

# リアルタイムのトラフィックのサポート ビデオ会議に使用するIPネットワークへの対応

ホワイト ペーパー

ポリコム グローバル  
サービス

2006年1月5日

## 目次

1 .....	概要	3
2 .....	リアルタイムのトラフィック	3
2.1 .....	リアルタイムのトラフィックとは?	3
3 .....	QOS (QUALITY OF SERVICE)とは?	5
3.1 .....	ネットワークのQoSへの実装	6
3.2 .....	分類	12
4 .....	帯域幅の需要	13
5 .....	利用可能な帯域幅	15
6 .....	需要の管理	17
7 .....	WANのベンダおよび技術	18
7.1 .....	WANコアのQoS	18
7.2 .....	WANアクセス リンクにおけるQoS	19
7.3 .....	SLAの解釈	19
7.4 .....	企業ネットワークからWANのQoSへのハンドオフ	20
7.5 .....	VPNやインターネット上でのリアルタイムトラフィック	20
8 .....	ネットワークの検証	20
9 .....	ネットワークの監視	22
10 .....	企業内SLA ( SERVICE LEVEL AGREEMENT )	23
11 .....	チェックリスト	24
12 .....	結論	25
13 .....	付録1	26
14 .....	参考文献	27

## 1.0 概要

VoIP (Voice over IP) およびIPを使用したビデオ会議では、通常のデータ アプリケーションとは大きく異なるリアルタイムのトラフィック ストリームが生成されます。IPネットワークでオーディオ/ビデオ会議を行う場合、この大きく異なる複雑なトラフィックを処理するための準備が必要です。実際、企業のネットワークはビデオ会議のトラフィックを処理するのに十分な機能を備えていない場合も多いため、評価とテストを行って、再構成やアップグレードによって品質を向上させる必要があります。

この文書はオーディオ/ビデオ会議のトラフィックの課題を特定し、企業のネットワークでサポートするための青写真を提供することを目的としています。そのため、帯域幅、パケット ロス、ジッター、待ち時間の処理とQoSの実装の手法、ネットワークの検証およびネットワークの継続的な監視のテスト手法を紹介します。また、最後にIPネットワークのインフラストラクチャでビデオ会議を行う場合の需要を特定して、その管理方法について説明します。

IPネットワークの構成と配置の知識があると、このガイドで説明するIPネットワークの配置の一般的な要素(スイッチング、ルーティング、帯域幅、エラーのメカニズムなど)を理解する上で役立ちます。ただし、この文書では、NAT (Network Address Translating Router) を使用してオーディオ/ビデオ会議のトラフィックを処理する場合の問題やファイアウォールに関連した問題は取り上げません。

## 2.0 リアルタイムのトラフィック

リアルタイムのトラフィックでは双方向のアプリケーションがリアルタイムでサポートされます。その最も一般的な例がオーディオ会議とビデオ会議です。いずれの会議でも接続の両端にいるユーザーの発言や行動が、「瞬時に」接続のもう一方の端のユーザーに送信され、両者が1つの部屋にいるかのように会話が進められます。リアルタイムのトラフィックが複雑化する大きな原因のひとつは速度に対する需要です。通常のデータ ネットワークがこの需要に対応できない理由については後で説明します。

この文書で使用するリアルタイムトラフィックという用語には、VoIP (Voice Over IP) のトラフィックだけでなく、ビデオ会議アプリケーションのビデオとオーディオの両方のストリームも含まれます。

### 2.1 リアルタイムのトラフィックとは

IP (Internet Protocol) は現在のあらゆるネットワークの中核であり、一方の端末を他方のエンドポイントに接続するために使用します。ただし、IPは信頼性を強化するために開発されたプロトコルではありません。つまり、一方の端末から他方の端末にすべてのパケットを確実に送信することを目的としていません。

データ アプリケーションでは送信に信頼性が求められるため、送信先のコンピュータにデータのすべてのビットが確実に送信されることが保証されている必要があります。そのために、一般的なネットワークではIPにTCP ( Transmission Control Protocol ) を組み合わせています ( TCP/IP )。TCPでは送信されるすべてのパケットが確実に受信されることが保証され、送信中に紛失したパケットは再送信されます。また、TCPではアプリケーションに送信する前に、すべてのデータが適切であるか検証されます。

データ アプリケーションはネットワークの帯域幅を集中的に使用します。データのファイルやブロックをネットワーク経由で送信する準備ができたなら、送信元では他の作業をするために、なるべく早くそのデータを送信しようとします。その結果、ネットワークでは短時間にアクティビティが集中し、それが一通り終わると利用が極端に減ります。

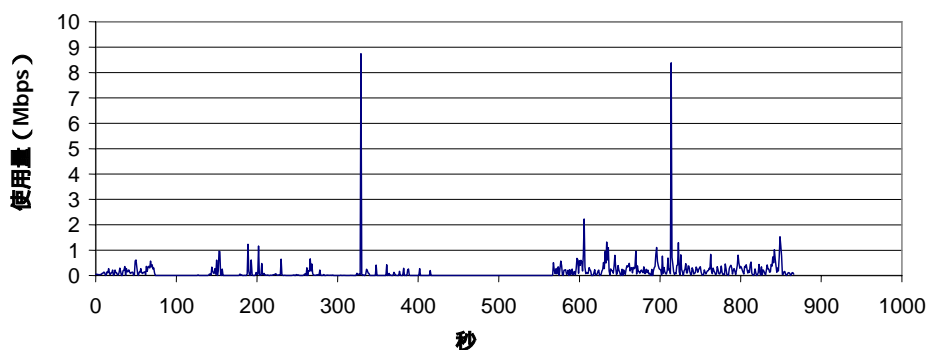


図1 - 代表的なデータによる帯域幅の使用

図1は代表的なデータ アプリケーションをグラフ化し、ネットワークの使用量の多い時間と少ない時間を示しています。

IPベースのネットワークではパケット ロスが発生しますが、これはネットワークの運用では一般的な現象です。実際、TCPプロトコルではパケット ロスはフロー制御のメカニズムとして利用されます。TCPではデータの送信速度を決めるために、パケット ロスが発生するまで送信レートを増加させ、発生したら減少させます。これはネットワークでTCPストリームが生成されるたびに繰り返し行われます。

リアルタイムのトラフィックはまったく異なる特性を持っています。コーデックを使用したリアルタイムのトラフィックでは、実際の連続した環境 ( オーディオまたは画像 ) がサンプリングされ、その一定の更新情報が送信されて、オーディオまたは画像として再生されます。そのため、アプリケーションの実行中、オーディオとビデオには一定の帯域幅が使用されます。図2では384Kのビデオ会議をグラフ化して、オーディオとビデオの2つのストリームとその比較的安定した帯域幅の利用を示しています。

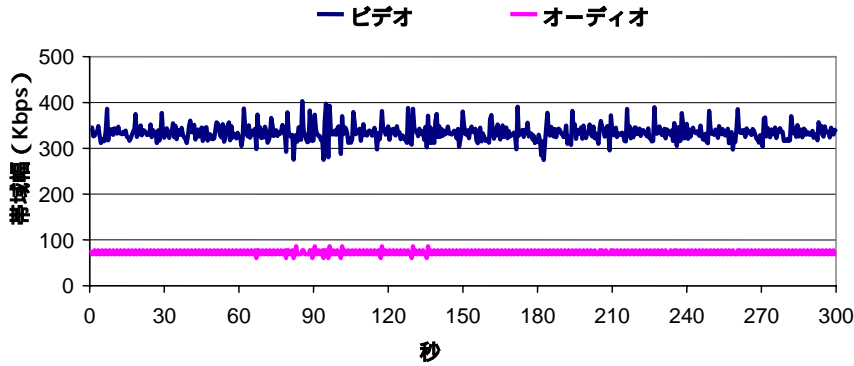


図2 - ビデオ会議における帯域幅の使用

リアルタイムのストリームのもうひとつの特徴は、遅延に対する感度です。リアルタイムのストリームではスピーチなどの連続したイベントがサンプリングされて再生されるため、個々のデータ サンプルは送信先に正しい時間に到着して「再生」される必要があります。パケットの到着が遅れたり送信中に紛失すると、プレーヤーで再生される情報にギャップが生じ、再生されるオーディオやビデオの品質が低下します。この品質の深刻な低下は比較的低レベルのパケット遅延やパケットロスでも発生します。

リアルタイムのパケットは適時に到着している必要があるため、紛失したパケットの再送信をトランスポートプロトコルで依頼して、送信元が再送信するのを待つというわけにはいきません。送信元から再送信までの往復の遅延が大きすぎるため、そのパケットは再生されません。TCPではこのようなストリームに値が追加されないため、代わりにUDP (User Datagram Protocol) で送信されますが、UDPには復旧のメカニズムがありません。送信元からネットワークに送信されたパケットは受信元に時間通りに到着するとは限らず、遅れて到着したり、送信中に紛失したりすることもあります。

そのため、オーディオ/ビデオ会議に関連するパケットがネットワーク経由で適時に送信されることを保証し、送信プロトコルに依存せずに紛失を防止する方法が必要になります。これがリアルタイムのアプリケーションをサポートするときの課題です。QoS (Quality of Service) はオーディオとビデオのストリームに優先順位を付け、正しく送信するためにネットワークに配置するメカニズムです。この文書ではQoSのさまざまなアプローチを取り上げて、オーディオとビデオのためのQoSの実装方法について説明します。

### 3.0 QoS (Quality of Service) とは

QoSという用語はネットワーク環境において、数種類のトラフィックに対するサービスを向上させるさまざまな方法を説明するときに使用されます。その方法には優先順位付きのキューイング、アプリケーション固有のルーティング、帯域幅管理、トラフィックシェーピングなどがあります。ここでは、最も広く実装されているQoSのアプローチとして、優先順位付きのキューイングについて説明します。ただし、利用できるアプローチは優先順位付きキューイングだけではありません。適時にパケットを送信できる信頼性の高いアプローチであれば、オーディオ会議やビデオ会議をサポートできます。ここでは、最も広く利用されているQoSとして優先順位付きキューイングを取り上げて、その機能とオーディオ/ビデオ会議に最適な構成方法について説明します。

