

NSE-1 (Network Service Engine) を使用した インテリジェントサービスの高速処理

IPネットワークからWebベースのアプリケーションまで、インターネット技術を幅広く採用することにより、スケラブルで、信頼性があり、広範囲に接続された情報システムの構築を実現できます。インターネット技術の進歩と共に、シスコではより洗練された機能をネットワークに展開しています。

ネットワークは従来のストアアンドフォワードやパケットベースのモデルから、リアルタイムトラフィックが伝送されるモデルへと変わりつつあります。このサービスをベースにしたネットワークでは、ネットワーク技術を活用するためにビジネスで利用できる豊富な機能が用意されています。

サービススペースのネットワーク

サービススペースのネットワークは、ネットワークの数年来の進歩が頂点に達したことの象徴です。接続指向のインフラの管理と予測が可能になり、伝送ネットワークはスケラビリティと自己回復機能を備えるようになりました。

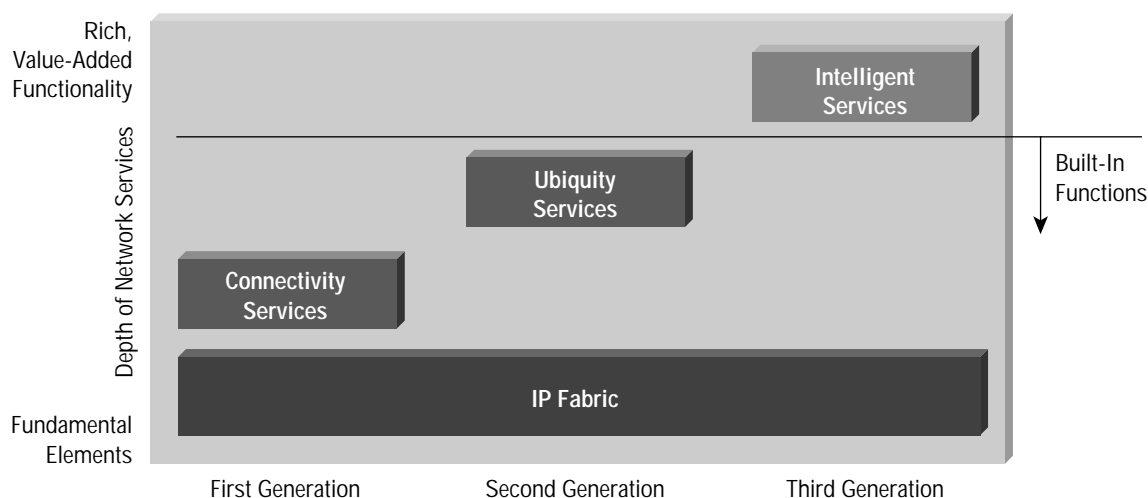
いつのまにか、転送やDNSといった初期のネットワークサービスはネットワーク機構の基礎部分となっています。これらの

サービスには、ネットワークリンクを維持したり、データの配達や順序付けを行ったりするなどの非常に基本的な機能しかありません。言い換えれば、アプリケーションがネットワークに期待できるのは、接続されているということだけだったのです。

接続サービスは、すぐにネットワークインフラの「標準装置」になりました。ネットワークの普及に焦点を絞った新しいサービスによって、IPファブリックは組織全体とインターネットワーク全体に広がりました。ここで提供されたサービスには、サービスロケーション、パフォーマンスの差別化、フローの集約といった基本的な機能が含まれていました。この時点で、アプリケーションがIP上で動作すれば、広く利用されることになるだろうという予測ができました。

第3世代のネットワークサービスは、接続性と偏在性の上にインテリジェンスを供給するようになっています。インテリジェント・ネットワークサービスがいったんネットワークで展開されると、インテリジェント・ネットワークサービスは、コールセンタ、統合化メッセージング、IPテレフォニー、対話型ビデオ、レガシートランザクション処理など、ビジネスアプリケーションのインフラとして機能します。図1にこの変化を示します。

図1：接続性と偏在性サービスはIPファブリックの一部になっている



シスコのインテリジェント・ネットワークサービス

シスコのインテリジェント・ネットワークサービス(図2参照)は、現在、最も包括的で完全なネットワークサービス群で構成されています。セキュリティ、レガシーおよびSNAの発展、QoS、音声、ビデオ、レプリケーション、キャッシング、アドレス管理、VPN、出版、負荷分散、マルチキャスト機能を実現し、電子ビジネスへの新しい対応が可能になっています。

これらのサービスは、顧客が要求する高いレベルの可用性、スケーラビリティ、接続性に対応したIPファブリックで機能します。これは、一定範囲のネットワーキングプラットフォームで稼働し、強力なソフトウェアと超高速ハードウェアを活用して、高性能で幅広い機能を実現しています。サービスは、高いレベルのビジネス目的をネットワーク設定へ変換する高度のポリシーシステムによって管理されます。

図2：シスコのインテリジェント・ネットワークサービス・モデル

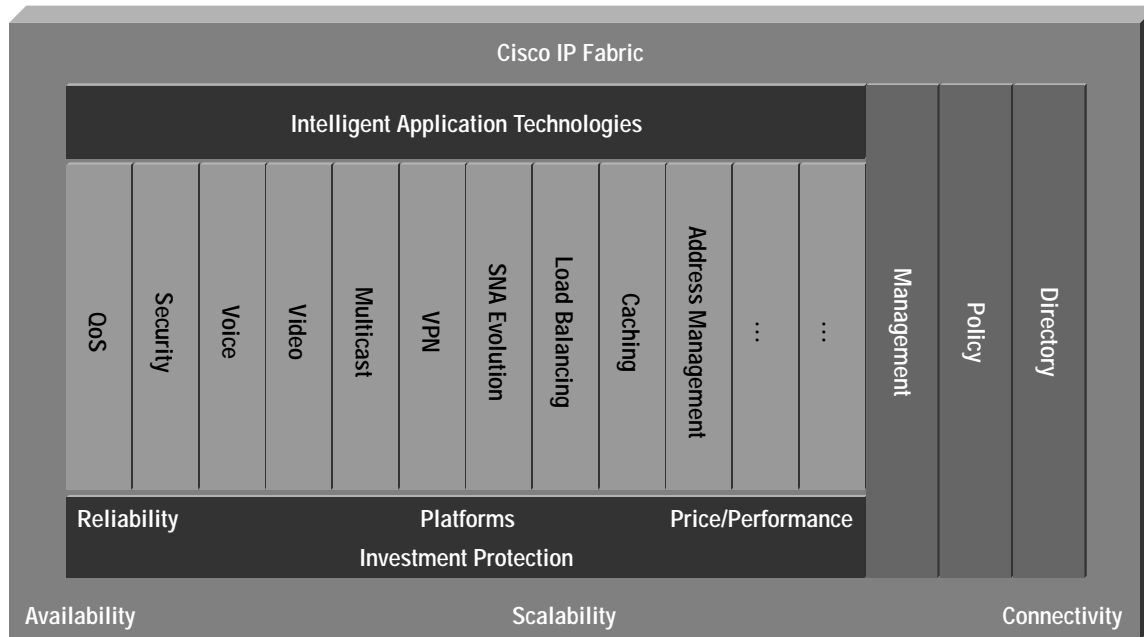


図2にあるように、シスコのインテリジェント・ネットワークサービスでは、最も良質のサービスを最も幅広く提供しています。もちろん、これらのサービスでは、現在台頭しつつある、コンテンツベースで、コネクションレス型のデータネットワークモデルが十分に考慮されています。

これらのサービスを取り入れることにより、次世代のアプリケーションをビジネスで展開することができます。リアルタイムの取引、インタラクティブなサポート、オンデマンドの画像、マルチサイトコミュニケーション、統合メッセージ機能など、インターネットアプリケーション技術は、競争力を高める新しいビジネスモデルの基礎であり、これらの技術を活用することにより、顧客サービスが改善されると共に、大胆に経費を見直すことができます。

従来、ルータなどのネットワーク装置を介してサービスを提供すると、パフォーマンスが犠牲にされてきました。顧客は自社のネットワークでより多くのサービスを展開し、ネットワークをさらにインテリジェント化しつつあります。マルチサービス機能が利用され、マルチメディアトラフィックに対しては、より予測しやすい応答が求められています。現在のネットワーク装置に対して、サービスを高速化して欲しいという需要があることは明らかです。

この問題に対処したシスコの新製品が、Cisco 7200VXRルータファミリ用のNSE-1(Network Service Engine)です。シスコで

は、ハードウェアによってサービスを高速化するCisco 7200VXR対応のNSE-1を発表しました。製品発表の時点で、NSE-1は、最も一般的なサービスをハードウェアで処理することによって、従来にない高速処理を実現しています。将来は、さらに多くの高速サービスが提供できる予定です。NSE-1と従来のスイッチングエンジンを比較すると、NSE-1はサービスに対して大幅な性能の向上が見られます。

NSE-1は定評のあるCisco IOSソフトウェアと最先端のプロセッシングハードウェア技術で構成されており、Cisco 7200VXR高性能スイッチングルータの基盤となっています。NSE-1には、PXF(Parallel Express Forwarding)という新しいフォワーディングパラダイムに基づいた、独自の分散並行処理アーキテクチャが実装されています。これは、従来のスイッチングエンジンに比べて、これらの「インテリジェント」ネットワークサービスをはるかに高速に処理できます。

PXFプロセッサにより、IPマルチパケットプロセッシング機能が可能になり、プライマリプロセッサと並行処理するため、IPのレイヤ3機能を高速に処理できるようになります。PXFプロセッサによって、ルート/スイッチプロセッサのIPパケット処理とスイッチング機能の負荷が軽減され、アクセス制御リスト、アドレス変換、QoS(Quality of Service)、フローの課金、トラフィックシェイピングなど、1つまたは複数のIPサービス機能の処理中にも、スイッチング性能が落ちることなく安定化します。

