APPENDIX **B**

概要

この付録では、インターネット サービス プロバイダーまたはネットワーク管理者がシスコ ルータを設定する際に役立つ機能の概要について説明します。一般的なネットワーク構成を再検討するには、第 11 章「構成例」を参照してください。

この付録に記載されている内容は、次のとおりです。

ADSL

ADSL は、データと音声の両方を同一回線を介して伝送するためのテクノロジーです。ADSL のパケットベース ネットワーク テクノロジーを使用すると、Network Service Provider（NSP; ネットワーク サービス プロバイダー）のセントラル オフィスとカスタマー サイト間のローカル ループ（「ラスト マイル」）、または建物やキャンパス内で形成されるローカル ループ上で、ツイストペア銅線による高速伝送を実現できます。

シリアル回線またはダイヤルアップ回線と比較した ADSL の利点は、常時接続状態になり、ダイヤルアップ回線または専用線に比べて帯域幅が増え、コストが低下することです。ADSL テクノロジーは非対称的であり、カスタマー サイトから NSP のセントラル オフィス方向での帯域幅よりも、セントラル オフィスからカスタマー サイト方向での帯域幅を大きくすることができます。この非対称性と常時

アクセス（コール セットアップが不要）を組み合わせることにより、ADSL はインターネットとイントラネットへのアクセス、ビデオ オン デマンド、およびリモート LAN アクセスに最適な手段になります。

SHDSL

SHDSL は、データと音声の両方を同一回線を介して伝送するための、G.SHDSL（G.991.2）標準に基づくテクノロジーです。SHDSL のパケットベース ネットワーク テクノロジーを使用すると、ネットワーク サービス プロバイダー（NSP）のセントラル オフィスとカスタマー サイト間で、または建物やキャンパス内で形成されるローカル ループ上で、ツイストペア銅線による高速伝送を実現できます。

G.SHDSL 装置は、セントラル オフィスおよびリモート端末からの到達距離を約 26,000 フィート（7925 m）に拡張することができます（72 kbps ～ 2.3 Mbps の対称的なデータ速度の場合）。また、より低速でリピートすることができるため、到達距離は事実上、無制限になります。

SHDSL テクノロジーは対称的であり、NSP のセントラル オフィスとカスタマー サイト間の両方向の帯域幅を同じにすることができます。この対称性と常時アクセス（コール セットアップが不要）を組み合わせることにより、SHDSL は LAN アクセスに最適な手段になります。

ネットワーク プロトコル

ネットワーク プロトコルを使用すると、送信元から特定の宛先に、LAN または WAN リンクを介してデータを渡すことができます。ネットワーク プロトコルには、ネットワークを介してデータを送信するための最適パスが格納されたルーティング アドレス テーブルが組み込まれています。

IP

インターネットワーク レイヤで最も一般的な Transmission Control Protocol/Internet Protocol（TCP; 伝送制御プロトコル/IP; インターネット プロトコル）は IP です。IP は、すべての TCP/IP ネットワークに基本的なパケット配信サービスを提供します。IP プロトコルは、物理ノード アドレスの他に、IP アドレスと呼ばれる論理ホスト アドレス システムを実装します。IP アドレスは、インターネットワーク以上のレイヤで、装置を特定したり、インターネットワーク ルーティングを実行するために使用されます。Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用すると、IP は指定の IP アドレスと一致する物理アドレスを識別できるようになります。

IP 以外のレイヤ内のすべてのプロトコルでは、データを配信するために IP を使用しています。つまり、最終宛先に関係なく、送受信される TCP/IP データはすべて IP を通過します。

IP はコネクションレス プロトコルであるため、データを伝送する前に、制御情報（*ハンドシェイク*）を交換してエンドツーエンド接続を確立することはありません。対照的に、コネクション型プロトコルはリモート コンピュータと制御情報を交換して、データ受信準備が完了したことを確認してから、データを送信します。ハンドシェイクに成功した場合は、コンピュータによって接続が確立されています。コネクション型サービスが必要な場合、IP は他のレイヤ内のプロトコルによって接続を確立します。

