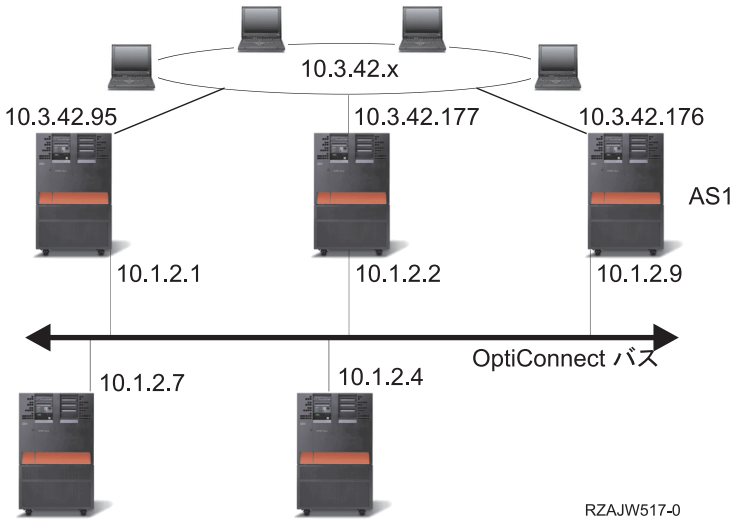
TCP/IP と OptiConnect

OptiConnect バス全体の TCP/IP 接続を定義することができます。OptiConnect 上の TCP/IP は、プロキシー ARP、IP アドレスが定義されていない 2 地点間ネットワーク、仮想 IP インターフェースなどの経路指定組み立てブロックに対する別の方式を提供します。

OptiConnect によってエミュレートされた LAN 構成または OptiConnect 2 地点間構成を使用して、OptiConnect 上の TCP/IP を構成することができます。

以下の図に示されるように、**OptiConnect によってエミュレートされた LAN 構成**により、OptiConnect バスは TCP/IP への LAN として表示されます。構成は簡単ですが、LAN OptiConnect 接続は経路指定情報プロトコル (RIP) や静的経路が必要となるため、自動的には行われません。

OptiConnect によってエミュレートされた LAN 構成



OptiConnect 2 地点間構成では、OptiConnect ホストの各組み合わせに対して構成する 2 地点間の IP アドレスが定義されていないインターフェースを使用します。新しいネットワークは作成されないため、LAN OptiConnect 接続が自動的に行われます。この構成の 1 つの利点は、経路を追加して定義する必要がないことです。 あるネットワークのホストから別のネットワークのホストへの接続は自動的に行われます。もう 1 つの利点は、両方のネットワークが活動状態である場合、システム間で送信されるデータが OptiConnect バスを流れることです。これは、これらの経路が最も細かいサブネット・マスクを持っているためです。 OptiConnect バスがダウンすると、トラフィックは自動的にトークンリング LAN に切り替えられます。

仮想 IP による OptiConnect 2 地点間構成は、IP アドレスが定義されていない 2 地点間構成のバリエーションです。 IP アドレスが定義されていない 2 地点間のインターフェースを使う時は、各インターフェースは必ず関連付けられたローカルのインターフェースを指定しなければなりません。これは、2 地点間リンクのリモート・エンドにあるシステムがローカル・システムの認識に使用する IP アドレスです。 上の図が示すように、システムのプライマリー LAN インターフェースを、この関連付けられたローカル・インターフェースにすることもできます。また、仮想 IP インターフェースをローカルのインターフェースに関連付けて使うこともできます。

仮想 IP を使用した OptiConnect 2 地点間構成では、OptiConnect バスを 2 地点間接続の集まりとして使います。ホストの各組み合わせに IP アドレスが定義されていない接続を定義します。 OptiConnect 2 地点間構成と同様に、経路を追加して定義する必要はなく、あるネットワークのホストから別のネットワークのホストへは自動的に接続されます。この構成の利点は、片方のネットワークが活動状態であれば、i5/OS オペレーティング・システム上で稼働しているいずれかのシステムに接続するパスが存在することです。

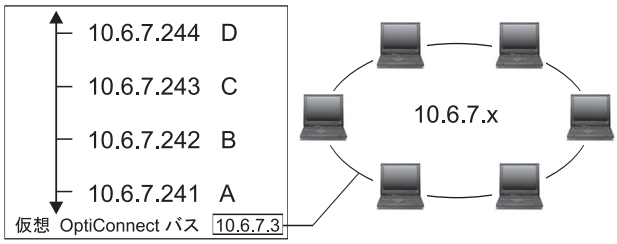
仮想 OptiConnect および論理区画による経路指定

論理区画を使用すると、1 つのシステムに論理区画が作成され、複数の仮想システムに分割されます。 仮想 OptiConnect の TCP/IP インターフェースは、区画間の通信パスとして使用されます。

それぞれの区画は固有のアドレス・スペースや TCP/IP のインスタンスを持ち、固有の専用 I/O アダプターを持つことができます。 TCP/IP 側からは、各区画が別個のシステムとして認識されます。 異なる区画間の TCP/IP 通信は、OptiConnect 仮想バスを使って行われます。TCP/IP の経路指定コードで使用する別の区画へのパスは、OptiConnect 物理バスで接続した別システムへのパスと同じです。