QoSをネットワークで有効にすることは問題の一部に過ぎません。ネットワークでQoSを正しく機能させるには、次の4つのステップがあります。

- ネットワークへの QoS の実装
- 分類
- 帯域幅の需要と帯域幅の可用性
- 帯域幅の管理

キューはネットワークにおけるパケット ロスや遅延の主な原因です。ネットワークのルータの各出力ポートとスイッチにはキューがあり、パケットは通過する各デバイスの出力キューに挿入されて出力されます。キューが空または空に近い状態にある場合、パケットは挿入された直後に出力リンクに転送されます。

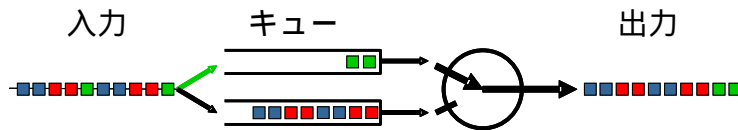


図3 - パケットのキューの図解

トラフィックが一時的に混雑してキューが一杯になると、先にキューに挿入されたすべてのパケットが出力リンクに送信されるまで後続のパケットが待機するため、遅延が発生します。一時的にトラフィックが集中してキューが一杯になると、パケットの廃棄や紛失が起こります。

優先順位付きのキューイングのメカニズムでは、各スイッチまたはルータの出力ポートに優先順位の高いトラフィック専用のキューが追加されます。図3は単純な2つのキューを持つ出力ポートを示しています。ベスト エフォートではすべてのトラフィックが下のキューに挿入され、優先順位の高いトラフィック(図中の緑色部分)は上のキューに挿入されます。両方のキューに待機しているパケットがある場合、キューを空にする方法はキューのポリシーによって決まります。

単純な優先順位付きのキューは低遅延キューとも呼ばれ、優先順位の低いキューを送信する前に必ず空になります。そのため図3では、キューのポリシーが単純な優先順位である場合、2つの緑色のパケットが最初に処理されてから、ベスト エフォートのキューにある残りのパケットが処理されます。下のキューを空にしているときに優先順位の高いパケットが追加されると、優先順位の高いキューに瞬時に切り替えられて処理が行われます。

レートベースのキューの処理は少し異なります。レートベースのポリシーでは、各キューに割り当てられた帯域幅に基づいてキューが空になります。利用できる帯域幅の40%をキュー1に、60%をキュー2に割り当てた場合、キュー2はキュー1と比べて6/4倍の頻度で処理されます。レートベースのポリシーを使用すると、キューは十分な頻度で処理されるため、割り当てられたフローはキュー内を迅速に移動しますが、トラフィックの量が過剰になると、そのキューの処理が停止して、もう一方のキューが優先されます。図3の例では、緑色のパケットが必ずしも最初に出力されるとは限りません。これはキューに割り当てられた帯域幅と各キューで空にしたトラフィックの量によって決まります。

### 3.1 ネットワークへのQoSの実装

ネットワークではQoSのメカニズムによって、各スイッチとルータでリアルタイムのトラフィックの優先順位を決定する必要があります。ネットワークには現在、IntServ( RSVP )、DiffServ、IEEE 802.1p/Q、IP Precedenceをはじめ、さまざまなメカニズムがあります。また、オーバー プロビジョニングを使

用する企業もありますが、オーバー プロビジョニングではQoSのメカニズムを利用する代わりに十分な帯域幅を確保します。この手法の危険性については後で説明します。

QoSのメリットを最大化するためにはエンド ツー エンドで適用します。リアルタイムの送信元と受信元の間にあるすべてのルータとスイッチでQoSのメカニズムを利用します。リンクでのパケットロスや遅延を防止するために部分的なソリューションを利用しても、送信の品質を確保するには、すべてのリンクにQoSを適用する必要があります。

オーディオ/ビデオ会議のトラフィックをサポートするのに最適なQoSのメカニズムを決定するため、次に例を挙げて説明します。

## オーバー プロビジョニング

上記では、キューが空または空に近い状態になったとき、後続のパケットの送信には遅延が発生しないと説明しました。オーバー プロビジョニングではこの原則を利用して、リンクの帯域幅を必要以上に多くすることで、キューを常時空の状態にします。高帯域幅の構内リンクでビデオ会議のテストを行うと、QoSを追加実装しなくても好結果が得られますが、残念ながら、これは近視眼的なアプローチに過ぎず、後で問題が発生することになります。

適切なQoSのメカニズムを使用しないでリアルタイムのトラフィックを処理するのは危険な賭けです。データ アプリケーションにおける処理の集中化についてはすでに説明しましたが、データ アプリケーションのユニークな特徴は、多くのアプリケーションが統合されていると、処理のピークが分散されるような気がすることです。実際にはまったく逆で、データ トラフィックは統合レベルやタイム スケールが異なっても、その集中化の傾向が変わることはありません。そのため、バックボーンのリンクが1ギガビットであろうとも10ギガビットであろうとも、データ トラフィックの大規模な集中は、いつ発生してもおかしくありません。処理が集中すると、オーディオ/ビデオ会議のストリームに遅延やパケットロスが発生します。データ トラフィックは営業時間中に集中することが多く、オーディオ/ビデオ会議が行われる時間帯と重複します。そのため、パケットロスの発生する可能性はますます高くなります。

## 第2層および第3層のQoS

QoSはプロトコル スタックの第3層と第2層の両方に実装します。第3層のQoSはネットワークのルータで認識および処理されます。ただし、スイッチの出力キューが過密状態になると第2層のQoSも必要になります。WANネットワークはルータ間が長いリンクで接続される構造のため、これには当てはまりません。ただし、エンタープライズ ネットワークでは多くの場合、第2層と第3層の両方にQoSを実装する必要があります。

## 第3層のQoS

第3層にQoSを実装する場合、多くのネットワークではIntServ (RSVP)、DiffServおよびIP Precedenceの3種類のアプローチが利用されます。これらのアプローチを比較してみましょう。

IntServ (Integrated Services) は、処理が集中するIPネットワークで優先順位の高いトラフィックを適切に処理するため、QoSの包括的なアプローチとしてIETFによって定義されました。IntServではRSVPプロトコルを使用して、特定のリアルタイム ストリームのパスにあるすべてのルータにリクエストを送信し、優先順位付きのキューと一定の帯域幅の使用の許可を求めます。各ルータでリソースが利用可能であると確認されるとパスが有効になり、ストリームがそのパスで優先されます。IntServはすべてのルータでRSVPプロトコルがサポートされ、リアルタイムのストリームの数量に制限のある環境では効果的です。

**表1 - DiffServとイーサネットIEEE 802.1pの優先順位の対応**

DiffServコード ポイント (DSCP)	PPP クラス番号
CS7, CS6	7
EF, CS5	6
AF4x, CS4	5
AF3x, CS3	4
AF2x, CS2	3
AF1x, CS1	2
DE, CS0	0

参考資料：『Introduction to Quality of Service (QoS)』（Nortel 社 ホワイトペーパー）

トラフィックに対する帯域幅が制限されていても、そのクラスの帯域幅の需要が管理されずに、トラフィックの処理だけが行われる点にあります。そのため、DiffServではネットワークによる処理を簡略化できますが、帯域幅の管理の問題がアプリケーションの問題に入れ替わるだけです。帯域幅の管理の詳細については、この文書の後半で説明します。

**IP Precedence**は本来、IPの仕様から開発された手法です。そのメカニズムは優先順位の高いマーキングのIPパケットを優先させるだけの非常に単純なものです。IP PrecedenceとTOS (Type of Service) で使用されていたIPヘッダのビットの位置は、DiffServでは再定義されます。DiffServを標準でサポートしていないルータ以外では、DiffServの代わりにIP Precedenceを使用するメリットはありません。

WAN (広域通信網) のベンダの多くは現在、ネットワークのQoS管理にDiffServのマーキングを使用しています。WANネットワークもオーディオ/ビデオ会議を利用する企業のネットワークの一部であるため、構内と広域の両方のネットワークで一貫して利用できるアプローチを選択すると効果的です。DiffServのマーキングを慎重に選択することで、構内ネットワークとWANベンダの両方でオーディオ/ビデオ会議のストリームを適切なポリシーで処理できます。

## 第2層のQoS

第2層のQoSで現在主流の規格はIEEE 802.1pです。過去7年間に販売されたスイッチの大半にこの機能が組み込まれています。IEEE 802.1pの機能は、VLANの機能を定めたIEEE 802.1Qと連携しています。いずれの規格も同じビットフィールドをイーサネットのヘッダに追加して、ストリームの優先順位とVLANとの関係を指定します。

IEEE 802.1p対応のスイッチでは、各スイッチの出力ポートに複数の出力キューがあります。優先順位の高いトラフィックは優先順位の上位のキューに割り当てられ、前のルータの説明と同様に、優先順位の下のキューより先に処理されます。

表1では、イーサネットIEEE 802.1pの優先順位とDiffServのコードポイントの対応を示しています。802.1pを使用している構内ネットワークで、第3層のQoSがコアルータやWANルータなどの第2層のQoSと一致する場合、この変換が必要になります。

VLANは、トラフィックを割り当てることでトラフィックがネットワークから完全に独立し、そのた

RSVPではアクティブなリアルタイムのストリームに関する情報を各ルータで管理する必要があるため、ネットワーク設計者であれば、すぐに拡張性が不十分であることに気づくはずですが。各ルータで消費されるリソースが多すぎます。現在、IntServを導入している企業はほとんどありません。