Internetwork Packet Exchange（IPX）は、動的なディスタンス ベクタ ルーティング プロトコルである Routing Information Protocol（RIP）を使用して、ルーティング情報を交換します。RIP については、この後で詳細に説明します。

ルーティング プロトコルのオプション

ルーティング プロトコルには次のものがあります。

- Routing Information Protocol（RIP）
- Enhanced Interior Gateway Routing Protocol（EIGRP）

RIP と EIGRP には、いくつか異なる点があります（表 B-1 を参照）。

表 B-1　RIP と EIGRP の比較

プロトコル	最適なトポロジ	メトリック	ルーティング アップデート
RIP	15 ホップ以内のトポロジに適しています。	ホップ カウント。最大ホップ カウントは 15 です。最良ルートは、ホップ カウントが最小のルートです。	デフォルトで 30 秒間隔。この間隔を変更することもできますし、RIP のトリガ拡張機能を使用することもできます。
EIGRP	宛先までのホップ数が 16 以上の、大規模なトポロジに適しています。	距離情報。後継ルータ（ルーティング ループを形成しないことが保証され、宛先までのコスト パスが最小になる近接ルータ）を基準にします。	hello パケットが 5 秒間隔で送信されます。さらに、宛先のステートが変化した時点で差分更新が送信されます。

RIP

RIP は IP に関連するプロトコルで、インターネット上のルーティング プロトコル トラフィックとして幅広く使用されます。RIP は、ディスタンス ベクタ ルーティング プロトコルです。つまり、ルート選択のためのメトリックとして距離（ホップ カウント）を使用します。*ホップ カウント*は、パケットが宛先に到達するために経由しなければならないルータ数です。たとえば、あるルートのホップ カウントが 2 である場合、パケットを宛先に送るには 2 台のルータを経由しなければなりません。

デフォルトでは、RIP のルーティング アップデートは 30 秒おきにブロードキャストされます。ルーティング アップデートをブロードキャストする間隔は、ユーザ側で再設定することができます。さらに、RIP のトリガ拡張機能を使用して、ルーティング データベースが更新されたときにだけルーティング アップデートを送信するように設定することもできます。RIP のトリガ拡張機能については、Cisco IOS 12.3 のマニュアルを参照してください。

EIGRP

EIGRP は、シスコ独自仕様による高度なディスタンス ベクタおよびリンク ステート ルーティング プロトコルであり、距離（ホップ カウント）よりも洗練されたメトリックに基づいてルートを選択します。EIGRP は、後継ルータ（ルーティング ループを形成しないことが保証され、宛先までのコスト パスが最小になる近接ルータ）を基準とするメトリックを使用します。特定の宛先への後継ルータが存在しないにもかかわらず、近接ルータが宛先をアドバタイズしている場合、ルータはルートを再計算しなければなりません。

EIGRP が稼動する各ルータは、5 秒おきに hello パケットを送信して、近接ルータに自らが動作していることを知らせます。所定時間内に hello パケットを送信しないルータがあれば、EIGRP は宛先のステートに変化があったと見なし、差分更新を送信します。

EIGRP は IP をサポートするため、マルチプロトコル ネットワーク環境で 1 つのルーティング プロトコルを使用して、ルーティング テーブルのサイズおよびルーティング情報の量を最小限に抑えることができます。

PPP 認証プロトコル

Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）は、ポイントツーポイント リンクを介して送信されるネットワーク レイヤ プロトコル情報をカプセル化します。