Cisco 7200シリーズでは、企業とサービスプロバイダーの両方の要望に合った優れた価格性能比を実現しています。スケラブルな性能、密度、ポート当たりの価格の安さが特徴のCisco 7200では、ネットワーク層の機能を拡張でき、より幅広いネットワーク構成や環境に対応することができます。NSE-1を使うと、多くのロケーションに分散している企業ネットワークに必要な、セキュリティ、QoS、トラフィック管理といった高性能なネットワーク層のスイッチングとサービスを楽しむことができます。

NSE-1にはプログラマブルな超高速スイッチング エンジンが搭載されていて、常に変化しているルーティング機能に対する要件にも対応できる柔軟性を備えています。NSE-1には、PXF プロセッサというオンボード型の先進のASICマルチ プロセッサが搭載されていて、IPベースの機能が高速に処理されます。PXFプロセッサを使用すると、ネットワークサービスやネットワーク機能をハードウェアによって高速化できます。

初回出荷時点で、PXF プロセッサにより、WFQ (Weighted Fair Queuing) や輻輳回避をするためのWRED(Weighted Random Early Detection) などの従来のQoS機能に加えて、NAT (ネットワークアドレス変換) NetFlow サービス、T-ACL (Turbo-Access Control Lists) などのサービスも高速な処理が可能です。cRTPやLFIなどのマルチサービスは、初回出荷後のソ

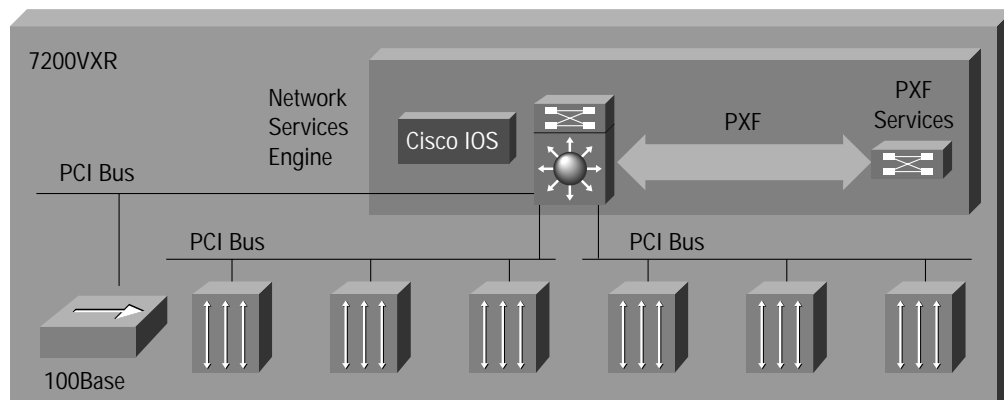
フトウェアリリースで追加される予定です。性能テストでは、従来のスイッチングエンジンにリストされた5つの機能で、50 ~ 350%の性能の向上が確認されました。

PXFの特徴は、ハードウェアベースのスイッチング機能に加え、プログラム可能なアーキテクチャの柔軟性を備えていることです。PXFアーキテクチャは将来を見据えた設計になっていて、今後、新しい機能が追加された場合でも、ASICは必要ありません。サービスを高速化するための新機能は、PXFプロセッサのプログラムを書き換えることによって追加できます。

NSE-1では、以下の最も一般的なサービスがPXF プロセッサハードウェアによって高速処理されます。

サービス	ソフトウェアサポート	ハードウェアによる高速処理サポート
CEF		
NAT(ネットワークアドレス変換)		初回出荷時
T-ACL(ターボアクセス制御リスト)		初回出荷時
NetFlowサービス		初回出荷時
WRED(輻輳回避)		初回出荷時
WFQ(Weighted Fair queuing)		初回出荷時
cRTP		対応予定
トラフィックシェイピング		対応予定
トンネリング		対応予定
IPマルチキャスト		対応予定

図3 : NSE-1 アーキテクチャ



NAT (ネットワークアドレス変換)

インターネットが直面している重要な問題の2つは、IPアドレス空間の枯渇とルーティングされる量の増大です。NAT(ネットワークアドレス変換)は、実際に組織内で使用されているものとは違うIPアドレスを使って、組織外との通信を可能にする機能です。このように、NATではインターネットを経由しないアドレスをインターネットを経由するアドレス空間へ変換することによって、プライベートアドレスを使っているユーザーでもインターネットへ接続できるようになります。また、NATでは、サービスプロバイダーを変えようとする組織が手間をかけずに番号の変更ができたり、自主的にCIDRブロックへ番号を変える際にも有効です。NATはRFC 1631にも記述されています。

NAT アプリケーション

NATは、以下のような目的で使用されます。

インターネットには接続したいが、すべてのホストにグローバルIPアドレスを割り当てられない。

NATを利用すると、登録されていないIPアドレスを使用するプライベートIPインターネットネットワークをインターネットに接続できます。NATは、スタブドメイン(内部ネットワーク)とインターネットなどの公衆ネットワーク(外部ネットワーク)の境界にあるルータで設定されます。外部ネットワークにパケットを送信する前に、NATによって、内部のローカルアドレスがグローバルIPアドレスに変換されます。

内部アドレスを変更する必要がある。

アドレスの変更には、大変な労力が必要です。内部アドレスを変更する代わりにNATを使用して、アドレスを変更することができます。

TCPトラフィックの基本的な負荷を共有したい。

TCPの負荷分散機能を使用することによって、多くのローカルIPアドレスに1つのグローバルIPアドレスを割り当てることができます。

NATの利点

NATの大きなメリットは、NATの設定が必要なルータを除いて、それ以外のホストやルータの変更をする必要がないという点です。ただし、スタブドメイン内の大量のホストがドメイン外部と通信をする場合、NATは実用的ではないことがあります。さらに、アプリケーションによっては、埋め込まれたIPアドレスが使用され、NATデバイスに変換を任せられないこともあります。これらのアプリケーションの場合、NATデバイスでは自動的に処理できなかったり、まったく機能しなかったりすることがあります。また、NATを使用すると、外部からはホストIDが見えなくなるのですが、これには良い面と悪い面があります。

NATが設定されたルータには、少なくとも、内部に対するインタフェースが1つと外部に対するインタフェースが1つあります。従来の環境では、スタブドメインとバックボーンの間にあるルータにNATが設定されます。パケットがドメインから出て行くとき、ローカル環境で使われている送信元アドレスがNATによってグローバルアドレスに変換されます。ドメインに入るパケットについては、宛先となっているグローバルアドレスがNATによってローカルアドレスに変換されます。2つ以上の出口がある場合は、それぞれのNATに同じ変換テーブルがなければなりません。

初回出荷時点で、NSE-1はPXFスイッチングによってNATをサポートしており、ハードウェアによる高速処理に対応しています。

図4 : NAT プール

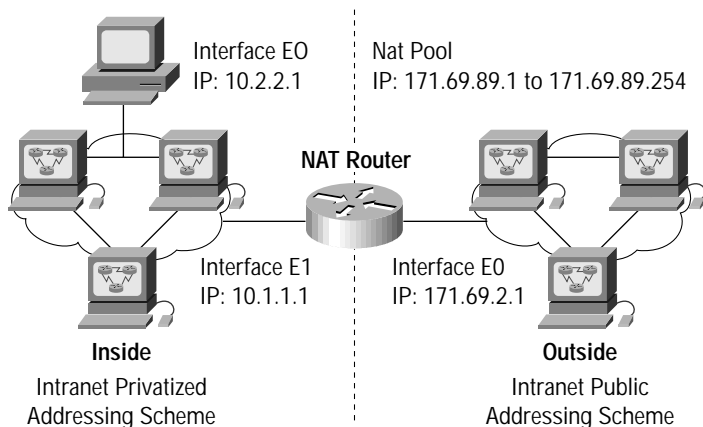
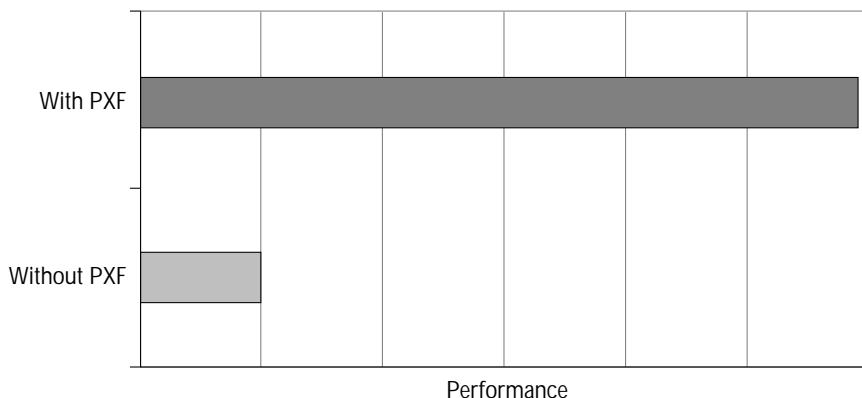


図5：NSE-1のPXFスイッチングを使ってハードウェアで処理することによってNATの処理速度が向上



NetFlow サービス

急速にインターネットとイントラネットが発展して普及したことで、企業と消費者両方のコンピューティング環境に大きな変化が起きました。こうした変化により、ネットワークの帯域幅、性能、予測可能なサービス品質のほか、マルチメディアやセキュリティを重視したネットワークサービスに対する需要がさらに強くなっています。同時に、こうした変化をサポートするため、ネットワークやアプリケーションの活用状況を効率的に記録して提供できる測定技術に対するニーズも高まっています。シスコのNetFlowサービスには、これらの問題に対する解決策が用意されています。