論理区画: 仮想 OptiConnect TCP/IP インターフェースは、
区画間通信パスとして使用されます。

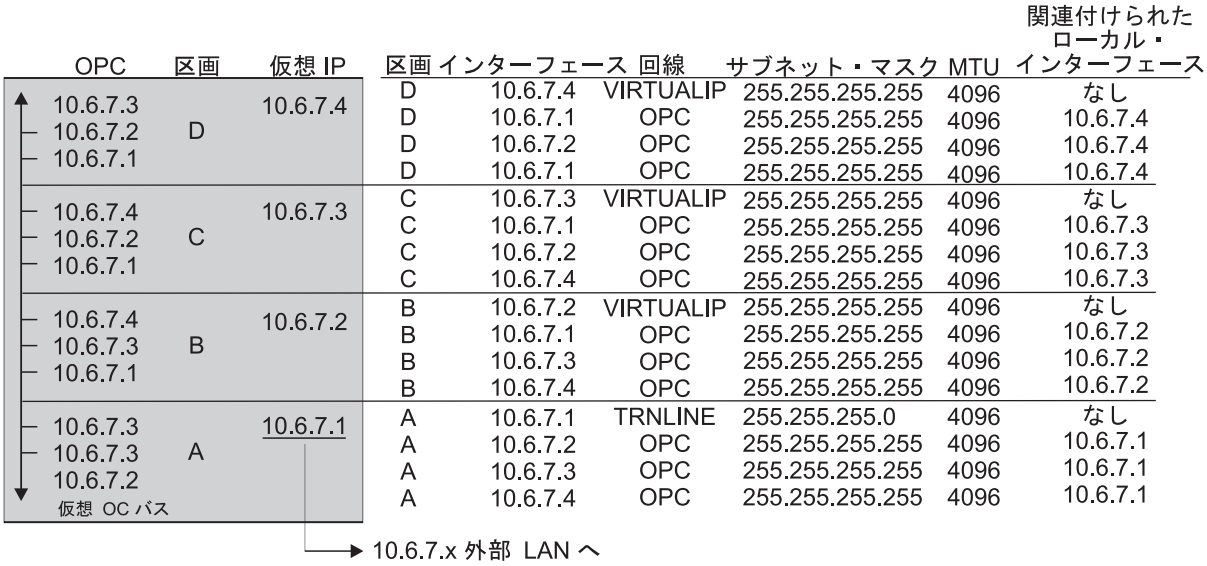
仮想 OptiConnect ネットワーク = 10.6.7.241 - 10.6.7.254
14 区画間までアドレスを提供します。



区画	インターフェース	回線	サブネット・マスク	MTU	
D	10.6.7.244	*OPC	255.255.255.240	4096	
C	10.6.7.243	*OPC	255.255.255.240	4096	
B	10.6.7.242	*OPC	255.255.255.240	4096	関連付けられた
A	10.6.7.241	*OPC	255.255.255.240	4096	ローカル・インター
A	10.6.7.3	TRNLINE	255.255.255.0	4096	フェース = 10.6.7.3)

RZAJW515-0

これらの例では、システムの中に LAN アダプターが 1 つだけインストールされています。 LAN アダプターは、区画 A に割り当てられます。LAN のクライアントは、システムで定義された別の区画と通信する必要があります。そのためには、OptiConnect 仮想バス上で透過サブネットを定義します。この LAN システムは 10.6.7.x のネットワーク・アドレスを持ちます。区画を追加する場合は、IP アドレスが必要になります。 12 個のアドレスを取得するには、255.255.255.240 のサブネット・マスクを使用します。こうすれば 10.6.7.241 から 10.6.7.254 まで、合計 14 個のアドレスを使用することができます。必ず、これらのアドレスが LAN で使われていないことを確認してください。アドレスを取得したら、各区画に割り当てます。各区画にインターフェースを 1 つ追加して、OptiConnect 仮想バスのアドレスを定義します。



区画	インターフェース	回線	サブネット・マスク	MTU	関連付けられたローカル・インターフェース
D	10.6.7.4	VIRTUALIP	255.255.255.255	4096	なし
D	10.6.7.1	OPC	255.255.255.255	4096	10.6.7.4
D	10.6.7.2	OPC	255.255.255.255	4096	10.6.7.4
D	10.6.7.1	OPC	255.255.255.255	4096	10.6.7.4
C	10.6.7.3	VIRTUALIP	255.255.255.255	4096	なし
C	10.6.7.1	OPC	255.255.255.255	4096	10.6.7.3
C	10.6.7.2	OPC	255.255.255.255	4096	10.6.7.3
C	10.6.7.4	OPC	255.255.255.255	4096	10.6.7.3
B	10.6.7.2	VIRTUALIP	255.255.255.255	4096	なし
B	10.6.7.1	OPC	255.255.255.255	4096	10.6.7.2
B	10.6.7.3	OPC	255.255.255.255	4096	10.6.7.2
B	10.6.7.4	OPC	255.255.255.255	4096	10.6.7.2
A	10.6.7.1	TRNLINE	255.255.255.0	4096	なし
A	10.6.7.2	OPC	255.255.255.255	4096	10.6.7.1
A	10.6.7.3	OPC	255.255.255.255	4096	10.6.7.1
A	10.6.7.4	OPC	255.255.255.255	4096	10.6.7.1

rzajw516-0

以下の記述が「真」の場合に、透過サブネットは自動的に使用可能になります。第 1 に、OptiConnect 仮想バスが LAN 実インターフェースの MTU のサイズ以下であること。第 2 に、OptiConnect バス・サブネットが LAN ネットワーク・アドレスのサブネットであること。この 2 つの記述が「真」の場合、透過

サブネットが自動的に使用可能になります。インターフェース 10.6.7.3 は、区画で定義したすべてのインターフェースのプロキシーとして機能します。これによって、LAN のクライアントは区画に接続することができます。

