

TCP/IP の概要

内容

[概要](#)

[TCP/IP テクノロジー](#)

[TCP](#)

[IP](#)

[IP 環境でのルーティング](#)

[内部ルーティング プロトコル](#)

[RIP](#)

[IGRP](#)

[EIGRP](#)

[OSPF](#)

[Integrated IS-IS](#)

[外部ルーティング プロトコル](#)

[EGP](#)

[BGP](#)

[シスコの TCP/IP 実装](#)

[アクセス制限](#)

[トンネリング](#)

[IP マルチキャスト](#)

[ネットワーク情報の抑制](#)

[アドミニストレーティブ ディスタンス](#)

[ルーティング プロトコルの再配布](#)

[サーバレス ネットワークのサポート](#)

[ネットワークのモニタリングとデバッグ](#)

[要約](#)

[関連情報](#)

概要

ネットワークが発明されてから 20 年、イーサネット、トークン リング、Fiber Distributed Data Interface (FDDI)、X.25、フレーム リレー、スイッチド マルチメガビット データサービス (SMDS)、統合デジタル通信網サービス (ISDN)、そして最近では非同期転送モード (ATM) が導入され、その多様性は拡大を続けています。インターネット プロトコルは、この多様な LAN および WAN テクノロジーを相互接続する方法として最も実績があります。

インターネット プロトコル スイートには、伝送制御プロトコル (TCP) やインターネット プロトコル (IP) などの低レベルの仕様だけではなく、電子メール、端末エミュレーション、ファイル転送といった一般的なアプリケーションの仕様も含まれています。[図 1 に、TCP/IP プロトコル スイートと OSI 参照モデルの対比を示します。図 2 は、いくつかの重要なインターネット プロトコルと、それらの OSI 参照モデルとの関係を示しています。](#) OSI 参照モデルと各階層の役割

の詳細については、『インターネットワーキングの基礎』に関するドキュメントを参照してください。

インターネット プロトコルは、現在使用されている最も広く実装されたマルチベンダー プロトコルスイートです。少なくとも、インターネット プロトコル スイートの部分的なサポートは、ほとんどすべてのコンピュータベンダーで利用できます。

TCP/IP テクノロジー

この項では、TCP、IP、関連プロトコル、およびこれらのプロトコルが動作する環境の技術的側面について説明します。このドキュメントは主にルーティング (レイヤ 3 機能) に重点を置いているため、TCP (レイヤ 4 プロトコル) については比較的簡単な説明になります。

TCP

TCP は、非構造化バイト ストリームとしてデータを送信するコネクション型のトランスポート プロトコルです。TCP では、シーケンス番号と確認応答メッセージを使用することで、宛先ノードに送信されたパケットの配信情報が送信側ノードに提供されます。送信元から宛先への転送中にデータが失われた場合、タイムアウト状態になるか、正常に配信が完了するまで、TCP はデータを再送信できます。TCP は重複メッセージを認識することもでき、該当するメッセージを適切に破棄します。送信側コンピュータの転送速度が速すぎて受信側コンピュータが対応できない場合、TCP はフロー制御メカニズムを使用してデータ転送速度を下げることもできます。TCP は、サポートする上位層プロトコルとアプリケーションに配信情報を伝えることもできます。これらすべての特性により、TCP はエンドツーエンドの信頼性の高いトランスポート プロトコルとされています。TCP の仕様は、[RFC 793](#) で規定されています。