NetFlowは、シスコのインターネットおよび企業におけるQoS (Quality of Service) の測定基準となっています。NetFlowにより、トラフィックの選別情報やフローごとに優先順位を付けて、QoSに基づく差別化された課金が可能になります。

ネットワークフローは、所定の送信元と宛先のエンドポイントとの間で一定方向へ流れる連続したパケットとして定義できます。また、フローのエンドポイントは、IPアドレスと同時にトランスポート層のアプリケーションポート番号によって識別されます。さらにNetFlowでは、IPプロトコルタイプ、ToS (Type of Service) 入力インタフェースIDを利用し、フローが一意に識別されます。

NetFlowが機能していないスイッチングの場合、着信パケットは別々に処理され、スイッチング、セキュリティ、サービス、トラフィックの測定は、個別のタスクによってパケットごとに行われます。NetFlowが機能しているスイッチングの場合、セキュリティ (ACL) 処理はフローの最初のパケットにだけ適用され、このパケットの情報を利用して、NetFlowキャッシュのエントリが作成されます。同じフローのそれ以降のパケットについては、スイッチング、サービス、データ収集を同時に処理する1つの効率的なタスクによって処理されます。このように、NetFlowサービスは、ネットワークトラフィックのフロー特性を活用して、以下の機能を提供しています。

ルータの性能に及ぼす影響を最小限にして詳細なデータ収集を行う。

効率的にアクセスリストを処理し、パケットのフィルタリングやセキュリティサービスを提供する。

NetFlow によるアプリケーション

課金と請求書の発行

NetFlow データには、IPアドレス、パケットおよびバイト数、タイムスタンプ、サービスタイプ、アプリケーションポートが含まれていますから、柔軟性が高く、リソースを細かに活用して課金をする厳密な測定が可能です。この情報を利用することで、サービスプロバイダーは、単一料金・定額料金の請求方法から、時間帯、帯域幅使用量、アプリケーションの使用方法、サービス品質など、より柔軟性のある課金方式に移行することができます。一般企業ではこの情報を活用して、部署の入金取消しや資源利用のための経費分担に利用することもできます。

ネットワーク計画と分析

NetFlow データには、Netsysなどの洗練されたツールで活用できる重要な情報が含まれているので、長期戦略に基づくネットワーク計画 (接続先の決定、バックボーンのアップグレード計画、ルーティングポリシーの策定など) と短期戦略に基づくネットワークエンジニアリング (ルータへのVIPの追加、リンク容量のアップグレードなど) の両方を明確にすることができます。さらに、ネットワーク運用にかかる全体的な費用を最小限に抑えつつ、ネットワークの性能、容量、信頼性を最大限に引き出すことができます。

ネットワークの監視

NetFlowデータに基づき、ほぼリアルタイムで広範囲にネットワークを監視する機能を使用できます。フローベースの分析技法を用いれば、個々のルータやスイッチごとのデータの他にも、ネットワーク全体をベース (トラフィックやアプリケーション全体が見える表示方法) にして、トラフィックパターンを視覚化し、問題の事前検出、効率的な障害の復旧、短時間での問題解決が可能になります。

アプリケーションの監視とプロファイリング

NetFlow データをネットワーク管理者が活用することによって、ネットワーク上で使用されているアプリケーションの使用状況を詳細かつ時間帯別に表示できます。この情報をコンテンツプロバイダーやサービスプロバイダーが活用すれば、ネットワークやアプリケーション資源 (Webサーバーの規模やロケーションなど) を計画し、割り当てて、顧客の要望に対して素早く対処できます。

ユーザーの監視とプロファイリング

NetFlow データをネットワーク管理者が活用することによって、顧客やユーザーのネットワーク資源またはアプリケーション資源の使用状況を詳細に知ることができます。こうした情報は、アクセスやバックボーン、またはアプリケーション資源を効率的に計画して割り当てる際に利用できるほか、考えられるセキュリティやポリシーの侵害を検出して、それらを解決する際にも役立ちます。

NetFlow データハウジングとデータマイニング

NetFlow データ（またはその派生情報）を蓄積して、積極的なマーケティングや顧客サービスプログラム（内部および外部ユーザーがどのアプリケーションとサービスを使用しているかを理解し、サービスや広告を改善するなどのプログラム）をサポートするための検索や分析に後日使用することができます。これは、とりわけ、インターネット接続を提供するプロバイダーにとっては効果的です。なぜなら、NetFlow データを活用することで、サービス提供方法の幅が格段と広がるからです。また、インターネット市場のリサーチであれば、NetFlow データを分析して、インターネットの消費者に関連する「誰が」「何を」「どこで」「どれ程の時間」使用したかといった情報を知ることができます。

NetFlow のキャッシュ管理とデータエクスポート

NetFlow が機能するスイッチングのスケラビリティと性能の鍵を握るのは、高度でインテリジェントなフローキャッシュの管理をすることです。なかでも、短時間に同時発生するフローを大量に処理する高密度なエッジルータに対する管理は重要です。NetFlow のキャッシュ管理ソフトウェアには、高度に洗練されたアルゴリズムが組み込まれています。このソフトウェアでは、パケットが既存フローの一部であるかどうか、NetFlow キャッシュに格納されているフローごとの課金測定値とキャッシュのエージング/フロー期限の決定を動的にアップグレードするかどうか、などが効率的に決定されます。

期限の切れたフローは「NetFlow Export」UDP データグラムにまとめられて、NetFlow が機能するデバイスからエクスポートされます。バージョン 5 のフローエクスポートの場合、NetFlow Export データグラムに最大 30 までのフロー記録が含まれます（バージョン 1 のフローエクスポートの場合、最大 25 までのフロー記録）。フローデータグラムは、少なくとも、毎秒 1 回か、期限の切れたフローの完全な UDP データグラムが発生した時点で、NetFlow が機能するデバイスからエクスポートされます。NetFlow 機能はインタフェース単位で設定されます。

Cisco IOS ルータベースの NetFlow 集約

単位時間あたりに多数のフローをスイッチするハイエンドルータ（Cisco 7500 や Cisco 7200 など）の多くのインタフェースで NetFlow が機能している場合、NetFlow からエクスポートされたデータ量は膨大になることが予想できます。Cisco IOS® ソフトウェア機能拡張として、NetFlow Export のデータ量を大幅に削減し、NetFlow のスケラビリティを改善するために設計されたルータベースの NetFlow 集約があります。これによって、NetFlow Export データのルータベース集約を制限することができます。ルータベースの NetFlow 集約は、バージョン 5 から対応している機能で、Cisco NetFlow FlowCollector v2.0 などの NetFlow データ収集デバイスにデータがエクスポートされる前に、ルータで NetFlow Export データを集約できます。この機能を使用すると、集約された NetFlow Export データが収集デバイ

スにエクスポートされ、NetFlow Export データの帯域幅要件と NetFlow データ収集デバイスのプラットフォーム要件が少なくすみすみます。さらに、この機能には、新しい Export データグラム形式の NetFlow Export バージョン 8（v8）が採用されており、NetFlow Export の性能と帯域幅の活用を最適化できます。

ルータベースの NetFlow 集約機能は、フィールドの組み合わせによってフローをグループ化し、別のフローキャッシュを維持することによって、オンボード集約を可能にします。これらのキャッシュを集約キャッシュと言います。主要フローキャッシュのフローの期限が切れると、フローキャッシュは集約キャッシュに追加されます。通常のフローエージング処理は、主要キャッシュと同じく、アクティブな集約キャッシュで実行されます。必要に応じて、エージングにも対応します。

セカンダリ NetFlow 集約キャッシュ（v8 NetFlow Export データグラムと共にエクスポートされるキャッシュ）のデフォルトサイズは、Cisco IOS NetFlow をサポートするどのプラットフォームでも 4096 エントリです。

NetFlow のアクティブ化とデータ収集戦略

サービスプロバイダーがエッジおよび集約ルータ上で NetFlow を展開するにしても、企業が計画、監視、課金アプリケーションに必要なデータの取得を行うために WAN アクセスルータ上で NetFlow を展開するにしても、NetFlow サービスを利用する場合には、綿密な計画を立てる必要があります。NetFlow を展開する上での注意事項を紹介します。

NetFlow サービスはエッジ測定とアクセスリストの高速化ツールとして活用してください。コア/バックボーンルータや CPU 稼働率の高いルータでは、アクティブにしないでください。アプリケーションからのデータ収集要件を理解してください。課金アプリケーションでは、始点と終点ルータのフロー情報しか必要ありませんが、監視アプリケーションでは、より包括的（データ集約的）なエンドツーエンドの表示が必要になることがあります。

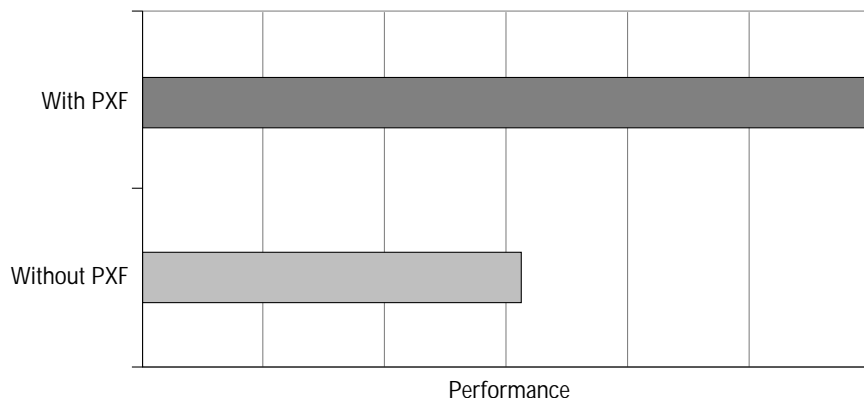
ネットワークポロジの影響とフロー収集のルーティングポリシーを理解してください。例えば、トラフィックの起点や終点となる主要な集約ルータで NetFlow をアクティブにして、フロー情報を重複して収集しないようにします。バックボーンルータや同じフロー情報を収集する可能性のある中継ルータではアクティブにしないでください。