本来、PPP はポイントツーポイント リンクを介して IP トラフィックを転送するためのカプセル化プロトコルとして開発されました。また、IP アドレスの割り当てと管理、非同期（スタート/ストップ）カプセル化とビット型同期カプセル化、ネットワーク プロトコルの多重化、リンク コンフィギュレーション、リンク品質テスト、エラー検出、およびネットワーク レイヤ アドレス ネゴシエーションやデータ圧縮ネゴシエーションなどのオプションのネゴシエーション機能に関する標準も、PPP によって確立されました。上記機能をサポートするために、PPP には拡張可能な Link Control Protocol（LCP）および Network Control Protocol（NCP）ファミリーが備わっており、これらによってオプションの設定パラメータおよびファシリティをネゴシエートします。

PPP の最新の実装では、PPP セッションを認証するためのセキュリティ認証プロトコルが 2 つサポートされています。

- Password Authentication Protocol（PAP）
- Challenge Handshake Authentication Protocol（CHAP）

通常、PPP と PAP または CHAP 認証の組み合わせは、接続されているリモート サイトを中央サイトに通知する場合に使用されます。

PAP

PAP は双方向のハンドシェイクを使用して、ルータ間のパスワードを検証します。PAP の仕組みを理解するために、リモート オフィスのシスコ ルータが本社オフィスのシスコ ルータに接続されているネットワーク トポロジを例にとります。PPP リンクが確立された後、リモート オフィス ルータは、本社オフィス ルータが認証を受け付けるまで、設定されているユーザ名およびパスワードの送信を繰り返します。

PAP の特徴は、次のとおりです。

- 認証のパスワード部分は、リンク上をクリア テキストで送信されます（スクランブル処理または暗号化は行われません）。
- PAP では、プレイバック攻撃または反復的な総当り攻撃からの保護機能が提供されません。
- 認証試行の頻度およびタイミングは、リモート オフィス ルータが制御します。

CHAP

CHAP は 3 ウェイ ハンドシェイクを使用して、パスワードを検証します。CHAP の仕組みを理解するために、リモート オフィスのシスコ ルータが本社オフィスのシスコ ルータに接続されているネットワーク　トポロジを例にとります。

PPP リンクが確立された後、本社オフィス ルータはリモート オフィス ルータに対し、チャレンジ メッセージを送信します。リモート オフィス ルータは可変の値で応答します。本社オフィス ルータは、独自に計算した値と照らし合わせて、この応答をチェックします。両方の値が一致していれば、本社オフィス ルータは認証を受け付けます。リンクを確立した後は、いつでも認証プロセスを繰り返すことができます。

CHAP の特徴は、次のとおりです。

- 認証プロセスでは、パスワードではなく、可変のチャレンジ値を使用します。
- CHAP は、一意の予測不可能な可変のチャレンジ値の使用により、プレイバック攻撃から保護します。チャレンジの反復により、1 回の攻撃にさらされる時間を限定します。
- 認証試行の頻度およびタイミングは、本社オフィス ルータが制御します。

（注）　2 つのプロトコルのうち、より安全性の高い CHAP の使用を推奨します。

TACACS+

Cisco 860 および Cisco 880 シリーズ ルータは、Telnet を介して Terminal Access Controller Access Control System Plus（TACACS+）プロトコルをサポートします。TACACS+ は、リモート アクセス認証およびイベント ロギングなどの関連ネットワーク セキュリティ サービスを提供するシスコ独自の認証プロトコルです。ユーザ パスワードは、個々のルータではなく中央のデータベースで管理されます。TACACS+ は、ルータごとに設定された、別個のモジュールである Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）ファシリティもサポートします。

ネットワーク インターフェイス

ここでは、Cisco 860 および Cisco 880 シリーズ ルータがサポートするネットワーク インターフェイス プロトコルについて説明します。サポートされるネットワーク インターフェイス プロトコルは、次のとおりです。

- イーサネット
- ATM（DSL 用）

イーサネット

イーサネットは、Carrier Sense Multiple Access Collision Detect（CSMA/CD; キャリア検知多重アクセス/衝突検知）を使用してデータおよび音声パケットを WAN インターフェイスに送信するベースバンド LAN プロトコルです。この用語は、通常、すべての CSMA/CD LAN を表します。イーサネットは、散発的な、場合によっては大量のトラフィックが発生するネットワーク内で機能するように設計されました。IEEE 802.3 仕様は、本来のイーサネット テクノロジーに基づいて、1980 年に開発されました。