図 1 : TCP/IP プロトコルスイートと OSI 参照モデルの対比

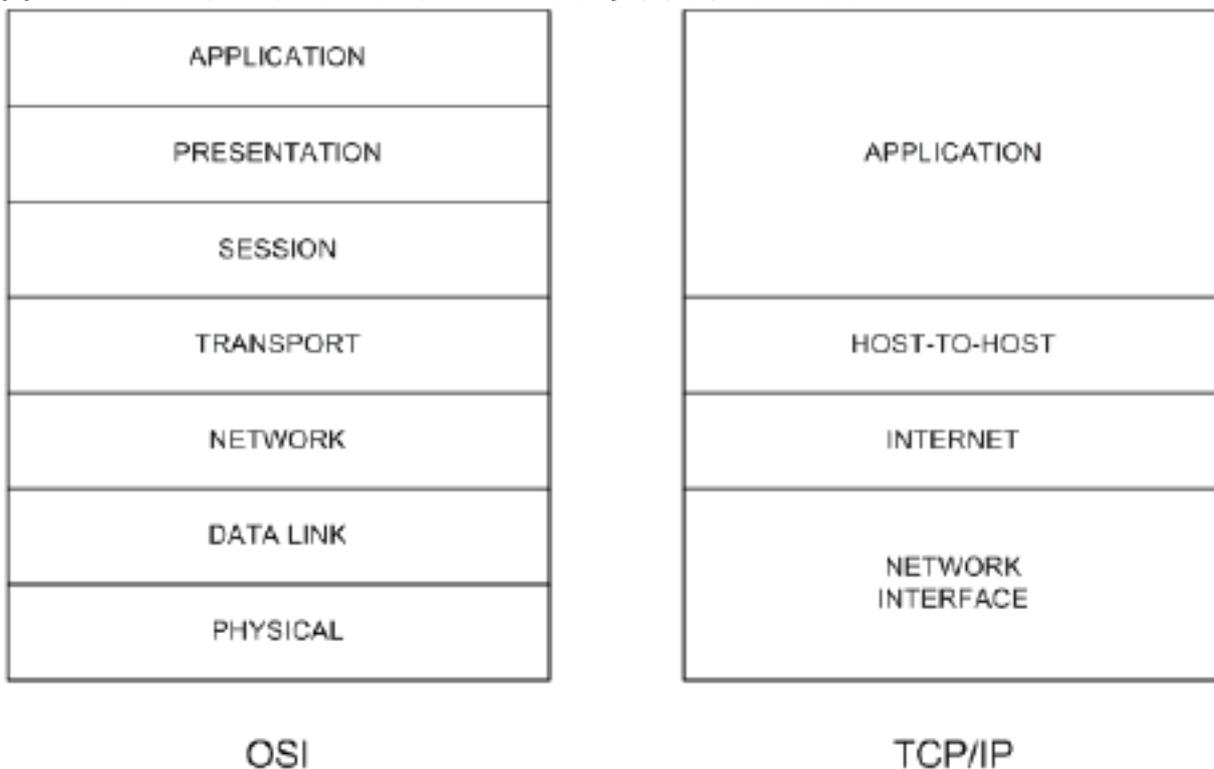
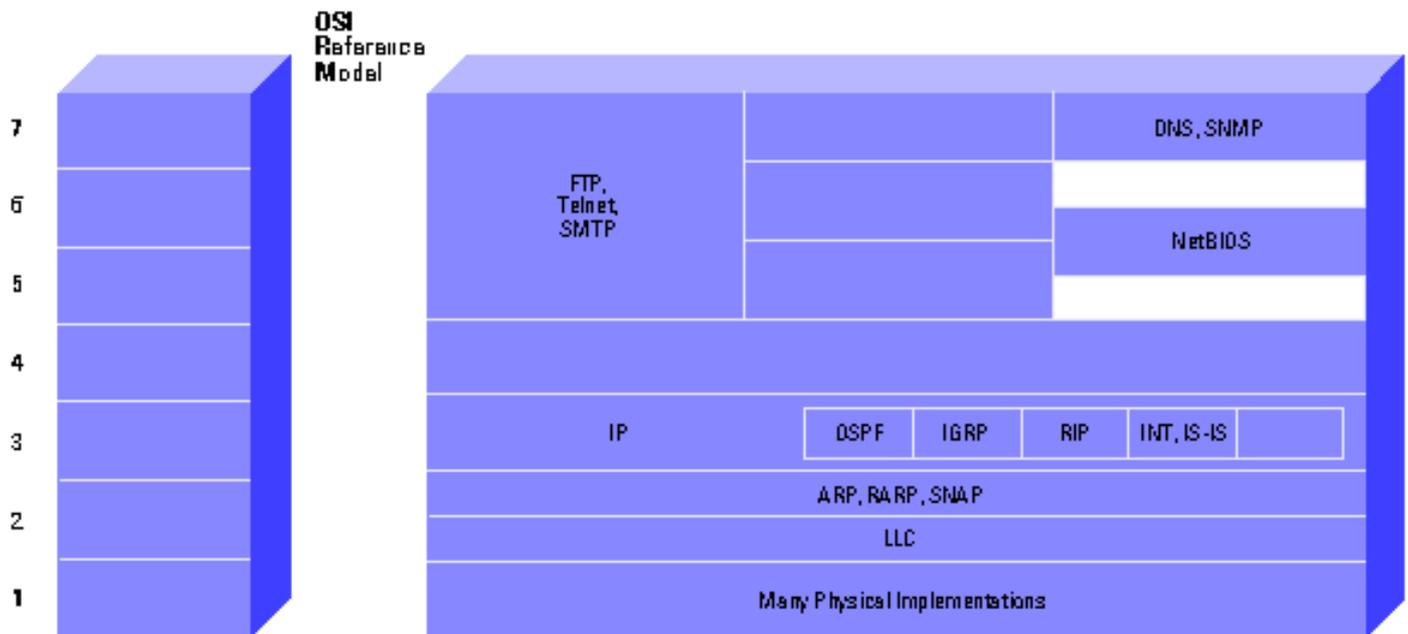