「中継通信事業」業務を営むサービスプロバイダー（すなわち、自社ネットワークが始点にも終点にもならないトラフィックを中継する業者）の場合、NetFlow Export データからネットワーク資源の通過トラフィック使用状況を測定し、課金・請求書の発行にデータを利用できます。

NetFlow は入力側の測定技術です。データへの課金や監視、ネットワークの計画を考えている顧客のニーズを満たし、起点と終点のトラフィックを包括的に表示するには、エッジ/集約ルータまたは WAN アクセスルータの正しいインタフェース上で NetFlow を展開する必要があります。NetFlow のデータ量を管理する際に重要なのは、NetFlow の展開を入念に計画することです。ネットワーク内の全ルータに広範囲にわたって NetFlow を展開しなくても、ルータのインタフェース単位で徐々に展開することもできます。

初回出荷時点で、NSE-1 は PFX スwitchングによって NetFlow をサポートしており、ハードウェアによる高速処理に対応しています。

図 6 : NSE-1 の PXF スイッチングを使ってハードウェアで処理することによって NetFlow の処理速度が向上



ターボアクセス制御リスト

通常、ACL (アクセス制御リスト) は順番に一致するルールを探します。そのため、ACL は様々な要因を考慮して配列されています。Cisco IOS のアクセスリストでは、レイヤ 2 とレイヤ 3 のプロトコルで使用できますが、なかでも、最も一般的に使用されるのは IP アクセスリストです。Cisco IOS には、単純アクセスリストと拡張アクセスリストという 2 種類の IP アクセスリストがあります。単純アクセスリストの場合、パケットの IP 送信元アドレスしかチェックしません。拡張アクセスリストでは、ヘッダフィールドの番号もチェックします。多くの場合、アクセスリストを使用してセキュリティの確保とパケットのフィルタリングを行っています。何百ものルールが設定されたアクセスリストが使用されていることも珍しくありません。セキュリティのフィルタリングとパケットの優先順位付けなどへのニーズが高まるにつれ、パケットが転送されるときに ACL を検索するのに多大な時間とメモリが必要になるところまで肥大化しています。これまで Cisco IOS では、各アクセスリストの要素がパケットに一致するまで順番に比較することによって、アクセスリストを処理していました。これでは、大規模なアクセスリストのために性能に問題が生じることがあります。さらに、リストを検索するためにルータが必要とする時間は必ずしも一定ではなく、パケット転送に伴う遅延も定まりません。もちろん、CPU にかかる負荷も大きくなります。

ターボ ACL 機能は、ACL をコンパイルして、最初の一致要件を維持したルックアップテーブルを作成します。パケットヘッダは、既存の ACL エントリ数に関係なく、小さくて固定した数のルックアップに入っている、これらのテーブルにアクセスする際に使用されます。この機能の利点として以下の点が考えられます。

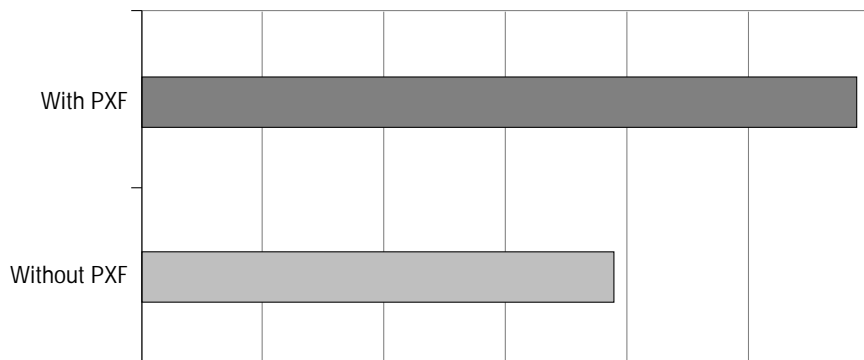
エントリ数が 3 より大きい ACL の場合、既定のパケット一致ルールにパケットを一致させるためにかかる CPU の負荷が軽減される。ACL の大きさに関係なく、CPU の負荷は固定されていて、CPU のオーバーヘッドという代償を払わずに、より大きな ACL を利用できる。ACL が大きいほど、より大きなメリットを享受できる。

パケットを一致させるためにかかる時間が固定されているため、パケットの遅延が短く (大きな ACL の場合は余計に) 、さらに重要な点としては、一定であり、その結果、ネットワークの安定性が向上し、通過時間がより正確になる。

NSE-1 には高速ターボアクセス制御リスト機能があります。これは、従来のアクセスリストやターボアクセスリストより、はるかに優れた性能を備えています。アクセスリストは単にセキュリティを確保する以上に、多様な経路マップやサービス品質チェックを行う手段としても利用可能です。

初回出荷時点で、NSE-1 は PXF スイッチングによってターボ ACL をサポートしており、ハードウェアによる高速処理に対応しています。

図 7 : NSE-1 の PXF スイッチングを使ってハードウェアで処理することによってターボ ACL の処理速度が向上



WFQ によるインテリジェントなキューイング機構

QoSは次世代のビジネストラフィックの重要な構成要素です。「ストアアンドフォワード」モデルからインターネットワーキングの「ストリームと廃棄」モデルへ移行する際、配信条件を定義するための能力がますます欠かせなくなっています。ビジネスにおいて、オンデマンドの会話型トラフィック(ビデオ会議)やスピードが要求される情報配信(株取引)を使用するには、QoSが必要です。

QoSを確保することにより、ネットワークリンクを効率よく使用でき、WAN(Wide-Area Network)のコストが削減されます。QoSが確保されると、ネットワーク管理者は加入超過を相当のレベルまでは心配する必要がなくなり、自分の仕事に取りかかることができます。トラフィック構成を管理して、時間に敏感なトラフィックが遅れないように手を打つ必要はありません。またQoSにより、音声、ビデオ、データトラフィックを統合できます。

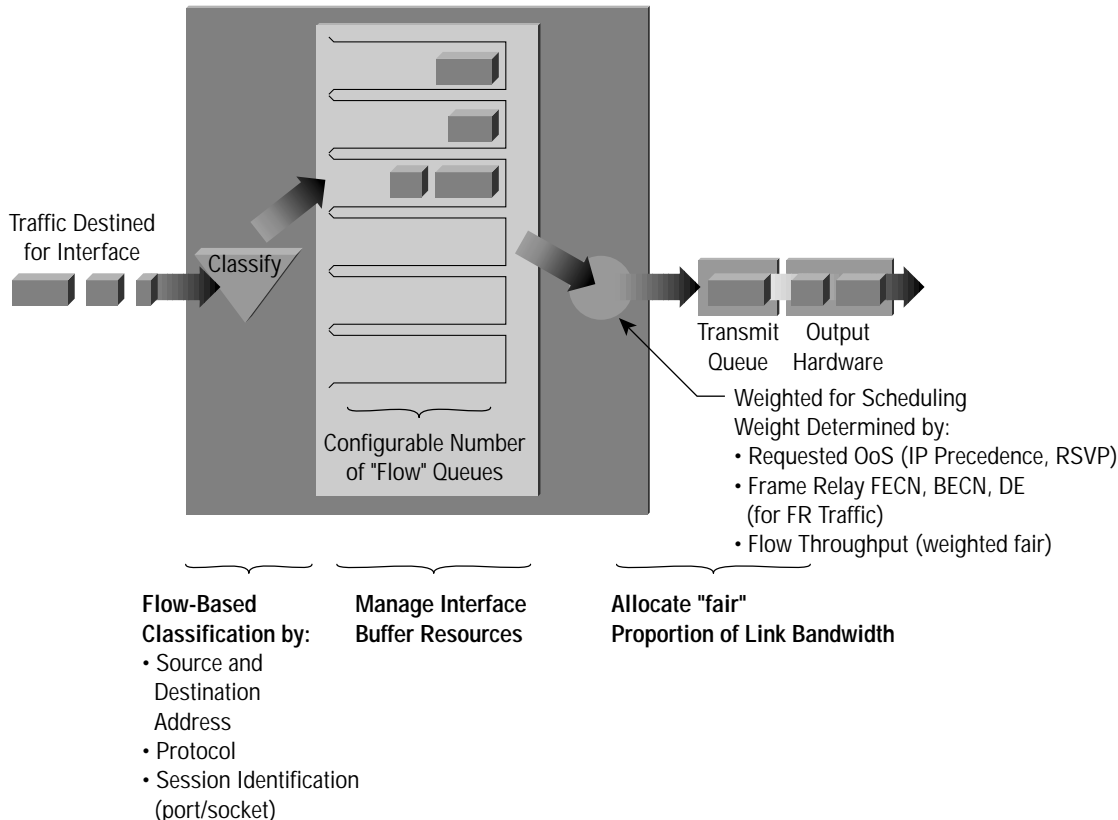
過度の帯域幅を使用せずに、ネットワークを頻繁に利用するユーザーとそうでないユーザーとに対して、同じように一定の応答時間を返すことが望ましいような状況では、WFQ(Weighted Fair Queuing)が有効です。WFQは、シスコの最も重要なキューイング技術で、現在、NSE-1にも実装されています。このキューイングアルゴリズムでは、フローの種類に応じて2つのことを同時に処理します。インタラクティブなトラフィックは、キューの最初に来るようにスケジュールされて応答時間が短縮されます。残りの帯域幅は、その他のフローで均等に共有されます。