イーサネット CSMA/CD メディアアクセス プロセスでは、CSMA/CD LAN 上のすべてのホストはいつでもネットワークにアクセスできます。データを送信する前に、CSMA/CD ホストはネットワークを通過するトラフィックを待ち受けます。データを送信するホストは、トラフィックが検出されなくなるまで待機してから、データを送信します。イーサネットでは、ネットワーク上をデータが流れていない場合、ネットワーク上のすべてのホストがデータを送信できます。トラフィックを待ち受けていた 2 台のホストがトラフィックを検出せず、同時にデータを送信すると、衝突が発生します。衝突が発生すると両方の送信内容が破壊されるため、ホストは後で再送信する必要があります。衝突したホストがいつ再送信を行うかは、アルゴリズムによって決まります。

ATM（DSL 用）

Asynchronous Transfer Mode（ATM; 非同期転送モード）は、音声、データ、ビデオ、画像など複数のトラフィック タイプをサポートする、高速な多重化およびスイッチング プロトコルです。

ATM は、ネットワークのすべての情報をスイッチングおよび多重化する固定長セルで構成されます。ATM 接続は、単に宛先ルータまたはホストに情報を転送するために使用されます。ATM ネットワークは、帯域幅を幅広く利用できる LAN と考えられます。コネクションレス型である LAN と異なり、ATM を使用してユーザに LAN 環境を提供するには、特定の機能が必要となります。

各 ATM ノードは、ATM ネットワーク内の通信する必要があるすべてのノードに対して、接続を個別に確立する必要があります。このような接続はすべて、Permanent Virtual Circuit（PVC; 相手先固定接続）によって確立されます。

PVC

PVC はリモート ホストとルータ間の接続です。PVC は、ルータが通信する ATM エンド ノードごとに確立されます。PVC の作成時に確立される PVC の特性は、ATM Adaptation Layer（AAL; ATM アダプテーション レイヤ）およびカプセル化タイプによって設定されます。AAL は、ユーザ情報をセルに変換する方法を定義します。AAL は、送信時に上位レイヤ情報をセルに分割し、受信時にセルを再び組み立てます。

シスコ ルータは AAL5 形式をサポートしています。AAL5 は、AAL3/4 よりもオーバーヘッドが少なく、エラー検出および訂正機能が優れている最新のデータ トランスポート サービスを提供します。AAL5 は通常、Variable Bit Rate（VBR; 可変ビット レート）トラフィックおよび Unspecified Bit Rate（UBR; 未指定ビット レート）トラフィックを対象とします。

ATM カプセル化は、特定のプロトコル ヘッダーによりデータをラップする機能です。接続しているルータのタイプにより、ATM PVC カプセル化タイプが決まります。

ルータがサポートする ATM PVC カプセル化タイプは、次のとおりです。

- LLC/SNAP（RFC 1483）
- VC-MUX（RFC 1483）
- PPP（RFC 2364）

各 PVC は、宛先ノードへの完全な、独立したリンクと見なされます。ユーザは必要に応じて、接続間でデータをカプセル化できます。ATM ネットワークは、データの内容を無視します。必要となるのは、特定の AAL 形式に従って、ルータの ATM サブシステムにデータを送信することだけです。

ダイヤラ インターフェイス

ダイヤラ インターフェイスは、PVC に PPP 機能（認証方法や IP アドレス割り当て方法など）を割り当てます。PPP over ATM を設定する場合に使用します。

ダイヤラ インターフェイスは、すべての物理インターフェイスから独立して設定し、必要に応じて動的に適用することができます。

ダイヤル バックアップ

ダイヤル バックアップを使用すると、ユーザはバックアップ モデム回線接続を設定できるようになるため、WAN のダウンタイムが短縮されます。Cisco IOS ソフトウェアのダイヤル バックアップ機能を起動するために、以下を使用できます。