TCP/IP 作業負荷の平準化の方式

*作業負荷の平準化*を行うと、複数のプロセッサー、複数のインターフェース・アダプター、または複数のホスト・システム間でアクセス数が多いシステムのネットワーク・トラフィックおよび作業負荷が再分散されます。

i5/OS オペレーティング・システムで最高のパフォーマンスを実現するには、通信作業負荷をシステムの複数の部分に分散する必要があります。

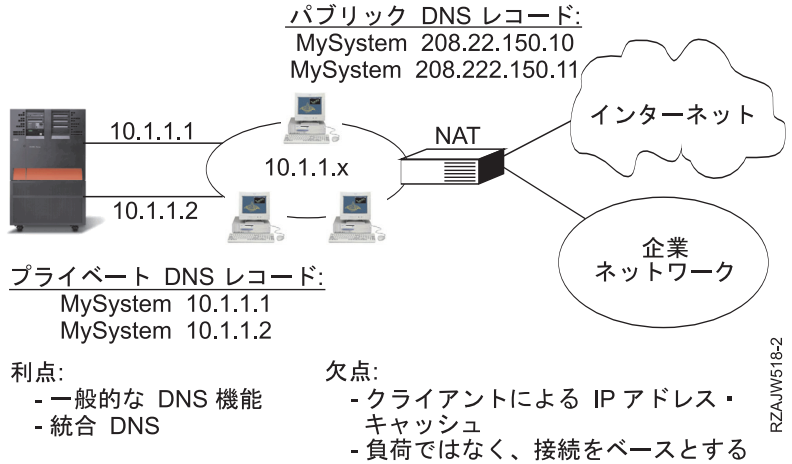
以下のようなさまざまな TCP/IP 経路指定方式を使って、システムの作業負荷の平準化を行うことができます。

DNS ベースの負荷平準化

インバウンドの作業負荷には、DNS ベースの負荷平準化を使用します。ローカル・クライアントのために負荷平準化が必要な場合、DNS 負荷平準化を使用します。

DNS ベースの負荷平準化は、インバウンドの負荷平準化に使用されます。複数のホスト IP アドレスは、単一のホスト・システム名の DNS で構成されます。 DNS によって、連続するクライアント・ホスト名の解決要求に対して返されるホスト IP アドレスが変更されます。このタイプの負荷平準化の利点は、一般的な DNS 機能であるということです。このソリューションの不便な点は、IP アドレスがクライアントによってキャッシュ可能であることと、負荷ベースのソリューションではなく、接続ベースのソリューションであるということです。

負荷平準化を達成する最初の方法は、DNS 機能を使って、同一のシステム名に複数のアドレスを配布することです。システム名のアドレス・レコードに対して要求が行われるたびに、DNS によって、異なる IP アドレスが提供されます。以下の例では、各アドレスは異なるシステムに対応します。これによって、2 つの異なるシステム間に負荷平準化を提供できます。私設ネットワーク上のクライアントの場合、各要求ごとに異なるアドレスを受け取ります。これが、一般的な DNS 機能です。パブリック DNS にも 2 つのアドレス項目があることに注意してください。これらのアドレスは、静的 NAT を使って変換され、ユーザーがインターネット上にいる場合、2 つのシステムにアクセスできます。



最初の接続後に特定のシステムにアクセスするか、または同じシステムに返るかがプログラムによって異なる場合、最初の接続が行われた後に異なるシステム名を送信するように Web ページおよびサイトをコード化する必要があります。追加 DNS エントリーを MyServer1 208.222.150.10 および MyServer2 208.222.150.11 に追加することができます。これを行うことにより、Web サイトは、たとえば、最初の接触の後に MyServer2 を指すことができます。このタイプの負荷平準化では、接続要求による平準化が提供されます。多くの場合、アドレスを解決した後、クライアントはアドレスをキャッシュに入れて、再び要求しません。このタイプの負荷平準化では、各システムへのトラフィックの量は考慮されません。このタイプの負荷の平準化はインバウンド・トラフィックのみ考慮し、2 つのシステム上に 1 つのアダプターを所有する代わりに、1 つのシステム上に 2 つのアダプターを所有できます。

関連概念

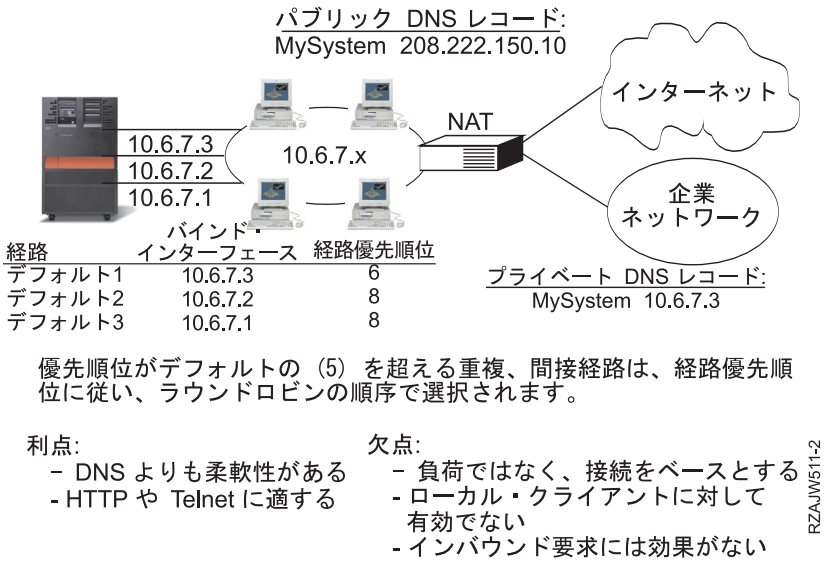
23 ページの『静的 NAT』
静的 NAT では、公衆ネットワークから私設ネットワークへのインバウンド接続を使用することができます。

重複経路ベースの負荷平準化

重複経路ベースの負荷平準化は、複数のインターフェースに及ぶアウトバウンドの作業負荷の平準化に使用できます。

これは、DNS ベースの負荷平準化より柔軟性がある接続ベースのソリューションですが、ローカル・クライアントには有効ではありません。このタイプの負荷平準化を使用する利点は、これが i5/OS 全体のソリューションであること、DNS よりも柔軟性があること、および HTTP や Telnet のようにトラフィックのほとんどがアウトバウンドのアプリケーションに適していることです。 欠点は、接続ベースのソリューションであること (負荷ベースのソリューションではなく)、ローカル・クライアントに対してアクティブでないこと、およびインバウンド要求に影響がないことです。