WFQを使用することによって、キューが帯域幅を独占せず、予想できるサービスをトラフィックが受けるように保証されます。少量のトラフィックストリーム(トラフィックの大部分を占める)は優先的にサービスを受け、負荷全体がタイミングよく転送されます。図8にあるように、大量のトラフィックストリームの場合、残りの容量がストリーム間で均等に共有されます。

WFQは、ユーザーの設定作業が最少になり、変化するネットワークトラフィック条件に自動的に対応できるように設計されています。実際、WFQはほとんどのアプリケーションにとって有効であるため、E1速度(2.048Mbps)またはそれ以下で稼動するシリアルインタフェースの多くで、デフォルトのキューイングモードとして使われています。

WFQでは、優先順位の高いフローがない場合は優先順位の低いフローからトラフィックを転送していくことによって、利用可能な帯域幅が効率良く使用されます。これは、単純に帯域幅を分割し、特定の種類のトラフィックがない場合は使用されないまま帯域幅を放置するTDM(時分割多重)とは異なります。WFQは、シスコの主要QoSシグナリング方式であるIP PrecedenceやRSVPと共に機能し、差別化されたQoSと保証されたQoSサービスを提供します。

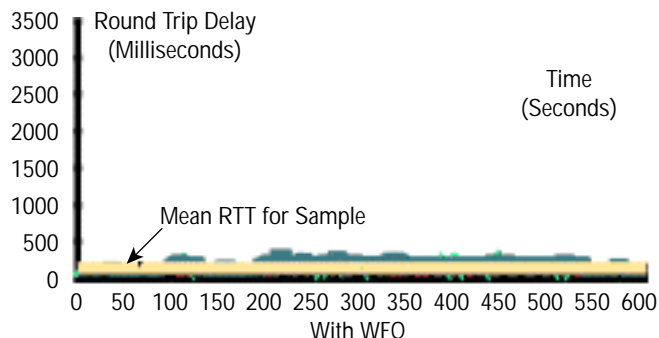
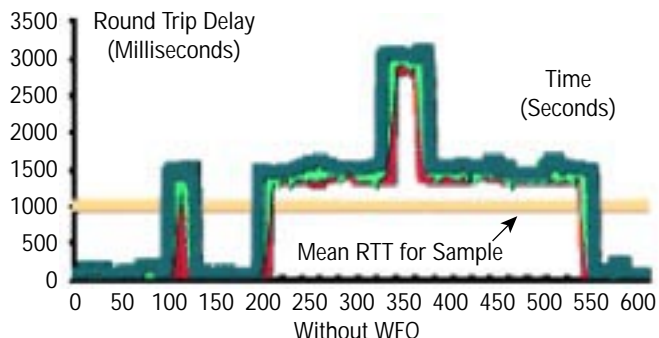
図8 : NSE-1でのWFQ



WFQ アルゴリズムは、往復にかかる遅延のばらつきの問題にも対応しています。複数の大量の会話が交わされている場合、それらの転送レートと到着までの時間が予測しやすくなります。WFQにより、SNAのLLQ(論理リンク制御)やTCP(Transmission

Control Protocol)の輻輳制御とスロースタート機能などのアルゴリズムが大幅に強化されています。その結果、図9にあるように、アクティブなフローごとのスルーputと応答時間が予測しやすくなっています。

図9：ラウンドトリップ遅延

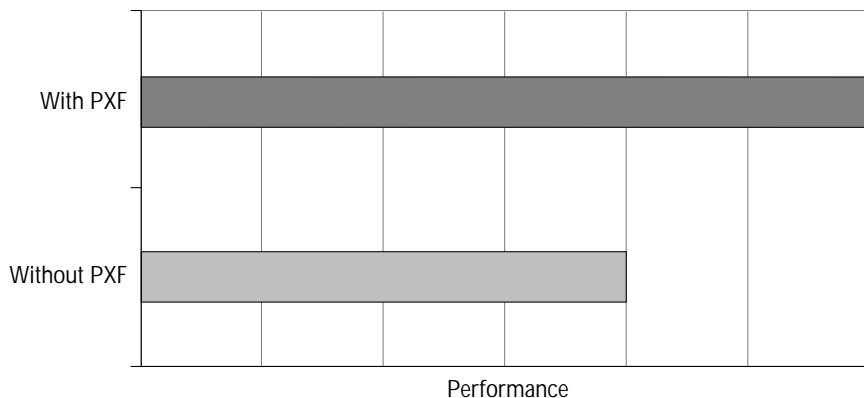


WFQはIP Precedenceを認識します。すなわち、IP転送機能によって高い優先順位がつけられた packets をWFQが検出して、それらを高速にスケジュールし、そのトラフィックの応答時間を格段に短くします。IP Precedence フィールドには0(デフォルト)~7までの値を設定できます。優先順位の値が大きくなれば、アルゴリズムによって、そのトラフィックにより大きな帯域幅が割り当てられ、輻輳が発生した場合も、早くサービスが受けられるように保証されます。WFQが各フローに対して重みを割り当てて、キューに入った packets の伝送順位を決定します。この方式では、重みの低いフローが優先されます。IP Precedenceはこの重み係数に対して除数として機能します。たとえば、IP Precedence フィールド値が7のトラフィックは、IP Precedence フィールド値が3のトラフィックより低い重みを受け取り、伝送順位も優先されます。

また、WFQはRSVPも認識します。RSVPはWFQを使用してバッファスペースを割り当て、packetのスケジュールを立てて、予約されたフローに対して帯域幅を保証します。さらに、フレームリレーネットワークでは、輻輳の発生はFECN(順方向明示的輻輳通知)とBECN(逆方向明示的輻輳通知)のフラグが立てられます。フレームリレーのスイッチングモジュールによってトラフィックがスイッチされる際、WFQの重みは、フレームリレーのDE(廃棄適性)、FECN、BECNビットの影響を受けます。いったん輻輳のフラグが立てられると、アルゴリズムが使用する重みを変更されて、輻輳に遭遇した会話が伝送される頻度が少なくなります。

初回出荷時点で、NSE-1はPXFスイッチングによってWFQをサポートしており、ハードウェアによる高速処理に対応しています。

図10：NSE-1のPXFスイッチングを使ってハードウェアで処理することによってWFQの処理速度が向上



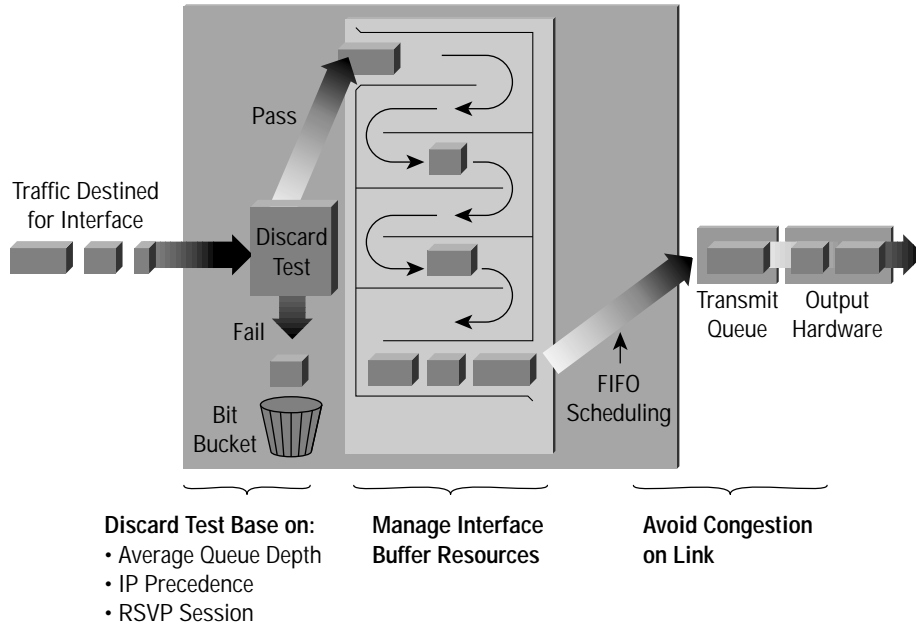
輻輳回避ツール

輻輳が発生してから輻輳を制御しようとする輻輳管理手法とは異なり、輻輳回避手法では、一般的なネットワークのボトルネックで発生する輻輳を予測および回避するためにネットワークトラフィックの負荷を監視します。主要なCisco IOSの輻輳回避ツールは、WRED (Weighted Random Early Detection) です。

輻輳を回避する WRED

RED (Random Early Detection) という種類のアルゴリズムは、輻輳が問題となる前に、インターネットワーク内で輻輳を回避するように設計されています。REDはネットワーク内の複数の地点でトラフィックの負荷を監視し、輻輳が大きくなり始めると、パケットを選別して破棄します。破棄されたトラフィックについては送信元が検出し、伝送を遅らせます。REDは、IPインターネットワーク環境のTCPで機能するように設計されています。

図 11 : WRED メカニズム



WREDは、TCPのように、トラフィックのかなりの割合のパケットが消失しても問題とならないような環境で正常に機能します。Novell NetwareやAppleTalkのように、パケットの消失に対して脆弱なトラフィックの場合、トラフィックを破棄することによって輻輳を管理しようとするアルゴリズムは、重大な副作用の影響を受ける可能性があります。また、音声などのリアルタイムトラフィックは、一度しか送信されないため、パケットの消失に対する応答も不十分です。WREDの管理オーバーヘッドは非常に少なく、OC-3までの高速インタフェース上で正常に機能します。