- バックアップ インターフェイス
- フローティング スタティック ルート
- ダイヤラ ウォッチ

バックアップ インターフェイス

バックアップ インターフェイスは、WAN ダウンタイムなど、自らが起動する特定の環境が発生するまで、アイドル状態にとどまるインターフェイスです。バックアップ インターフェイスとして設定できるのは、Basic Rate Interface（BRI; 基本速度インターフェイス）などの物理インターフェイス、またはダイヤラ プールで使用されるように割り当てられたバックアップ ダイヤラ インターフェイスです。プライマリ回線が起動している場合、バックアップ インターフェイスはスタンバイ モードです。スタンバイ モードのバックアップ インターフェイスは、イネーブルになるまで、事実上のシャットダウン状態です。バックアップ インターフェイスに関連付けられたルートは、ルーティング テーブルに格納されません。

バックアップ インターフェイス コマンドは、インターフェイスが物理的にダウンしていることを識別したルータによって異なるため、通常は、ISDN BRI 接続、非同期回線、および専用線をバックアップするために使用されます。プライマリ回線に障害が発生すると、上記接続に対するインターフェイスがダウンして、バックアップ インターフェイスがこれらの障害をただちに識別します。

フローティング スタティック ルート

フローティング スタティック ルートは、管理距離がダイナミック ルートよりも長いスタティック ルートです。スタティック ルートに管理距離を設定すると、スタティック ルートの優先度をダイナミック ルートよりも小さくすることができます。この方法では、ダイナミック ルートが使用可能な場合、スタティック ルートは使用されません。ただし、ダイナミック ルートが失われると、スタティック ルートが引き継ぎ、この代替ルートを通してトラフィックを送信できます。この代替ルートに Dial-on-Demand Routing（DDR; ダイヤルオンデマンド ルーティング）インターフェイスが使用されている場合は、DDR インターフェイスをバックアップ インターフェイスとして使用できます。

ダイヤラ ウォッチ

ダイヤラ ウォッチは、ダイヤル バックアップとルーティング機能を統合するバックアップ機能です。ダイヤラ ウォッチを使用すると、中央ルータにおいて発信コールをトリガするトラフィックを定義しなくても、信頼できる接続を確立できます。したがって、ダイヤラ ウォッチは対象トラフィックに関する条件がない正規の DDR と見なすことができます。プライマリ インターフェイスを定義するウォッチ対象ルートを設定することにより、ウォッチ対象ルートの追加および削除にともない、プライマリ インターフェイスのステータスを監視し追跡することができます。

ウォッチ対象ルートを削除すると、ダイヤラ ウォッチはウォッチ中のいずれかの IP アドレスまたはネットワークに対して、有効なルートが少なくとも 1 つ存在するかどうかを確認します。有効なルートが存在しない場合、プライマリ回線はダウンしており、使用不可能であると見なされます。定義済みのウォッチ対象 IP ネットワークの少なくとも 1 つに有効なルートが存在し、このルートがダイヤラ ウォッチに設定されたバックアップ インターフェイス以外のインターフェイスを示している場合、プライマリ リンクは起動していると見なされ、ダイヤラ ウォッチはバックアップ リンクを起動しません。

NAT

Network Address Translation（NAT; ネットワーク アドレス変換）はプライベートにアドレス指定されたネットワークから、インターネットなどの登録済みネットワークにアクセスするためのメカニズムを提供します。サブネット アドレスが登録されている必要はありません。このメカニズムにより、ホスト番号の再設定は不要になり、複数のイントラネットで同じ IP アドレス範囲を使用できます。

NAT は、*内部ネットワーク*（登録されていない IP アドレスを使用するネットワーク）と*外部ネットワーク*（グローバルに一意な IP アドレスを使用するネットワーク [この場合はインターネット]）の境界に配置されたルータに設定されます。NAT は内部ローカル アドレス（内部ネットワークのホストに割り当てられた登録されていない IP アドレス）をグローバルに一意な IP アドレスに変換してから、パケットを外部ネットワークに送信します。