次の例では、ご使用のシステム上の 3 つのアダプターはすべて同じ LAN セグメントに接続されています。アダプターのうちの 1 つをインバウンド回線専用として設定し、その他の 2 つのアダプターをアウトバウンドとして設定しています。ローカル・クライアントは、これまでと同様に動作します。つまり、アウトバウンド・インターフェースはインバウンド・インターフェースと同じです。ローカル・クライアントは、アクセスするためにルーターを必要としないシステムです。ルーターの代わりにスイッチを使用する場合、これは大規模ネットワークになる場合があります。



TCP/IP 経路追加 (ADDTCPRTE) コマンドまたはSystem i ナビゲーター・インターフェースを使用して重複経路ベースの負荷平準化を構成することができます。これは重複経路の優先順位または優先バインド・インターフェースのどちらかを設定することで達成されます。重複経路の優先順位の値がデフォルトの 5 のままの場合、何も起こりません。 5 より大きい値が設定されている場合、接続は同じ優先順位で経路間に分配されます。優先バインド・インターフェースは、IP アドレスによる特定のインターフェースへの経路をバインドするために使用されます。

前の例では、重複経路優先順位 6 を持つ「インバウンド」アダプター (10.6.7.3) があります。他の 2 つのアダプターは重複経路優先順位 8 を使用して構成されます。1 つのアダプターの重複経路優先順位は 6 なので、すべての単一経路優先順位インターフェース 8 がダウンしていない限り、アウトバウンド接続のために選択されません。

すべてのアウトバウンド・インターフェースを同じ優先順位にする必要があります。異なる優先順位を設定した場合、最高値のインターフェースのみが使用されます。

DNS は 10.6.7.3 インターフェースにポイントし、それをインバウンド・インターフェースにします。重複経路の優先順位を使用しないことにした場合でも、優先バインド・インターフェース・パラメーターを使って、各インターフェースにシステムからのデフォルト経路を常に定義する必要があります。

仮想 IP およびプロキシー ARP を使用した負荷平準化

仮想 IP およびプロキシー ARP を使用して、複数のインターフェースに及ぶ負荷平準化を達成することができます。この作業負荷の平準化の方式は、インバウンドおよびアウトバウンドの作業負荷の両方をサポートします。

以下は、仮想 IP およびプロキシー ARP を作業負荷の平準化の方式として使用した場合の利点です。

- インバウンドおよびアウトバウンドの作業負荷の両方をサポートします。
- ローカル・クライアントをサポートします。
- DNS ベースおよび重複経路ベースの負荷平準化の方式よりもすぐれた柔軟性を提供します。

この作業負荷の平準化の方式の不便な点は、負荷ベースのソリューションではなく、接続ベースのソリューションであるということです。各インターフェースの負荷は考慮されていません。すべての接続のトラフィックの負荷は同じであることを前提としています。

以下の例は、仮想 IP アドレスの使用の利点を最大限に活用した例です。各アプリケーションに固有の仮想 IP アドレスをバインドする以外に、この例ではインバウンドおよびアウトバウンド接続の平衡化、およびフォールト・トレランスのいくつかのレベルを提供しています。