REDの仕組みを完全に理解するには、パケットの消失が発生する条件に対して堅牢なプロトコル(TCP)での働きを理解する必要があります。

TCPの受信側がデータセグメントを受けとったとき、そのセグメントがTCPの受信側が期待する次のセグメントであるか(オクテットのシーケンス番号が期待した番号かどうか)が重要になります。受信したのが次のセグメントであれば、可能な全部のデータをアプリケーションに配信し、次に期待されるシーケンス番号を更新し、ACK(肯定応答)そのシーケンス番号を除いて、その前のすべてのデータを受信したというメッセージをすぐに返すか、少し遅れて、そのセグメントが送信されてくるようにスケジュールします。通常、1つおきのセグメントに対してACKが返されるようになっていきます。その理由は簡単です。多くのアプリケーションでは、ACKを送るための返信応答が用意されており、少し遅らせることによってACKを一緒に運ぶことができ

るためです。しかし、順番通りになっていないデータを受け取ったときは、一般的には、すぐにACKが返信されます。何か欠損があれば、最初の再送だけで修復できるようにするためです。

TCPの送信側がACKを受け取ると、最初に何か未送信のデータがないかどうかをチェックします。何もなければ、キーアライブメッセージが送出されます。未送信のデータがあれば、そのデータの一部があるか、または何もないかが確認されます。一部が残っている場合、送信側は新しく承認された内容があるかどうかをチェックし、さらに送信ができるようになります。何もデータがない状態で未送信データの通知があれば、考えられる理由は1つだけです。それは、確認が繰り返されただけということです。それでは、なぜ送信側は確認を繰り返すのでしょうか。最も可能性が高いのは、順番通りになっていないいくつかのデータ(最初のACKを強制)を受信し、順番通りになっていない2番目のセグメント(2番目のACKを強制)を受け取ったためです。それにしても、なぜ順番通りになっていない2つのセグメントを受け取ったのでしょうか。おそらく、1つは消失したためでしょう。

単純にヒューリスティックが記述されているか、または伝送時間のタイムアウトが発生したことが原因で、TCP送信側が欠損セグメントを検出すると、(a)最初のセグメントが確認待ちリストに渡され(データのフローを再始動するため)、(b)スロースタートフェーズに入ります。ネットワークがテストされ、欠損データなしに送信できるレートが探されます。

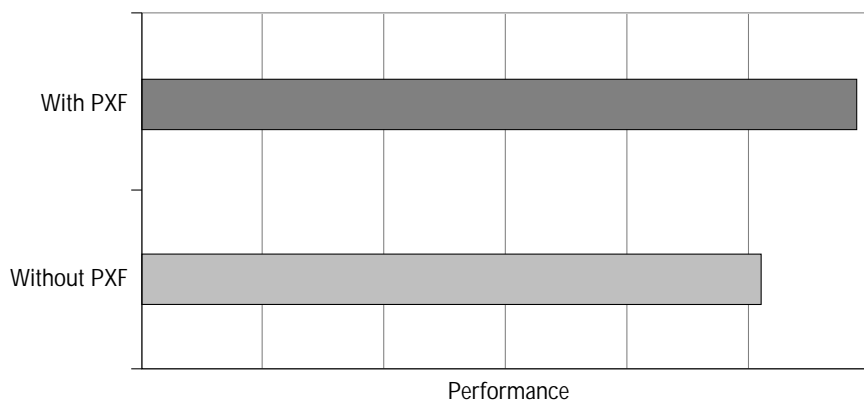
WREDを利用していないネットワークでは、バッファが一杯になり、パケットの末尾が消失すると、複数のTCPセッションがすべてスロースタート方式で再開します。この場合、TCPのウィンドウサイズが大きくなり、最終的にはネットワークトラフィックが急増してしまいます。ルータでREDを使用すると、TCPのスロースタート方式を管理し、個別のTCPフローを制御して、影響を測定したり、TCPフローが増大したときに、必要に応じてパケットを廃棄できます。

REDには、2種類のキューがあります。1つは、「通常の操作」と考えられる部分で、ここでは、意図的にデータが破棄されることはありません。もう1つは、増大するTCPセッションの振幅が大きくなったときにオーバーフローに対処する部分です。これらのオーバーフローは、伝送と保持されているキューの深さに直接的な相関関係があります。また、REDによってキューの平均の深さが測定されます。キューの平均の深さが低い範囲にある場合、

上位の範囲が一時バッファとして使用されます。キューの平均の深さが高ければ、データの廃棄が開始されます。すべてのデータが廃棄されるわけではありませんが、一定のレートで廃棄が始まります。

REDにはキューの深さの指数加重移動平均が維持されています。また、REDには、この移動平均に使用されるしきい値のテーブルがあり、保持されたキューの組み合わせの半分の深さと、TXキューの制限と、満杯の深さの間の地点に分散されています。キューに入れるために、保持されているキューにパケットが渡されると、REDにより、パケットの優先度が決定されます（IP Precedenceが0.7、RSVPの優先レベルは8として設定）。キューの平均の深さが指定されたしきい値を越えた場合、確率関数が呼び出され、乱数が作成されます。その確率を基にパケットが破棄されます。失敗した場合はキューに入ります。

図 12 : NSE-1 の PXF スイッチングを使ってハードウェアで処理することによって WRED の処理速度が向上



WREDではREDアルゴリズムとIP Precedence機能の両方を使用できます。これらの機能を併用することにより、優先度の高いパケットに対してトラフィックを優先的に処理することができます。インタフェースに輻輳が発生し始めたときに、優先度の低いトラフィックを選択して廃棄し、異なるクラスのサービスに差別化したパフォーマンス特性を与えることができます。

WREDはRSVPも認識し、負荷を制御するQoS統合サービスを利用できます。

初回出荷時点で、NSE-1はPXFスイッチングによって輻輳回避WREDをサポートしており、ハードウェアによる高速処理に対応しています。

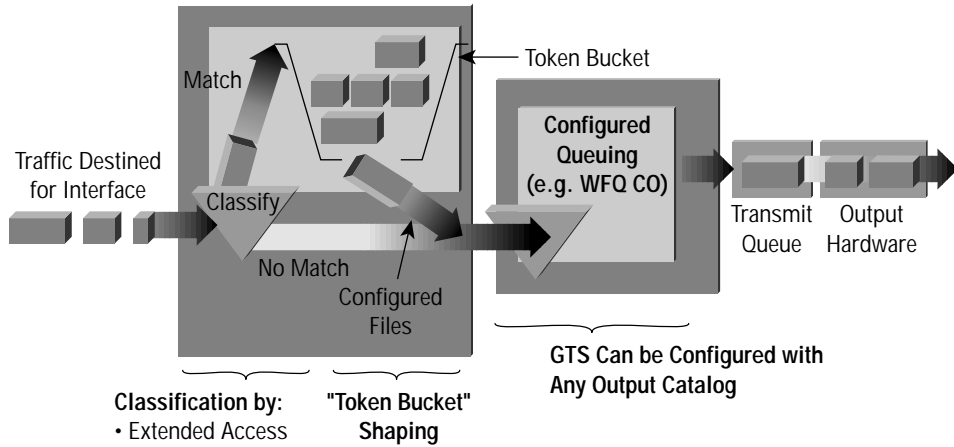
トラフィックシェイピング

シスコのQoSソリューションには、トラフィックシェイピングツールGTS (Generic Traffic Shaping) が含まれており、ネットワーク上のトラフィックや輻輳を管理できます。

アウトバウンドのトラフィックフローを制御するGTS

GTS (Generic Traffic Shaping) により、特定のインタフェースでトラフィックフローを制御することができます。指定したトラフィックのバーストをキューに入れる一方で、指定したトラフィックを特定のビットレートに制限することによって(トークンパケット方式とも言う) アウトバウンドのトラフィックフローを削減し、輻輳を回避できます。このようにして、特定のプロファイルに一致するトラフィックを調整し、下流の要件を満たすことによって、データレートの不一致があるトポロジのボトルネックを解消します。図 13 に GTS を説明します。

図 13 : トラフィックシェイピングの例



GTSはインタフェース単位で適用することができ、アクセスリストを使用してトラフィックを選択して調整し、フレームリレー、ATM、SMDS (交換マルチメガビットデータサービス)、イーサネットを含むさまざまなレイヤ 2 の技術で機能します。

フレームリレーのサブインタフェースで、BECON信号を統合化し、使用可能な帯域幅に動的に対応するように設定するか、既定レートに合わせて調整するように設定するか、どちらかにGTSを設定できます。GTSはATM/AIPインタフェースカードで設定して、静的に設定されたATMのPVC(相手先固定接続)上でRSVP信号に対応することもできます。

今後、NSE-1はPXFスイッチングのトラフィックシェイピングをサポートし、ハードウェアによる高速処理に対応する予定です。初回出荷時点では、NSE-1はソフトウェア機能としてトラフィックシェイピングをサポートしています。