図 2 : 重要なインターネット プロトコルと OSI 参照モデルの対比



詳細については、「[インターネットプロトコル](#)」の「TCP」の項を参照してください。

IP

IP は、インターネットスイートにおける主要なレイヤ 3 プロトコルです。インターネットワークルーティングに加えて、IP は最大データ単位サイズが異なるネットワークを介した転送に対して、データグラムと呼ばれる情報単位のエラーレポート、フラグメンテーション、リアセンブルを提供します。IP はインターネットプロトコルスイートの中核を担っています。

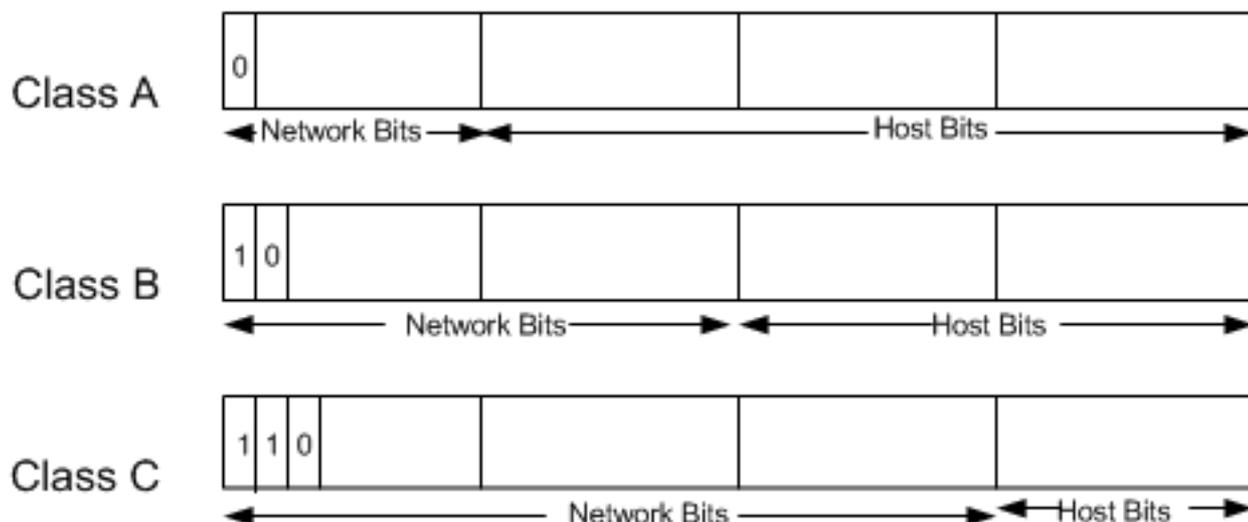
注：特定の無い限り、このセクションのIPはIPv4を指します。

IP アドレスはグローバルに一意的な 32 ビットの数値で、ネットワークインフォメーションセンターによって割り当てられます。グローバルに一意的なアドレスによって、世界中のあらゆる IP ネットワークが相互に通信できます。