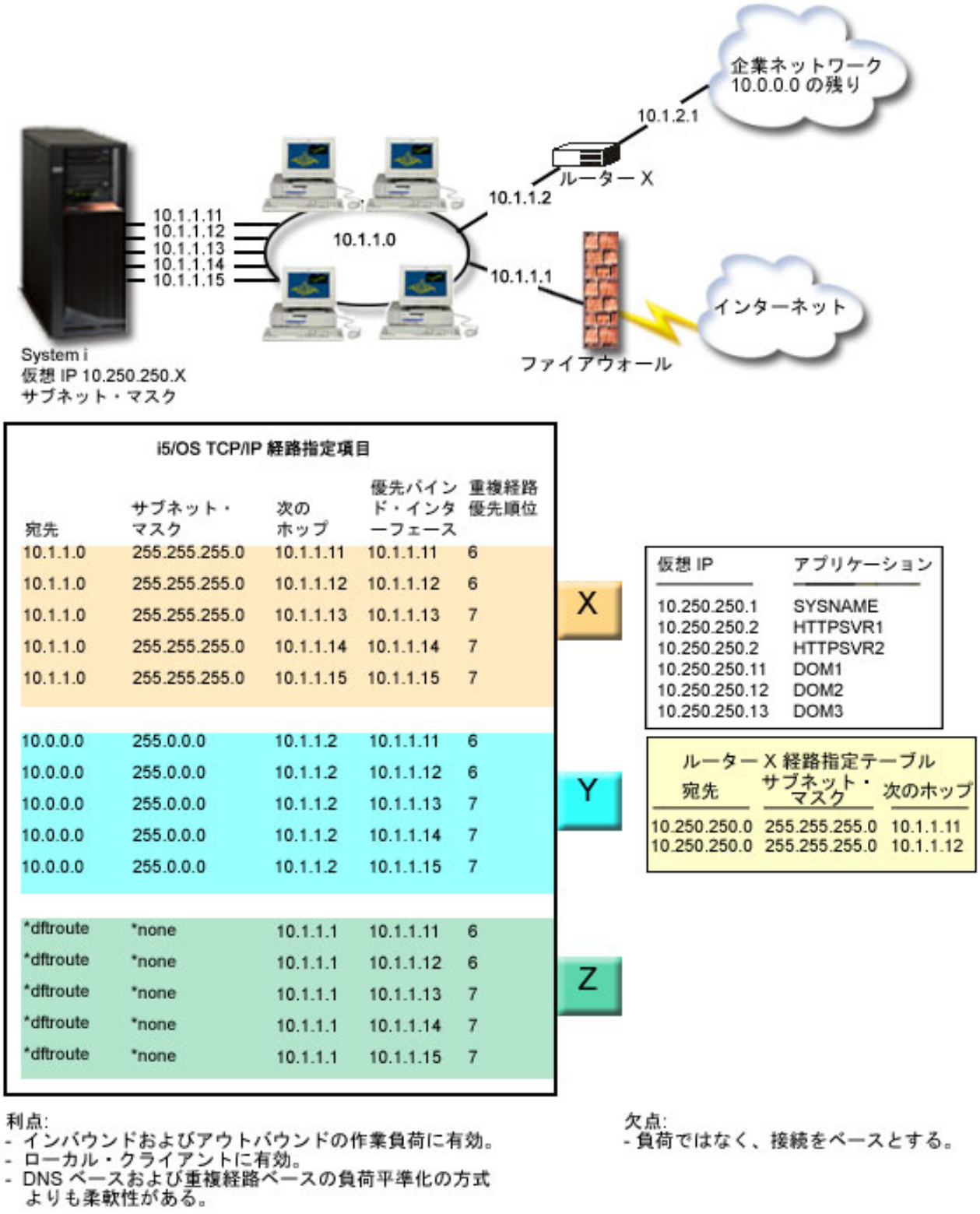


図 3. 仮想 IP およびプロキシー ARP を使用した負荷平準化

この例では、インバウンド接続の平衡化は、システムで定義される仮想 IP アドレス、および外部ルーター、ファイアウォール、およびレイヤー 3 (ネットワーク層) の経路指定を実行できるスイッチを使用する

ことによって達成されます。アウトバウンド接続の平衡化は、i5/OS TCP/IP 経路指定項目で優先バインド・インターフェースおよび重複経路の優先順位のパラメーターを使用することによって達成されます。アウトバウンド接続は、重複経路の優先順位の値がデフォルトの 5 より大きく設定されているとき、同じ重複経路の優先順位ですべてのインターフェース間にラウンドロビン方式で分配されます。1 つの値ですべてのインターフェースが使用不可になった場合、システムはその次に低い値のインターフェースに切り替わります。

ルーター X で構成されている経路指定ディレクティブでは、インターフェース 10.1.1.11 および 10.1.1.12 がプライマリー・インバウンド・インターフェースとしてセットアップされます。インバウンド接続は、インターフェース 10.1.1.11 および 10.1.1.12 間にラウンドロビン方式で分配されます。これはほとんどのルーターで提供される機能です。

i5/OS TCP/IP 経路指定項目では、重複経路の優先順位 7 のインターフェース 10.1.1.13、10.1.1.14、および 10.1.1.15 が、プライマリー・アウトバウンド・インターフェースとしてセットアップされます。アウトバウンド接続は、インターフェース 10.1.1.13、10.1.1.14、および 10.1.1.15 間にラウンドロビン方式で分配されます。これらの 3 つのインターフェースすべてがダウンした場合、重複経路の優先順位 6 のインターフェース 10.1.1.11 および 10.1.1.12 は、アウトバウンドおよびインバウンドの両方の接続として使用されます。

この例では、i5/OS TCP/IP 経路指定項目は 3 つのグループから構成されます。グループ X は、企業ネットワーク (10.1.1.0) のローカル・セグメントにアウトバウンド接続の平衡化を提供します。グループ Y は、ルーターを通して企業ネットワーク (10.0.0.0) の残りにアウトバウンド接続の平衡化を提供します。グループ Z は、ファイアウォールを通してインターネットにアウトバウンド接続の平衡化を提供します。

関連概念

『シナリオ: 仮想 IP およびプロキシー ARP を使用したアダプター・フェイルオーバー』
仮想 IP アドレスを使用すると、特定のインターフェースではなく、システムにアドレスを割り当てることができます。 複数のシステムに同じアドレスを定義することにより、負荷平準化の多数の新しいオプションが使用可能になります。

シナリオ: 仮想 IP およびプロキシー ARP を使用したアダプター・フェイルオーバー

仮想 IP アドレスを使用すると、特定のインターフェースではなく、システムにアドレスを割り当てることができます。 複数のシステムに同じアドレスを定義することにより、負荷平準化の多数の新しいオプションが使用可能になります。

注: このフェイルオーバーのシナリオでは、クラスタリングのような主要なタイプのシステム障害ではなく、単一の LAN アダプターについて説明します。このソリューションには、外部の負荷平準化システムが必要です。

状態

ご使用の実動用システムは、リモート・クライアントと LAN クライアントの両方からデータ入力を処理します。 iSeries には企業の重要なアプリケーションが含まれています。企業の成長に従い、System i ハードウェアおよびネットワークに対する要求も増大します。 企業の成長により、予定にないダウン時間を発生させることなくシステムをネットワーク上で使用可能にすることが必須となってきました。何らかの理由で、ネットワーク・アダプターが使用不可能になった場合は、システム上の他のネットワーク・アダプターがこれを引き継ぎ、ネットワーク・クライアントからはいかなる障害も感知されないようにする必要があります。

目標

可用性という概念には、障害が生じているコンポーネントの冗長度やバックアップに関するさまざまな局面が関与します。このシナリオでは、アダプターに障害が生じたときにシステムのクライアントに対してネットワークを使用可能にすることを目的としています。