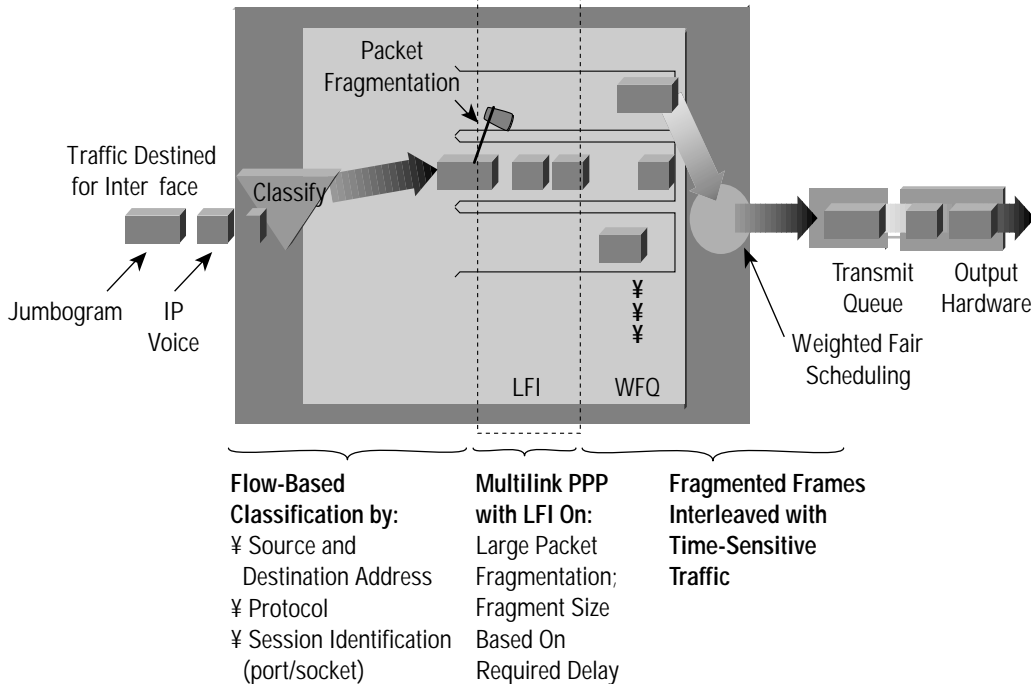
リンク効率化のための仕組み

Cisco IOSは、cRTP(Real Time Protocol Header Compression)とLFI(Link Fragmentation and Interleaving)の2つの方法でリンクを効率化します。これらは、キューイングやトラフィックシェイピングと共に機能し、これらを活用すると、アプリケーションサービスレベルが効率化し、予測もしやすくなります。

IPトラフィックのLFIフラグメントとインタリーブ

ネットワークが大きなパケットを処理している場合(WANリンクをまたがるFTP転送など)、それらのパケットがスピードの遅いリンクのキューに入ってしまうと、TelnetやVoIPなど対話型のトラフィックの遅延やジッタが大きくなり、その影響をまともに受けてしまいます。Cisco IOSのLFI(Link Fragmentation and Interleaving)機能を利用すると、大きなデータグラムが分割されて、小さくなったパケットが他のトラフィックの合間に転送されるようになり、遅い速度のリンク上で発生する遅延やジッタが軽減されます(図14を参照)。

図 14 : LFIメカニズム



Flow-Based Classification by:	Multilink PPP with LFI On:	Fragmented Frames Interleaved with Time-Sensitive Traffic
¥ Source and Destination Address	Large Packet Fragmentation; Fragment Size Based On Required Delay	
¥ Protocol		
¥ Session Identification (port/socket)		

Cisco IOS LFI機能には、シスコが実装しているMLP(マルチリンクPPP)が使用されます。これはRFC 1717の分割およびパケット順序制御に関する仕様に準拠しています。

LFIでは、キューの予約をして、RTP(Real-Time Protocol)ストリームが加重均等化されたキューセット設定のなかで、より高い優先順位を持つキューにマッピングされるように設定することができます。

MLPを使用したLFIがどのように機能するかを理解するには、対象とする問題を理解するのが近道です。リアルタイムパケットの場合、完全なエンドツーエンドの遅延目標となるのは、特に、音声パケットの場合は、150～200ミリ秒(ms)です。音声を伝送するためのIPベースのデータグラム伝送技術は、帯域幅の制限と、150msという非常に厳格なテレフォニーの遅延制限による問題に十分に対応していません。

小さなリアルタイムパケットに対するキューイングの遅延は、RSVP(Resource Reservation Protocol)やWFQ(Weighted Fair Queuing)などのQoS機能を使用しても、本来のビットレートを64Kbpsから最高8 Kbpsまで削減するCELP(Compressed Encoding for Linear Prediction)などの音圧縮アルゴリズムを使用しても発生します。こうした対策をとっても、パケットヘッダごとのオーバーヘッドが大きすぎて、許容可能なバルク伝送効率を実現するには大きなMTU(最大伝送ユニット)が必要になるため、リアルタイムの遅延は依然として発生するのです。

1500バイトという大きなMTUが56Kbpsの回線を通過するには、215ミリ秒が必要です。しかし、これは遅延目標を超えています。このため、56Kbpsのフレームリレーや64KbpsのISDN Bチャネルなどの比較的遅い帯域幅のリンクでは、リアルタイムパケットの遅延を制限するため、大きなパケットを細分化し、その細分化されたフラグメント間に小さなパケットをキューイングする方式が必要になります。この問題の解決には、LFIを介したMLPが有効です。MLPは、複数の論理データリンク上でデータグラムを分割、再統合、配列するための手法です。LFIの方法は比較的単純です。大きなデータグラムは、多重連結され、カプセル化されます。次に、遅延に弱いトラフィックの遅延要件を満たすような小さなサイズのパケットに分割されます。遅延に弱い小さなパケットは多重連結されてカプセル化されることはありませんが、大きなデータグラムから細分化されたパケットの間に交互に配置されます。

MLPにより、分割されたパケットは複数のポイントツーポイントリンクを介して、同じリモートアドレスへ同時に送信されます。ユーザーが定義したダイヤラの負荷しきい値に応じて複数のリンクが確立されます。負荷は、インバウンドトラフィックとアウトバウンドトラフィックか、もしくは特定のサイト間のどちらか一方のトラフィック要件に応じて計算できます。MLPはオン

デマンドで帯域幅を供給し、WANリンク全体の伝送の遅延を軽減します。

LFIは、特に、連続した遅延が顕著な低速リンク用に設計されています。LFIの場合、インタリーブが機能しているインタフェース上でマルチリンクPPPを設定する必要があります。MCML(Multiclass Extensions to Multilink PPP)という、これに関連するIETFドラフトでは、LFIとほぼ同じ機能が具体化されています。

今後、NSE-1はPXFスイッチングを介してLFIをサポートし、ハードウェアによる高速処理に対応する予定です。初回出荷時点では、ソフトウェア機能としてLFIをサポートしています。

リアルタイムトラフィックを効率化する RTP ヘッダ圧縮

RTP(Real-time Transport Protocol)は、パケット化された音声やビデオを含む比較的新しいマルチメディアアプリケーショントラフィックをIPネットワーク上で転送するために使用するホストツーホストのプロトコルです。RTPにより、音声、ビデオ、シミュレーションデータなどのようなリアルタイムで転送する必要のあるマルチキャストまたはユニキャストネットワークサービスのアプリケーションが、エンドツーエンドネットワーク転送機能を利用できるようになります。RTPヘッダ圧縮を行うと、RTPを利用する比較的新しいVoIPやマルチメディアアプリケーションの多くの効率が向上します。図15にRTPヘッダ圧縮の仕組みを示します。

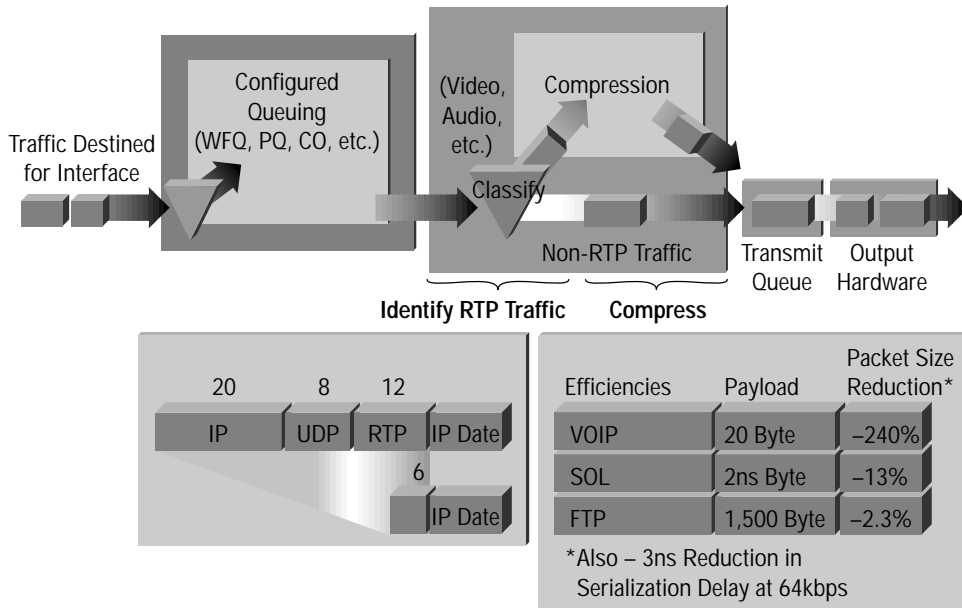
ペイロードを圧縮した音声アプリケーションでは、RTPパケットには40バイトのヘッダと、通常20～150バイトのペイロードが含まれます。IP/UDP/RTPヘッダを組み合わせるときのサイズを考えると、圧縮していないヘッダを転送することは効率的ではありません。RTPヘッダ圧縮によって、40バイトのRTP/UDP/IPヘッダが2～5バイトに圧縮され、特に低速リンクでRTPが効率よく機能します。とりわけ、低速リンク(385Kbps以下)で送出される小さなパケット(IP音声トラフィックなど)には効果的です。スピードの遅いリンクでは、RTPヘッダ圧縮により、オーバーヘッドと転送遅延が著しく減少します。