IP アドレスは 2 つの部分に分かれています。前半部分はネットワークアドレス、後半部分はホストアドレスを指します。

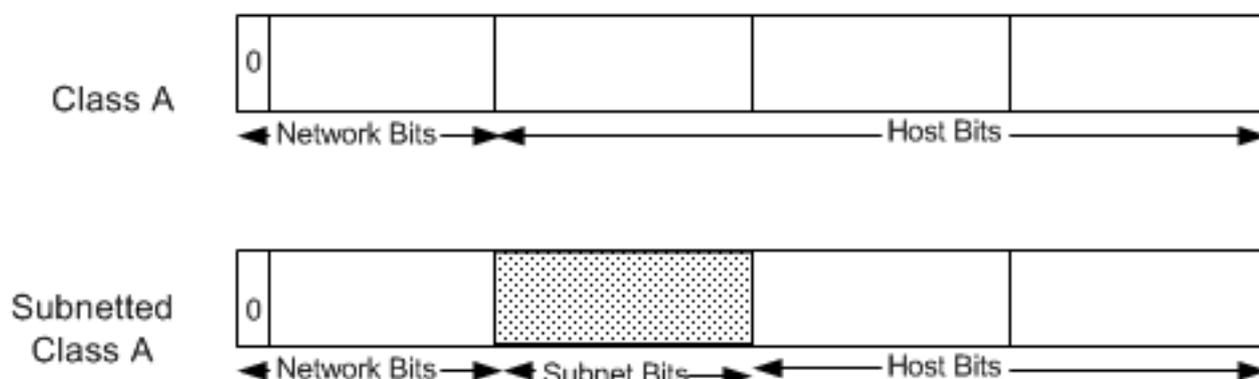
IP アドレス空間はさまざまなネットワーククラスから構成されています。クラス A ネットワークは、ネットワークアドレスフィールドが 8 ビットのみであるため、主に少数の大規模ネットワークでの使用を対象としています。クラス B ネットワークはネットワークアドレスフィールドに 16 ビットが割り当てられ、クラス C ネットワークは 24 ビットが割り当てられています。ただし、クラス C ネットワークはホストフィールドが 8 ビットのみであるため、ネットワークあたりのホスト数が制限要因となる場合があります。3 つのすべてのクラスで、左端のビットはネットワーククラスを示します。IP アドレスはドット付き 10 進表記で表されます。たとえば、34.0.0.1。図3は、[クラスA](#)、[クラスB](#)、および[クラスC](#)のIPネットワークのアドレス形式を示しています。

図 3：クラス A、B、C の IP ネットワークのアドレス形式



IP ネットワークは、サブネットワークまたは「サブネット」と呼ばれる、さらに小さい単位に分割することもできます。サブネットによってネットワークをより柔軟に管理できます。たとえば、クラス A アドレスが割り当てられたネットワークで、すべてのノードがクラス A アドレスを使用しているとします。さらに、このネットワークのアドレスをドット付き 10 進表記で 34.0.0.0 と仮定します (アドレスのホストフィールドのゼロはすべてネットワーク全体を指定します)。管理者はサブネット化によってネットワークを分割できます。具体的には、[図 4 に示すように、アドレスのホスト部からビットを「借り」てサブネット フィールドとして使用します。](#)

