

TCP/IP の概要

目次

[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およびデバッグ](#)

[要約](#)

[関連情報](#)

概要

ネットワークが開発されて 20 年がたち、その不均一性はイーサネット、トークン リング、ファイバ分散データ インターフェイス (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)、サービス総合デジタル ネットワーク (ISDN)、そしてごく最近では非同期転送モード (ATM) が導入され、さらに拡大しています。インターネット プロトコルは、こうした多様な LAN 技術や WAN 技術を相互接続するのに最も実績のある方式です。

インターネット プロトコル スイートには、低レベルの仕様 (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) だけでなく、電子メール、ターミナル エミュレーション、ファイル転送などの共通アプリケーションの仕様も含まれています。図 1 に、OSI 参照モデルと TCP/IP プロトコル スイートとの関係を示します。図 2 に、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知識』のドキュメントを参照してください。

インターネット プロトコルは今日使用されている、最も広範囲に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、このインターネット プロトコルスイートの部分的なサポートは、事実上すべてのコンピュータベンダーから利用可能となっています。

TCP/IP テクノロジー

このセクションでは、TCP、IP、関連プロトコル、およびこれらのプロトコルの動作環境の技術的な側面について説明します。この文書では主としてルーティング（レイヤ 3 機能）を中心に説明するため、TCP（レイヤ 4 機能）の記述は比較的手短に説明します。

TCP

TCP は、バイト形式の非構造化ストリームとしてデータを送信するコネクション型転送プロトコルです。シーケンス番号と確認応答メッセージを使用して、TCP は着信ノードへ送信したパケットに関する配信情報を、送信側ノードに提供できます。送信元から送信先への転送でデータが失われた場合、タイムアウト条件を満たすか、データ配信が成功するまで、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可能で、こうしたメッセージを適切に破棄します。送信側コンピュータのデータ送信速度が大き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およびアプリケーションへの配信情報の通信も可能です。これらの特性をすべて兼ね備えた TCP は、エンドツーエンドの信頼性の高いトランスポート プロトコルとして機能します。TCP の仕様は、[RFC 793](#) で規定されています。

図 1 OSI 参照モデルに関連する TCP/IP プロトコルスイート 図 2 OSI 参照モデルに関連する重要なインターネット プロトコル

詳細は、「[インターネット プロトコル](#)」の「[TCP](#)」セクション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、IP は最大データユニットサイズが異なるネットワークを介した転送に対して、情報ユニット（データグラム）のエラーレポート、断片化、およびの再構成機能を提供します。IP は、インターネット プロトコルスイートの中核をなします。

注: このセクションで IP という用語は、特に断りのない限り IPv4 を指します。

IP アドレスは全世界で一意的な 32 ビットの数字で、Network Information Center によって割り当てられます。全世界で一意的なアドレスを使用することによって、IP ネットワークは世界中のどこにあっても、相互に通信できます。

IP アドレスは 3 つの部分に分けられます。最初の部分はネットワークアドレス、2 番目の部分はサブネットアドレス、3 番目の部分はホストアドレスを表します。

IP アドレス空間は、3 つの異なるネットワーククラスに分割されます。クラス A ネットワークは主に、ごく少数の大規模ネットワークでの使用を意図しており、ネットワークアドレスフィールドが 8 ビットに抑えられています。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 ビットを割り当てられています。ただしクラス C ネットワークではホストフィールドに 8 ビットしか使用できないため、ネットワークあたりのホスト数が制限要因となることがあります。3 つのケースではすべて、左端のビ

ットがネットワーク クラスを示します。IP アドレスは、ドット付き 10 進表記で表記されます (34.0.0.1 など)。 [図 3](#) にクラス A、B、および C の各 IP ネットワークのアドレス形式を示します。

図 3 クラス A、B および C IP ネットワークのための \hat{a} アドレスフォーマット

IP ネットワークは、サブネットワークまたは「サブネット」というより小さなユニットに分割することもできます。サブネットを使用すると、ネットワーク管理者はネットワークをより柔軟に管理できます。たとえば、ネットワークにクラス A アドレスが割り当てられていて、ネットワークの全ノードがクラス 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がドット付き 10 進表記で 34.0.0.0 であるとし (アドレスのホスト フィールドがすべて 0 だと、そのネットワーク全体を意味します)。管理者はサブネット化により、ネットワークをさらに分割できます。これは、[図 4](#) に示すように、アドレスのホスト部分からビットを「借り」、そのビットをサブネット フィールドとして使用することで実現されます。

図 4 「ビットを借りる \hat{a} 」

ネットワーク管理者がサブネット化で 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。上記の例で、アドレス 34.1.0.0 は、ネットワーク 34、サブネット 1 を意味し、以下、アドレス 34.2.0.0 は、ネットワーク 34、サブネット 2 などとなります。