ヘッダ圧縮により、マルチメディアRTPトラフィックに対する回線のオーバーヘッドが削減され、それと共に遅延も少なくなります。特に、ヘッダ長のわりに小さいパケットを使用するトラフィックに対して効果があります。

cRTPヘッダ圧縮は、フレームリレー、HDLC、PPPカプセル化を使用するシリアル回線に対応しています。また、ISDNインタフェースにも対応しています。

今後、NSE-1はPXFスイッチングによってcRTPをサポートし、ハードウェアによる高速処理に対応する予定です。初回出荷時点では、ソフトウェア機能としてcRTPをサポートしています。

図 15 : 圧縮リアルタイム転送プロトコル

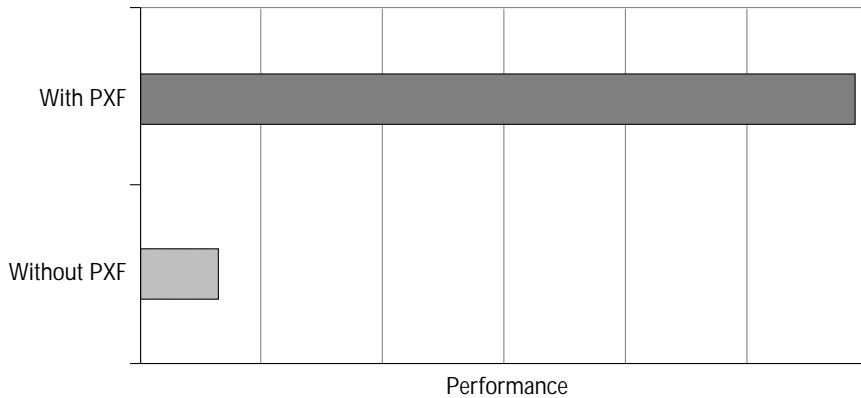


マルチサービスの同時高速処理

顧客は自社ネットワークでより多くのサービスを展開し、ネットワークをさらにインテリジェント化し、マルチメディアトラフィックに対しては、より予測しやすい応答を求める一方、マルチサービス機能を使用するようになってきました。従来、ルータなどのネットワーク装置を介してサービスを提供すると、パフォーマンスが犠牲になっていました。特に複数のサービスが提供され

る場合、ルータの性能が重要な要因となります。先進のPXFスイッチングをベースにしたNSE-1は、並列アーキテクチャとパイプラインアーキテクチャの独自の組み合わせによって構成されています。複数の高速サービスを同時に使用しても、NSE-1の性能にはほとんど影響がありません。NSE-1を活用すれば、特定の領域に応じたマルチサービス(QoS、セキュリティ、アドレス変換など)を同時に使用しても、性能が落ちることはありません。

図 16 : NSE-1 のPXF スwitchングを使ってハードウェアで処理することによって、T-ACL と NAT を同時に実行することが可能



Cisco 7200VXR と NSE-1 アプリケーション

最新のNSE-1を搭載したCisco 7200VXRシリーズルータでは、性能、セキュリティ、安定性、制御能力を備えたCisco IOSの堅牢な機能を、LAN、WAN、IBM環境で利用できるほか、ハードウェアによるサービスの高速度処理にも対応しています。

エンタープライズWANゲートウェイ

エンタープライズWANゲートウェイは、キャンパスとWANを相互接続し、サイト間で、音声、ビデオ、データを高速に交換できます。これには、ATM DS3、ATM OC3、Packet-over-DS3、Packet-over-OC3(SONET/SDH)などの高速WANインターフェ

ス、ファーストイーサネットなどの高速LANインターフェース、そして高性能ネットワークサービスの3つの機能が必要となります。シスコでは、ハードウェアによってサービスを高速処理するCisco 7200VXR用のNSE-1を発表しました。初回出荷時点で、NSE-1は、最も一般的なサービス、特にエンタープライズWANゲートウェイ機能に必要とされるサービスに対して、ハードウェアによる高速処理を実現しています。将来は、さらに多くの高速サービスが提供できる予定です。初回出荷時のPXFプロセッサでは、WFQやWREDなどのQoS機能のほか、NetFlow、T-ACL、NATなどの機能についても高速処理が可能です。

サービスプロバイダーや一般企業に向けた専用アクセス集約接続

POPや企業の中央サイトの集合システムとして機能するCisco 7200VXRを中央に配置することで、複数のサイトを相互に接続できます。新しいマルチチャンネルポートアダプタが開発され、ポートは高密度になり、ポート当たりの価格は安くなります。新しい拡張ATMポートアダプタにより、仮想チャンネルごとのトラフィックシェイピングが拡大され、高速接続が可能になります。他にも、Cisco 7200VXR用の新しいIPOS(Packet over SONET/SDH)ポートアダプタでは、堅牢かつ高速で高スループットのIPトラフィックの転送ができます。専用回線、フレームリレー、ATM、パケットベース転送を使用した専用アクセス接続も可能です。NSE-1の発表により、一般企業やサービスプロバイダーはNSE-1による高性能サービスを活用できるようになりました。NSE-1によって高速処理されるNetFlow、T-ACL、QoS機能などのサービスは、高性能WANの集約要件に合致しています。今後NSE-1は、さらに多くのハードウェアによるサービスの高速処理をサポートする予定です。また、Cisco 7200VXRはモジュラ型で、製品の組み合わせが自由にできるように設計されているため、必要に応じてサイトを追加することが可能です。Cisco 7200VXRはラック3つ分の高さしかないので、取り扱いも簡単です。

マルチサービスVPN

Cisco 7200VXRシリーズルータは、優れた性能、信頼性、機能が1つにまとまった、高性能VPNゲートウェイアプリケーションに適したプラットフォームです。Cisco 7200VXRルータは、L2F(レイヤ2転送機能)、L2TP(レイヤ2トンネル伝送プロトコル)、GRE(一般ルーティングカプセル化)トンネリングなどのトンネリング機能、IPSecやファイアウォールなどのセキュリティ機能を含むCisco IOS VPNサービス、さらには、300KppsのCEFスイッチング性能、選択可能なポートアダプタを備えており、ゲートウェイアプリケーションにとって理想的なソリューションです。

Cisco 7200VXRルータには、PIXスイッチングとISAなどの専用暗号化処理サービスが統合されています。したがって、暗号化、セキュリティ、QoSを含むすべての必要なサービスが業界をリードするVPNソリューションとなっています。

NSE-1を搭載したCisco 7200VXRでは、音声、ビデオ、データ用のVPN(仮想プライベートネットワーク)を構築するのに必要な高性能トンネリング、セキュリティ、QoS機能が利用できます。ユーザー単位またはアプリケーション単位で、セキュリティ、優先順位、ネットワーク帯域幅を動的に割り当てることができます。NSE-1によって実現されたハードウェアによるサービスの高速処理は、マルチサービスVPNを構築しようとしている顧客にとって有益です。

マルチサービス

Cisco 7200シリーズルータでは、フレームリレー、ATM、レイヤ3機能が統合されていて、混合IPトラフィック、フレームのATM変換、回線エミュレーション サービスなど、すべてのサービスを同一のWANリンク上で伝送できます。数多くの次世代マルチサービスソフトウェアとハードウェア機能がCisco 7200シリーズルータに集約されているため、大規模なマルチサービスネットワークの転送ノードとゲートウェイノードの両方として機能することができます。これらの機能は4つの領域で発展しています。

レイヤ2とレイヤ3のQoS

マルチサービス転送

デジタル音声終端

マルチサービストラフィックの柔軟なスイッチング

Cisco 7204 VXRおよびCisco 7206 VXRシステムには、新しいマルチサービス機能MIX(Multiservice Interchange)が含まれています。シスコのオープンマルチサービスアーキテクチャ用に開発されている音声アプリケーションが将来完成すれば、パケットとデジタル音声の領域両方で、シームレスなエンドツーエンドのコール管理が可能になります。MIXを搭載したCisco 7200VXRシリーズルータは、構内にある旧来のPBX(構内交換機)とPSTN(公衆交換電話網)の両方に接続でき、エンタープライズネットワーク上のVoXコールと同様に、PBXからPSTNへのコールに対しても同じコールの制御を実行できます。また、MIXを使用したマルチチャンネルポートアダプタでは、デジタル音声チャンネルとパケットチャンネルをチャンネル化されたアクセスリンクで統合し、アクセスコストを削減できます。ただし、別個のTDM(時分割多重化方式)多重化装置は必要ありません。これにより、チャンネル化されたWANリンクから、PBX、ビデオコーデックその他のTDM指向の装置に接続するインタフェースに128DS0チャンネルを切り替えられます。

Cisco 7200VXRとNSE-1により、リアルタイムの音声やビデオのトラフィックに必要な、ハードウェアにより高速処理されたQoSサービスが可能になります。また、NSE-1はcRTPを高速化し、マルチサービスのスケーラビリティがさらに拡張されます。これらのマルチサービス機能により、企業やサービスプロバイダーは、簡単な管理の下に堅牢で経済性に優れたマルチサービスネットワークに移行できます。

©2000 Cisco Systems, Inc. All rights reserved.

CiscoとCisco Systemsは商標です。CiscoのロゴはCisco Systems, Inc.の登録商標です。

この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。

本仕様は予告なしに変更される場合があります。



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>

E-mail: cnac@cisco.com

〒100-0005 東京都千代田区丸の内3-2-3 富士ビルヂング

TEL.03-5645-8856 FAX.03-5641-3523

お問い合わせ先