**DiffServ** (Differentiated Services) は拡張性を向上させたもうひとつのアプローチとして開発されました。DiffServでは個々のリアルタイムストリームに対してリソースを指定する代わりに、トラフィックのクラスに対してリソースを割り当てます。同じクラスに割り当てられたすべてのトラフィックは同じポリシーで処理(優先順位の高いキューに挿入されるなど)されます。主な違いは、ネットワークでは優先順位の高いクラスのトラ

めにオーディオとビデオのトラフィックに適したソリューションであると一般的に誤解されています。VLANの割り当ては、VLANに許可されていないネットワークの一部にトラフィックが転送されるのを防止するため、許可という観点からトラフィックが独立しているに過ぎません。ただし、優先順位の割り当ては独立して行われます。VLANの割り当てと優先順位の割り当ては多くの場合、連携しています（Red VLANには優先順位の高いトラフィックが割り当てられるなど）。これがすべてに該当するならば、優先順位の高いVLANのトラフィックはスイッチでも優先的に処理されるはずですが、この2つの割り当て（VLANと優先順位）は必ずしも連携しているわけではありません。複数の「優先順位の高い」VLANが同じスイッチを通過する場合、それらは同じ出力キューのリソースをめぐる競争をします。

VLANはトラフィックにマーキングするために使用されることもあります。端末でトラフィックにマーキングできない場合、または、トラフィックに正しくマーキングできない可能性がある場合、VLANの割り当てを使用して、優先順位の高いトラフィックであることを示します。VLANは指定された物理ポートで受信したトラフィックへの割り当てが可能のため、室内ビデオ会議システムなど、指定されたシステムから受信したトラフィックを指定されたVLANに割り当てることで、ネットワークでの優先順位を指定できます。これについては、セクション3.2で詳しく説明します。

## WANのQoS

WAN（広域通信網）にはさまざまな技術があり、それぞれQoSのアプローチが異なります。ここでは専用線、フレームリレー、ATMおよびMPLSについて説明します。

表2 - DiffServとPPPの優先順位の対応

DiffServコード ポイント (DSCP)	PPP クラス番号
EF	7
CS7, CS6, CS5	6
AF4x, CS4	5
AF3x, CS3	4
AF2x, CS2	3
AF1x, CS1	2
DE, CS0	1

参考資料：『Introduction to Quality of Service (QoS)』（Nortel社 ホワイトペーパー）

専用線はQoSの観点では最も管理が簡単な技術ですが、トポロジやコストの点では必ずしも最良の選択肢ではありません。企業が2つの施設間でT1回路またはT3回路をリースしている場合、WAN接続のトラフィックのスケジュールはその企業の両側のルータで完全に制御され、リンクはその企業のネットワークにある他のリンクと同様に機能します。このような企業のネットワークでは、選択したQoSのアプローチはWANリンクにも使用できます。

表2では、DiffServコードポイントとPPPのクラス番号の対応を示しています。この対応はエンドツーエンドのリンクの両側に接続したルータで行います。

フレームリレーは実績のある技術で、比較的低い帯域幅での接続を必要とする企業に多く利用されています。フレームリレーサービスを使用してリアルタイムのトラフィックを送信する場合、ジッターを十分に抑えることがむずかしい場合があるため注意が必要です。また通常、ジッターが適切なリアルタイムの転送に必要な値の範囲内であることは保証されません。

フレームリレーでは、特定のトラフィックタイプを他のトラフィックより優先する、さまざまなクラスのサービスを利用できます。これらのサービスクラスはTelnetやCitrixなど、相互に作用するアプリケーションを電子メールの送信やファイルのバックアップよりも優先させる場合には効果的です。ただし、リアルタイムのトラフィックに必要な優先順位付けは行われません。また、フレームリレーサービスでは複数のPVCで同じ物理接続を使用するため、優先順位付けのキューで正しい順位付けをすることは困難です。ルータを複数のPVCに使用する場合、各PVCに対して仮想ポートが作成され、それぞれに優先順位の高いキューとベストエフォートのキューが作成されます。ただし、同じ物理ポートを使用する2つの仮想ポート間で通信は行われません。そのため、優先順位の高いトラ

フィックが仮想ポートの一方のキューに挿入されても、他方の仮想ポートのベスト エフォートのキューにあるトラフィックより優先されることはありません。つまり、本当の意味での優先順位のキューイングが行われていないことになり、オーディオ/ビデオが断続的になる問題が発生します。

**ATM（非同期転送モード）**は1990年代に広域通信網のベンダが大規模に配置した技術です。ATMには高度なQoSメカニズムが組み込まれ、トラフィックが的確に分離されます。

ATMの導入初期にはATMフォーラムによって、帯域幅のフローの測定およびポリシーの設定に関する多くの技術が開発されました。これらの技術は現在、DiffServおよびMPLSの実装にも使用されています。

**表3 - DiffServとATM QoSの対応**

DiffServコード ポイント (DSCP)	ATMの サービスの分類
CS7, CS6, CS5, EF	CBR or rt-VBR
AF4x, CS4, AF3x, CS3	rt-VBR
AF2x, CS2, AF1x, CS1	nrt-VBR
DE, CS0	UBR

参考資料：『Introduction to Quality of Service (QoS)』（Nortel社 ホワイトペーパー）

ATMのサービスの分類はDiffServの分類とは異なりますが、DiffServの分類はネットワークの境界でATMの分類にマッピングできます。表3はDiffServのコードポイントとATMのサービスカテゴリの対応を示しています。

ATMを社内で使用している企業は、このQoSのメカニズムも使用できます。大規模企業では主要なサイト間

にATMバックボーンを構築しています。ATMのQoSではこのリストの上位のクラスが優先されます。

**MPLS（マルチプロトコルラベルスイッチング）**は最新のWAN技術で、WANのサービスプロバイダの多くが導入済みまたは導入を予定しています。MPLSはサービスプロバイダがネットワークのトラフィックの制御に利用できるATMのさまざまな特性を備えています。そのため、プロバイダは柔軟にサービスを提供でき、異なるサービスに対する新しい市場需要にも短期間で対応できます。MPLSの柔軟性により、多くのプロバイダが品質の保証されたサービスを提供しています。また、これはMPLSがQoSと誤解される原因にもなっていますが、実際にはそうではありません。サービスプロバイダの多くがMPLSをベース優れたQoSを構築していますが、リアルタイムのトラフィックを正しく処理するには、そのQoSの詳細を理解する必要があります。

MPLSを使用しているサービスプロバイダはルータを設定してMPLSタグの内容を認識させるか、個々のラベルによって特定のルートを優先させることでクラスの異なるサービスを提供しています。いずれの方法でもクラスの数は通常8個以下に固定されています。そのため、ここでもDiffServのマーキングとMPLSのコアによる指定されたトラフィックのクラスをマッピングする必要があります。MPLSベースのWANのプロバイダは多くの場合、DiffServを使用してトラフィックのクラスを特定しています。ご検討中のMPLSネットワークのベンダーと話し合い、そのベンダーがサポートするトラフィックのクラスに対し、異なるDiffServのマーキングをマップしてサポートする方法を把握します。

### 推奨 – DiffServのマーキング

IETFのワーキンググループが特定のタイプのトラフィックに対して推奨されるDiffServのマーキングの原案を発表しました。

推奨内容は表4のとおりです。この原案はWANベンダ間で一貫性を確保して、複数のWANプロバイダ全体でQoSを実現し、転送動作を統一することを目的としています。IETFの推奨に従ってこれらのマーキングを利用すると、企業とWANベンダの間に互換性が成立します。

表4 - IETFが推奨するDSCPのマーキング

サービスクラス	DSCP	使用するPHB	キューイング	AQM
ネットワーク制御	CS6	RFC2474	レート	はい
電話	EF	RFC3246	優先順位	いいえ
信号	CS5	RFC2474	レート	いいえ
マルチメディア会議	AF41 AF42 AF43	RFC2597	レート	はい (DSCP)
マルチメディアストリーミング	AF31 AF32 AF33	RFC2597	レート	はい (DSCP)
OAM	CS2	RFC2474	レート	はい
スループットの高いデータ	AF11 AF12 AF13	RFC2597	レート	はい (DSCP)
優先順位の低いデータ	CS1	RFC3662	レート	はい
標準	DF (CS0) +その他	RFC2474	レート	はい

参照用インターネット原案 (draft-ietf-tsvwg-diffserv-service-classes-02)

EF (Expedited Forwarding) は優先順位付きのキューで実行される電話への使用を推奨します。前に述べたように、優先順位付きのキューはトラフィックの待ち時間を最小化するために、他のキューより先に空になります。また、ビデオ会議にはレートベースのキューで実行される、優先順位の高いAF (Assured Forwarding) マーキングの使用を推奨します。このマーキングを使用すると、帯域幅が高く、パケットサイズの大きいビデオ会議のストリームよりオーディオトラフィックが優先されるため、トラフィックが集中するネットワークでオーディオ会議とビデオ会議の両方を実行する場合に適しています。レートベースのキューでは、キューのレートがビデオ会議ストリームで生成されるトラフィックの量の最低値を上回るよう設定すると、ビデオ会議のトラフィックが適切に転送されます。この帯域幅を管理することは非常に重要なので、後で詳しく説明します。

ビデオ会議のストリームのオーディオ部分とビデオ部分の分離にはさまざまな推奨事項があります。ビデオ会議のオーディオ部分をビデオ部分より先に送信することに意味はないとされる場合がありますが、これは受信側のユニットでオーディオを遅らせてビデオ信号に同期させる必要があるためです。ただし、オーディオを優先することで他のストリームへの干渉が抑制できれば、送信の信頼性も向上します。ビデオ会議の画像が低品質であっても、オーディオがクリアであれば進行に問題はありませんが、オーディオが低品質では会議になりません。