詳細

上記の状態を取り扱う方法の 1 つは、System i プラットフォームから LAN への複数の物理接続を用意することです。次の図を検討してください。

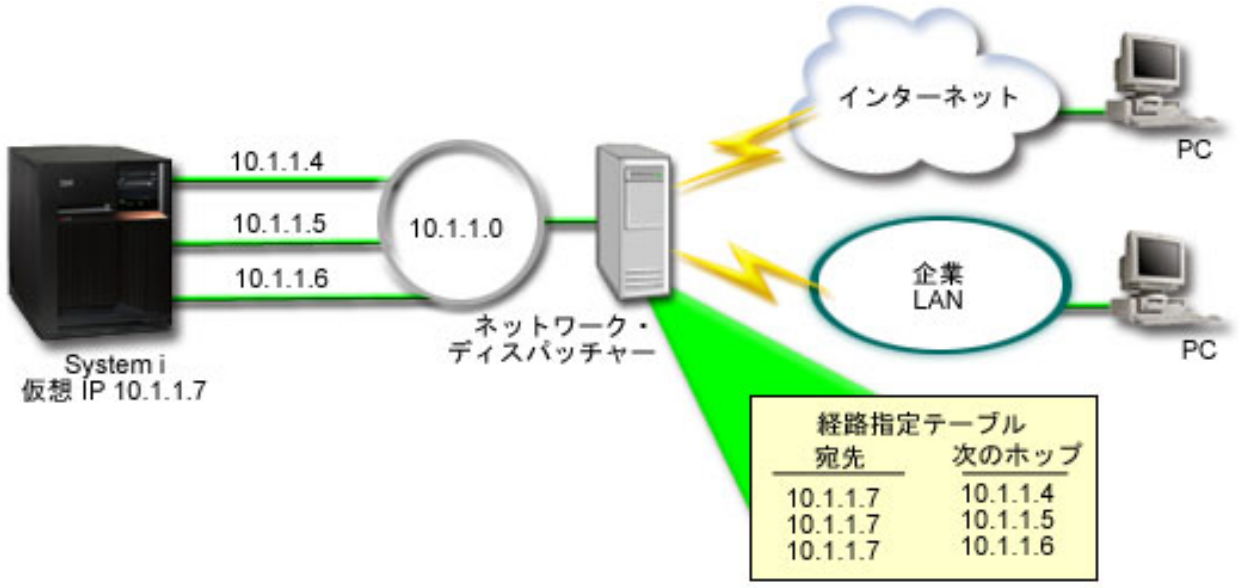


図 4. ローカル・クライアントを使用しない場合のアダプター・フェイルオーバー

各物理接続は異なる IP アドレスを持ちます。その後、ユーザーがシステムに対し、仮想 IP アドレスを割り当てることができます。すべてのクライアントは、この仮想 IP アドレスによって、IP アドレスを認識します。すべてのリモート・クライアント (System i プラットフォームと同じ LAN に物理的に接続されていないクライアント) は、ネットワーク・ディスパッチャーなどの外部の負荷平準化サーバーを経由してシステムと通信します。リモート・クライアントからの IP 要求がネットワーク・ディスパッチャーを経由すると、ネットワーク・ディスパッチャーは仮想 IP アドレスをシステム上のネットワーク・アダプターの 1 つに経路指定します。

システムが接続している LAN にクライアントがある場合、これらのクライアントでは、ローカル内に向けたトラフィックを送信する場合にネットワーク・ディスパッチャーは使用しません。ネットワーク・ディスパッチャーが必要以上に過負荷になるからです。 ネットワーク・ディスパッチャーの経路指定テーブルに似た経路指定項目を各クライアントに作成することはできます。しかし、LAN にローカル・クライアントの数が多い場合には、これは非実用的です。 このような状況を以下の図に示します。

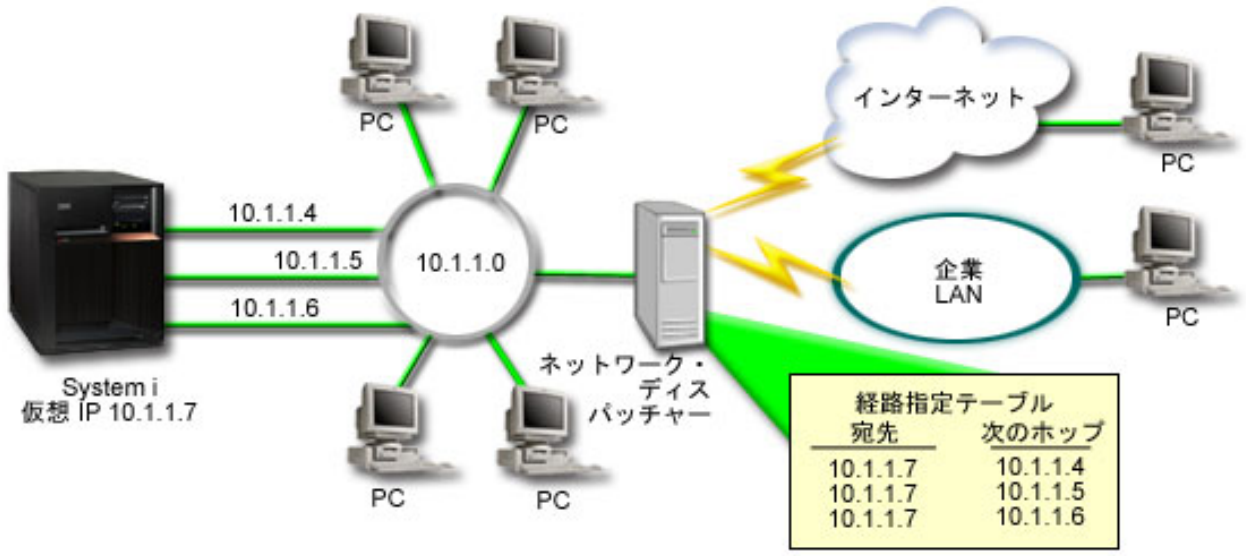


図 5. ローカル・クライアントを使用する場合のアダプター・フェイルオーバー

ARP を使用してローカル・クライアント (システムと同じ LAN に接続されているクライアント) をシステムの仮想 IP アドレスに接続することが可能になりました。これにより、ローカル・クライアントでアダプター・フェイルオーバーのソリューションを使用することも可能になりました。