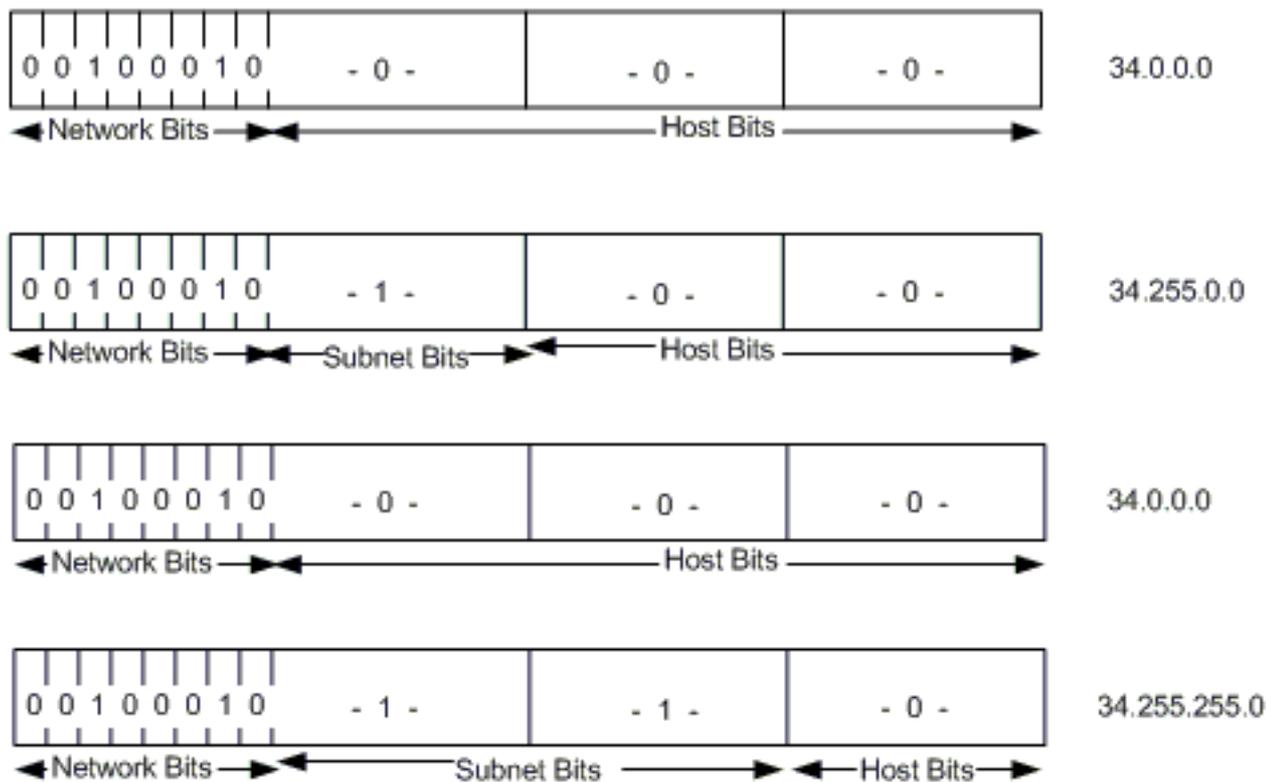
図 4 : ビットを「借りる」



ネットワーク管理者がサブネット化による 8 ビットの使用を選択した場合、クラス A IP アドレスの 2 番目のオクテットはサブネット番号を示します。この例では、アドレス 34.1.0.0 はネットワークが 34 でサブネットが 1、アドレス 34.2.0.0 はネットワークが 34 でサブネットが 2 になります。

サブネット アドレス用に借りることができるビット数は決まっています。アドレスのネットワーク部とサブネット部を示すために使用するビット数を指定するために、IP はサブネット マスクを提供します。サブネット マスクは、IP アドレスと同じ形式および表記法を使用します。サブネット マスクでは、ホスト フィールドを指定するビット以外がすべて 1 になります。たとえば、クラス A アドレス 34.0.0.0 に 8 ビットのサブネット化を指定するサブネットマスクは 255.255.0.0 です。クラス A アドレス 34.0.0.0 に 16 ビットのサブネット化を指定するサブネットマスクは 255.255.255.0 です。両方のサブネットマスクはネットワークを通じて必要に応じて渡されます。

図 5 : サブネット マスク



従来、ネットワーク番号が同一のサブネットはすべて、同じサブネットマスクを使用していました。つまり、ネットワークマネージャはネットワーク内のすべてのサブネットに対して1つの8ビットマスクを選択します。これは、ネットワーク管理者とルーティングプロトコルの両方にとって管理しやすい方法です。しかし、この方法は一部のネットワークでアドレス空間を浪費します。ホスト数の多いサブネットもあれば、少ないサブネットもありますが、いずれの場合もサブネット番号全体を使用します。シリアル回線は、1つのシリアル回線サブネットで2台のホストしか接続できないため、この最も顕著な例です。

IPサブネットの拡大に伴い、管理者はアドレス空間をより効率的に使用する方法を模索してきました。その成果の1つが可変長サブネットマスク（VLSM）と呼ばれる技法です。VLSMを使用すると、ネットワーク管理者はホスト数の少ないネットワークで長いマスクを使用し、ホスト数の多いサブネットには短いマスクを使用できます。ただし、この技法はマスクをすべて同じサイズにする場合よりも複雑で、アドレスを慎重に割り当てる必要があります。