ネットワークでビデオ会議のみにリアルタイムのトラフィックを使用している場合、ビデオ会議のストリームにEF (Expedited Forwarding) を使用できます。ただし、VoIPに移行したり、将来的な移行を検討している企業も多いため、ビデオにEFを使用するのは長期的な戦略には適していません。

#### AQM (Active Queue Management)

表4の最後の列には推奨されるAQM (Active Queue Management) を示しています。電話の欄では「いいえ」になっています。AQMの主流となるメカニズムはRED (Random Early Discard) です。このア

表4にはEFマーキングを使用した電話 (VoIP) とAF41、AF42またはAF43のマーキングを使用したビデオ会議を示しています。電話の信号はCS5のマーキングを使用してこの2つの間に挿入されます。ビデオ会議の信号は直接呼び出されません。ビデオとオーディオのストリームのレベルを下回る必要がありますが、ユーザーは信号のトランザクションの結果を待っているため「標準」とはみなされません (ベストエフォートとみなされます)。「スループットの高いデータ」の分類 (AF11、AF12またはAF13) はビデオ会議の信号に適しています。

表4の3番目と4番目の列には推奨される転送動作を示しています。詳細は該当するIETFの仕様を参照してください。

ルゴリズムはリンクが過密状態に近づいたときに、複数のTCPのフロー制御をサポートすることを目的としています。REDでキューが長くなることが予測されると、キューから無作為にパケットが選択されて廃棄されます。TCPのストリームでパケットロスが発生すると、送信速度が減速して集中化が緩和されます。

前に述べたように、パケットロスが発生するとリアルタイムのストリームの品質が低下するため、パケットロスを発生させることはメリットにはなりません。表4では、IETFはAQMをビデオ会議のストリームに使用することを推奨していますが、これは、パケットロスが発生したときにビデオ会議の端末で送信速度を減速できることを前提としています。この機能があれば、パケットロスを検知したときにビデオ会議のストリームでビデオのレートを低い帯域幅に変更し、それによってネットワークの集中化が緩和されて、すべてのストリームのパフォーマンスを再度向上させることができます。

アプローチが優れていれば、そもそもこのような状態にはなりません。主に会議室のビデオ会議システムでビデオ会議の帯域幅を使用する環境では、帯域幅の予測と同意、スケジュール設定が必要です。端末のネゴシエーションで帯域幅を削減すると、ビデオ会議の品質が一時的に干渉され、品質が低下します。これではビジネスのためのビデオ会議環境として利用できません。

今後、デスクトップのビデオ会議機能を臨時のビデオ会議に利用する機会が増えることを考えると、ビデオ会議のトラフィックを2つのクラスに分けて、それぞれの帯域幅を個別に管理することが必要になります。臨時のビデオ会議を利用するユーザーの管理はオーディオ通話と同様、平均化して行います。ビデオ電話をサポートする十分な帯域幅が確保できない場合、ネットワークの混雑時や話中信号を受信したときに、平均化したユーザーのグループのビデオ品質を低下させます。このような臨時で利用されるクラスとは別に、正式なビデオ会議にはスケジュールどおりの帯域幅を使用して、品質の一貫性を確保します。

## 3.2 分類

分類とは、処理の優先順位の高いストリームを判断する作業です。マーキングによってストリームを識別し、ネットワークを切り替えて、ルータで認識します。前述のQoSの実装に関する説明はすべて、優先的に処理されるストリームとベストエフォートのストリームを識別できることを前提にしています。分類ではこのような決定を行ってから、ストリームにマーキングします。

### 端末による分類

多くの場合、端末（電話、ビデオ会議の端末、ゲートウェイまたはブリッジ）でオーディオとビデオのストリームを識別できます。端末ではアプリケーションがインストールされ、利用されているため、ネットワークの中でも最も情報の多い構成要素です。端末ではオーディオやビデオを含むストリーム、データの転送やトラフィックを制御するストリームを簡単に識別できます。また、オーディオとビデオの端末の大半には設定オプションがあり、QoSのマーキングを指定して、優先順位の高いストリームに適用できます。

ただし、端末でのストリームのマーキングがネットワークで信頼されるとは限りません。ビデオ会議システムではオーディオ、ビデオ、データ、制御の別でトラフィックが正しく識別されても、PCでは同じマーキングを優先順位の低いトラフィックに適用して、便利に利用される可能性があります。これでは、相乗りレーンをたった1人で運転しているようなものです。

### ネットワークによる分類

ネットワークではデータ ストリーム自体を分類することで、この問題を回避します。つまり、エッジのスイッチやルータでデータ ストリームのパケットを読み取って、優先順位の高低を識別してマーキングします。ネットワークではこの分類はエッジ/アクセス ルータで行われ、配布用、コアおよびWANのルータではエッジのマーキングが使用されます。分類は次を基準に行われます。

- IP アドレス (一般的な端末)
- TCP または UDP のポート番号
- 物理ポート

これらのパラメータは組み合わせて使用されることが多く、端末によるマーキングと連携させる場合もあります。たとえば、ビデオ/オーディオブリッジは統計的に割り当てられたIPアドレスで識別され、UDPベースのトラフィックはすべて優先順位の高いトラフィックとしてマーキングされます。スプーフィングの対象になりにくい一般的なIPアドレスの端末からリアルタイムのトラフィック ストリームが送信されるため、この分類方法は効果的です。それに対して、デスクトップのIP電話やビデオの端末が全社的に設置されている場合、「承認済みの」優先順位の高いデバイスの最新の一覧を作成してこの分類方法を適用するのは困難です。その場合、企業の部門ごとに端末で独自のトラフィックの分類を行って、異なる信頼レベルで運用します。

### 企業の分類ポリシー

企業には分類方法に関するポリシーが必要です。このポリシーは電話やビデオの端末の増設に合わせて拡張します。また、ネットワークの統合性を妥協せずに、リアルタイムのストリームを信頼性の高い方法で識別するためにもポリシーを使用します。優先順位の高いサービスを利用するユーザーの管理については、次の帯域幅のセクションで詳しく説明します。

端末の分類を使用しないデフォルト設定のルータでは、受信したパケットはベスト エフォートとして分類されます。システムのQoSと端末のマーキングを有効にするだけでは不十分な場合がほとんどです。エッジ ルータで、端末のマーキングを使用するか、ルータでパケットを分類してマーキングするか、いずれかを設定します。受信元でデータをキャプチャして、ネットワークを通過するときにパケットからQoSのマーキングが紛失していないか確認すると効果的です。

## 4.0 帯域幅の需要

帯域幅の使用はQoSに含まれます。予想したリアルタイムのトラフィックを確保するには、各リンクに十分な帯域幅が必要です。では、予想したトラフィックとは何でしょうか。予想される需要を分析して、ネットワークの各リンクでビデオ会議をサポートするのに必要な帯域幅を計画的に確保することは重要です。

帯域幅の需要の分析にはさまざまな方法があります。ビデオ会議のサービスがすでに組織に導入されている場合、1日の通話数、発信先、通話時間および通話の帯域幅などの履歴を利用できます。この情報を使用してリンクごとの需要をグラフ化することで、最大値を算出できます。図4はその分析の一例です。ビデオ会議通話のネットワーク図を作成して、各通話で使用されるWANのリンクを特定します。また、通話の時間帯、所要時間および帯域幅を記入します。毎日30分おきに各リンクの通話ごとに使用される帯域幅を集計し、その時間帯に各リンクに必要な帯域幅の合計を算出します。図4では、あるWANリンクの集計を示しています。このリンクはビデオ会議に最大6.5Mbpsを使用します。

現在ビデオ会議にISDN回線を使用している企業でも、同じように通話履歴を使用して、IPネットワークを代わりに使用した場合のIPネットワークの需要を判断できます。

通話に関する情報がない場合、通話の頻度とパターンは使用予測に基づいて算出する必要があります。ビデオ会議が基本的にビデオ会議室で行われる場合、会議室の利用に関する仮定から需要を算出できます。通話先は業務に精通して、ユーザーの通話パターンを推測できる社員に計算してもらいます。

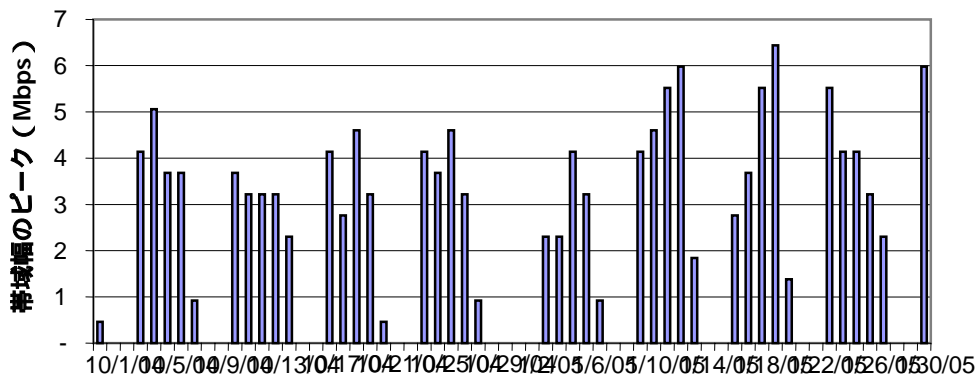


図4 - ビデオ会議における帯域幅の需要

ビデオ会議は通常、予定された会議で使用され、所要時間は最低30分ですが、1時間から1時間半に及ぶこともあります。デスクトップのビデオ会議システムを大規模に導入すると、このパターンも変化します。ユーザーがビデオシステムを電話のように利用して任意の時間に臨時に会議を行う機会が増え、所要時間も短くなります。電話のモデルはアーラン分布の統計に基づいて使用します。通話の頻度と所要時間が確認できている場合、アーランを使用して利用可能な帯域幅の量を計算し、必要な一定レベルの帯域幅を確保して、通話の妨害を回避します。アーラン分布および計算の詳細については[www.erlang.com](http://www.erlang.com)を参照してください。