いずれの場合も、ローカル・クライアントとリモート・クライアントはフェイルオーバーが発生しても認識しません。システムにより、どのアダプターと IP アドレスを、仮想イーサネットと仮想 IP アドレス (VIPA) プロキシー・アドレス解決プロトコル (ARP) エージェント選択のための優先インターフェースとするかが選択されます。

どのアダプターと IP アドレスを、VIPA プロキシー ARP エージェント選択のための優先インターフェースとするかを手動で選択することができます。アダプター障害が生じた場合に優先インターフェース・リストを作成することにより使用するインターフェースを選択することができます。優先インターフェース・リストは、障害が生じたアダプターを引き継ぐインターフェース・アドレスの番号付きリストです。 System i ナビゲーターまたは Change TCP/IP IPv4 Interface (QTOCC4IF) アプリケーション・プログラミング・インターフェース (API) を使用して、優先インターフェース・リストを構成することができます。 優先インターフェース・リストは、仮想イーサネットと仮想 IP アドレス・インターフェースの両方のために構成可能です。

図 2 を例として使用すると、リモート・クライアントは仮想 IP アドレス 10.1.1.7 を使用してローカル・システムと通信しています。10.1.1.4 がこの通信に使用する初期ローカル・アダプターで、10.1.1.4 に障害が生じた場合、10.1.1.5 に引き継ぐと仮定します。 10.1.1.4 と 10.1.1.5 のアダプターの両方に障害が生じた場合は、インターフェース 10.1.1.6 に引き継ぎます。 フェイルオーバー状態でこれらのインターフェースを使用する順序を制御するため、仮想 IP アドレス 10.1.1.7 の優先インターフェース・リストを定義することができます。この場合、これは 10.1.1.4、10.1.1.5 および 10.1.1.6 から構成されるインターフェース・アドレスの番号付きリストです。

このソリューションには複数の System i を使用して互いにサポートし合うことも含まれます。 システムのうち 1 つが使用不可になった場合、フェイルオーバーとして 2 番目のシステムでサービスを提供することができます。 以下の図は、同じセットアップで 2 つのシステムを使用した場合を示しています。

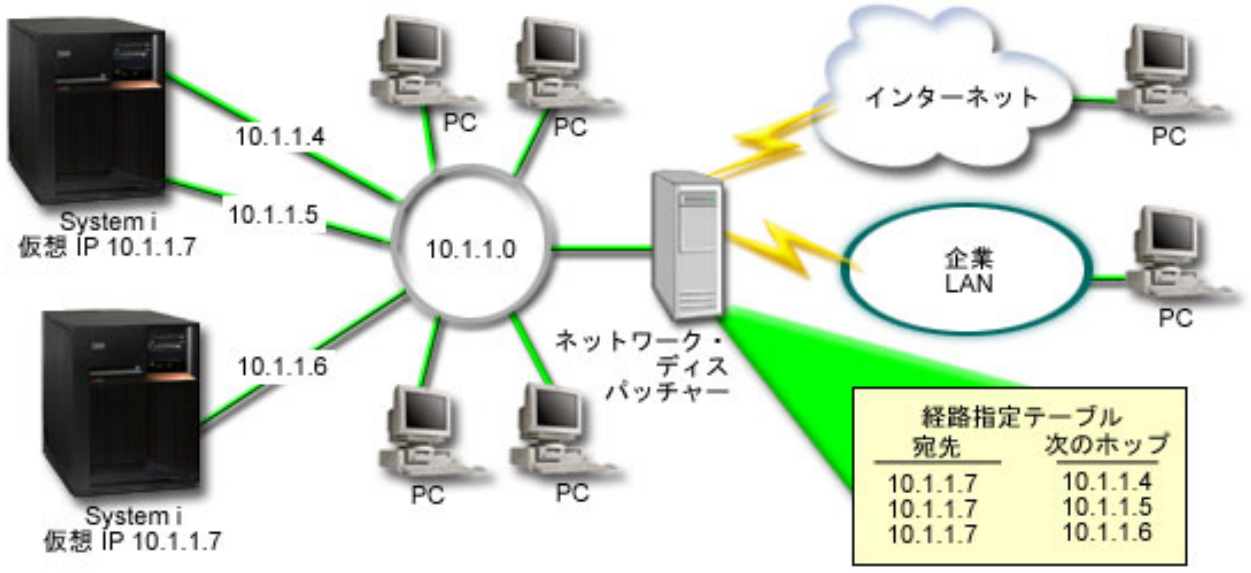


図 6. 複数の System i プラットフォームとローカル・クライアントを使用する場合のアダプター・フェイルオーバー

パケットの経路指定は、単一のシステムとそのリモート・クライアントの場合と同じです。しかし、ローカル・クライアントの場合は大きく異なります。 複数のシステムで同じ仮想 IP アドレスを使用している場合は、それらのシステムのうちの 1 つだけしかプロキシーとして使用することができません。この場合、LAN 接続を 2 つ持つシステムをプロキシーとして使用します。

構成ステップ

仮想 IP およびプロキシー ARP を使用した負荷平準化の構成は、標準の TCP/IP 構成に仮想 TCP/IP インターフェースを追加したものと似ています。

関連概念

29 ページの『仮想 IP およびプロキシー ARP を使用した負荷平準化』
仮想 IP およびプロキシー ARP を使用して、複数のインターフェースに及ぶ負荷平準化を達成することができます。この作業負荷の平準化の方式は、インバウンドおよびアウトバウンドの作業負荷の両方をサポートします。

自動インターフェース選択を使用したフェイルオーバー

以下のステップを使用して、このシナリオのアダプター・フェイルオーバーの状態に対する仮想 IP およびプロキシー ARP の構成を行います。

図 2 を例として使用して、一般的な構成ステップは次のようになります。

1. 仮想 TCP/IP インターフェースの構成

   System i ナビゲーターを使用して仮想 TCP/IP を作成します。以下のように選択して新規「仮想 IP インターフェース」ウィザードを表示します。「**ネットワーク**」 → 「**TCP/IP 構成**」 → 「**IPv4**」 → 「**インターフェース**」次に「**インターフェース**」を右マウス・ボタン・クリックして、「**新規インターフェース**」 → 「**仮想 IP**」を選択します。