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可変です。ネットワークおよびアドレスのサブネット部分の表現に使用するビット数を指定するため、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、および同じ表示方法を使用します。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は、すべてのビットが 1 になります。たとえば、クラス A アドレス 34.0.0.0 に対して、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 に対して、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によって [図 5](#) サブネット マスクで New ノードがサブネット化の何ビットがネットワークで使用されているか学ぶことができるようにオンデマンド式で渡ることができます描写されます。

図 5 \hat{a} サブネット マスク

従来、同じネットワーク番号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、ネットワーク管理者は、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。この方法は、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、管理しやすいものです。しかし、一部のネットワークでアドレス空間を浪費します。多くのホストが存在するサブネットもあれば、少数のホストしか存在しないサブネットもありますが、どちらでもサブネット番号を使い果たしてしまいます。シリアル回線サブネットを介して 2 台のホストだけが接続可能なシリアル回線は、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、ホストの数が少ないネットワークに対して長いマスクを使用でき、ホストの数が多きサブネットに対して短いマスクを使用できます。ただし、この技法はマスクのサイズを統一する場合と比べて複雑になり、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 を使用するためには、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。シスコのルータは、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についての詳細は、『[IP のアドレッシングとサブネット化について \(新規ユーザ向け \)](#)』を参照してください。

い。

いくつかのメディアで、IEEE 802 LAN のような、IP アドレスはインターネット プロトコル スイートの 2 人の他のメンバーの使用によって動的に検出されます: アドレス解決プロトコル (ARP) および逆アドレス解決プロトコル (RARP)。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 レイヤ アドレスに対応しているハードウェア (MAC レイヤ) のアドレスを識別します。ARP は非常に汎用的で、事実上、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 レイヤ アドレスを識別します。ディスクを装備していないノードに関して RARP は特に重要です。これは通常、起動時にはネットワーク レイヤ アドレスが判明していないためです。

IP 環境でのルーティング

「インターネット」という言葉は、相互接続されたネットワークの 1 つのグループを指しています。別の面では、インターネットは、ほとんどの研究施設、大学、その他世界中の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す。インターネット内のルータは階層構造をしています。一部のルータは、同じ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させるために使用されています (このようなエンティティを自律システムと呼びます)。自律システム内で情報交換のために使用されているルータを内部ルータといいます。内部ルータではさまざまな内部ゲートウェイ プロトコル (IGP) が、この目的のために使用されています。自律システム間で情報を移動するルータを外部ルータといいます。外部ルータは外部ゲートウェイ プロトコル (EGP) またはボーダーゲートウェイ プロトコル (BGP) を使用します。インターネット アーキテクチャを [図 6](#) に示します。

図 6 インターネット アーキテクチャの a 表示

IP で使用するルーティング 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 デバイスがルートを計算するソフトウェアを備えている必要があります。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、最適のルートを自動的に選択します。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立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ルートを変更しない限り、変わることはありません。

IP ルーティング テーブルは、送信先アドレスとネクスト ホップの対で構成されています。ルーティング テーブルの例では、最初のエントリは「ネットワーク 34.1.0.0 (ネットワーク 34 のサブネット 1) に到達するための、次の送信先がアドレス 54.34.23.12 にあるノードです」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#
```

これまで見てきたように、IP ルーティングが指定することは、IP データグラムがインターネット ワークを介して、一度に 1 台のルータをホップして移動するということです。データ送信を開始する前には、ルート全体は判明していません。その代わりに、送信先ごとに、データグラム内の送信先アドレスと、現在のノードのルーティング テーブル内のエントリを照合することにより、次のルータ ホップが決定されます。ルーティング プロセスにおいて各ノードが関与することは、内部情報に基づいて、パケットを転送することだけです。ルーティング障害が発生した場合、IP は送信元にエラー レポートを送り返しません。このタスクは別のインターネット protocolâ に

インターネット制御メッセージ プロトコル (ICMP) 任せられます。

ICMP は IP インターネットワークでさまざまなタスクを実行します。ICMP が作成された本来の理由 (送信元へのルーティング障害の報告) に加え、ICMP は、インターネットを経由したノードへの到達性のテストを実行する方法 (ICMP Echo メッセージと 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 of インターネット滞在時間が割り当て時間を越えたことを送信元へ通知する方法 (ICMP Time Exceeded メッセージ)、およびその他の有益なメッセージを提供します。全体から見ると、ICMP はすべての IP 実装 (特にルータ内で実行されている場合) に不可欠な部分です。詳細については、「[関連情報](#)」を参照してください。