### ブリッジ (MCU) の帯域幅の需要

ビデオ会議システムのインフラストラクチャの主要な構成要素には特別な配慮が必要です。たとえば、ビデオ会議のブリッジ (MCU) です。ビデオ会議用の20台の端末で会議電話を使用している場合、20台の端末すべてがブリッジにフル デュプレックスで接続しています。ブリッジのネットワーク接続は最大数の端末がすべて同時に会議通話を行なった場合をサポートする必要があります。そのため、ブリッジは帯域幅が十分にあるネットワークのコア付近に設置します。また、ブリッジは会議通話を利用するユーザー数の最も多い施設に設置して、会議通話をサポートするのに必要なWANのトラフィックを最小限にします。

接続したブリッジと各クライアント間では、そのビデオ会議に対して決められた帯域幅でトラフィックストリームが伝送されます。通話の帯域幅が384Kと決められたクライアントが20台ある場合、ブリッジは384K X 20台、つまり7.7Mbpsのトラフィックをサポートすることになります。IPパケットのオーバーヘッドに必要な帯域幅として20%を追加した場合、9.2Mbpsになります。

ビデオ会議の端末にはビルトインの会議モードをサポートするものもあります。小規模な会議でビデオ会議の端末をブリッジとして使用する場合、そのクライアントに合わせて帯域幅を増やします。4人の会議で4台のクライアントのうち1台をブリッジとして使用する場合、ブリッジとして使用するクライアントは3つのフルデュプレックスのストリームを生成します。他の3台のクライアントには単一のフルデュプレックスストリームが送信されます。

### ゲートウェイの帯域幅の需要

ゲートウェイは通常、IPベースのオーディオ/ビデオシステムをPSTNに接続して使用します。通話はISDNまたはPOTS接続へのゲートウェイを通過してIPインフラストラクチャのパス内に配置されません。ゲートウェイはスタンドアロンのユニットとして、またはブリッジに組み込んで使用できます。

ゲートウェイの帯域幅の需要は、ゲートウェイからPSTNに同時に送信される通話数をベースに計算します。PSTNは帯域幅の量が制限されているため、この計算は簡単です。ゲートウェイがブリッジに組み込まれている場合、この帯域幅を会議用の帯域幅に追加する必要があります

### IPおよびATMのオーバーヘッド

帯域幅の計算にはIPベースの通信のオーバーヘッドを考慮する必要があります。ISDN環境では、384Kbpsでビデオ会議通話を行う場合、利用できる帯域幅のうち384Kbpsを消費します。P環境では同じ384Kbpsのストリームは複数のパケットに分散されるため、RTPヘッダ、UDPヘッダ、IPヘッダおよび第2層の通信ヘッダのオーバーヘッドが追加されます。実際のIPネットワークへの影響を判断するには、このオーバーヘッドを各通話の帯域幅に追加する必要があります。帯域幅のオーバーヘッドは表5の値を使用して概算できます。低帯域幅でのG.729などのVoIP通話では、この表のオーディオの値より高くなります。WANリンクで送信される低帯域幅のオーディオ通話数が多い場合、オーバーヘッドを最小化するためにヘッダの圧縮を考慮します。

表5 - IP帯域幅のオーバーヘッド

タイプ	イーサネット/ MPLS	PPP	ATM
オーディオ G.711	36%	25%	40%
ビデオ	20%	18%	25%

表5のビデオはビデオ会議におけるビデオとオーディオのストリームのオーバーヘッドの合計です。たとえば、384Kのビデオ会議では $384\text{Kbps} \times 1.2 = 460\text{Kbps}$ のネットワーク帯域幅を使用します。

## 5.0 利用可能な帯域幅

帯域幅の需要を計算したら、新しいリアルタイムの負荷をサポートするのに十分なリソースがあるか確認するため、既存のネットワークの帯域幅と利用状況を評価します。ネットワークの各リンクには予想されるオーディオとビデオのトラフィックだけでなく、同じ接続を使用する既存のデータアプリケーションをサポートするのに十分な帯域幅が必要です。

これは複雑な作業のように見えますが、実際にはWAN接続、ブリッジのバックボーン接続、10Mbpsイーサネットまたは共有のイーサネット接続によるクライアントの接続を評価するだけです。企業のインフラストラクチャの大半は帯域幅を詳細に分析する必要がないため、これらの主要な要素のみを分析します。

クライアントの接続は可能であれば、すべて100Mbpsのフルデュプレックスにアップグレードします。ビデオ会議の端末でフルデュプレックスの運用をサポートしていない場合、100Mbpsのハーフ

デュプレックスの使用を推奨します。端末でフルデュプレックスがサポートされ、100Mbpsがサポートされない場合、10Mbpsのフルデュプレックスの使用を推奨します。ハブを利用した旧式のイーサネット接続など、ハーフデュプレックスのリンクをビデオ会議に使用する場合、ビデオ会議用のアプリケーションでは利用できる帯域幅の使用量が増加します。10Mbpsのフルデュプレックスのイーサネット接続では、クライアントとネットワークの間で10Mbpsが、ネットワークスイッチとクライアント間でさらに10Mbpsがサポートされます。クライアントを384Kで接続すると各方向に460Kbps、利用できる帯域幅の4.6%が使用されます。同じクライアントをハーフデュプレックスのイーサネットで接続すると、利用できる帯域幅の9.2%が使用されます。

WAN接続を評価する場合、2つの条件を考慮する必要があります。ひとつは、予測されるオーディオとビデオ（リアルタイム）の負荷がリンクの容量の35%を超えないことです。優先順位をベースとしたQoSのメカニズムでは、このレベルで効率が低下します。優先順位の高いトラフィックが35%を超えると、トラフィック内で競合が起こり、通信の信頼性が損なわれます。もうひとつの条件は、リアルタイムのコンポーネントとデータのコンポーネントを含めたリンクの帯域幅における利用率の合計です。データアプリケーションの帯域幅の需要を判断するのは、リアルタイムのアプリケーションほど簡単ではありません。セクション0で説明したように、データアプリケーションは処理が集中化する傾向があり、データアプリケーションが1つのリンクに統合されると、集中化はさらに加速します。データアプリケーションのパフォーマンスは帯域幅のオーバーヘッドに依存します。リンクの帯域幅がデータアプリケーションの平均的な使用量に制限されている場合、アプリケーション自体の処理速度が低下するため、ユーザーの不満が高まり、生産性が低下します。

既存のデータアプリケーションの使用量を判断するひとつの方法として、1日のうちで利用の多い時間帯の使用状況の測定があります。重要なリンクの利用状況を可能な限り詳細に測定します。代表的な帯域幅監視ツールでは、一定時間（15分や1時間など）の利用を平均化します。平均化すると利用のピークが緩やかになるため、データアプリケーションの適切なパフォーマンスに必要な帯域幅の量に対して誤った印象を与えます。監視を詳細（5分や1分など）に行うことで、より正確な結果が得られます。

もうひとつの便利な方法は、利用の多い時間帯にアプリケーションのパフォーマンスが低下するかそのアプリケーションのユーザーに確認することです。それによって、その時間帯に帯域幅が不足していることがわかります。そのようなネットワークリンクはトラフィックジェネレータでテストすると、予測したビデオ会議の負荷をシミュレートして、既存のアプリケーションのパフォーマンスへの影響を判断できます。このテストはアプリケーションへの負荷がピークになる利用の多い時間帯に行います。業務への影響が懸念される場合は、段階的にテストを行い、テスト用に帯域幅を追加して、アプリケーションのパフォーマンスを監視します。

帯域幅が不足している場合、利用の多い時間帯に重要なリンクのトラフィックの評価を行うと、本来の業務の目的以外のトラフィックを判断できます。このような不要なトラフィックのストリームを検出して除去することで、帯域幅の使用を緩和できる場合もあります。

企業によってトラフィックの組み合わせや需要が異なるため、すべてに受け入れられる利用率を特定するのは困難です。低い方では、利用率の合計が35%であれば、すべてのアプリケーションが問題なく動作します。高い方では、ほとんどすべてのアプリケーションで70%の利用率が限度です。ただし、幅広い選択の余地があります。

電子メールの転送、バックアップ、ダウンロード、データベースの同期など、時間が重要でないバックグラウンドでの作業は負荷の割合が高くても問題ありません。しかし、迅速なレスポンスが求められるHTTPベースのアプリケーション、クライアント/サーバーアプリケーション、CitrixやTelnetなどのキーストロークアプリケーションはそれほど寛大ではありません。QoSの戦略を調整して、こ

のような双方向のアプリケーションの優先順位をバックグラウンドのタスクよりも高く、オーディオ/ビデオのストリームよりも低くすることが効果的な場合もあります（表4参照）。

## 6.0 需要の管理

ネットワークのテストで重要なリンクの帯域幅が不十分であると判断されたら、次のような方法で競合を解消します。

- 帯域幅のアップグレード
- オーディオ/ビデオ会議の需要の削減
- 圧縮/アプリケーション高速化アプリケーション

**帯域幅のアップグレード** - 帯域幅はいつでもアップグレードできます。オーディオ/ビデオ会議の負荷を処理するのに帯域幅が不十分な場合の唯一のソリューションです。

**会議の需要の制限** - 2番目のオプションはビデオ会議の需要を制限することです。これにはさまざまな方法があります。まず、ビデオ会議通話に使用する帯域幅を制限します。高画質には1Mbpsや512Mbpsが必要ですが、384Kbps、あるいは256Kbpsでさえも、ある程度の画質を確保できます。H.264の新しいビデオ圧縮アルゴリズムでは、このような低帯域幅の通話を活用して高画質が得られます。そのため、リモート オフィスで通話に512Kを使用する予定であれば、H.264を導入して通話の帯域幅を384Kまたは256Kにすることで需要を十分に抑えることができます。