例では、サブネット・マスクを使用して 255.255.255.255 の IP アドレス 10.1.1.7 を入力します。仮想インターフェースを作成したら、そのインターフェースを右マウス・ボタン・クリックして、「**プロパティー**」を選択します。「**拡張**」タブをクリックして、「**プロキシー ARP の使用可能化**」チェック・ボックスを選択します。

2. すべての物理 LAN 接続について TCP/IP インターフェースを作成

   「TCP/IP インターフェースの作成」ウィザードを使用して、TCP/IP インターフェースを作成します。このウィザードは、System i ナビゲーターに入っており、以下のように選択して表示します。「**ネットワーク**」 → 「**TCP/IP 構成**」 → 「**IPv4**」 → 「**インターフェース**」 次に「**インターフェース**」を右マウス・ボタン・クリックして、「**新規インターフェース**」 → 「**ローカル・エリア・ネットワーク**」を選択します。 各 LAN 接続についてこのウィザードを完了してください。

   この例では、ウィザードを 3 回実行し、サブネット・マスク 255.255.255.0 を使用して IP アドレス 10.1.1.4、10.1.1.5、および 10.1.1.6 を入力します。 各インターフェースを完了後、インターフェースを右マウス・ボタン・クリックして、「**プロパティー**」を選択します。 「**拡張**」タブをクリックし、「**関連付けられたローカル・インターフェース (Associated local interface)**」チェック・ボックスを選択して、インターフェースを ステップ 1 で作成した仮想 IP インターフェースと関連付けます。

優先インターフェース・リストを使用したフェイルオーバー

優先インターフェース・リストを作成して、アダプター障害が発生したときにローカル・インターフェースを使用する順序を制御することができます。

優先インターフェース・リストを作成するには、以下のステップを実行します。

1. System i ナビゲーターで、「**ネットワーク**」 → 「**TCP/IP 構成**」 → 「**IPv4**」を選択します。
2. 「**インターフェース**」をクリックします。
3. 表示されるインターフェースのリストから、優先インターフェース・リストを作成する仮想 IP アドレスまたは仮想イーサネットのためのインターフェースを選択します。

   図 2 を例として使用して、仮想 IP アドレス 10.1.1.7 を選択します。
4. インターフェースを右マウス・ボタン・クリックしてから、「**プロパティー**」を選択します。
5. 「**拡張**」タブをクリックします。
6. パネルで、「Available interface list (使用可能なインターフェース・リスト)」からインターフェース・アドレスを選択して、「**追加**」をクリックします。

   図 2 を例として使用して、インターフェース 10.1.1.4、10.1.1.5、および 10.1.1.6 を選択して、優先インターフェース・リストに 1 つずつ追加します。

   「**削除**」ボタンを使用することにより右ペインの優先インターフェース・リストからインターフェースを削除するか、「**上へ移動**」と「**下へ移動**」ボタンを使用することにより、インターフェースを上下に移動して、順序を変更することもできます。
7. 「Available interfaces list (使用可能なインターフェース・リスト)」の上にある「**プロキシー ARP の使用可能化**」を選択して、リストを有効にします。
8. 「**OK**」をクリックして、作成した優先インターフェース・リストを保管します。

注: 優先インターフェース・リストに 10 個のみのインターフェースを含めることができます。10 個を超えるインターフェースを構成した場合は、最初の 10 個のみに切り捨てられます。

TCP/IP 経路指定および作業負荷の平準化に関する関連情報

他の Information Center のトピック・コレクションには、TCP/IP 経路指定および作業負荷の平準化のトピック・コレクションに関連する情報が含まれています。

その他の情報

- 「DNS」

  DNS は、TCP/IP ネットワーク上のインターネット・プロトコル (IP) アドレスに関連付けられたホスト名を管理するための拡張システムです。ここでは、DNS の構成および管理方法を理解するために必要な基本概念とプロシージャーについて説明します。

- 論理区画

  このトピック・コレクションでは、より多くの詳細なバックグラウンド情報が提供されます。

- IP フィルター操作とネットワーク・アドレス変換

  このトピック・コレクションの情報はフィルター規則を管理するのに役立ちます。この機能には、注釈の追加、編集、および表示が含まれます。

- OptiConnect

  このトピック・コレクションでは OptiConnect 経路指定に関する情報が提供されます。

- リモート・アクセス・サービス : PPP 接続

  Point-to-Point Protocol (PPP) はインターネットにコンピューターを接続するために通常使用されます。PPP は、インターネット標準であり、インターネット・サービス・プロバイダー (ISP) の間で最も広く使用されている接続プロトコルです。

  関連資料

  2 ページの『TCP/IP 経路指定および作業負荷の平準化の PDF ファイル』
  この情報の PDF ファイルを表示および印刷することができます。

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

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

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

〒106-8711
東京都港区六本木 3-2-12
IBM World Trade Asia Corporation
Intellectual Property Law & Licensing

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

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

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

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

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

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

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

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

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

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

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

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

著作権使用許諾:

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

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

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

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

プログラミング・インターフェース情報

この「TCP/IP 経路指定および作業負荷の平準化」資料には、プログラムを作成するユーザーが IBM i5/OS のサービスを使用するためのプログラミング・インターフェースが記述されています。

商標

以下は、International Business Machines Corporation の米国およびその他の国における商標です。

i5/OS
IBM
IBM (ロゴ)
System i

Adobe、Adobe ロゴ、PostScript、および PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における商標です。

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

使用条件

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

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

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

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

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

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

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

Printed in Japan

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