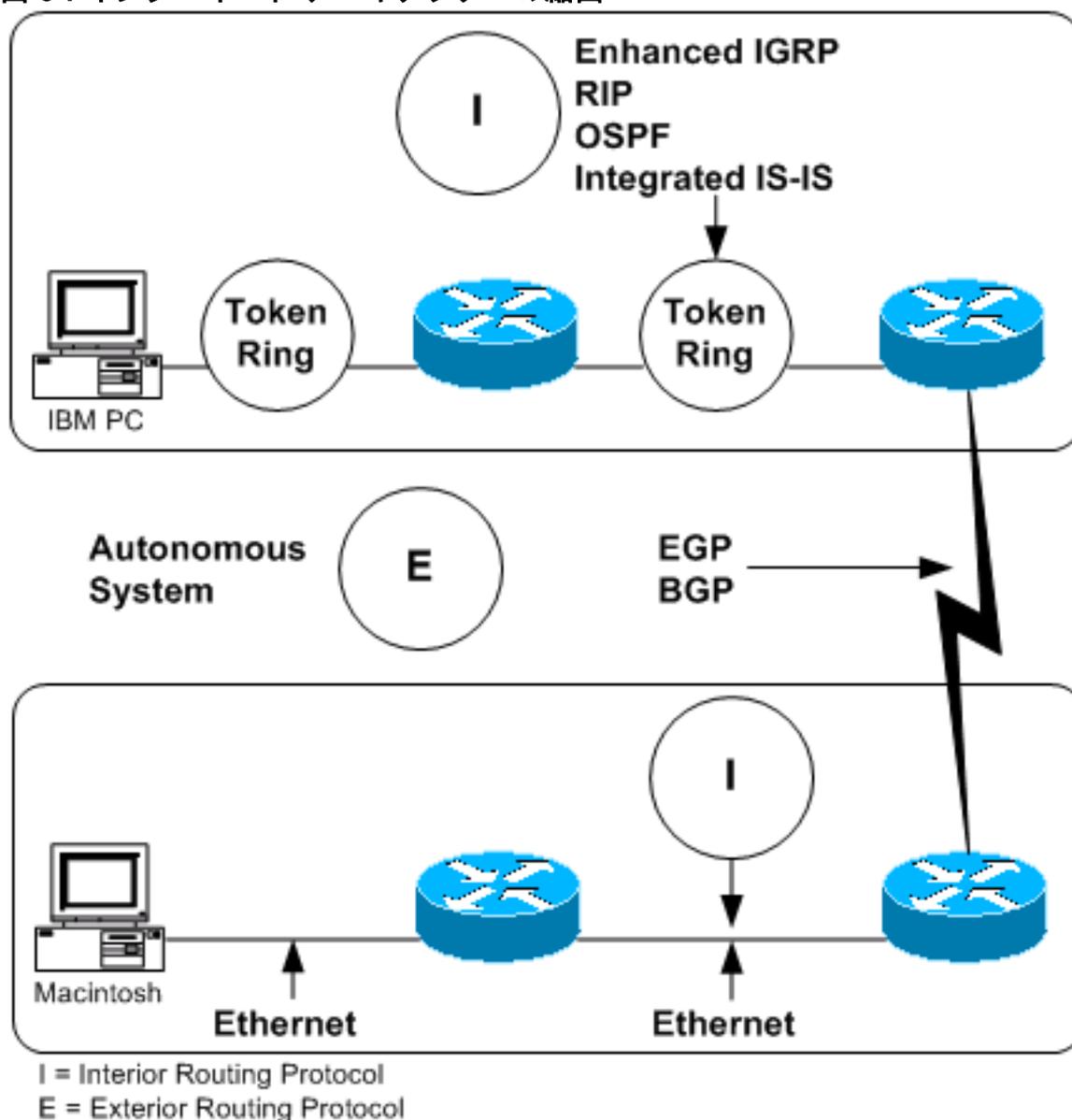
当然のことですが、VLSMを使用するには、ネットワーク管理者はVLSMをサポートしているルーティングプロトコルを使用する必要があります。シスコルータは、Open Shortest Path First（OSPF）、Integrated Intermediate System to Intermediate System（Integrated IS-IS）、Enhanced Interior Gateway Routing Protocol（Enhanced IGRP）、およびスタティックルーティングを使用したVLSMをサポートしています。IPのアドレッシングとサブネット化の詳細については、[『IPのアドレッシングとサブネット化（新規ユーザ向け）』](#)を参照してください。