需要を削減するための2番目の方法では、通話の量を管理して、各リンクで同時に処理する通話数を制限します。リモート オフィスに3組のビデオ会議ユニットがあるのに、リンクの帯域幅では同時に2つの通話しかサポートできない場合、スケジューリング ポリシーを作成して、同時に2つのシステムのみを使用します。この場合の最も単純なポリシーでは、そのリモート オフィスにはリンクがサポートできる数量と同数のビデオ会議用端末を設置します。

オーディオの需要を削減するには、低帯域幅のコーデック（G.729など）を使用して、低帯域幅のリンクでヘッダを圧縮します。

オーディオ/ビデオ会議のゲートキーパーは、帯域幅の利用の管理にも使用できます。ゲートキーパーには、ネットワークのトポロジに関係する端末のプール間で利用できる最大の帯域幅を割り当てることができます。ゲートキーパーはそのリンクに割り当てられた、利用可能なリアルタイムの帯域幅をそのリンクのすべての通話に対して許可します。ゲートキーパーに割り当てられた帯域幅の値はリンクの容量ではなく、リンクに許可されたリアルタイムのトラフィックの最大量です。リンクの利用がこの最大値に達したら、ゲートキーパーはそれ以上の通話のリクエストを拒否します。

接続拒否が適切でない環境では、オーバーフロー戦略も検討します。リモート オフィスまでのパスが冗長なデータ ネットワークでは、アプリケーション固有のルーティングを使用して、通話量の増加に対応する追加のパスを利用します。もうひとつのアプローチは、ISDN接続を利用して、トラフィックのオーバーフローを必要に応じてISDN接続で処理します。利用が多い時間帯にISDNの利用を監視することで、単純な事例をベースにIPの帯域幅を高コスト効果で追加できる時期を確認できます。

**圧縮** - もうひとつのオプションは既存のデータ トラフィックの圧縮です。データ トラフィックを削

減し、同時にアプリケーションのパフォーマンスを向上させるさまざまな技術を利用した新しいクラスのデータ アプライアンスが市場に参入しています。このようなアプライアンスでは目的別に圧縮、キャッシュ、TCPターミネーション、プロトコルの効率化などの技術を使用しています。状況に応じてデータ ストリームに最適なアプローチを決定するには多少の困難は伴いますが、このようなアプライアンスではリンクにスペースが作られるため、ビデオ会議やオーディオのトラフィックは帯域幅をアップグレードしなくても導入できます。

**スケジューリング** – 帯域幅管理の主な目的は、会議室と会議用ブリッジ ポートのスケジュールと同時に、帯域幅のスケジュールを設定できるようにすることです。帯域幅のスケジューリングによって、来週予定されている幹部会議での通話のために適切な帯域幅を事前に確保して、会議が開始する直前になって臨時のオーディオ/ビデオ会議のユーザーがリンクの帯域幅を最大まで使用しないようにします。中央で管理されたビデオ会議の環境では、このような帯域幅管理は手動で行えます。会議のスケジューラでは、たとえば1時間半の会議中に特定のネットワーク リンクを使用する会議の最大数を超えないように調整できます。この作業には、ビデオ会議の接続に使用するネットワークのトポロジに対応した会議スケジューラが必要です。

より動的な環境でスケジュールに含まれない臨時の通話を利用する場合、高度なアプローチが必要です。ポリコムではPolycom Conference Suite ( PCS ) やReadiManagerをはじめとする端末、MCUポートおよび帯域幅スケジューリングなどのツールを提供しています。

## 7.0 WANのベンダおよび技術

企業の複数のオフィスを接続する場合は通常、WAN ( 広域通信網 ) のサービス プロバイダがサポートします。サービス プロバイダのリンクは企業のネットワークおよびリアルタイムのトラフィックのサポートに統合されます。そのため、サービス プロバイダがアクセス リンクとコア ネットワークに実装しているQoSを詳細に確認し、企業のリアルタイムのストリームの送受信への影響を理解することが重要です。

### 7.1 WANコアのQoS

WANのサービス プロバイダは高速のコア ネットワークを構築し、リンクではOC48 ( 2.4Gbps ) またはOC192 ( 9.7 Gbps ) の速度でデータが転送されます。このデータ転送速度ではキューが短時間で空になるため、ジッターが最小になります。コア ネットワークにQoSを実装せずに、高品質のリアルタイム トラフィックを提供できると主張するベンダもありますが、このようなベンダを利用する前に、慎重に検討する必要があります。

セクション0のオーバー プロビジョニングの説明を思い出してください。このようなベンダの戦略とは、高帯域幅のコアを提供することでパケット ロスとジッターを最小限に抑え、QoSのアルゴリズムを実装するためのオーバーヘッドを解消してサービス品質を向上させます。このようなベンダの多くが、リアルタイムのトラフィックをサポートするのに十分な仕様を確保していることをSLA ( Service Level Agreement ) に明記しています。SLAの読み方と評価の仕方については後で説明します。

さまざまなタイプのストリームにサービス クラスを提供しているWANベンダもいます。このようなベンダではリアルタイムのトラフィックの品質に対してよりよい保証条件を提示している場合もあるため、この文書の読者にはこのようなベンダを探して、そのサポートを受けながらWAN戦略を導

入することをお勧めします。

## 7.2 WANアクセス リンクにおけるQoS

オーディオ/ビデオ会議の2つの端末間には多くのネットワーク リンクがありますが、利用できる帯域幅が最も少ない接続は、おそらくWANのアクセス リンクです。これは、パケットロスやジッターの問題が発生する可能性が最も高いリンクとも言えます。キューイングの問題は、高速リンクが低速リンクに切り替わる位置で、アクセス リンクのいずれの側でも発生します。そのため、このリンクにQoSを実装することは重要です。

企業のLANから送信されるトラフィックは企業のルータで管理されるため、WANで受信するトラフィックの優先順位付けは簡単です。LANで適切な分類が行われていれば、リアルタイムのトラフィックはLANからWANのアクセス リンクに送られたときに優先順位が付けられます。

優先順位の付けられたトラフィックはWANのコアから送信され、アクセス リンクで受信されるため、WANベンダの責任になります。WANベンダがQoSを実装している場合、この機能がサポートされます。WANベンダがコアにQoSを実装していない場合、少なくともコアからアクセス リンクに送信されるトラフィックにQoSが適用されていることを確認します。また、ベンダのコア全体でQoSのマーキングが適用され、送信側ルータのトラフィックでも利用できることも確認します。アクセス リンクからのトラフィックを企業で受信したときに、トラフィックをキャプチャして、QoSのマーキングが破損していないか検証すると効果的です。

## 7.3 SLAの解釈

WANベンダから提供されるSLA (Service Level Agreement) には、可用性とパフォーマンスに関する規定値のほかに、リンクに問題が発生した場合の対応、リンクの問題に対する企業への補償の詳細などが含まれています。ここではパフォーマンスの規定値について説明します。

パフォーマンスの規定値には待ち時間、パケットロス、ジッターも含まれます。待ち時間は光の速度に限界があるため、WAN接続の地理的な距離に影響されます。大陸間を接続する場合、SLAでは国内接続のみの場合よりも待ち時間が長く規定されます。

企業とWANベンダ間のアクセス リンクを通過するトラフィックがSLAの対象になっていることを確認します。SLAによっては、WANベンダのネットワークのエッジ デバイス間のトラフィックのみを保証している場合もあります。

パケットロスとジッターは一定期間の平均値が規定されている場合が大半です。平均する期間は1か月など、長すぎる場合もあるため慎重に検討します。帯域幅の平均化と同様に、平均化することによって、利用の多い重要な時間帯におけるリンクのパフォーマンスを長期的な数値で覆い隠すことができます。たとえば、パケットロスの規定値が1か月に0.1%の場合は次のようになります。

夜間と週末のパケットロス = 0.02%

平日 (利用の多い時間帯を除く) のパケットロス = 0.05%

利用の多い時間帯 (1日2時間) のパケットロス = 1.3%

利用の多い時間帯のパケットロスが0.1%ではなく、1.3%であった場合、ビデオとオーディオに深刻な障害が発生しても、すべてSLAで規定された範囲の値です。適切に規定されたSLAであれば、より短い期間、たとえば1時間などのパフォーマンスが保証されます。

#### 7.4 企業ネットワークからWANのQoSへのハンドオフ

現在導入されているWANの多くで、IETF DiffServのコードポイントのマーキングが認識され、それによってトラフィックは特定のトラフィッククラスにマップされます。企業のQoSのクラスをWANベンダのクラスと統一し、企業内で複数のベンダを利用している場合、異なるWANベンダ間でも一貫性を確保する必要があります。WANクラウドのエッジにQoSのマーキングを再度マップすることで、企業のマーキングはWANのクラスに統一されますが、不必要に行われると複雑化するだけです。QoS戦略を作成するときには、現在および将来利用する可能性のあるWANベンダにそのQoSマーキングの戦略を確認しておく、企業の戦略と円滑に整合できます。

#### 7.5 VPNやインターネット上でのリアルタイムトラフィック

多くの中小企業では現在、VPN (Virtual Private Networks) を利用して、地理的に分散したオフィス間を接続しています。VPNでは公開されたインターネットで暗号トンネルが作成されます。VPNのメリットは専用回線に比べ、コストが大幅に削減できる点にあります。企業のVPNには2つのオフィス間を単一のWANプロバイダで接続している場合と、公開されたインターネットを経由しているために複数のプロバイダとその関連するピアリングポイントを使用する場合の2種類あります。