NAT が設定されている場合、内部ネットワークは既存のプライベート アドレスまたは古い形式のアドレスを引き続き使用します。これらのアドレスが有効なアドレスに変換された後、パケットは外部ネットワークに転送されます。変換機能は標準ルーティングと互換性があります。この機能が必要となるのは、内部ネットワークと外部ドメインを接続しているルータだけです。

変換はスタティックにもダイナミックにも行えます。スタティック アドレス変換は、内部ネットワークと外部ドメインの 1 対 1 のマッピングを確立します。ダイナミック アドレス変換は、変換されるローカル アドレスと、外部アドレスの割り当て元となるアドレス プールとを指定することによって、定義されます。割り当ては番号順に行われ、連続するアドレス ブロックからなる複数のプールを定義できます。

NAT を使用すると、外部へのアクセスが必要なすべてのホストにアドレスを再指定する必要がなくなるため、時間が短縮され、コストが削減されます。また、アプリケーション ポートレベルの多重化によって、アドレスも節約されます。NAT が設定されていると、内部ホストはすべての外部通信に対して、1 つの登録済み IP アドレスを共有できます。このタイプの設定では、多数の内部ホストをサポートするために必要な外部アドレスが比較的少なくてすむため、IP アドレスが節約されます。

内部ネットワークのアドレス指定方式は、インターネット内で割り当てられた登録済みアドレスと競合することがあります。したがって、NAT は重複ネットワークごとに個別のアドレス プールを使用して、適切に変換することができます。

Easy IP（フェーズ 1）

Easy IP（フェーズ 1）機能は、ネットワーク アドレス変換と PPP/Internet Protocol Control Protocol（IPCP; インターネット プロトコル コントロール プロトコル）を組み合わせた機能です。この機能を使用すると、シスコ ルータは、独自の登録済み WAN インターフェイス IP アドレスを中央サーバから自動的にネゴシエートし、すべてのリモート ホストがこの単一の登録済みアドレスを使用してインターネットにアクセスできるようにします。Easy IP（フェーズ 1）では、Cisco IOS ソフトウェアに組み込まれた既存のポートレベル多重化 NAT 機能が使用されるため、リモート LAN 上の IP アドレスはインターネットから参照できません。

Easy IP（フェーズ 1）機能は、NAT と PPP/IPCP を組み合わせた機能です。NAT が設定されているルータは、LAN 装置で使用される登録されていない IP アドレスを、ダイヤラ インターフェイスで使用されるグローバルに一意な IP アドレスに変換します。複数の LAN 装置でグローバルに一意な同一 IP アドレスを使用する機能は、*オーバーローディング*といいます。NAT は、内部ネットワーク（登録されていない IP アドレスを使用するネットワーク）と外部ネットワーク（グローバルに一意な IP アドレスを使用するネットワーク [この場合はインターネット]）の境界に配置されたルータに設定されます。

PPP/IPCP が設定されている場合、シスコ ルータは、Internet Service Provider（ISP; インターネット サービス プロバイダー）ルータからダイヤラ インターフェイス用のグローバルに一意な（登録済み）IP アドレスを自動的にネゴシエートします。

Easy IP（フェーズ 2）

Easy IP（フェーズ 2）機能は、Dynamic Host Configuration Protocol（DHCP）サーバとリレーを組み合わせた機能です。DHCP は、IP ネットワーク上の装置（DHCP クライアント）が DHCP サーバ内の設定情報を要求できるようにするためのクライアント/サーバ プロトコルです。DHCP は必要に応じて、中央プールのネットワーク アドレスを割り当てます。DHCP は、一時的にネットワークに接続されるホストに IP アドレスを割り当てる場合や、永久的な IP アドレスが不要なホスト グループ間で、限られた IP アドレス プールを共有する場合に便利です。