IEEE 802 LANなどの一部のメディアでは、インターネットプロトコルスイートに含まれる、Address Resolution Protocol（ARP）およびReverse Address Resolution Protocol（RARP）の2つを使用することで、IPアドレスが動的に検出されます。ARPはブロードキャストメッセージを使用して、特定のネットワーク層アドレスに対応するハードウェア（MAC層）アドレスを特定します。ARPは十分に汎用的で、ほとんどのようなタイプの基本メディアアクセスメカニズムでもIPを使用できます。RARPはブロードキャストメッセージを使用して、特定のハードウェアアドレスに関連付けられたネットワーク層アドレスを特定します。ディスクレスノードでは一般的にブート時にネットワーク層アドレスが特定されていないため、RARPが特に重要です。

[IP環境でのルーティング](#)

「インターネット」は相互接続されたネットワークのグループです。一方で、インターネットは、ほとんどの研究施設や大学、および世界中のその他多くの組織間での通信を可能にするネットワークの集合体でもあります。インターネット内のルータは階層的に編成されます。一部のルータは、同一の管理権限と制御の下で特定のネットワークグループを介して情報を移動するために使用されます（このようなエンティティを自律システムと呼びます）。自律システム内の情報交換に使用されるルータは内部ルータと呼ばれ、この情報交換にはさまざまな内部ゲートウェイプロトコル（IGP）が使用されます。自律システム間で情報を移動するルータは外部ルータと呼ばれ、外部ゲートウェイプロトコル（EGP）または Border Gateway Protocol（BGP）を使用します。 [図 6 にインターネットアーキテクチャを示します。](#)

図 6：インターネットアーキテクチャの縮図



IP で使用されるルーティング プロトコルは、本質的にダイナミックなものです。ダイナミックルーティングでは、ルーティング デバイスのソフトウェアがルートを選択する必要があります。ダイナミックルーティング アルゴリズムは、ネットワークの変化に対応して自動的に最適なルートを選択します。ダイナミックルーティングとは対照的に、スタティックルーティングでは、ネットワーク管理者がルートを確認する必要があります。スタティックルートは、ネットワーク管理者が変更しない限り変わることはありません。

IP ルーティング テーブルは、宛先アドレスとネクスト ホップのペアで構成されます。次に示すシスコルータのルーティング テーブルの例では、最初のエントリが「ネットワーク 34.1.0.0 (ネットワーク 34 上のサブネット 1) に到達するための次の送信先はアドレス 54.34.23.12 のノード

である」という意味に解釈されます。

```
R6-2500# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
34.0.0.0/16 is subnetted, 1 subnets
O 34.1.0.0 [110/65] via 54.34.23.12, 00:00:51, Serial0
54.0.0.0/24 is subnetted, 1 subnets
C 54.34.23.0 is directly connected, Serial0
R6-2500#
```

以上のように、IP ルーティングでは IP データグラムが一度に 1 つのルータ ホップによってインターネットワークを移動することが指定されます。ルーティング開始時にルート全体が特定されるのではなく、データを受け取った各ノードで、データグラム内の宛先アドレスがそのノードのルーティング テーブル エントリと照合され、次のルータ ホップが決まります。ルーティングプロセスで各ノードが関与するのは、内部情報に基づいたパケットの転送のみです。ルーティングに異常が発生しても、IP は送信元にエラー レポートを返しません。これはインターネット制御メッセージ プロトコル (ICMP) という別のインターネット プロトコルが行います。

ICMP は IP インターネットワーク内でさまざまなタスクを実行します。ICMP が作成された主な目的 (送信元へのルーティング障害の報告) 以外にも、ICMP はインターネットを介したノードの到達可能性をテストする方法 (ICMP エコー メッセージおよび Reply メッセージ)、ルーティング効率を向上させる方法 (ICMP Redirect メッセージ)、データグラムに割り当てられたインターネット滞在時間を超過したことを送信元に通知する方法 (ICMP Time Exceeded メッセージ) などの便利なメッセージを提供します。一般的に、ICMP は IP 実装に不可欠であり、特にルータでの役割は重要です。詳細については、[「関連情報」を参照してください。](#)