このようなVPNでリアルタイムのトラフィックを処理することは、QoSでオーバープロビジョニングを使用するのと同じくらい危険です。VPN接続では通常、QoSの機能は提供されません。単一のサービスプロバイダが両側に接続を提供している場合は妥当な品質が得られますが、帯域幅、パケットロス、ジッターについては保証されません。それでもこのアプローチを使用する企業があるのは、アジアの製造工場やヨーロッパの開発センターとのオーディオ通話やビデオ会議ではリスクを正当化でき、ユーザーも障害に対して寛大な場合が多いためです。品質に対する期待が大きく、管理スタッフの会議、営業報告、顧客へのプレゼンテーションまたは画像が重視されるその他の用途で利用する場合、品質低下や通話の障害のリスクがあまりに高いサポートは利用できません。

リアルタイムのトラフィックにインターネットを使用する場合、VPNと同じリスクがあり、制御はむずかしくなります。インターネットで接続する場合、複数の通信事業者が関係する場合も多く、ユーザーは通話のルーティングを制御できません。ホットポテトルーティングのアルゴリズムでは、一方向へのトラフィックに逆方向へのトラフィックとは異なるルートが確保されます。教育機関や研究機関で運良く高帯域幅接続のインターネットを利用できたとしても、低品質の接続になるリスクも高くなります。

### 8.0 ネットワークの検証

IPネットワークの状態を十分に理解する唯一の方法は、IPネットワークでのリアルタイムのサポートをテストすることです。多くのベンダがネットワークをテストするためのツールを提供し、ネットワークを監査するコンサルタント契約も利用できます。それによって、ネットワークがリアルタイムのトラフィックに必要な帯域幅とタイミングを処理できることが直接証明されます。総合的なテストツールではハードウェアまたはソフトウェアのエージェントを使用しますが、それらはネットワーク

内のオーディオやビデオのクライアントの位置にインストールします。これらのエージェントを中央のコンソールで調整して、リアルタイムのテストを実施します。テストでは対象となるネットワークで予測されるリアルタイムのトラフィックが再現され、量や帯域幅を変更してオーディオ通話とビデオ会議通話をシミュレートできます。

この2つのエージェント間のトラフィックが帯域幅を消費して、ネットワークに負荷を与えます。この追加の帯域幅の消費が他のビジネス アプリケーションのパフォーマンスに影響する場合、通知してから帯域幅の詳細な調査を行い、問題を解決します。

各テスト用ストリームを受信するエージェントでは、パケットの待ち時間、パケット ロス、ジッターも調査します。この3つの特性によって、ネットワークでリアルタイムのデータを適時に送信できるかどうかが決まります。テスト用ストリームでリアルタイムのパフォーマンスの低下が確認されたら、分析作業によってパケット ロスやジッターの発生する位置を特定します。

ネットワークを検証すると、高レベルの問題と低レベルの問題の両方が検出されます。高レベルの問題は適切なQoSの有効化、エッジルータでの分類マーキングの紛失、リンクの不十分な帯域幅など、デザイン段階での誤りが原因です。低レベルの問題には、ルータでの旧版のソフトウェアの使用、アクセス リストの不適切な定義、不十分なメモリやCPUリソースなどが含まれます。10Mbpsイーサネット接続の共有やCAT3ケーブルなど、貧弱なLAN接続もリアルタイムのパフォーマンスを低下させる原因になります。特に多いのが、イーサネットのネゴシエーション機能が不十分なためにリンクの一方でハーフ デュプレックス、もう一方でフル デュプレックスを使用している場合です。このような不一致はデータ トラフィックでは問題になりませんが、リアルタイムのトラフィックでは障害が発生します。

**表6 - リアルタイムのテスト パラメータ**

パラメータ	値
パケット ロス	< 0.1%
パケットの待ち時間	<= 100 ms
パケットのジッター	< 40 ms

リアルタイムのトラフィックを導入する前にネットワークを十分に検証し、検証中に検出された問題はリアルタイムのトラフィックを使用する前に解決します。

表6ではオーディオ/ビデオ会議をサポートする企業のネットワークの目標値を示しています。これらの

目標値に一致させるとオーディオ/ビデオ会議に適した品質を確保できます。

パケット ロスは一致させるのが最も難しいパラメータです。多くのベンダ製品では、ここで示したパケット ロスよりもはるかに高い値を持つ高品質のオーディオやビデオを提供しています。これら製品ではそれぞれアルゴリズムを使用して、紛失した情報を補正しています。情報が失われると品質も低下するため、紛失したパケットに相当する時間のオーディオまたはビデオの情報の内容を各製品で予測する必要があります。このようなアプローチでは良好な結果が得られますが、優れたアプローチであれば情報の紛失自体が起こりません。IPネットワークは動的なため、不具合が発生してパケット ロスを補正するアルゴリズムをテストする機会はたくさんあります。まず、適切なネットワークを構築し、パケット ロスの補正は予備的に使用します。

一方向のレスポンスの速度が低下すると、待ち時間は双方向のオーディオ/ビデオ会議通話の品質に影響します。待ち時間が200ミリ秒に達すると遅延の影響が強くなり、ユーザーは相互に中断され、通常の会話の流れを維持できなくなります。200ミリ秒の値は話し手から聞き手に対する遅延を表し、信号のエンコード、送信およびデコードのすべての遅延が含まれます。ネットワークはこの遅延の送信部分にのみ関係します。ネットワークの待ち時間を100ミリ秒以下に制限して、話し手から聞き手への待ち時間を200ミリ秒以下に抑制します。

待ち時間は処理の集中と地理的距離に影響されます。集中化は帯域幅管理とQoSによって管理できますが、地理的距離と光の速度を管理するのは困難です。遠方信号は静止衛星を往復するため、衛星を使用すると遅延が長くなります。グローバルなルーティングでは、場合によっては効果的なルートがあります。たとえば、アジアからヨーロッパへのパスのトラフィックでは、米国を経由する場合があります。同じトラフィックに対してより直線的な地理的ルートを使用する通信事業者があれば、待ち時間の影響をより低く抑えることができます。衛星が不要な単一の大陸内で事業を行う企業では、距離による待ち時間の問題はありません。

ジッターはパケットがネットワークを通過するときのパケット遅延の偏差です。ジッターは通常、パケットの到着時間の間隔として測定されますが、その間隔がまったく同じになることはなく、オーディオストリームのように定期的な間隔で送信されるパケットのストリームでは抑制されます。ジッターの主な原因はキューの遅延です。空に近い状態のキューをパケットが通過すると遅延は短縮されます。その次のパケットが通過するときと同じキューが一杯になっていると、転送まで長時間待機することになります。ジッターはキューの長さで管理します。キューが短い場合、パケットの待ち時間も短くなりますが、トラフィックが集中するとパケットロスが発生します。そのため、ジッターを適切に管理しようとする、パケットロスの問題が起こります。

ジッターはジッターバッファのある受信側の端末で管理します。このバッファでは、正しい間隔で到着したパケットを送信する前に一定時間保留します。ジッターバッファのサイズによって正しい間隔で到着したパケットが保留される時間が決まります。到着が遅れたパケットは正しい時間に「再生」されるよう、ジッターバッファ内をすばやく移動します。ジッターは表6で40ミリ秒と指定されているのは、ポリコムの会議システムの中にジッターバッファが40ミリ秒の製品があるためです。これは、40ミリ秒遅れて到着したパケットでも時間通りに再生されることを意味しますが、40ミリ以上遅れて到着したパケットは廃棄されます。ネットワークではジッターをこの範囲にすると、廃棄されるパケットも抑制され、オーディオやビデオの品質が低下するのを防げます。

## 9.0 ネットワークの監視

ネットワークの監視は継続的にネットワークを検証することです。ネットワークは動的で、変更や追加は毎日行われています。データのネットワークングに使用する管理ツールは一般的に、リアルタイムのサポートに関する問題の追跡および管理には不十分です。これは、正しいパラメータが測定されず、また、十分詳細に測定されないためです。リアルタイムのトラフィックをサポートするネットワークを適切に管理するには、リアルタイムの測定ツールを導入する必要があります。

リアルタイムのトラフィックを処理するIPネットワークの健全性を正しく監視するには、ネットワーク検証ツールには次の機能が必要です。

- ネットワーク全体でのエンド ツー エンドのテスト
- パケットロス、ジッター、待ち時間のテスト
- 詳細な分析のために履歴データを並べ替えたデータベース
- 品質が低下したときの警告に使用するしきい値

VoIPをサポートするネットワーク監視ツールでも、オーディオ通話の品質基準であるMOS ( Mean Opinion Score ) の計算および報告が行えます。同様に、ビデオ会議の画像で認識される品質の基準

値がITUによって策定されています。この計算は近い将来、ベンダ各社のツールに追加されることになるでしょう。通話の品質を直接示すテスト結果をツールで取得できれば、IT管理者はそれを利用してITインフラストラクチャの効率を判断することができます。

ネットワークの監視は目的別に開発されたハードウェアとソフトウェアのツールで行います。多くのベンダがリアルタイムのトラフィックを処理するネットワークのためのテスト ツールを提供しています（付録1参照）。このようなツールでは、ネットワークの周辺に少量のトラフィックを合成するハードウェアまたはソフトウェアのプロンプトを配置して、ネットワークでトラフィックが適切に送信されるか測定します。また、リアルタイムのトラフィック ストリームを受動的に監視して、品質を評価するツールもあります。

もうひとつのアプローチでは、リアルタイム接続に関係するオーディオ/ビデオ会議の端末を利用します。これらのデバイスでは一般的に、離れた場所から送信されたトラフィックの品質が監視され、その情報はCDR（Call Detail Record）に記録されます。品質の情報は端末からのMIBデータを読み込むか、オーディオ/ビデオ通話中の端末への管理用接続を開放することで動的に利用できます。CDR情報を長期的に収集しておく、提供するサービスの全体的な品質の追跡だけでなく、品質の低下と通話に使用する端末または地理的条件の間の相互関係を確認するのにも役立ちます。