DHCP を使用すると、ユーザはクライアントごとに IP アドレスを手動で設定する必要がなくなります。

DHCP では、ルータが DHCP クライアントからの User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ブロードキャスト（IP アドレス要求を含む）を転送するように設定します。DHCP には、自動化を促進しネットワーク管理の問題を減少させるために、次の機能が備わっています。

- 各コンピュータ、プリンタ、および共有ファイル システムの手動設定が不要
- 2 つのクライアントで同じ IP アドレスが同時に使用される状況を防止
- 中央サイトからの設定が可能

QoS

ここでは、Quality of Service（QoS; サービス品質）パラメータについて説明します。具体的な内容は、次のとおりです。

- IP precedence
- PPP フラグメンテーションおよびインターリーブ
- CBWFQ
- RSVP
- 低遅延キューイング（LLQ）

QoS は、ATM、イーサネットおよび IEEE 802.1 ネットワーク、これらの基本テクノロジーの一部またはすべてを使用した IP ルーテッド ネットワークなど、さまざまなテクノロジーを介して、選択されたネットワーク トラフィックに対し、より優れたサービスを提供するためのネットワーク機能です。QoS の主な目的は、専用帯域幅の確保、ジッタおよび遅延の制御（一部のリアルタイム トラフィックおよび対話型トラフィックで必要）、および損失特性の改善です。QoS テクノロジーは、キャンパス、WAN、およびサービス プロバイダー ネットワークの今後のビジネス用途に対応するための基本的な構成単位を提供します。

音声ネットワークのパフォーマンスを高めるには、VoIP が稼動しているルータだけでなく、ネットワーク全体に QoS を設定する必要があります。すべての QoS 技術が、あらゆるネットワーク ルータに適しているとは限りません。ネットワーク内のエッジ ルータとバックボーン ルータは、必ずしも同じ動作をするわけではありません。同様に、実行する QoS の作業もそれぞれ異なる場合があります。リアルタイム音声トラフィックに対応するように IP ネットワークを設定するには、ネットワーク内のエッジ ルータとバックボーン ルータの両方の機能を検討する必要があります。

QoS ソフトウェアを使用すると、複雑なネットワークにおいて、さまざまなネットワーク アプリケーションおよびトラフィック タイプを制御し、予測どおりに処理することができます。ほとんどすべてのネットワークは、小規模企業ネットワーク、インターネット サービス プロバイダー、エンタープライズ ネットワークのいずれであるかに関係なく、QoS を利用して効率を最適化できます。

IP precedence

IP precedence を使用すると、最大 6 つのサービス クラスにトラフィックを分類できます（他の 2 つのクラスは、内部ネットワーク用に予約されています）。ネットワークに適用されたキューイング テクノロジーは、この信号を使用して処理を促進することができます。

ポリシーベース ルーティングや Committed Access Rate（CAR; 専用アクセス レート）などの機能を使用すると、拡張アクセスリスト分類に基づいて優先順位を設定できます。これにより、アプリケーションまたはユーザ別、宛先および送信元サブネット別など、優先順位をきわめて柔軟に割り当てることができます。通常、この機能は可能な限りネットワーク（または管理ドメイン）のエッジ付近に配備されるため、これ以降のネットワーク要素は決定されたポリシーに基づいてサービスを提供できます。

オプションの信号方式を使用している場合は、ホストまたはネットワーク クライアントに IP precedence を設定することもできます。IP precedence を使用すると、既存ネットワーク キューイング メカニズム（Class-Based Weighted Fair Queuing [CBWFQ; クラス ベース WFQ] など）を使用して、サービス クラスを確立できます。既存アプリケーションの変更の必要性や複雑なネットワーク要件はありません。