これら2つの監視のアプローチを組み合わせると、リアルタイムのトラフィックを処理するネットワークのパフォーマンスを最も的確に示す情報を入手できます。監視戦略を決定および導入することは、リアルタイムの通話の品質を管理する上で重要です。

## 10.0 企業内SLA（Service Level Agreement）

リアルタイムのトラフィックを企業に導入すると、オーディオ/ビデオ チームとネットワーク チームの業務が変化します。ネットワークには突然新しい期待値が適用され、従来のアプローチは機能しなくなります。この変化によって2つのチームの間に問題が発生すると、オーディオやビデオの導入が遅延します。また、問題が発生したときにチーム同士が責任を押し付けあうことで、問題解決が遅れます。

企業内SLAは、移行期間中におけるチーム間の意見の相違を解消することを目的としています。それによって、両チームを成功に導くだけでなく、組織全体がIPネットワークを使用したリアルタイムのトラフィックという新しい現実にも対応しやすくなります。

企業内SLAはオーディオ/ビデオ チームとネットワーク チーム間における合意を示す文書として、リアルタイムのトラフィックをサポートするIPネットワークに必要な機能を定義します。外部のWANプロバイダとの契約書と非常によく似ています。SLAでは、ネットワークに必要な次のパラメータを指定します。

- 帯域幅 - リンク別リアルタイムのトラフィックの予想負荷
- 待ち時間 - 2つの任意のビデオ/オーディオの端末間の最大待ち時間
- パケットロス - 営業時間中の任意の一定時間に許容されるパケットロスの最大値
- ジッター - 営業時間中の任意の一定時間に許容されるジッターの最大値

これらのパラメータの規定には、それぞれの測定を行う時間枠、情報を収集する頻度（1時間ごと、25分ごとなど）が含まれます。平日の利用の多い時間帯で品質を維持できるように詳細を決定します。

上記の4つが最も重要な項目ですが、SLAのその他の項目にはユーザーが問題を報告するプロセスの定義、リアルタイムに関連する問題について2つのチームが連絡する方法などがあります。また、SLAではこれらのパラメータ、特に、リアルタイムの配置が拡張された場合、帯域幅について再度交渉するプロセスも指定します。

SLAの文書ではオーディオ/ビデオ チームがテストするネットワークの詳細も指定します。このSLAに従ってテストを実行するツールがあれば、オーディオ/ビデオ チームは報告された問題がネットワークの障害によるものか、装置の障害によるものかを迅速に判断できます。それによって、責任の追及を避けて迅速に問題を解決できます。

ネットワーク チームに対しては、SLA文書でオーディオ/ビデオ会議をサポートするのに必要なリソースを定義します。IPネットワークを使用した送信は「無料」と思われがちですが、ITチームは新しいアプリケーションのサポートには費用が発生することを知っています。SLA文書で要件を定義することで、ネットワーク チームは規定の遵守に必要なインフラストラクチャのサポートを判断して、幹部に対してサポートに適したリソースを申請できます。

## 11.0 チェックリスト

次のチェックリストはこの文書のまとめとして、現在のネットワークでオーディオ/ビデオの導入にどの程度対応できるかを判断するのに使用します。

- リンクごとにリアルタイムの帯域幅の需要が特定されている
- リンクごとにデータの帯域幅の需要が特定されている（利用率）
- リンクごとに利用可能な帯域幅が算出され、必要に応じてアップグレードしている
- 企業の QoS の分類方法が決定している
- 構内ネットワーク（LAN）に使用する企業の QoS 技術が決定している
- WAN に対する企業の QoS 技術が決定し、WAN ベンダが選択されている
- 企業の QoS のアプローチに対する WAN のサポートをテストで検証している
- リアルタイムのトラフィックをサポートするネットワークのすべての部分に QoS を実装している
- リアルタイムのトラフィックをサポートするネットワークを総合的なテストで検証している
- 帯域幅管理の手法を導入している
- リアルタイムのネットワーク監視機能を導入している
- 企業内 SLA の作成、交渉および署名が完了している

## 12.0 結論

VoIPやビデオ会議のようなリアルタイムのトラフィックを使用するアプリケーションを導入すると、IPネットワーク チームは新しく複雑な問題に対応することになります。導入を成功させるには、リアルタイムのトラフィックの要件を慎重に確認する必要があります。この文書で説明した各段階を確認して、ネットワークの日常の運用に取り入れることで、適切に導入できるだけでなく、アプリケーション、位置、ネットワークに必要な変更を行って、IPネットワークで高品質のサービスを維持できます。

## 13.0 付録 1

Vendors of network tools:

### Network Qualification Tools

- Apparent Networks ([www.apparentnetworks.com](http://www.apparentnetworks.com))
- Clarus Systems ([www.clarussystems.com](http://www.clarussystems.com))
- Ixia Chariot ([www.ixiacom.com](http://www.ixiacom.com))
- NetIQ Vivinet Assessor ([www.netiq.com](http://www.netiq.com))
- Viola NetAssessor ([www.violanetworks.com](http://www.violanetworks.com))

### Network Monitoring Tools

- Brix ([www.brixnetworks.com](http://www.brixnetworks.com))
- Clarus Systems ([www.clarussystems.com](http://www.clarussystems.com))
- Computer Associates ([www.ca.com](http://www.ca.com))
- Corvil Networks ([www.corvil.com](http://www.corvil.com))
- NetIQ Vivinet Manager ([www.netiq.com](http://www.netiq.com))
- Opticom ([www.opticom.de](http://www.opticom.de))
- Prominence ([www.prominencenet.com](http://www.prominencenet.com))
- Qovia ([www.qovia.com](http://www.qovia.com))
- RADcom Performer ([www.radcom.com](http://www.radcom.com))
- Telchemy Vqmon ([www.telchemy.com](http://www.telchemy.com))
- Visual Networks ([www.visualnetworks.com](http://www.visualnetworks.com))
- Volia NetAssessor ([www.violanetworks.com](http://www.violanetworks.com))

### Network Diagnostic Tools

- Computer Associates ([www.ca.com](http://www.ca.com))
- Ixia Chariot ([www.ixiacom.com](http://www.ixiacom.com))
- NetIQ Vivinet Diagnostics ([www.netiq.com](http://www.netiq.com))
- Touchstone Technologies ([www.touchstone-inc.com](http://www.touchstone-inc.com))
- Visual Networks ([www.visualnetworks.com](http://www.visualnetworks.com))
- WildPackets ([www.wildpackets.com](http://www.wildpackets.com))

## 14.0 参考文献

- "DiffServ, The Scalable End-to-End QoS Model", Cisco Systems, 2001, updated Aug. 2005, [http://www.cisco.com/application/pdf/en/us/guest/tech/tk766/c1550/ccmigration\\_09186a00800a3e2f.pdf](http://www.cisco.com/application/pdf/en/us/guest/tech/tk766/c1550/ccmigration_09186a00800a3e2f.pdf)
- "Implementing QoS Solutions for H.323 Video Conferencing over IP, Cisco Systems, Document ID 21662, <http://www.cisco.com/warp/public/105/video-qos.pdf>
- "VoIP over PPP Links with Quality of Service (LLQ /IP RTP Priority, LFI, cRTP)", Cisco Systems, <http://www.cisco.com/warp/public/788/voice-qos/voip-mlppp.pdf>
- "Low Latency Queuing", Cisco Systems, IOS Release 12.0(7)T <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/pqcbwfg.pdf>
- "Voice over IP, Per Call Bandwidth Consumption", Cisco Systems, May 2005, [http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth\\_consume.pdf](http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.pdf)
- "Cisco IOS Quality of Service Solutions Configuration Guide", Cisco Systems, [http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos\\_c/qcfbook.pdf](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/qcfbook.pdf)
- "Blueprint for Convergence", Nortel Networks brochure, <http://www.nortelnetworks.com/solutions/conv/collateral/nn108081-052004.pdf>
- "Introduction to Quality of Service (QoS)", Nortel Networks White Paper, [http://www.nortelnetworks.com/products/02/bstk/switches/bps/collateral/56058.25\\_022403.pdf](http://www.nortelnetworks.com/products/02/bstk/switches/bps/collateral/56058.25_022403.pdf)
- "QoS Recommendations for VoIP", Nortel Networks White Paper, Ralph Santituro
- "Nortel Guide for Planning and Deploying Converged VoIP Networks to Enterprises", Nortel Networks, November 2005, [http://www142.nortelnetworks.com/bvdoc/bestpractice/Nortel\\_Guide\\_for\\_Planning\\_and\\_Deploying\\_Converged\\_VoIP\\_Networks\\_to\\_Enterprises\\_1.2.pdf](http://www142.nortelnetworks.com/bvdoc/bestpractice/Nortel_Guide_for_Planning_and_Deploying_Converged_VoIP_Networks_to_Enterprises_1.2.pdf)

### Proprietary and Confidential

The information contained herein is the sole intellectual property of Polycom, Inc. No distribution, reproduction or unauthorized use of these materials is permitted without the express written consent of Polycom, Inc. Information contained herein is subject to change without notice and does not represent commitment of any type on the part of Polycom, Inc. Polycom and are registered trademarks of Polycom, Inc.

### Notice

While reasonable effort was made to ensure that the information in this document was complete and accurate at the time of printing, Polycom, Inc., cannot assume responsibility for any errors. Changes and/or corrections to the information contained in this document may be incorporated into future issues.

© 2006 Polycom, Inc. All rights reserved. Polycom and the Polycom logo are registered trademarks of Polycom, Inc. All noted Polycom trademarks are the property of Polycom, Inc. in the U.S. and various countries. All other trademarks are the property of their respective owners. All prices are US MSRP. Specifications and pricing subject to change without notice.