PPP フラグメンテーションおよびインターリーブ

マルチクラス マルチリンク PPP インターリーブにより、大きいパケットをマルチリンクでカプセル化し、リアルタイム音声トラフィックの遅延条件を満たす小さいパケットに分割することができます。もともと小さいリアルタイム パケットは、マルチリンクでカプセル化されず、大きいパケットのフラグメントの合間に伝送されます。インターリーブ機能はさらに、小型で遅延に敏感なパケット用に特殊な送信キューを提供するので、そのようなパケットを他のフローより先に送信できます。インターリーブ機能は、他のベスト エフォート型トラフィックに使用される低速リンク上で、遅延に敏感な音声パケットに遅延限度を設定します。

マルチリンク PPP インターリーブは、通常、CBWFQ および RSVP または IP precedence と組み合わせて使用し、音声パケットの配信を保証します。データの管理方法を定義する場合は、マルチリンク PPP インターリーブおよび CBWFQ を使用します。音声パケットにプライオリティを設定する場合は、Resource Reservation Protocol（RSVP; リソース予約プロトコル）または IP precedence を使用します。

CBWFQ

通常、CBWFQ はマルチリンク PPP インターリーブおよび RSVP または IP precedence と組み合わせて使用し、音声パケットの配信を保証します。データの管理方法を定義する場合は、CBWFQ とマルチリンク PPP を組み合わせて使用します。音声パケットにプライオリティを設定する場合は、RSVP または IP precedence を使用します。

ATM キューと Cisco IOS キューの 2 つのキューイング レベルがあります。CBWFQ は Cisco IOS キューに適用されます。PVC が作成されると、First-in first-out（FIFO; 先入れ先出し）Cisco IOS キューが自動的に作成されます。CBWFQ を使用してクラスを作成し、それらを PVC に関連付けると、クラスごとにキューが作成されます。

CBWFQ により、キューに十分な帯域幅が確保され、トラフィックは予測どおりのサービスを受けます。小容量トラフィック ストリームが優先されます。大容量トラフィック ストリームに残りの容量が分配され、同等または比例配分された帯域幅が与えられます。

RSVP

RSVP を使用すると、ルータはインターフェイス上に十分な帯域幅を確保して、信頼性および品質性能を高めることができます。RSVP により、エンド システムはネットワークに特定の QoS を要求できます。リアルタイム音声トラフィックには、ネットワークの一貫性が不可欠です。一貫した QoS が得られなかった場合、リアルタイム トラフィックにジッタ、帯域幅不足、遅延変動、または情報損失が生じる可能性があります。RSVP は、最新のキューイング メカニズムと連動します。予約がどのように実行されるかは、インターフェイス キューイング メカニズム（CBWFQ など）に依存します。

RSVP は、PPP、HDLC、および同様なシリアル回線インターフェイス上で適切に動作します。マルチアクセス LAN 上では、適切に動作しません。RSVP は、パケット フローに関するダイナミック アクセス リストと同様のものと考えることができます。

ネットワークに次の条件が存在する場合は、RSVP を設定して QoS を保証する必要があります。

- 小規模な音声ネットワークの実装
- 2 Mbps 未満のリンク
- 使用率の高いリンク
- 可能なかぎり最良の音質を必要とする場合

低遅延キューイング（LLQ）

Low Latency Queuing（LLQ; 低遅延キューイング）は、リアルタイム トラフィック用の低遅延完全優先送信キューを提供します。完全優先キューを使用すると、（他のキュー内のパケットがキューから取り出される前に）最初に遅延に敏感なデータをキューから取り出して送信することにより、遅延に敏感なデータを他のトラフィックよりも優先的に処理することができます。

アクセス リスト

基本的な標準アクセス リストおよびスタティック拡張アクセス リストを使用すると、**permit** コマンドにキーワードを指定して、セッション フィルタリングと同様の処理を行うことができます。指定されたキーワードは、ACK または RST ビットが設定されているかどうかに基づいて、TCP パケットをフィルタリングします （ACK または RST ビットが設定されているパケットはセッション内の最初のパケットではないため、このパケットは確立されたセッションに属します）。このフィルタ基準は、インターフェイスに永久的に適用されるアクセス リストの一部になります。